AppTec360 Enterprise Mobile Manager & ContentBox

Manual de administrare | Versiunea 5.0 (202110)

Tabla de conținut

- SecurePIM Securitate
- Browser SecurePIM
- Schimb

Gestionarea conexiunilor

- Wi-Fi
  - Configurare proxy
  - Tip de securitate
- VPN
  - Tip VPN
    - VPN
    - VPN per aplicație
  - Configurare proxy
- APN
- Celulare
- Proxy HTTP
- AirPrint
- AirPlay

Gestionarea PIM

- Exchange Active Sync
- eMail
  - Poșta de intrare
  - Poșta de ieșire
- CalDav
- Calendare abonate
- LDAP

Management web

- Clipuri web
- Filtru de conținut web

Gestionarea aplicațiilor

- Enterprise App Manager
  - Aplicații instalate (numai la nivel de dispozitiv)
  - Aplicații obligatorii
    - Opțiuni de instalare
  - Aplicații web

- Restricții și setări
  - Aplicații pe lista neagră / pe lista albă
  - Restricții SysApp
  - App-VPN
  - Setări aplicație
- Magazin de aplicații pentru întreprinderi
  - Aplicații iTunes
  - In-House
- Modul Kiosk
  - Tip de aplicație
    - Pachet
    - URL
  - Setări pentru modul Kiosk

Android Enterprise – Configurare complet gestionată a dispozitivelor

Generalități

- Prezentare generală a profilului grupului (numai la nivel de grup)
- Prezentare generală a dispozitivului (numai la nivel de dispozitiv)
- Revizuirea configurației (numai la nivel de dispozitiv)
- Jurnalul dispozitivului (numai la nivel de dispozitiv)
  - Jurnal de comandă
  - Stări posibile ale comenzii
- Setări dispozitiv
  - Configurare client
  - Wallpaper

Gestionarea activelor (numai la nivel de dispozitiv)

- Informații despre dispozitiv
  - Wi-Fi
- Celulare
- Bluetooth

Managementul securității

- Anti-furt (numai la nivel de dispozitiv)
  - Informații GPS (numai la nivelul dispozitivului)
  - Ștergere și blocare (numai la nivel de dispozitiv)

- Ștergere și blocare (numai la nivel de dispozitiv)
- Mesaj (numai la nivel de dispozitiv)
- Configurația de securitate
  - Codul de acces
  - Criptare
  - AntiVirus
- Sfârșitul duratei de viață (numai la nivel de dispozitiv)
  - Ștergere (numai la nivel de dispozitiv)
- Setări de restricționare
  - Restricții
  - Proprietar dispozitiv AE

Container BYOD

- Android Enterprise
  - Android Enterprise
  - Gmail Exchange
  - Aplicații de sistem AE
  - Codul de acces al containerului
- Samsung KNOX
  - Activare
  - Codul de acces Knox
  - Knox Securitate
  - Knox Exchange
  - Knox eMail
  - Aplicații Knox

Gestionarea conexiunilor

- Wifi
  - Tip de securitate
    - WEP
    - WPA/WPA2
    - 802.1x EAP
- VPN
- Restricții
- APN
- Bluetooth

Gestionarea PIM

- Schimb
- eMail
- AE Gmail Exchange

Gestionarea aplicațiilor

- Enterprise App Manager
  - Aplicații instalate (numai la nivel de dispozitiv)
  - Aplicații de sistem (numai la nivel de dispozitiv)
  - Aplicații obligatorii
  - Aplicații de sistem AE
- Restricții și setări
  - Lista neagră și lista albă
  - Restricții aplicații sistem
    - Aplicații Samsung
    - Aplicații Huawei
  - Setări de gestionare a aplicațiilor
- Magazin de aplicații pentru întreprinderi
  - Playstore
  - In-House
- Magazin Play pentru întreprinderi
- Mod chioșc și lansator
  - Modul Kiosk
  - Lansator AppTec360
  - Setări AppTec360

Telecomandă

- Splashtop
- Teamviewer

Gestionarea conținutului

- Caseta de conținut
- Browser securizat

Configurare Windows 10 PC

Generalități

- Prezentare generală a profilului grupului (numai la nivel de grup)
- Prezentare generală a dispozitivului (numai la nivel de dispozitiv)
- Setări

Prezentare generală

Introducere în AppTec360

Soluția Enterprise-Mobile-Management de la AppTec oferă opțiunea de a gestiona și configura toate dispozitivele mobile cu ajutorul consolei sale intuitive de gestionare. În acest scenariu, serverul EMM poate funcționa fie în mediul dvs. propriu, fie puteți utiliza soluția noastră bazată pe cloud.

Chiar și în ceea ce privește instalarea centralizată a aplicațiilor corporative pe smartphone-uri, ați ajuns la locul potrivit. Cu Enterprise Mobile Manager, puteți distribui aplicațiile și documentele corporative pe dispozitive în câteva secunde sau puteți bloca aplicațiile nedorite cu ajutorul unei liste albe/negre.

Utilizarea dispozitivelor private în cadrul companiilor reprezintă o nouă provocare pentru securizarea smartphone-urilor și tabletelor. Din cauza faptului că angajații doresc să își folosească din ce în ce mai mult smartphone-urile, administratorii IT trebuie să protejeze un număr mare de tipuri diferite de dispozitive. Vă vom ajuta să securizați toate dispozitivele și datele sensibile care sunt stocate pe acestea și să le gestionați dintr-o consolă intuitivă.

Sisteme de operare pentru dispozitive acceptate

AppTec360 oferă suport pentru dispozitive iOS, Android și Windows. Vă rugăm să rețineți că capacitatea funcțională a platformelor menționate poate fi diferită de la un sistem de operare la altul.

- Apple iOS 11.0 sau o versiune mai recentă*
- Apple macOS 10.11 sau o versiune mai recentă
- Google Android 4.4 sau o versiune mai recentă** pe versiunea Cloud
- Google Android 4.1 sau o versiune mai recentă** pe versiunea OnPrem
- MS Windows 10 sau o versiune mai recentă*** (computer de birou, notebook și tabletă)

**Te rugăm să reții că dispozitivele cu iOS 10 sau mai devreme nu pot fi înscrise din cauza schimbărilor drastice făcute de Apple în procesul de înscriere.*

***Dispozitivele pot fi conectate și configurate chiar dacă utilizează o versiune care nu mai este susținută de producător. Vă rugăm să rețineți că este posibil ca anumite funcții să necesite o anumită versiune Android. În cazurile de asistență, urmăm asistența oficială a producătorului. În cazul unor probleme sau erori cauzate de o versiune învechită care nu mai este susținută de producător, ne rezervăm dreptul de a oferi doar asistență limitată.*

****Versiunea Home a Windows nu este suportată din cauza limitărilor sistemului de operare. Vă recomandăm să folosiți o versiune de sistem de operare care este încă acceptată de producător. Nu numai din motive de compatibilitate, ci și de securitate. Prin urmare, vă recomandăm iOS 12 sau o versiune mai recentă și Android 9 sau o versiune mai recentă.*

Directoare LDAP acceptate

- Microsoft Active Directory
- Deschideți LDAP

Informații actualizate despre "Sisteme de operare pentru dispozitive acceptate" și "directoare LDAP acceptate" pot fi găsite aici:

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

Explicarea „Modul supravegheat” pe dispozitivele Apple

Modul supravegheat reprezintă o interfață extinsă pentru dispozitivele iOS.

Pe dispozitivul respectiv configurat, se pot aplica limitări suplimentare, în ceea ce privește funcționalitatea dispozitivului utilizatorului final. Acestea se regăsesc, de asemenea, în manualul administrativ și sunt marcate cu un banner.

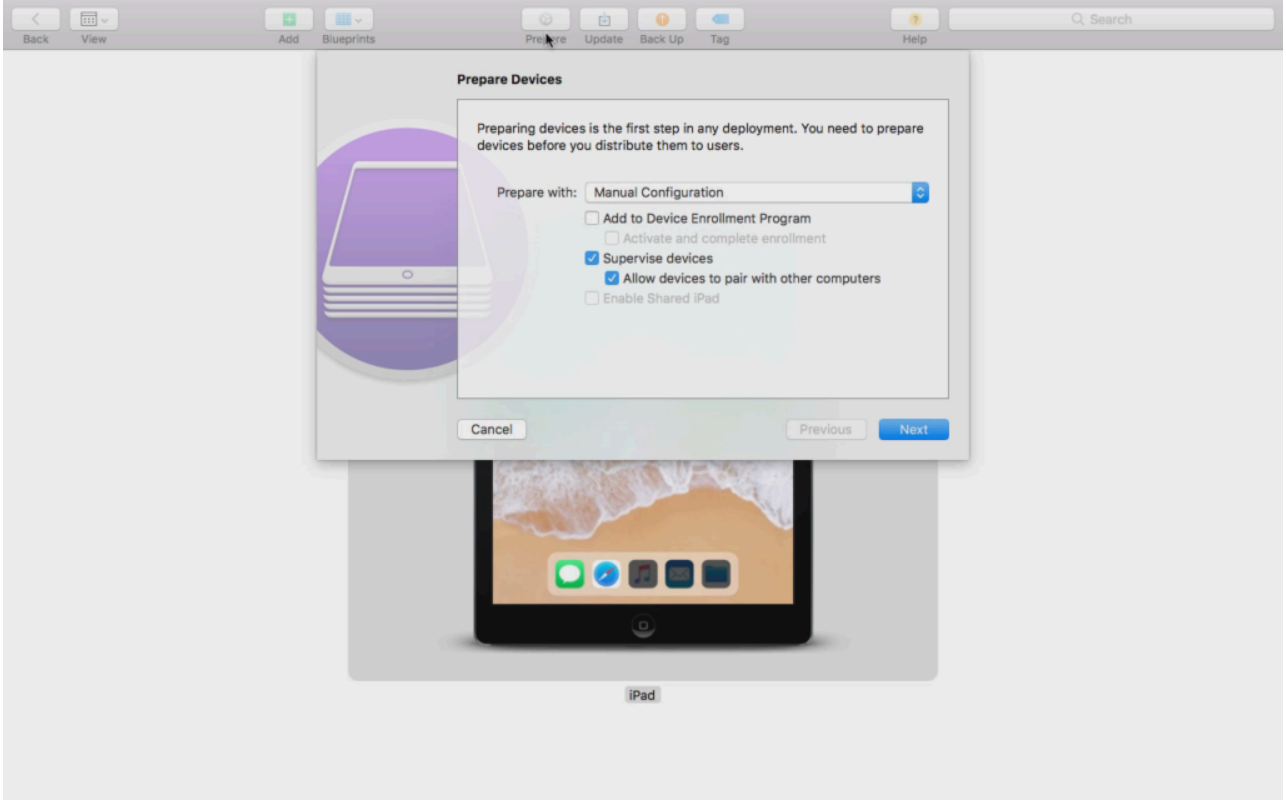
Disponibil în modul supravegheat

Modul "Supervised-Mode" poate fi activat cu ajutorul programului "Apple Configurator". Apple Configurator poate seta setările implicite pe noile dispozitive iOS ca instrument de configurare (prin intermediul interfeței USB).

Instrumentul poate instala nu numai profiluri de configurare, ci și aplicații. Este gratuit, dar necesită un computer Mac.

Activați modul supravegheat

1. Deschideți Apple Configurator



2. Faceți clic pe dispozitiv și alegeți "Pregătiți"
3. Alegeți "Configurație manuală" și "Supraveghează dispozitivele".
4. Faceți clic pe "Următorul"
5. (Opțional) Acum puteți adăuga un server MDM unde va fi înregistrat dispozitivul. Legătura pentru aceasta poate fi găsită în "Setări generale - Configurare iOS - Configurator și URL" Alegeți Organizația dvs. sau creați una nouă.
6. Alegeți Organizația dumneavoastră sau creați una nouă
7. Alegeți care pași trebuie să fie săriți în configurarea inițială și faceți clic pe "Next" (ATENȚIE: Continuarea va șterge dispozitivul dvs.!).

Acum, dispozitivul dvs. va fi pus în modul supravegheat. Acest lucru poate dura câteva minute. După aceea, dispozitivul se va reporni.

Acum dispozitivul este supravegheat!

Adăugarea unui dispozitiv la DEP

De asemenea, puteți adăuga dispozitive la DEP (Device Enrollment Programm) folosind Apple Configurator, dacă dispozitivele dvs. sunt pe iOS 11 sau o versiune mai recentă.

Mai multe informații despre DEP: https://www.apple.com/business/dep/

Urmați aceiași pași ca și cum ați supraveghea un dispozitiv și bifați în plus "Add to Device Enrollment Programm". Vi se vor solicita datele de autentificare DEP dacă nu v-ați mai autentificat în DEP cu Apple Configurator.

După finalizarea procesului, dispozitivul poate fi găsit în serverul DEP "Dispozitive adăugate de Apple Configurator 2". Acum puteți utiliza acest server și îl puteți conecta la consola de administrare sau puteți transfera dispozitivul la un server deja existent.

Ați adăugat cu succes un dispozitiv la DEP!

Explicații privind Android Enterprise

Ce este Android Enterprise?

Android Enterprise oferă un control mai bun al dispozitivelor de lucru care sunt gestionate cu un MDM. Acest lucru permite administratorilor fie să aibă control deplin asupra dispozitivelor android, fie să separe datele companiei de datele private de pe dispozitivele container. În plus, Android Enterprise permite o înscriere mai ușoară a dispozitivelor și o distribuție ușoară a aplicațiilor.

Care sunt cerințele pentru a utiliza Android Enterprise?.

Android Enterprise poate fi utilizat gratuit de către toată lumea. Trebuie doar să conectați un cont Google la MDM pentru a activa toate caracteristicile Android Enterprise. Mai multe informații despre acest lucru pot fi găsite în secțiunea Android Enterprise.

Android Enterprise poate fi utilizat pe dispozitive cu Android 5.1 sau o versiune ulterioară, cu excepția profilului de lucru îmbunătățit (a se vedea mai jos). Recomandăm cel puțin Android 7 sau o versiune superioară pentru o înscriere mai ușoară sau Android 11 pentru a utiliza toate funcțiile disponibile.

Care sunt modurile disponibile cu Android Enterprise?

Există 3 moduri diferite de utilizare atunci când utilizați Android Enterprise.

AE Dispozitiv gestionat integral (gestionat pentru muncă): Un dispozitiv complet gestionat care este utilizat numai pentru muncă. Aceasta permite administratorului controlul deplin asupra dispozitivului. Aceasta nu permite o utilizare privată a dispozitivului. Pentru a înscrie dispozitivele în acest mod, dispozitivele trebuie resetate și înscrise cu un cod QR (consultați AE Enrollment) sau înscrise prin Knox Enrollment sau Zero Touch.

Container AE BYOD: Containerul BYOD (bring your own device) permite utilizatorilor să acceseze datele companiei pe telefonul lor privat într-un container separat. În acest mod, aplicațiile private nu pot vedea datele și aplicațiile companiei și viceversa. Pentru a înscrie dispozitivele în acest mod, trebuie descărcată aplicația AppTec și poate fi scanat un cod QR. Creați un dispozitiv în consolă și selectați "AE Container (BYOD & Enahnced Work Profile)" ca tip de dispozitiv. Faceți clic pe codul QR de pe dispozitivul nou generat pentru a obține codul QR și setați primul comutator la "Legacy & BYOD".

AE Enhanced Work Profile: (necesită Android 11 sau o versiune mai recentă) În timp ce containerul BYOD menționat anterior aduce datele companiei pe un dispozitiv privat, Enhanced Work Profile face același lucru, dar pentru un dispozitiv deținut de companie. Acesta creează același container, dar oferă administratorului un control puțin mai mare asupra dispozitivului, astfel încât utilizatorul nu poate elimina pur și simplu MDM-ul de pe dispozitiv. Creați un dispozitiv în consolă și selectați "AE Container

(BYOD & Enahnced Work Profile)" ca tip de dispozitiv. Faceți clic pe codul QR de pe dispozitivul nou generat pentru a obține codul QR și setați primul comutator la "Profil de lucru îmbunătățit". Acest cod QR poate fi scanat după resetarea dispozitivului și apăsarea de 6 ori pe ecran, după cum se explică în Metoda 1 din AE Enrollment.

Cum pot atribui aplicații dispozitivelor Android Enterprise?

Mai întâi trebuie să aprobați aplicațiile pe care doriți să le utilizați în Setări generale → Gestionare aplicații → AE Play Store → Aplicații Play Store. După ce aprobați o aplicație, o puteți atribui listei de aplicații obligatorii → din profilul dvs. făcând clic pe "+" și selectând aplicația din fila "AE Play Store". Acest lucru va descărca și instala aplicația în mod automat. Nu este necesar niciun cont Google pe dispozitiv și utilizatorul nu trebuie să confirme sau să permită acest lucru.

Încărcați propriile aplicații în Magazinul Google Play

Este posibil să vă încărcați aplicațiile interne în Google Play Store. În acest fel, puteți beneficia de diferite avantaje, cum ar fi mecanismul de actualizare al Magazinului Play.

Pentru a face acest lucru, aveți nevoie de un cont de dezvoltator Google. Conectați-vă utilizând Google Play Console(https://play.google.com/apps/publish)

Faceți clic pe "Creare aplicație". Alegeți limba implicită și titlul aplicației.

Create application

Default language *

English (United Kingdom) – en-GB ▾

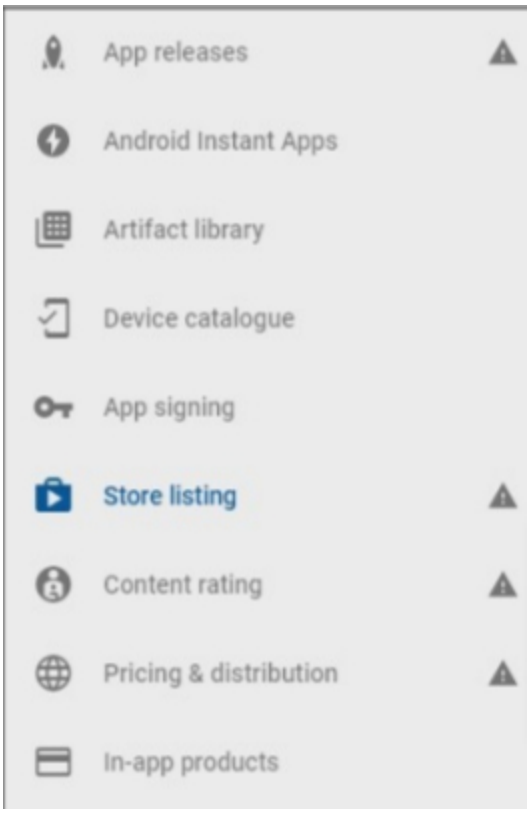
Title *

AppTec Demo App

15/50

CANCEL CREATE

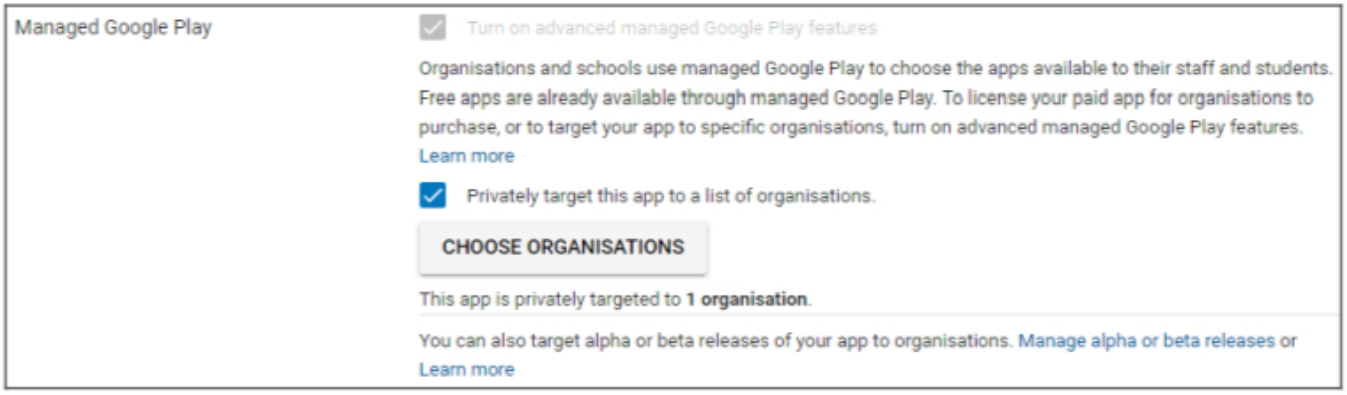
Pe pagina următoare vi se va cere să introduceți diferite detalii despre aplicația dvs.



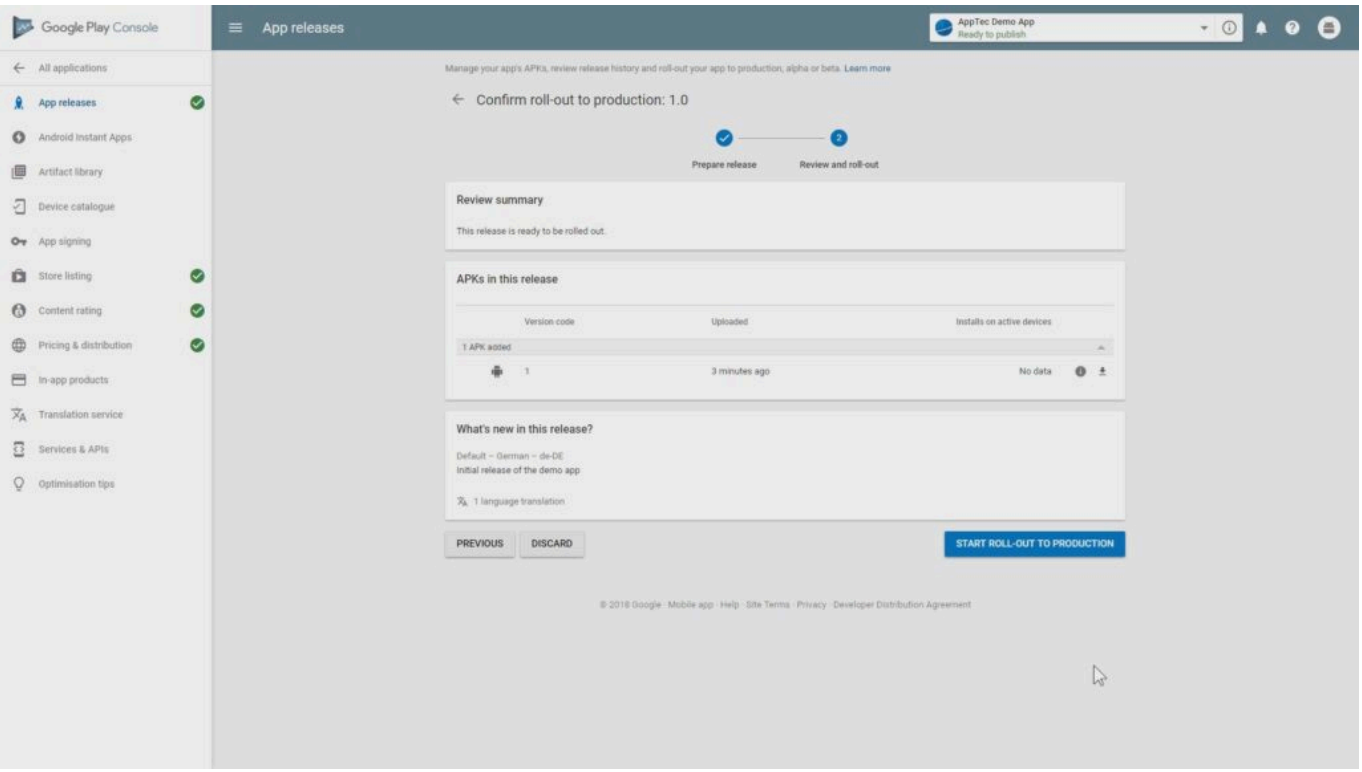
După ce ați introdus toate detaliile, veți vedea diferite simboluri de indiciu în partea stângă.

Treceți cu privirea peste ele pentru a vedea care sunt pașii rămași și urmați-i în orice ordine doriți.

Notă: Asigurați-vă că bifați cele două căsuțe de selectare de la "Gestionat Google Play" sub "Prețuri și distribuție". În caz contrar, aplicația va fi publică și va putea fi accesată de toată lumea. De asemenea, asigurați-vă că alegeți țara pentru distribuție.



După ce ați finalizat fiecare etapă, puteți merge la "App releases". Faceți clic pe "Revizuire" și pe "Start Roll-Out to Production" pentru a finaliza proiectul și a publica aplicația.



Poate dura ceva timp până când aplicația este disponibilă în Magazinul Play. După ce procesul este finalizat, puteți căuta aplicația în magazinul Play for Work și o puteți aproba. După aceea, puteți pur și simplu să atribuiți aplicația dispozitivelor utilizând consola EMM, la fel cum faceți cu alte aplicații.

Cerințe și instalare

Cerințe

Cerințe de sistem

Dispozitivul virtual este disponibil în format de virtualizare deschis (VMWare, VirtualBox, Citrix Xen Server) și ca fișier comprimat .vhdx (Hyper-V)*.

*Nota: Mașina trebuie să fie creată cu generația 1 atunci când se utilizează Hyper-V.

Discul virtual are o dimensiune țintă de 20 GB, iar mașina necesită 4 GB de RAM.

Aparatul este bazat pe Debian 9 64bit

Actualizați mașina importată la cea mai recentă compatibilitate (de exemplu, în VMWare) și asigurați-vă că tipul de sistem de operare al mașinii este setat corect în hipervizor.

Cheie de licență

Pentru a activa și instala cu succes serverul, veți avea nevoie de un fișier de licență valabil. Puteți obține unul direct de la AppTec360 și/sau de la revânzătorul respectiv.

Rezoluția adreselor IP și DNS

Dispozitivul AppTec360 trebuie să poată fi accesat de către dispozitivul care utilizează numele de gazdă pentru care a fost emisă licența.

Pentru a înscrie dispozitivele Windows 10, trebuie, de asemenea, să configurați un subdomeniu suplimentar sub forma "enterpriseenrollment.", direcționat către dispozitiv.

Certificatul SSL

Deoarece toate conexiunile către și de la dispozitive trebuie să fie securizate utilizând SSL, aveți nevoie de un certificat valabil pentru numele de gazdă emis de o autoritate de certificare în care dispozitivul are încredere. Cheia privată pentru certificat trebuie să fie încărcată fără protecție prin parolă. În majoritatea cazurilor, este necesar un certificat intermediar pentru CA pentru ca dispozitivele să recunoască certificatul serverului.

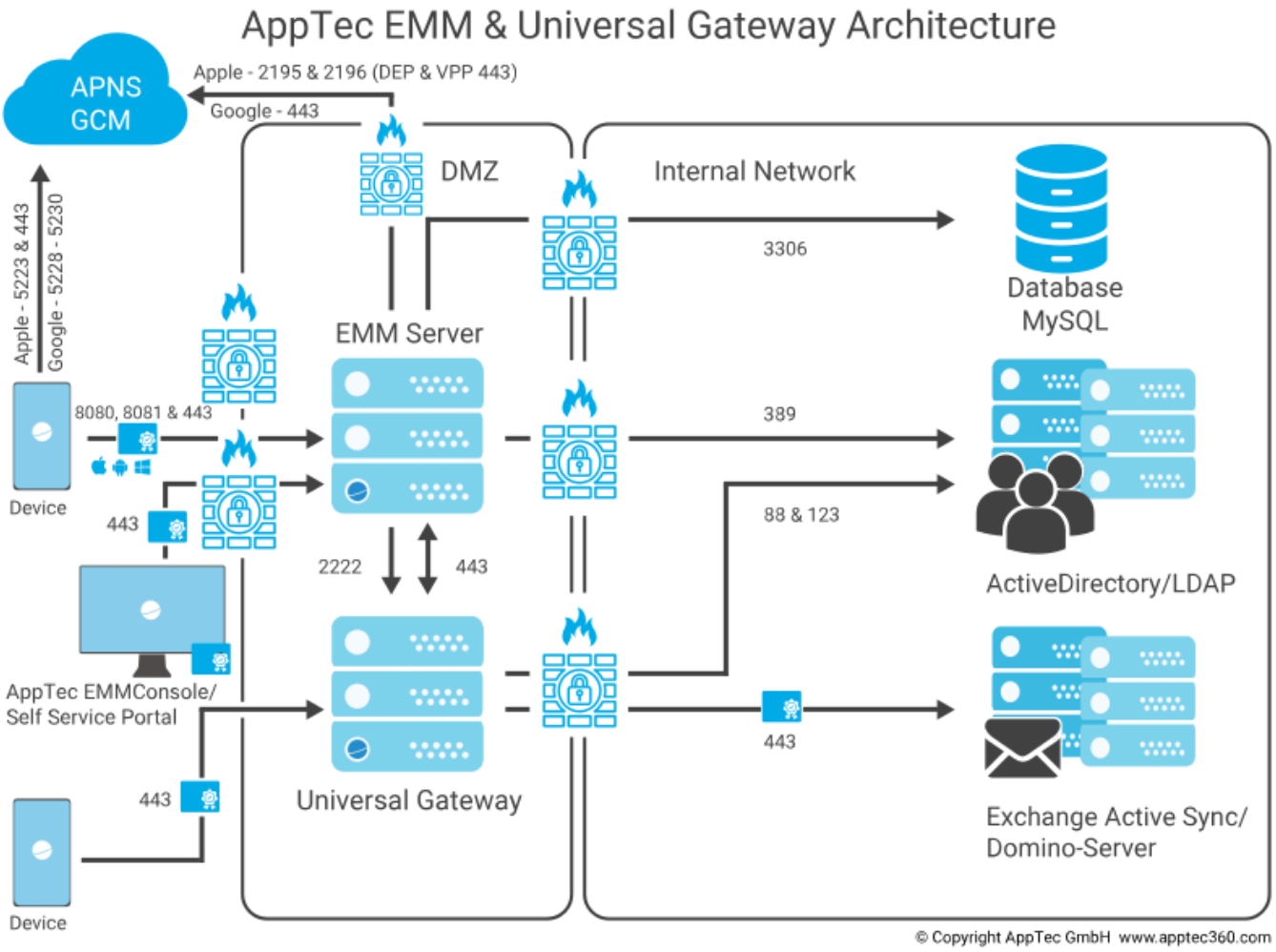
Dispozitivele Windows 10 vor necesita un certificat specific pentru subdomeniul dvs. enterpriseenrollment.

Începând cu versiunea 202104 a dispozitivului, puteți utiliza și certificatele Let's Encrypt, care sunt generate automat (descrise în Pasul doi - Certificat SSL).

Server SMTP

Este necesar un server de e-mail și/sau un releu de e-mail, pentru a permite AppTec360 EMM să trimită e-mailuri (de exemplu, pentru înregistrarea dispozitivului și validarea contului).

Reguli Firewall



Această diagramă arată ce conexiune este necesară în funcție de serviciile pe care doriți să le utilizați.

Pentru o descriere mai detaliată, consultați tabelul de pe pagina următoare.

Orice (extern/Dispozitive)	→	**Aparat AppTec360 / emmconsole.com**
Porturi	443	Management, Enterprise AppStore și Windows Phone Communication
	8080	Comunicare Android & iOS
	80	Prima instalare a Let´s Encrypt. Utilizează 443 după aceea.
Orice (Dispozitive)	→	**Orice (extern)**
Porturi	5223, 443	Apple Push Service, trebuie să fie accesibil fără proxy, 443 ca Fallback, vezi https://support.apple.com/en-us/HT203609
	5228-5230	Serviciul Android Push (FCM), trebuie să poată fi accesat fără proxy
Aparat AppTec360	→	**Controlor de domeniu**
Porturi	389, (LDAPS 636)	Sincronizarea utilizatorilor cu LDAP
Aparat AppTec360	→	**Orice**
Port	443	Utilizat pentru serviciul Android Push (GCM) Căutare în AppStore / Play Store
Aparat AppTec360	→	**emmconsole.com**
Porturi	443	AppTec360 Appliance Updates, generarea certificatului APNS
Aparat AppTec360	→	**Rețeaua Apple (17.0.0.0/8)**
Porturi	2195, 2196	Serviciul Apple Push și Serviciul de feedback
	443	DEP & VPP

Actualizări de securitate

Sistemul de operare Debian trebuie actualizat în mod regulat pentru a obține cele mai noi soluții de securitate. Cu toate acestea, asigurați-vă că nu faceți manual actualizarea la o versiune majoră mai nouă a Debian. Atunci când AppTec360 EMM este compatibil cu o versiune majoră mai nouă, vom adăuga o modalitate de actualizare într-o actualizare a dispozitivului.

Parole implicite ale dispozitivului virtual

Autentificare utilizator (Autentificarea rădăcină este dezactivată. Utilizați "sudo" pentru sarcinile de administrare)

apptec

Parola de conectare

apptec

Utilizator rădăcină MySQL

rădăcină

Parolă rădăcină MySQL

apptec

Utilizator implicit MySQL

AppTec

Parola implicită a utilizatorului MySQL

AppTec

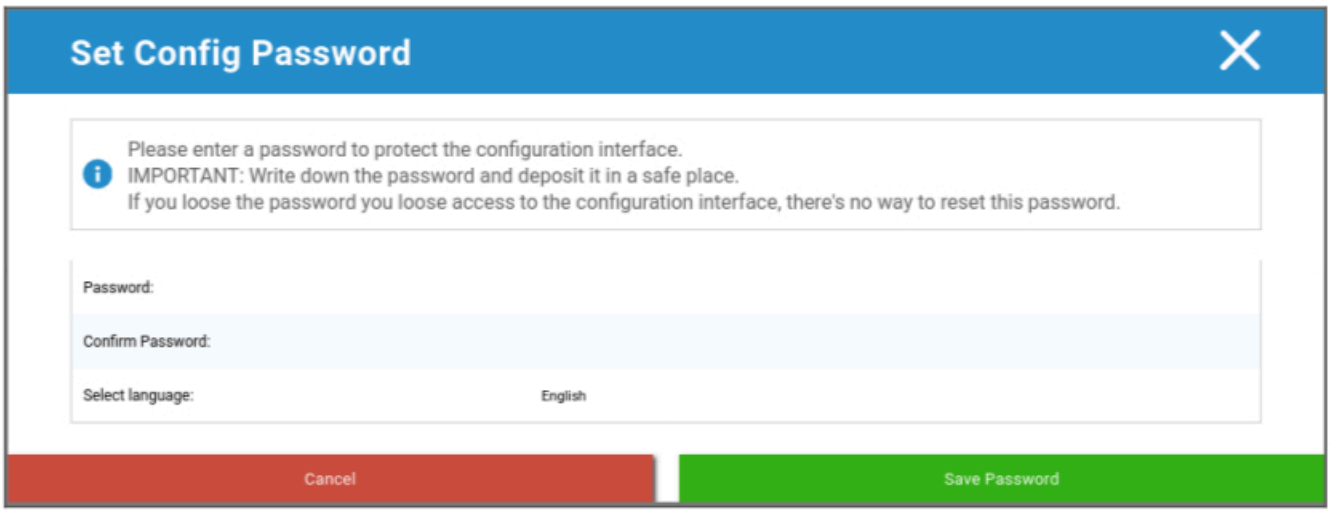
Configurarea dispozitivului virtual

Important: Înainte de a începe configurarea aplicației virtuale, rezoluția ecranului trebuie setată la cel puțin 1280 x 800 pixeli.

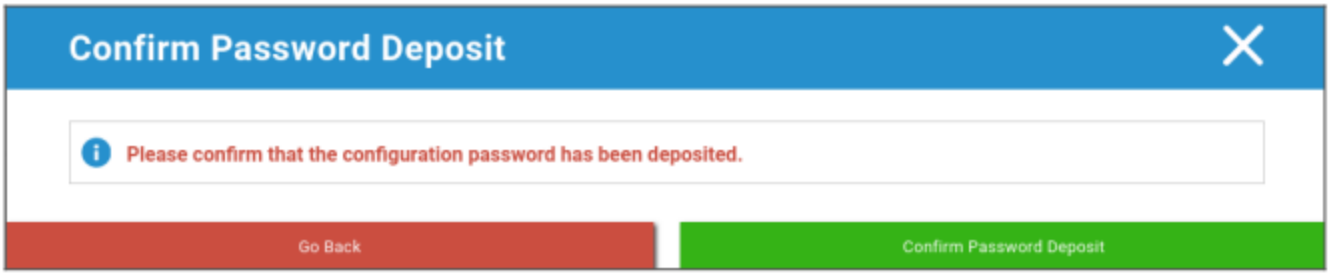
După conectarea la dispozitiv, Firefox ar trebui să pornească automat și să afișeze interfața de configurare.

Pregătire

Mai întâi trebuie să furnizați o parolă pentru interfața de configurare. Această parolă este utilizată pentru a cripta toate informațiile și fișierele introduse în interfața de configurare. Aici puteți seta, de asemenea, limba în care trebuie să fie afișată interfața (poate fi modificată ulterior).

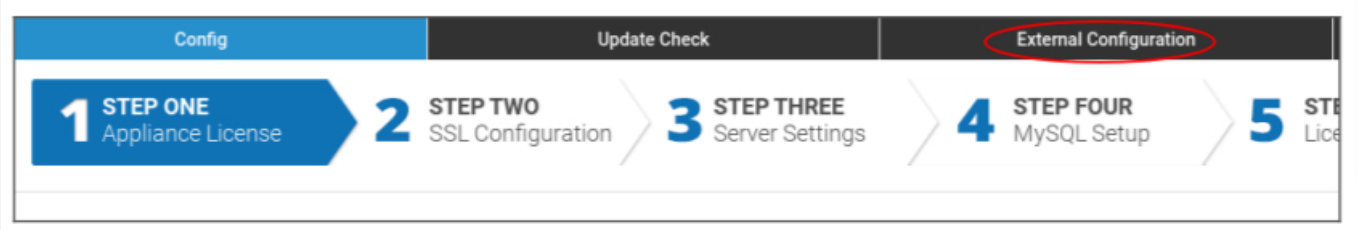


Parola poate fi resetată numai de AppTec360 Support, așa că asigurați-vă că o depozitați într-un loc sigur și confirmați fereastra pop-up viitoare.



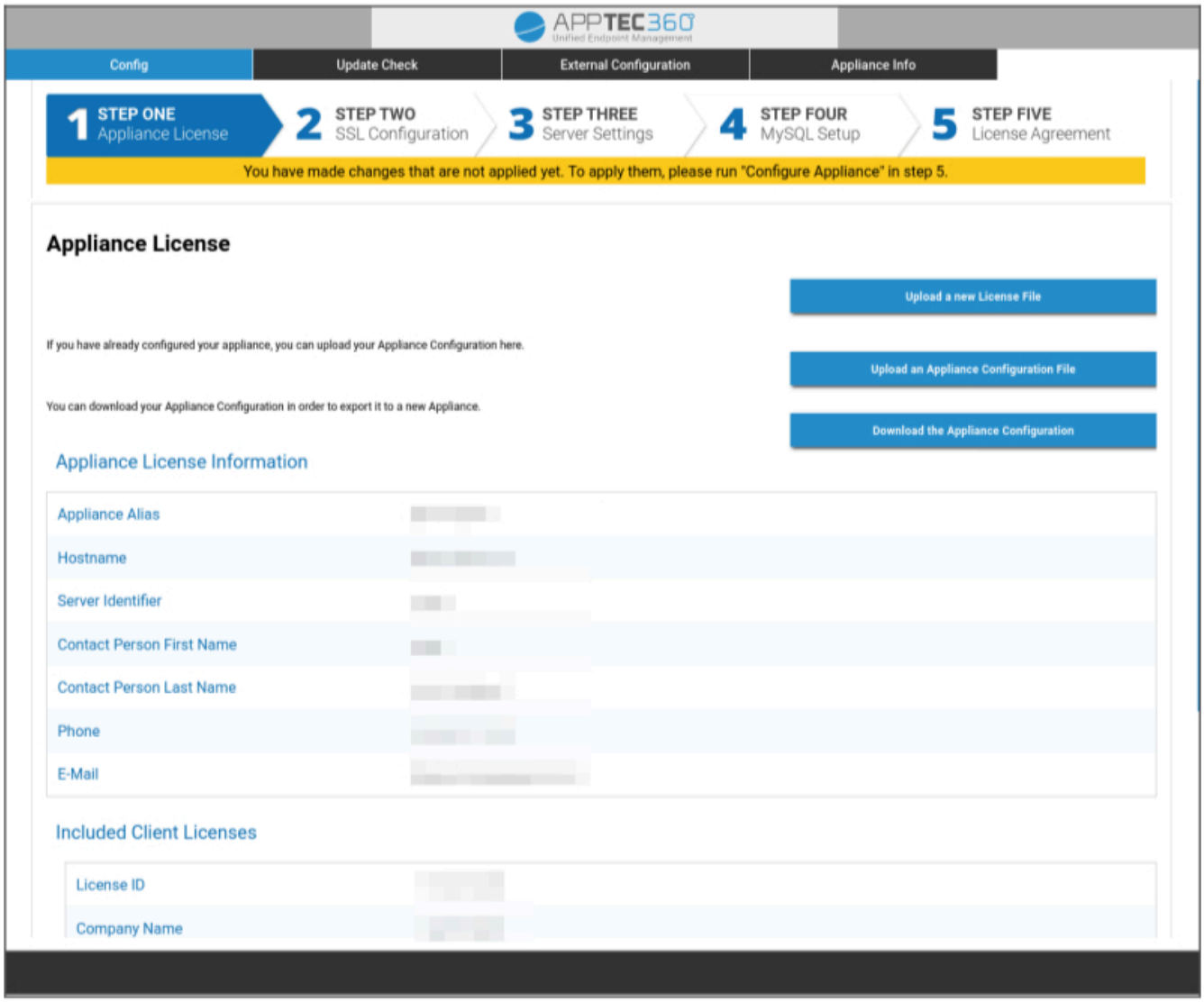
Configurare de la o gazdă externă

Pentru a ușura procesul de configurare, puteți face pagina de configurare accesibilă de la distanță. Pentru a face acest lucru, urmați pașii din "Configurare de la o gazdă externă".



Primul pas – Licența aparatului

1. Vă rugăm să încărcați fișierul de licență pe care l-ați primit de la AppTec.
2. Dacă fișierul de licență a fost încărcat cu succes, puteți vedea informațiile privind licența aparatului ca în captura de ecran de mai jos.



Pasul doi – Certificatul SSL

Puteți fie să utilizați configurarea automată a certificatelor utilizând Let's Encrypt, fie să furnizați singur certificatele (consultați SSL-Certificate pentru mai multe informații).

Automată

Certificatul va fi generat automat utilizând serviciul Let's Encrypt.

AppTec360 EMM utilizează provocarea HTTP-01 pentru validarea domeniului, ceea ce înseamnă că portul HTTP trebuie să fie deschis de la internet pentru prima solicitare a unui certificat. Solicitările ulterioare de reînnoire pot fi validate prin HTTPS.

Comutați butoanele radio la "Automatic (Let's Encrypt)" și apăsați "SAVE VALUES". Certificatul va fi solicitat automat atunci când se aplică configurația din Pasul cinci - Contract de licență. Certificatul va fi reînnoit automat dacă este necesar și veți primi un e-mail dacă certificatul este pe cale să expire (ceea ce implică faptul că reînnoirea ar fi putut eșua).

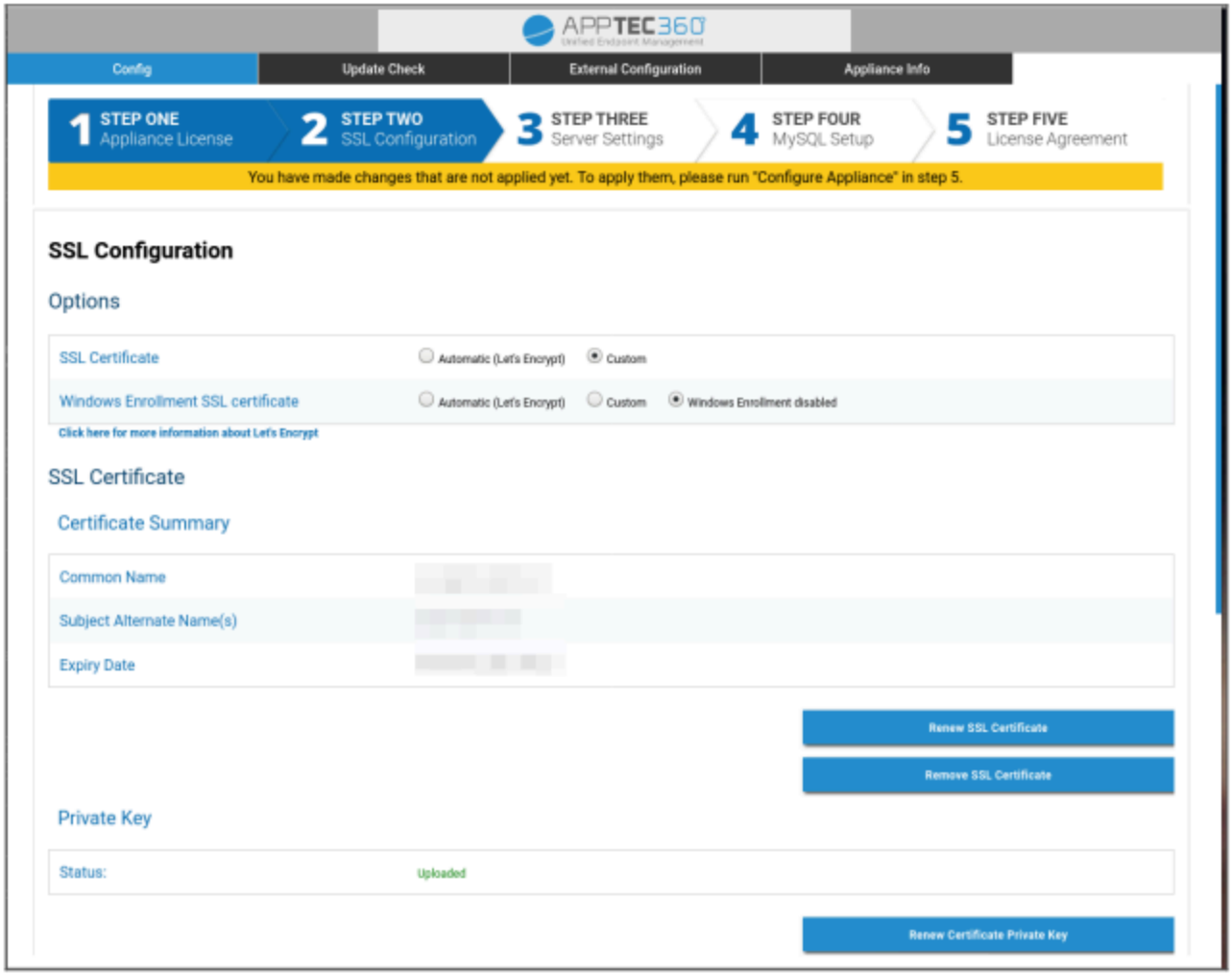
Personalizat

1. Încărcați certificatul SSL pentru numele dvs. de gazdă licențiat. Puteți vedea numele de gazdă în Pasul 1 - Licența dispozitivului.

2. De asemenea, vă rugăm să încărcați cheia privată pentru certificat și, dacă este necesar, certificatul intermediar.

Important: Cheia nu trebuie să fie protejată prin parolă. Dacă este protejată, vă rugăm să eliminați parola înainte de a o încărca.

Indicație: Dacă doriți să utilizați și dispozitive Windows 10, trebuie să activați "Windows Enrollment SSL certificate" și să încărcați certificatul, cheia privată și certificatul intermediar pentru subdomeniul dvs. (descris în Descărcarea adresei IP și a rezoluției DNS) în partea de jos a paginii.



Pasul trei – Setări server

1. Vă rugăm să introduceți o adresă de e-mail pentru asistență globală. Această adresă va fi utilizată în e-mailurile către utilizatorii dvs., astfel încât aceștia să știe pe cine să contacteze în cazul unor probleme legate de dispozitivul lor.
2. Furnizați setările de e-mail care vor fi utilizate de sistem pentru a trimite e-mailuri. Setările vor fi utilizate pentru a trimite e-mailuri utilizatorului și, de asemenea, pentru a trimite rapoarte de erori și solicitări de caracteristici la"support@apptec360.com".După salvarea setărilor de e-mail, trebuie să le verificați făcând clic pe "Test E-Mail Configuration" și urmând instrucțiunile.

Pasul patru – Configurarea MySQL

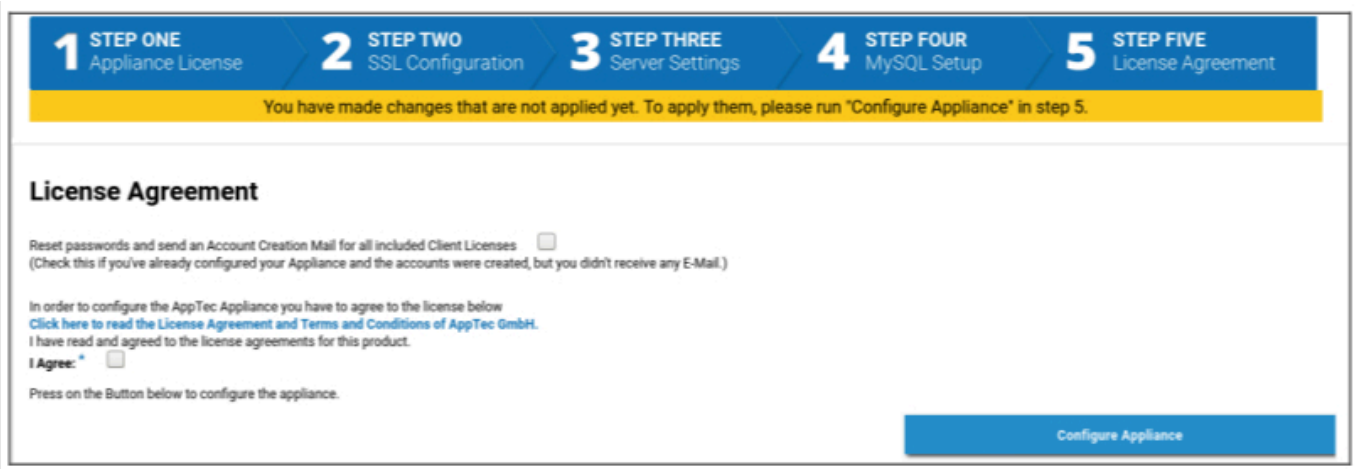
1. Dacă doriți să utilizați baza de date internă, puteți sări peste acest pas. În caz contrar, puteți introduce informațiile de conectare pentru serverul dvs. de baze de date externe.


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)

Pasul cinci – Acordul de licență

1. Vă rugăm să citiți contractul de licență.
2. Bifați "I Agree" și apăsați butonul "Configure Appliance" pentru a aplica setările.

Indicație: Va trebui să executați "Configure Appliance" de fiecare dată când modificați setările în cei 5 pași pentru a aplica setările.



Felicitări!

Ați finalizat configurarea dispozitivului virtual.

Un e-mail cu parola dvs. a fost trimis la adresa pe care ați furnizat-o pentru licență (vizibilă la "Licențe client incluse" în Pasul unu - Licența aparatului).

Acum vă puteți conecta la consolă folosind această parolă și adresa de e-mail pe care ați primit-o.

Pentru a vă conecta la consolă, vă rugăm să introduceți numele de gazdă al consolei în bara de adrese a browserului.

Puteți găsi numele de gazdă al aparatului dvs. în Pasul 1 - Licența aparatului.

Rezolvarea problemelor

1. Nu ați primit un e-mail la configurarea dispozitivului în Pasul cinci - Acord de licență:

Asigurați-vă că setările de e-mail din Pasul trei - Setări server sunt corecte. Pentru a retrimite parola, verificați "Reset passwords and send an Account Creation Mail for all included Client Licenses" în Pasul cinci - Contract de licență înainte de a executa din nou "Configure Appliance".

2. Ați primit o eroare în ceea ce privește Let's Encrypt în timpul configurării din Pasul cinci - Acordul de licență:

Asigurați-vă că aparatul este accesibil prin numele său de domeniu pe portul 80. Let's encrypt scrie, de asemenea, un jurnal în "/var/log/letsencrypt", care ar putea ajuta la depanarea ulterioară.

Recomandări de securitate

Este recomandat să efectuați următorii pași pentru a vă securiza dispozitivul AppTec360.

Acesta nu este un set complet de instrucțiuni, este doar o recomandare pentru o configurație de bază.

- Modificarea parolei pentru utilizatorul AppTec360
- Schimbați parola pentru utilizatorii MySQL "root" și "AppTec" și actualizați Pasul patru - Configurarea MySQL în consecință
- Modificați portul implicit al serverului SSH
- Blocați portul 80 în consola dvs. și nu permiteți traficul HTTP de intrare, utilizați numai HTTPS. Odată configurat, este posibilă și o configurare externă prin HTTPS.
- Restricționați accesul la interfața de administrare doar pentru anumiți Ips în partea de jos a Pasului trei - Setări server
- Configurați firewall-ul

Setări generale

Prezentare generală a contului

Informații despre cont

Prezentare generală

Aici, puteți vedea o prezentare generală a contului dumneavoastră AppTec360.

Numele companiei	Numele companiei dvs.
Data creării	Data creării contului dvs.
Tip de licență	Plătit = licență plătită Gratuit = licență neplătită Notă: Conturile de pe un dispozitiv OnPremise vor fi întotdeauna afișate ca fiind plătite din motive tehnice
Identificator client	Identificatorul contului dvs. (acesta NU este numărul dvs. de client)
Data expirării licenței	Data expirării licenței dumneavoastră AppTec360
Licență ContentBox	Gratuit = licență gratuită pentru 25 de dispozitive Plătit = licență plătită pentru x dispozitive
Lansator	Arată dacă puteți utiliza sau nu lansatorul personalizat pentru Android
Dispozitive	Număr de licențe utilizate în prezent / total licențe
Persoană de contact	Persoană de contact furnizată
Telefon	Numărul de telefon furnizat
eMail*	Adresa de e-mail furnizată
Utilizator rădăcină	Root Utilizatori care se pot conecta
Versiunea software	Versiunea curentă a software-ului

**Nota: Adresa de e-mail afișată aici este cea pe care ați introdus-o pentru a înregistra contul. Pe baza acesteia, se va crea un utilizator în arborele utilizator/dispozitiv și acesta poate fi modificat. Editarea*

acestui utilizator va modifica adresa de e-mail pe care trebuie să o utilizați pentru a vă conecta, dar nu și informațiile din prezentarea generală a contului .

Raport de eroare

Un raport de eroare poate fi trimis direct către asistență pentru a raporta probleme sau erori și include informații și jurnale despre contul și configurarea dvs.

Subiect	Subiectul raportului de eroare. Includeți un număr de bilet dacă doriți să adăugați acest lucru la un bilet de asistență existent.
Comportamentul așteptat	Descrieți în detaliu ce ați făcut și ce vă așteptați să se întâmple
Comportamentul real	Descrieți în detaliu ce se întâmplă exact. Vă rugăm să citați mesajele de eroare EXACT. De asemenea, este util dacă adăugați capturi de ecran la atașament.
La ce oră ați întâmpinat problema?	Vă rugăm să precizați momentul în care ați primit un anumit mesaj de eroare/problemă. În cel mai bun caz, includeți și secundele, de ex. 18:55:27
Problema poate fi reprodusă? Dacă da, cum (în detaliu)?	Descrieți în detaliu modul în care puteți reproduce problema.
Această caracteristică a funcționat anterior așa cum vă așteptați? Dacă da, până când?	Lăsați gol dacă nu știți.
Au fost efectuate modificări specifice ale sistemului înainte de apariția acestei probleme? Dacă da, ce modificări (în detaliu)?	Menționați întotdeauna care a fost ultima dvs. schimbare sau acțiune înainte de apariția problemei, chiar dacă considerați că este irelevantă.
Dacă este cazul: Ce modele de dispozitive și versiuni ale sistemului de operare sunt afectate?	Vă rugăm să menționați întotdeauna versiunea exactă a sistemului de operare (de exemplu, iOS 14.7.1 sau Android 11)
Dacă este cazul: Care este adresa IP publică sau/și numărul de serie al dispozitivului?	Numiți cel puțin unul, chiar dacă toate dispozitivele sunt afectate.
Includerea fișierelor jurnal	Bifați această opțiune pentru a trimite fișierul jurnal împreună cu raportul de eroare. Este recomandat să faceți acest lucru.
Obțineți starea VPP curentă de la Apple și includeți-o în raportul de eroare	Include informații despre atribuirea licențelor VPP. Activați această opțiune numai dacă vi se solicită acest

	lucru de către asistență sau dacă problema dvs. este legată de VPP.
Atașament	Atașați orice fișier care ar putea fi util (de exemplu, capturi de ecran ale unui mesaj de eroare)

Cerere de caracteristici

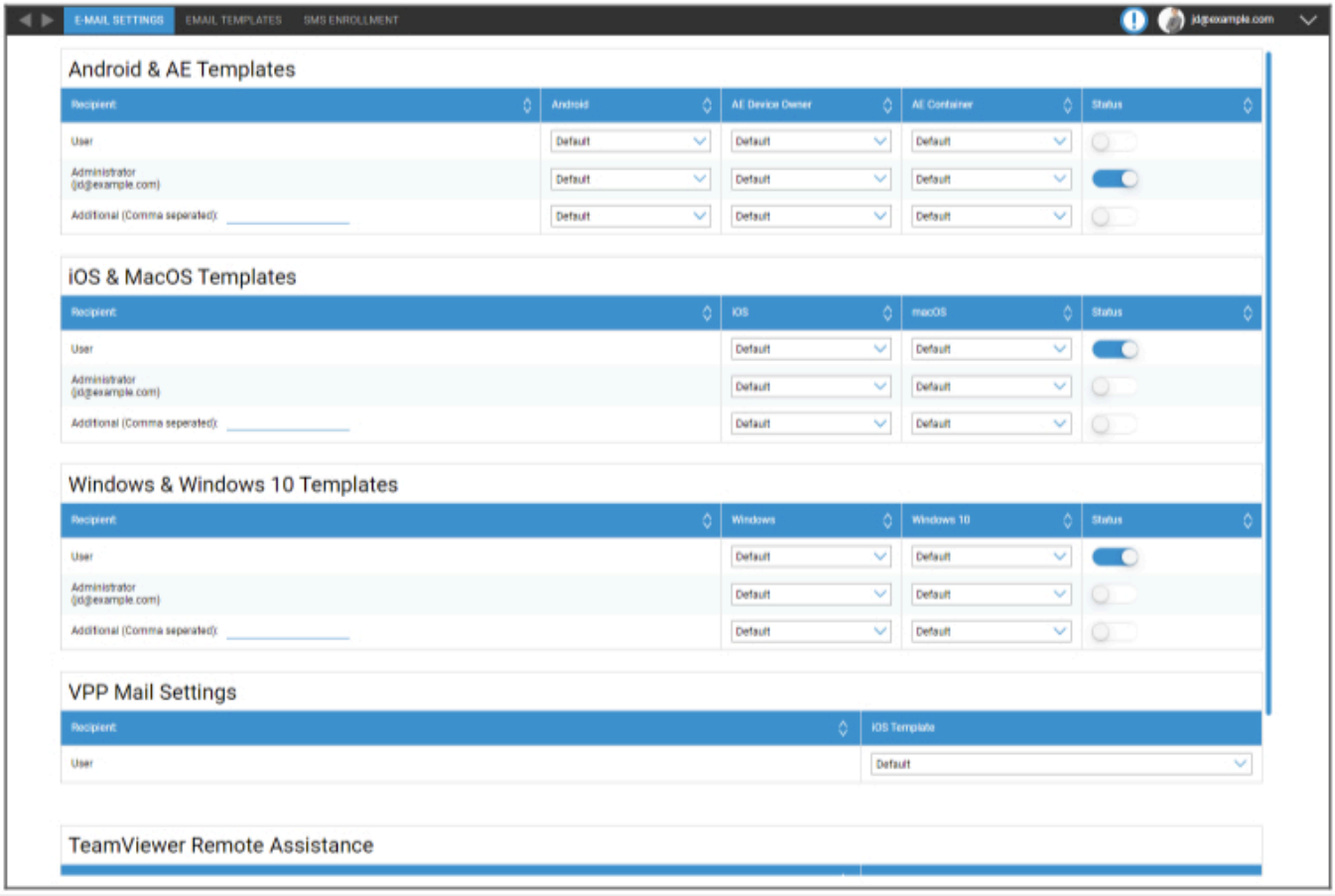
O cerere de funcționalitate poate fi trimisă direct către asistență. Aceasta poate conține o cerere pentru o caracteristică specifică sau o îmbunătățire pentru

Rezumat	Un scurt rezumat al problemei dvs.
Descriere	O descriere detaliată a problemei dumneavoastră, vă rugăm să fiți cât mai specific posibil
Atașament	Atașați fișiere la raportul de eroare

Configurare globală

Setări eMail

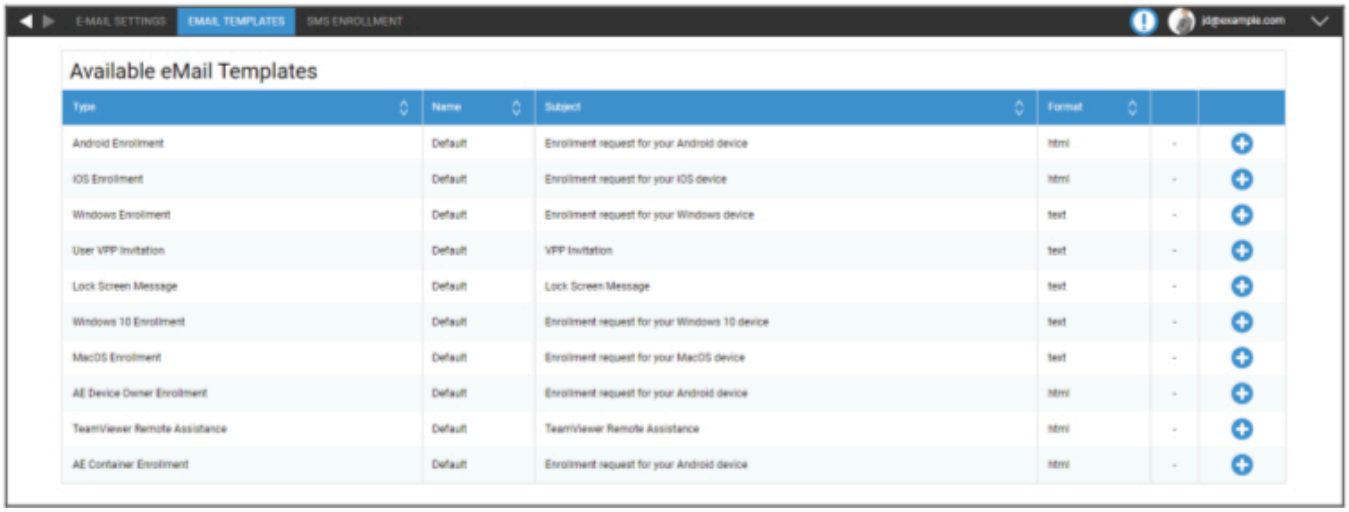
Aici puteți defini cine primește un e-mail atunci când este generată o cerere de înscriere și ce șablon de text este utilizat pentru e-mailul respectiv.



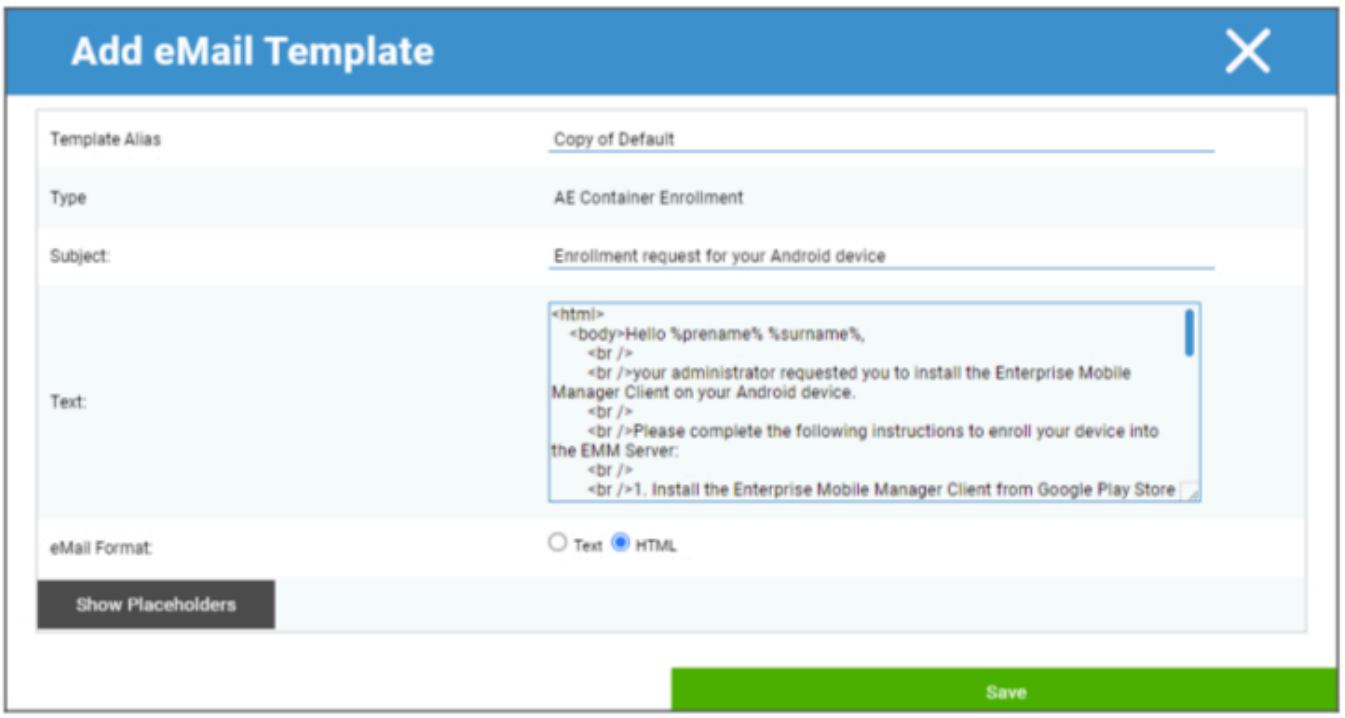
Șabloane eMail

Aici vă puteți genera și edita șabloanele pentru diferite scenarii. Acestea pot fi în formă de text normal sau în HTML. Cu HTML puteți controla mai bine formatarea textului.

Șabloanele implicite nu pot fi editate sau șterse.



De asemenea, puteți utiliza Placeholders ca variabile care vor fi înlocuite automat. Faceți clic pe "Show Placeholders" în timpul editării pentru a vedea Placeholders disponibile. Categorii diferite au Placeholder-uri diferite.



Înscriere SMS

Aici puteți activa/dezactiva procesul de înscriere prin SMS.

(Implicit: dezactivat)

Veți vedea, de asemenea, un afișaj care va indica câte credite SMS mai sunt disponibile.

Creditele SMS trebuie să fie achiziționate separat.

Confidențialitate

Acces GPS

Aici puteți proteja vizualizarea GPS pentru fiecare dispozitiv cu 1 sau 2 parole (principiul celor patru ochi). Vi se va solicita să introduceți parola (parolele) de fiecare dată când încercați să accesați locația unui dispozitiv.

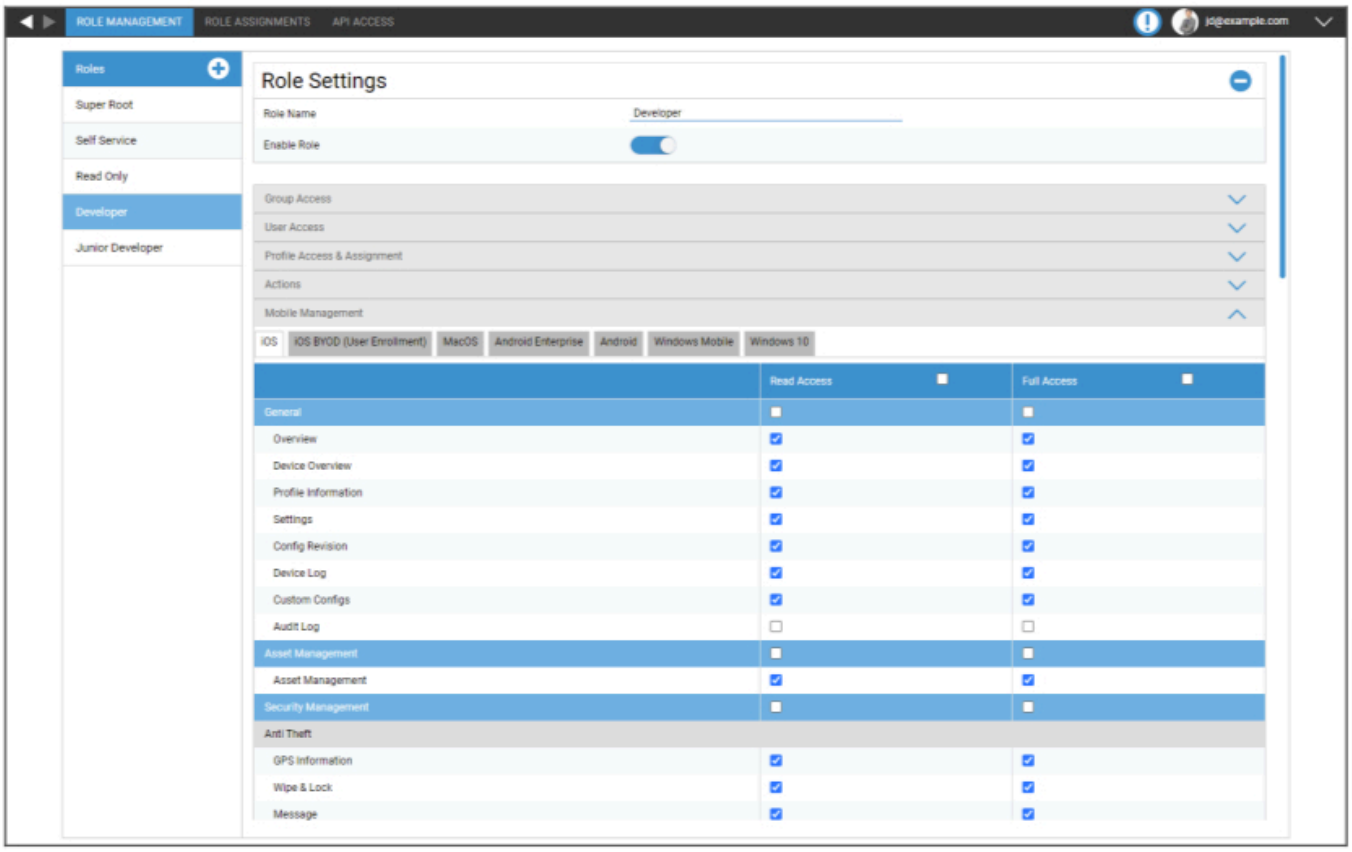
Restricționați accesul la setările GPS	Oprit = funcția este oprită și nu este necesară nicio parolă pentru localizare
	On = funcția este activată și este necesară o parolă pentru localizare
Metoda de protecție	Utilizați o parolă = utilizați o parolă pentru localizare
	Utilizați două parole = utilizați două parole pentru localizare
Introduceți parola (1)	Introduceți parola aleasă
Repetați parola (1)	Introduceți din nou parola aleasă
opțional: Introduceți parola 2	Introduceți a doua parolă aleasă
opțional: Repetați parola 2	Introduceți din nou a doua parolă aleasă

Notă: După setarea codului (codurilor) de acces, trebuie să îl mai introduceți o dată înainte ca acesta să fie complet activat.

Acces bazat pe roluri

Managementul rolurilor

Rolurile definesc ceea ce un utilizator poate vedea și face atunci când se conectează la consola de administrare. Acest lucru vă permite să creați utilizatori care se pot conecta, dar au funcționalități limitate.



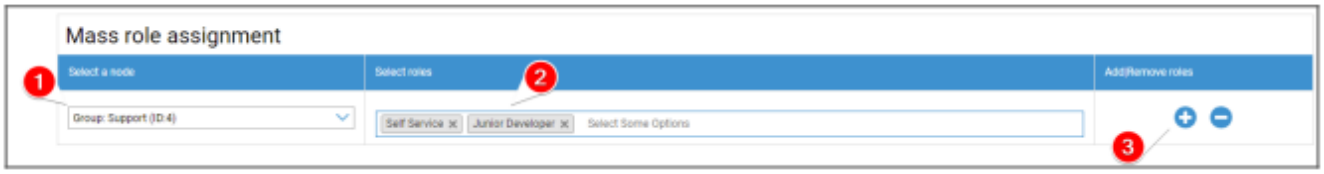
Rolul Super Root este un rol implicit care poate vedea și modifica întotdeauna totul. Acesta nu poate fi modificat sau șters. Rolul Self Service poate vedea doar propriul utilizator și propriile dispozitive. Puteți combina Self Service și un rol personalizat pentru a permite, de exemplu, utilizatorilor să se conecteze și să înscrie dispozitive pe cont propriu și numai pentru utilizatorul lor.

Rolurile personalizate pot fi activate sau dezactivate manual. Rolurile noi sunt dezactivate în mod implicit. Utilizatorii cu un rol dezactivat lucrează ca și cum nu ar avea rolul respectiv. Acest lucru vă permite, de exemplu, să restricționați temporar un anumit rol de la acțiunile sale.

Toate permisiunile sunt împărțite între "Acces la citire" și "Acces complet". Acordarea accesului de citire unui rol îi permite să vadă partea specifică a consolei. Acordarea accesului complet permite rolului să vadă și să modifice partea specifică a consolei.

Atribuirea rolurilor

Aici obțineți o prezentare generală a tuturor utilizatorilor care au un rol și vedeți care este rolul lor. De asemenea, aici puteți atribui un rol utilizatorilor sau grupurilor întregi:

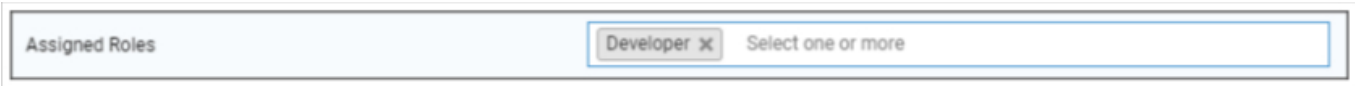


1. Selectați grupul sau utilizatorul pentru care doriți să adăugați sau să eliminați roluri. Puteți selecta fie un singur utilizator, fie un grup. Atunci când selectați un grup, modificarea dvs. va afecta toți utilizatorii din grupul respectiv și toți utilizatorii din subgrupurile din grupul selectat.
2. Selectați ce rol doriți să adăugați sau să eliminați. Puteți selecta unul sau mai multe roluri.
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. Salvați pentru a finaliza procesul. Utilizatorii care anterior nu aveau niciun rol și opțiunea "Can Login" dezactivată vor primi automat un e-mail cu un link pentru a seta o parolă.

Sub atribuirea masivă a rolurilor puteți găsi o prezentare generală a rolurilor atribuite. De asemenea, acolo puteți modifica manual rolurile pentru anumiți utilizatori.

Atribuirea unui rol

Pentru a atribui un rol unui utilizator, trebuie să mergeți la Mobile Management, unde găsiți arborele grupurilor, utilizatorilor și dispozitivelor dvs. Modificați utilizatorul pentru a-i atribui un rol. Alternativ, puteți utiliza metoda menționată mai sus și pentru utilizatori unici.



Acces API

Accesați AppTec360 REST API

AppTec360 REST API necesită un simbol de autentificare (cheie API) și o cheie privată care trebuie generate în Consola de administrare.

Pentru a face acest lucru, autentificați-vă în AppTec360 EMM și mergeți la

Setări generale → Acces bazat pe roluri → Acces API și adăugați o nouă cheie.

Trebuie să selectați un utilizator ale cărui permisiuni se vor aplica la cheia API.

Cheia privată poate fi descărcată o singură dată. După începerea descărcării, cheia va fi ștearsă, iar butonul "Descărcare" va dispărea.

Dacă vă pierdeți cheia privată, trebuie să generați o nouă cheie API.

Reguli generale

- API REST este disponibil sub URL-ul de bază:

/public/external/api

- Toate cererile trebuie să fie trimise prin POST.
- API REST acceptă solicitări numai prin HTTPS.
- Cererile trebuie să conțină următoarele antete:

Denumirea antetului	Valoarea antetului	Descriere
Tip conținut	aplicație/json	fixat
autorizație	123...xyz	Cheia API din fila "Acces API"
semnătură	Semnătura codificată Base64	Semnătura încărcăturii utile generate cu cheie privată din fila "Acces API"

- Corpul cererii trebuie să fie un obiect codificat json care trebuie să conțină următoarele valori:

Câmp	Câmp Exemplu Valoare	Descriere
api	v2/device/listdevices	Denumirea API
timp	1529662725	Timestamp Unix (UTC) al computerului client. Diferența maximă de timp permisă între client și server este de 30 minute.

- În caz de succes, API returnează datele solicitate (a se vedea interogările de mai jos) și un cod de stare HTTP 200.
- Dacă apare o eroare, codul de stare HTTP va fi între 4xx și 5xx, în funcție de eroare, iar obiectul răspuns va conține un array cu cheia "errors", care conține o listă de mesaje de eroare lizibile de către om.
- Dacă nu există date corespunzătoare pentru un dispozitiv, va fi returnat un array gol.
- Dacă Id-ul unui dispozitiv nu există, datele returnate vor fi nule.

Exemplu de cerere

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]}}

Întrebări

Lista tuturor dispozitivelor

Funcționalitate: Returnează o listă a tuturor dispozitivelor conținând ID-ul dispozitivului, IMEI și seria
API URI: v2/device/listdevices
Parametri obligatorii: niciunul
Parametri opționali: niciunul

Exemplu de corp al cererii


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


Exemplu de corp de răspuns


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

Obțineți lista de poziții (GPS)

Funcționalitate: Returnează o listă a tuturor intrărilor stocate în jurnalul poziției pentru id-urile dispozitivului
API URI: v2/device/listposition
Parametri obligatorii: "ids" - Array de ID-uri ale dispozitivelor
Parametri opționali: niciunul

Exemplu de corp al cererii


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


Exemplu de corp de răspuns


```
{
"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":[],
]
}
```

Obțineți harta activelor

Funcționalitate:
Returnează o listă a tuturor activelor posibile stocate care pot fi solicitate utilizând Get any asset data. Puteți utiliza fie forma lizibilă de către om, fie eticheta activului pentru a solicita datele.
API URI: v2/device/getassetmap
Parametri obligatorii: niciunul
Parametri opționali: niciunul

Exemplu de corp al cererii

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

Exemplu de corp de răspuns

Acest răspuns a fost scurtat pentru a fi mai ușor de citit.

{
"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": []
}

Obțineți orice date despre active

Funcționalitate: Returnează o listă de date privind activele solicitate pentru id-urile dispozitivului
API URI: v2/device/getassetdata
Parametri obligatorii: "ids" - Array de ID-uri ale dispozitivelor
Parametri opționali:
"assetkeys" - Cheile pentru datele privind activele care trebuie returnate. Dacă nu sunt specificate, toate datele disponibile privind activele vor fi
returnate. Puteți obține o listă de chei ale activelor utilizând Get asset map.

Exemplu de corp al cererii


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


Exemplu de corp de răspuns


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

Exemplu de cod în Python3

```
! /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)
```

Configurația Apple

Certificat APNS

Aici puteți încărca un certificat APNS. Acesta este necesar pentru gestionarea dispozitivelor iOS și MacOS.

Notă: Certificatul APNS este valabil doar pentru un an. Acesta trebuie reînnoit înainte să expire. Procesul de reînnoire este identic cu cel de creare (a se vedea mai jos) și durează doar câteva minute.

În cazul în care uitați să reînnoiți acest lucru la timp, nu puteți face modificări la dispozitivele deja înscrise **și va trebui să înscrieți din nou toate dispozitivele**.

Pasul 1

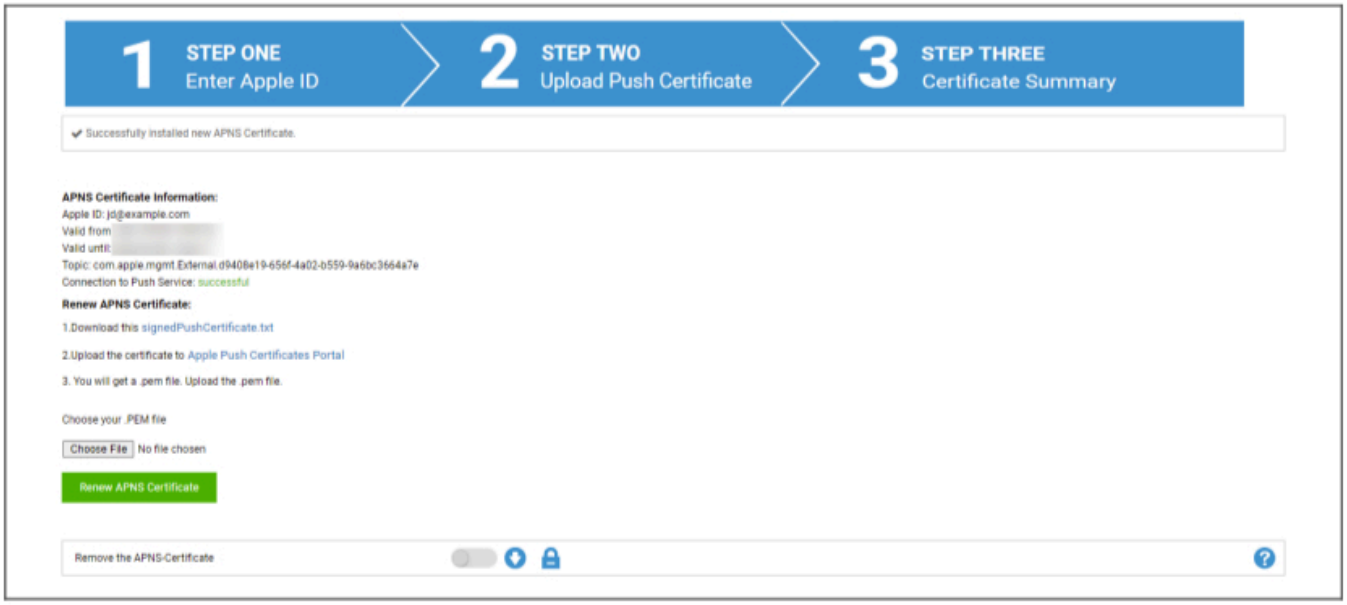
- Mai întâi, introduceți ID-ul Apple pe care doriți să îl utilizați pentru a crea certificatul APNS.

Notă: Acest ID Apple este utilizat numai pentru crearea certificatului APNS. Acest ID Apple nu are nicio legătură cu dispozitivele și dispozitivele nu vor ști despre acest ID Apple. În plus, aveți nevoie de acces la acest ID Apple și pentru a reînnoi certificatul APNS. Prin urmare, este recomandat să utilizați un ID Apple generic și să documentați datele de conectare. Înainte de expirarea certificatului APNS, se trimite un memento la adresa de e-mail utilizată a ID-ului Apple.

- Faceți clic pe "Pasul următor" pentru a continua.
- (opțional) De asemenea, puteți recupera certificatul APNS șters anterior dacă l-ați șters accidental

Pasul 2

- Descărcați signedPushCertificate.txt
- Accesați https://identity.apple.com/pushcert/ și autentificați-vă cu ID-ul Apple de la Pasul 1
- Faceți clic pe "Creați un certificat"
- (opțional) introduceți o notă. Acest lucru poate fi util dacă gestionați mai mulți chiriași pentru a-i identifica cu ușurință.
- Faceți clic pe "Choose File" pentru a selecta fișierul signedPushCertificate.txt descărcat anterior
- Faceți clic pe "Încărcare".
- Veți vedea acum confirmarea că ați creat un certificat APNS.
- Faceți clic pe "Descărcare" și salvați-l.
- Reveniți la consola de administrare.
- Faceți clic pe "Choose File" și selectați certificatul APNS pe care doriți să îl încărcați.
- Faceți clic pe "Încărcare"



Pasul 3

Ați configurat cu succes certificatul APNS și acum puteți gestiona dispozitive iOS și MacOS.

La Pasul 3 veți vedea o prezentare generală a certificatului APNS utilizat în prezent.

De asemenea, aveți opțiunea de a reînnoi certificatul APNS urmând pașii afișați pe ecran. Nu uitați să reînnoiți certificatul înainte ca acesta să expire.

Atunci când reînnoiți certificatul APNS, rețineți să vă conectați cu ID-ul Apple prezentat la Pasul 3 și, de asemenea, să reînnoiți certificatul utilizat anterior și să NU creați unul nou. Veți vedea "subiectul" certificatului APNS în Pasul 3 și atunci când faceți clic pe "i" în portalul Apple Push Certificate. Acesta este ID-ul unic care identifică certificatul. Acest lucru vă va ajuta să identificați certificatul corect și să îl reînnoiți pe cel corect.

Când primiți mesajul "Error: The Push Certificate has a different topic!" în timpul reînnoirii, înseamnă că ați reînnoit un alt certificat sau ați creat unul nou.

Dacă doriți să încărcați un nou certificat, de exemplu, dacă nu mai puteți accesa ID-ul Apple utilizat anterior, trebuie mai întâi să ștergeți certificatul încărcat în prezent.

Oricum, ștergerea certificatului APNS înseamnă că nu mai puteți face modificări pentru dispozitivele înscrise în prezent până când nu le înscrieți din nou. Prin urmare, asigurați-vă că sunteți pregătit pentru acest lucru și eliminați certificatul numai dacă nu există altă modalitate.

Acces gestionat

Aici puteți activa Înscrierea utilizatorului pentru dispozitive iOS și iPad partajat pentru dispozitive iOS.

Înscrierea utilizatorului

"Înscrierea utilizatorului" permite un mod special pentru dispozitivele BYOD.

Pentru fiecare utilizator trebuie creat un Apple-ID gestionat în Apple Business Portal.

În timpul procesului de înscriere, utilizatorilor li se vor cere datele de identificare Apple-ID.

"Înscrierea utilizatorului" garantează o siguranță maximă pentru utilizator, deoarece permite doar un set limitat de setări și restricții care pot fi configurate de MDM.

Domeniu gestionat:

Domeniul utilizat pentru a corela adresa de e-mail a utilizatorului cu Apple-ID-ul gestionat (trebuie să fie în formatul: "@appleid.company.com").De exemplu, john.doe@example.com va fi corelat cu john.doe@appleid.company.com

Consultați Apple Business Manager pentru a vă vedea domeniul administrat

iPad partajat

Un iPad partajat este un dispozitiv DEP configurat cu un profil DEP special.

Acest lucru permite mai multor utilizatori să se conecteze la dispozitiv utilizând Apple-ID-ul gestionat.

ID-ul Apple gestionat trebuie să fie creat în Apple Business Portal sau în Apple School Manager.

Utilizatorilor care se conectează la un iPad partajat li se cer acreditările Apple-ID gestionate.

Domeniu gestionat:

Domeniul utilizat pentru a corela adresa de e-mail a utilizatorului cu Apple-ID-ul gestionat (trebuie să fie în formatul: "@appleid.company.com").De exemplu, john.doe@example.com va fi corelat cu john.doe@appleid.company.com

Consultați Apple Business Manager pentru a vă vedea domeniul administrat

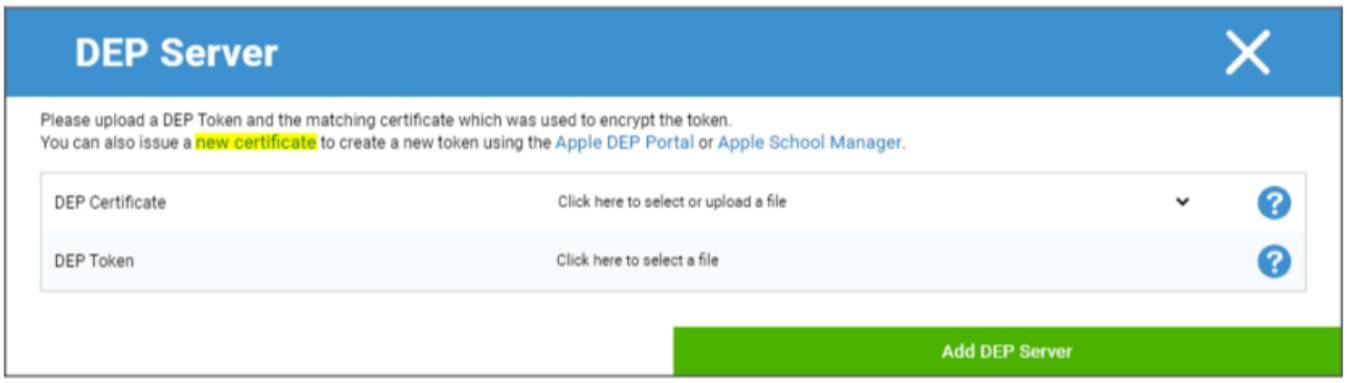
DEP

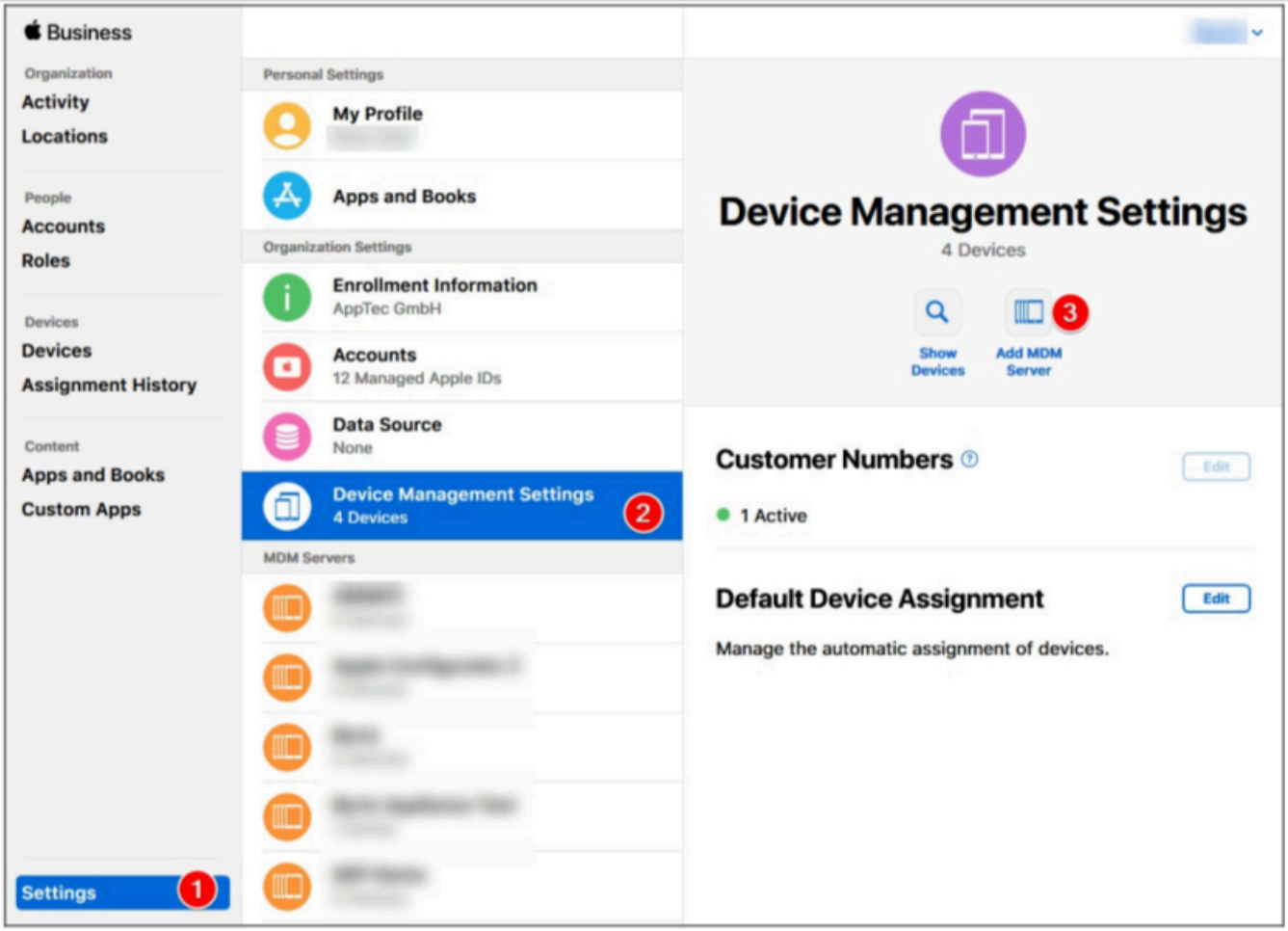
DEP (Device Enrollment Program) vă permite să înscrieți cu ușurință dispozitive în MDM. Atunci când utilizați DEP, dispozitivele vor fi conectate automat la MDM la configurarea dispozitivului. De asemenea, puteți sări peste aproape toți pașii de configurare care sunt de obicei obligatorii pe iOS.

Rețineți că trebuie să cumpărați dispozitivele de la un distribuitor care acceptă DEP. Pentru mai multe informații, contactați distribuitorul dvs. sau Apple.

Mai multe informații despre DEP: https://www.apple.com/business/dep/

Faceți clic pe "+" pentru a adăuga un jeton DEP. În fereastra pop-up, faceți clic pe "certificat nou" în text (marcat cu galben în imaginea de mai jos). Acest lucru va genera și descărca un certificat DEP. După aceea, mergeți la Apple Business Manager(https://business.apple.com/) sau Apple School Manager(https://school.apple.com/).

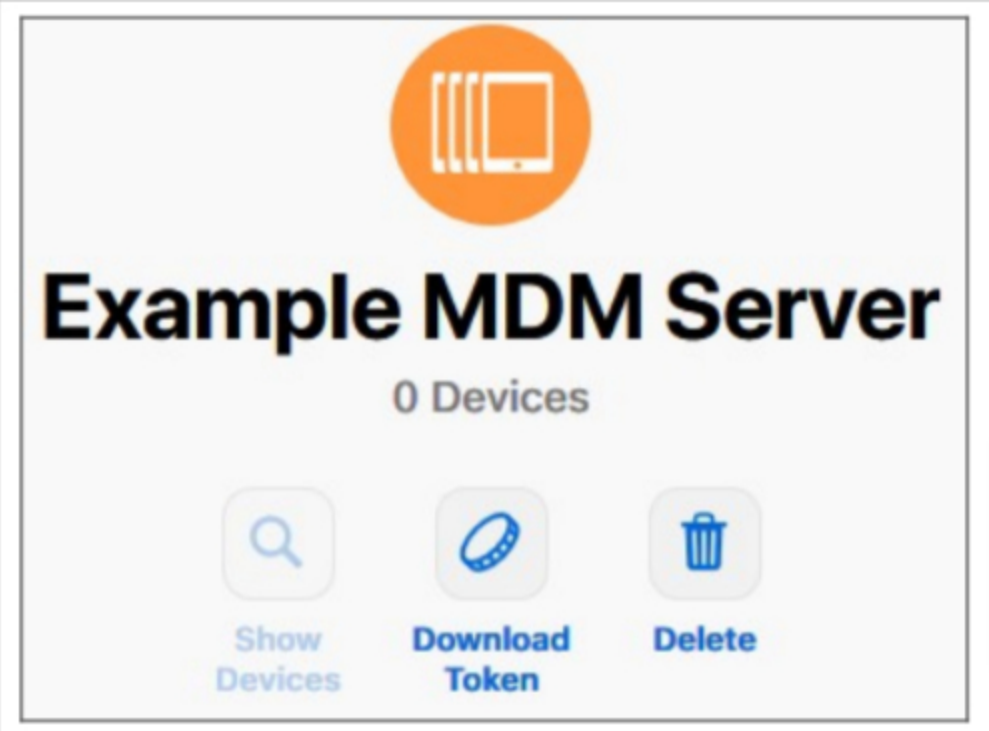




În Apple Business Manager, urmați pașii, după cum se arată în imaginea de mai sus. Settings → Device Management Settings → Add MDM Server.

Dați Serverului orice nume doriți și încărcați Certificatul DEP descărcat anterior sub MDM Server Settings → Upload Public Key și faceți clic pe "Save".

Veți avea acum opțiunea "Download Token". Faceți clic pe aceasta și salvați-l. Token-ul este valabil doar timp de 1 an. Dar dacă faceți clic din nou pe "Descărcați jetonul", veți primi unul nou, ceea ce face ca reînnoirea jetonului să fie foarte ușoară.



Acum vă puteți întoarce la MDM, unde ați descărcat anterior certificatul DEP. Dacă nu ați închis fila, fereastra pop-up pentru adăugarea unui server DEP ar trebui să fie încă deschisă, iar certificatul DEP ar trebui să fie deja selectat. Acum puteți încărca Token-ul în câmpul "DEP Token" și faceți clic pe DEP Server.

În coloana "**Devices**" (**Dispozitive**) veți vedea numărul de dispozitive care sunt alocate acestui server DEP. Dispozitivele adăugate la acest server DEP vor fi create automat în DEP Pool în Mobile Management.

Puteți face clic pe acest număr pentru a obține o imagine de ansamblu asupra tuturor dispozitivelor DEP și a stării acestora.

Notă: În funcție de fluxul dvs. de lucru sau de configurația din Business Manager, este posibil să trebuiască să atribuiți manual aceste dispozitive serverului DEP. De asemenea, puteți seta un server DEP implicit în Apple Business Manager pentru dispozitivele noi.

În coloana "**Profiluri**" puteți vedea numărul de profiluri DEP pe care le aveți. De asemenea, puteți face clic pe acest număr pentru a vedea detalii despre profilurile DEP și puteți șterge aici profilurile vechi/neutilizate. În prezent, nu este posibilă modificarea acestora. Dacă doriți să faceți o modificare, trebuie să creați unul nou.

În coloana "**Ultima sincronizare**" puteți sincroniza manual serverul DEP (de exemplu, dacă tocmai ați adăugat un dispozitiv nou la DEP) și puteți vedea data ultimei sincronizări reușite.

În coloana "**Profil automat**" puteți seta un profil DEP ca profil automat implicit. Acest profil va fi atribuit automat dispozitivelor noi. Dacă nu setați un profil automat, va trebui să atribuiți manual un profil dispozitivelor noi de fiecare dată.

În coloana "**Add Profile**" puteți adăuga un nou profil DEP. Dispozitivul va primi acest profil la începutul configurării dispozitivului. Profilul DEP definește modul în care dispozitivul este configurat și care etape de configurare vor fi omise.

Notă: după înscrierea unui dispozitiv, aceste setări pot fi modificate numai prin efectuarea unei resetări din fabrică și înscrierea dispozitivului cu un profil nou. Acest lucru este relevant în special pentru "**Removable**" și "**Allow pairing**". În cazul "**Allow pairing**" se recomandă activarea acesteia, deoarece poate fi dezactivată prin restricții MDM, dar nu poate fi activată din nou dacă este dezactivată în profilul DEP.

În coloana "**Editare**" puteți încărca un jeton nou, de exemplu, la reînnoirea jetonului.

Configurator & URL

URL-uri de înscriere în bazin

Aici puteți crea o adresă URL de înscriere și un cod QR de înscriere care este valabil o anumită perioadă de înscriere și până la o anumită dată. Acest lucru vă permite să înscrieți mai multe dispozitive cu un singur link sau cod QR.

Dispozitivele înregistrate cu această adresă URL sau cod QR vor fi în Pool în Mobile Management și va trebui să le atribuiți manual unui grup sau utilizator ulterior.

Notă: acest lucru este valabil numai pentru înscrierea manuală. Nu utilizați acest URL dacă înscrieți dispozitivele prin intermediul Apple Configurator

Profil MDM – Configurator Apple

Aici puteți obține URL-ul de care aveți nevoie atunci când înscrieți dispozitive prin intermediul Apple Configurator. În timpul pregătirii dispozitivelor cu Apple Configurator, puteți adăuga dispozitivele la MDM în același proces. Apple Configurator necesită acest URL pentru acest lucru.

Dispozitivele adăugate prin intermediul Apple Configurator vor fi în Pool în Mobile Management și va trebui să le atribuiți manual unui grup sau utilizator ulterior.

Veți găsi aici și un fișier .mobileconfig care poate fi utilizat pentru a înscrie dispozitivele prin intermediul Apple Configurator. Oricum, utilizarea URL-ului este recomandată.

Configurare Android

Configurare Android

Dezinstalați protecția	Dacă această funcție este activată, utilizatorul nu poate dezactiva administratorul dispozitivului, fără a introduce parola setată de administratorul MDM. Parola este setată în timpul înregistrării, astfel încât dispozitivele trebuie să fie reînregistrate pentru a actualiza parola. Există două opțiuni pentru eliminarea administratorilor de dispozitive: 1. Manual pe dispozitiv ◦ Deschideți aplicația EMM pe dispozitiv ◦ Treceți la fila Stare ◦ Apăsați pe "Dezinstalare protecție" ◦ Introduceți parola Puteți utiliza Revision pentru a obține parola corectă din "Istoricul parolelor" din consolă. ◦ Derulați în jos și atingeți punctul nou adăugat,"Atingeți pentru a dezinstala AppTec360 MDM App" (aveți la dispoziție 20 de secunde pentru a efectua această sarcină) ◦ Confirmați dialogul "Uninstall AppTec360 MDM App" cu "ok". Acest lucru va anula înscrierea dispozitivului din consolă. ◦ Pentru a elimina aplicația de pe dispozitiv, confirmați dialogul "AppTec360 MDM va fi dezinstalat" cu "UNINSTALL" 2. automat (consolă) ◦ Selectați dispozitivul în consolă ◦ Faceți clic pe pictograma angrenajului albastru și selectați "Enterprise Wipe" Notă: Disponibil numai cu Android 4.x și versiuni inferioare sau pe dispozitive cu API KNOX (dispozitive Samsung)
Parolă de dezinstalare	Parola stabilită, cu ajutorul căreia utilizatorul poate elimina administratorul dispozitivului

(Revizia x)	Revizuire x = contor, de câte ori a fost deja schimbată parola Este important de ce parolă are nevoie utilizatorul, deoarece este posibil ca dispozitivul să nu fi comunicat cu serverul AppTec360 și, prin urmare, cea mai nouă parolă să nu fi fost încă transmisă
Istoricul parolei	Când faceți clic pe butonul albastru ("Afișați istoricul"), puteți vizualiza parolele stabilite anterior
Protecție extinsă de dezinstalare	Această opțiune oferă protecție împotriva dispozitivelor non-SAFE Atâta timp cât această setare este activată, nu este posibilă dezactivarea cu ușurință a administratorului dispozitivului
Invitați utilizatorul să dezinstaleze aplicațiile blocate?	Dacă este posibil, aplicațiile blocate nu vor fi doar blocate, ci și dezinstalate automat. Utilizatorului i se va solicita să dezinstaleze aplicațiile blocate dacă dezinstalarea automată nu este posibilă.
Sistem inteligent de blocare a aplicațiilor	Dacă lista albă este activată, clientul MDM Android blochează toate aplicațiile instalate de utilizator. Activați această setare pentru a bloca toate aplicațiile de sistem lansabile în modul Whitelisting.

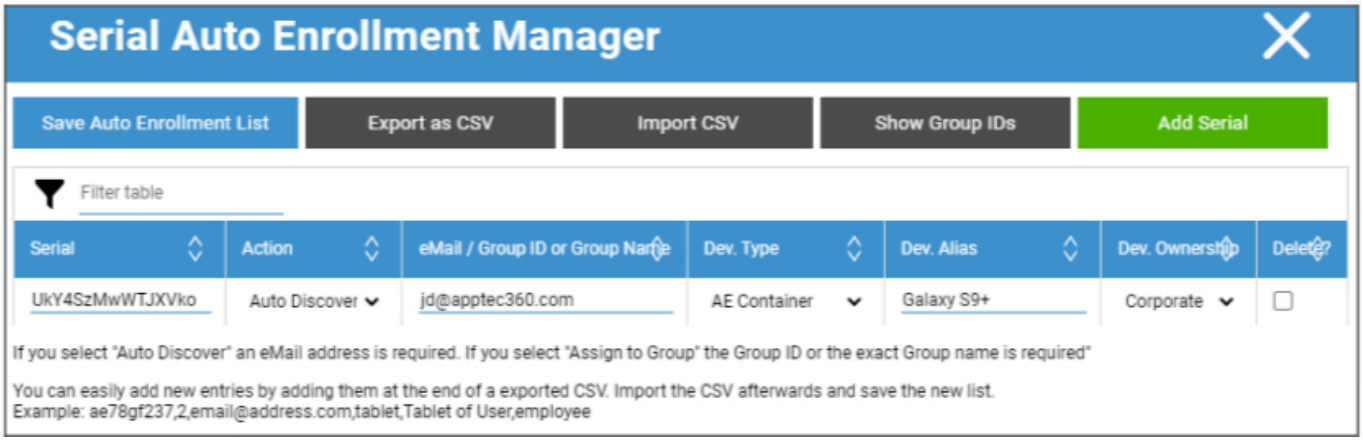
Înscriere automată

Aici puteți activa funcția Înscriere automată pentru a vă înscrie dispozitivele automat atunci când AppTec360 MDM Client este deschis pe dispozitiv.

Important: Această metodă de înscriere este depășită și nu mai funcționează pe Android 10 sau o versiune ulterioară. Oricum, atunci când utilizați Android 7 sau o versiune ulterioară, ar trebui oricum să înscrieți dispozitivele ca fiind gestionate integral de Android Enterprise. Dacă doriți să utilizați containerul Android Enterprise BYOD și utilizați Android 10 sau o versiune ulterioară, trebuie să înscrieți manual dispozitivul prin acreditări, cod QR sau SMS. Oricum, lista de înscriere automată este încă utilizată pentru a automatiza procesul de înscriere, de exemplu pentru AE Enrollment, Knox Enrollment etc.

Oricum, lista de înscriere automată este încă utilizată pentru a automatiza procesul de înscriere pentru, de exemplu, AE Enrollment, Knox Enrollment, etc.

Făcând clic pe "Serial Manager" sau "IMEI Manager", puteți adăuga seria sau IMEI a dispozitivelor dvs. Nu este necesar să le faceți pe amândouă pentru dispozitivele dvs., doar una este suficientă.



Acțiunea definește dacă dispozitivele vor fi înscrise în pool, într-un utilizator sau într-un grup.

De asemenea, puteți exporta și importa un fișier .csv și vă puteți filtra intrările după cuvinte cheie.

Android Enterprise

Aici puteți configura Android Enterprise. Acest lucru este necesar pentru a utiliza toate caracteristicile Android Enterprise.

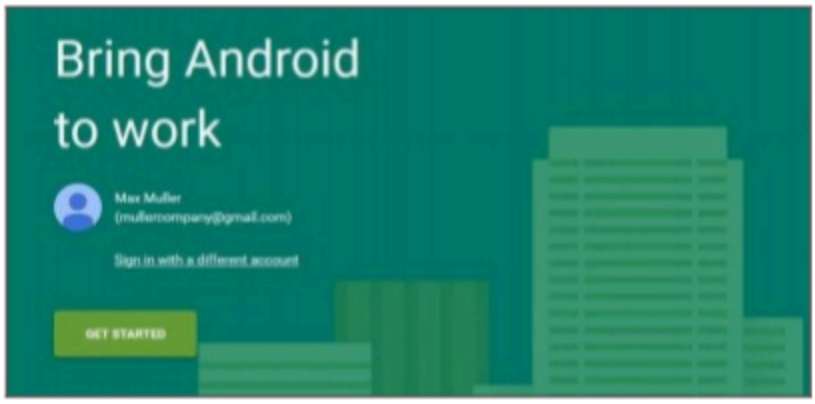
Prima metodă: Cont Android Enterprise (Cont Google)

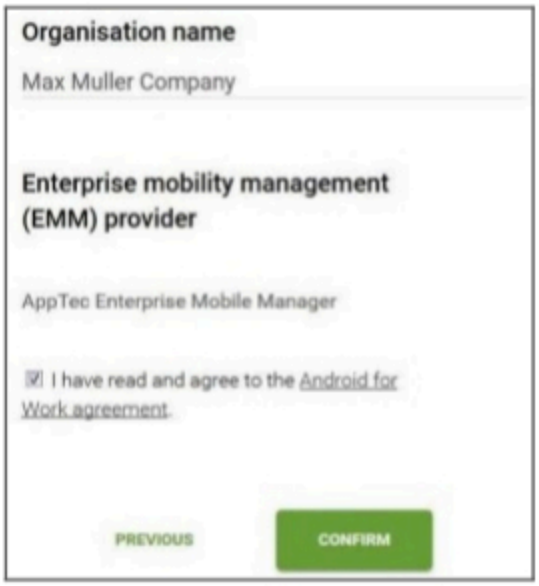
Apăsați mai întâi "Pregătiți configurarea", iar după un scurt moment ar trebui să apară butonul "Start Setup".

Aceasta vă va duce la pagina de configurare Android Enterprise de la Google.

Conectați-vă cu contul Google pe care doriți să îl utilizați, dacă nu sunteți deja conectat și apăsați "Începeți".

Acum puteți introduce numele companiei dumneavoastră. După ce ați făcut acest lucru, bifați caseta de selectare și apăsați "Confirmare"





În ultimul pas puteți finaliza înregistrarea și ar trebui să reveniți la consolă. Dacă totul a funcționat, ar trebui să arate astfel:

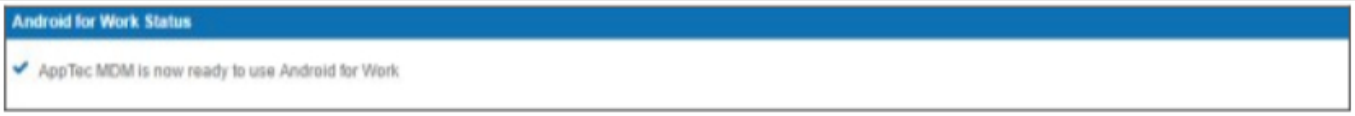
Acum puteți începe configurarea containerului Android Enterprise.

A doua metodă: Cont G-Suite

Apăsați "Use G-Suite" și conectați-vă la contul dvs. de administrator Google. Acolo mergeți la "Security" -> "Show more" -> "Manage EMM provider for Android" și generați un Token. Notă: Dacă nu vedeți Android Enterprise Settings în contul dvs. G-Suite, trebuie să mergeți la "Get more apps and services" și să adăugați gestionarea dispozitivelor Android. Acum introduceți Token-ul și domeniul dvs. primar în consola noastră și faceți clic pe "Save Changes". Când ați terminat, faceți clic pe "Use Android Enterprise Account".

Acum ar trebui să vedeți butonul "Creați cont de serviciu". Faceți clic pe acesta. Acest proces poate dura câteva momente.

Dacă totul a funcționat, ar trebui să arate astfel:



Acum puteți începe configurarea containerului Android Enterprise.

Protecție la resetarea din fabrică

Cu ajutorul Protecției la resetarea din fabrică, vă puteți lega dispozitivul la un cont Google la alegere, care anulează, de asemenea, orice legare existentă la un cont Google. Pentru a utiliza Protecția la resetarea din fabrică, trebuie să o configurați mai întâi aici și să o activați apoi în profilurile dvs.

Pentru a configura protecția la resetarea din fabrică, faceți clic pe "Configurare FRP" și urmați instrucțiunile de pe ecran.

NOTĂ: Citiți cu atenție și efectuați pașii. Vă recomandăm să faceți acest lucru într-o fereastră nouă de browser incognito pentru a evita conectarea automată la un cont Google greșit. Vă puteți bloca complet în afara dispozitivului, dacă introduceți un ID greșit sau pierdeți accesul la contul Google utilizat!

Înscriere AE

Aici puteți activa Android Enterprise Ernollment. Folosind această metodă, vă veți înscrie dispozitivele în modul Android Enterprise Device Owner. În acest mod, veți avea control deplin asupra dispozitivului.

Activați înscrierea AE	Activează AE Enrollment Atenție: Dacă dezactivați AE Enrollment, codurile QR existente și dispozitivele programator NFC deja configurate nu vor mai funcționa. Dacă activați din nou AE Enrollment, va trebui să retrimiteți configurațiile push NFC / să generați noi coduri QR.
Activați descoperirea automată	Atunci când un dispozitiv se înscrie prin "AE Enrollment", sistemul va încerca să îl atribuie unui utilizator pe baza informațiilor setate în Lista albă serială / IMEI ("General Settings" > "Android Configuration" > "Auto Enrollment").
Blocarea dispozitivelor necunoscute	Numai dispozitivele care au fost incluse pe lista albă în Lista albă serială / IMEI ("Setări generale" > "Configurare Android" > "Înscriere automată") pot fi înscrise.

Notă privind metodele 1 și 2: "Ecranul de bun venit" se referă la primul ecran pe care îl vedeți după resetarea din fabrică. Acesta poate arăta diferit în funcție de versiunea android și/sau modelul dispozitivului pe care îl utilizați.

Metoda 1: Înscrierea codului QR

(necesită Android 7.0 sau o versiune mai recentă) Vă recomandăm să utilizați întotdeauna această metodă dacă utilizați Android 7 sau o versiune mai recentă.

1. Resetarea din fabrică a dispozitivului
2. Generați codul QR pentru înscriere utilizând una dintre următoarele două metode:
   - Faceți clic în "Setări generale -> Configurare Android -> AE Enrollment" pe "Generare cod QR". Alegeți dacă doriți să săriți peste criptarea stocării și/sau toate aplicațiile de sistem trebuie eliminate.
   - (alternativ) Alegeți un dispozitiv existent. În "Device Overview" faceți clic pe codul QR afișat acolo. Alegeți dacă doriți să săriți peste criptarea stocării și/sau toate aplicațiile de sistem trebuie eliminate.
3. Acum atingeți de 6 ori ecranul de întâmpinare al dispozitivului. Acest lucru ar trebui să pornească modul de înscriere QR.
4. Acum conectați-vă la o rețea fără fir și așteptați puțin timp până când cititorul de coduri QR este instalat
5. Acum scanați codul QR
6. Asta este tot. Dispozitivul dvs. este acum înscris în Android Enterprise Device Mode.

- a. Dacă ați utilizat codul QR în "Setări generale", puteți găsi dispozitivul dvs. în "Pool -> AE Device Owner Devices". (Indicație: este posibil să trebuiască să reîncărcați site-ul pentru a vedea dispozitivele). Dacă ați bifat "Enable Auto Discover", îl veți găsi în cadrul utilizatorului Auto Discover.
- Dacă ați utilizat codul QR al unui profil de dispozitiv existent, dispozitivul va fi înscris în acest profil.

Metoda 2: Înscrierea NFC

(necesită NFC și Android 6.0 sau o versiune mai recentă)

Pregătire: Introduceți informațiile WiFi în "General Settings -> Android Configuration -> AE Enrollment -> Data for NFC provisioning". Acum utilizați "NFC Device" pentru a căuta dispozitivul care va deveni programatorul. Acest dispozitiv va fi utilizat pentru a trimite informațiile de înscriere către celelalte dispozitive prin NFC.

1. Resetați dispozitivul din fabrică
2. Deschideți aplicația de împerechere NFC de la AppTec360 pe programatorul dvs.
3. Alegeți dacă doriți să săriți peste criptarea spațiului de stocare și/sau toate aplicațiile de sistem să fie eliminate.
4. Țineți ambele dispozitive spate în spate
5. Acum Android Enterprise Enrollment ar trebui să steak
6. Acum vă găsiți dispozitivul în consolă
    - a. În pool, dacă nu ați configurat Auto Discover
    - b. În cadrul utilizatorului, ați configurat pentru Auto Discover
    - c. Indicație: Este posibil să trebuiască să reîncărcați site-ul pentru a vedea dispozitivele

Metoda 3: Contul Google

(necesită Android 5.1 sau o versiune mai recentă)

(Notă: Dacă utilizați această metodă, dispozitivul nu va fi înscris automat. În schimb, trebuie să îl înscrieți manual sau să automatizați procesul prin utilizarea înscrierii automate).

1. Resetați dispozitivul din fabrică
2. Parcurgeți pașii de configurare până când vă puteți conecta cu un cont Google
3. Introduceți "afw#apptec" ca Nume utilizator/Mail
4. Apăsați pe "Următorul"
5. Dispozitivul dvs. este acum un dispozitiv Android Enterprise

KNOX Înscriere

Aici puteți activa KNOX Enrollment și găsi informațiile necesare pentru a crea un profil KNOX Enrollment în KNOX Deployment Portal. Aveți nevoie de un cont la portalul de implementare KNOX pentru a configura și utiliza acest lucru.

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

Activați înscrierea KNOX	Activează înscrierea KNOX. Atenție: Dacă dezactivați KNOX Enrollment, profilurile MDM existente nu vor mai funcționa. Dacă activați din nou KNOX Enrollment, va trebui să actualizați câmpul "Custom JSON Data" din profilul MDM
Activați descoperirea automată	Atunci când un dispozitiv se înscrie prin "KNOX Enrollment", sistemul va încerca să îl atribuie unui utilizator pe baza informațiilor stabilite în Lista albă serială / IMEI ("Setări generale" > "Configurare Android" > "Auto Enrollment").

1. Conectați-vă la portalul Samsung KNOX Mobile Enrollment https://eukme.samsungknox.com/itadmin
2. Mergeți la "Profiluri MDM"
3. Faceți clic pe "Adaugă"
4. Alegeți "Server URI not required for my MDM" și faceți clic pe "Next"
5. Acum creați un profil cu informațiile afișate în consola de administrare

Acum, acest profil de înregistrare KNOX poate fi instalat direct pe dispozitiv de către Samsung dacă achiziționați dispozitivele direct de la Samsung.

Alternativ, puteți descărca aplicația KNOX Deployment, vă puteți conecta cu contul dvs. KNOX Deployment și puteți trimite profilul de înscriere KNOX prin NFC către alte dispozitive.

Dacă dispozitivul are instalat un profil de înscriere KNOX, acesta va descărca aplicația noastră și va înscrie dispozitivul, dacă are o conexiune la internet funcțională.

Înscrierea dispozitivelor prin KNOX Enrollment poate fi găsită în "Pool -> KNOX Enrollment", sau în cadrul utilizatorului specificat în Auto Discover.

Zero-Touch

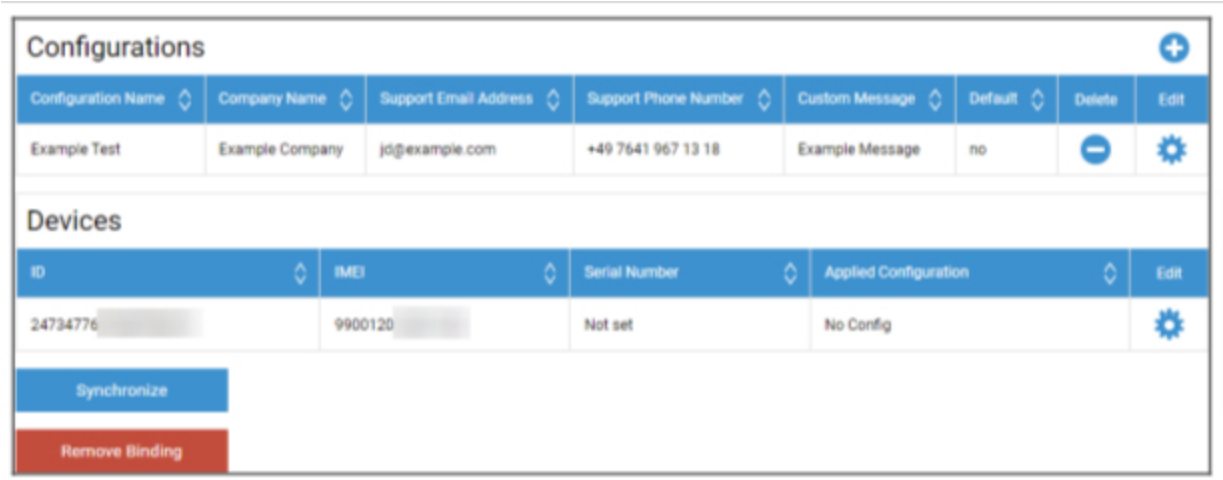
Cu Zero-Touch vă puteți înscrie cu ușurință dispozitivele fără a fi nevoie să le atingeți sau să configurați ceva pe dispozitivul în sine. Trebuie doar să îl porniți, să continuați configurarea în mod normal, iar dispozitivul va primi toate informațiile privind modul de configurare și conectare la MDM în mod complet automat.

Pentru a utiliza Zero-Touch, trebuie să vă cumpărați dispozitivele de la un distribuitor care acceptă Zero-Touch. Același distribuitor creează și un cont pentru dvs. în portalul Zero-Touch. Contactați distribuitorul pentru a obține mai multe informații despre procedură sau dacă aveți probleme la accesarea portalului Zero-Touch.

Faceți clic pe "Start Setup" pentru a începe configurarea. Veți fi redirecționat către o pagină de conectare unde trebuie să vă selectați contul Google care are acces la portalul Zero-Touch.

NOTĂ: Este posibil să selectați ORICE cont. Prin urmare, asigurați-vă că selectați contul corect în acest pas. Dacă nu vă vedeți dispozitivele/configurările, este foarte probabil să fi folosit un cont greșit.

După finalizarea autentificării, aceasta va arăta astfel:



Faceți clic pe "+" pentru a adăuga o configurație și completați câmpurile așa cum sunt prezentate pe ecran. Dacă activați configurația ca configurație implicită, aceasta va fi atribuită automat noilor dispozitive. Crearea sau setarea unei configurații implicite nu o atribuie dispozitivelor deja existente.

Dacă unui dispozitiv nu i se atribuie o configurație, acesta se va configura ca un dispozitiv normal și nu se va conecta la MDM. Prin urmare, asigurați-vă că dispozitivele dvs. au o configurație atribuită.

După ce v-ați conectat contul, dispozitivele dvs. sunt vizibile și aveți o configurație atribuită acestora, puteți începe să configurați dispozitivele.

Puteți adăuga dispozitivele la lista de înscriere automată, astfel încât acestea să fie înscrise automat într-un grup sau utilizator specificat. Dacă nu ați configurat nimic în lista de înscriere automată, dispozitivele vor fi înscrise în grup.

Configurarea Windows

Configurarea Windows

Aici aveți opțiunea de a activa următoarele configurații pe PC-ul dvs. cu Windows 10:

Conexiune DM instantanee	
Timp inițial de rescriere	Stabilește prima încercare de conectare la dispozitiv, această valoare crește exponențial
Reîncercări ale conexiunii	Indică numărul de încercări de conectare pe care clientul DM ar trebui să le efectueze în timpul unei erori de conectare
Timp maxim de somn	Indică timpul maxim de așteptare după o eroare de conectare
Prima încercare de sincronizare	intervalele la care dispozitivul trebuie să comunice cu serverul, după prima conexiune
Primul interval de reîncercare	Se referă la "Prima încercare de sincronizare" Aici orele sunt listate în minute De exemplu, la "First Sync Retries" este listată valoarea "2" și la "First Retry Interval" este listată valoarea "4 Minutes", în acest fel dispozitivul comunică de 2 ori la fiecare 4 minute, după prima conexiune
A doua încercare de sincronizare	Intervale la care dispozitivul trebuie să comunice cu serverul, după finalizarea "First Sync Retries"
Al doilea interval de reîncercare	Același principiu ca și pentru "Primul interval de rescriere" - doar că aici, se aplică la "A doua rescriere a sincronizării"
Reîncercări regulate de sincronizare	Intervale, de câte ori ar trebui să comunice dispozitivul cu serverul în viitor Implicit: "Infinit" Vă recomandăm să nu modificați această valoare, deoarece dacă introduceți "10", dispozitivul va comunica cu serverul de 10 ori și apoi se va opri Prin urmare, comunicarea cu serverul AppTec360 este deconectată!
Interval regulat de reîncercare	Același principiu ca și pentru "Primul/al doilea interval de reintroducere" - doar că aici, se aplică setările pentru viitor
Interval regulat de reîncercare	Același principiu ca și pentru "Primul/al doilea interval de reintroducere" - doar că aici, se aplică setările pentru viitor

ContentBox

Configurație

Aici puteți configura ContentBox. Puteți plasa fișiere pentru grupuri în ContentBox, care pot fi accesate cu aplicația ContentBox de pe dispozitiv.

Activați caseta de conținut	Activați ContentBox. Dezactivarea acestei opțiuni, dacă nu utilizați ContentBox, poate economisi resurse pe echipamentele OnPremise.
Utilizați instalarea ContentBox externă	ContentBox poate fi operat și cu propriul dumneavoastră Nextcloud.
URL	URL-ul complet al entității Nextcloud
Utilizator rădăcină	Utilizator rădăcină al contului Nextcloud
Parolă rădăcină	Parola rădăcină a contului Nextcloud
Permisiuni implicite pentru dosarele de grup	Permisiuni implicite pentru dosarele de grup, pot fi modificate individual de către grup (în Mobile Management)
Partajarea folderului de grup cu subgrupuri	Dacă este activ, fiecare subgrup poate citi toate folderele grupului principal, poate fi, de asemenea, configurat individual pentru fiecare grup (Mobile Management)
Permisiuni pentru subgrupuri	Permisiuni pentru subgrupuri pot fi configurate individual pentru fiecare grup (Mobile Management)
Permiteți partajarea	Permite utilizatorului să partajeze conținutul prin intermediul linkurilor, poate fi configurat individual pentru fiecare grup
Dimensiunea maximă de încărcare a fișierului în MB	Dimensiunea maximă a unui fișier Standard: 512 MB Configurație maximă: 2048
Acreditări WebDAV	
URL WebDAV	De asemenea, puteți deschide ContentBox cu WebDAV. Vă rugăm să nu ștergeți următoarele foldere, sub nicio formă: /apptecgroups /apptecgroups/AppTecGroup-X
Utilizator rădăcină	Numele utilizatorilor rădăcină
Parolă	Parola utilizatorilor rădăcină

Sincronizarea cu ContentBox are loc automat. Cu toate acestea, puteți efectua o sincronizare manuală cu "Synchronize ContentBox".

În plus, aici puteți activa/dezactiva ContentBox pe fiecare dispozitiv individual.

Acest lucru este relevant numai în cazul în care nu ați licențiat suplimentar ContentBox, atunci aveți încă acces la 25 de dispozitive cu care puteți testa ContentBox - aici puteți activa acest lucru pentru dispozitivele respective.

Configurarea LDAP

Prezentare generală LDAP

Aici puteți stabili o conexiune la directorul dvs. activ prin LDAP pentru a importa în masă utilizatori și grupuri. Sincronizarea trebuie să fie efectuată manual. Puteți configura mai multe conexiuni LDAP la sisteme diferite sau cu configurații/filtre diferite.

Numele serverului	Numele de afișare al serverului
Tip	În prezent, sunt acceptate numai Active Directories care acceptă LDAP
Domeniu LDAP	Domeniul LDAP primar (de exemplu, example.com)
Gazdă LDAP	Este necesar numai dacă gazda LDAP nu este accesibilă în cadrul domeniului LDAP dat.
Port	Lăsați gol pentru a utiliza portul standard (389 sau 636 pentru SSL)
Nume utilizator	De exemplu, CN=John,OU=Users,DC=EXAMPLE,DC=COM Notă: Majoritatea sistemelor solicită numele de utilizator în acest format și nu acceptă "John" ca nume de utilizator
Parolă	
Confirmați parola	
Securitatea conexiunii	Notă: atunci când se utilizează SSL sau TLS, se va verifica certificatul din Active Directory. Dacă acesta este auto-semnat, trebuie să adăugați CA rădăcină la depozitul de încredere al mașinii OnPremise. Dacă sunteți pe Cloud, Active Directory trebuie să furnizeze un certificat de încredere sau conexiunea va funcționa doar fără criptare
Sincronizare automată.	Activează sincronizarea automată a directorului LDAP în intervalul de timp specificat în setările LDAP generale.
DN de bază	Dacă nu doriți să sincronizați întregul director, puteți specifica aici o OU.De exemplu, OU=AndroidUsers,OU=Users,DC=EXAMPLE,DC=COM
Membru al	Toți utilizatorii importați vor fi adăugați la grupul selectat
Doar utilizatorii activați?	Atunci când este activat, atributul userAccountControl va fi luat în considerare, utilizatorii fără acest atribut nu vor fi importați.
Filtru LDAP	Puteți utiliza filtrul LDAP pentru a filtra utilizatorii care vor fi importați
Filtru Regex	Puteți utiliza filtrul Regex pentru a filtra utilizatorii care vor fi importați

Conexiune de testare	Testează conexiunea la salvarea configurației
Resetarea structurii directoarelor la sincronizare?	Dacă este adevărat, toate intrările LDAP vor fi mutate înapoi la locația lor inițială în arborele LDAP. Este recomandat să fie activat.
Reimportarea utilizatorilor și grupurilor șterse?	Atunci când este activat, utilizatorii și grupurile care au fost șterse vor fi recreate. Este recomandat să fie activat.
Sincronizarea ștergerilor?	Atunci când este activat, grupurile și utilizatorii vor fi șterși atunci când sunt șterși de pe serverul LDAP. De asemenea, dispozitivele utilizatorilor șterși vor fi șterse.

Sub lista de configurații LDAP puteți defini perioada în care sistemul se sincronizează automat. Utilizează pentru sincronizarea automată numai configurațiile LDAP care au opțiunea corespunzătoare activată.

Gestionarea aplicațiilor

Aplicație internă DB

Android

Aici puteți încărca aplicațiile Android pe care le-a dezvoltat compania dvs. și le puteți distribui ulterior în Mobile Management în profiluri de dispozitiv sau de grup.

Vă rugăm să rețineți că vă sfătuim să distribuiți în acest mod numai aplicații care nu sunt disponibile în Magazinul Google Play.

Faceți clic pe "+" pentru a încărca APK-ul unei aplicații pe care doriți să o încărcați. În prezent, este acceptat doar formatul APK.

Limita de încărcare pe dispozitivele OnPremise poate fi mărită la Pasul 3 din Configurarea dispozitivului. Dacă doriți să măriți limita de încărcare pe Cloud, vă rugăm să contactați asistența pentru mai multe informații.

Rețineți că, de obicei, APK-urile sunt un pic mai mici decât conținutul lor. Este posibil ca o încărcare să eșueze din această cauză, deoarece APK-ul este despachetat în timpul procesului. De exemplu, este posibil ca un APK de 95 MB să eșueze cu o limită de încărcare de 100 MB. În acest caz, măriți limita de încărcare așa cum s-a menționat mai sus.

De asemenea, vă recomandăm să mutați mai întâi manual APK-ul pe un dispozitiv de testare (de exemplu, prin USB) și să încercați să îl instalați manual cu aplicația Fișiere a dispozitivului. Dacă acest lucru nu funcționează din orice motiv, va eșua și prin MDM.

Actualizare țintă

Cu ajutorul funcției "Actualizați ținta", puteți alege ce versiune a unei aplicații trebuie instalată sau la ce versiune trebuie actualizată o aplicație dacă ați activat "Păstrați la zi" pentru o aplicație.

Dacă nu ați selectat o țintă de actualizare, va fi utilizată cea mai recentă versiune.

Rețineți că Android nu poate retrograda aplicațiile. De asemenea, rețineți că "codul versiunii" determină dacă o versiune este mai mare, mai mică sau aceeași. Așadar, asigurați-vă că măriți corect această versiune în aplicația dvs. atunci când creați o actualizare.

iOS

Aici puteți încărca aplicațiile iOS pe care le-ați dezvoltat și le puteți distribui ulterior în Mobile Management în profilul dispozitivului sau al grupului.

Faceți clic pe "+" pentru a încărca IPA-ul unei aplicații pe care doriți să o încărcați. Doar formatul IPA este acceptat deocamdată.

Limita de încărcare pe dispozitivele OnPremise poate fi mărită la Pasul 3 din Configurarea dispozitivului. Dacă doriți să măriți limita de încărcare pe Cloud, vă rugăm să contactați asistența pentru mai multe informații.

Actualizare țintă

Cu ajutorul funcției "Actualizați ținta", puteți alege ce versiune a unei aplicații trebuie instalată sau la ce versiune trebuie actualizată o aplicație dacă ați activat "Păstrați la zi" pentru o aplicație.

Dacă nu ați selectat o țintă de actualizare, va fi utilizată cea mai recentă versiune.

MacOS

Aici puteți încărca aplicațiile MacOS pe care le-ați dezvoltat și le puteți distribui ulterior în Mobile Management în profilul dispozitivului sau al grupului dvs.

Faceți clic pe "+" pentru a încărca PKG-ul unei aplicații pe care doriți să o încărcați. Doar formatul PKG este acceptat deocamdată.

Limita de încărcare pe dispozitivele OnPremise poate fi mărită la Pasul 3 din Configurarea dispozitivului. Dacă doriți să măriți limita de încărcare pe Cloud, vă rugăm să contactați asistența pentru mai multe informații.

Actualizare țintă

Cu funcția "Actualizați ținta" puteți alege ce versiune a unei aplicații trebuie instalată sau la ce versiune trebuie actualizată o aplicație dacă ați activat "Păstrați la zi" pentru o aplicație.

Dacă nu ați selectat o țintă de actualizare, va fi utilizată cea mai recentă versiune.

Windows 10

Aici puteți încărca aplicațiile Windows 10 și le puteți distribui ulterior în Mobile Management în profilul dispozitivului sau al grupului.

Faceți clic pe "+" pentru a încărca APPX, APPXBUNDLE sau MSI al unei aplicații pe care doriți să o încărcați. Doar formatul APPX, APPXBUNDLE sau MSI este acceptat începând de acum.

De asemenea, puteți încărca și defini dependențe pentru o aplicație, care vor fi distribuite și instalate automat înainte de instalarea aplicației dorite.

Limita de încărcare pe dispozitivele OnPremise poate fi mărită la Pasul 3 din Configurarea dispozitivului. Dacă doriți să măriți limita de încărcare pe Cloud, vă rugăm să contactați asistența pentru mai multe informații.

Actualizare țintă

Cu funcția "Actualizați ținta" puteți alege ce versiune a unei aplicații trebuie instalată sau la ce versiune trebuie actualizată o aplicație dacă ați activat "Păstrați la zi" pentru o aplicație.

Dacă nu ați selectat o țintă de actualizare, va fi utilizată cea mai recentă versiune.

Pachet Win32 (.exe)

De asemenea, puteți distribui fișiere .exe/installers pe dispozitivele dvs.

Numele pachetului	Numele care va fi afișat în MDM
Descriere	Descriere afișată în MDM
Fișier pachet	Sunt permise numai fișiere .zip. Introduceți fișierele pe care doriți să le implementați în acest fișier zip.
Contextul de desfășurare	**Sistem**: Comanda de instalare rulează cu privilegii de sistem, care sunt mai mari decât "User". De asemenea, atunci când se utilizează "System", procesul nu are interfață, deci va fi silențios, iar profilul utilizatorului, de exemplu variabilele de mediu precum %AppDat%, nu este accesibil. **User (Utilizator)**: Comanda de instalare are acces la profilul utilizatorului și poate afișa IU dacă este necesar. Notă: Unele procese pot funcționa într-un singur context. De exemplu, dacă un software se instalează în AppData, acesta va funcționa numai atunci când se selectează "User"
Comanda de instalare	Comanda utilizată pentru a instala programul. De exemplu, comanda de instalare pentru un fișier zip care conține "setup.exe" în rădăcina sa, care acceptă parametrul "/s" pentru o instalare silențioasă, comanda de instalare ar fi "setup.exe /s". Fiți conștienți de faptul că diferite programe pot avea parametri diferiți.
Comanda de dezinstalare	Comanda care trebuie executată pentru a dezinstala software-ul prin MDM. De obicei, aceasta indică programul de dezinstalare. De exemplu "C:\Program Files\ExampleSoftware\uninstall.exe".
Cerințe	
Notă: Toate cerințele stabilite trebuie să fie îndeplinite pentru ca software-ul să fie instalat. În caz contrar, acesta nu va fi instalat. Unele câmpuri pot fi obligatorii. Dacă nu este setată nicio valoare pentru o cerință, cerința va fi ignorată.	
Arhitectura sistemului de operare	Arhitectura sistemului de operare
Versiunea minimă a sistemului de operare	Versiunea minimă a sistemului de operare
Spațiu liber minim pe disc (MB)	Spațiu liber minim pe disc (MB)

Memorie fizică minimă (MB)	Memorie fizică minimă (MB)
Numărul minim de procesoare logice	Numărul minim de procesoare logice
Viteza CPU minimă (MHz)	Viteza CPU minimă (MHz)
Cerințe suplimentare	De asemenea, puteți defini manual reguli sau încărca aici un script pentru a efectua verificări suplimentare ale cerințelor, dacă doriți.
Reguli de detectare	
Metoda de detectare	Aici puteți defini cum să detectați dacă aplicația este instalată pe dispozitiv. Comenzile de instalare vor fi executate numai atunci când aceste reguli detectează că aplicația NU este instalată. Comenzile de dezinstalare se execută numai atunci când aceste reguli detectează că aplicația nu este instalată. **Definirea manuală a regulilor**: Vă permite să definiți manual una sau mai multe reguli pentru a verifica, de exemplu, dacă un anumit fișier, dosar, MSI sau cheie de registru este prezent. Dacă toate regulile de detectare date sunt adevărate, aplicația va fi considerată prezentă. **Utilizați scriptul**: Încărcați propriul script cu propriile verificări. Dacă scriptul returnează "$TRUE", aplicația va fi considerată prezentă.
Reguli de detectare	

Setări aplicație

Setări aplicație iOS

Aici puteți defini setările implicite pentru adăugarea unei aplicații la magazinul de aplicații obligatorii sau la magazinul de aplicații pentru întreprinderi.

Notă: Acest lucru stabilește doar ceea ce este selectat în mod implicit la adăugarea aplicațiilor. Aceasta NU modifică setările existente pentru aplicațiile care sunt deja adăugate în aplicațiile obligatorii sau în magazinul de aplicații al întreprinderii.

Țineți-vă la curent	Menține aplicația actualizată în mod automat. Vă rugăm să rețineți că poate dura până la 7 zile de la lansarea unei actualizări până când aplicația este actualizată.
Depășire atunci când nu sunt gestionate	Dacă o aplicație este deja instalată ca negestionată (de către utilizator), aplicația va fi preluată și gestionată de MDM.
Eliminarea aplicației atunci când profilul MDM este eliminat	Dezinstalează aplicația atunci când MDM este eliminat.
Prevenirea copierii de rezervă a datelor aplicației	Împiedică copierea de rezervă a datelor aplicației.

Setări aplicație Android

Aici puteți defini setările implicite pentru adăugarea unei aplicații la magazinul de aplicații obligatorii sau la magazinul de aplicații pentru întreprinderi.

Notă: Acest lucru stabilește doar ceea ce este selectat în mod implicit la adăugare. Aceasta NU modifică setările pentru aplicațiile care sunt deja adăugate în magazinul de aplicații obligatorii sau în magazinul de aplicații pentru întreprinderi.

Țineți-vă la curent	Menține aplicația actualizată în mod automat. Disponibil numai pentru aplicațiile InHouse.
Actualizare client Controlled AppTec360 EMM	Dacă este activat, administratorii pot specifica ținta de actualizare pentru clientul AppTec360 EMM. O listă cu toate versiunile disponibile ale Clientului AppTec360 EMM va fi afișată în "Setări generale" → "Gestionarea aplicațiilor" → "In-House App DB" → "Android".

Aplicații terță parte

Android

Aici puteți seta codul de activare pentru Ikarus.

Setați acest lucru la "Utilizați codul de activare" și introduceți codul de activare aici.

Notă: După introducerea codului și salvarea acestuia, codul nu este încă adăugat la profilul care este trimis către dispozitiv. Trebuie să efectuați orice modificare în profilul dvs. pentru ca codul să fie adăugat la profil. De exemplu, schimbați orice comutator din profil din oprit → pornit → oprit - Salvați → Atribuiți acum.

iOS

Aici puteți introduce licența SecurePIM. După introducerea licenței, apăsați "Salvare modificări" și puteți utiliza opțiunile SecurePIM.

VPP / KNOX Premium

Programul Apples Volume Purchase Program (VPP) vă permite să distribuiți cu ușurință aplicații plătite și gratuite pe dispozitivele dumneavoastră. Acest lucru este foarte recomandat deoarece nu aveți nevoie de un ID Apple pe dispozitive, utilizatorii nu trebuie să confirme instalarea (supravegheată), utilizatorii nu vor trebui să introducă parola ID-ului Apple și puteți distribui cu ușurință aplicații plătite fără a le cumpăra din nou pe fiecare dispozitiv.

Pentru a utiliza VPP trebuie să vă înregistrați în Apple Business Manager.

Licențe VPP

Aici puteți obține o prezentare generală a aplicațiilor VPP, a numărului de licențe utilizate și a numărului de licențe disponibile.

Făcând clic pe roată, veți vedea ce dispozitive au o licență atribuită și care este starea acestei atribuiri.

Făcând clic pe Actualizează cache-ul VPP care compară licențele atribuite în MDM cu licențele atribuite pe partea Apple. Acest lucru poate rezolva problemele de licență în unele cazuri.

Token VPP

Aici puteți încărca tokenul VPP, care poate fi găsit în Apple Business Manager în Setări → Aplicații și cărți. Puteți încărca mai multe jetoane VPP.

Puteți reînnoi un jeton prin simpla descărcare a unuia nou în Apple Business Manager, faceți clic pe roata "Editare" și încărcați noul jeton.

"Modul VPP" decide modul în care este gestionată atribuirea licenței. În funcție de scenariul dvs., trebuie să utilizați moduri diferite:

"Bazat pe dispozitiv" trebuie să fie utilizat la înscrierea dispozitivelor prin intermediul codului QR, linkului, Apple Configurator sau DEP.

"Bazat pe utilizator" este necesar dacă dispozitivele sunt înscrise cu înscrierea utilizatorului sau ca iPad partajat.

Dacă activați "Gestionarea automată a licențelor", utilizatorilor care sunt mutați de la un grup la altul li se vor atribui automat licențe Apple VPP în funcție de profilul grupului în care sunt mutați.

Licențele Apple VPP existente din grupul din care s-au mutat nu vor fi revocate.

Utilizatorilor noi adăugați la un grup li se vor atribui automat licențe Apple VPP în funcție de profilul grupului respectiv.

Cheie KNOX Premium

Aici puteți introduce cheia dvs. KNOX Premium pentru a utiliza Samsung KNOX Container.

Vă rugăm să rețineți că acest lucru nu mai este acceptat de la Android 10. Utilizați în schimb Android Enterprise Container.

Setări App Store

Regiune și limbă

Aici puteți seta limba și regiunea implicite pentru Căutarea aplicațiilor în Gestionarea aplicațiilor.

Vă rugăm să rețineți că setările pentru iTunes definesc, de asemenea, modul în care sistemul preia informații despre anumite aplicații. Dacă întâlniți aplicații în listele dvs. care sunt afișate într-un mod ciudat (de exemplu, lipsește pictograma), este posibil să fi setat o regiune în care aplicația respectivă nu este disponibilă.

AE Magazin Play

Aici puteți găsi toate opțiunile pentru Play Store pentru dispozitive Android Enterprise pentru a aproba aplicații, pentru a încărca propriile aplicații în Play Store sau pentru a vă crea propriile aplicații web.

Aplicații aprobate

Aici puteți obține o imagine de ansamblu asupra tuturor aplicațiilor pe care le-ați aprobat.

Aplicații Play Store

Aceasta va încărca un iFrame care va afișa Magazinul Play. Căutați orice aplicație doriți, faceți clic pe ea și aprobați-o. În timpul aprobării aplicației, puteți defini, de asemenea, ca aprobarea să fie revocată dacă permisiunile necesare se modifică. Vă recomandăm să lăsați aceste setări implicite atunci când aprobați aplicații.

După ce o aplicație a fost aprobată, o puteți adăuga la profilurile dvs.

Butonul "Aprobă" se va schimba în "Revocă aprobarea" după aprobare, astfel încât să puteți elimina oricând aplicațiile dacă nu mai aveți nevoie de ele.

Aplicații private

Aici puteți încărca propria dvs. aplicație ca aplicație privată în Magazinul Google Play. Acest lucru vă permite să distribuiți aplicația prin intermediul serviciilor Google și să o actualizați prin intermediul

acestora. Acest lucru are, de asemenea, avantajul că propriile aplicații pot fi instalate fără confirmarea utilizatorului, care în mod normal este necesară.

Aplicații web

Aici puteți crea aplicații web, care sunt legături către anumite pagini web care pot fi atribuite ca aplicații.

Puteți, de asemenea, să îi dați o pictogramă personalizată și să definiți mai precis modul în care este afișată.

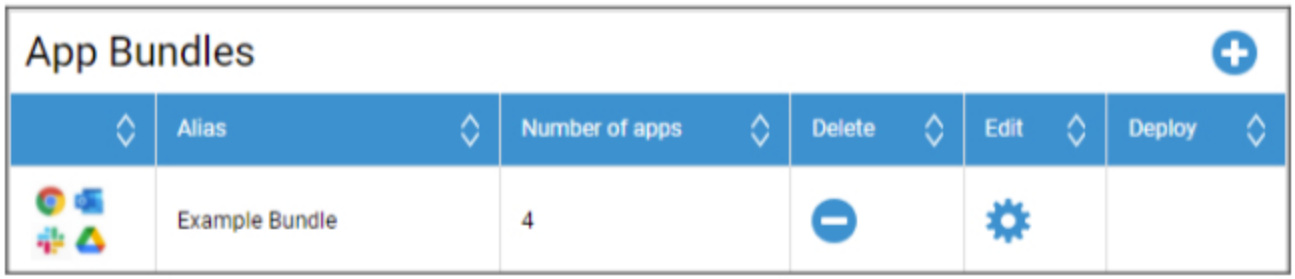
Layout magazin

Layout-ul Magazinului definește modul în care sunt afișate aplicațiile în Magazinul Play sau dacă acestea sunt afișate deloc.

Rețineți că, dacă doriți să afișați aplicații în Play Store pentru ca utilizatorul să le instaleze manual, acestea trebuie adăugate aici în Layout **ȘI** în profil la Magazinul Play al întreprinderii. Dacă adăugați o aplicație doar la unul dintre ele, aceasta nu va fi afișată.

Pachet de aplicații

Cu pachetele de aplicații puteți defini grupuri de aplicații care pot fi atribuite profilurilor de dispozitiv sau de grup cu un singur clic.



Faceți clic pe "+" pentru a crea un nou pachet de aplicații. După crearea unui pachet de aplicații, puteți face clic pe "Editare" pentru a adăuga aplicații din diverse surse la pachet.

Un pachet poate fi adăugat la profiluri ca orice altă aplicație. Atunci când adăugați aplicații, veți avea un tab suplimentar numit "Grupuri de aplicații" în care veți avea Grupurile.

Dacă efectuați orice modificare la un App Bundle, va apărea un buton în coloana "Deploy". Acesta vă va permite să împingeți aceste modificări către toate profilurile care conțin acest pachet. Așadar, rețineți că trebuie să faceți acest lucru manual după adăugarea sau eliminarea aplicațiilor dintr-un pachet.

Telecomandă

TeamViewer

Conector TeamViewer

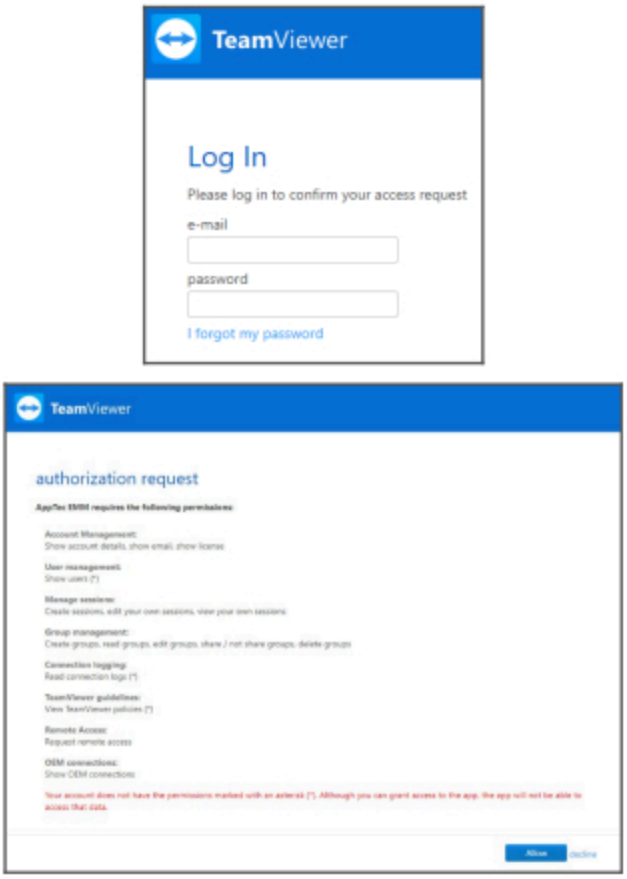
Notă: În versiunea de încercare gratuită a versiunii noastre cloud nu puteți să vă conectați contul TeamViewer. În schimb, veți avea un cont demo gratuit conectat automat.

Accesați Setări generale -> Control la distanță -> TeamViewer. Aici puteți conecta contul TeamViewer la consolă sau puteți vedea informații despre contul dvs. conectat în prezent. De asemenea, puteți vizualiza toate sesiunile active în prezent dacă mergeți la "Active Sessions" (Sesiuni active).

Pentru a vă conecta contul, faceți clic pe "Start Setup".

Astfel, veți fi redirecționat către o nouă pagină unde va trebui să vă conectați cu contul TeamViewer.

După conectare, trebuie să autorizați AppTec360 MDM să utilizeze acest cont. După confirmare, trebuie să așteptați câteva secunde și contul este conectat.


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

Instalați TeamViewer QuickSupport

Adăugați aplicația "TeamViewer QuickSupport" la aplicațiile obligatorii din profilul dispozitivului dvs. sau din profilul de grup și faceți clic pe "Assign Now". Așteptați până când aplicația este instalată pe dispozitiv.

Dacă încercați să accesați un dispozitiv pe care aplicația nu este instalată, aceasta va fi instalată sau vi se va cere să o instalați, în funcție de configurația dispozitivului.

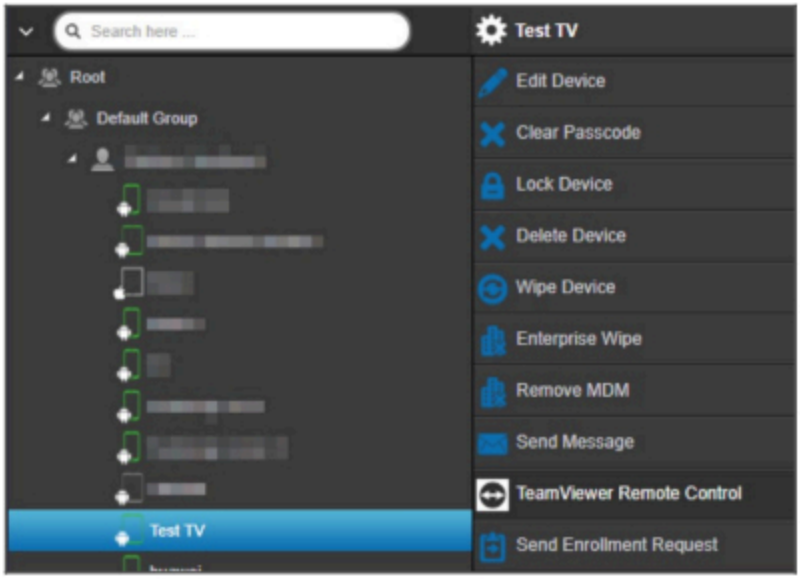
Controlați de la distanță dispozitivul dvs.

Pentru a vă controla dispozitivul de la distanță, selectați dispozitivul, faceți clic pe rotiță și alegeți "TeamViewer Remote Control"

Dacă există deja o sesiune activă, puteți fie să utilizați sesiunea veche, fie să creați una nouă.

Confirmați că doriți să creați o nouă sesiune TeamViewer.

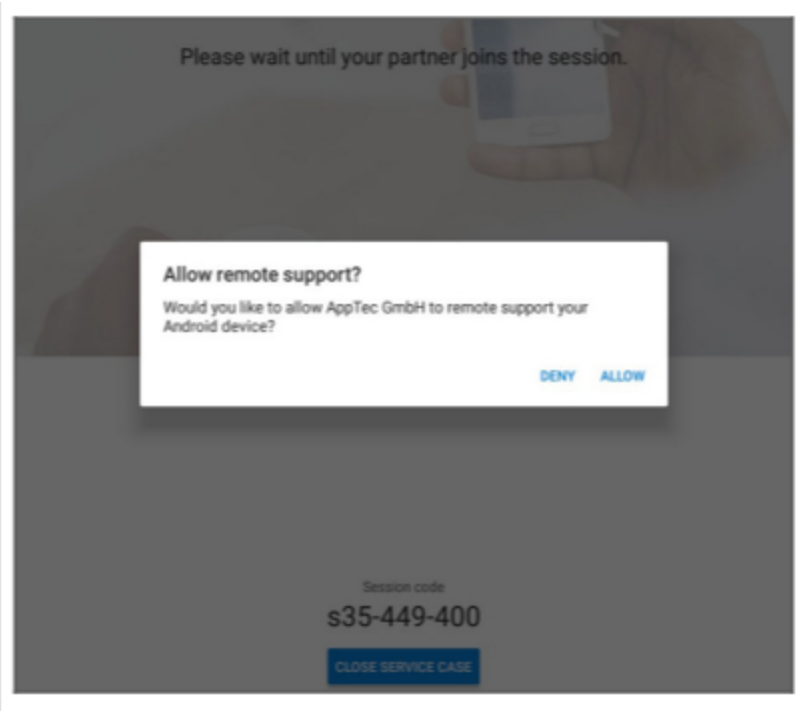
După câteva secunde, veți primi un link pentru sesiunea TeamViewer. Puteți face clic pe "Start" pentru a deschide acest link într-o fereastră nouă.


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

Acest link va deschide TeamViewer-ul instalat și vă va conecta la dispozitivul dvs.

Acum trebuie să confirmați conexiunea pe dispozitivul în sine pentru a-l controla de la distanță.

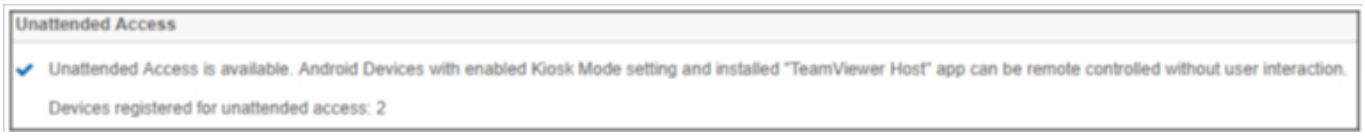


Dacă utilizați iOS, veți primi un mesaj în AppTec360 MDM Client. Cu acest link, dispozitivul se va alătura sesiunii la distanță. În funcție de setările de notificare ale dispozitivului, este posibil să nu primiți o notificare și să trebuiască să deschideți manual AppTec360 MDM Client.

Pe unele dispozitive Android (de exemplu, Samsung) este necesar să instalați o aplicație suplimentară ca addon. Aplicația TeamViewer de pe dispozitiv vă va informa în acest sens, dacă acest lucru este necesar pe dispozitivul dvs.

Acces nesupravegheat

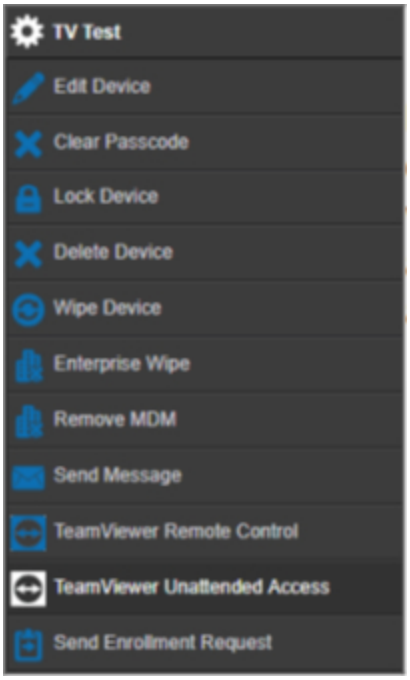
Notă: Accesul fără supraveghere este posibil numai pe dispozitivele Android.



Vă puteți conecta la dispozitivele dvs., fără a accepta conexiunea pe dispozitiv, numai dacă contul dvs. TeamViewer utilizează o licență "Tensor" sau "Corporate".

Puteți verifica acest lucru, după conectarea contului dvs., în "Setări generale"

Pentru a utiliza accesul nesupravegheat, trebuie să instalați aplicația "TeamViewer Host" și să activați "Enable Unattended Access" în "Kiosk Mode & Launcher" în profilul dvs. Vă rugăm să rețineți că acest lucru este posibil numai dacă utilizați modul Kiosk.



Acum puteți selecta accesul nesupravegheat dacă vă selectați dispozitivul și faceți clic pe roată. Acest lucru vă va conecta la dispozitivul dvs. fără a fi nevoie de confirmare pe dispozitivul însuși. Vă rugăm să fiți conștienți de faptul că poate dura câteva momente până când veți primi link-ul de acces la dispozitivul dvs.

Splashtop

Dacă activați opțiunea Splashtop, veți vedea opțiunile de configurare Splashtop în profilurile dvs.

Pentru a utiliza Splashtop, trebuie să setați Splashtop Streamer (com.splashtop.streamer.csrs) ca aplicație obligatorie în profilul dvs. După aceea, puteți activa Configurarea Splashtop în profilul dvs. în "Control de la distanță". Activarea acesteia va configura aplicația Splashtop Streamer. Dacă utilizați Splashtop Streamer, dar nu în combinație cu MDM, trebuie să dezactivați această opțiune.

În profilul dvs. sub "Control de la distanță" trebuie să setați și un cod de implementare. Accesați https://my.splashtop.com și autentificați-vă în contul Splashtop. Faceți clic pe "Add Computer" (Adăugare computer) și copiați codul de desfășurare de 12 cifre din pagina rezultată.

Fără codul Deploy, controlul de la distanță NU este posibil.

După ce ați făcut acest lucru, puteți face clic dreapta pe dispozitivul dvs. și puteți începe o sesiune la distanță făcând clic pe "Splashtop Remote Control"

Gestionarea cartelei Sim

Import masiv CSV

Aceasta afișează o imagine de ansamblu asupra cartelelor Sim alocate și a tuturor informațiilor despre acestea. Acest lucru vă ajută să aveți toate informațiile, nu numai despre dispozitivele dvs., ci și despre cartelele Sim într-un singur sistem.

NOTĂ: Aceasta este o gestionare/documentare manuală. Nu este posibilă obținerea automată a acestor date de la dispozitive din cauza mecanismelor de confidențialitate/securitate ale sistemelor de operare.

De asemenea, puteți ex- și importa această listă ca CSV.

Transportator și tarif

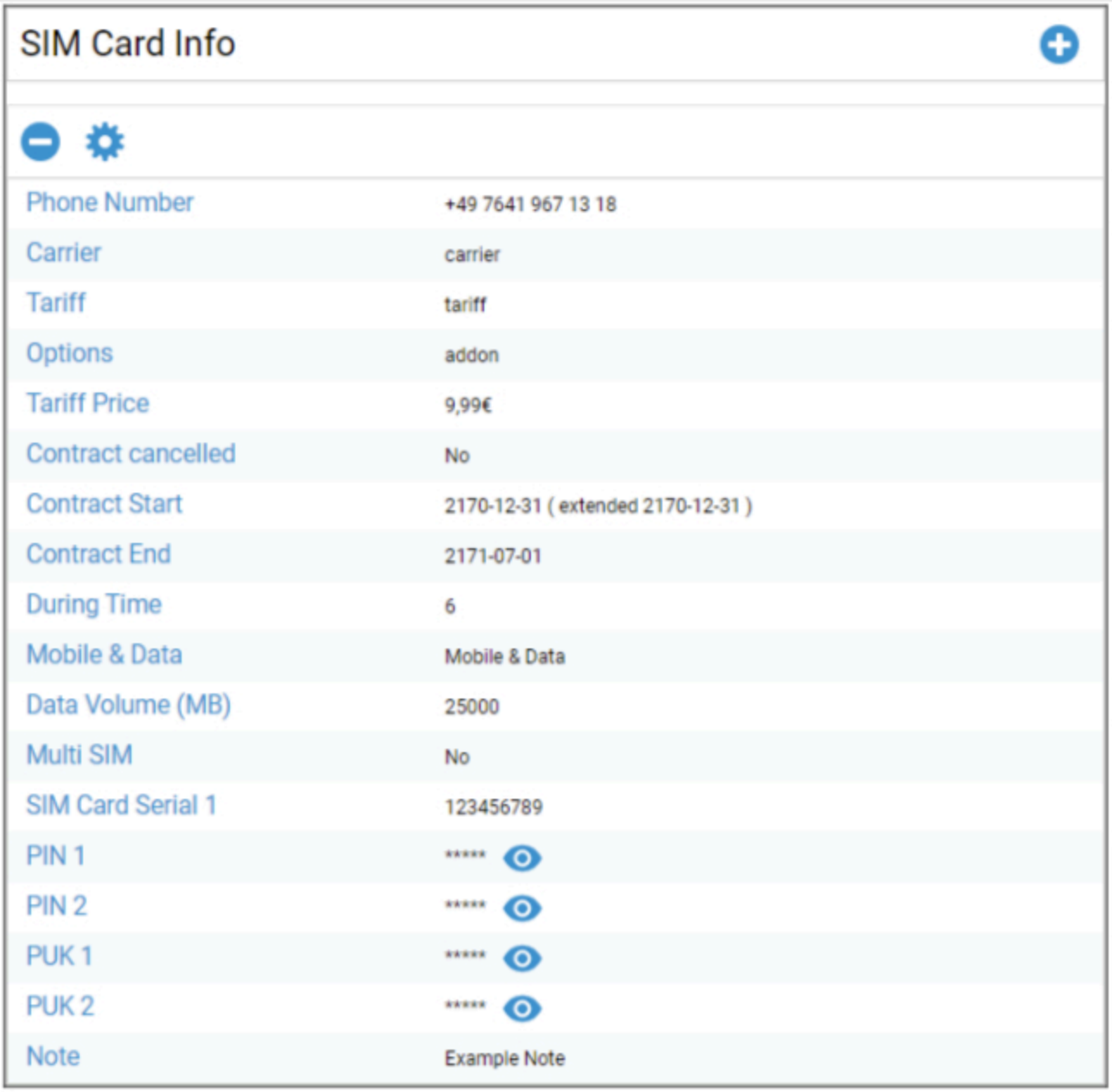
Pentru a adăuga o cartelă Sim, faceți mai întâi clic pe butonul pentru a adăuga unul sau mai mulți operatori.

Ulterior, faceți clic pe "+" pe "Informații tarifare" pentru a adăuga un tarif unui transportator.

Opțional, puteți adăuga Add-Ons opționale mai jos dacă aveți ceva de genul acesta.

Acesta a pregătit tot ce aveți nevoie pentru a adăuga un card Sim real. Cardurile Sim sunt alocate în prezent unui utilizator. Prin urmare, accesați Mobile Management, selectați un utilizator și accesați "Sim Card Overview.

Aici puteți vedea cartelele SIM ale acestui utilizator. Dacă există una, o puteți edita sau elimina. Utilizatorii pot avea mai multe cartele Sim.

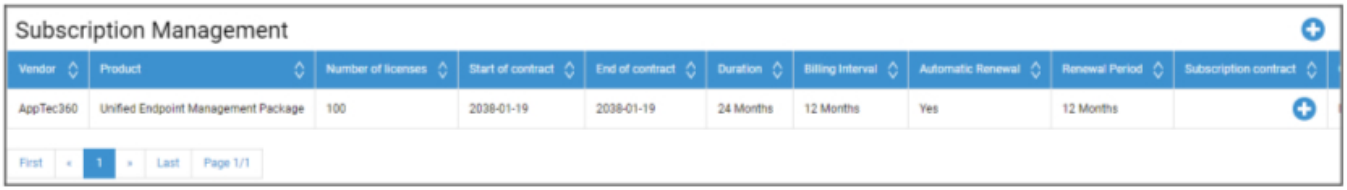


Faceți clic pe "+" pentru a adăuga o cartelă SIM și adăugați toate informațiile necesare. Aceste cartele Sim vor fi, de asemenea, listate în lista tuturor cartelelor Sim din Setări generale → Gestionare cartele Sim.

Gestionarea abonamentelor

Gestionarea abonamentelor

Aici puteți documenta abonamentele în derulare, detaliile acestora și, de asemenea, puteți stoca diferite fișiere, de exemplu, contractul semnat, scrisoarea de reziliere etc. De asemenea, puteți configura memento-uri care vă reamintesc prin e-mail înainte de terminarea abonamentului și poate se prelungește automat.



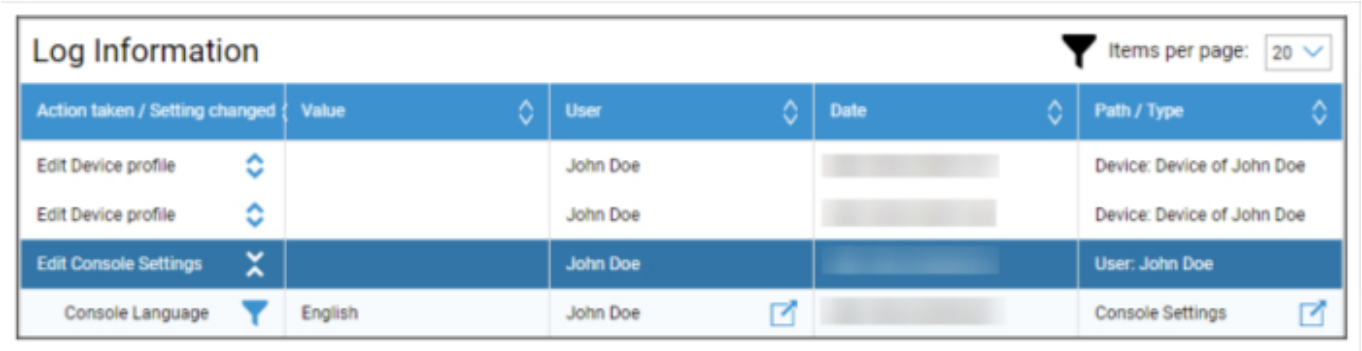
Faceți clic pe "+" din partea de sus pentru a adăuga un abonament. Puteți adăuga cât de multe abonamente doriți.

Faceți clic pe "+" în diferitele câmpuri pentru a încărca fișiere referitoare la acest abonament. Tehnic, puteți încărca orice tip de fișier, dar rețineți că nu toate tipurile de fișiere pot fi previzualizate în browser.

Jurnalul general de audit

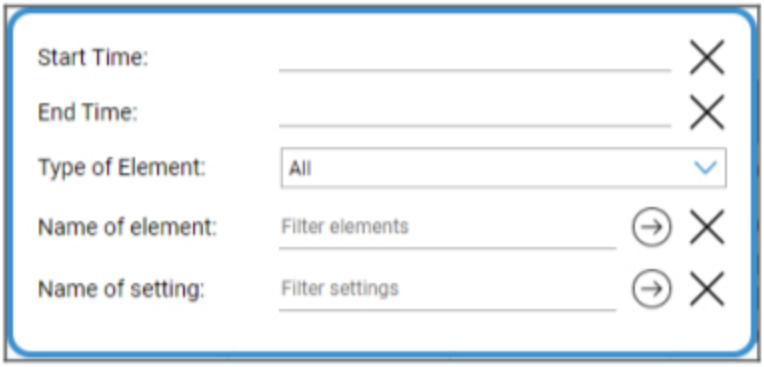
Jurnal de audit

Aici aveți un jurnal de audit general care arată toate modificările efectuate. În timp ce jurnalul de audit al unui utilizator sau grup afișează numai modificările referitoare la acest utilizator sau grup, acesta afișează TOATE modificările efectuate oriunde în consolă.



Puteți vedea ce a fost modificat, de către cine, când și unde. În unele cazuri, puteți, de asemenea, extinde intrarea pentru a vedea detalii suplimentare.

Este posibil să faceți clic pe utilizator sau pe intrarea din "Cale / Tip" pentru a ajunge la locația în care a fost efectuată modificarea.



În partea din dreapta sus puteți defini, de asemenea, un filtru care poate ajuta la găsirea anumitor modificări într-un mediu în care au loc multe modificări.

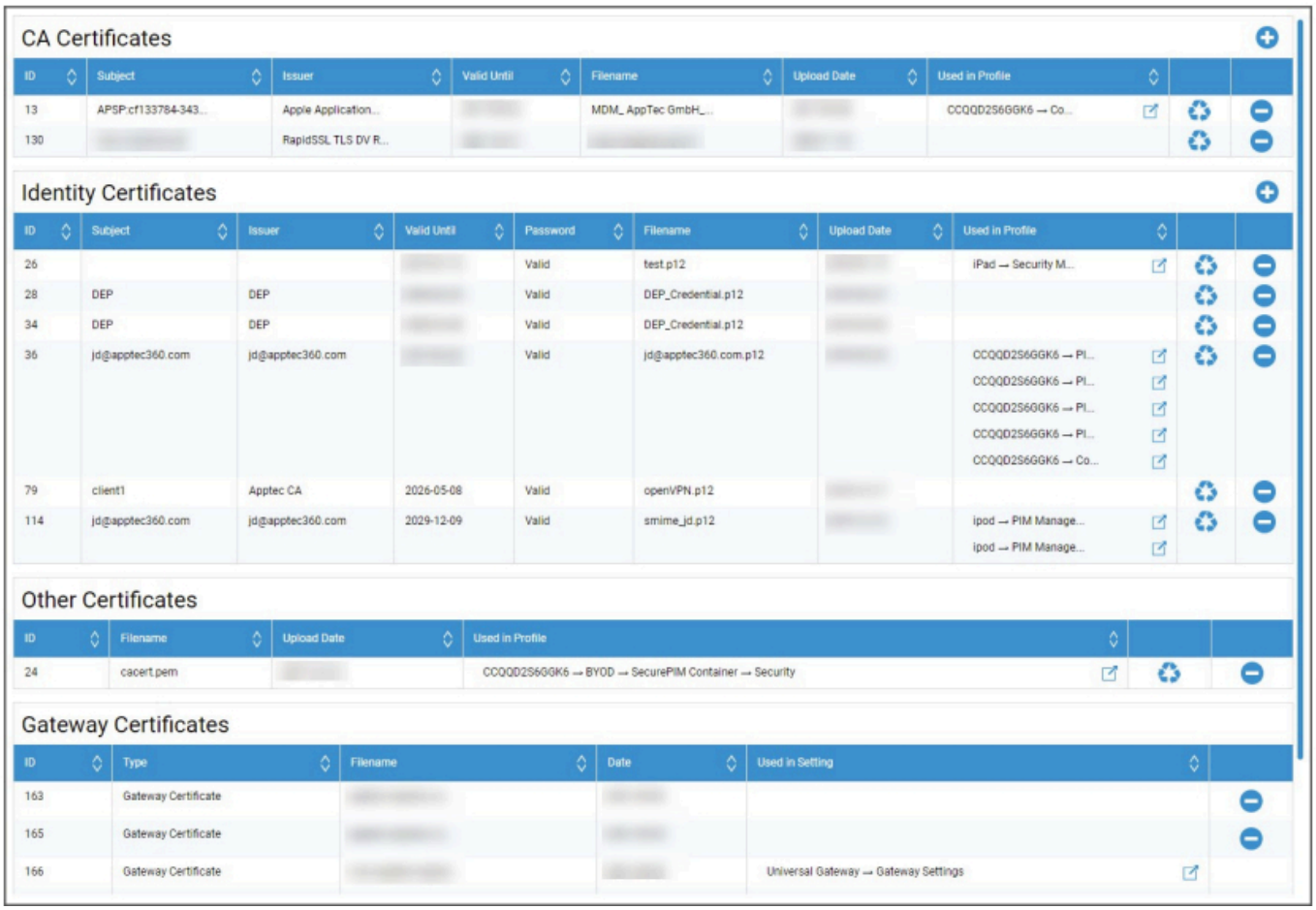
Setări jurnal de audit

"Perioada de păstrare a jurnalelor de audit" definește cât timp trebuie păstrate jurnalele de audit înainte de ștergere.

Managementul certificatelor

Aici veți obține o prezentare generală a tuturor certificatelor încărcate și utilizate în consolă. Aceasta este doar o prezentare generală. Configurarea efectivă pentru, de exemplu, certificatele Wi-Fi se face în continuare în profil, la locația corespunzătoare.

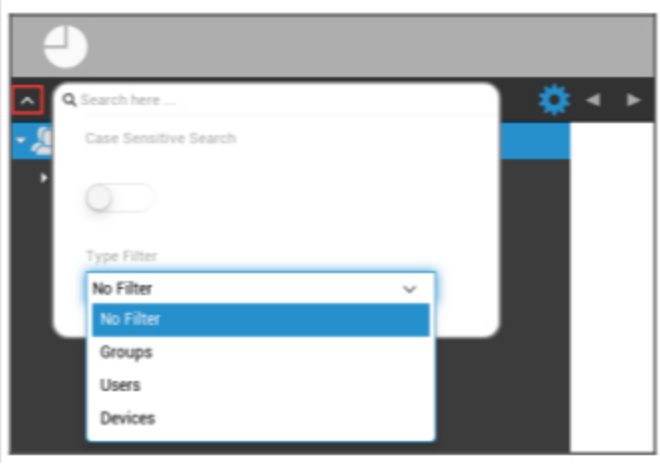
Aici puteți, de asemenea, să eliminați sau să actualizați certificate, care se vor reflecta automat în profilurile afectate. Faceți clic pe informațiile din "Used in Profile" (Utilizat în profil) pentru a vedea unde anume mai este atribuit un certificat.



Management mobil

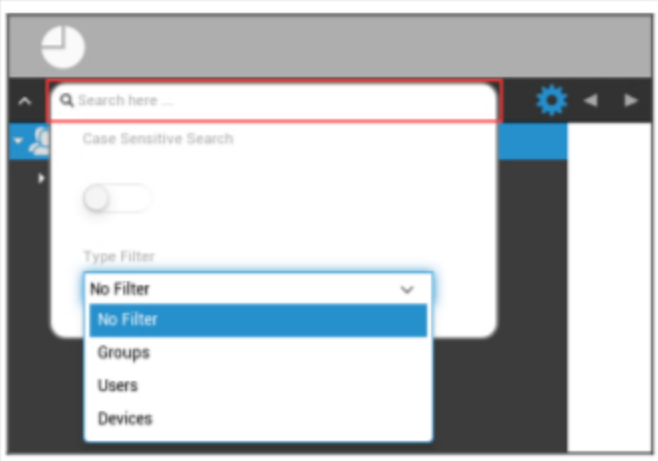
Ecran de gestionare mobilă

Filtru dispozitiv



Cu un clic în colțul din stânga sus al ecranului, puteți găsi o varietate de filtre pentru afișarea dispozitivelor.

Fereastra de căutare



Fereastra de căutare vă permite să căutați toate dispozitivele și/sau utilizatorii cu un anumit cuvânt cheie.

Angrenaj opțiuni

După ce faceți clic pe simbolul respectiv, este afișată o listă de opțiuni disponibile.

Acestea se schimbă cu fiecare fereastră curentă și sunt explicate în capitolele respective.

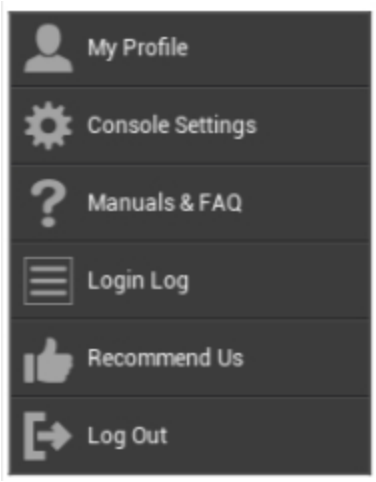
Săgeți de navigare

Cu un clic pe săgeata din stânga, veți fi redirecționat către pagina anterioară.

Apoi, cu un clic pe săgeata din dreapta, veți fi dus la pagina pe care tocmai ați părăsit-o.

Administrare setări cont

Făcând clic pe adresa de e-mail, așa cum se vede mai sus, se afișează următorul meniu:



Profilul meu	Modificați detaliile contului de administrator
Setări consolă	Configurați setările consolei pentru contul Admins
Manuale și întrebări frecvente	Vizualizați pagina "Manuale și întrebări frecvente" în "Setări generale"
Jurnal de conectare	Accesați "Jurnalul de conectare"
Recomandă-ne	Vizualizați pagina "Recomandă-ne" în "Setări generale"
Deconectare	Ieșiți din consola MDM

Informații privind utilizatorul

Aici puteți edita detaliile contului administratorului conectat în prezent.

Nume utilizator	Numele de utilizator și/sau adresa de e-mail a contului
Nume și prenume	Prenumele administratorilor
Numele de familie	Numele de familie al administratorilor
Nume de utilizator	Numele de autentificare al administratorilor
Adresa eMail	Adresa de e-mail a administratorilor
Adresa de e-mail alternativă	Adresa de e-mail alternativă a administratorilor
Imagine	Imagine de profil
Număr de telefon	Numărul de telefon al administratorilor
Număr de mobil	Numărul de telefon mobil al administratorilor
Extensie telefon	Extensie telefon
Locație	Locație
Poziția	Poziția în cadrul societății
Grup de utilizatori	Selectați grupul de utilizatori căruia doriți să îi atribuiți contul de administrator
Comentariu	Introduceți un comentariu
Introduceți parola nouă	Introduceți parola pentru o schimbare a parolei
Repetați parola nouă	Repetați noua parolă pentru confirmare

Vă rugăm să rețineți că accesul de administrare poate fi, de asemenea, depus ca un cont de utilizator local în structura ierarhică. Fără stabilirea unui administrator suplimentar, acesta nu ar trebui să fie șters!

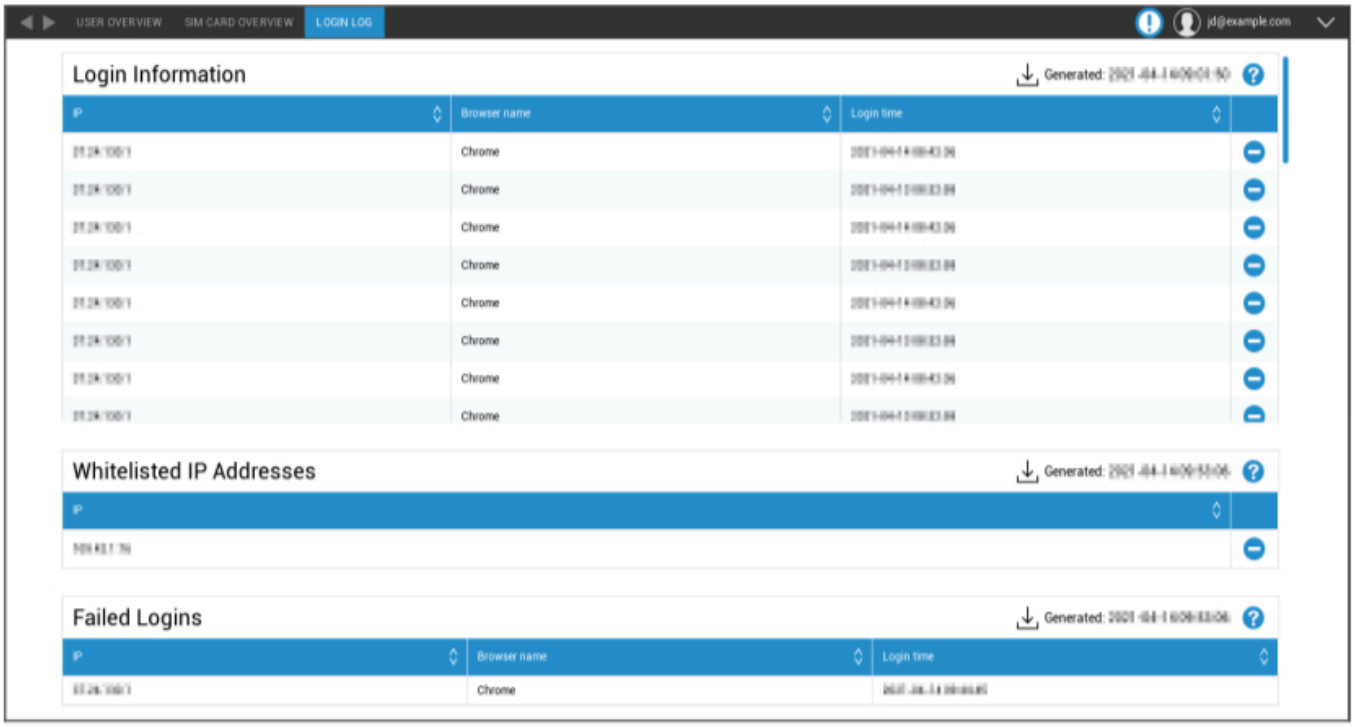
Setări consolă

Aici puteți configura următoarele setări ale consolei pentru contul Admins:

Opțiuni de afișare a utilizatorului din director	Definiți modul în care utilizatorii ar trebui etichetați în arbore
Opțiuni de afișare a dispozitivului director	Definiți modul în care dispozitivele ar trebui etichetate în arbore
Timeout sesiune	Dacă utilizatorul nu face nimic în timpul specificat, acesta va fi deconectat. Valoarea implicită este de 60 de minute. Vă rugăm să vă deconectați și să vă conectați din nou după modificarea acestei setări.
Zona orară	Alegeți fusul orar care este utilizat
Format de timp	Alegeți modul de afișare a marcajelor temporale
Limba consolei	Alegeți limba în care trebuie să fie afișată consola. Sunt disponibile limbile engleză și germană.
Culoare principală	Puteți seta o culoare care va fi utilizată ca bază pentru schema de culori a consolei. Puteți fie să utilizați selectorul de culori, fie să introduceți o culoare în notația HTML HEX. Formatoarele RGB precum "roz", "galben" funcționează de asemenea.
Salvare comandă	Combinația de taste pentru a declanșa o salvare fără a apăsa butonul "Salvare".
Utilizați autentificarea cu doi factori	Activați utilizarea autentificării cu doi factori la conectare. Veți primi un e-mail la conectare cu un cod pe care va trebui să îl introduceți pentru a vă conecta.
Timeout de autentificare cu doi factori	Setați o perioadă de timp în care nu vi se va solicita o autentificare cu doi factori după o autentificare deja reușită.
Trimiteți codul de verificare prin	Codul de verificare va fi trimis la opțiunile selectate. Mesajul dispozitivului va fi afișat în AppTec360 MDM App pe toate dispozitivele Android și iOS care vă aparțin.
Trimiteți mesajul de conectare după conectare	Dacă este activat, va fi trimis un e-mail pentru fiecare autentificare de la o adresă IP care nu este pe lista albă. E-mailul conține informații despre autentificare (de exemplu, IP, browser).

Jurnal de conectare

Aici puteți vedea informații referitoare la autentificările contului de administrator conectat în prezent.



Informații de conectare	O listă care conține autentificările contului de administrator conectat în prezent, înregistrate de consolă. Această listă afișează toate autentificările reușite în ultimele 30 de zile.
Adrese IP pe lista albă	Aceasta este lista tuturor adreselor dvs. IP din lista albă. Dacă vă conectați de la un IP care este listat aici, nu veți primi mesajul de conectare. Puteți adăuga o adresă IP la această listă făcând clic pe butonul de lângă o intrare din lista "Informații de conectare" de mai sus. Puteți elimina o adresă IP din această listă făcând clic pe butonul de lângă o intrare din această listă sau din lista "Informații de conectare" de mai sus.
Autentificări eșuate	Aceasta este o listă a tuturor încercărilor de conectare eșuate din ultimele 30 de zile. Dacă nu ați reușit să introduceți parola corectă de cel puțin 3 ori în 20 de minute, va apărea o intrare în această listă. De asemenea, veți fi informat prin e-mail cu privire la încercările eșuate de conectare.

Administrația corporativă (Root-Node) în Mobile Management

După ce ați ajuns la Root-Node (primul grup), puteți efectua o serie de setări pentru compania dvs., în ceea ce privește Mobile Management.

Crearea unui subgrup	Crearea unui subgrup
Redenumirea nodului rădăcină	Redenumirea nodului rădăcină (de exemplu, numele companiei dvs.)
Înscrierea în masă	Înscrierea mai multor dispozitive/utilizatori în același timp
Atribuirea masei	Atribuiți un profil pentru grupurile respective, cu o singură privire
Administrare rapidă a aplicației	Trimiteți cereri de (dez)instalare pentru o aplicație către grupurile de dispozitive respective
Import utilizator CSV	Importați utilizatorii din CSV în grupul respectiv

Crearea unui subgrup

Cu "Creați un subgrup" puteți crea un subgrup suplimentar.

Puteți stabili sub ce grup ar trebui să fie atribuit subgrupul.

(În mod implicit, este creat un nou grup care este atribuit ca subgrup în nodul rădăcină)

Redenumirea nodului rădăcină

Aici vă puteți redenumi numele rădăcină. De obicei, în acest caz se utilizează numele companiei.

Înscrierea în masă

Cu "Înscriere în masă" puteți înscrie mai multe dispozitive și utilizatori.

Puteți selecta direct modul în care utilizatorul trebuie să primească înscrierea (e-mail; e-mail alternativ; SMS)

În funcție de dispozitivul pe care îl va primi utilizatorul (iOS, Android, Windows Phone), puteți marca direct acest lucru aici.

Distincția dintre smartphone și tabletă poate fi configurată și aici, pe care va trebui să o selectați corect, cu o bifă.

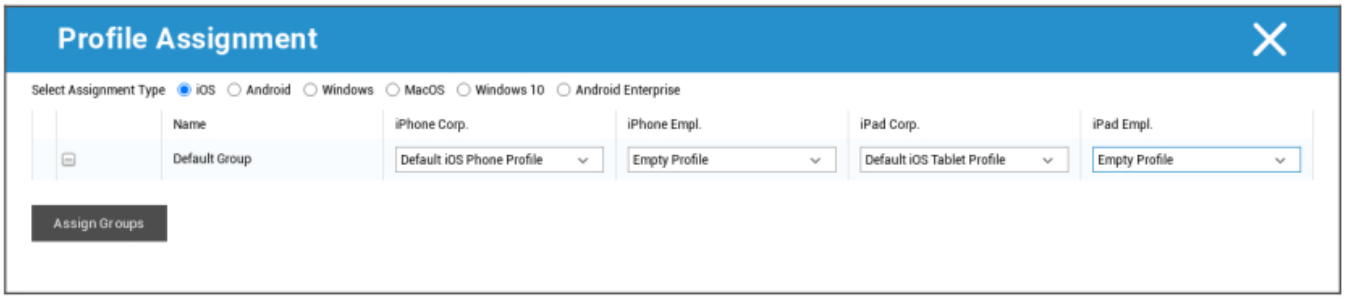
Ca ultim pas, puteți stabili dacă dispozitivul respectiv este corporativ sau privat (BYOD).

Cu "Export as CSV", puteți exporta informațiile ca fișier de date CSV. În schimb, puteți importa și fișierul de date CSV cu "Import CSV", fișierul ar trebui să arate ca exemplul de mai jos:

Philipp Reiss; philipp.reis@apptec360.com; pr@apptec360.com; +41 61 511 3210;

Atribuirea masei

Sub Atribuire în masă puteți atribui un profil tuturor grupurilor, acesta fiind împărțit în iOS - Android - Windows - MacOS - Windows 10 - Android Enterprise

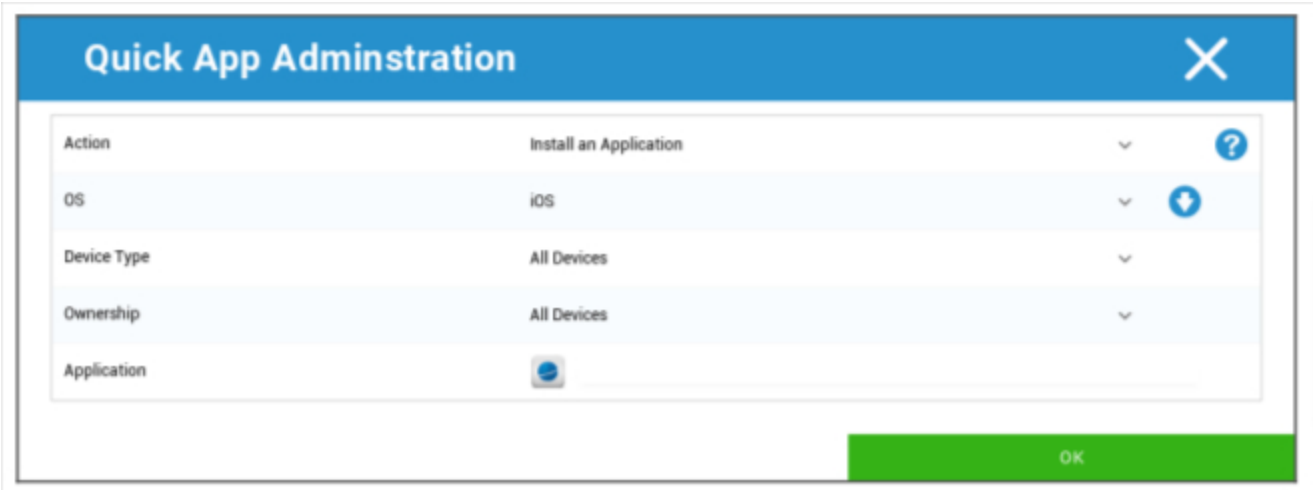


Windows - MacOS - Windows 10 - Android Enterprise

Administrare rapidă a aplicației

Sub Administrarea rapidă a aplicațiilor puteți trimite cereri de instalare sau dezinstalare pentru o anumită aplicație către un sistem de operare ales de dvs.

De asemenea, puteți defini dacă solicitarea trebuie trimisă tuturor tipurilor de dispozitive ale sistemului de operare selectat sau numai unui anumit tip de dispozitiv.



Import utilizator CSV

Importați utilizatorii din CSV în grupul respectiv.

Cu "Descărcare șablon CSV", puteți exporta un fișier șablon CSV, care poate fi completat (sau poate fi utilizat ca referință).

De asemenea, puteți utiliza opțiunile "Show Role Ids" și "Show Group Ids" ca referință pentru a vă crea propriul fișier CSV.

Fișierul CSV poate fi încărcat în MDM cu "Upload CSV".

Ca ultim pas, puteți începe importul făcând clic pe "Start Import".

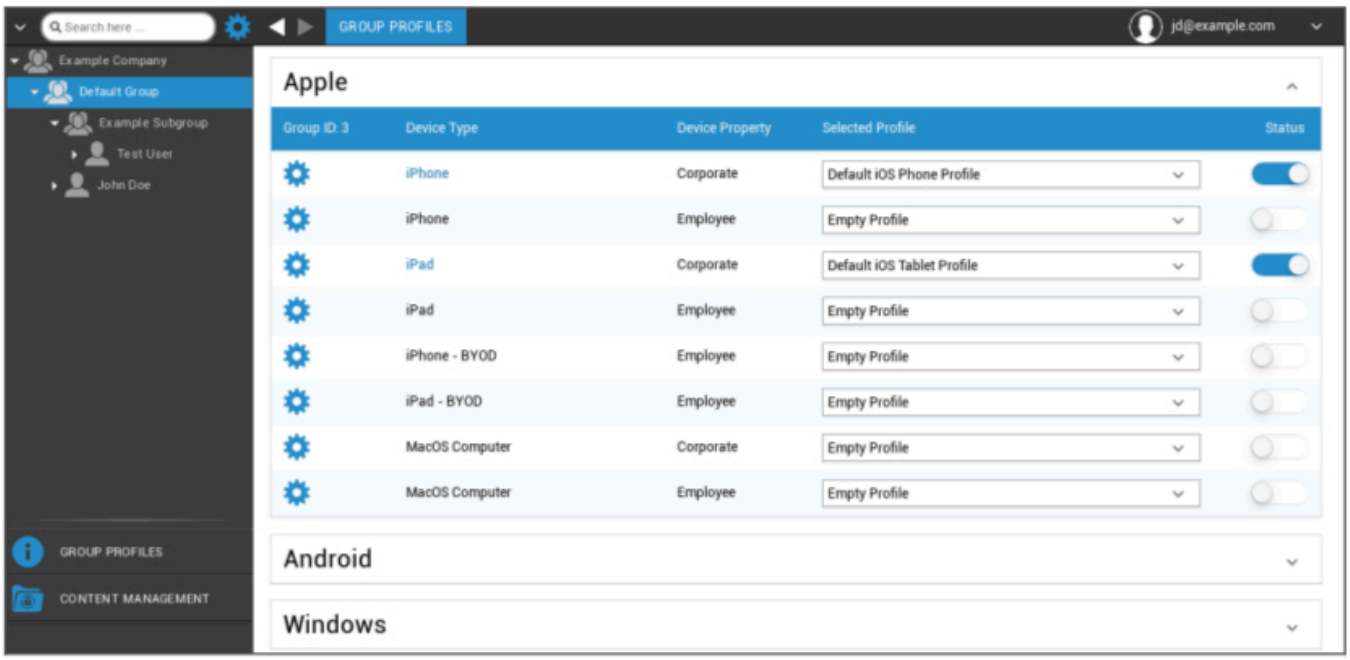
Management de grup în managementul mobil

Un clic pe prezentarea generală afișează diferitele profiluri de configurare pentru platformele respective.

Un profil conține toate opțiunile de configurare care pot fi stabilite în prealabil cu AppTec360 pe dispozitivul utilizatorului final. Pe fiecare platformă puteți crea profiluri pentru dispozitive corporative (Corporate) sau pentru dispozitive de tip Bring-Your-Own-Device (Employee).

Pentru a diferenția configurațiile pentru grupurile de dispozitive, de exemplu în funcție de locație sau funcție, se recomandă crearea mai multor subgrupuri.

Vă rugăm să țineți cont de Gestionarea profilului în Gestionarea telefoniei mobile



Cu ajutorul meniului de unelte, setați o varietate de setări pentru (sub)grupul respectiv.

Crearea unui subgrup	Crearea unui subgrup pentru (sub)grupul respectiv
Editarea grupului selectat	Editarea grupului selectat
Ștergeți grupul selectat	Ștergeți grupul selectat
Înscrierea în masă	Înscrierea simultană a mai multor dispozitive / utilizatori pentru profilul selectat
Atribuirea masei	Atribuiți profiluri grupului care este selectat în prezent
Crearea unui subgrup	Crearea unui subgrup pentru (sub)grupul respectiv

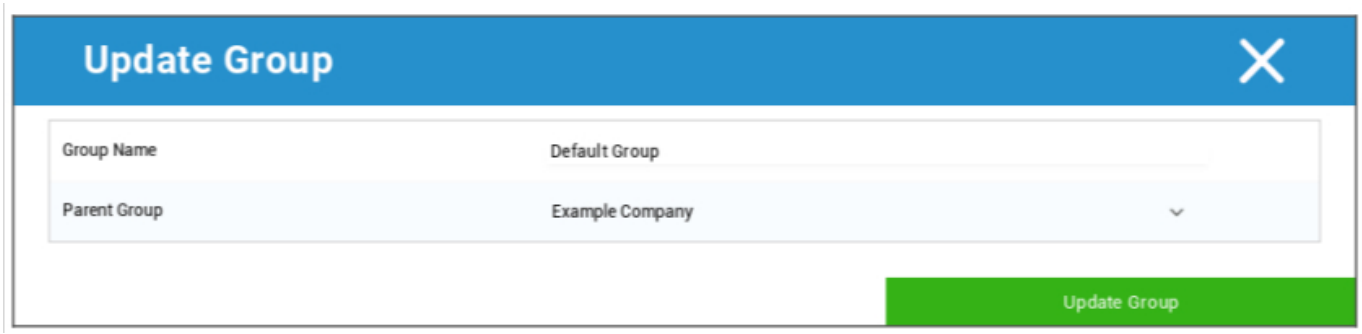
Crearea unui utilizator	Crearea unui utilizator pentru (sub)grupul respectiv

Crearea unui subgrup

Cu "Creați un subgrup", puteți crea un subgrup suplimentar.

Puteți stabili sub ce grup va fi atribuit subgrupul (în mod implicit, subgrupul este atribuit grupului care este selectat în prezent).

Editarea grupului selectat



Aici puteți edita profilul - aici sunt posibile următoarele setări:

- Numele grupului poate fi schimbat
- Grupul de părinți poate fi schimbat

Ștergeți grupul selectat

Sub "delete selected Group" (șterge grupul selectat) sunt afișate toți utilizatorii și dispozitivele care fac parte din grupul respectiv. Aici, aveți opțiunea de a le șterge.

Pentru un utilizator puteți efectua următoarele comenzi de ștergere:

Ștergeți utilizatorul	Utilizatorul este șters
Mutați utilizatorul în grup:	Puteți muta utilizatorul într-un alt grup (următoarea coloană, ex. "Admins)

Pentru un dispozitiv puteți efectua următoarele comenzi de ștergere:

Ștergere și ștergere	Ștergeți și ștergeți dispozitivul
Ștergeți din sistem	Scoateți dispozitivul numai din AppTec

Referință: Înscrierea în masă

Referință: Atribuirea masei

Crearea unui utilizator

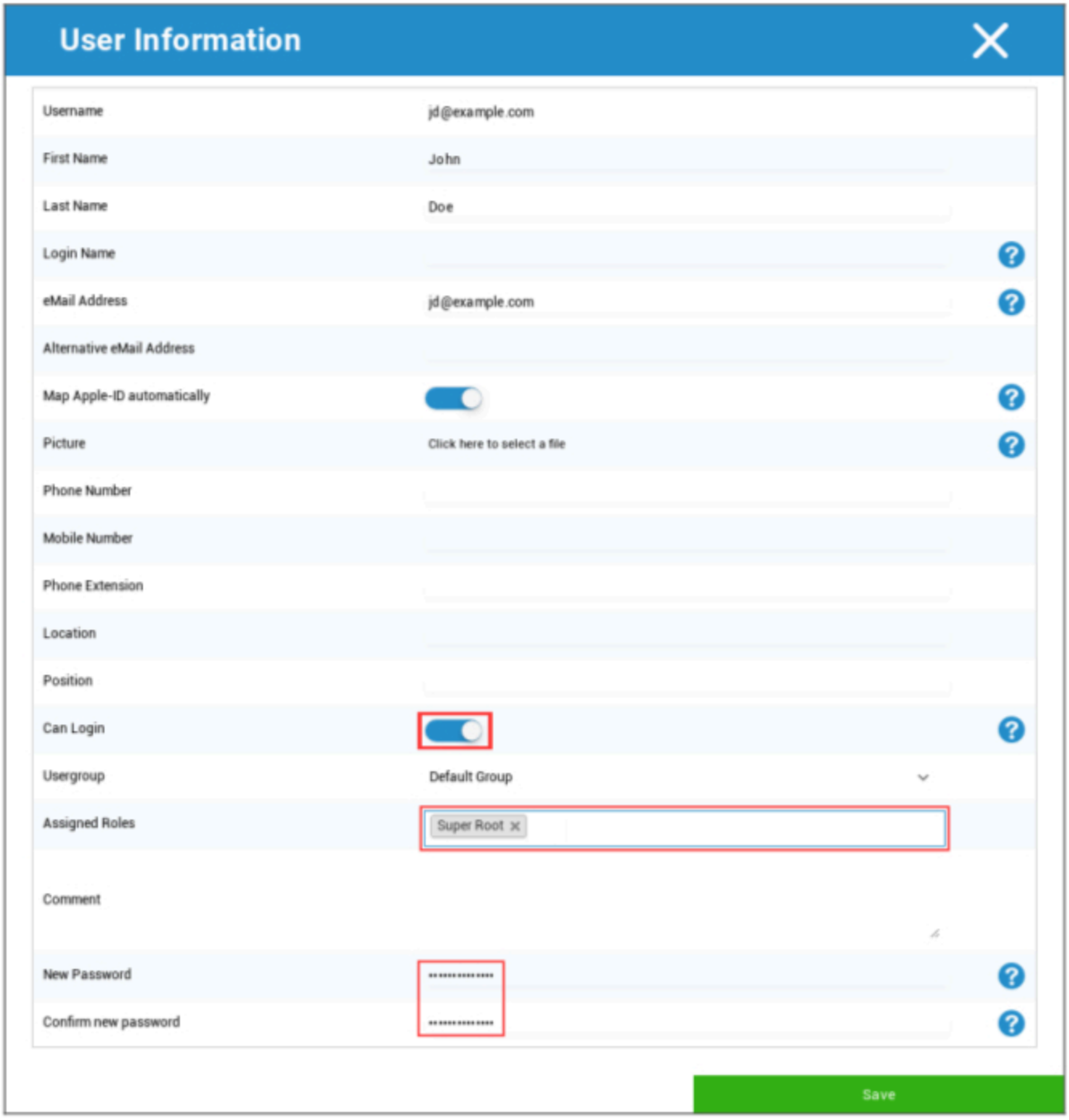
Cu "Creați un utilizator", puteți adăuga un utilizator nou.

Creați un nou utilizator administrator

Puteți seta un utilizator ca Admin-User. Acest lucru îi va da permisiunea de a se conecta la consolă și, de asemenea, de a schimba utilizatori/grupuri/dispozitive.

Creați un utilizator normal sau utilizați un utilizator existent. Alegeți utilizatorul căruia doriți să îi acordați permisiuni de administrare, faceți clic pe rotiță și alegeți "Editare utilizator":

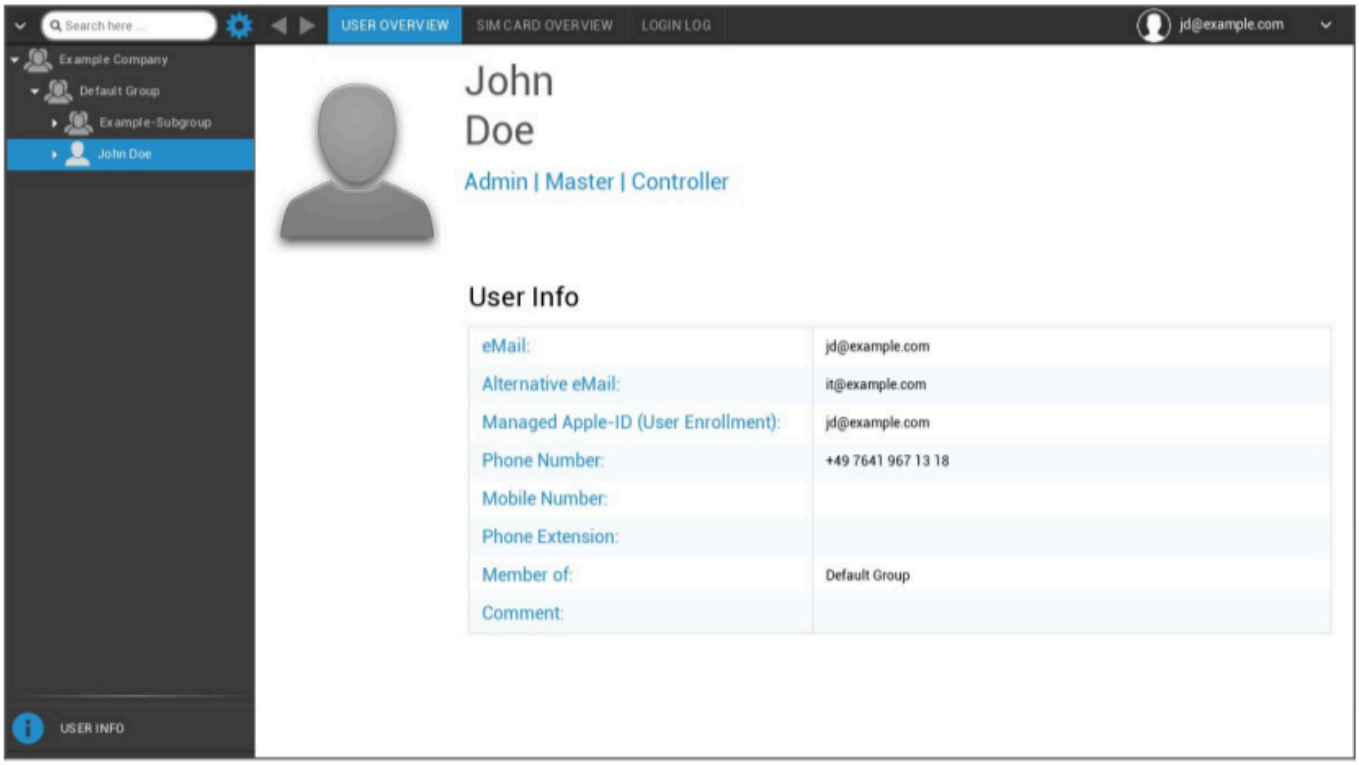
Activați comutatorul pentru "Can Login", atribuiți rolul "Super-Root" utilizatorului și setați o parolă.



Salvați acest lucru și utilizatorul se poate conecta acum cu numele de utilizator și parola.

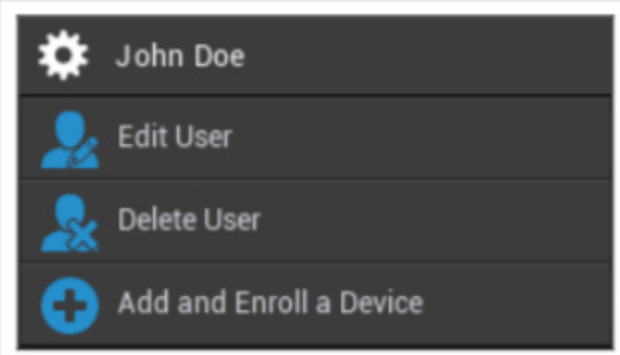
Gestionarea utilizatorilor în cadrul Mobile Management

Atunci când selectați un anumit utilizator, veți vedea următoarea prezentare generală:



Veți primi o prezentare generală a tuturor informațiilor pe care le-ați introdus anterior în "Crearea unui utilizator".

Cu uneltele instalate în partea superioară, puteți efectua următoarele configurații:



Nume utilizator	Numele de utilizator al utilizatorului selectat
Editare utilizator	Editarea informațiilor despre utilizator
Ștergeți utilizatorul	Ștergeți utilizatorul

	• Șterge din sistem = Dispozitivul va fi eliminat din AppTec • Ștergere și eliminare = Dispozitivul va fi restaurat la setările din fabrică și va fi eliminat din AppTec
Adăugarea și înscrierea unui dispozitiv	Înscrieți un dispozitiv pentru utilizatorul selectat

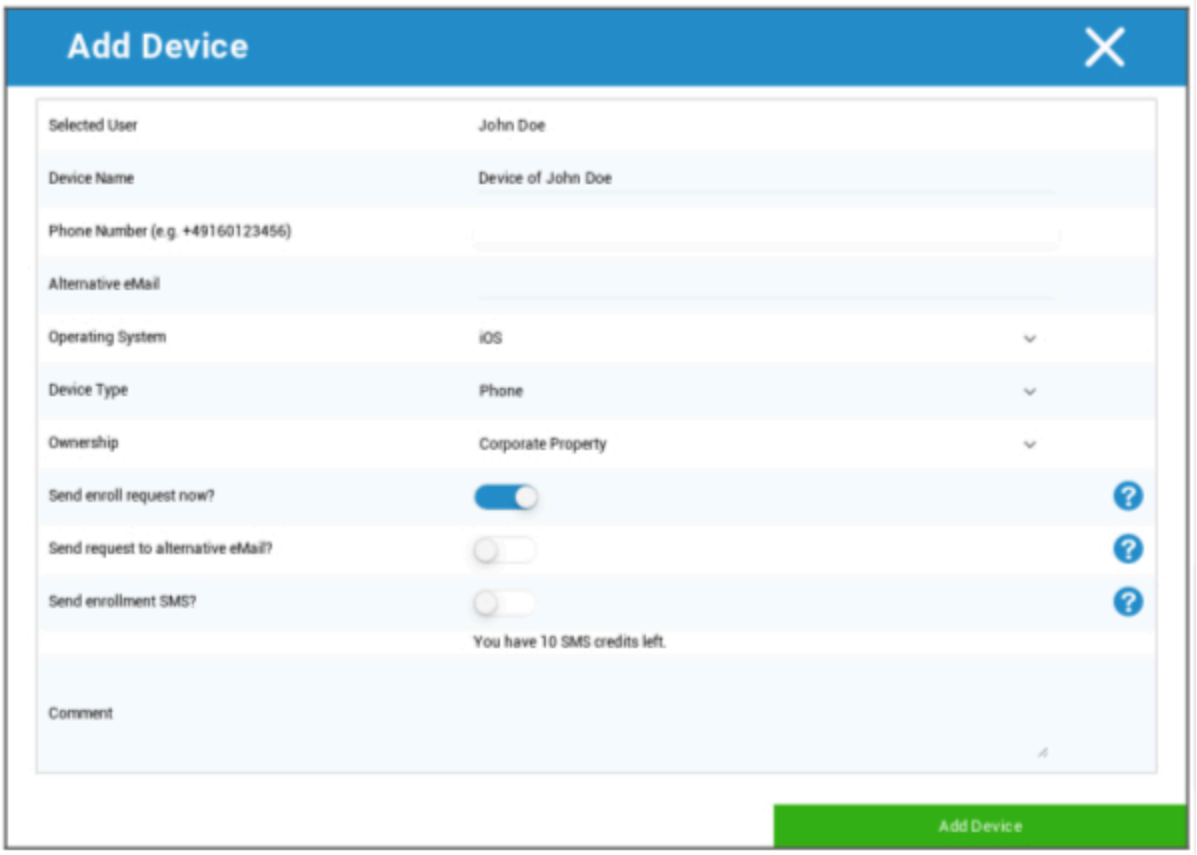
Vă rugăm să rețineți că accesul de administrare poate fi, de asemenea, depus ca un cont de utilizator local în structura ierarhică. Fără stabilirea unui administrator suplimentar, acesta nu ar trebui să fie șters!

Adăugarea și înscrierea unui dispozitiv

Aici puteți selecta un dispozitiv pentru utilizarea selectată.

Alternativ, puteți înscrie direct dispozitive într-un grup. Pentru a face acest lucru, faceți clic pe grup, faceți clic pe rotiță și selectați "Adăugați și înscrieți un dispozitiv".

Ar trebui să vedeți următoarea prezentare generală:



În funcție de tipul de dispozitiv pe care doriți să îl înscrieți, trebuie să efectuați următoarele configurări:

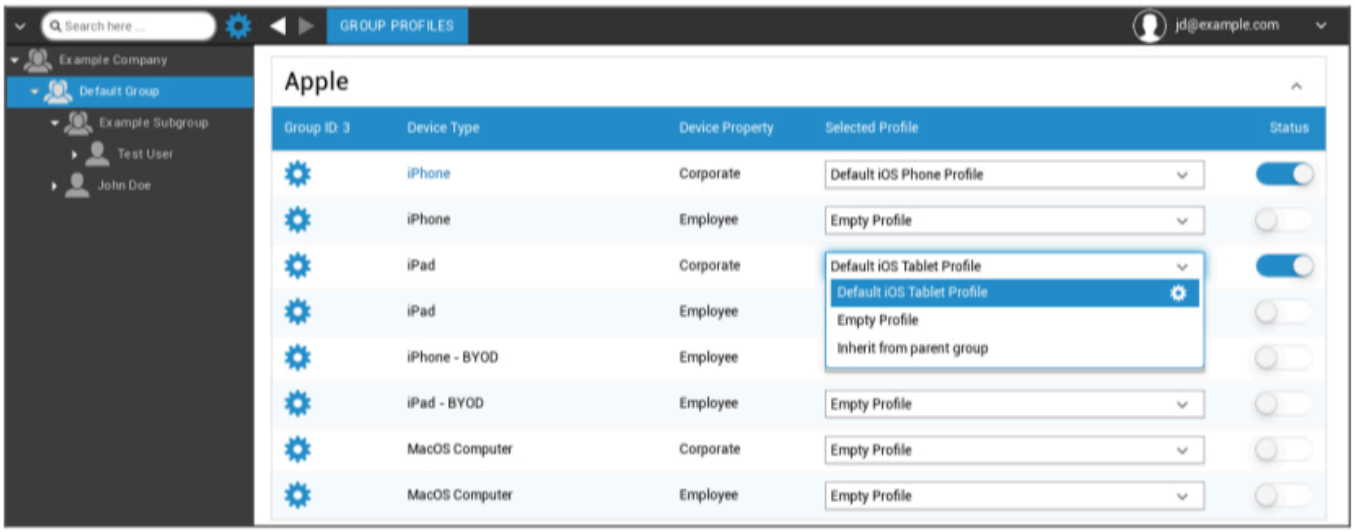
Utilizator selectat	Utilizatorul selectat (va fi completat automat)
Numele dispozitivului	Va fi completat automat (dispozitiv pentru "numele utilizatorului") - poate fi, totuși, modificat
Număr de telefon	Numărul de telefon, va fi completat automat (atâta timp cât a fost furnizat de utilizator) - aici, cu toate acestea, poate fi adăugat sau modificat
Email alternativ	E-mail alternativ, va fi completat automat (atâta timp cât a fost furnizat de utilizator) - aici, cu toate acestea, acesta poate fi adăugat sau modificat
Proprietarul dispozitivului	Proprietate corporativă = dispozitiv corporativ Proprietatea angajatului = dispozitiv BYOD
Alegeți sistemul de operare	Aici, puteți alege între următoarele sisteme de operare: • iOS • iOS BYOD (Înscrierea utilizatorului) • MacOS • Android Enterprise • Android • Windows Mobile • Windows 10
Trimiteți o cerere de înscriere?	E-mailul este trimis imediat la adresa principală de e-mail, iar utilizatorului i se solicită să își conecteze dispozitivul
Trimiteți cererea la un e-mail alternativ?	Trimiteți e-mailul suplimentar sau exclusiv (în cazul în care opțiunea "Trimitere cerere de înscriere?" a fost dezactivată) la adresa de e-mail alternativă (e-mailul este diferit de e-mailul "normal" al cererii de înscriere)
Trimiteți SMS de înscriere?	Trimiteți o cerere de înscriere prin SMS (trebuie introdus "Numărul de telefon")

După trimiterea cererii de înscriere, dispozitivul va fi afișat imediat (marcat cu roșu).

De îndată ce dispozitivul a fost conectat cu succes, dispozitivul va fi marcat cu verde la scurt timp după aceea și este astfel pregătit să primească restricții, aplicații etc.

Gestionarea profilului în Mobile Management

După ce faceți clic pe un grup, veți primi o prezentare generală a tuturor platformelor de dispozitive care urmează să fie configurate și a profilurilor alocate.



	Efectuați configurarea pentru profilul selectat
Tip dispozitiv	Tipul și/sau modelul dispozitivului
Proprietatea dispozitivului	Proprietarul dispozitivului (Corporate = proprietate corporativă, Employee = dispozitiv privat al angajatului)
Profil selectat	Profilul selectat (uneltele deschid dialogul de configurare a profilului)
Statut	On/Off (profilul este activat/dezactivat)

Când selectați uneltele, veți primi următoarele opțiuni:

Creați un profil

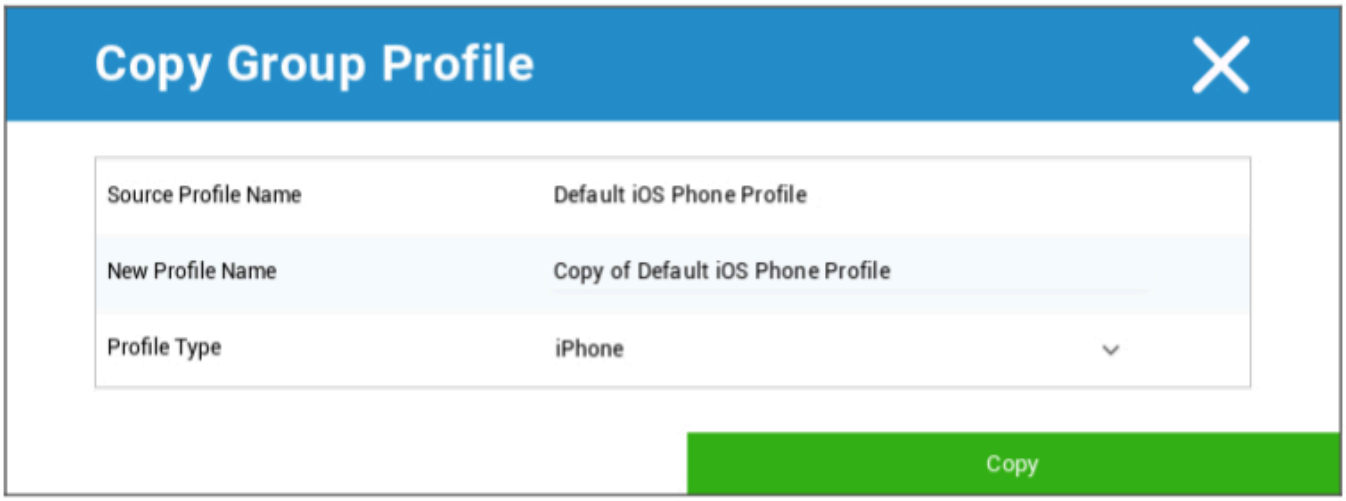
Puteți crea și configura un profil nou pentru fiecare intrare și/sau platformă. După ce faceți clic pe acest subpunct, profilul va fi creat imediat și puteți începe imediat cu configurarea iOS, Android și Windows Phone.

Editare profil

După ce faceți clic pe "Editare profil", veți ajunge la ecranul de configurare pentru profilul respectiv, unde puteți seta configurațiile.

Copiați profilul

Cu ajutorul funcției "Copiere profil", puteți copia setările/configurările dintr-un profil deja existent și le puteți adăuga la un profil nou.

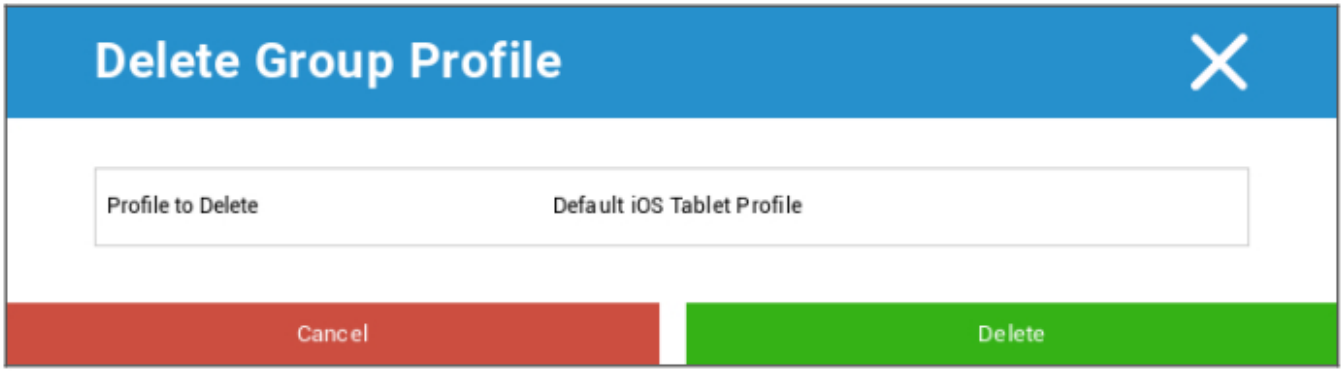


Sursă Nume profil	Numele profilului care urmează să fie copiat
Nume profil nou	Numele noului profil
Tip profil	Tipul de profil (telefon/tabletă)

După ce faceți clic pe "Copiere", profilul va fi creat și poate fi acum atribuit grupului

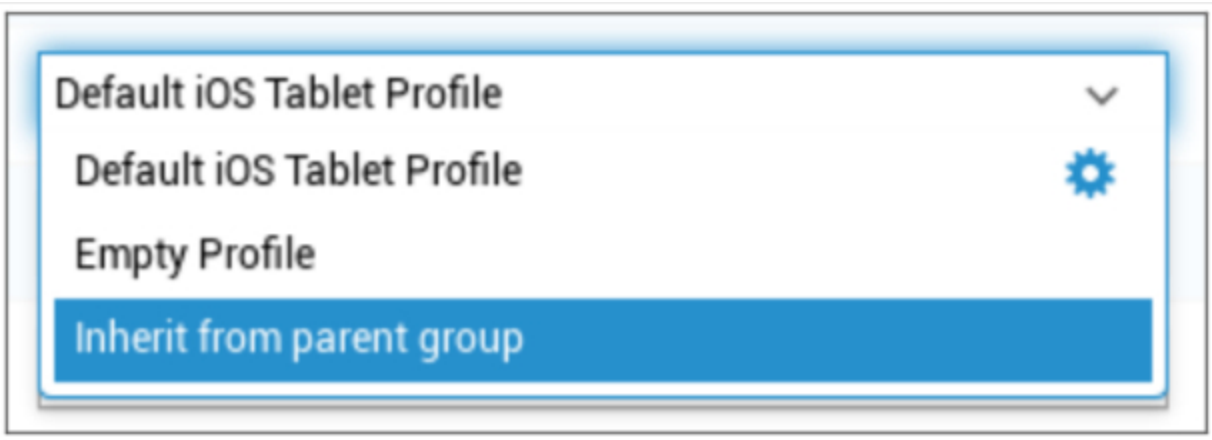
Ștergeți profilul

Aici puteți șterge definitiv un profil. Vă rugăm să rețineți că, în timpul procesului de ștergere și al următorului proces "Atribuiți acum" pentru profil, configurația va dispărea de pe dispozitivele respective ale unui grup afectat și nu va putea fi recuperată!


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

Moștenirea profilurilor

În timpul selectării profilurilor, este disponibilă opțiunea "Moștenire din grupul părinților".



Atunci când profilul este activat, profilul grupului părinte va fi utilizat pentru dispozitivul respectiv selectat (și tipul respectiv de dispozitiv). Vă rugăm să rețineți, de asemenea, că modificările aduse acestui profil ar putea afecta numeroase grupuri.

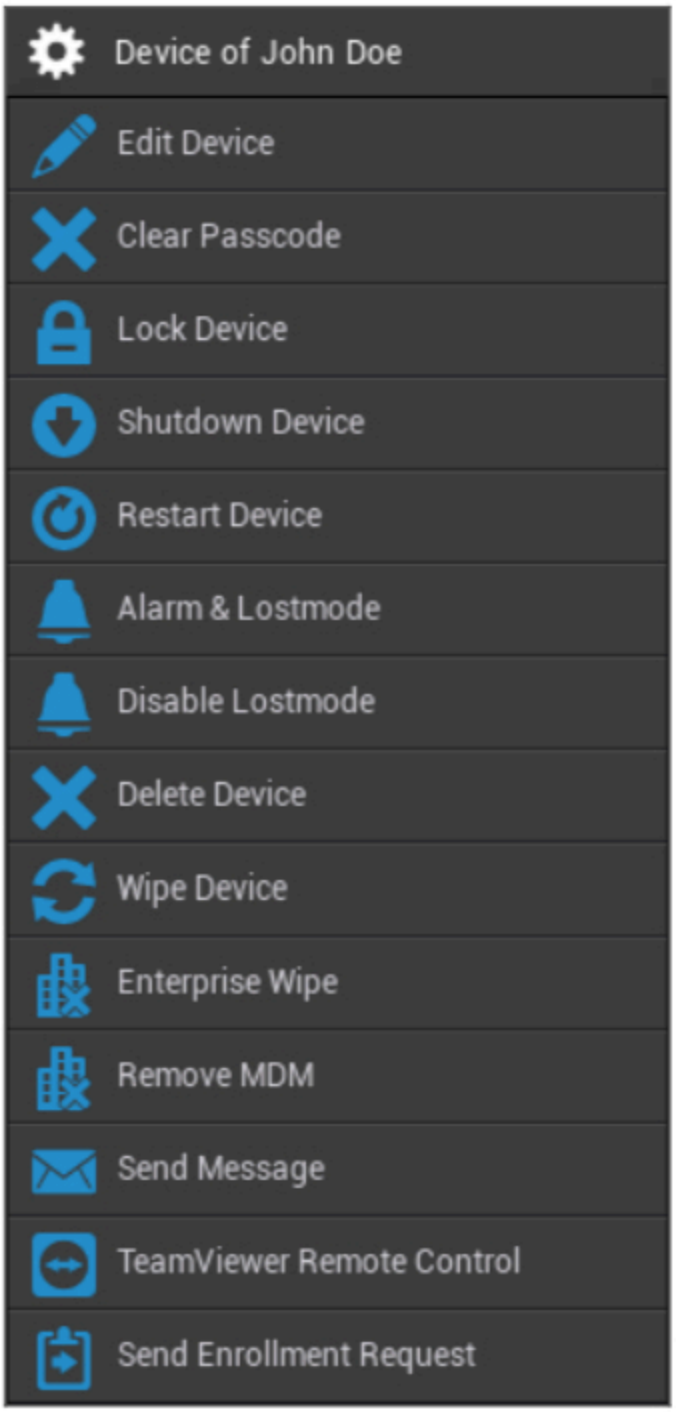
Această configurație este setată ca valoare implicită atunci când se creează un nou subgrup.

Configurația "Profil gol" este, de asemenea, disponibilă, ceea ce corespunde unui profil gol, ceea ce înseamnă că, în cele din urmă, pe dispozitivul utilizatorului final nu vor fi efectuate noi configurații.

Gestionarea dispozitivelor în gestionarea dispozitivelor mobile

Atunci când selectați un dispozitiv, puteți efectua o serie de sarcini prin intermediul "uneltelor". Acestea sunt diferite, în funcție de platformele sistemului de operare (iOS, Android Enterprise, Android, Windows Mobile, Windows 10).

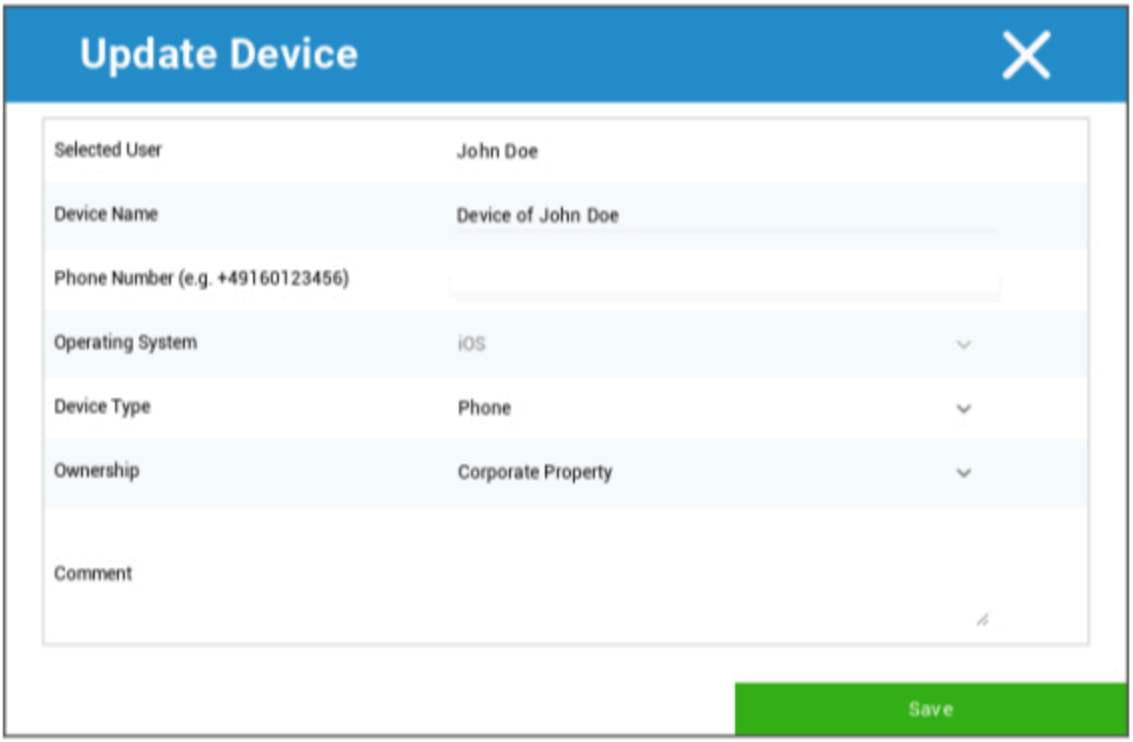
IOS



Editare dispozitiv	Editare dispozitiv
Ștergeți codul de acces	Codul de acces al dispozitivului este șters
Dispozitiv de blocare	Blocare dispozitiv (ecran de blocare)
Dispozitiv de oprire	Dispozitiv de oprire

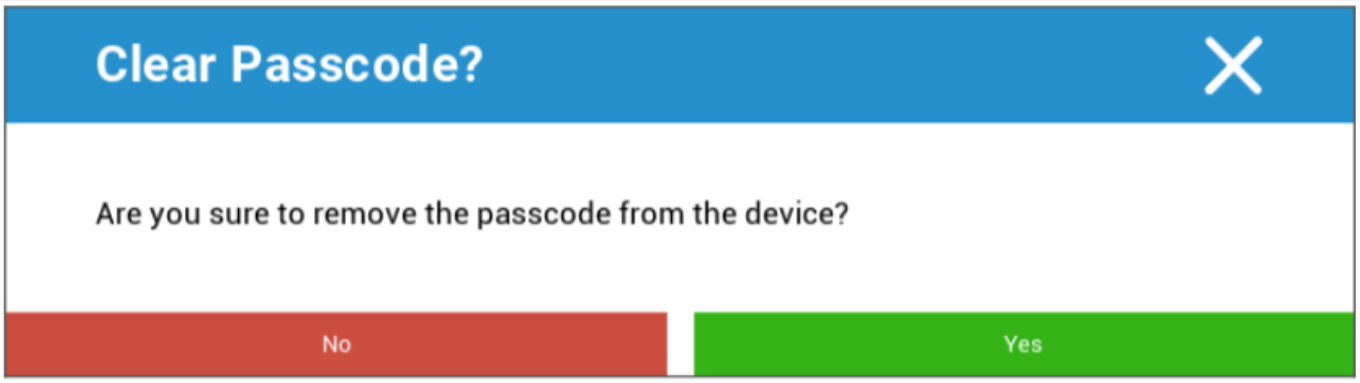
Reporniți dispozitivul	Reporniți dispozitivul
Alarmă și mod pierdut	Alarmă de pornire & Lostmode
Dezactivați Lostmode	Dezactivați Lostmode
Ștergeți dispozitivul	Îndepărtați dispozitivul din AppTec
Ștergeți dispozitivul	Restaurarea dispozitivului la setările din fabrică
Ștergere Enterprise	Informațiile, aplicațiile și profilurile furnizate de AppTec360 sunt șterse (dispozitivul este separat de MDM)
Eliminați MDM	
Trimite mesaj	Trimiteți notificări push către dispozitiv Mesajul va fi afișat în AppTec360 App (fila Mesaj)
TeamViewer Control de la distanță	Începeți sesiunea de control de la distanță utilizând TeamViewer
Trimiteți cererea de înscriere	Trimitere (repetată) Cerere de înscriere

Editare dispozitiv



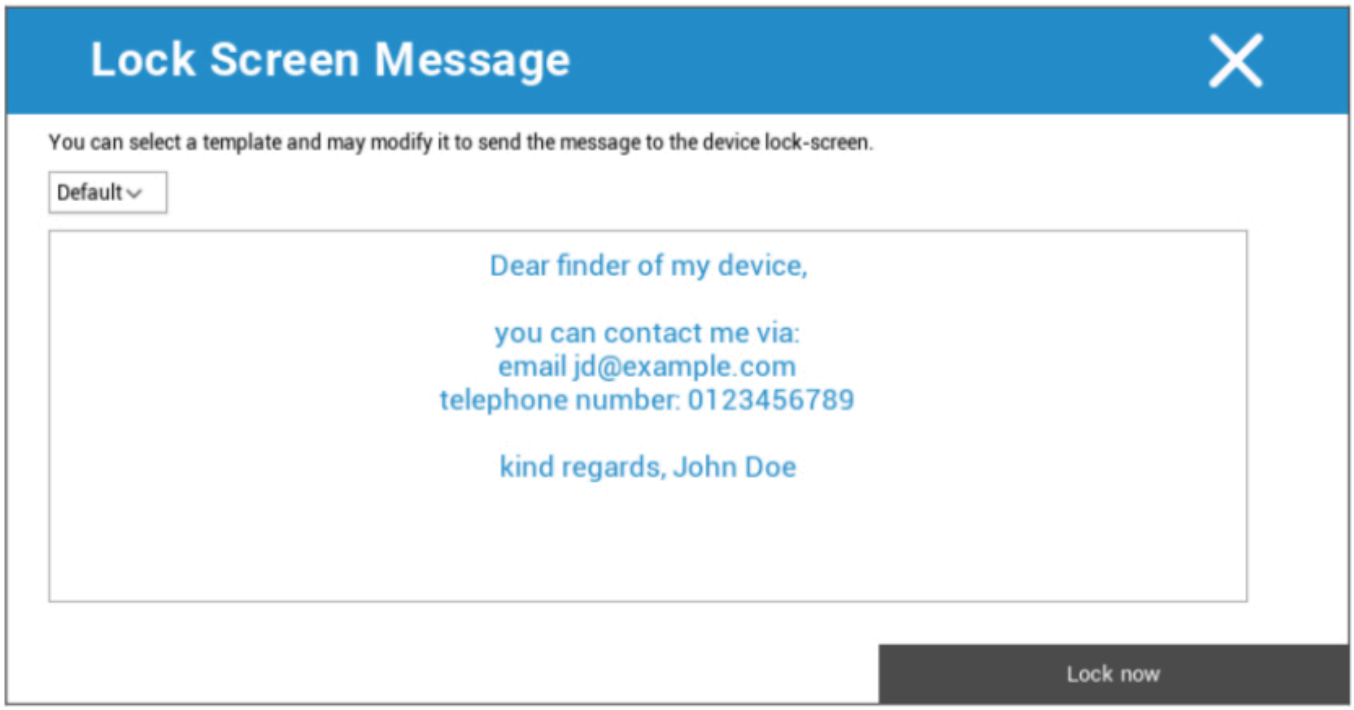
Aici puteți actualiza o varietate de informații despre dispozitiv.

Ștergeți codul de acces



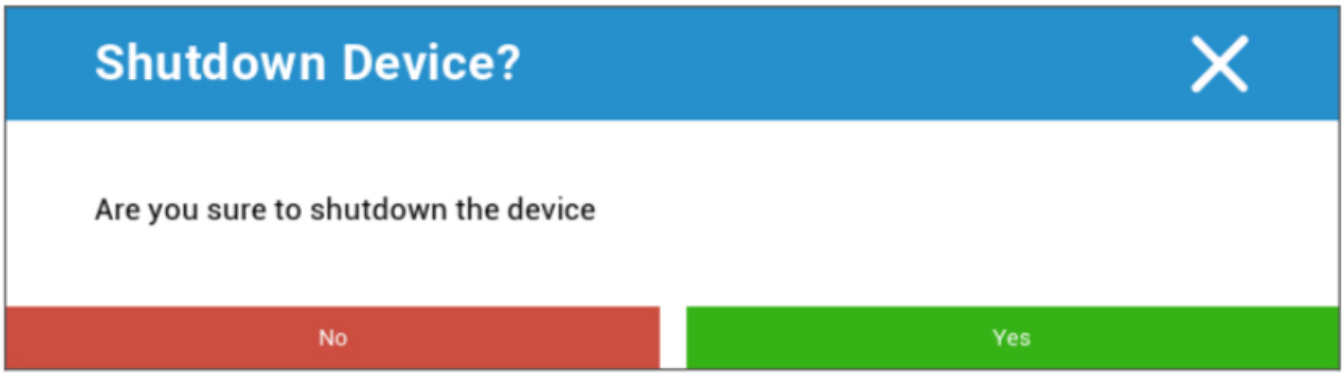
La "Clear Passcode" puteți elimina de la distanță codul de acces de pe dispozitiv. Ulterior, utilizatorului i se va solicita să emită o nouă parolă (în funcție de orientările privind codul de acces).

Dispozitiv de blocare



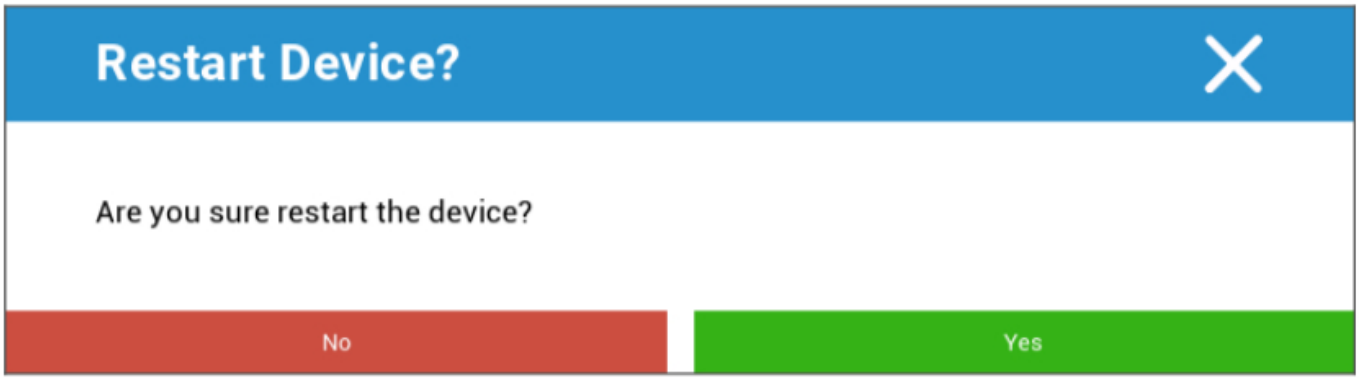
Aici este trimisă o comandă de blocare către dispozitivul utilizatorului final (ecran de blocare).

Dispozitiv de oprire



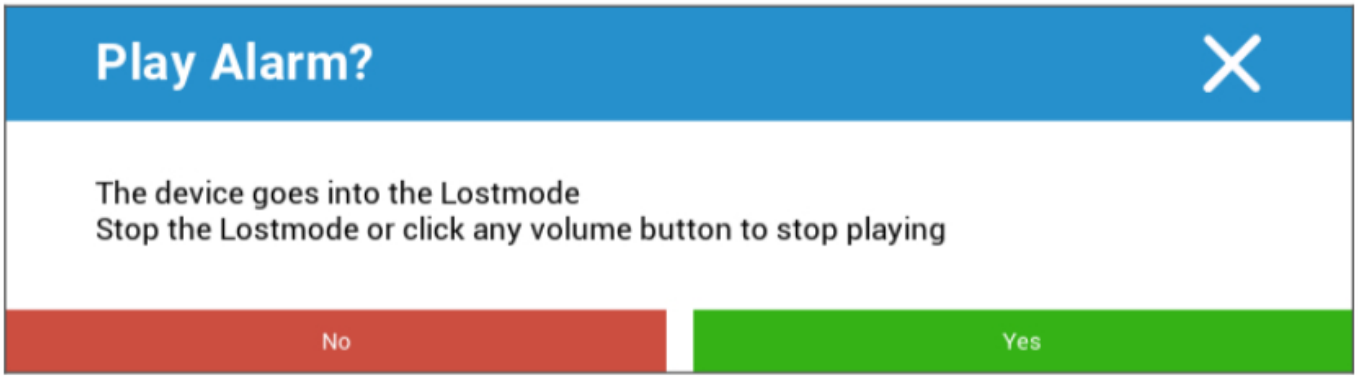
Aici este trimisă o comandă de închidere către dispozitivul utilizatorului final.

Reporniți dispozitivul

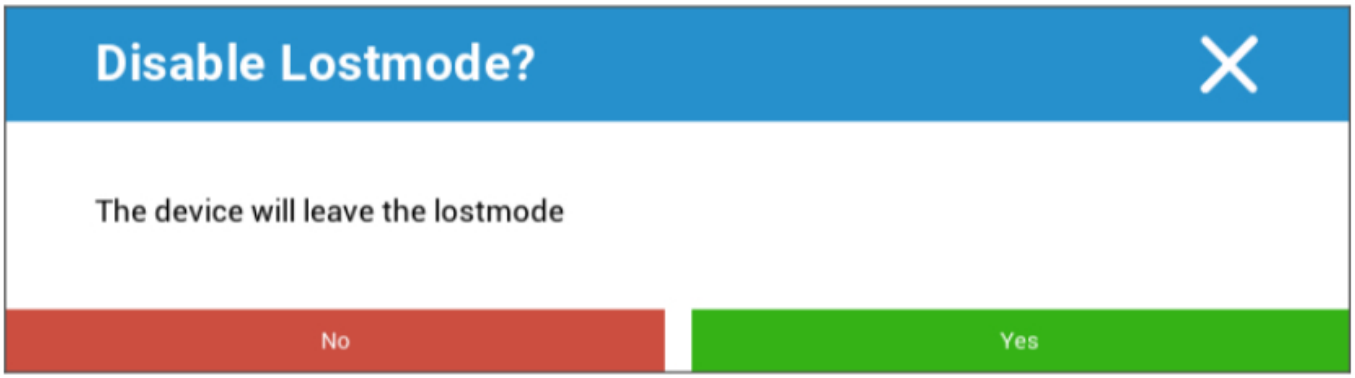


Aici este trimisă o comandă de repornire către dispozitivul utilizatorului final.

Alarmă și mod de pierdere | Dezactivare mod de pierdere



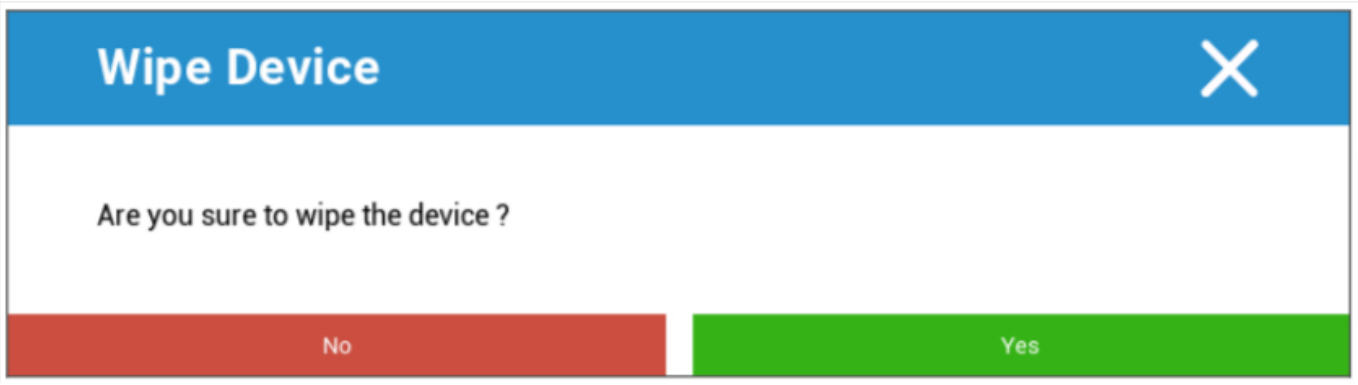
Aici dispozitivul poate fi setat în modul Lostmode, care setează dispozitivul pentru a reda constant un sunet de alarmă. Modul Lostmode poate fi oprit prin apăsarea oricărui buton de volum al dispozitivului sau de la distanță, făcând clic pe "Disable Lostmode":



Ștergeți dispozitivul

Aici poate fi executată comanda de ștergere. Puteți decide încă o dată dacă dispozitivul trebuie eliminat numai din AppTec360 ("Ștergere din sistem") sau dacă dispozitivul trebuie eliminat din AppTec360 și, de asemenea, readus la setările din fabrică ("Ștergere și eliminare).

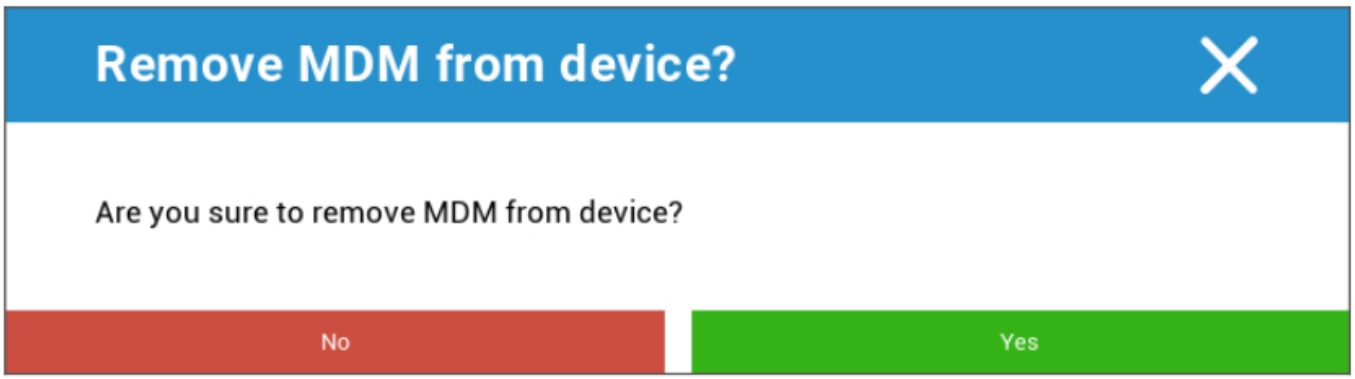
Ștergeți dispozitivul



Sub "Ștergere dispozitiv" puteți efectua o ștergere completă a dispozitivului. Dispozitivul va fi restaurat la setările din fabrică.

Ștergere Enterprise | Eliminare MDM

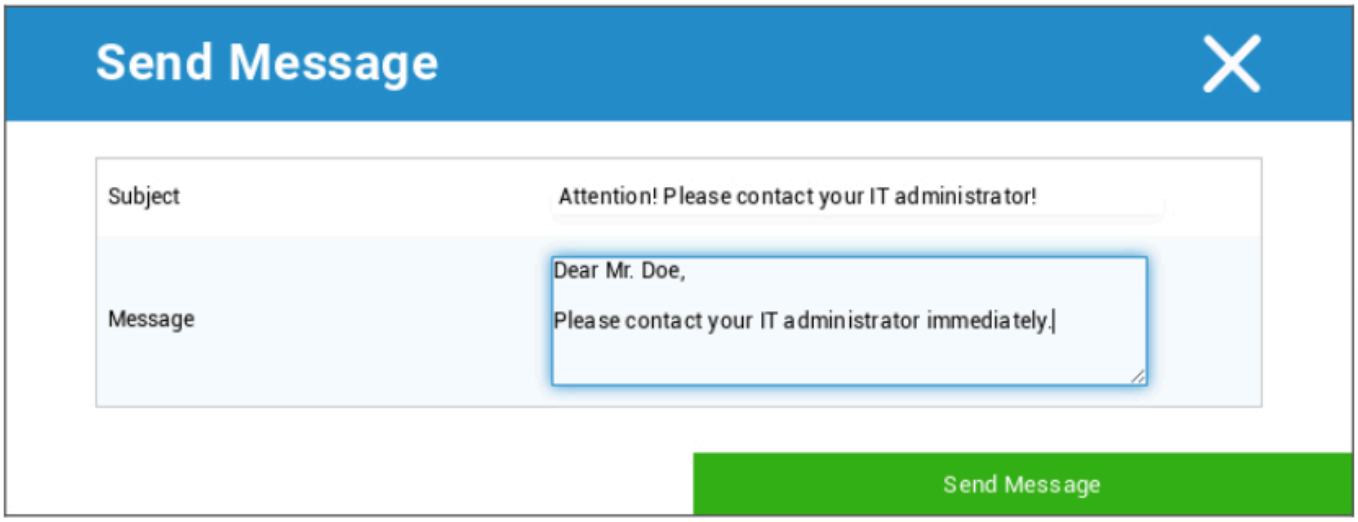
Doar informațiile, aplicațiile și profilurile furnizate de AppTec360 sunt șterse. În acest fel, datele corporative nu vor mai fi disponibile pe dispozitivul utilizatorului final. Zona privată nu este afectată și continuă să rămână pe dispozitivul utilizatorului final.



Cu "Eliminare MDM" puteți elimina profilul MDM de pe dispozitivul utilizatorului final și toate celelalte elemente furnizate de AppTec.

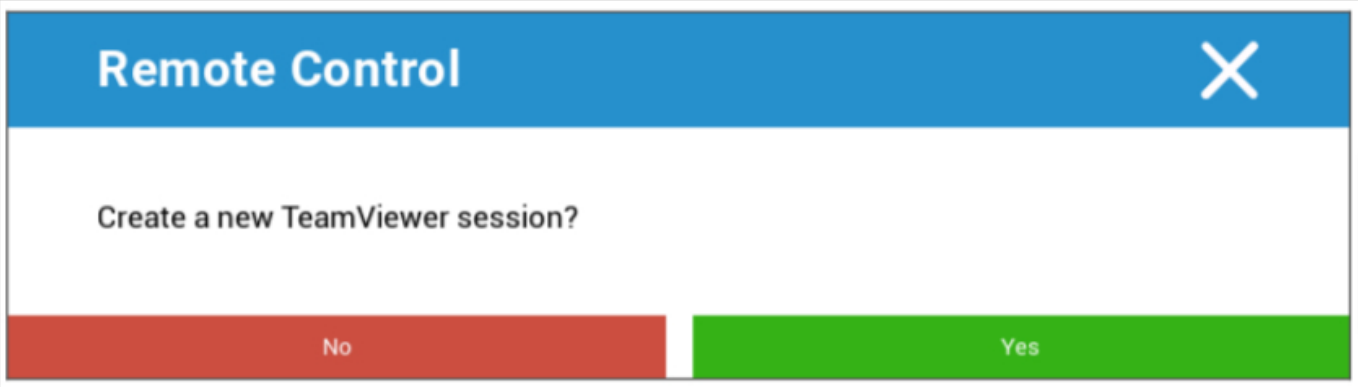
Această comandă efectuează aceeași acțiune ca și "Enterprise Wipe".

Trimite mesaj



Aici puteți trimite o notificare push către dispozitivul respectiv.

TeamViewer Control de la distanță



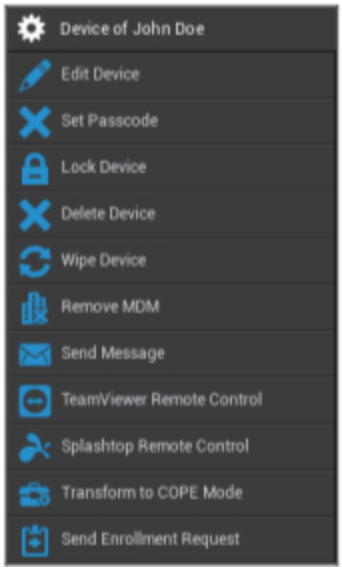
Aici poate fi inițiată o sesiune Teamviewer Remote Control.

Trimiteți cererea de înscriere

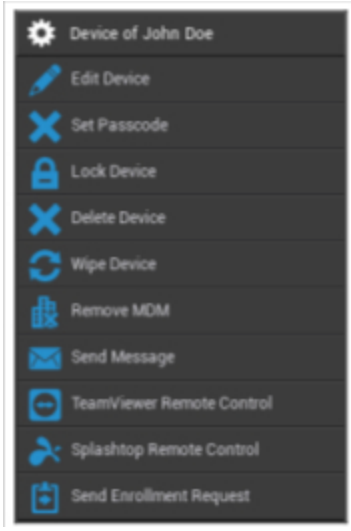
Cu "Trimite cerere de înscriere", puteți trimite o cerere de înscriere (din nou) către utilizatorul respectiv.

Android

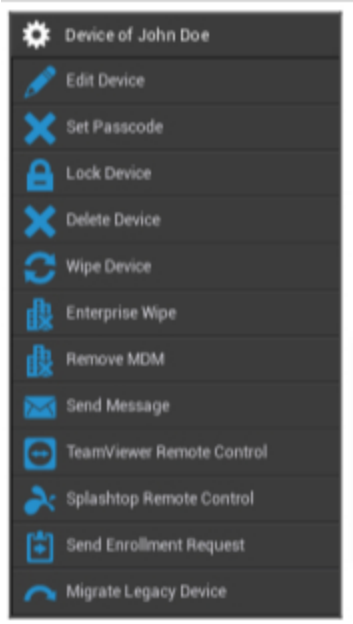
AE Dispozitiv complet administrat (administrat la locul de muncă)



Profil de lucru AE (Container)



Telefon Android | Tabletă

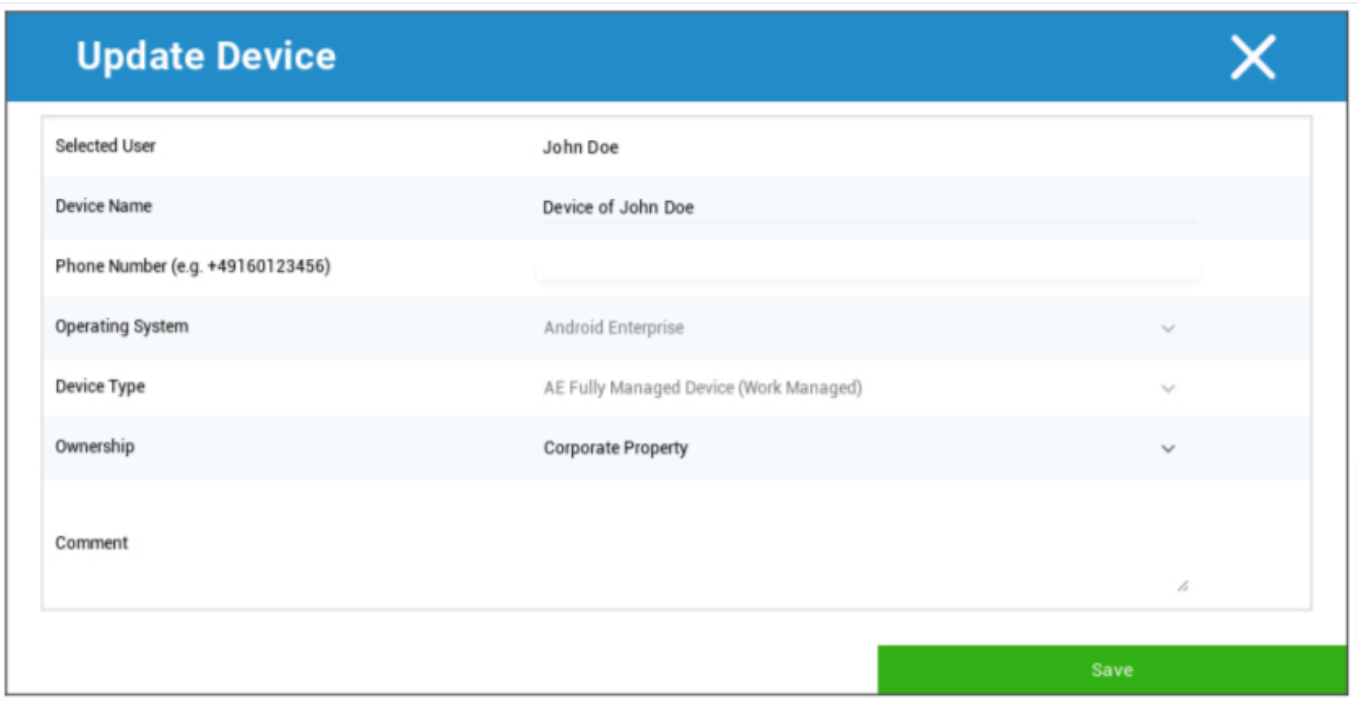


Editare dispozitiv	Editarea informațiilor despre dispozitiv
Setați codul de acces	Setați codul de acces al dispozitivului
Dispozitiv de blocare	Blocare dispozitiv (ecran de blocare)
Ștergeți dispozitivul	Ștergeți dispozitivul din AppTec
Ștergeți dispozitivul	Restaurarea dispozitivului la setările din fabrică
Ștergere Enterprise	Informațiile, aplicațiile, profilurile care sunt furnizate de AppTec360 sunt șterse (dispozitivul va fi separat de MDM)
Eliminați MDM	
Trimite mesaj	Trimiteți notificări Push către dispozitiv Mesajul va fi afișat în AppTec360 App (fila Mesaj)
TeamViewer Control de la distanță	Începeți o sesiune de control de la distanță pentru acest dispozitiv utilizând TeamViewer
Splashtop Telecomandă	Începeți o sesiune de control de la distanță pentru acest dispozitiv utilizând Splashtop
Transformarea în modul COPE (numai pe dispozitivul AE complet administrat (Work Managed))	Creați un profil de lucru pe acest dispozitiv AE administrat integral (administrat la locul de muncă)
Trimiteți cererea de înscriere	Trimitere (repetată) a cererii de înscriere

Migrare dispozitiv vechi (numai pe telefonul/tableta Android atunci când este înscrisă utilizând Provisionarea în modul proprietar al dispozitivului)	Migrează profilul telefonului / tabletei Android către profilul AE Fully Managed Device (Work Managed)

Editare dispozitiv

Aici puteți actualiza o varietate de informații despre dispozitiv.



Utilizator selectat	Utilizatorul dispozitivului
Numele dispozitivului	Numele dispozitivului
Număr de telefon	Numărul de telefon al dispozitivului
Sistem de operare	Android Enterprise Android
Tip dispozitiv	Android Enterprise: • AE Dispozitiv complet administrat (administrat la locul de muncă) • Modul profil de lucru AE (numai container) • AE Dispozitiv complet administrat cu profil de lucru (COPE) Android: • Telefon • Tabletă
Proprietate	Corporate = proprietate corporativă

	Angajat = proprietatea angajat
Comentariu	Descrieri suplimentare pentru dispozitiv

Ștergeți codul de acces

Aici puteți elimina codul de acces al dispozitivului de pe dispozitivul selectat. În mod implicit pe Android, codul de acces va fi setat la "123456" - acesta poate și trebuie să fie schimbat ulterior de către utilizator.

Dispozitiv de blocare

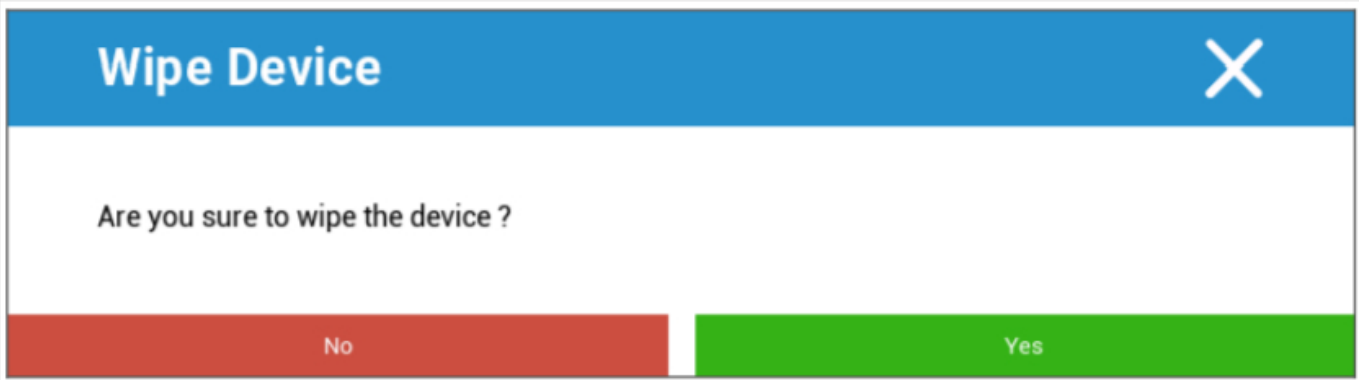
Aici va fi trimisă o comandă de blocare a dispozitivului către dispozitiv (ecran de blocare).

Ștergeți dispozitivul

Aici poate fi efectuată o comandă de ștergere. Puteți decide încă o dată dacă dispozitivul trebuie eliminat numai din AppTec360 ("Ștergere din sistem") sau dacă dispozitivul trebuie eliminat din AppTec360 și, în plus, readus la setările din fabrică ("Ștergere și eliminare).

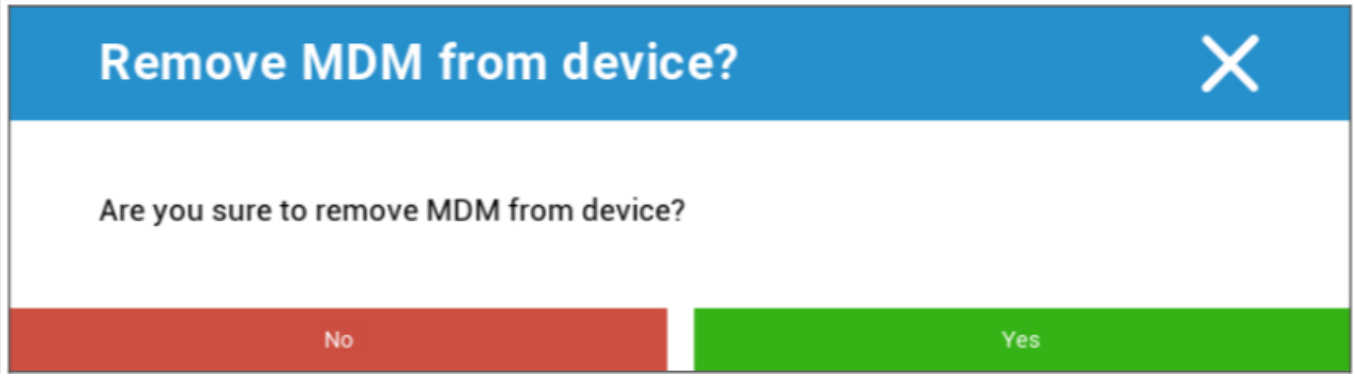
Ștergeți dispozitivul

Sub "Ștergere dispozitiv" puteți efectua o ștergere completă a dispozitivului. Dispozitivul va fi apoi readus la setările din fabrică.



În plus, dacă dispozitivul conține un card SD, puteți șterge cardul SD. Puteți realiza acest lucru, prin setarea "Ștergeți și cardul SD? " la "Activat".

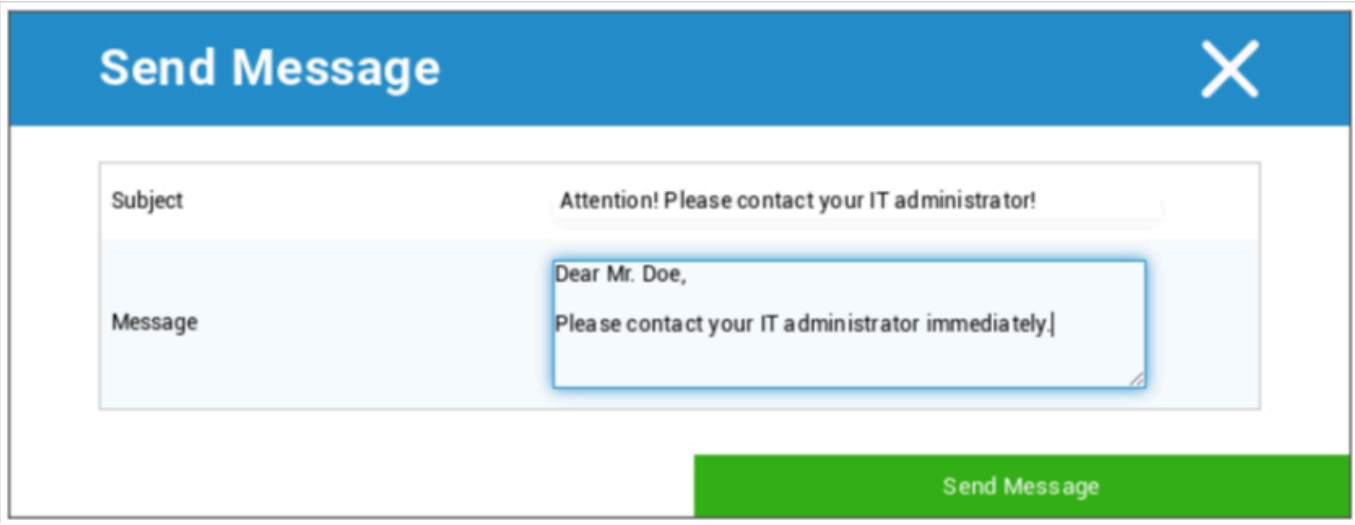
Eliminați MDM



Aceasta este metoda recomandată pentru crearea unei separări de MDM.

Doar informațiile, aplicațiile și profilurile furnizate de AppTec360 sunt șterse, ceea ce înseamnă că toate datele corporative nu vor mai fi disponibile pe dispozitivul utilizatorului final. Cu toate acestea, sfera privată nu este afectată și continuă să rămână pe dispozitivul utilizatorului final.

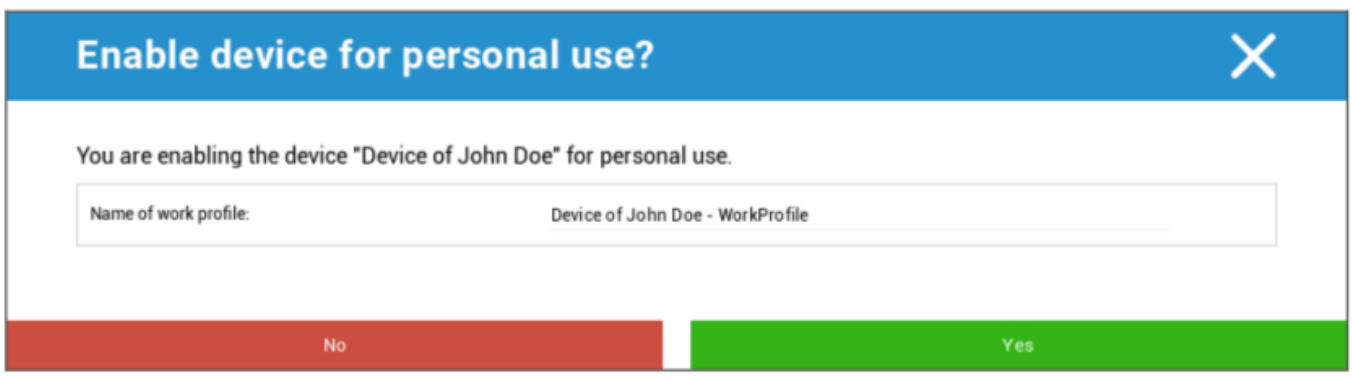
Trimite mesaj



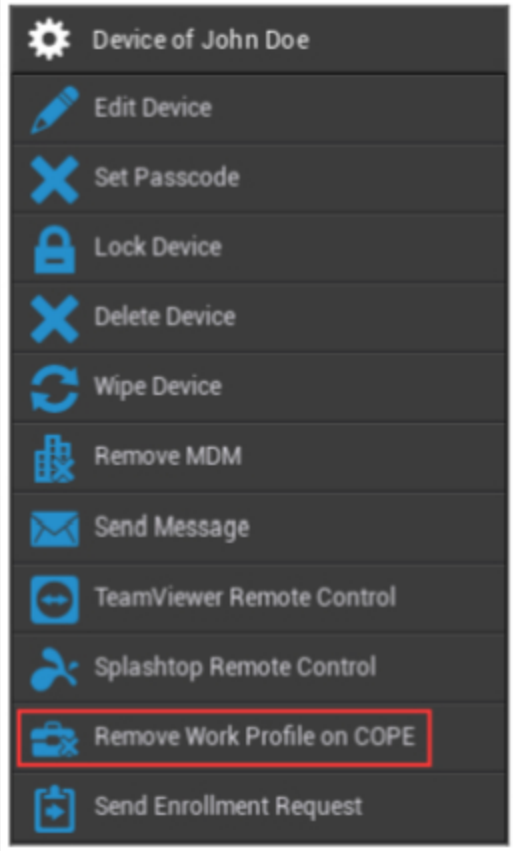
Aici puteți trimite o notificare push către dispozitivul respectiv al utilizatorului final.

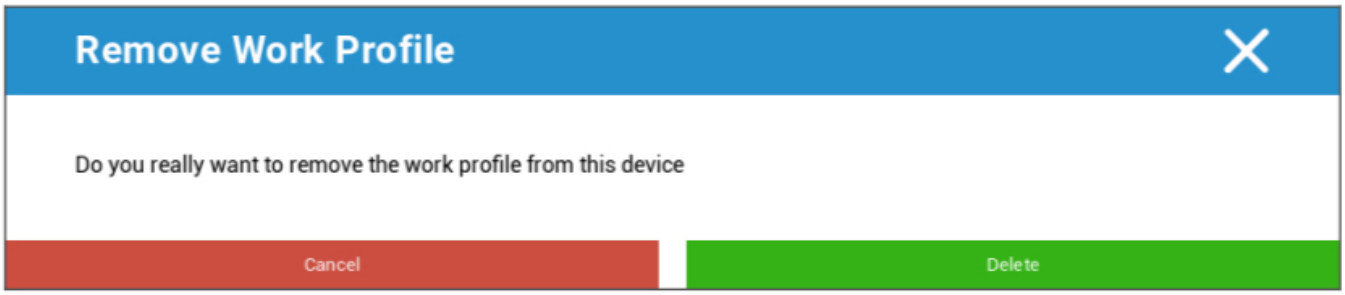
Transformarea în modul COPE

Creați un profil de lucru pe acest dispozitiv AE administrat integral (administrat la locul de muncă)



După transformarea dispozitivului în modul COPE, puteți elimina profilul de lucru făcând clic pe opțiunea din angrenaj **Eliminare profil de lucru pe COPE:**




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

Trimiteți cererea de înscriere

Cu "Trimite cerere de înscriere" puteți trimite o cerere de înscriere (din nou) utilizatorului respectiv.

Vă rugăm să rețineți că numai cea mai recentă cerere de înscriere este valabilă.

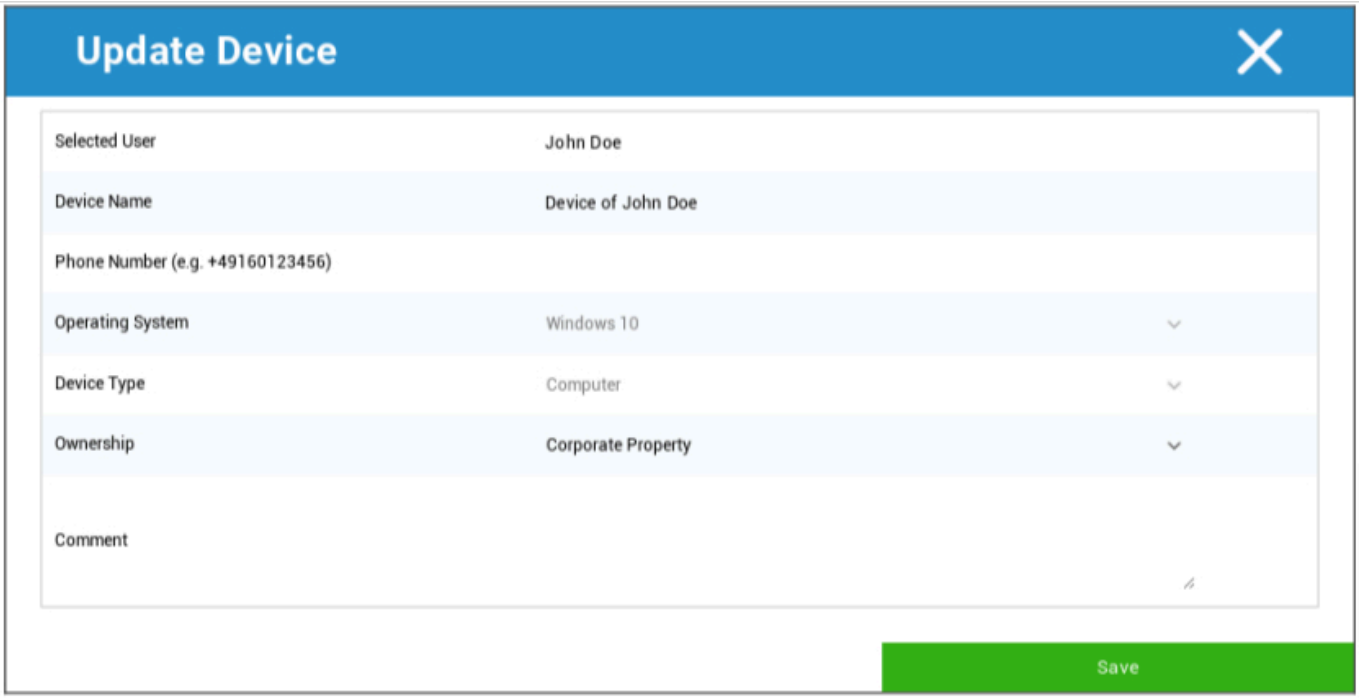
Migrare dispozitiv tradițional

Migrează profilul telefonului / tabletei Android către profilul AE Fully Managed Device (Work Managed)

Ferestre

Numele dispozitivului	Numele dispozitivului selectat
Editare dispozitiv	Editare dispozitiv
Ștergeți dispozitivul	Îndepărtați dispozitivul din AppTec
Ștergere Enterprise	Informațiile, aplicațiile și profilul furnizate de AppTec360 sunt șterse
Eliminați MDM	
TeamViewer Control de la distanță	Controlați dispozitivul de la distanță cu TeamViewer
Trimiteți cererea de înscriere	Trimiteți cererea de înscriere (din nou)

Editare dispozitiv

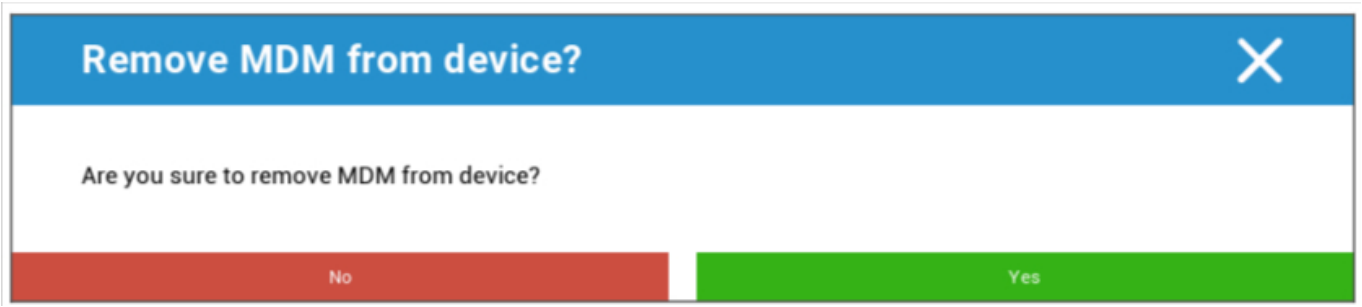


Aici puteți actualiza o varietate de informații despre dispozitiv.

Ștergeți dispozitivul

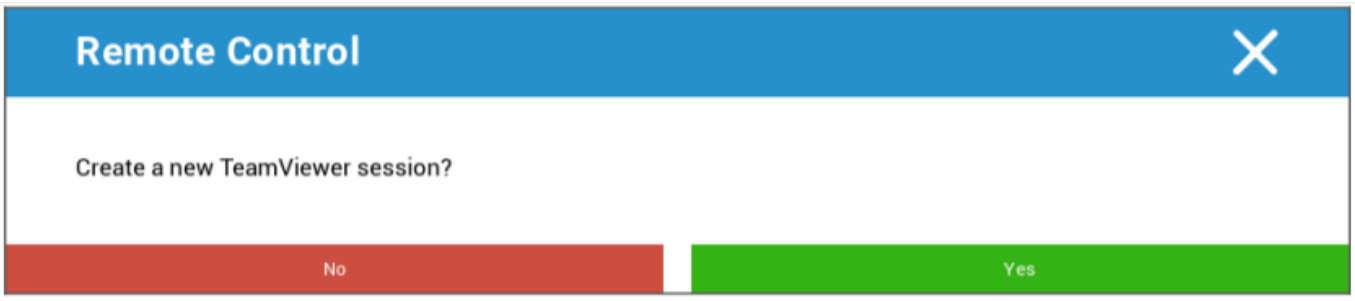
Aici poate fi executată comanda delete, care elimină dispozitivul din AppTec360.

Ștergere Enterprise | Eliminare MDM



Doar informațiile, aplicațiile și profilurile furnizate de AppTec360 sunt șterse. În acest fel, datele corporative nu vor mai fi disponibile pe dispozitivul utilizatorului final. Zona privată nu este afectată și continuă să rămână pe dispozitivul utilizatorului final.

TeamViewer Control de la distanță



Aici puteți începe o sesiune TeamViewer Remote Control pentru acest dispozitiv.

Trimiteți cererea de înscriere

Cu "Trimite cerere de înscriere", puteți trimite o cerere de înscriere (din nou) către utilizatorul respectiv.

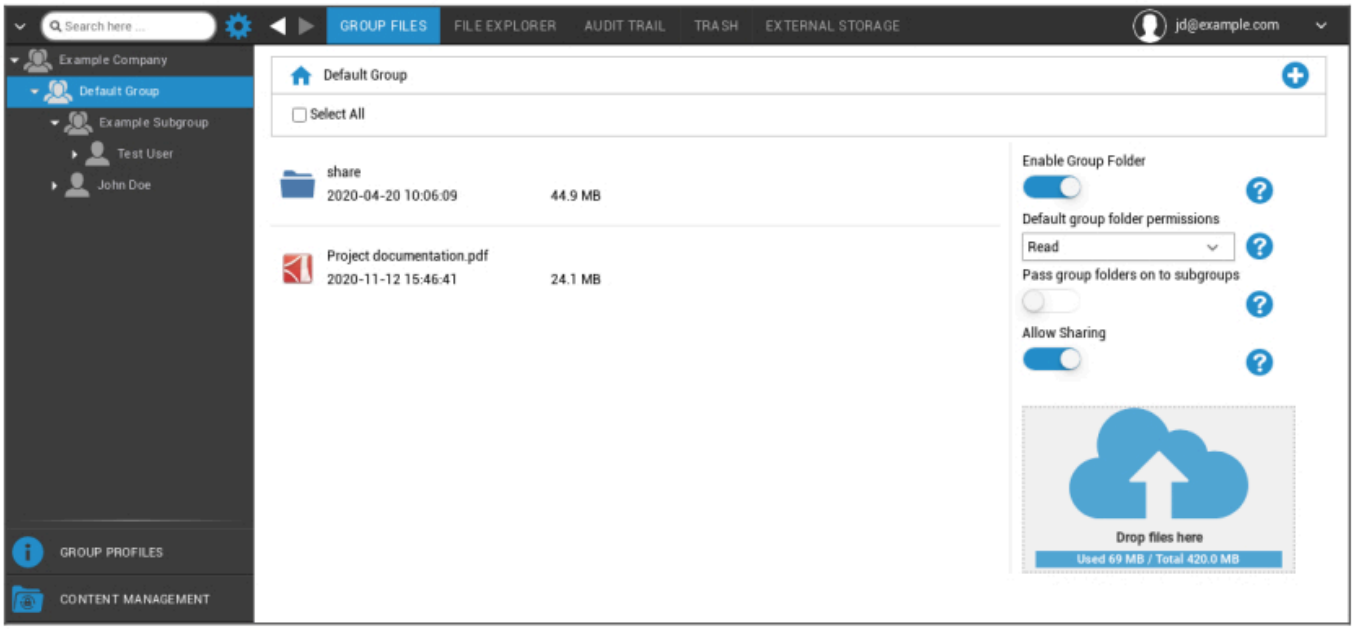
Gestionarea conținutului

Atunci când sunteți într-un grup, puteți gestiona AppTec's ContentBox cu "Managementul conținutului".

Cu Content Box puteți distribui în siguranță documente și alte date corporative către dispozitivele utilizatorilor finali.

Fișiere de grup

"Group Files" reprezintă o parte fundamentală ContentBox. Aici se stabilesc setările, se încarcă documente, se creează foldere noi etc.



Cu ajutorul simbolului din colțul din dreapta sus puteți crea noi dosare care sunt desemnate grupului respectiv cu "Adăugați dosar".

Cu ajutorul simbolului din colțul din dreapta sus, puteți crea un nou dosar prin "Adăugați dosar", care ar trebui să fie atribuit grupului respectiv.

Puteți denumi folderul cum doriți.

Prin "Încărcare fișiere", puteți încărca date. Aici va fi deschis Standard-Explorer. Desigur, puteți efectua aceste două acțiuni în fiecare (sub)dosar.

Cu simbolul din colțul din stânga sus, vă puteți întoarce la meniul principal.

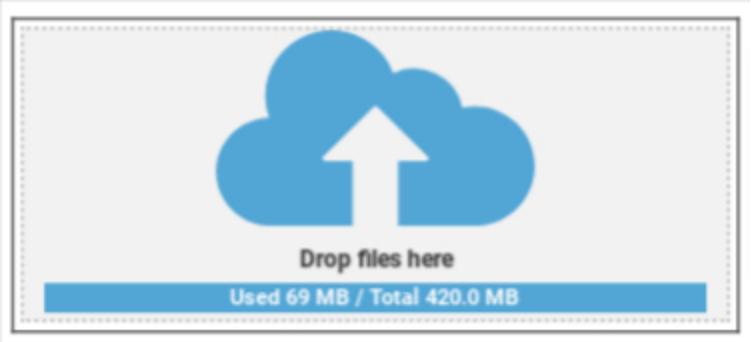
Puteți selecta mai multe foldere și fișiere și le puteți descărca cu "Descărcare" sau le puteți șterge făcând clic pe "Ștergere".

De asemenea, puteți selecta toate fișierele și folderele cu și executa comenzile "Descărcare" și "Ștergere".

Atunci când treceți cu mouse-ul peste un dosar sau fișier, veți vedea următoarea imagine de ansamblu:

- Cu "Redenumire", puteți redenumi folderul/fișierul
- Cu "Descărcare", puteți descărca folderul/fișierul
- Cu "Șterge", puteți șterge folderul/fișierul

Activarea dosarului de grup	Dacă este activat, toți membrii grupului au acces la folderul respectiv
Permisiuni implicite pentru dosarele de grup	Permisiunile utilizatorilor din grupul selectat: Read = permisiune numai de citire Actualizare = permisiune de actualizare Create = permisiune de creare Ștergere = permisiune de ștergere
Transmiterea folderelor de grup către subgrupuri	Dacă este activat, subgrupurile respective pot avea acces la fișierele de date părinte
Permisiuni pentru subgrupuri	Permisiunile utilizatorilor din subgrupul selectat: Citire = permisiune de numai citire Actualizare = permisiune de actualizare Create = permisiune de creare Ștergere = permisiune de ștergere
Permiteți partajarea	Dacă este activat, utilizatorul poate partaja fișiere prin intermediul unui link



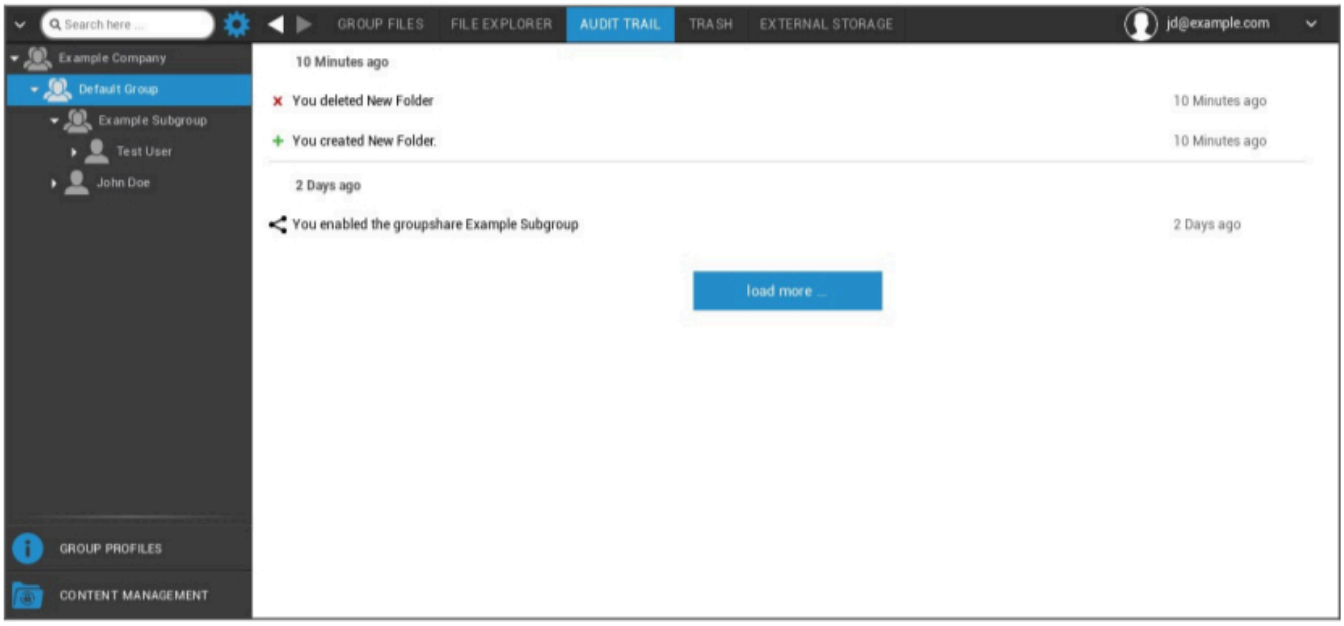
Pentru a încărca fișiere, puteți utiliza acest câmp, trăgând un fișier prin Drag & Drop în această fereastră. De asemenea, puteți face clic pe acest câmp, pentru a selecta și încărca un fișier cu ajutorul Internet Explorer.

Explorator de fișiere

Cu "File Explorer", puteți gestiona toate folderele și fișierele - indiferent de grupul în care sunt depuse.

De asemenea, veți găsi setările și butoanele despre care ați învățat în "Fișiere de grup".

Pista de audit



În "Audit Trail", puteți vedea din istoric ce utilizator a creat, șters sau partajat ce. În acest fel, puteți stabili în orice moment ce s-a făcut cu datele companiei.

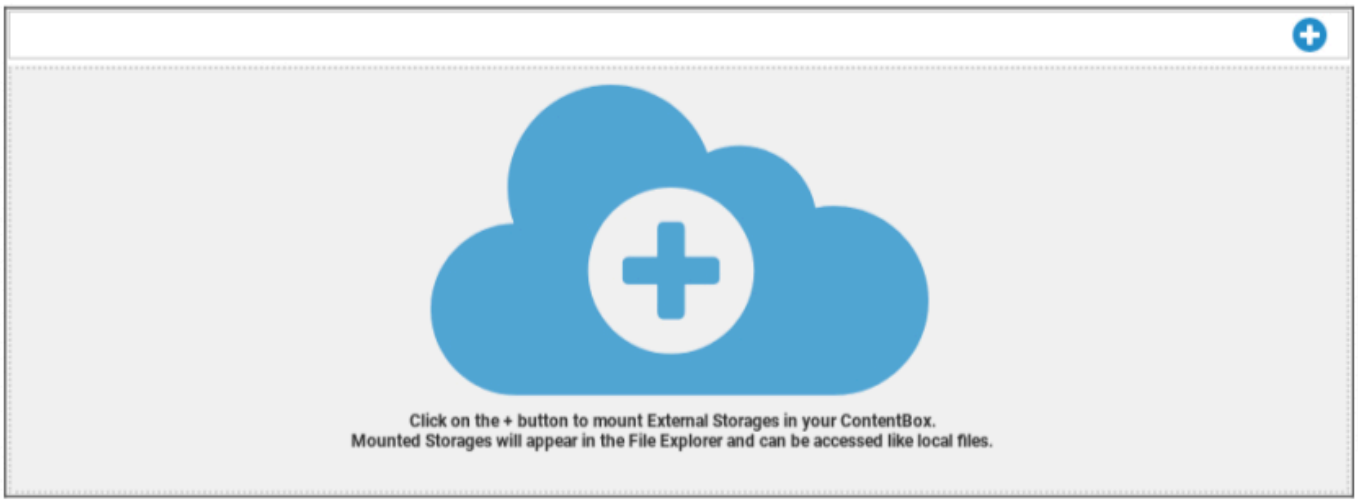
Gunoi

Dacă ați șters ceva (din greșeală), puteți vedea folderele și fișierele din "Coșul de gunoi" și le puteți recupera, în funcție de dorințele dvs.

- Cu "Undelete", puteți recupera datele/folderul.
- Cu "Șterge", puteți șterge definitiv datele/folderul - trebuie să confirmați comanda șterge încă o dată.

Vă rugăm să rețineți că capacitatea de stocare care este utilizată în coșul de gunoi reduce "Spațiul total" disponibil - aceasta este o cerință ownCloud.

Stocare externă



Sub titlul "Stocare externă", puteți conecta o unitate de stocare externă.

Cu ajutorul simbolului, se poate adăuga spațiu de stocare (suplimentar).

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

Amazon S3	
Nume afișat	Nume afișat
Cheie de acces	Cheie de acces
Cheie secretă	Cheie de securitate
Găleată	Identitatea definitivă a subfolderului care v-a fost atribuit
Nume gazdă (opțional)	Nume gazdă (opțional)
Port (opțional)	Port (opțional)
Regiunea	Regiune (opțional)
Activați SSL	Activați SSL
Activarea stilului de cale	Clear Path Adresa care v-a fost atribuită

FTP	
Nume afișat	Nume afișat
Gazdă	Adresă gazdă
Nume utilizator	Nume utilizator
Parolă	Parolă
Rădăcină	Meniu principal
Secure ftps://	

SFTP	
Nume afișat	Nume afișat
Gazdă	Adresă gazdă
Nume utilizator	Numele utilizatorului
Parolă	Parolă
Rădăcină	Meniu principal

propriulCloud	
Nume afișat	Nume afișat
URL	URL ownCloud
Nume utilizator	Nume utilizator
Parolă	Parolă
Subfolder la distanță	Dosar standard
Secure https://	

WebDAV	
Nume afișat	Nume afișat
URL	URL WebDAV
Nume utilizator	Numele utilizatorului
Parolă	Parolă
Rădăcină	Meniu principal
Secure https://	
Partajare Windows	Suportul pentru Windows Share va fi disponibil în curând
SharePoint	Suportul pentru Microsoft SharePoint va fi disponibil în curând

Jurnal de audit

Aici puteți găsi un jurnal care înregistrează informații despre acțiunile care sunt efectuate în consola MDM.

Cu pictograma filtru puteți aplica filtre listei afișate.

Cu ajutorul meniului derulant **Elemente pe pagină**: puteți selecta numărul de elemente care urmează să fie afișate pe o pagină a listei.

Măsuri luate / Setare schimbată	Măsura care a fost luată / Setarea care a fost modificată
Valoare	Valoarea acțiunii întreprinse/setarea modificată
Utilizator	Numele utilizatorului care a întreprins acțiunea / a modificat setarea
Data	Marca temporală a momentului în care această acțiune a fost întreprinsă / această setare a fost modificată
Cale / Tip	Calea către locul unde a fost efectuată această acțiune / a fost modificată această setare

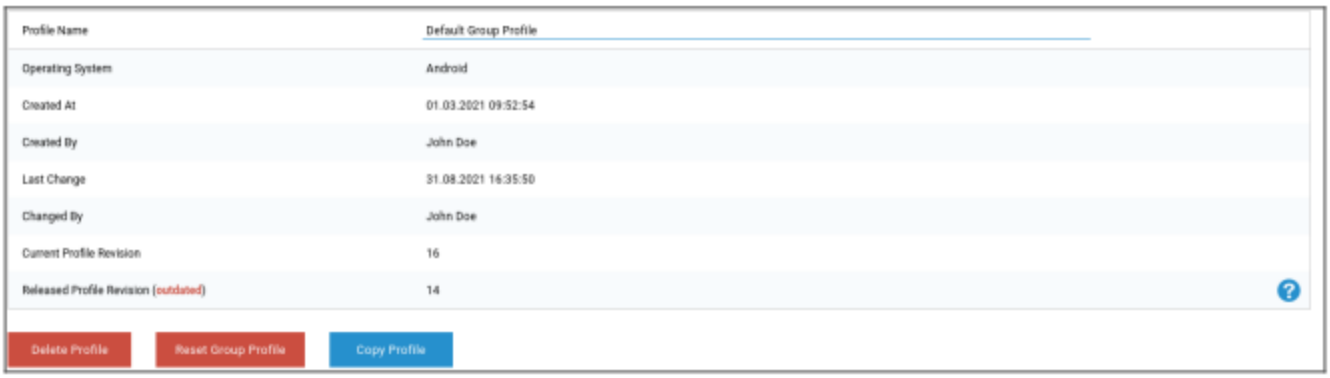
Configurarea iOS

Generalități

În funcție de faptul dacă ați selectat în prezent un grup sau un dispozitiv, afișajul și subpunctele sale sunt diferite - vă rugăm să acordați o atenție deosebită acestui aspect!

Prezentare generală a profilului grupului (numai la nivel de grup)

Atunci când deschideți un profil de grup, veți obține o prezentare generală rapidă a profilului



Nume profil	Numele profilului (poate fi modificat aici)
Sistem de operare	Sistemul de operare pentru care este creat profilul
Creat la	Momentul creației
Creat de	Creatorul profilului
Ultima schimbare	Ora ultimei modificări a profilului
Schimbat de	Contul care a efectuat ultimele modificări
Revizuirea actuală a profilului	Revizuirea stării profilului salvat
Revizuire profil eliberată	Revizuirea profilului atribuit ("Atribuie acum"). Dacă eticheta afișează "(învechit)" în spatele textului, înseamnă că ați salvat profilul, dar nu l-ați atribuit încă, astfel încât dispozitivele vor primi în continuare o versiune mai veche.

Informații generale

Dacă vă aflați direct pe dispozitiv, veți primi o scurtă prezentare generală a dispozitivului selectat.

Numele dispozitivului	Numele dispozitivului
Număr de telefon	Numărul de telefon al dispozitivului
Model	Numărul modelului
Sistem de operare	SO
Numărul de serie	Numărul de serie al dispozitivului
Proprietatea dispozitivului	Dispozitiv corporativ sau privat Corporate = dispozitiv corporativ Angajat = dispozitiv privat
Tip dispozitiv	Tipul dispozitivului (tabletă sau telefon)
Jailbroken	Dacă există un Jailbreak pe dispozitiv
Supravegheat	Indică dacă acesta este un dispozitiv supravegheat
Conform	Dacă au fost încălcate anumite orientări
Văzut ultima dată	Starea când dispozitivul a comunicat ultima dată cu serverul AppTec360

Setări

Aceste setări conțin numele dispozitivului și un fundal predefinit.

Nume dispozitiv la numele sistemului	Numele care va fi emis în Consola AppTec360 (în structura ierarhică din stânga), va fi același cu cel de pe dispozitivul utilizatorului final respectiv (poate fi vizualizat în setările dispozitivului)
Utilizați tapet personalizat (numai dispozitive supravegheate)	Aici puteți predefini fundalul care ar trebui să fie afișat pe dispozitivul utilizatorului final (de exemplu, pentru un tip de branding corporativ pentru dispozitiv) Este disponibil numai în modul supravegheat!
Actualizări automate ale sistemului de operare	Forțează actualizările sistemului de operare dacă sunt disponibile. Numai pentru dispozitivele DEP în modul supravegheat.
Fonturi personalizate	Aici puteți adăuga fonturi personalizate.
Nume și prenume	Opțional. Numele vizibil pentru utilizator al fontului. Acest câmp este înlocuit de numele real al fontului după instalare.
Font	Încărcați fișierul fontului (.otf sau .ttf).

Revizuire configurare

Aici veți primi o prezentare generală a profilului de grup care este desemnat pentru dispozitiv.

Dacă faceți clic pe profilul grupului, veți accesa direct profilul și veți putea efectua setările.

Cu ajutorul simbolului, puteți readuce aplicațiile alocate la setările profilului de grup.

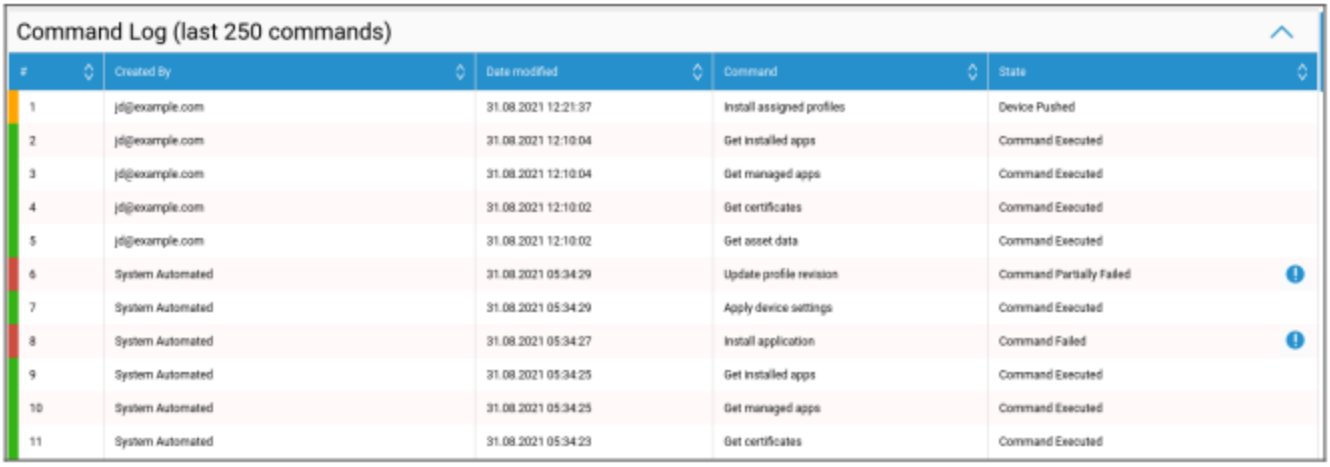
Cu ajutorul simbolului, puteți reseta profilul dispozitivului pentru a nu avea niciun fel de setări.

"Newer Revision available" indică faptul că profilul grupului a fost modificat și salvat, dar nu a fost atribuit. Profilul de grup trebuie să fie atribuit cu "Assign now" la nivel de grup pentru a aplica modificările dispozitivelor.

Jurnalul dispozitivului (numai la nivel de dispozitiv)

Jurnal de comandă

Aici puteți vedea ce comenzi au fost emise pentru dispozitiv și care este starea lor.



Comenzile create de "System Automated" sunt create automat de sistem.

Stări posibile ale comenzii

Dispozitiv împins	O solicitare push a fost trimisă către serviciul push (de exemplu, APNS) pentru a indica dispozitivului să se conecteze din nou la serverul EMM.
Comandă creată	Comanda a fost creată în sistem.
Comandă trimisă	Comanda a fost trimisă către dispozitiv după ce acesta s-a conectat la server.
Comandă executată	Comanda a fost executată cu succes.
Comandă eșuată	Comanda a eșuat. *
Comandă eșuată parțial	În funcție de sistemul de operare al dispozitivului, unele comenzi pot fi grupate împreună. În acest caz, unele părți ale acestui grup de comandă au eșuat. *
Comandă executată, eventual eșuată	Comanda a fost executată, dar poate că nu a fost.
Comanda Repushed	Comanda a fost respinsă de un utilizator.
Aruncată	Comanda a fost eliminată. De exemplu, pentru că a fost înlocuită de o altă comandă sau pentru că dispozitivul a fost înrolat din nou și comenzile vechi au fost eliminate

Dacă în spatele mesajului există un semn al exclamării, puteți obține mai multe informații dacă treceți cu cursorul peste pictogramă.

Gestionarea activelor (numai la nivel de dispozitiv)

Gestionarea activelor (numai la nivel de dispozitiv)

Informații despre dispozitiv

Model	Numărul de model al dispozitivului
Sistem de operare	SO
Versiunea sistemului de operare	Versiunea sistemului de operare
Numărul de serie	Numărul de serie
UDID	UDID dispozitiv
Numele dispozitivului	Numele dispozitivului
Supravegheat	Afișează dacă dispozitivul este supravegheat
Starea bateriei	Starea bateriei

Wi-Fi

Adresa IP	Adresa IP a dispozitivului
WiFi MAC	Adresa MAC WiFi

Celulare

Statut	Stare (cartela SIM prezentă)
Număr de telefon	Numărul de telefon
Starea de roaming	Starea curentă de roaming
Roaming (voce/date)	Starea de roaming pentru voce/date
Adresa IP	Adresa IP
IMEI	Numărul IMEI
Operator/Carrier	Furnizor de servicii celulare
Rețea SIM Carrier	Rețeaua operatorului SIM
Versiunea de transport	Versiunea de transport
Firmware modem	Modem firmware
Actual MCC/MNC	Consultați "SIM MCC/MNC"
SIM MCC/MNC	Codul de țară mobil este un cod de identificare a țării stabilit de ITU în conformitate cu standardul E.212, care, împreună cu codul rețelei mobile (MNC), este utilizat pentru a identifica o rețea celulară (= cod de țară) Atunci când intrați într-o altă rețea celulară, "Current MCC/MNC" și "SIM MCC/MNC" sunt, prin urmare, diferite.

Bluetooth

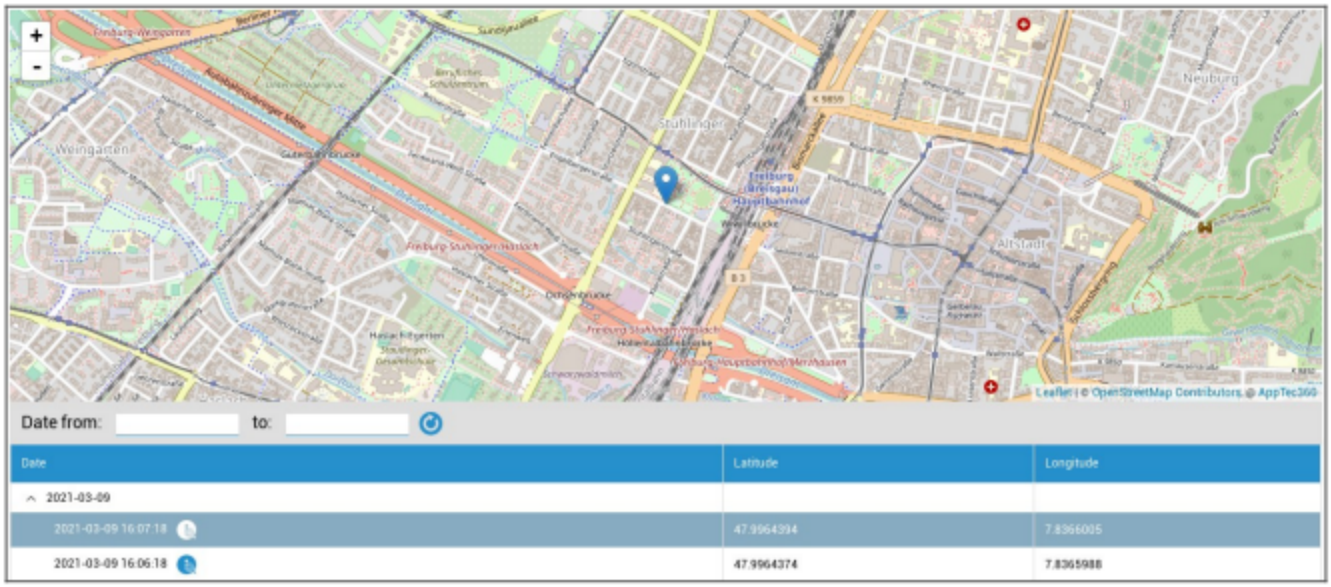
Bluetooth MAC	Adresa MAC Bluetooth

Managementul securității

Anti-furt (numai la nivel de dispozitiv)

Informații GPS (numai la nivelul dispozitivului)

Aici puteți evalua locația curentă/ultima locație a dispozitivului. Localizarea poate fi protejată cu una sau chiar două parole - Consultați: Setări generale - Confidențialitate - Acces GPS



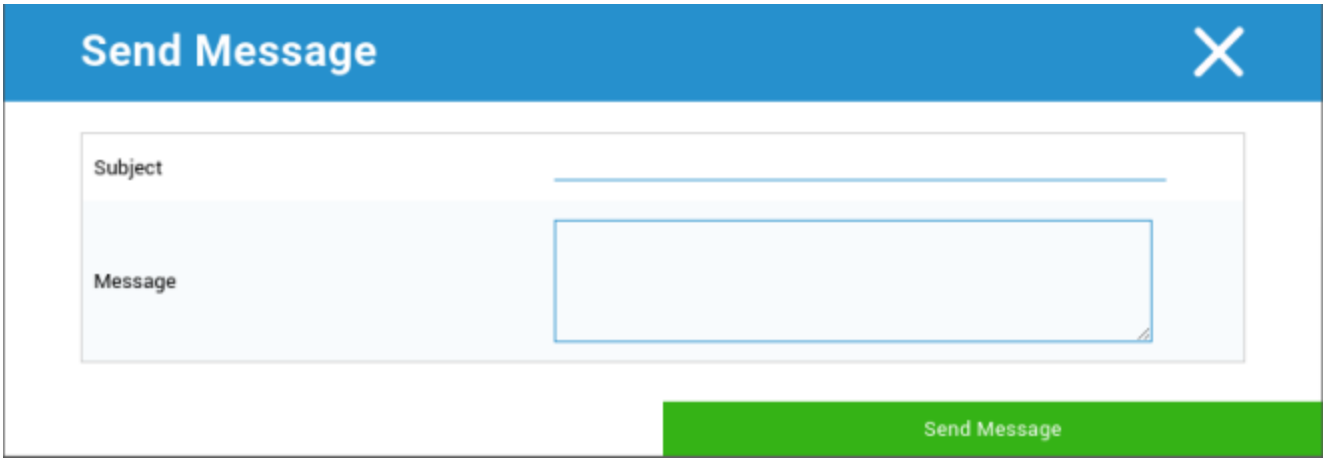
Ștergere și blocare (numai la nivel de dispozitiv)

Sub "Ștergere și blocare", puteți efectua următoarele trei acțiuni:

Ștergere completă	Dispozitivul este readus la setările din fabrică (datele corporative, precum și cele personale sunt șterse)
Ștergere Enterprise	Doar datele corporative sunt eliminate de pe dispozitivul utilizatorului final (toate aplicațiile, datele, etc. care au fost furnizate de AppTec)
Ecran de blocare	Blocarea ecranului este activată, este suficient să deblocați dispozitivul cu ajutorul parolei dispozitivului/PIN
Blocare criminalistică (numai dispozitive supravegheate)	În cazul în care această funcție este activată cu simbolul  , dispozitivul va fi blocat, afișând un mesaj care nu poate fi închis. De asemenea, angajatul nu poate debloca dispozitivul. Numai administratorul poate debloca dispozitivul în consolă cu simbolul de deblocare  .
Permiteți blocarea activării (numai dispozitive supravegheate)	În cazul în care această funcție este activată , dispozitivul va fi blocat, de îndată ce "Găsiți iPhone-ul meu" este activat în setările iCloud

Mesaj (numai la nivel de dispozitiv)

Cu ajutorul următoarei ferestre, puteți completa subiectul și un mesaj și le puteți trimite către un dispozitiv al utilizatorului final:



Configurația de securitate

Codul de acces

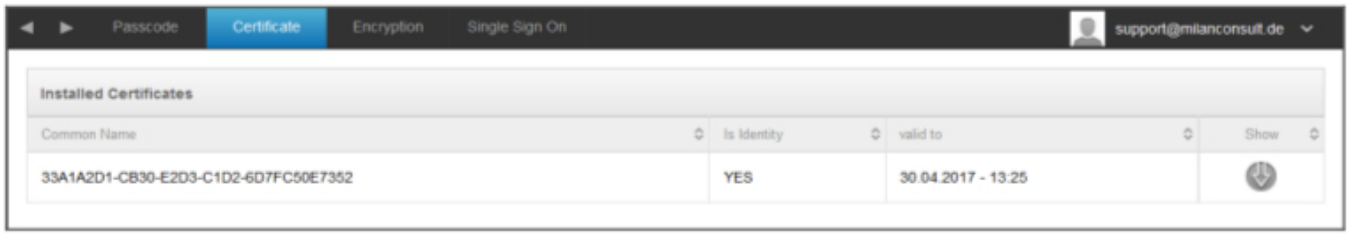
Aici se stabilesc setările pentru parola dispozitivului

Dezactivarea codului este permisă	Atunci când această setare este activată, nu există nicio solicitare de introducere a unei parole De îndată ce o parolă este stabilită, aceasta nu poate fi dezactivată
Permiteți o valoare simplă	Permiteți utilizatorului să utilizeze aceleași șiruri de numere, crescătoare și reducătoare (ex. 1234, 1111)
Necesită valoare alfanumerică	Parolele trebuie să conțină cel puțin o literă
Lungimea minimă a codului de acces	Lungimea minimă a parolei
Numărul minim de caractere complexe	Numărul minim de simboluri alfanumerice din parolă
Vârsta maximă a codului de acces	Numărul de zile, după care parola trebuie schimbată
Blocare automată maximă	Timpul maxim după care dispozitivul este blocat
Perioada maximă de grație pentru blocarea dispozitivului	Timp, după care dispozitivul intră în Stand-By blocat
Numărul maxim de încercări eșuate	Stabilește de câte ori o parolă poate fi introdusă incorect, înainte de a se efectua o ștergere completă a dispozitivului
Vârsta maximă a codului de acces (1-730 de zile)	Vârsta maximă a parolei
Istoricul codurilor de acces (1-50 coduri de acces)	Utilizarea unei parole vechi este permisă după acest număr

Un clic pe coșul de gunoi deschide dialogul de resetare a parolei, cu ajutorul căruia poate fi ștearsă parola uitată a dispozitivului.

Certificat (numai la nivel de dispozitiv)

Afișează certificatele care sunt disponibile pe dispozitiv


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

Criptare

Cer criptarea stocării	Activați funcția de criptare a dispozitivului instalat

Conectare unică

La punctul "Single Sign-On", puteți configura autentificarea Kerberos.

Aici, se stabilesc acreditările de acces și URL-urile/aplicațiile respective care au permisiunea de a utiliza jetoanele Kerberos.

Disponibil în modul supravegheat	
Numele contului	Numele contului
Nume principal	Identitate unică pentru care pot fi distribuite bilete Kerberos
Tărâm	Kerberos Realm, care urmează să fie utilizat (de exemplu, domeniul dvs.)

Cu ajutorul simbolului, puteți stabili URL-uri suplimentare.

Model URL utilizat pentru a limita acest cont	URL-uri care urmează să fie stabilite, la care pot fi distribuite bilete Kerberos

Cu ajutorul simbolului, puteți stabili aplicații suplimentare.

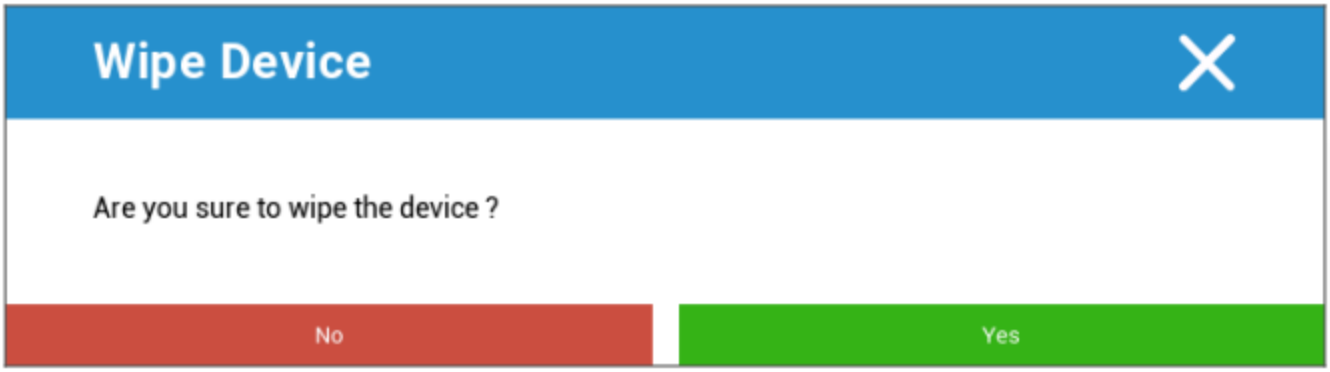
Aplicații pentru a limita acest cont	De determinat Aplicații, la care pot fi distribuite bilete Kerberos

Sfârșitul duratei de viață (numai la nivel de dispozitiv)

Ștergere (numai la nivel de dispozitiv)

Sub "Ștergere", puteți readuce dispozitivul la setările din fabrică. Aici, atât datele corporative, cât și cele private vor fi șterse de pe dispozitivul utilizatorului final.

Făcând clic pe "Simbolul minus", ar trebui să primiți următorul mesaj



Cu "Da" puteți efectua ștergerea.

Sub "Raport ștergere" pot fi afișate următoarele elemente

Șters de	Istoricul persoanei care a efectuat ștergerea
Data	Data
Statut	Stare (de exemplu, dacă ștergerea a fost efectuată cu succes)

Setări de restricționare

Funcționalitatea dispozitivului

Aici puteți bloca funcționalitățile individuale ale dispozitivelor utilizatorilor finali

Permiteți instalarea aplicațiilor	Permiteți instalarea de aplicații
Permiteți camerei	Permiteți utilizarea camerei
Permiteți FaceTime	Permiteți FaceTime
Permiteți capturarea ecranului	Permiteți capturarea ecranului
Permiteți sincronizarea automată în roaming	Permiteți sincronizarea automată în roaming
Permiteți Siri	Permiteți Siri
Permiteți apelarea vocală	Permiteți apelarea vocală
Permiteți achiziționarea în aplicație	Permiteți achiziționarea în aplicație
Solicitați parola iTunes Store pentru toate achizițiile	Solicitați parola iTunes Store pentru toate achizițiile
Permite jocuri multiplayer	Permite jocuri multiplayer
Permite adăugarea de prieteni Game Center	Permite adăugarea de prieteni Game Center
Permiteți deschiderea de la gestionat la negestionat	Permiteți deschiderea conținutului din aplicațiile gestionate în aplicațiile negestionate
Permiteți deschiderea de la negestionat la gestionat	Permiteți deschiderea conținutului din aplicațiile negestionate în aplicațiile gestionate
Permiteți vizualizarea zilei de astăzi în ecranul de blocare	Când această setare este activă, vizualizarea "Astăzi" va fi afișată în Centrul de notificări pe ecranul de blocare
Permiteți centrul de control în ecranul de blocare	Permiteți Centrul de control pe ecranul de blocare
Permiteți TouchID	Permiteți TouchID
Permiteți actualizarea PKI prin aer (over-the-air)	Permiteți actualizarea PKI prin aer (over-the-air)
Permiteți cartela în timpul blocării	Permiteți agenda în timp ce dispozitivul este blocat

Limitați urmărirea anunțurilor	Această funcție dezactivează urmărirea anunțurilor (de exemplu, agenții de publicitate nu pot utiliza urmărirea anunțurilor pentru a distribui anunțuri personalizate)
Permiteți Handoff	Permiteți Handoff
Permiteți afișarea rezultatelor de pe internet în lumina reflectoarelor	Permiteți rezultatele internetului în lumina reflectoarelor (ex. Bing sau Wikipedia)
Cer codul de acces la prima împerechere AirPlay	Cer codul de acces la prima împerechere AirPlay
Force Watch Protecție pentru încheietura mâinii	Dacă este activat, Apple Watch este forțat să utilizeze "Wrist Protection" (recunoașterea încheieturii mâinii)
Permiteți Biblioteca foto iCloud	Permite Biblioteca foto iCloud. Dacă nu este permis, atunci toate fotografiile care nu au fost descărcate complet din iCloud vor fi șterse de pe spațiul de stocare local
Disponibil în modul supravegheat	
Permiteți modificarea contului	Permiteți modificarea "e-mail, contacte, calendar"
Permiteți AirDrop	Permiteți AirDrop
Permiteți modificarea celulară a aplicației	Această setare blochează setarea pentru care aplicații li se permite să utilizeze date mobile Această setare poate fi, de exemplu, setată manual pe dispozitivul utilizatorului final și apoi această restricție poate fi activată
Permiteți Siri să interogheze conținut generat de utilizatori de pe web	Căutarea pe internet pe anumite site-uri este blocată, de exemplu Wikipedia, deoarece fiecare poate face modificări după cum dorește
Activați filtrul de profanare Siri	Înjurăturile care sunt adresate lui Siri sunt cenzurate
Permiteți iBook Store	Permiteți iBook Store
Permiteți iBook Store Erotica	Permiteți iBook Store Erotica
Permiteți modificarea setărilor Găsiți-mi prietenii	Permiteți modificarea setărilor Găsiți-mi prietenii
Permiteți Game Center	Permiteți Game Center
Permiteți împerecherea gazdelor	Asocierea computerului de control
Permiteți instalarea profilurilor de configurare	Permite instalarea de profiluri de configurare

Permiteți Eliminarea aplicației	Eliminarea aplicațiilor de control
Permiteți iMessage	Permiteți iMessage
Permiteți ștergerea întregului conținut și a setărilor	Permite ștergerea întregului conținut și a setărilor
Permiteți configurarea restricțiilor	Permiteți configurarea restricțiilor
Allow Podcast	Allow Podcast
Permiteți căutarea definiției	Permite căutarea definiției
Permiteți tastatură predictivă	Permiteți tastatura predictivă
Permiteți corecția automată	Permiteți corecția automată
Permiteți instalarea aplicației UI	Dacă este dezactivat, nu pot fi instalate aplicații din AppStore-ul public (pictograma nu va mai fi afișată). Cu toate acestea, aplicațiile pot fi în continuare instalate prin iTunes și Configurator
Permiteți comenzile rapide de la tastatură	Permiteți comenzile rapide de la tastatură, dacă dispozitivul este atașat la o tastatură fizică
Permiteți împerecherea Apple Watch	Interzice o împerechere între dispozitiv și Apple Watch, conexiunile existente vor fi întrerupte
Permiteți modificarea codului de acces	Dacă nu este permisă, nicio parolă a dispozitivului nu poate fi adăugată, modificată sau eliminată
Permiteți modificarea numelui dispozitivului	Ghid pentru a determina dacă numele dispozitivului poate fi schimbat
Permiteți modificarea tapetului	Ghid pentru a determina dacă tapetul poate fi schimbat
Permiteți descărcarea automată a aplicațiilor	Dacă este dezactivată, o aplicație achiziționată nu va fi instalată automat pe alte dispozitive. Nu se aplică actualizărilor pentru aplicațiile existente
Allow News	Permiteți News pe dispozitivul iOS
Permiteți încrederea în aplicațiile Enterprise	Dacă este setat la false, previne încrederea în aplicațiile enterprise

iCloud

Blocați anumite funcționalități în timpul împerecherii iCloud

Permiteți backup	Permiteți backup
Permiteți sincronizarea documentelor	Permiteți sincronizarea documentelor
Permiteți fluxul foto	Permiteți fluxul foto
Permiteți fluxul foto partajat	Permiteți fluxul foto partajat
Permiteți sincronizarea lanțului de chei Cloud	Permiteți sincronizarea lanțului de chei Cloud
Permiteți aplicațiilor gestionate să stocheze date	Permiteți aplicațiilor gestionate să stocheze date
Permiteți sincronizarea notelor și a evidențelor pentru cărțile întreprinderii	Permiteți sincronizarea notelor și a evidențelor pentru cărțile întreprinderii
Permiteți copierea de rezervă a registrelor întreprinderii	Permiteți copierea de rezervă a registrelor întreprinderii

Securitate și confidențialitate

Blocați aceste funcționalități asociate cu datele de diagnosticare

Permite trimiterea datelor de diagnosticare către Apple	Permiteți trimiterea datelor de diagnosticare către Apple
Permiteți utilizatorului să accepte certificate TLS care nu sunt de încredere	Permiteți utilizatorului să accepte certificate TLS neîncrezătoare
Forțarea backup-urilor criptate	Forțarea backup-urilor criptate

BYOD

Securitate iOS încorporată (container)

iOS a fost întotdeauna capabil să facă diferența între gestionat (business) și negestionat (privat). Tot ceea ce provine din sistemul MDM este tratat ca fiind gestionat. De exemplu, dacă instalați o aplicație prin MDM sau configurați un cont Exchange, acest lucru va fi tratat ca fiind gestionat de iOS.

Orice altceva care este configurat/instalat manual pe dispozitiv va fi tratat ca fiind negestionat. De exemplu, dacă utilizatorul instalează singur WhatsApp sau dacă adaugă un cont Exchange. Cu toate acestea, această separare nu a afectat niciodată contactele. Dar începând cu iOS 11.3 (și versiunile ulterioare), acest lucru a fost adăugat și pentru contacte.

Deoarece aceasta este o funcționalitate de bază a sistemului de operare, nu trebuie să instalați nimic sau să configurați un container special.

Activați funcția încorporată pentru a separa aplicațiile/informațiile/fișierele private de cele de afaceri. Această setare va dezactiva și alte funcții, care ar putea dezactiva din greșeală părți ale acestei separări.

Activare

Activați soluțiile de containere care sunt acceptate de AppTec360

Activați Google Divide Container	Activați Google Divide Container
Activați SecurePIM Container	Activați SecurePIM Container

În cazul în care ați activat SecurePIM Container, veți găsi, de asemenea, următorul punct sub "Activare". În plus, se vor deschide imediat alte patru file, care sunt descrise mai jos.

Adresă de e-mail pentru asistență	Adresa de e-mail de asistență la care un utilizator se poate adresa cu probleme

Parolă SecurePIM

Sub "Parolă SecurePIM", puteți stabili liniile directoare pentru puterea de securitate a parolei.

Timeout sesiune	Aici puteți stabili după câte minute trebuie introdusă din nou o nouă parolă, odată ce SecurePIM rulează în fundal
Lungimea parolei	Lungimea parolei pentru accesul la SecurePIM Container
Caractere majuscule	Minimum de caractere majuscule
Caractere minuscule	Minimum de caractere minuscule
Caractere speciale	Caractere speciale minime
Cifre	Cifre minime
Aplicație de ștergere	Numărul de ori în care o parolă poate fi introdusă incorect, înainte ca conținutul SecurePIM să fie șters (Cu toate acestea, aplicația rămâne în continuare pe dispozitivul utilizatorului final)

SecurePIM Securitate

Sub "Securitate SecurePIM", puteți stabili o varietate de setări de securitate.

Detectarea dispozitivelor Jailbroken	În cazul în care această setare este activată, accesul la containerul SecurePIM va fi blocat, de îndată ce dispozitivul este detectat ca fiind jailbroken
Câmpuri text securizate	Conținutul câmpurilor de depunere va fi criptat, nicio informație nu ajunge la sistemul de operare (iOS) Notă: Atâta timp cât această setare este activă, autocorectarea nu mai este disponibilă
Exportul datelor de contact către dispozitiv	Dacă această setare este activată, atunci utilizatorului i se permite să exporte contactele Exchange pe dispozitivul său local Notă: Numai numele și numărul de telefon sunt exportate
Afișați locația evenimentului	În cazul în care această setare este activată, locația evenimentelor viitoare va fi afișată în bara de notificare
Afișați titlul evenimentului	În cazul în care această setare este activată, locația titlului viitorului eveniment va fi afișată în bara de notificare

Browser SecurePIM

Aici puteți configura browserul SecurePIM.

Cu ajutorul simbolului, puteți defini o nouă adresă URL.

Cu ajutorul simbolului, puteți elimina din nou un URL definit.

"Whitelisted URLs" sunt URL-uri care pot fi încărcate.

"URL-urile de pe lista neagră" sunt URL-uri care nu pot fi încărcate și sunt astfel blocate.

Vă rugăm să rețineți că intrările de pe lista albă au o prioritate mai mare decât intrările de pe lista neagră. Sub "Titlu marcaj" puteți emite un titlu. Cu "Bookmark URL", puteți asocia adresa URL cu titlul marcajului - în acest fel puteți distribui marcaje individualizate utilizatorilor respectivi.

Schimb

Sub "Exchange" puteți configura un cont Exchange.

Adresa de e-mail ActiveSync	Adresa de e-mail de schimb (luați notă de "Placeholders")
Conectare ActiveSync Exchange	Numele utilizatorilor de schimb (luați notă de "Placeholders")
ActiveSync Exchange Server	Adresa serverului Exchange (FQDN)
ActiveSync Domeniu Exchange	Adresa domeniului Exchange
Certificat de utilizator	Certificat de utilizator
Autentificare pe bază de certificat	Utilizatorul se autentifică cu un certificat
Permiteți criptarea S/MIME	Permite utilizatorului să își cripteze corespondența
Permiteți semnarea S/MIME	Permite utilizatorului să își semneze corespondența
Verificarea CRL	Dacă este activ, certificatul privat va fi comparat cu CRL (Certificate Revocation List)

Gestionarea conexiunilor

Wi-Fi

Identificatorul setului de servicii (SSID)	SSID al rețelei care urmează să fie conectată
Auto Join	Activarea participării automate la aderarea la o rețea
Rețea ascunsă	Activare, în cazul în care AP nu transmite SSID-ul

Configurare proxy

Configurarea unui proxy pentru fiecare punct de acces

Niciuna	Nu stabiliți niciun Proxy
Manual	Stabilirea unui proxy manual
URL server proxy	Adresa pentru accesarea setărilor proxy
Port	Stabiliți portul pentru Proxy
Autentificare	Numele de utilizator pentru autentificarea pe Proxy
Parolă	Parolă pentru autentificarea pe Proxy
Automată	Stabiliți automat un proxy
URL server proxy	URL pentru accesul la setările Proxy

Tip de securitate

Stabilirea tipului de securitate pentru AP

WEP	
Parolă	Parolă pentru AP

WPA/WPA2	
Parolă	Parolă pentru AP

WEP Enterprise - WPA / WPA2 Enterprise - Any Enterprise			
	Protocoale		
	TLS	Activare/Dezactivare	
	TTLS	Activare/Dezactivare	
	LEAP	Activare/Dezactivare	
	PEAP	Activare/Dezactivare	
	EAP-FAST	Activare/Dezactivare	
	EAP-SIM	Activare/Dezactivare	
	Utilizați PAC		Utilizarea PAC (Protected Access Controll)
	Dispoziție PAC	Configurarea PAC Provision	
	Furnizați PAC în mod anonim	Furnizarea anonimă de PAC	
	Autentificări interne	Protocolul de autentificare care ar trebui utilizat: PAP, CHAP, MSCHAP, MSCHAPv2	
	Nume utilizator	Nume utilizator de autentificare	
	Nu utilizați parola per-conectare	Nu utilizați parola per-conectare	
	Certificat de identitate	Încărcați/selectați certificatul de autentificare	
	Identitate exterioară	Identitate care poate fi văzută în exterior	
	Încredere		
	Certificat de încredere 1	Încărcați primul certificat de încredere	
	Certificat de încredere 2	Încărcați al doilea certificat de încredere	
	Certificat de încredere 3	Încărcați al treilea certificat de încredere	
	Numele certificatelor serverului de încredere	Numele certificatelor de server așteptate (într-o listă separată prin virgulă)	

Niciuna	Nu stabiliți nicio securitate

VPN

Nume conexiune	Numele profilului VPN

Tip VPN

VPN

Tot traficul de rețea al dispozitivului va fi direcționat printr-o conexiune VPN.

Tip de conexiune	Stabilirea tipului de conexiune VPN
IPsec (cisco)	Protocolul IPsec de cisco
PPTP	Protocol PPTP
L2TP	Protocolul L2TP
Cisco AnyConnect	Protocolul AnyConnect
Juniper SSL	Protocol SSL Juniper
F5 SSL	Protocolul SSL F5
SonicWall mConnect	SonicWall mobile Connect
Aruba VIA	Protocolul Aruba VIA
SSL personalizat	Conexiune prin SSL personalizat
OpenVPN	Protocolul OpenVPN

VPN per aplicație

La deschiderea unei anumite aplicații, se va stabili o conexiune VPN

Pornirea automată a conexiunii VPN per aplicație		Pornirea automată a conexiunii VPN per aplicație
Tip de conexiune		Stabilirea tipului de conexiune VPN
	Cisco AnyConnect	Protocolul AnyConnect
	Juniper SSL	Protocol SSL Juniper
	F5 SSL	Protocolul SSL F5
	SonicWall mConnect	SonicWall mobile Connect
	Aruba VIA	Protocolul Aruba VIA
	SSL personalizat	Conexiune prin SSL personalizat
	OpenVPN	Protocolul OpenVPN

Configurare proxy

Configurarea unui proxy pentru conexiunea VPN

Niciuna	Nu stabiliți niciun Proxy
Manual	Stabilirea manuală a unui Proxy
URL server proxy	Adresa pentru accesul la setările proxy
Port	Stabiliți portul pentru Proxy
Autentificare	Nume de utilizator pentru autentificarea la Proxy
Parolă	Parolă pentru autentificarea la Proxy
Automată	Stabiliți automat un proxy
URL server proxy	URL pentru accesul la setările Proxy

Afișați marcajele de poziție	Afișează toate variabilele de utilizator disponibile , pe care AppTec360 le poate utiliza

APN

Nume punct de acces	Numele punctului de acces
Nume utilizator punct de acces	Nume utilizator punct de acces
Parola punctului de acces	Parola punctului de acces
Server proxy	Adresa serverului proxy
Port	Portul Proxy respectiv

Celulare

Activarea roamingului de date	Activarea roamingului de date
Activarea roamingului de voce	Activarea roamingului de voce
Activați Hotspot	Activați Hotspot

Proxy HTTP

Tip Proxy	
Manual	Stabiliți manual un Proxy
URL server proxy	Adresa pentru accesul la setările proxy
Port	Stabilirea portului Proxy
Autentificare	Nume de utilizator pentru autentificarea la Proxy
Parolă	Parolă pentru autentificarea la Proxy
Automată	Stabiliți automat un proxy
URL proxy PAC	URL proxy PAC
Permiteți conexiunea directă dacă PAC este inaccesibil	Permiteți conexiunea directă (fără VPN), dacă PAC este inaccesibil
Permite ocolirea proxy-ului pentru a accesa rețele captive	Permiteți ocolirea proxy-ului pentru a accesa rețele interne captive

AirPrint

Adresa IP	Adresa IP a imprimantei
Calea resurselor	Cale definită către dispozitivul AirPrint

AirPlay

Numele dispozitivului	Numele dispozitivului
Parolă	Parolă de împerechere
Lista albă	Definiți o listă de dispozitive, cu care dispozitivul se poate împerechea exclusiv

Gestionarea PIM

Exchange Active Sync

Numele contului	Numele contului de e-mail
Gazdă Exchange ActiveSync	Adresa/FQDN a serverului
Permiteți mutarea	Permiteți mutarea e-mailurilor
A se utiliza numai în poștă	Interacțiunile pot avea loc numai pe aplicația nativă Mail App
Utilizați SSL	Utilizați criptarea SSL
Domeniu	Domeniul serverului
Utilizator	Nume utilizator
Adresa eMail	adresa de e-mail (numai la nivel de dispozitiv)
Parolă (numai la nivel de dispozitiv)	Parola utilizatorului
Certificat de identitate	Selectați certificatul respectiv pentru autentificarea la server
Zilele trecute ale Mail to Sync	Numărul de zile până când e-mailurile ar trebui sincronizate înapoi. Fără limită = nelimitat
Activați S/MIME	Activați criptarea S/MIME
Semnarea certificatului	Încărcați certificatul de semnare respectiv
Certificat de criptare	Încărcați certificatul de criptare respectiv

eMail

Configurarea conturilor POP3 / IMAP pe dispozitivul utilizatorului final

Descrierea contului	Nume des Conturi de e-mail			
Tip de cont	IMAP	Prefixul căii	Prefixul căii pentru folderele speciale	
	POP			
Nume afișare utilizator	Numele de afișare al utilizatorului			
Adresa de e-mail	Adresa de e-mail a utilizatorului			
Permiteți mutarea	Permiteți mutarea e-mailurilor			
Activați S/MIME	Activați criptarea S/MIME			
Semnarea certificatului	Încărcați certificatul de semnare respectiv			
Certificat de criptare	Încărcați certificatul de criptare respectiv			

Poșta de intrare

Setări server de intrare

Adresa serverului de poștă electronică	Adresa serverului de poștă electronică
Portul serverului de e-mail	Portul serverului de poștă electronică
Nume utilizator	Numele utilizatorului respectiv
Tip de autentificare	Tip de autentificare
Niciuna	Niciun tip de autentificare
Parolă (numai la nivel de dispozitiv)	Solicitare parolă
MDM provocare-răspuns	
NTLM	Autentificare NTLM
HTTP MD5 Digest	
Utilizați SSL	Utilizați SSL, dacă este necesar

Poșta de ieșire

Setări server de ieșire

Adresa serverului de poștă electronică	Adresa serverului de poștă electronică
Portul serverului de e-mail	Portul serverului de e-mail
Nume utilizator	Numele utilizatorului respectiv
Tip de autentificare	
Niciuna	Nicio metodă de autentificare
Parolă (numai la nivel de dispozitiv)	Solicitare parolă
MDM provocare-răspuns	
NTLM	Autentificare NTLM
HTTP MD5 Digest	
Utilizați SSL	Utilizați SSL, dacă este necesar
Parola de ieșire este aceeași cu cea de intrare	Parola de ieșire este aceeași cu cea de intrare

Utilizați numai în poștă	Activați, dacă toate e-mailurile de ieșire vor fi trimise prin intermediul aplicației Mail-App

CalDav

Configurați înființarea și distribuirea unui cont CalDav

Descrierea contului	Numele de afișare al contului
Nume gazdă	Nume gazdă și/sau adresă IP
Port	Port al contului CalDav
URL principal	URL-ul principal al contului
Nume utilizator	Numele de utilizator CalDav respectiv
Parolă (numai la nivel de dispozitiv)	Respectiva parolă CalDav
Utilizați SSL	Utilizați SSL, dacă este necesar

Calendare abonate

Configurarea și distribuirea de calendare subscrise

Descriere	Numele de afișare al contului
URL	Adresa URL a bazei de date a calendarului
Nume utilizator	Numele de utilizator al abonamentului calendaristic
Parolă (numai la nivel de dispozitiv)	Parola abonamentului calendaristic
Utilizați SSL	Utilizați SSL, dacă este necesar

LDAP

În această zonă, configurați o conexiune LDAP, pentru a permite un schimb dinamic de certificate între dispozitivul utilizatorului final și Active Directory.

Vă rugăm să rețineți că utilizatorul selectat are nevoie de permisiunea respectivă de citire.

Descrierea contului	Descrierea contului
Nume utilizator cont	Utilizator pentru acces LDAP
Parolă cont	Parolă pentru accesul LDAP
Nume gazdă cont	Nume gazdă/adresa IP a serverului LDAP

Utilizați SSL	Utilizați SSL, dacă este necesar

În a doua parte, puteți defini filtre individuale pentru căutarea în registrul LDAP.

Descriere	Domeniul de aplicare	Baza de căutare
Descrierea filtrului	Nivelul de căutare în registrul LDAP	Definirea filtrului individual

Management web

Clipuri web

În această locație definiți marcaje, cu linkuri către pagini web, portaluri intranet etc., care vor fi vizibile ca aplicație pe dispozitivul utilizatorului final.

Etichetă	Numele conexiunii de pe dispozitivul utilizatorului final
URL	Link către site-ul respectiv
Detașabil	Dacă este activat, utilizatorul poate elimina webclip-ul
Icoană	Prin intermediul acestui dialog, încărcați un logo pentru conexiune: Dimensiuni 180x180, format png
Icoană precompusă	Dacă este activat, nu vor fi afișate efecte suplimentare (umbră, reflexie) pe pictogramă
Ecran complet	La deschiderea clipurilor web, browserul se deschide în modul ecran complet

Filtru de conținut web

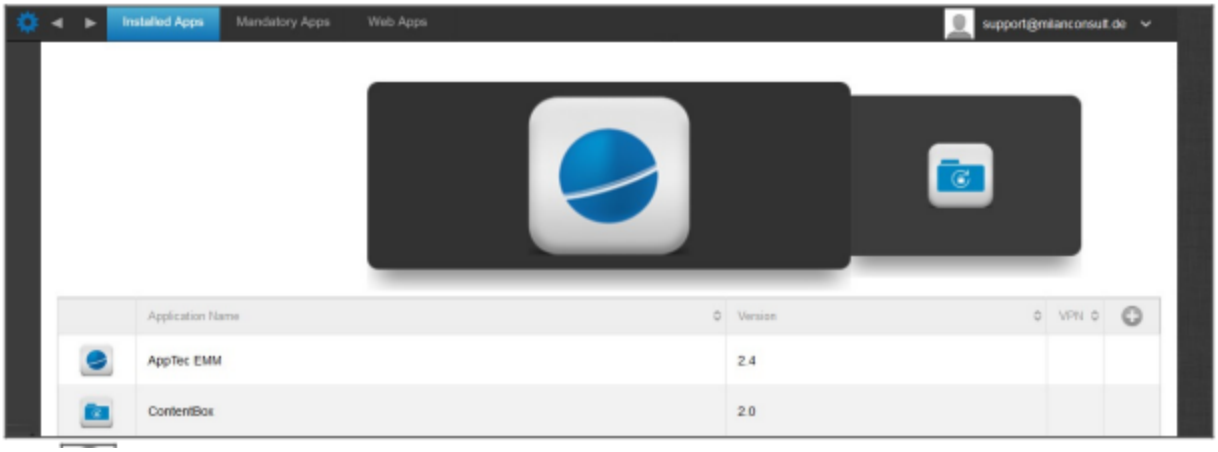
Filtrul de conținut web face posibilă limitarea accesului la anumite pagini de internet.

Site-uri web permise	
Limitați conținutul pentru adulți	Webfilterul este aplicat automat pentru conținutul pentru adulți
URL-uri permise	Cu simbolul + adăugați pagini permise
URL-uri pe lista neagră	Cu simbolul + adăugați pagini blocate
Numai site-uri web specifice	Doar conținutul specific poate fi afișat, pe care îl puteți adăuga cu simbolul +.

Gestionarea aplicațiilor

Enterprise App Manager

Aplicații instalate (numai la nivel de dispozitiv)



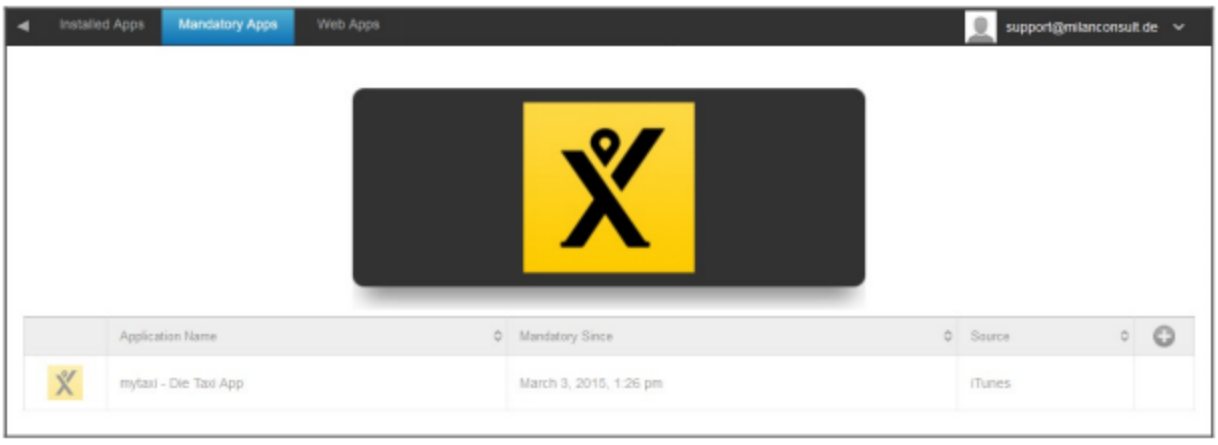
Aici puteți vedea aplicațiile care sunt instalate în prezent pe dispozitiv.

Aplicații obligatorii

Sub Aplicații obligatorii, puteți impune aplicațiile necesare.

Utilizatorului i se va reaminti în permanență să instaleze aplicația menționată.

Prin intermediul , poate fi definită aplicația mandatată.



Aceasta poate fi o aplicație Apple App Store, dar și o aplicație internă.

În cazul în care este vorba despre un dispozitiv supravegheat, aplicația va fi instalată automat.

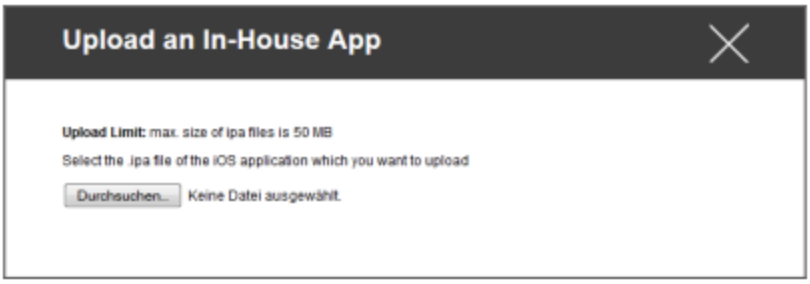
Puteți introduce pe dispozitiv o aplicație "Apple AppStore" din AppStore-ul public, precum și o aplicație dezvoltată intern.

Sau puteți selecta din categoria "iOS In-House Apps" și să alegeți o aplicație In-House, pe care ați încărcat-o în Setări generale.

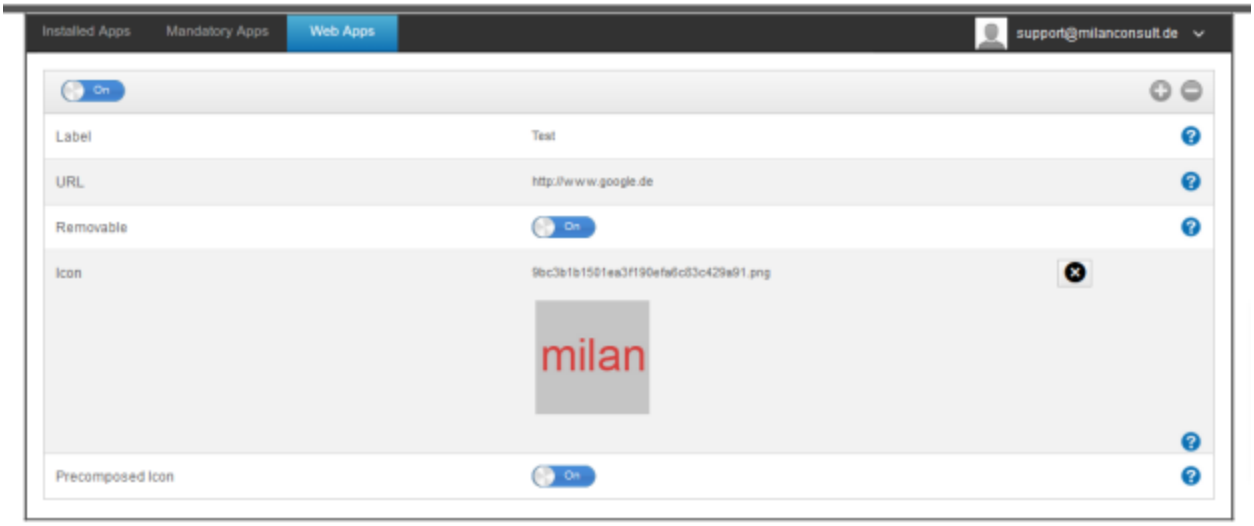
Opțiuni de instalare

Menținerea la zi (acceptat numai pentru VPP pe dispozitiv)	O dată pe săptămână, se va determina dacă există o actualizare pentru aplicație. Dacă da, această actualizare va fi instalată Pentru aplicațiile interne, ținta de actualizare configurată în Setările generale va fi utilizată pentru procesul de actualizare.
Depășire atunci când nu sunt gestionate	Dacă aplicația este deja instalată, MDM va prelua aplicația și o va gestiona
Eliminarea aplicației atunci când profilul MDM este eliminat	În cazul eliminării gestionării dispozitivului, aplicația va fi dezinstalată
Prevenirea copierii de rezervă a datelor aplicației	Nu va fi creată o copie de rezervă a datelor specifice aplicației
Setarea aplicației	Sub "Setări aplicație", puteți atribui aplicației anumite valori în prim-plan (atâta timp cât aplicația acceptă acest lucru, dacă este necesar, întrebați dezvoltatorul aplicației).

De asemenea, puteți selecta și încărca direct un fișier ipa, prin "Încărcare aplicație internă".



Aplicații web



La punctul "Aplicații web", puteți, la fel ca în cazul "Clipurilor web", să împingeți pagini de internet sau portaluri intranet ca aplicație pe dispozitivul utilizatorului final, în zona de gestionare web. În mod prestabilit, aplicațiile Web vor fi afișate în modul ecran complet, care poate fi configurat la punctul Webclips.

Etichetă	Numele conexiunii de pe dispozitivul utilizatorului final
URL	Link către site-ul respectiv
Detașabil	Dacă este activat, utilizatorul poate elimina Webclip-ul
Icoană	Prin intermediul acestui dialog, încărcați un logo pentru conexiune: Dimensiuni 180x180, format png
Icoană precompusă	Dacă este activat, nu vor fi afișate efecte suplimentare (umbră, reflexie) pe pictogramă

Restricții și setări

Aplicații pe lista neagră / pe lista albă

Aici puteți seta aplicațiile care sunt blocate (sau permise) în funcție de setările dvs. din "Setări generale". Un clic pe va afișa căutarea aplicațiilor cunoscute. Aici puteți căuta aplicațiile pe care doriți să le adăugați.

Rețineți că este necesar un dispozitiv supravegheat pentru această funcție

Restricții SysApp

Blocați anumite aplicații sau funcții ale dispozitivului dvs.

Permiteți utilizarea YouTube	Permiteți utilizarea YouTube
Permiteți utilizarea iTunes Store	Permiteți utilizarea iTunes Store
Permiteți utilizarea Safari	Permiteți utilizarea Safari
Activați completarea automată	Permite completarea automată
Avertisment privind fraudarea forței	Forțează avertismentul de fraudă
Activați JavScript	Permite utilizarea JavaScript
Blocați ferestrele pop-up	Blochează toate tipurile de pup-up-uri
Permiteți cookie-urile	Alegeți când Safari va accepta cookie-uri

App-VPN

Prin intermediul simbolului, puteți defini aplicații care vor lansa automat conexiunea VPN selectată la pornire.

Setări aplicație

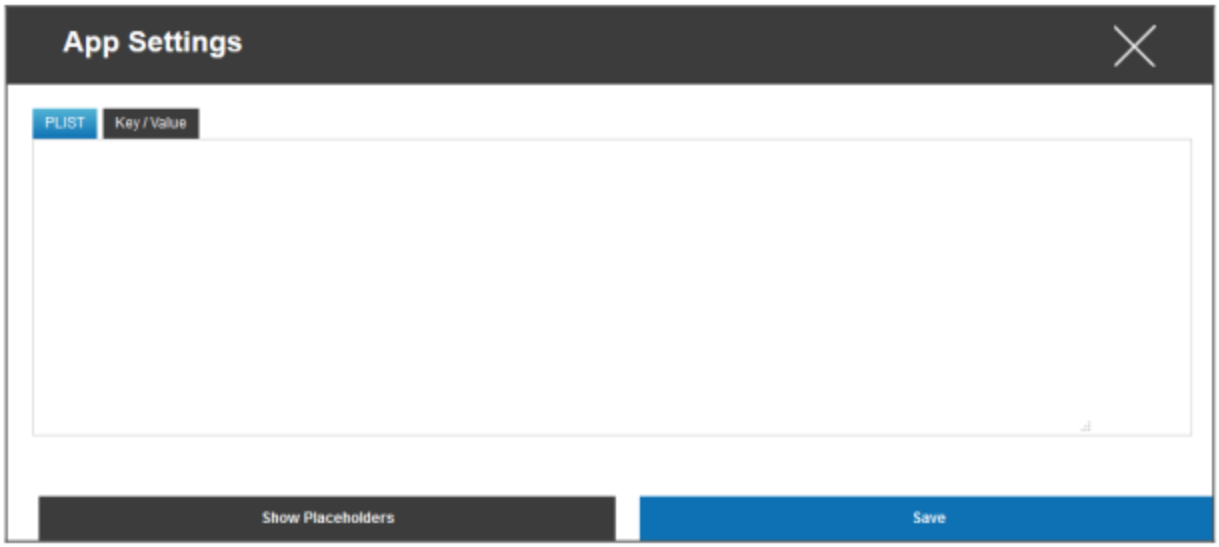
Sub "Setări aplicație", puteți atribui aplicației anumite valori în prim-plan (atâta timp cât aplicația acceptă acest lucru, dacă este necesar, întrebați dezvoltatorul aplicației).

Prin intermediul simbolului, adăugați o aplicație (suplimentară). Veți găsi, încă o dată, reprezentarea familiară AppTec360 a unui App-Import.

Căutați aici aplicația pe care doriți să o configurați și selectați-o. Setările se vor aplica numai aplicațiilor gestionate.

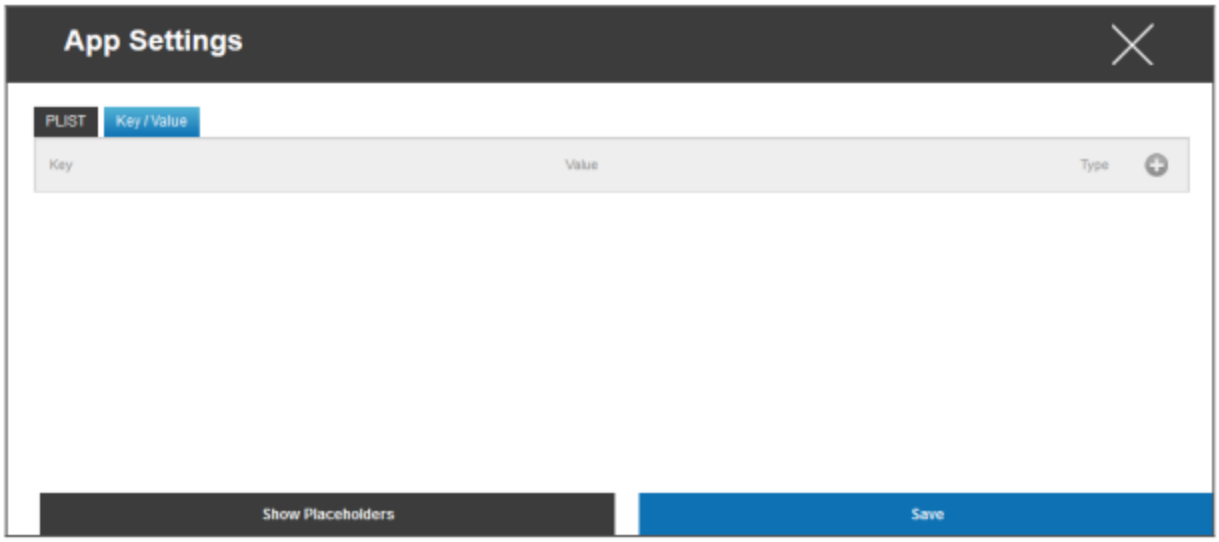
În cazul în care importul a avut succes, veți vedea următorul afișaj:

Acum, cu un clic pe , puteți efectua o varietate de configurații. Veți primi apoi următoarea prezentare generală:

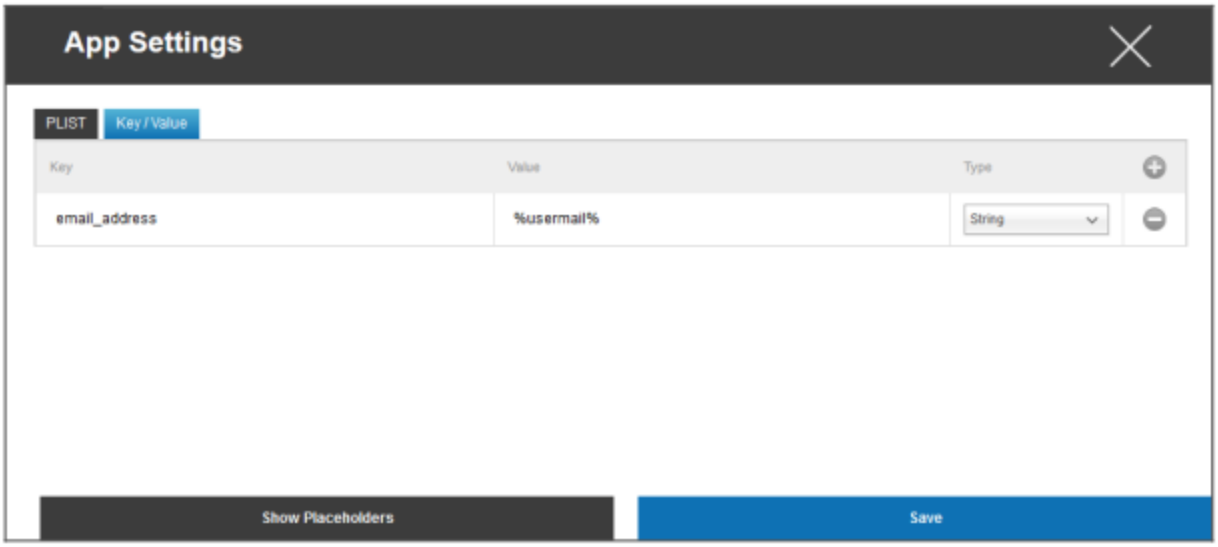


Dacă aveți deja un PLIST (textul sursă al configurației), îl puteți adăuga aici și salvați totul cu "Save".

Sub "Cheie / Valoare", puteți atașa configurații specifice la aplicație



Aici, puteți stabili o nouă cheie și valoarea acesteia cu ajutorul simbolului.



Bineînțeles, toate marcajele AppTec sunt la dispoziția dumneavoastră

Explicație "Tip":

Șir de caractere	Text
Boolean	Adevărat/Fals
Număr	Număr

Cu ajutorul simbolului, puteți elimina din nou o aplicație.

Magazin de aplicații pentru întreprinderi

Aplicații iTunes

La acest punct, puteți distribui aplicații opționale pentru utilizatorul dvs.

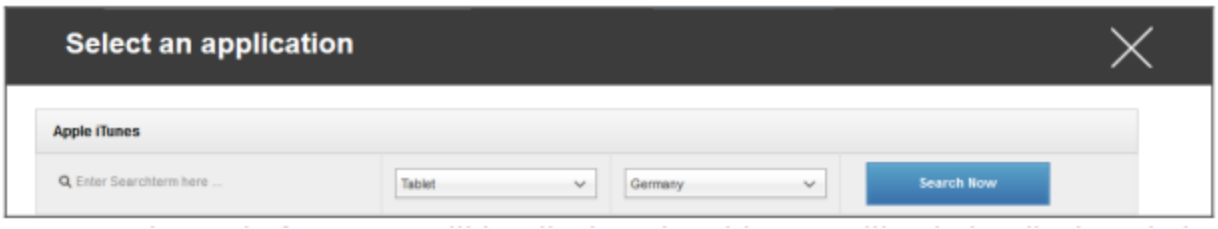
Dacă există o aplicație aici, aceasta va fi instalată automat pe dispozitivul utilizatorului final al magazinului AppTec360.

Acestea sunt doar linkuri către Apple App Store oficial. Din acest motiv, fiecare dispozitiv al utilizatorului final trebuie să fie echipat cu un ID Apple.

În acest moment, vă recomandăm ca fiecare utilizator să aibă propriul ID Apple.

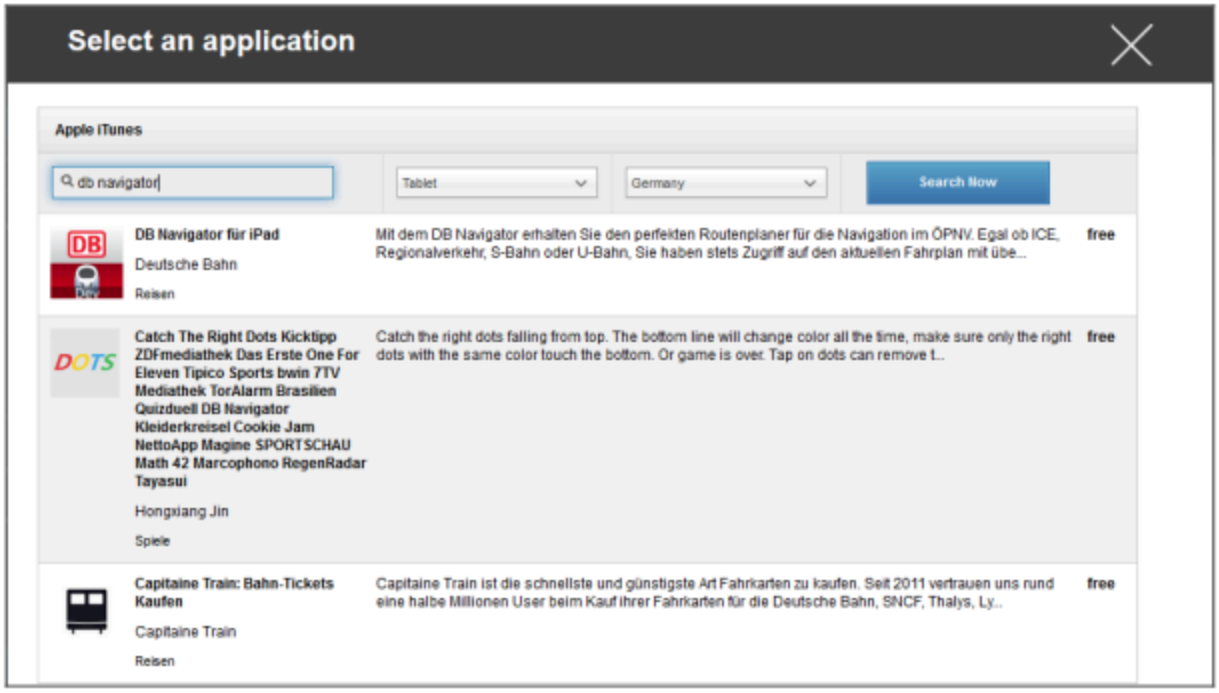
Cu ajutorul simbolului, puteți adăuga aplicații suplimentare.

După aceea, ar trebui să se deschidă o fereastră cu următoarea prezentare generală.



Vă rugăm să rețineți că vor fi afișate numai aplicațiile gratuite, aplicațiile plătite vor fi afișate numai prin VPN.

Sub "Introduceți termenul de căutare aici ...", puteți căuta o aplicație care se află în Apple App Store.



După ce faceți clic pe pictogramă sau pe numele aplicației, vi se va cere din nou să efectuați configurații suplimentare.

Țineți-vă la curent	O dată pe săptămână, se va determina dacă există o actualizare pentru aplicație. Dacă da, această actualizare va fi instalată
Eliminarea aplicației atunci când profilul MDM este eliminat	În cazul eliminării gestionării dispozitivului, aplicația va fi dezinstalată
Prevenirea copierii de rezervă a datelor aplicației	Nu va fi creată o copie de rezervă a datelor specifice aplicației
App-VPN	Selectați o conexiune VPN, care va fi lansată la deschiderea aplicației

După un clic pe "Instalare", aplicația va fi adăugată la Enterprise App Store și poate fi instalată pe dispozitivul utilizatorului final, prin AppTec360 AppStore.

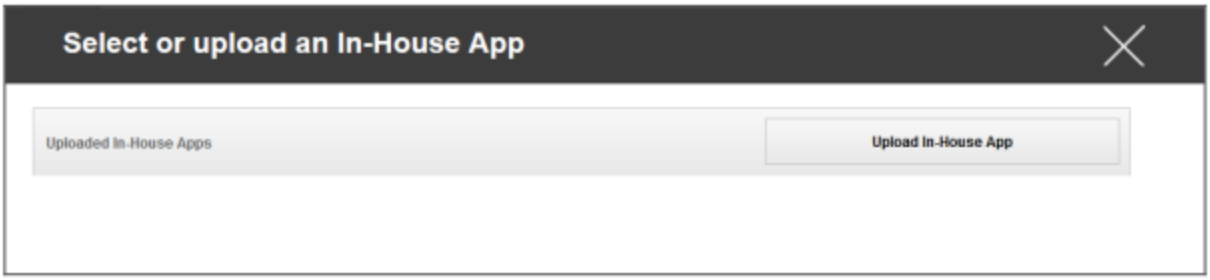
În cazul în care Importul App-Store a fost efectuat cu succes, veți primi următoarea prezentare generală:

In-House

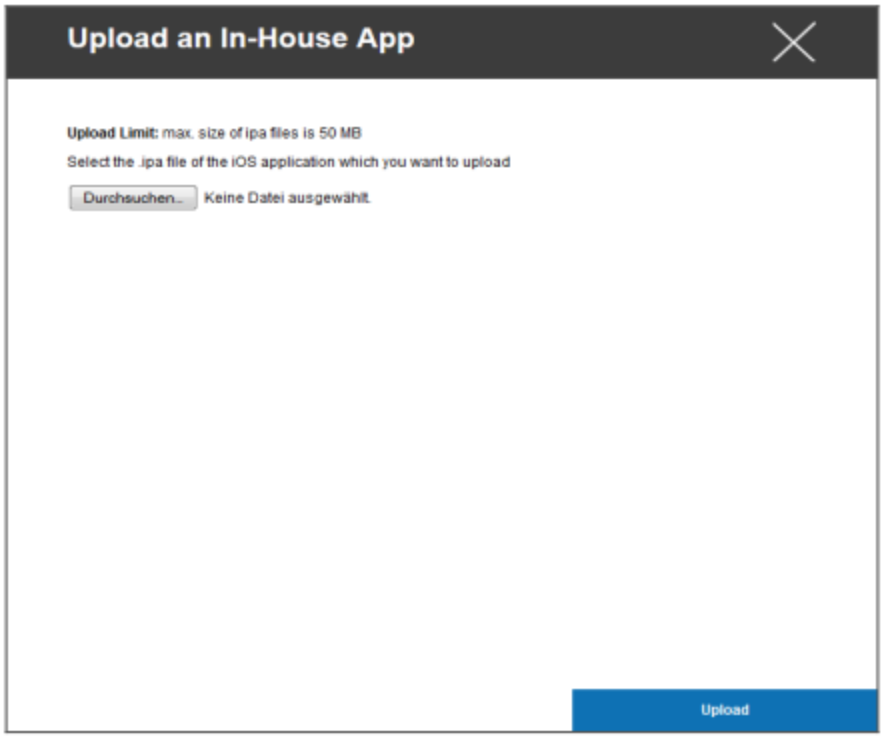
Sub punctul "In-House", puteți încărca aplicații dezvoltate intern și le puteți distribui.

Cu ajutorul simbolului, puteți distribui aplicații In-House suplimentare.

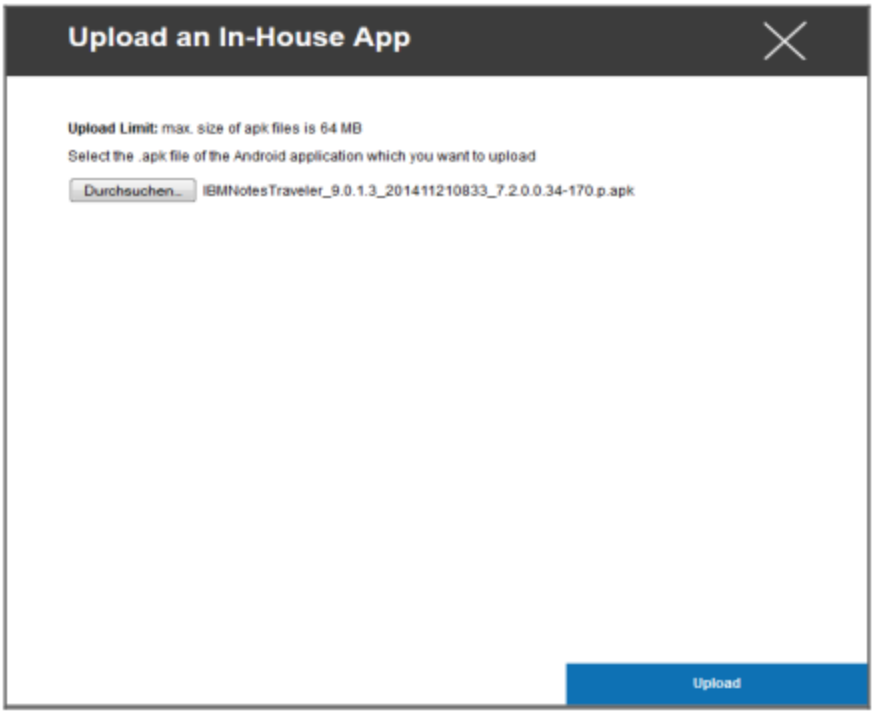
Dacă nu ați distribuit niciodată aplicația In-House, veți primi următoarea prezentare generală:



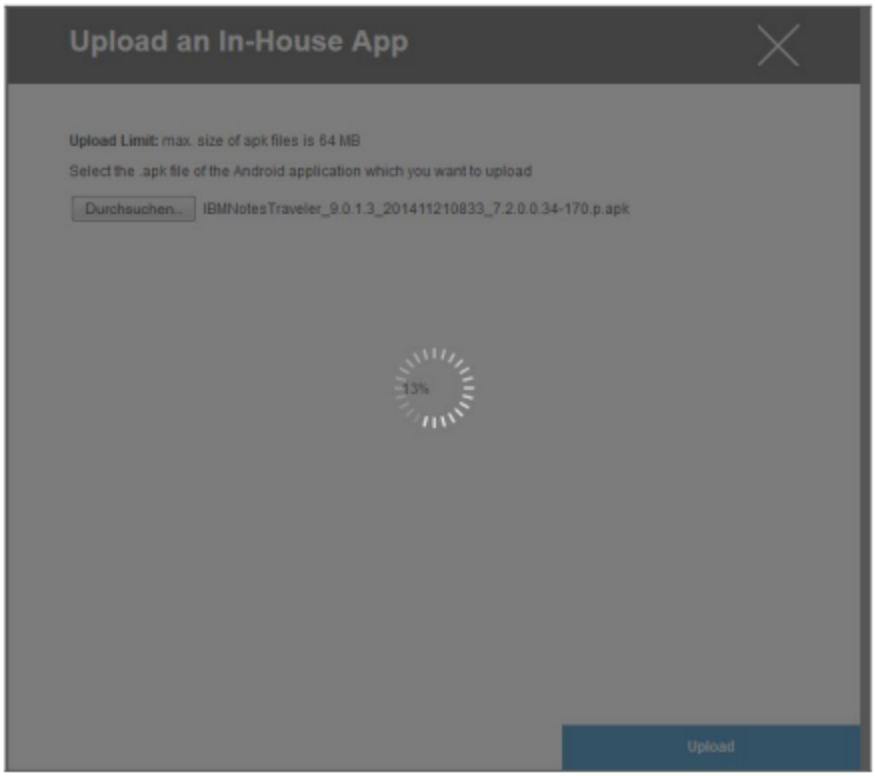
Pentru aceasta, faceți clic pe "Încărcați aplicația In-House", apoi veți primi următoarea prezentare generală:



Acum, selectați cu "Search..."un fișier .ipa și apoi faceți clic pe "Upload"



Aplicația dvs. va fi acum încărcată. În mijlocul cercului, puteți vedea procentul din aplicația dvs. care a fost deja încărcată.



În cazul în care încărcarea aplicației In-House a fost efectuată cu succes, veți vedea aplicația nou încărcată în Catalogul de aplicații.

Utilizatorul are acum opțiunea de a vedea și instala această aplicație în AppTec360 Store pe dispozitivul utilizatorului final, la categoria "In-House".

Datorită faptului că acest lucru nu implică o aplicație Apple AppStore publică, utilizatorul nu are nevoie de un ID Apple stocat pe dispozitivul utilizatorului final.

Modul Kiosk

Modul iOS Kiosk este disponibil numai în modul supravegheat

Modul Kiosk vă permite să predefiniți o aplicație sau un URL, astfel încât va fi posibil să rulați/vizitați exclusiv această aplicație/url.

În plus, puteți dezactiva diverse butoane hardware în modul Kiosk.

Tip de aplicație

Pachet

Dacă doriți să lansați aplicația în modul chioșc, selectați "Pachet" la "Tip aplicație"

Aplicație kiosk	Faceți clic aici, pentru a selecta o aplicație care ar trebui lansată în modul chioșc Veți găsi o prezentare generală curentă a gestionării aplicației Puteți selecta între "Apple iTunes Apps" și "iOS In-House Apps"

URL

Dacă doriți să lansați un URL în modul chioșc, selectați "URL" la "Tip aplicație"

URL	Acum, definiți adresa URL dorită
Politica privind aceeași origine	În cazul în care această funcție este activă, utilizatorul poate naviga numai pe subpaginile URL-ului predefinit De exemplu, dacă ați definit următoarea adresă URL: www.mypage.com, atunci utilizatorul poate naviga pe www.mypage.com/subpage
URL-uri pe lista albă	Aici puteți menține o listă albă, toate aceste URL-uri sunt permise Maximum 1 URL pe linie O adresă URL trebuie să înceapă cu http:/ sau https://
URL-uri pe lista neagră	Aici puteți menține o listă neagră, toate aceste URL-uri sunt interzise Maximum 1 URL pe linie O adresă URL trebuie să înceapă cu http:/ sau https://
Ștergeți browserul după inactivitate	După inactivitate, Cache-ul browserului va fi golit
Parola de ieșire activată	Dacă activați această funcție, utilizatorul are opțiunea de a încheia modul Kiosk cu o parolă predefinită de dvs.
Parola de ieșire	Aceasta este parola care a fost predefinită de dvs.

Setări pentru modul Kiosk

Modul Kiosk programat	Pe baza orei din zi, puteți seta modul Kiosk, astfel încât modul să înceapă și să se încheie automat la o oră prestabilită
Ora de începere	Ora de începere
Timp în minute	Timp în minute, după care modul Kiosk ar trebui să fie încheiat din nou
Dezactivare atingere	Dacă este activat, ecranul tactil este dezactivat
Dezactivarea rotirii dispozitivului	Dacă este activată, adaptarea automată a ecranului este dezactivată
Dezactivare comutator sonerie	Dacă este activat, comutatorul de sonerie va fi apoi dezactivat. Din acel moment, comportamentul depinde de funcția setată anterior
Dezactivați butoanele de volum	Dacă sunt activate, butoanele de volum vor fi dezactivate
Dezactivarea butonului de trezire	Dacă este activat, comutatorul pornit/oprit va fi dezactivat
Dezactivarea blocării automate	Dacă este activat, dispozitivul nu va fi comutat în standby
Activați Voice Over	Dacă este activat, va fi activat asistentul Voice Over
Activați Zoom	Dacă este activat, zoom-ul va fi activat
Activați inversarea culorilor	Dacă este activat, va fi activat modul de afișare inversat
Activați funcția Assistive Touch	Dacă este activat, AssistiveTouch va fi activat
Activați selectarea vorbirii	Dacă este activată, va fi activată selecția de vorbire
Activați audio mono	Dacă este activat, va fi activat audio mono
VoiceOver	Dacă este activat, utilizatorul poate activa VoiceOver
Zoom	Dacă este activat, utilizatorul poate activa Zoom
Inversarea culorilor	Dacă este activat, utilizatorul poate activa culorile inversate
Atingere asistivă	Dacă este activat, utilizatorul poate activa atingerea asistivă

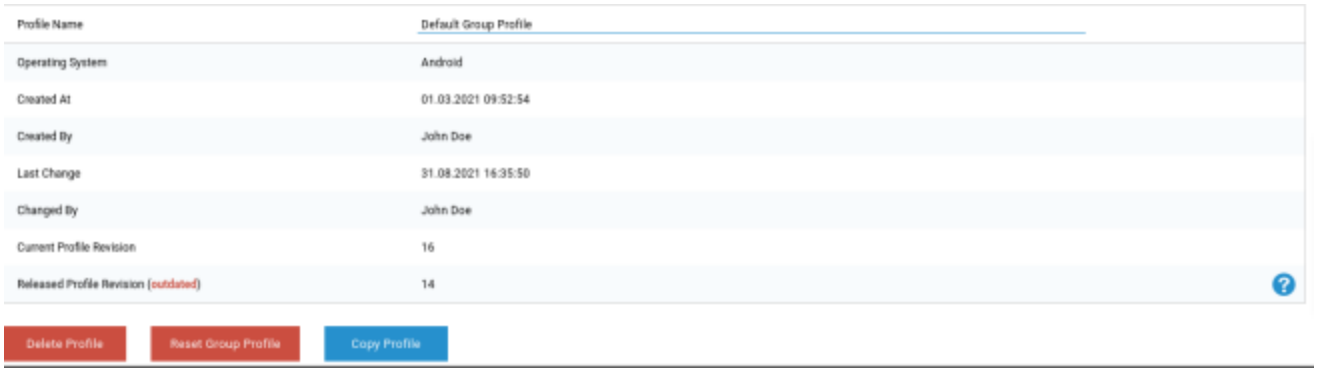
Android Enterprise – Configurare complet gestionată a dispozitivelor

În funcție de faptul dacă ați selectat în prezent un profil de grup sau un dispozitiv, prezentarea generală și subpunctele sale diferă - vă rugăm să luați în considerare acest lucru cu atenție!

Generalități

Prezentare generală a profilului grupului (numai la nivel de grup)

Atunci când deschideți un profil de grup, veți obține o prezentare generală rapidă a profilului.



Nume profil	Numele profilului (poate fi modificat aici)
Sistem de operare	Sistemul de operare pentru care este creat profilul
Creat la	Momentul creației
Creat de	Creatorul profilului
Ultima schimbare	Ora ultimei modificări a profilului
Schimbat de	Contul care a efectuat ultimele modificări
Revizuirea actuală a profilului	Revizuirea stării profilului salvat
Revizuire profil eliberată	Revizuirea profilului atribuit ("Atribuie acum"). Dacă eticheta afișează "(învechit)" în spatele textului, înseamnă că ați salvat profilul, dar nu l-ați atribuit încă, astfel încât dispozitivele vor primi în continuare o versiune mai veche.

Prezentare generală a dispozitivului (numai la nivel de dispozitiv)

Dacă vă aflați pe un dispozitiv, veți primi o recapitulare generală a dispozitivului selectat, care conține următoarele informații:

Numele dispozitivului	Numele dispozitivului
Locație	Coordonate locație
Număr de telefon	Număr de telefon
Aplicații obligatorii atribuite	Numărul de aplicații obligatorii alocate
Versiunea sistemului de operare	Versiunea sistemului de operare al dispozitivului
Sistem de operare	Sistem de operare (Android Enterprise)
Numărul de serie	Numărul de serie al dispozitivului
Proprietatea dispozitivului	Dispozitiv corporativ sau privat
Tip dispozitiv	Dispozitiv gestionat de AE Work
Înrădăcinat	Stare, indicând dacă dispozitivul a fost rădăcinat
Conform	În conformitate cu liniile directoare
Adresa IP	Adresa IP a dispozitivului
Văzut ultima dată	Momentul în care dispozitivul s-a conectat ultima dată la AppTec
Ultimul impuls	Momentul în care a fost trimis ultimul push către dispozitiv
AE Mod proprietar dispozitiv	Da
Atribuirea utilizatorului	Utilizatorul sau grupul căruia îi este atribuit acest dispozitiv

Revizuirea configurației (numai la nivel de dispozitiv)

Aici primiți o prezentare generală a profilului de grup care este atribuit dispozitivului.

Dacă faceți clic pe profilul grupului, veți obține acces direct la acest profil și veți putea efectua setările.

Cu acest simbol, puteți readuce aplicațiile distribuite la setările profilului de grup.

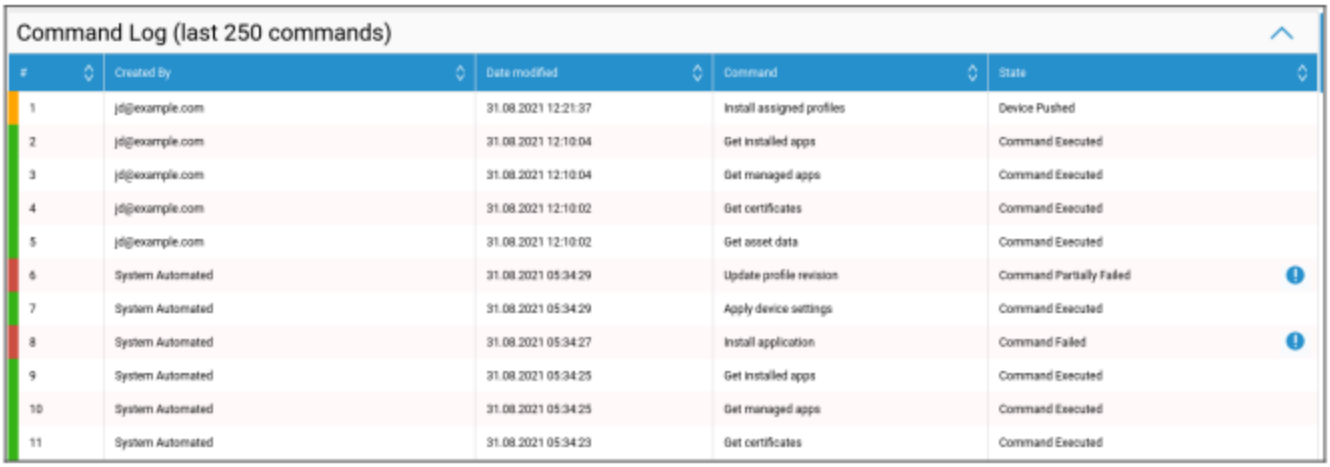
Cu acest simbol, puteți readuce toate aplicațiile utilizate la setările profilului de grup.

"Newer Revision available" indică faptul că profilul grupului a fost modificat și salvat, dar nu a fost atribuit. Profilul de grup trebuie să fie atribuit cu "Assign now" la nivel de grup pentru a aplica modificările dispozitivelor.

Jurnalul dispozitivului (numai la nivel de dispozitiv)

Jurnal de comandă

Aici puteți vedea ce comenzi au fost emise pentru dispozitiv și care este starea lor.



Comenzile create de "System Automated" sunt create automat de sistem.

Stări posibile ale comenzii

Dispozitiv împins	O solicitare push a fost trimisă către serviciul push (de exemplu, APNS) pentru a indica dispozitivului să se conecteze din nou la serverul EMM.
Comandă creată	Comanda a fost creată în sistem.
Comandă trimisă	Comanda a fost trimisă către dispozitiv după ce acesta s-a conectat la server.
Comandă executată	Comanda a fost executată cu succes.
Comandă eșuată	Comanda a eșuat. *
Comandă eșuată parțial	În funcție de sistemul de operare al dispozitivului, unele comenzi pot fi grupate împreună. În acest caz, unele părți ale acestui grup de comandă au eșuat. *
Comandă executată, eventual eșuată	Comanda a fost executată, dar poate că nu a fost.
Comanda Repushed	Comanda a fost respinsă de un utilizator.
Aruncată	Comanda a fost eliminată. De exemplu, pentru că a fost înlocuită de o altă comandă sau pentru că dispozitivul a fost înrolat din nou și comenzile vechi au fost eliminate

Dacă în spatele mesajului există un semn al exclamării, puteți obține mai multe informații dacă treceți cu cursorul peste pictogramă.

Setări dispozitiv

Configurare client

Aici puteți efectua următoarele configurații pe dispozitivul Android:

Timp de neconformitate	Limita de timp de răspuns a utilizatorului după care se aplică acțiunea de executare.
Acțiune de punere în aplicare după expirarea termenului de conformitate	Acțiune de punere în aplicare atunci când un utilizator nu efectuează acțiuni care conduc la un statut de dispozitiv conform
Frecvența colectării datelor	Frecvența cu care trebuie colectate informațiile despre dispozitiv/GPS
Frecvența bătăilor inimii dispozitivului	Intervalul în care dispozitivul trebuie să contacteze serverul AppTec360 Min. 1 minut Max. 24 de ore
Activați actualizările locației	Dacă este activat, dispozitivul trimite actualizări ale locației către serverul AppTec360
Locație Ora actualizării	Determină în ce intervale de timp dispozitivul trimite actualizări ale locației către AppTec360
Utilizați Google Location Accuracy pentru actualizarea locației	Dacă este activată, locația de rețea va fi utilizată pentru actualizările locației (dacă a fost dezactivată la "Restricții", atunci această setare nu va afecta nimic)
Utilizați locația GPS pentru actualizarea locației	Dacă este activat, GPS-ul va fi utilizat pentru actualizarea locației
Permiteți locații fictive (false)	Permite falsificarea informațiilor de localizare prin intermediul aplicațiilor terță parte
Acțiune de pierdere a conexiunii	Dacă este activat, puteți specifica o acțiune pentru cazul în care un dispozitiv nu se conectează la serverul MDM în intervalul de bătaie a inimii. De exemplu, dacă dispozitivul are un timp de bătaie a inimii de 5 minute, acesta se conectează la server la ora 10:35 AM. După aceea, dispozitivul părăsește raza Wi-Fi. Următorul heartbeat la ora 10:40 AM va eșua, iar acțiunea specificată va fi executată.
Acțiune	Acțiunea care trebuie întreprinsă imediat ce un dispozitiv devine neconform.

	• Dispozitiv de blocare = dispozitiv de blocare • Ștergere dispozitiv = dispozitivul va fi restaurat la setările din fabrică • Ștergere dispozitiv și card SD = dispozitivul va fi restaurat la setările din fabrică, iar spațiul de stocare de pe cardul SD va fi șters
Prag	Puteți specifica un prag de bătăi cardiace eșuate care sunt necesare pentru a declanșa acțiunea specificată.

Modul de aplicare a politicii	Implicit:	Utilizatorilor li se va solicita periodic să execute acțiunile restante
	Aplicare lenește a politicilor:	Utilizatorilor nu li se va solicita niciodată să execute acțiunile restante. Toate acțiunile deschise vor fi afișate în clientul AppTec360
	Aplicarea agresivă a politicilor:	Utilizatorilor li se va solicita neîncetat să execute acțiunile restante
Blocarea versiunii AppTec360	Dacă este activat, poate fi specificat un cod de versiune pentru clientul MDM AppTec360. Clientul AppTec360 se va actualiza numai la versiunea specificată. Versiunile mai noi vor fi ignorate. Un downgrade NU este posibil.	
Codul versiunii	Codul versiunii pentru clientul MDM AppTec360 care urmează să fie blocat.	
Dezactivați Notificarea AppTec360	Dacă este dezactivat, clientul AppTec360 nu va afișa o notificare în bara de notificări. Astfel, utilizatorii pot închide clientul AppTec360 prin intermediul managerului de activități. Dacă clientul AppTec360 este închis, mai multe caracteristici, inclusiv modul Kiosk și App Black/Whitelisting, nu vor funcționa corect. Dispozitivele Samsung oferă un mecanism de protecție pentru clientul AppTec360. Notificarea este dezactivată implicit pe dispozitivele Samsung care acceptă API-urile KNOX. Notificarea nu ar trebui să fie dezactivată pe dispozitivele cu Android 8.0 sau o versiune ulterioară.	

Wallpaper

Setați tapet personalizat	Activați/dezactivați imaginea de fundal personalizată
Wallpaper	Setați modul tapet pentru a utiliza un cod de culori sau o imagine
Specificați o culoare	Specificați o culoare de fundal ca valoare hexagonală, de exemplu #000000 pentru negru sau #ffffff pentru alb
Setați imaginea ca tapet	Încărcați fișierul imagine pe care doriți să îl utilizați ca tapet

Gestionarea activelor (numai la nivel de dispozitiv)

Informații despre dispozitiv

Model	Denumirea modelului dispozitivului
Sistem de operare	SO
Versiunea sistemului de operare	Versiunea sistemului de operare
Numărul de serie	Numărul de serie
Numele dispozitivului	Numele dispozitivului
Starea bateriei	Starea bateriei
Memorie liberă / totală	Memorie liberă / totală
Samsung Safe	Interfața Samsung SAFE, necesară pentru o varietate de opțiuni de setare
Card SD disponibil	Card SD disponibil
Card SD emulat	Card SD emulat
Card SD detașabil	Card SD detașabil
SD Memorie liberă / totală	SD Liber / Total memorie card SD

Wi-Fi

Adresa IP	Adresa IP a dispozitivului
WiFi MAC	Adresa MAC WiFi

Celulare

Statut	Stare (cartela SIM instalată)
Număr de telefon	Număr de telefon
Roaming (voce / date)	Roaming pentru voce / date
Starea de roaming	Starea curentă de roaming
Adresa IP	Adresa IP
Operator/Carrier	Operator/Carrier
Tehnologie celulară	Tehnologie celulară
IMEI	Numărul IMEI
ICCID	Acesta este ID-ul cartelei SIM, de multe ori și un Smartcard sau o cartelă cu circuit integrat (ICC)
IMSI	Identitatea internațională a abonatului mobil (IMSI) oferă în rețelele mobile GSM și UMTS o identificare definitivă a utilizatorilor rețelei IMSI este compus din maximum 15 cifre și este configurat în felul următor: • Codul țării mobile (MCC), 3 cifre • Codul rețelei mobile (MNC), 2 sau 3 cifre • Numărul de identificare a abonatului mobil (MSIN), 1-10 cifre
Actual MCC/MNC	Consultați "SIM MCC/MNC"
SIM MCC/MNC	Codul țării mobile este un identificator de țară stabilit de ITU conform standardului E.212. Acesta funcționează împreună cu codul rețelei mobile (MNC) pentru identificarea rețelei mobile. Înseamnă țara/codul rețelei mobile a cartelei SIM. Dacă vă deplasați într-o altă rețea mobilă, atunci, în mod logic, "MCC/MNC curent" și "SIM MCC/MNC" vor fi diferite.

Bluetooth

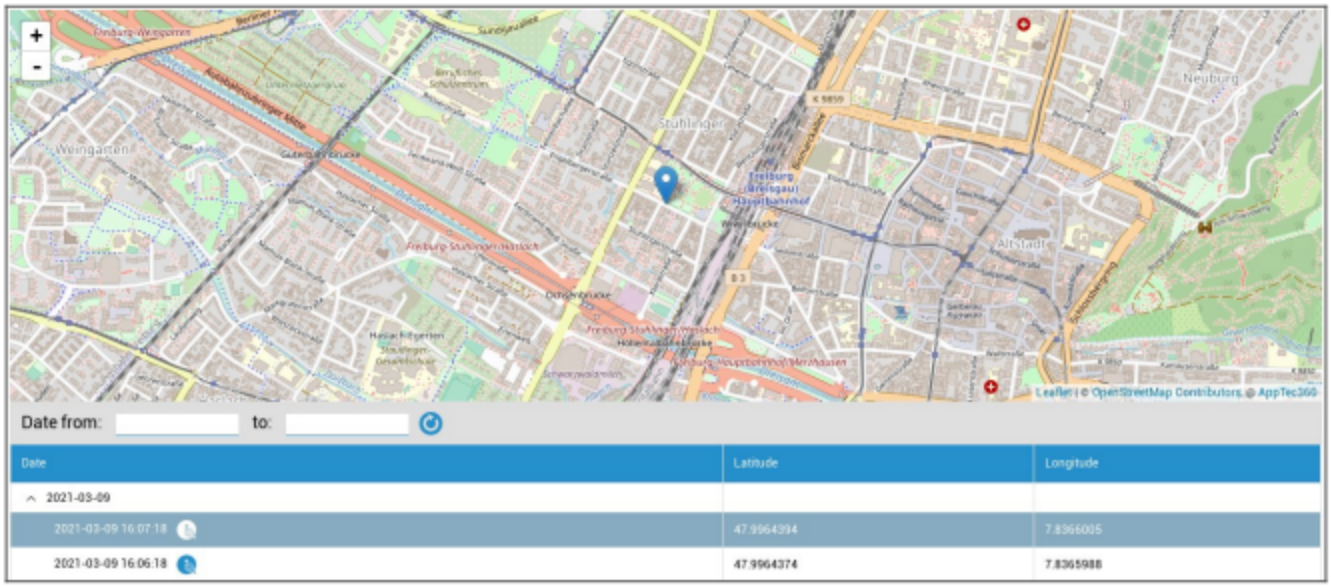
Bluetooth MAC	Adresa MAC Bluetooth

Managementul securității

Anti-furt (numai la nivel de dispozitiv)

Informații GPS (numai la nivelul dispozitivului)

Aici puteți stabili locația curentă/ultima a dispozitivului. Localizarea poate fi protejată cu una sau chiar două parole - Consultați: Setări generale - Confidențialitate - Acces GPS



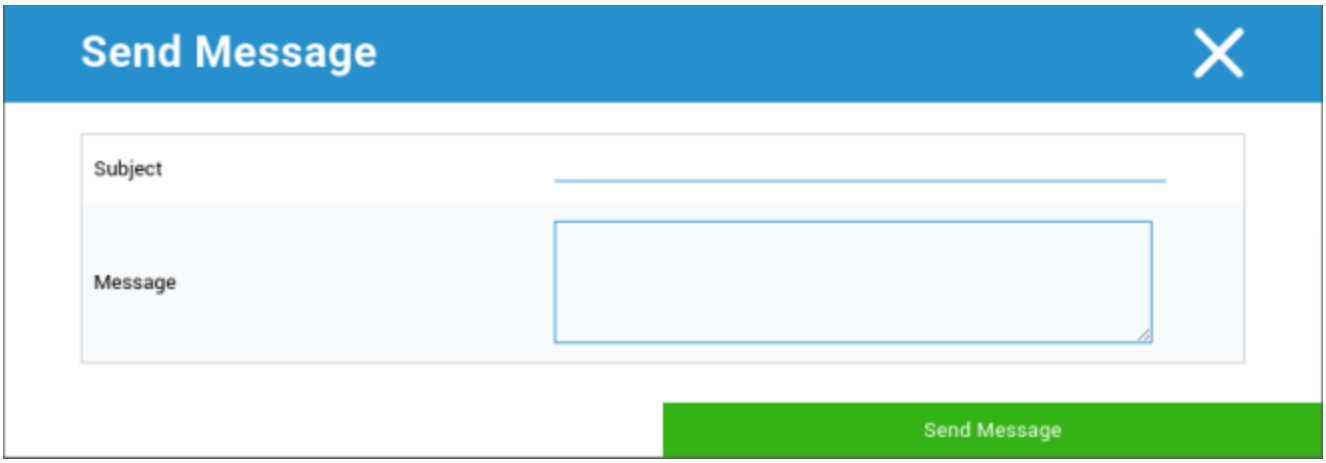
Ștergere și blocare (numai la nivel de dispozitiv)

Sub "Ștergere și blocare", puteți efectua următoarele trei acțiuni:

Ștergere completă	Dispozitivul este readus la setările din fabrică (datele corporative, precum și cele personale sunt șterse)
Ștergere Enterprise	Doar datele corporative sunt eliminate de pe dispozitivul utilizatorului final (toate aplicațiile, datele, etc. care au fost furnizate de AppTec360)
Ecran de blocare	Blocarea ecranului este activată, este suficient să deblocați dispozitivul cu ajutorul parolei dispozitivului/PIN

Mesaj (numai la nivel de dispozitiv)

Aici puteți completa subiectul și un mesaj și îl puteți trimite către un dispozitiv al utilizatorului final.



Configurația de securitate

Codul de acces al dispozitivului

Sub "Cod de acces" puteți trimite o parolă pentru dispozitiv, fiind disponibile următoarele opțiuni de setare

Lungimea minimă a parolei	Stabilește numărul minim de simboluri pe care trebuie să le aibă o parolă	
Calitatea parolei	Nespecificat	Această politică nu are cerințe privind parola.
	Biometric Slab	Această politică permite utilizarea tehnologiei de recunoaștere biometrică de securitate redusă. Aceasta implică tehnologii care pot recunoaște identitatea unei persoane până la un cod PIN de aproximativ 3 cifre (detectarea falsă este mai mică de 1 la 1 000).
	Ceva	Această politică necesită setarea unui anumit tip de parolă sau model, dar nu impune nicio regulă specifică.
	Alfabetic	Utilizatorul trebuie să fi introdus o parolă care să conțină cel puțin caractere alfabetice (sau alte simboluri).
	Alfanumeric	Utilizatorul trebuie să fi introdus o parolă care să conțină cel puțin caractere numerice și alfabetice (sau alte simboluri).
	Complex	Utilizatorul trebuie să fi introdus o parolă care să conțină cel puțin o literă, o cifră numerică și un simbol special, în mod implicit. Cu această calitate a parolei, parolele pot fi restricționate pentru a conține diferite seturi de caractere, cum ar fi cel puțin o literă mare, etc.
Lungimea minimă a parolei	Setați numărul necesar de caractere pentru parolă. De exemplu, puteți solicita ca PIN-ul sau parolele să aibă cel puțin șase caractere.	
Minimum de cifre numerice necesare în parolă	Minimum de cifre numerice necesare în parolă	
Minimum de litere minuscule necesare în parolă	Minimum de litere minuscule necesare în parolă	
Minimum de litere majuscule necesare în parolă	Minimum de litere majuscule necesare în parolă	

Numărul minim de caractere din afara literelor necesare în parolă	Numărul minim de caractere din afara literelor necesare în parolă
Simboluri minime necesare în parolă	Simboluri minime necesare în parolă

Timp maxim de inactivitate blocare	Inactivitatea maximă a utilizatorului până la blocarea timpului
Timpul de expirare a parolei	Se stabilește, interval de timp după care parola expiră și trebuie emisă o nouă parolă
Restricționarea istoricului parolelor	Numărul de parole utilizate anterior care nu sunt permise
Numărul maxim de încercări de parole eșuate	Stabilește de câte ori o parolă poate fi introdusă incorect, înainte de a se efectua o ștergere completă a dispozitivului
Permiteți autentificarea biometrică	Permite autentificarea prin scanarea amprentei sau a irisului. Numai pentru Samsung KNOX 2.1 și versiuni ulterioare

AntiVirus

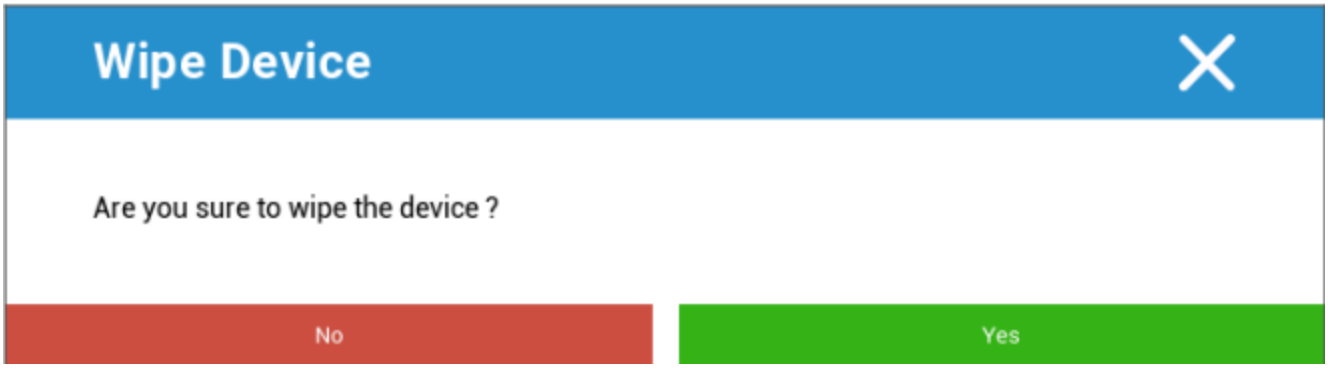
Scanare automată	Activați scanările automate periodice
Interval de scanare	Interval de examinare (rapid / complet)
Scanare automată completă	Activați scanările automate complete
Actualizări automate	Activați actualizările automate
Interval de verificare a actualizării	Cât de des trebuie actualizate aplicația și baza sa de date (viruși / cod deteriorat)
Protecția aplicațiilor	Activați scanarea automată a aplicațiilor
Protecția cardului SD	Activați scanarea automată a cardului SD
Actualizare numai Wi-Fi	Atunci când este activat, actualizările vor fi aplicate numai atunci când dispozitivul este conectat cu succes la o rețea Wi-Fi

Sfârșitul duratei de viață (numai la nivel de dispozitiv)

Ștergere (numai la nivel de dispozitiv)

Sub "Ștergere", puteți readuce dispozitivul la setările din fabrică. Aici, atât datele corporative, cât și cele private vor fi șterse de pe dispozitivul utilizatorului final.

La un clic pe "Simbolul minus" primiți următorul mesaj:



Cu "Da" puteți efectua ștergerea.

Sub "Raport ștergere" pot fi afișate următoarele elemente

Șters de	Istoricul persoanei care a efectuat ștergerea
Data	Data
Statut	Stare (de exemplu, dacă ștergerea a fost efectuată cu succes)

Setări de restricționare

Restricții

Aici, pot fi restricționate și blocate o varietate de lucruri.

Activați camera	Permiteți utilizarea camerei	
Forțați sincronizarea automată	Pe	Sincronizarea este activată permanent
	Oprit	Sincronizarea este dezactivată permanent
	Alegerea utilizatorului	Selectat de utilizator
Forța Bluetooth	Pe	Bluetooth este activat permanent
	Oprit	Bluetooth este dezactivat permanent
	Alegerea utilizatorului	Selectat de utilizator
Forța GPS	Pe	GPS-ul este activat permanent
	Oprit	GPS-ul este dezactivat permanent
	Alegerea utilizatorului	Selectat de utilizator
Localizarea rețelei Force	Pe	Internet-localizare permanentă
	Oprit	Dezactivarea permanentă a localizării pe internet
	Alegerea utilizatorului	Selectat de utilizator

Securitate		
Interziceți locația de partajare	Specifică dacă unui utilizator nu i se permite să activeze partajarea locației.	
Interziceți Safe Boot	Specifică dacă utilizatorului nu i se permite să repornească dispozitivul în modul de pornire sigură.	
Nu permite resetarea rețelei	Specifică dacă unui utilizator nu i se permite să reseteze setările de rețea din Setări.	
Nu permite resetarea din fabrică	Specifică dacă unui utilizator îi este interzisă resetarea dispozitivului.	
Activează ADB	Permite conectarea la un PC prin ADB	
Dezactivați cheia de protecție	Dezactivează Keyguard	
Proprietar dispozitiv Informații privind ecranul de blocare	Setează informațiile despre proprietarul dispozitivului care urmează să fie afișate pe ecranul de blocare.	
Aplicarea conformității	Mod Prompt Utilizator	Utilizatorul va fi rugat să efectueze acțiunile necesare.
	Modul Lock-Down Container	Ascundeți toate aplicațiile până când toate cerințele sunt îndeplinite

Gestionarea aplicațiilor	
Permiteți legarea aplicațiilor între profiluri	Permite aplicațiilor din profilul părinte să gestioneze linkurile web din profilul gestionat.
Interziceți controlul aplicațiilor	Specifică dacă unui utilizator nu i se permite să modifice aplicații în Setări sau lansatoare.
Interziceți instalarea aplicației	Specifică dacă unui utilizator îi este interzisă instalarea de aplicații.
Interziceți dezinstalarea aplicațiilor	Specifică dacă unui utilizator nu i se permite să dezinstaleze aplicații.
Politica de autorizare în timpul rulării	Specifică modul în care vor fi gestionate noile cereri de permisiune din partea aplicațiilor.
Permiteți surse necunoscute	Dacă este activată, utilizatorii pot încărca aplicații prin instalarea unui fișier .apk.

Conectivitate	
Interziceți configurarea rețelei mobile	Specifică dacă unui utilizator îi este interzisă configurarea rețelelor mobile.
Interziceți configurația Tethering	Specifică dacă unui utilizator nu i se permite să configureze Tethering și hotspoturi portabile.
Interziceți configurația VPN	Specifică dacă unui utilizator îi este interzisă configurarea unui VPN.
Interziceți configurarea Wifi	Specifică dacă unui utilizator nu i se permite să schimbe punctele de acces WiFi.
Interzice ieșirea fasciculului NFC	Specifică dacă utilizatorului nu i se permite să utilizeze NFC pentru a transmite date din aplicații.
Blocare configurare WiFi	Această setare controlează dacă configurațiile WiFi create de o aplicație a proprietarului dispozitivului ar trebui să fie blocate (adică să fie editabile sau detașabile numai de aplicația proprietarului dispozitivului, nu și de aplicația Setări).
Activarea roamingului de date	Activează roamingul de date

Bluetooth	
Interziceți Bluetooth	Specifică dacă bluetooth nu este permis pe dispozitiv. Necesită Android 8.0
Interziceți partajarea Bluetooth	Specifică dacă partajarea bluetooth de ieșire nu este permisă pe dispozitiv. Necesită Android 8.0
Interziceți configurarea Bluetooth	Specifică dacă unui utilizator îi este interzisă configurarea bluetooth.

Gestionarea conturilor	
Interzice adăugarea profilului gestionat	Specifică dacă unui utilizator nu i se permite să adauge profiluri gestionate. Necesită Android 8.0
Interzicerea adăugării de utilizatori	Specifică dacă unui utilizator îi este interzis să adauge noi utilizatori.
Interziceți eliminarea profilului gestionat	Specifică dacă profilurile gestionate ale acestui utilizator pot fi eliminate, altfel decât de către proprietarul profilului său. Necesită Android 8.0
Interzicerea modificării contului	Specifică dacă unui utilizator îi este interzis să adauge și să elimine conturi, cu excepția cazului în care acestea sunt adăugate programatic de Authenticator.

Telefonie	
Interzicerea apelurilor de ieșire	Specifică faptul că utilizatorului nu i se permite să efectueze apeluri telefonice externe.
Interzicere SMS	Specifică faptul că utilizatorului nu i se permite să trimită sau să primească mesaje SMS.

Sistemul	
Interzicerea creării ferestrelor	Specifică că ferestrele în afară de ferestrele aplicației nu trebuie create.
Interzicerea setului User Icon	Specifică dacă unui utilizator nu i se permite să își schimbe pictograma.
Interziceți Set Wallpaper	Restricție utilizator pentru a nu permite setarea unui tapet de fundal.
Dezactivați bara de stare	Dezactivarea barei de stare blochează notificările, setările rapide și alte suprapuneri de ecran care permit evadarea de pe un dispozitiv de unică folosință.
Activați timpul automat	Setează automat ora.
Activați fusul orar automat	Setează automat fusul orar.
Rămâne pornit în timp ce este conectat la priză	Dispozitivul va rămâne activ în timp ce este conectat la o sursă de alimentare.

Depozitare	
Interziceți dezactivarea verificării aplicației	Specifică dacă unui utilizator nu i se permite să dezactiveze verificarea aplicațiilor.
Interziceți montarea suporturilor fizice	Specifică dacă unui utilizator nu i se permite să monteze suporturi externe fizice.
Activați serviciul de backup	Serviciul de backup gestionează toate mecanismele de backup și restaurare de pe dispozitiv. Dacă setați acest lucru la fals, datele nu vor mai putea fi salvate sau restaurate. Serviciul de backup este dezactivat în mod implicit. Necesită Android 8.0
Activare stocare în masă USB	Permite utilizarea USB Mass Storage.

Tastatură	
Interziceți completarea automată	Specifică dacă unui utilizator nu i se permite să utilizeze serviciile de completare automată. Necesită Android 8.0
Interzicerea copierii și lipirii între profiluri	Specifică dacă ceea ce este copiat în clipboard-ul acestui profil poate fi lipit în profilurile conexe.

Sunet	
Neadmiterea ajustării volumului	Specifică dacă unui utilizator îi este interzisă ajustarea volumului principal.
Dezactivare Dezactivare microfon	Specifică dacă unui utilizator nu i se permite să regleze volumul microfonului.
Dispozitiv mut	Dispozitiv mut.

Managementul certificatelor

Aici puteți distribui certificate de încredere și certificate de identitate dispozitivelor dvs.

Android 8 sau superior este necesar pentru a distribui certificate de încredere, iar Android 9 sau superior este necesar pentru a distribui certificate de identitate.

Cu "+" puteți adăuga mai multe certificate.

Certificatele de încredere trebuie să fie în format PEM.

Certificatele de identitate trebuie să fie în format PKCS12

Gestionarea conexiunilor

Wifi

Pentru această setare, efectuați preconfigurarea dispozitivelor utilizatorului final, pentru accesul la punctele interne Access

Identificatorul setului de servicii (SSID)	SSID pentru rețeaua care urmează să fie conectată
Rețea ascunsă	Activare, în cazul în care AP nu transmite SSID-ul

Tip de securitate

Stabilirea tipului de securitate al AP

WEP

Parolă	Parolă pentru AP

WPA/WPA2

Parolă	Parolă pentru AP

802.1x EAP

Metoda EAP

PWD	Identitate	Identitate
	Parolă	Parolă

PEAP	Protocolul de autentificare faza 2	niciunul	Fără protocol suplimentar
		MSCHAPV2	Protocolul MSCHAPV2
		GTC	Protocolul GTC
	Certificat CA	Certificat CA	
	Identitate	Identitate	
	Identitate anonimă	Identitate anonimă	
	Parolă	Parolă	

TTLS	Protocolul de autentificare faza 2	niciunul	Fără protocol suplimentar
		PAP	Protocolul PAP
		MSCHAP	Protocolul MSCHAP
		MSCHAPV2	Protocolul MSCHAPV2
		GTC	Protocolul GTC
	Certificat CA	Certificat CA	
	Identitate	Identitate	
	Identitate anonimă	Identitate anonimă	
	Parolă	Parolă	

TLS	Certificat CA	Certificat CA
	Identitate	Identitate
	Parolă	Parolă

VPN

Nume conexiune	Numele conexiunii VPN

Tip VPN

VPN

Client VPN

Client VPN AppTec360	
Configurarea gateway-ului	Selectați configurația Gateway VPN (consultați **Setări generale > Gateway universal > Setări VPN**)
VPN Always On	Activați blocarea nativă
Activați Lockdown AppTec360	Activați Lockdown AppTec360

Integrat (disponibil numai pe dispozitivele Samsung)			
Tip de conexiune	PPTP	Server	Server
		Activați criptarea PPTP	Activați criptarea PPTP
	L2TP / IPSec PSK	Server	Server
		Cheie IPSec precompartimentată	Cheie IPSec precompartimentată
		Activați L2TP Secret	Activați L2TP Secret
		Secret L2TP	Secret L2TP
	IPSec XAuth PSK	Server	Server
		Identificator IPSec	Identificator IPSec
		Cheie IPSec precompartimentată	Cheie IPSec precompartimentată
DNS Căutare Domenii	DNS Căutare Domenii		
Setări expert	Servere DNS	Servere DNS	
	Redirecționarea rutelor	Redirecționarea rutelor	

VPN deschis		
Server	Server	
Profil OpenVPN	Profil OpenVPN	
Aplicație OpenVPN	OpenVPN pentru Android (recomandat)	
	Conectare OpenVPN	
Setări expert	Servere DNS	Servere DNS
	Redirecționarea rutelor	Redirecționarea rutelor

Samsung / Lebădă puternică			
Tip de conexiune	PPTP	Server	Server
		Nume utilizator	Nume utilizator
		Parolă	Parolă
		Activați criptarea PPTP	Activați criptarea PPTP
	L2TP / IPSec PSK	Server	Server
		Cheie IPSec precompartimentată	Cheie IPSec precompartimentată
		Nume utilizator	Nume utilizator
		Parolă	Parolă
		Activați L2TP Secret	Secret L2TP
	IPSec XAuth PSK	Server	Server
		Identificator IPSec	Identificator IPSec
		Cheie IPSec precompartimentată	Cheie IPSec precompartimentată
		Nume utilizator	Nume utilizator
		Parolă	Parolă
Setări expert	Servere DNS	Servere DNS	
	Redirecționarea rutelor	Redirecționarea rutelor	

Cisco Any Connect		
Server	Server	
Mod certificat	Dezactivat	Dezactivat
	Automată	Automată
Setări expert	Servere DNS	Servere DNS
	Redirecționarea rutelor	Redirecționarea rutelor

VPN per aplicație

Client VPN

Client VPN AppTec360		
Configurarea gateway-ului	Selectați configurația Gateway VPN (consultați **Setări generale > Gateway universal > Setări VPN**)	
Aplicații VPN	Aplicații VPN	
VPN Always On	Activați blocarea nativă	VPN Always On
Activați Lockdown AppTec360	Activați Lockdown AppTec360	

Samsung / Lebădă puternică			
Tip de conexiune	PPTP	Server	Server
		Aplicații VPN	Aplicații VPN
		Nume utilizator	Nume utilizator
		Parolă	Parolă
		Activați criptarea PPTP	Activați criptarea PPTP
	L2TP / IPSec PSK	Server	Server
		Aplicații VPN	Aplicații VPN
		Cheie IPSec precompartimentată	Cheie IPSec precompartimentată
		Nume utilizator	Nume utilizator
		Parolă	Parolă
		Activați L2TP Secret	Secret L2TP
	IPSec XAuth PSK	Server	Server
		Aplicații VPN	Aplicații VPN
		Identificator IPSec	Identificator IPSec
		Cheie IPSec precompartimentată	Cheie IPSec precompartimentată
		Nume utilizator	Nume utilizator
		Parolă	Parolă
Setări expert	Servere DNS	Servere DNS	
	Redirecționarea rutelor	Redirecționarea rutelor	

Restricții

Aici puteți seta restricțiile legate de gestionarea conexiunilor.

Permiteți roamingul de date	Permiteți datele mobile în roaming
Forțați roamingul de date	Dacă este activat, roamingul pentru date mobile este activat permanent (nu este recomandat!) Această setare suprascrie setarea "Allow Data Roaming"!
Următoarele setări sunt disponibile numai pe SAFE 2.x sau o versiune superioară	
Permiteți numai apelurile de urgență	Permiteți numai apelurile de urgență
Permiteți WiFi	Permiteți WiFi
Nivelul minim de securitate al rețelei WiFi	Nivelul minim de securitate al rețelei WiFi Deschis = toate tipurile de WiFi sunt permise
Interziceți utilizatorului să adauge rețele WiFi	Utilizatorul nu poate adăuga singur o rețea WiFi Această setare este posibilă numai dacă a fost definit un profil WiFi în "Gestionarea conexiunii"
Permiteți SMS & MMS	Toate = Tot traficul SMS și MMS este permis Incoming SMS Only = Sunt permise numai mesajele SMS primite Outgoing SMS Only = Sunt permise numai mesajele SMS de ieșire Niciunul = Nu este permis traficul SMS / MMS
Permiteți sincronizarea în timpul roaming-ului	Permiteți sincronizarea în timpul roaming-ului Pornit = activat Oprit = dezactivat Alegerea utilizatorului = alegerea utilizatorului
Permiteți roamingul vocal	Permiteți roamingul vocal Pornit = activat Oprit = dezactivat Alegerea utilizatorului = alegerea utilizatorului
Utilizați serverul proxy http al sistemului	Utilizarea unui server proxy HTTP, care este furnizat de setările sistemului în setări, depinde de rețeaua conectată (WiFi sau APN)

Gestionarea PIM

Gmail Exchange

Info: Această configurare va fi aplicată aplicației Gmail. Deci trebuie să aprobați și să instalați Gmail.

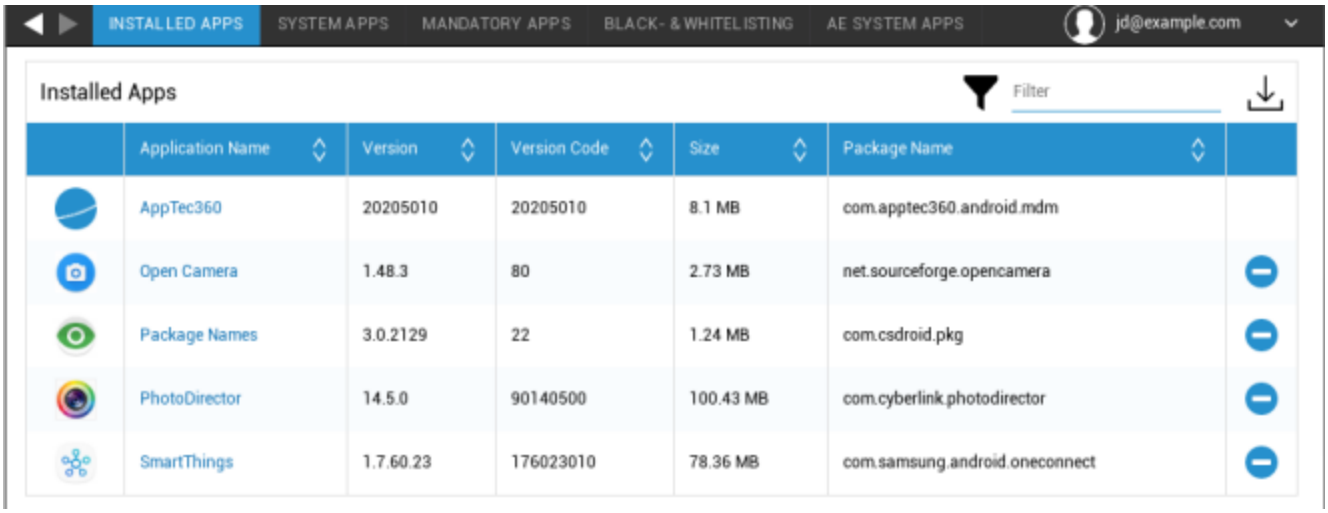
Adresa eMail	Adresa de e-mail a utilizatorului furnizat Vă rugăm să rețineți "Placeholders", pe care le puteți utiliza pentru a lucra cu acreditările și nu efectuați modificări manual pe fiecare dispozitiv Cu un clic pe le puteți afișa pentru tine
Nume gazdă server	Adresa de server a serverelor Exchange
Nume de utilizator	Numele de autentificare pentru dispozitivul respectiv al utilizatorului final, vă rugăm să rețineți și "Placeholders here
Semnătura	Se poate atașa o semnătură (Indicație: Unele dispozitive necesită formatare HTML pentru semnătură)
Numărul de zile anterioare pentru sincronizare	Numărul de zile, care determină momentul în care e-mailurile sunt sincronizate înapoi
Identificatorul dispozitivului	Ein String der die EAS DeviceID enthält. Dies ist Teil des EAS Protokols und wird in einigen Umgebungen benötigt
Utilizați Secure Sockets Layer (SSL)	Utilizați o conexiune SSL
Acceptați toate certificatele	Toate certificatele sunt acceptate. Vă rugăm să selectați această opțiune, dacă Exchange Server utilizează un certificat auto-semnat

Gestionarea aplicațiilor

Enterprise App Manager

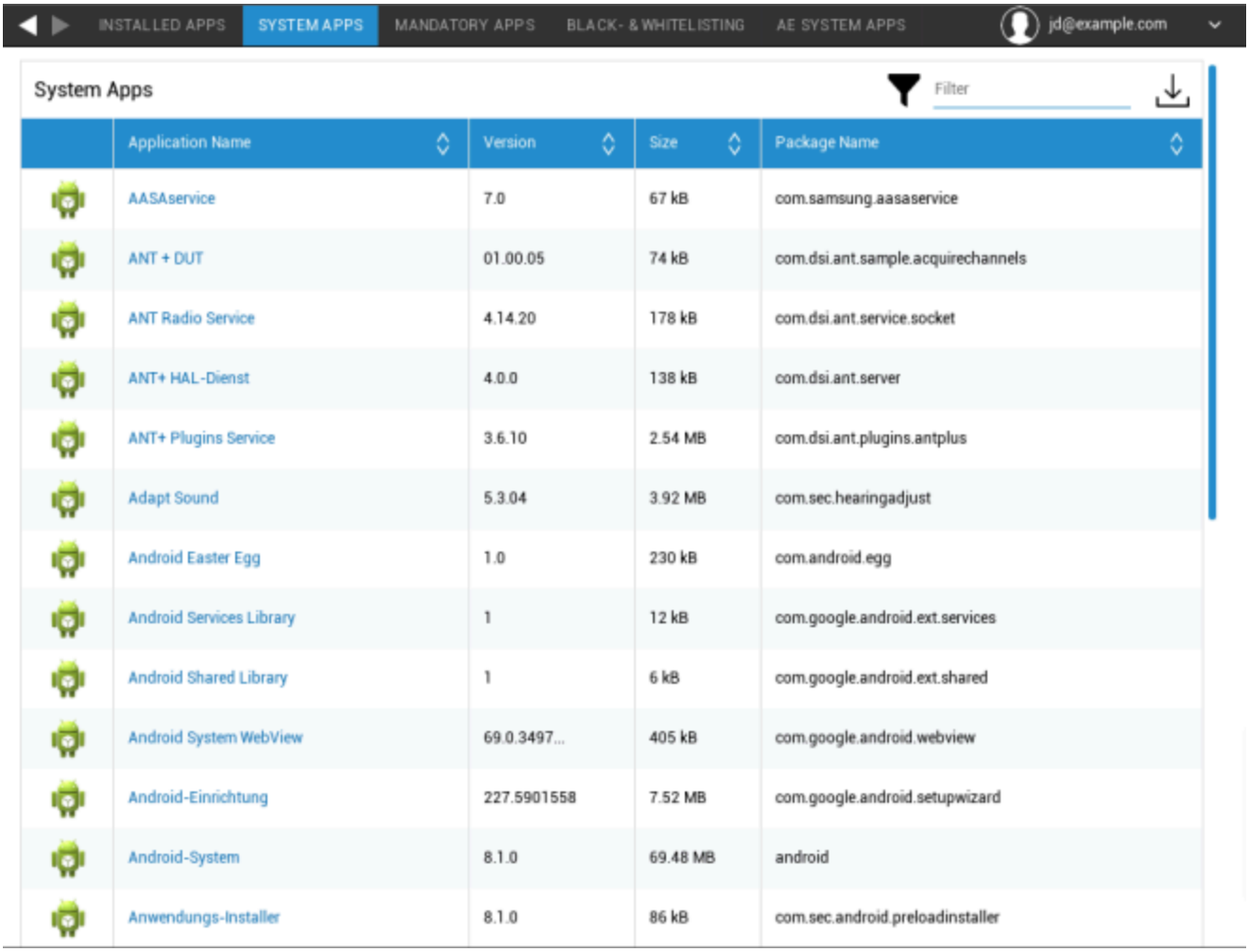
Aplicații instalate (numai la nivel de dispozitiv)

Aici vor fi afișate toate aplicațiile care sunt instalate în prezent pe dispozitivul utilizatorului final.



Aplicații de sistem (numai la nivel de dispozitiv)

Sub "Aplicații de sistem", toate aplicațiile și serviciile care au fost deja instalate pe dispozitivul utilizatorului final de către producătorul dispozitivului vor fi listate pentru dvs.

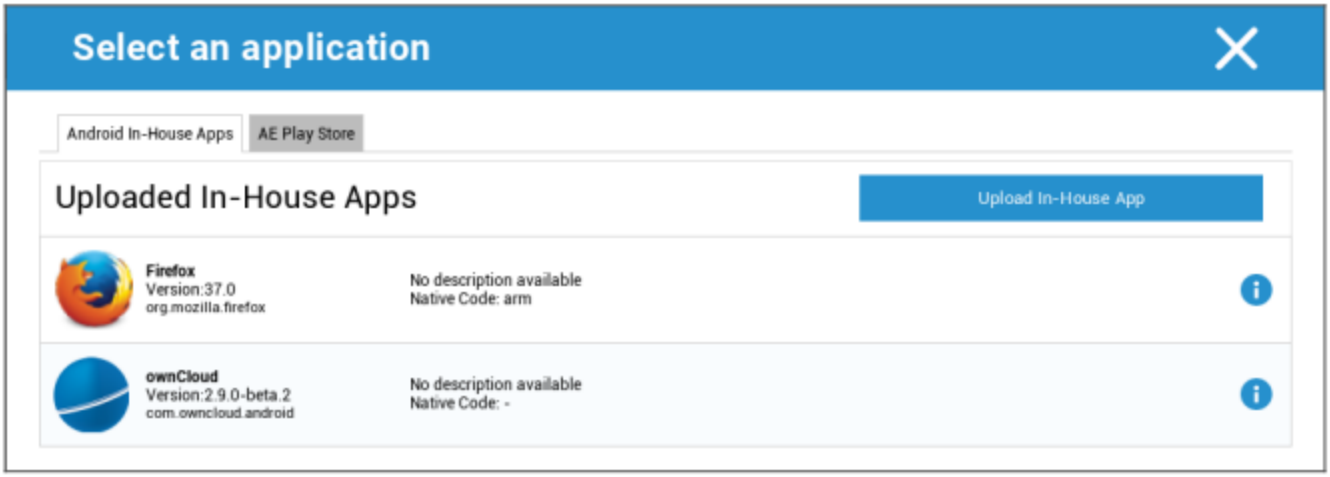


Aplicații obligatorii

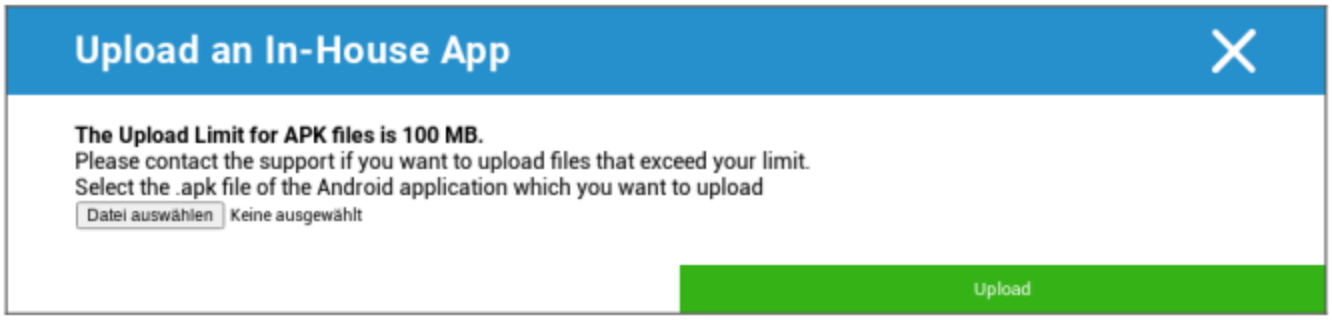
Sub Aplicații obligatorii, puteți stabili aplicațiile obligatorii obligatorii. Utilizatorului i se va solicita în permanență să instaleze această aplicație desemnată.

Prin intermediul , poate fi definită aplicația obligatorie obligatorie.

Aceasta poate fi o aplicație internă din "Aplicații interne Android", pe care ați încărcat-o în Setări generale.

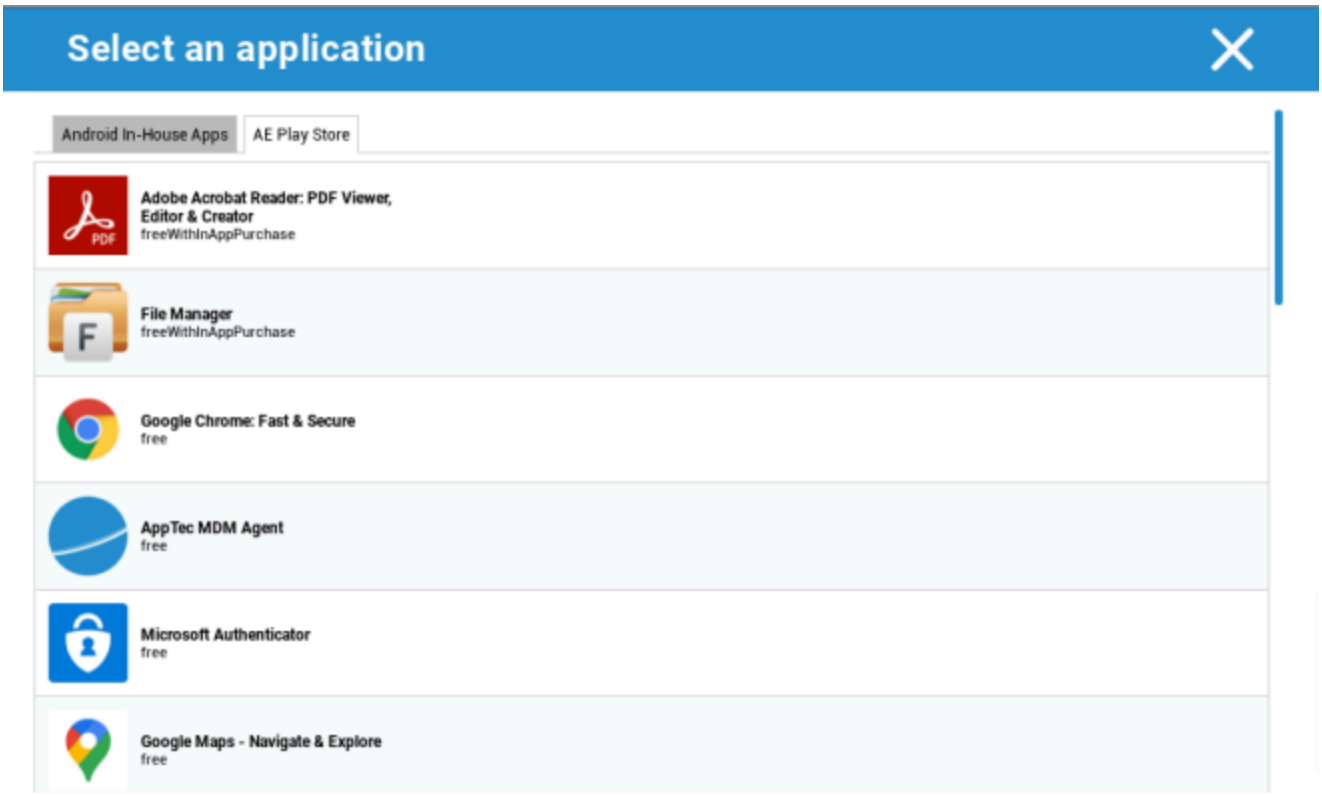


De asemenea, puteți selecta și încărca direct un fișier apk cu "Încărcare aplicație internă".



Dacă instalați o aplicație In-House, veți avea posibilitatea de a activa "Păstrați la zi". Dacă aceasta este activată și ați definit o versiune mai nouă în baza de date a aplicației In-House, aplicația va fi actualizată pe dispozitiv.

Sau poate fi o aplicație "AE Play Store" din Google Work Play Store.



Doar "AE Play Store Apps" aprobate vor fi afișate în această filă.

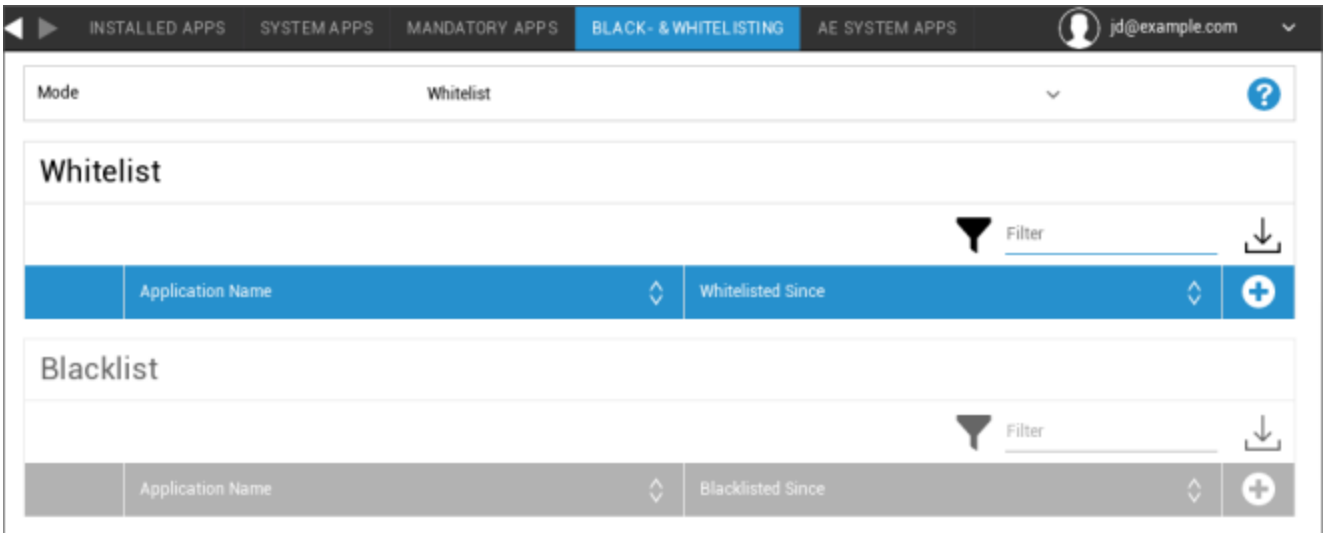
Pentru a aproba o "AE Play Store App", accesați "Setări generale" > "Administrare aplicații" > "AE Play

Store" și adăugați o aplicație prin intermediul butonului care vă va redirecționa către fila "Play Store Apps" (sau
puteți merge direct la fila "Play Store Apps").

În fila "Play Store Apps" puteți căuta aplicații. Când faceți clic pe o aplicație, se deschide pagina aplicației
și aici puteți aproba aplicația făcând clic pe "Aprobă".

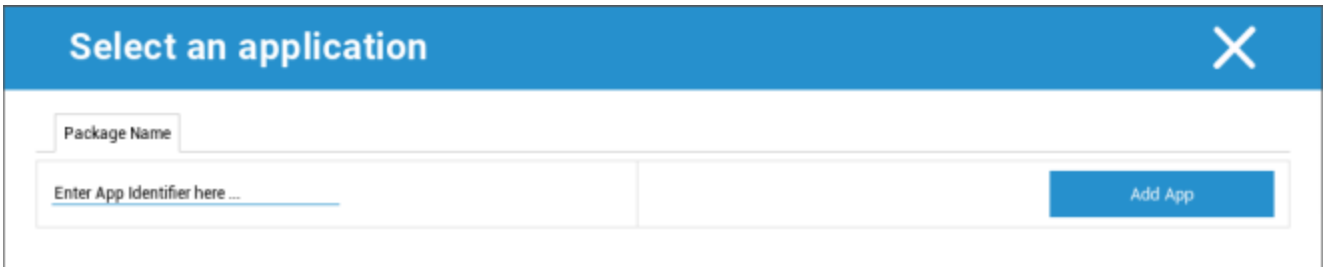
Lista neagră și lista albă

Sub "Listă albă și neagră", puteți alege între modul "Listă albă" și modul "Listă neagră".



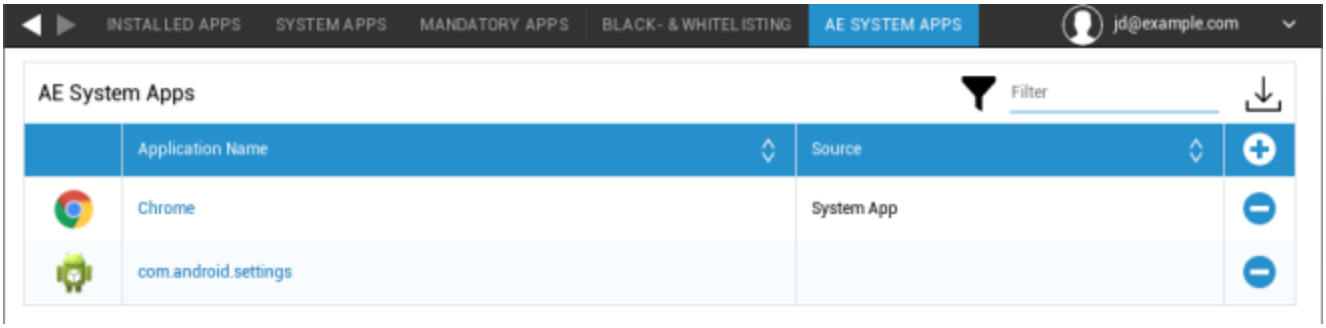
Lista albă	Numai aplicațiile și serviciile care sunt adăugate la listă pot fi instalate pe dispozitivul utilizatorului final. Dacă acestea sunt deja preinstalate pe dispozitivul utilizatorului final, ele vor fi activate și setate, astfel încât utilizatorul să le poată rula.
	Toate celelalte aplicații care nu sunt adăugate la listă nu pot fi instalate pe dispozitivul utilizatorului final. Dacă acestea sunt deja preinstalate pe dispozitivul utilizatorului final, ele vor fi dezactivate și setate, astfel încât utilizatorul să nu le poată rula.
Lista neagră	Aplicațiile și serviciile care sunt adăugate la listă nu pot fi instalate pe dispozitivul utilizatorului final. Dacă acestea sunt deja preinstalate pe dispozitivul utilizatorului final, ele vor fi dezactivate și setate astfel încât utilizatorul să nu le poată rula.
	Toate celelalte aplicații care nu sunt adăugate la listă pot fi instalate pe dispozitivul utilizatorului final. Dacă acestea sunt deja preinstalate pe dispozitivul utilizatorului final, ele vor fi activate și setate, astfel încât utilizatorul să le poată rula.

Prin , adăugați aplicații sau servicii suplimentare la lista utilizată în prezent.
Prin , adăugați aplicații sau servicii suplimentare la lista inactivă în prezent.
Puteți defini un "Packagename":

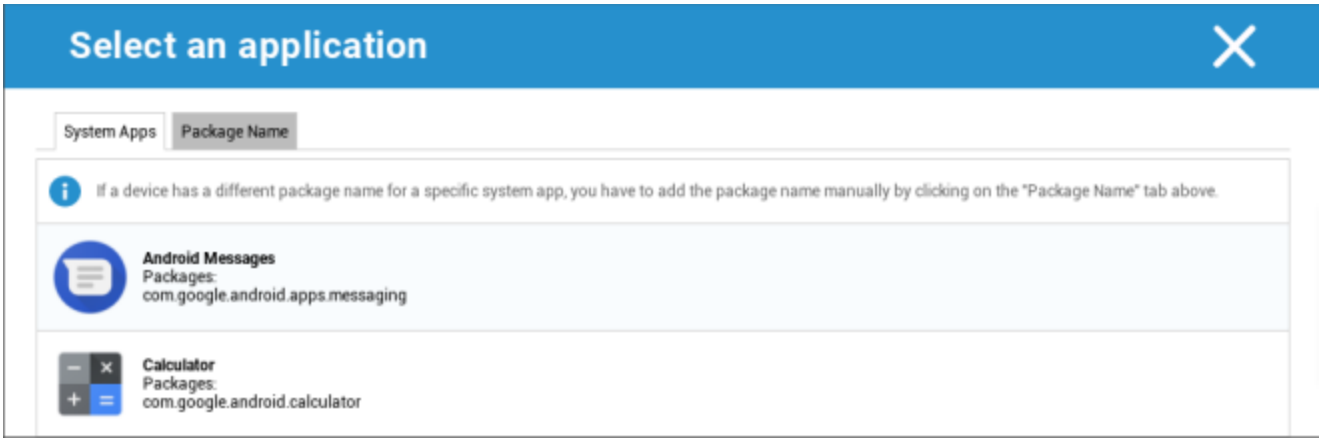

Select an application
Package Name
Enter App Identifier here ...
Add App

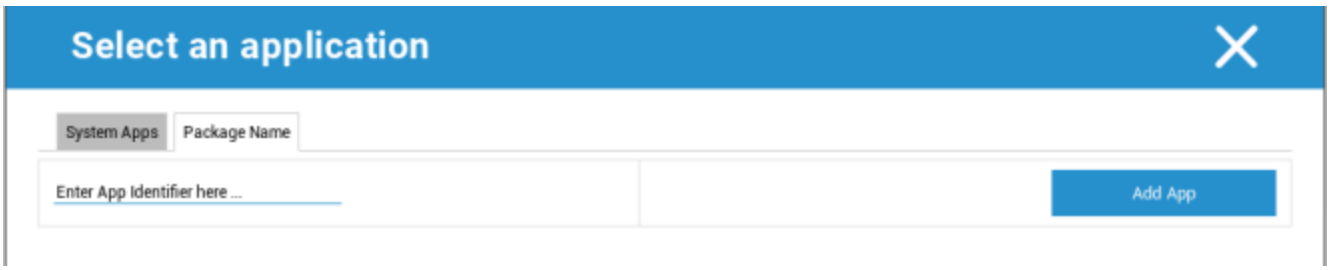
Aplicații de sistem AE

Aici puteți defini o listă care conține aplicații de sistem specifice care ar trebui să fie activate pe dispozitive.



Dacă faceți clic pe buton, puteți alege dintr-o listă de aplicații de sistem posibile furnizate de Google sau puteți introduce direct numele pachetului unei aplicații de sistem care trebuie activată.





Vă rugăm să rețineți că aplicațiile de sistem din lista furnizată de Google sunt doar aplicații care pot fi aplicații de sistem, dar nu trebuie neapărat să fie aplicații de sistem pe dispozitivele dvs.

Cu toate acestea, această listă afectează numai aplicațiile care sunt deja preinstalate.

Adăugarea de aplicații care nu sunt preinstalate pe dispozitivele dvs. nu va afecta dispozitivele, indiferent dacă aplicația este din lista furnizată de Google sau dacă numele pachetului de aplicații este introdus direct.

Restricții și setări

Setări de gestionare a aplicațiilor

Aici puteți configura comportamentul dispozitivului în ceea ce privește actualizările aplicațiilor.

Frecvența verificărilor de actualizare	Specificați intervalul în care clientul AppTec360 va căuta actualizări pentru aplicații. Valoarea implicită este de 24 de ore.
Prag Wi-Fi	Aplicațiile care sunt mai mari decât dimensiunea specificată vor fi descărcate prin Wi-Fi. Dacă este selectat "Doar Wi-Fi", toate aplicațiile vor fi descărcate prin Wi-Fi.

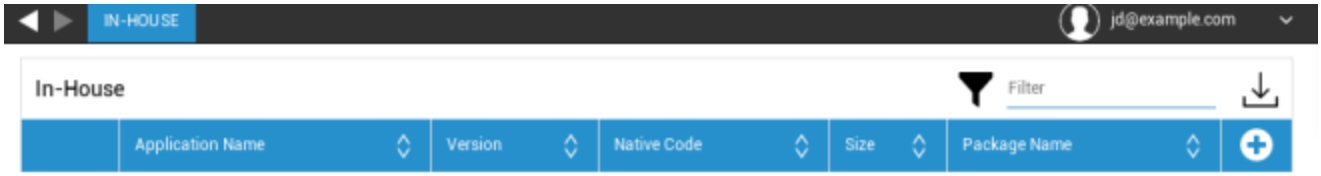
Magazin de aplicații pentru întreprinderi

In-House

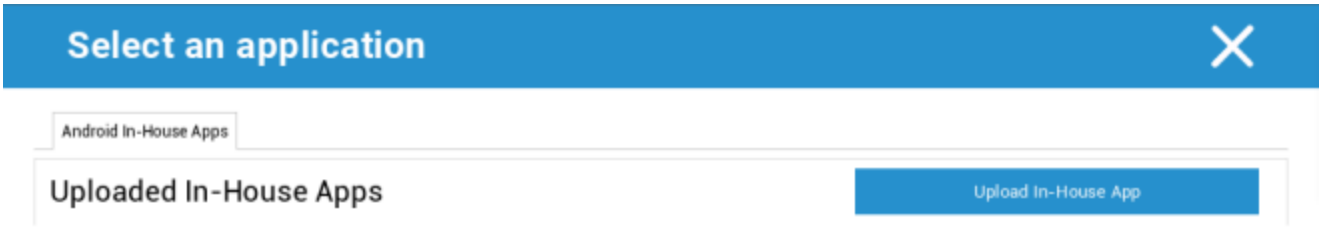
Sub punctul "In-House", puteți încărca și distribui aplicații dezvoltate intern.

Cu ajutorul simbolului, puteți distribui aplicații In-House suplimentare.

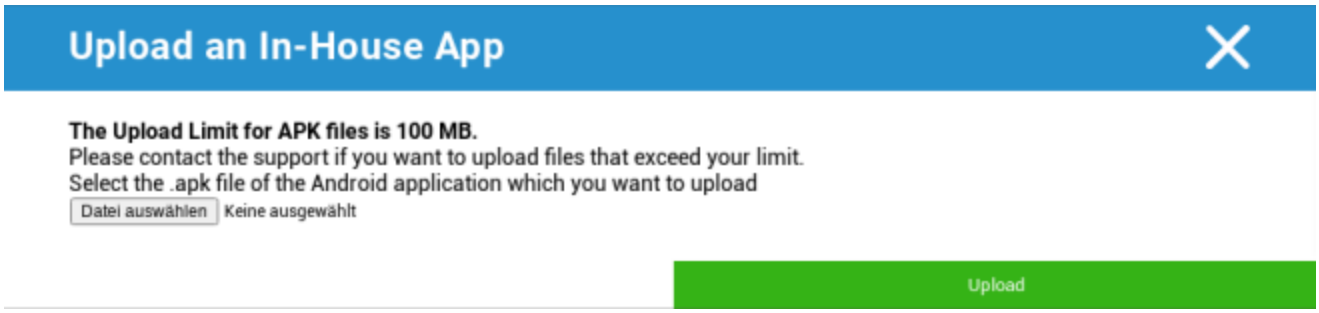
Dacă instalați o aplicație In-House, veți avea posibilitatea de a activa opțiunea "Keep up to date". Dacă
această opțiune este activată și ați definit o versiune mai nouă în In-House App DB, aplicația va fi actualizată pe dispozitiv.



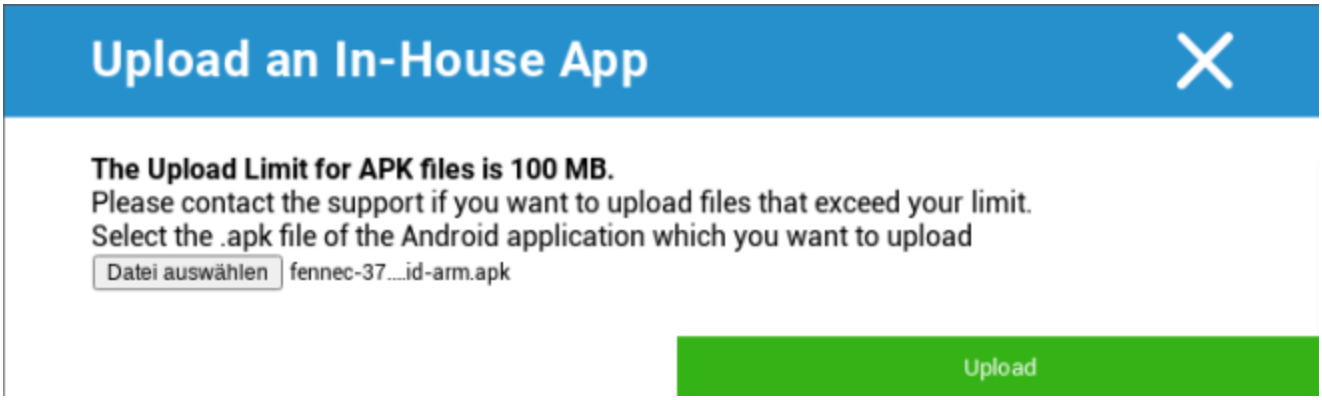
Dacă nu ați distribuit aplicații In-House, veți primi următoarea prezentare generală:



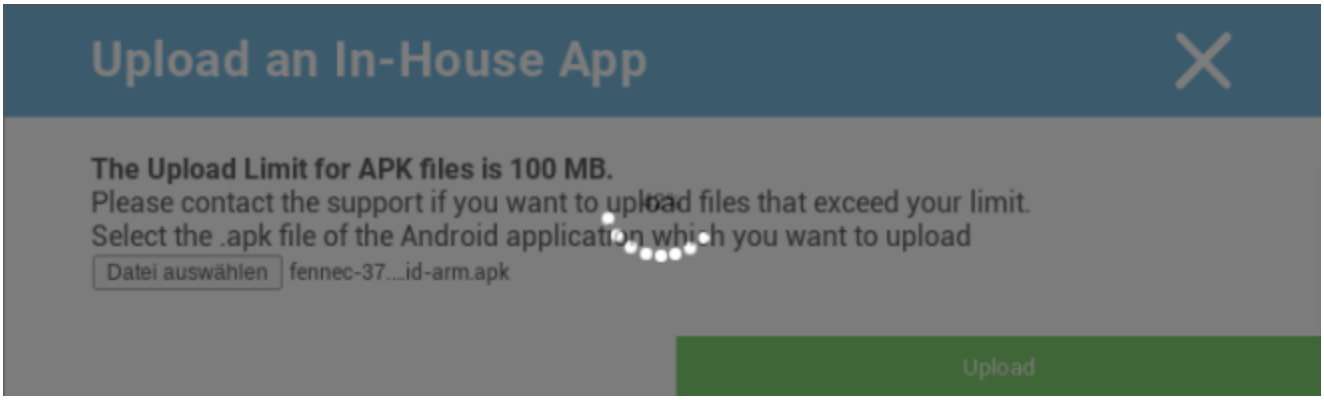
Pentru aceasta, faceți clic pe "Upload In-House App", apoi veți primi următoarea prezentare generală:



Acum, alegeți cu "Căutare..." un fișier .apk și apoi faceți clic pe "Încărcare".



Aplicația dvs. va fi acum încărcată, în mijlocul cercului veți vedea un indicator procentual, care arată cât de mult din aplicația dvs. a fost deja încărcată.



În cazul în care încărcarea aplicației dvs. In-House a avut succes, puteți găsi aplicația încărcată în Catalogul dvs. de aplicații.

Utilizatorul are acum opțiunea de a vedea și instala această aplicație în AppTec360 Store pe dispozitivul utilizatorului final
, la categoria "In-House".

Datorită faptului că aceasta nu implică o aplicație Google PlayStore, utilizatorul nu are nevoie de un ID Google
stocat pe dispozitivul utilizatorului final respectiv.

Magazin Play pentru întreprinderi

AE Magazin Play

Aici puteți adăuga aplicații la Android Enterprise Playstore. Vă rugăm să rețineți că trebuie să aprobați aplicațiile
cu contul dvs. de administrator AE înainte de a le putea adăuga.

Pentru aprobarea unei aplicații, vă rugăm să consultați instrucțiunile din Aplicații obligatorii.

Mod chioșc și lansator

Modul Kiosk

Modul Kiosk vă permite să predefiniți o aplicație sau un URL. Apoi va fi exclusiv posibil să rulați/vizitați această aplicație sau URL.

De asemenea, diverse butoane hardware pot fi dezactivate în diverse moduri Kiosk.

Start automat	Pornește automat modul Kiosk, de îndată ce profilul ajunge pe dispozitivul utilizatorului final
Modul Kiosk programat?	Puteți planifica o oră pentru modul Kiosk, care va începe și se va încheia automat, la ora stabilită de dvs.
Ora de începere	Ora de începere
Timp în minute	Timp în minute, după care modul Kiosk ar trebui să se încheie din nou

Tip de aplicație

Aplicație unică	Dacă doriți să porniți aplicația în modul chioșc, selectați Pachet" la "Tip aplicație"
Aplicație kiosk	Faceți clic aici, pentru a selecta o aplicație care ar trebui să fie pornită în modul Kiosk Veți găsi prezentarea generală obișnuită a gestionării aplicațiilor Puteți selecta între "Magazin Google Play", "Aplicații interne Android" și "Nume de pachet"

Tip de aplicație	
URL	Dacă doriți să lansați un URL în modul chioșc, selectați "URL" la "Tip aplicație" Apoi definiți adresa URL dorită
Ștergeți browserul după inactivitate	Aici puteți defini un interval de timp în minute, după care modul Kiosk ar trebui să fie relansat
Ștergeți cache-ul web și modulele cookie	Dacă activați această funcție, după o repornire a modului Kiosk, cache-ul web (cookie-uri și imagini în cache) va fi șters
Politica privind aceeași origine	Dacă această funcție este activă, atunci utilizatorul poate naviga numai pe subpaginile unui URL definit De exemplu, ați definit următoarea adresă URL:www.mypage.com Apoi, utilizatorul poate naviga pe: www.mypage.com/subpage
URL-uri pe lista albă	Aici puteți menține o listă albă, toate aceste URL-uri sunt permise Maximum 1 URL pe linie O adresă URL trebuie să înceapă cu http:/ sau https://
URL-uri pe lista neagră	Aici puteți menține o listă neagră, toate aceste URL-uri nu sunt permise Maximum 1 URL pe linie O adresă URL trebuie să înceapă cu http:/ sau https://
Orientarea ecranului	Această setare se referă la ajustările ecranului Automat = automat Portret = format vertical Peisaj = modul peisaj

Aplicație multiplă	Dacă selectați modul chioșc "Multi App", va fi impusă utilizarea lansatorului AppTec360.
Aplicații	Aplicație: Selectați o aplicație Playstore sau o aplicație internă ca aplicație pentru chioșc. De asemenea, este posibil să introduceți un nume de pachet. Aplicația de chioșc selectată trebuie să fie instalată pe dispozitiv. Nu uitați să setați aplicația de chioșc ca fiind obligatorie. Comandă rapidă pe ecranul de pornire: Dacă este setat la "Activat", va fi creată o comandă rapidă pe ecranul de pornire. Dacă este setată la "Off", aplicația va apărea în continuare în lista de aplicații.

Parola de ieșire activată	Dacă activați această funcție, atunci este posibil ca utilizatorul să încheie modul Kiosk cu o parolă predefinită de dvs.
Parola de ieșire	Aceasta este parola, care a fost predefinită de dvs.
Auto Collapse Status Bar	Dacă această opțiune este activată, bara de stare va fi automat colpasată. Cu această opțiune, utilizatorii pot vedea informațiile din bara de stare, dar nu pot accesa funcțiile acesteia
Dezactivați bara de stare	Bara de stare conține notificări, comenzi rapide și informații. Disponibil numai pentru dispozitivele Samsung cu SAFE 4.0 sau mai mare.
Dezactivarea tastelor de volum	Dezactivați tastele de volum (disponibil numai pe dispozitivele Samsung cu SAFE 3.0 sau versiune superioară)
Dezactivați comutatorul pornit / oprit	Dezactivați comutatorul Pornit / Oprit (disponibil numai pe dispozitivele Samsung cu SAFE 3.0 sau superior)
Dezactivați butonul Acasă	Dezactivarea butonului Acasă. Dacă această funcție a fost activată, atunci modul Kiosk poate fi oprit numai în consola AppTec360 (disponibil numai pe dispozitivele Samsung cu SAFE 3.0 sau versiune superioară)
Dezactivați bara de navigare	Cu aceasta puteți dezactiva bara de navigare (Înapoi / Meniu) În cazul în care această funcție a fost activată, modul Kiosk poate fi oprit numai în consola AppTec360 (disponibil numai pe dispozitivele Samsung cu SAFE 3.0 sau versiune superioară)

Lansator AppTec360

Activați lansatorul AppTec360	Pornit: Activează lansatorul AppTec360. Utilizatorul trebuie să îl seteze o singură dată ca lansator implicit. Notă: Dacă modul chioșc este activat, iar modul chioșc este setat la "Multi App", va fi impusă utilizarea lansatorului AppTec360.
Icoane mari	Pornit: Afișează o versiune mai mare a pictogramelor aplicației în lansator
Ascundeți pictograma AppTec360 App	Pornit: Ascunde complet aplicația AppTec360
Ascundeți pictograma magazinului AppTec360	Pornit: Ascunde complet AppTec360 Enterprise AppStore

Setări AppTec360

Activați AppTec360 Settings App	AppTec360 Settings App oferă control asupra conexiunilor WiFi și Bluetooth
Activați setările în Multi App Modul Kiosk	Dacă este activat, utilizatorii pot accesa AppTec360 Settings App în timp ce modul Multi App Kiosk este activ

Telecomandă

Splashtop

Pentru a începe o sesiune de control de la distanță pentru dispozitivul dvs., aplicația "Splashtop Streamer" trebuie să fie instalată pe dispozitiv prin adăugarea aplicației la **App Management → Enterprise App Manager → Aplicații obligatorii**.

Ulterior, configurați următoarele setări pentru Splashtop:

Activați Splashtop	Dacă este activat, AppTec360 va configura aplicația Splashtop pentru a permite controlul de la distanță
Implementare cod	Accesați https://my.splashtop.com și autentificați-vă în contul Splashtop. Faceți clic pe "Add Computer" (Adăugare computer) și copiați codul de implementare de 12 cifre de pe pagina rezultată.
Setați Gateway de desfășurare personalizat?	Implementare Gateway
Implementarea domeniului / gazdei Gateway	Implementare Gateway
Verificarea certificatului	Verificarea certificatului

Apoi puteți utiliza opțiunea Splashtop Remote Control din meniul contextual (uneltele de lângă bara de căutare, atunci când dispozitivul este selectat sau faceți clic dreapta pe dispozitiv în arbore) pentru a începe sesiunea de control de la distanță.

TeamViewer

Pentru a începe o sesiune de control de la distanță pentru dispozitivul dvs., aplicația "TeamViewer QuickSupport" trebuie să fie instalată pe dispozitiv prin adăugarea aplicației la **App Management → Enterprise App Manager → Aplicații obligatorii**.

Apoi puteți utiliza opțiunea **TeamViewer Remote Control** din meniul contextual (uneltele de lângă bara de căutare, atunci când dispozitivul este selectat sau faceți clic dreapta pe dispozitiv în arbore) pentru a începe sesiunea de control de la distanță.

Gestionarea conținutului

ContentBox

Aici puteți activa ContentBox.

De îndată ce comutați "Enable ContentBox" la "On", o aplicație ContentBox separată va fi instalată automat pe dispozitivul utilizatorului final.

Browser securizat

Aici puteți configura setările pentru AppTec360 Secure Browser.

De îndată ce comutați secțiunea "Browser securizat" la "Activat", o aplicație browser separată va fi instalată automat pe dispozitivul utilizatorului final.

Solicitare parolă	Cereți utilizatorului să configureze și să utilizeze o parolă pentru a accesa browserul.
Lungimea minimă necesară a parolei	Setați numărul necesar de caractere pentru parolă
Calitatea parolei necesare	Setați calitatea parolei necesare
Restricționați descărcările / Deschideți în	
Restricționarea încărcărilor	
Încărcați lista albă	O listă de URL-uri pentru care încărcarea va fi permisă întotdeauna.
Permiteți copierea	Permiteți copierea, tăierea sau partajarea textului din paginile web.
Permiteți capturarea ecranului	Permiteți capturarea de capturi de ecran.
Frecvența curățării datelor	Selectați frecvența cu care TOATE datele utilizatorului (istoric, cache etc.) ar trebui eliminate automat.
Marcaje companie	Marcajele vor apărea în folderul "Marcaje companie" din marcajele browserului. Acestea nu sunt editabile de către utilizator.
Ascundeți bara de adrese	
Lista albă în browser (fără Universal Gateway)	Activează lista albă URL pe partea de client. • Marcajele companiei sunt întotdeauna pe lista albă • Suportat numai pentru 100 de URL-uri • Vă rugăm să utilizați Universal Gateway pentru Black- și Whitelisting nelimitat
URL-uri pe lista albă	O listă de URL-uri permise.
Liste negre și albe bazate pe gateway	Lista neagră are următoarele cerințe:

	• Un Gateway universal AppTec360 funcțional ("Setări generale" → "Gateway universal") • O configurație VPN funcțională cu un server DNS specificat ("Setări generale" → "Universal Gateway" → "Setări VPN") • O configurare a listei negre ("Setări generale" → "Universal Gateway" → "Lista neagră a domeniului") • O conexiune VPN validă în profil ("Gestionarea conexiunii" → "VPN")

API suplimentare

Samsung KNOX

Restricții

Permiteți cardul SD	
Permiteți scrierea pe cardul SD	
Permiteți capturarea ecranului	
Permiteți Clipboard	
Copierea de rezervă a setărilor și a datelor aplicației în Google Cloud	
Restaurați setările din Google Cloud atunci când reinstalați o aplicație	
Permite depanarea USB	
Permiteți Google Crash Report	
Permiteți resetarea din fabrică	
Permiteți actualizarea OTA	
Permiteți stocare gazdă USB	Dacă este activată, un utilizator poate conecta orice pen drive (unitate de stocare USB portabilă), HD extern sau cititor de carduri Secure Digital (SD), iar acesta este montat ca unitate de stocare pe dispozitiv.
Permiteți USB Media Player (MTP,PTP)	
Permiteți microfonul	Dezactivează microfonul pentru aplicații terțe
Permiteți NFC (Near Field Communication)	
Permiteți surse necunoscute (APK Sideloading)	Dacă este activată, este permisă încărcarea laterală a aplicațiilor (fișiere APK). Odată ce această setare este dezactivată, utilizatorul trebuie să o activeze manual atunci când permiteți din nou instalarea APK-urilor din surse necunoscute.

Permiteți crearea de utilizatori	Dacă este activat, utilizatorului i se permite să creeze mai multe conturi pe dispozitiv, de exemplu, Conturi de oaspete

E-mail

Adresa eMail	
Protocol server de intrare	
Adresa serverului de intrare	
Portul serverului de intrare	
Autentificare/utilizator server de intrare	
Parola serverului de intrare	
Serverul de intrare utilizează SSL	
Serverul de intrare utilizează TLS	
Serverul de intrare acceptă toate certificatele	
Protocolul serverului de ieșire	
Adresa serverului de ieșire	
Portul serverului de ieșire	
Serverul de ieșire utilizează credențiale suplimentare	Dacă este dezactivat, sistemul utilizează acreditările de intrare și pentru serverul de ieșire.
Autentificare/utilizator server de ieșire	
Parola serverului de ieșire	
Serverul de ieșire utilizează SSL	
Serverul de ieșire utilizează TLS	
Serverul de ieșire acceptă toate certificatele	
Setați semnătura	
Semnătura	Notă: Pentru unele dispozitive, semnătura trebuie să fie specificată în format HTML.
Notificarea utilizatorului cu privire la primirea unui nou e-mail	

Schimb

Adresa eMail	
Nume gazdă server	Numele de gazdă al serverului Exchange
Nume de utilizator	Numele de utilizator utilizat pentru conectarea la serverul Exchange
Domeniu	Dacă este activată o configurare ACL Gateway și câmpul Domain nu este gol, AppTec360 Universal Gateway va autentifica dispozitivul cu următorul nume "Domain\Login Name
Parolă	
Numărul de zile anterioare pentru sincronizare	
Frecvența sincronizării eMail	
Sincronizare în roaming	
Setați semnătura	
Semnătura	Notă: Pentru unele dispozitive, semnătura trebuie să fie specificată în format HTML.
Cont implicit	
Utilizați Secure Sockets Layer (SSL)	
Utilizați securitatea stratului de transport (TLS)	
Acceptați toate certificatele	

APN

Nume de afișare APN	
Nume punct de acces	Denumirea APN
Protocolul serverului de ieșire	
MCC - Codul țării mobile	Lăsați gol pentru a utiliza mmc al SIM-ului instalat
MNC - Codul rețelei mobile	Lăsați gol pentru a utiliza mnc al SIM-ului instalat
Adresa serverului	
Numărul portului serverului	
Adresa proxy a serverului	
Adresa serverului MMS	Lăsați gol pentru implicit
Numărul portului MMS	Lăsați gol pentru implicit
Adresa proxy MMS	Lăsați gol pentru implicit
Nume utilizator	
Parolă	
Tip punct de acces	Tipurile acceptate sunt "default", "mms", "supl".
	Dacă se trece null sau empty, se utilizează implicit "default,supl,mms".
	Lăsați gol pentru valoarea implicită.
APN preferat	

Bluetooth

Permiteți descoperirea dispozitivului prin Bluetooth	
Permiteți împerecherea Bluetooth	
Permiteți dispozitivele Bluetooth Headset	
Permiteți utilizarea dispozitivelor Bluetooth Hands-free	
Permiteți dispozitive Bluetooth A2DP	A2DP, Advanced Audio Distribution Profile permite streamingul audio între dispozitive
Permiteți apelurile efectuate	
Permiteți transferul de date prin Bluetooth	
Permiteți Tethering Bluetooth	
Permiteți conectarea la computer prin Bluetooth	

Conexiune

Permiteți numai apeluri de urgență Permiteți Wi-Fi	
Nivelul minim de securitate al rețelei Wi-Fi	
Interziceți utilizatorului să adauge rețele Wi-Fi	Această restricție poate fi activată numai dacă cel puțin un profil Wi-Fi activ este definit în Gestionarea conexiunii
Permiteți SMS & MMS	
Permiteți sincronizarea în timpul roaming-ului	
Permiteți roamingul vocal	

Android Enterprise – Dispozitiv complet administrat cu profil de lucru (COPE)

Explicația generală a COPE

COPE este o abreviere pentru **Corporate Owned Personally Enabled**.

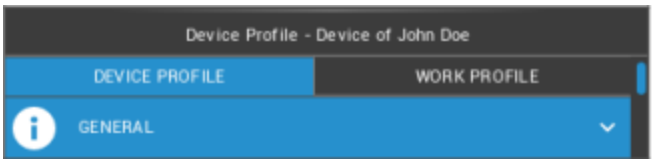
Modul COPE permite înscrierea unui dispozitiv Android ca **dispozitiv Android Enterprise - complet gestionat** , cu profil integrat **Android Enterprise - container**.

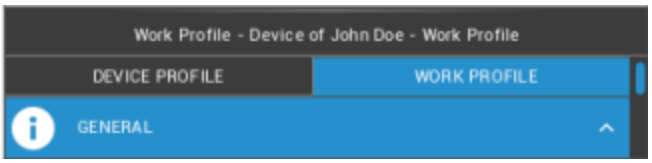
Acesta poate fi fie un dispozitiv Android care este deja înscris ca **dispozitiv Android Enterprise - Fully Managed** și pe care este configurat în plus **Android Enterprise - Container**, fie un dispozitiv Android nou înscris care este înscris direct ca **dispozitiv Android Enterprise - Fully Managed** împreună cu **Android Enterprise - Container** deasupra acestuia.

Modul COPE este disponibil numai pentru dispozitivele cu Android 8, 9 și 10

Configurarea profilurilor pentru dispozitivele COPE

Deoarece nu există un profil de configurare pentru modul COPE în sine, configurarea **Android Enterprise - dispozitiv complet administrat** și **Android Enterprise - container** este separată în două profiluri în cadrul profilului COPE. Este posibil să comutați între cele două profiluri pentru configurarea fiecărui profil făcând clic pe butonul respectiv din partea stângă a consolei:





Ambele profiluri pot fi configurate după cum este descris pentru fiecare profil în parte:

Android Enterprise - Dispozitiv complet administrat

Android Enterprise - Container

Revenirea la un dispozitiv AE complet administrat

Profilul **Android Enterprise - Container** poate fi eliminat conform descrierii din secțiunea **Gestionarea dispozitivelor mobile**.

Prin eliminarea profilului Container, profilul COPE va fi transformat într-un profil **Android Enterprise - Fully Managed Device**.

Android Enterprise – Configurarea containerului

În funcție de faptul dacă ați selectat în prezent un profil de grup sau un dispozitiv, prezentarea generală și subpunctele sale diferă - vă rugăm să luați în considerare acest lucru cu atenție!

Generalități

Prezentare generală a profilului (numai la nivel de profil)

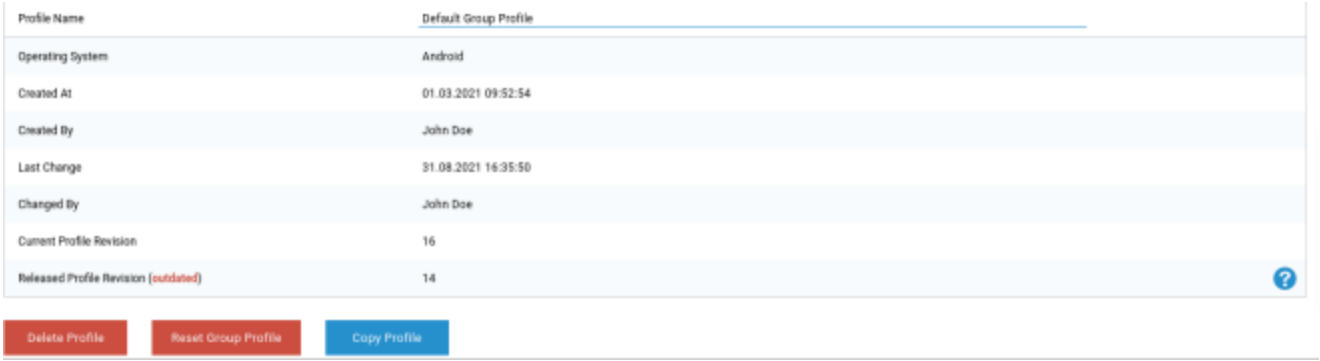
În cazul în care vă aflați într-un profil, veți primi o scurtă prezentare generală a profilului, în ceea ce privește numele, sistemul de operare, data creării, autorul etc.

Nume profil	Numele profilului - poate fi redenumit direct aici
Sistem de operare	Sistemul de operare valabil pentru profil
Creat la	Data creării
Creat de	Creat de
Ultima schimbare	Data ultimei modificări
Schimbat de	Utilizatorul care a efectuat ultimele modificări la acest profil
Revizuirea actuală a profilului	Numărul de ori în care profilul a fost deja actualizat
Revizuire profil eliberată	Numărul de ori în care profilul a fost deja actualizat și i s-au atribuit dispozitive

Ștergeți profilul	Ștergeți profilul
Resetarea profilului grupului	Resetarea profilului grupului
Copiați profilul	Copiați profilul

Prezentare generală a profilului grupului (numai la nivel de grup)

Atunci când deschideți un profil de grup, veți obține o prezentare generală rapidă a profilului.



Nume profil	Numele profilului (poate fi modificat aici)
Sistem de operare	Sistemul de operare pentru care este creat profilul
Creat la	Momentul creației
Creat de	Creatorul profilului
Ultima schimbare	Ora ultimei modificări a profilului
Schimbat de	Contul care a efectuat ultimele modificări
Revizuirea actuală a profilului	Revizuirea stării profilului salvat
Revizuire profil eliberată	Revizuirea profilului atribuit ("Atribuie acum"). Dacă eticheta afișează "(învechit)" în spatele textului, înseamnă că ați salvat profilul, dar nu l-ați atribuit încă, astfel încât dispozitivele vor primi în continuare o versiune mai veche.

Prezentare generală a dispozitivului (numai la nivel de dispozitiv)

Dacă vă aflați pe un dispozitiv, veți primi o recapitulare generală a dispozitivului selectat, care conține următoarele informații:

Numele dispozitivului	Numele dispozitivului
Locație	Coordonate locație
Număr de telefon	Număr de telefon
Aplicații obligatorii atribuite	Numărul de aplicații obligatorii alocate
Versiunea sistemului de operare	Versiunea sistemului de operare al dispozitivului
Sistem de operare	Sistem de operare (Android Enterprise)
Numărul de serie	Numărul de serie al dispozitivului
Proprietatea dispozitivului	Dispozitiv corporativ sau privat
Tip dispozitiv	Dispozitiv gestionat de AE Work
Înrădăcinat	Stare, indicând dacă dispozitivul a fost rădăcinat
Conform	În conformitate cu liniile directoare
Adresa IP	Adresa IP a dispozitivului
Văzut ultima dată	Momentul în care dispozitivul s-a conectat ultima dată la AppTec
Ultimul impuls	Momentul în care a fost trimis ultimul push către dispozitiv
Atribuirea utilizatorului	Utilizatorul sau grupul căruia îi este atribuit acest dispozitiv

Revizuire configurare

Aici primiți o prezentare generală a profilului de grup care este atribuit dispozitivului.

Dacă faceți clic pe profilul grupului, veți obține acces direct la acest profil și veți putea efectua setările.

Cu acest simbol, puteți readuce aplicațiile distribuite la setările profilului de grup.

Cu acest simbol, puteți readuce toate aplicațiile utilizate la setările profilului de grup.

"Newer Revision available" indică faptul că profilul grupului a fost modificat și salvat, dar nu a fost atribuit. Profilul de grup trebuie să fie atribuit cu "Assign now" la nivel de grup pentru a aplica

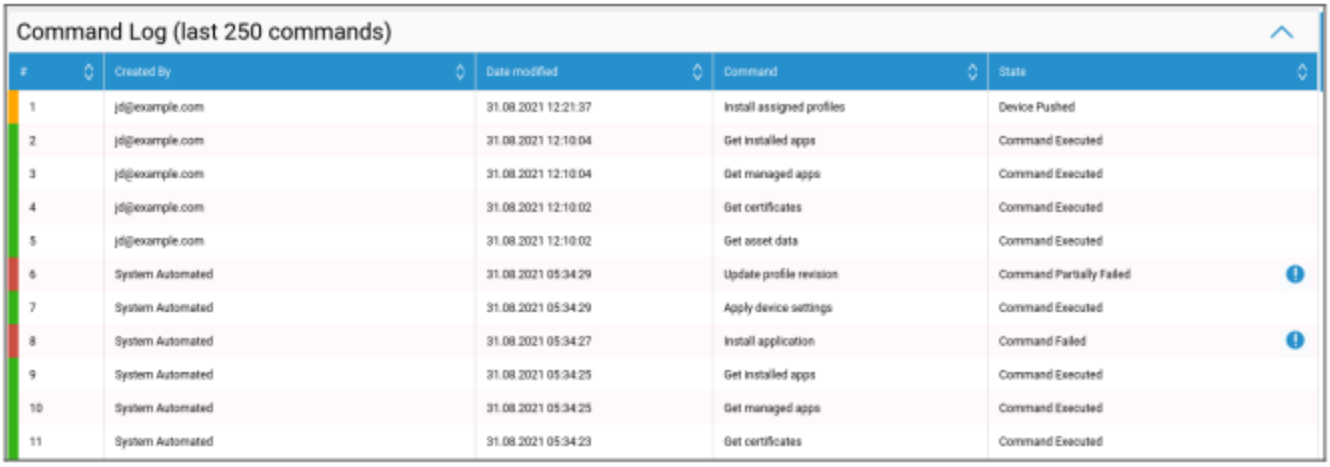
modificările dispozitivelor.

Jurnalul dispozitivului (numai la nivel de dispozitiv)

Aici veți primi diverse jurnale ale dispozitivului. Dacă este necesar, aici puteți afla direct cauza unei erori.

Jurnal de comandă

Aici puteți vedea ce comenzi au fost emise pentru dispozitiv și care este starea lor.



Stări posibile ale comenzii

Dispozitiv împins	O solicitare push a fost trimisă către serviciul push (de exemplu, APNS) pentru a indica dispozitivului să se conecteze din nou la serverul EMM.
Comandă creată	Comanda a fost creată în sistem.
Comandă trimisă	Comanda a fost trimisă către dispozitiv după ce acesta s-a conectat la server.
Comandă executată	Comanda a fost executată cu succes.
Comandă eșuată	Comanda a eșuat. *
Comandă eșuată parțial	În funcție de sistemul de operare al dispozitivului, unele comenzi pot fi grupate împreună. În acest caz, unele părți ale acestui grup de comandă au eșuat. *
Comandă executată, eventual eșuată	Comanda a fost executată, dar poate că nu a fost.
Comanda Repushed	Comanda a fost respinsă de un utilizator.
Aruncată	Comanda a fost eliminată. De exemplu, pentru că a fost înlocuită de o altă comandă sau pentru că dispozitivul a fost înrolat din nou și comenzile vechi au fost eliminate

*Dacă există un semn al exclamării în spatele mesajului, puteți obține mai multe informații trecând cu cursorul peste pictogramă.

Setări dispozitiv

Configurare client

Aici puteți efectua următoarele configurații pe dispozitivul Android:

Timp de neconformitate	Limita de timp de răspuns a utilizatorului după care se aplică acțiunea de executare.
Acțiune de punere în aplicare după expirarea termenului de conformitate	Acțiune de punere în aplicare atunci când un utilizator nu efectuează acțiuni care conduc la un statut de dispozitiv conform
Frecvența colectării datelor	Frecvența cu care trebuie colectate informațiile despre dispozitiv/GPS
Frecvența bătăilor inimii dispozitivului	Intervalul în care dispozitivul trebuie să contacteze serverul AppTec Min. 1 minut Max. 24 de ore
Activați actualizările locației	Dacă este activat, dispozitivul trimite actualizări ale locației către serverul AppTec
Locație Ora actualizării	Determină în ce intervale de timp dispozitivul trimite actualizări ale locației către AppTec
Utilizați Google Location Accuracy pentru actualizarea locației	Dacă este activată, locația de rețea va fi utilizată pentru actualizările locației (dacă a fost dezactivată la "Restricții", atunci această setare nu va afecta nimic)
Utilizați locația GPS pentru actualizarea locației	Dacă este activat, GPS-ul va fi utilizat pentru actualizarea locației
Permiteți locații fictive (false)	Permite falsificarea informațiilor de localizare prin intermediul aplicațiilor terță parte
Acțiune de pierdere a conexiunii	Dacă este activat, puteți specifica o acțiune pentru cazul în care un dispozitiv nu se conectează la serverul MDM în intervalul de bătaie a inimii. De exemplu, dacă dispozitivul are un timp de bătaie a inimii de 5 minute, acesta se conectează la server la ora 10:35 AM. După aceea, dispozitivul părăsește raza Wi-Fi. Următorul heartbeat la ora 10:40 AM va eșua, iar acțiunea specificată va fi executată.
Acțiune	Acțiunea care trebuie întreprinsă imediat ce un dispozitiv devine neconform. • Lock Dispozitiv = dispozitiv de blocare

	• Ștergere dispozitiv = dispozitivul va fi restaurat la setările din fabrică • Ștergere dispozitiv și card SD = dispozitivul va fi restaurat la setările din fabrică, iar spațiul de stocare de pe cardul SD va fi șters
Prag	Puteți specifica un prag de bătăi de inimă eșuate care sunt necesare pentru a declanșa acțiunea specificată.

Modul de aplicare a politicii	Implicit:	Utilizatorilor li se va solicita periodic să execute acțiunile restante
	Aplicare lenește a politicilor:	Utilizatorilor nu li se va cere niciodată să execute acțiunile în curs. Toate acțiunile deschise vor fi afișate în AppTec Client
	Aplicarea agresivă a politicilor:	Utilizatorilor li se va solicita neîncetat să execute acțiunile restante
Blocarea versiunii AppTec	Dacă este activat, poate fi specificat un cod de versiune pentru aplicația AppTec. Clientul AppTec se va actualiza numai la versiunea specificată. Versiunile mai noi vor fi ignorate. Un downgrade NU este posibil.	
Codul versiunii	Codul versiunii pentru aplicația AppTec care urmează să fie blocată.	
Dezactivați Notificarea AppTec	Dacă este dezactivat, clientul AppTec nu va afișa o notificare în bara de notificări. Astfel, utilizatorii pot închide clientul AppTec prin intermediul managerului de activități. În cazul în care clientul AppTec este închis, mai multe caracteristici, inclusiv modul Kiosk și App Black/Whitelisting, nu vor funcționa corect. Dispozitivele Samsung oferă un mecanism de protecție pentru AppTec Client. Notificarea este dezactivată implicit pe dispozitivele Samsung care acceptă API-urile KNOX. Notificarea nu ar trebui să fie dezactivată pe dispozitivele cu Android 8.0 sau o versiune ulterioară.	

Wallpaper

Setați tapet personalizat	Activați/dezactivați imaginea de fundal personalizată
Wallpaper	Setați modul tapet pentru a utiliza un cod de culori sau o imagine
Specificați o culoare	Specificați o culoare de fundal ca valoare hexazecimală, de exemplu #000000 pentru negru sau #ffffff pentru alb
Setați imaginea ca tapet	Încărcați fișierul imagine pe care doriți să îl utilizați ca tapet

Gestionarea activelor (numai la nivel de dispozitiv)

Informații despre dispozitiv

Model	Denumirea modelului dispozitivului
Sistem de operare	SO
Versiunea sistemului de operare	Versiunea sistemului de operare
Numărul de serie	Numărul de serie
Numele dispozitivului	Numele dispozitivului
Starea bateriei	Starea bateriei
Memorie liberă / totală	Memorie liberă / totală
Samsung Safe	Interfața Samsung SAFE, necesară pentru o varietate de opțiuni de setare
Card SD disponibil	Card SD disponibil
Card SD emulat	Card SD emulat
Card SD detașabil	Card SD detașabil
SD Memorie liberă / totală	SD Liber / Total memorie card SD

Wi-Fi

Adresa IP	Adresa IP a dispozitivului
WiFi MAC	Adresa MAC WiFi

Celulare

Statut	Stare (cartela SIM instalată)
Număr de telefon	Număr de telefon
Roaming (voce / date)	Roaming pentru voce / date
Starea de roaming	Starea curentă de roaming
Adresa IP	Adresa IP
Operator/Carrier	Operator/Carrier
Tehnologie celulară	Tehnologie celulară
IMEI	Numărul IMEI
ICCID	Acesta este ID-ul cartelei SIM, de multe ori și un Smartcard sau o cartelă cu circuit integrat (ICC)
IMSI	Identitatea internațională a abonatului mobil (IMSI) oferă în rețelele mobile GSM și UMTS o identificare definitivă a utilizatorilor rețelei IMSI este compus din maximum 15 cifre și este configurat în felul următor: • Codul țării mobile (MCC), 3 cifre • Codul rețelei mobile (MNC), 2 sau 3 cifre • Numărul de identificare a abonatului mobil (MSIN), 1-10 cifre
Actual MCC/MNC	Consultați "SIM MCC/MNC"
SIM MCC/MNC	Codul țării mobile este un identificator de țară stabilit de ITU conform standardului E.212. Acesta funcționează împreună cu codul rețelei mobile (MNC) pentru identificarea rețelei mobile. Înseamnă țara/codul rețelei mobile a cartelei SIM. Dacă vă deplasați într-o altă rețea mobilă, atunci, în mod logic, "MCC/MNC curent" și "SIM MCC/MNC" vor fi diferite.

Bluetooth

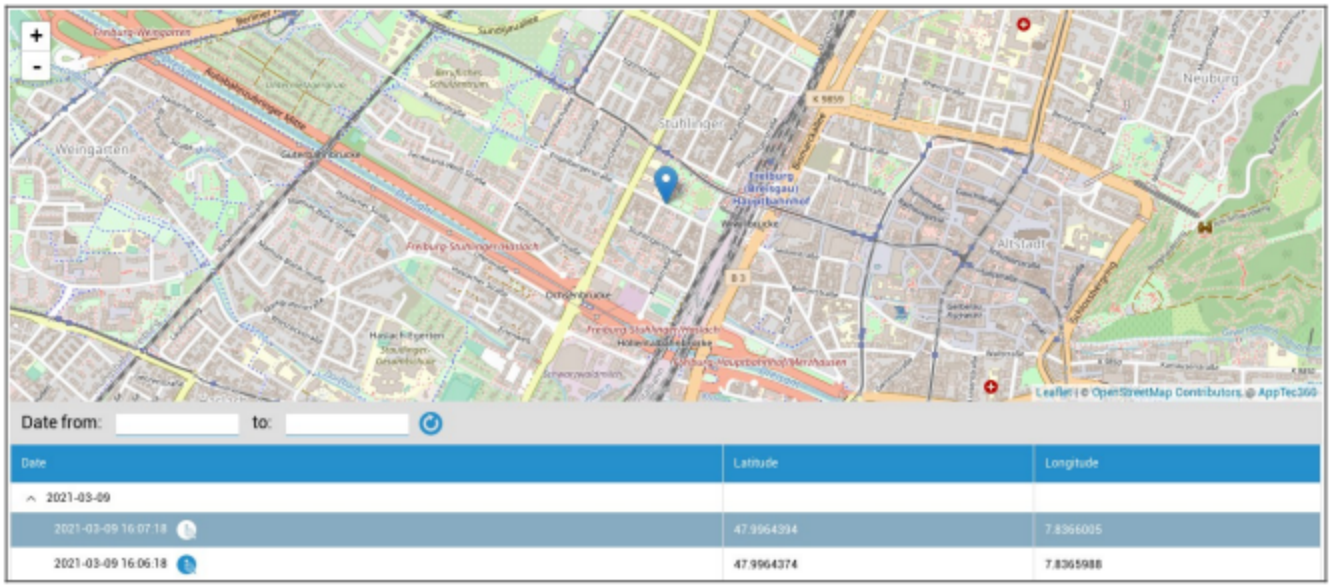
Bluetooth MAC	Adresa MAC Bluetooth

Managementul securității

Anti-furt (numai la nivel de dispozitiv)

Informații GPS (numai la nivelul dispozitivului)

Aici puteți stabili locația curentă/ultima a dispozitivului. Localizarea poate fi protejată cu una sau chiar două parole - Consultați: Setări generale - Confidențialitate - Acces GPS



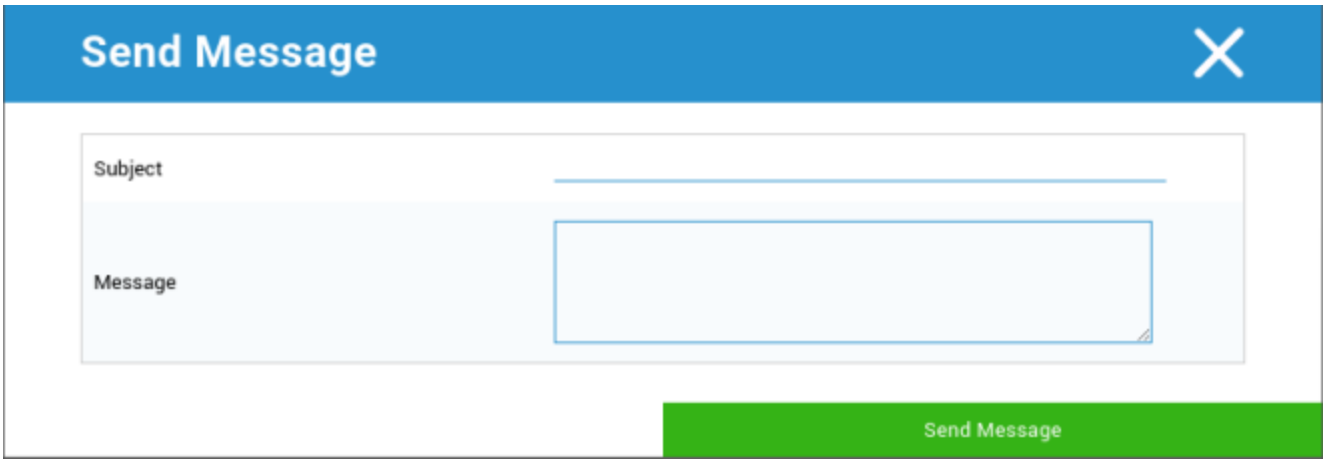
Ștergere și blocare (numai la nivel de dispozitiv)

Sub "Ștergere și blocare", puteți efectua următoarele trei acțiuni:

Ștergere completă	Dispozitivul este readus la setările din fabrică (sunt șterse atât datele personale, cât și cele ale companiei). Funcționează numai pentru profilul de lucru îmbunătățit
Ștergere Enterprise	Doar datele corporative sunt eliminate de pe dispozitivul utilizatorului final (toate aplicațiile, datele, etc. care au fost furnizate de AppTec)
Ecran de blocare	Blocarea ecranului este activată, este suficient să deblocați dispozitivul cu ajutorul parolei dispozitivului/PIN

Mesaj (numai la nivel de dispozitiv)

Aici puteți completa subiectul și un mesaj și să îl trimiteți unui dispozitiv utilizator final



Configurația de securitate

Codul de acces al dispozitivului

Sub "Cod de acces" puteți trimite o parolă pentru dispozitiv, fiind disponibile următoarele opțiuni de setare

Lungimea minimă a parolei	Stabilește numărul minim de simboluri pe care trebuie să le aibă o parolă	
Calitatea parolei	Nespecificat	Această politică nu are cerințe privind parola.
	Biometric Slab	Această politică permite utilizarea tehnologiei de recunoaștere biometrică de securitate redusă. Aceasta implică tehnologii care pot recunoaște identitatea unei persoane până la un cod PIN de aproximativ 3 cifre (detectarea falsă este mai mică de 1 la 1 000).
	Ceva	Această politică necesită setarea unui anumit tip de parolă sau model, dar nu impune nicio regulă specifică.
	Alfabetic	Utilizatorul trebuie să fi introdus o parolă care să conțină cel puțin caractere alfabetice (sau alte simboluri).
	Alfanumeric	Utilizatorul trebuie să fi introdus o parolă care să conțină cel puțin caractere numerice și alfabetice (sau alte simboluri).
	Complex	Utilizatorul trebuie să fi introdus o parolă care să conțină cel puțin o literă, o cifră numerică și un simbol special, în mod implicit. Cu această calitate a parolei, parolele pot fi restricționate pentru a conține diferite seturi de caractere, cum ar fi cel puțin o literă mare, etc.
Lungimea minimă a parolei	Setați numărul necesar de caractere pentru parolă. De exemplu, puteți solicita ca PIN-ul sau parolele să aibă cel puțin șase caractere.	
Minimum de cifre numerice necesare în parolă	Minimum de cifre numerice necesare în parolă	
Minimum de litere minuscule necesare în parolă	Minimum de litere minuscule necesare în parolă	
Minimum de litere majuscule necesare în parolă	Minimum de litere majuscule necesare în parolă	

Numărul minim de caractere din afara literelor necesare în parolă	Numărul minim de caractere din afara literelor necesare în parolă
Simboluri minime necesare în parolă	Simboluri minime necesare în parolă

Timp maxim de inactivitate blocare	Inactivitatea maximă a utilizatorului până la blocarea timpului
Timpul de expirare a parolei	Se stabilește, interval de timp după care parola expiră și trebuie emisă o nouă parolă
Restricționarea istoricului parolelor	Numărul de parole utilizate anterior care nu sunt permise
Numărul maxim de încercări de parole eșuate	Stabilește de câte ori o parolă poate fi introdusă incorect, înainte de a se efectua o ștergere completă a dispozitivului
Permiteți autentificarea biometrică	Permite autentificarea prin scanarea amprentei sau a irisului. Numai pentru Samsung KNOX 2.1 și versiuni ulterioare

Codul de acces al containerului

Sub "Cod de acces" puteți trimite o parolă pentru container, următoarele opțiuni de setare sunt disponibile la

Lungimea minimă a parolei	Stabilește numărul minim de simboluri pe care trebuie să le aibă o parolă	
Calitatea parolei	Nespecificat	Această politică nu are cerințe privind parola.
	Biometric Slab	Această politică permite utilizarea tehnologiei de recunoaștere biometrică de securitate redusă. Aceasta implică tehnologii care pot recunoaște identitatea unei persoane până la un cod PIN de aproximativ 3 cifre (detectarea falsă este mai mică de 1 la 1 000).
	Ceva	Această politică necesită setarea unui anumit tip de parolă sau model, dar nu impune nicio regulă specifică.
	Alfabetic	Utilizatorul trebuie să fi introdus o parolă care să conțină cel puțin caractere alfabetice (sau alte simboluri).
	Alfanumeric	Utilizatorul trebuie să fi introdus o parolă care să conțină cel puțin caractere numerice și alfabetice (sau alte simboluri).
	Complex	Utilizatorul trebuie să fi introdus o parolă care să conțină cel puțin o literă, o cifră numerică și un simbol special, în mod implicit. Cu această calitate a parolei, parolele pot fi restricționate pentru a conține diferite seturi de caractere, cum ar fi cel puțin o literă mare, etc.
Lungimea minimă a parolei	Setați numărul necesar de caractere pentru parolă. De exemplu, puteți solicita ca PIN-ul sau parolele să aibă cel puțin șase caractere.	
Minimum de cifre numerice necesare în parolă	Minimum de cifre numerice necesare în parolă	
Minimum de litere minuscule necesare în parolă	Minimum de litere minuscule necesare în parolă	
Minimum de litere majuscule necesare în parolă	Minimum de litere majuscule necesare în parolă	
Numărul minim de caractere din afara	Numărul minim de caractere din afara literelor necesare în parolă	

literelor necesare în parolă	
Simboluri minime necesare în parolă	Simboluri minime necesare în parolă

Timp maxim de inactivitate blocare	Inactivitatea maximă a utilizatorului până la blocarea timpului
Timpul de expirare a parolei	Se stabilește, interval de timp după care parola expiră și trebuie emisă o nouă parolă
Restricționarea istoricului parolelor	Numărul de parole utilizate anterior care nu sunt permise
Numărul maxim de încercări de parole eșuate	Stabilește de câte ori o parolă poate fi introdusă incorect, înainte de a se efectua o ștergere completă a dispozitivului

AntiVirus

Scanare automată	Activați scanările automate periodice
Interval de scanare	Interval de examinare (rapid / complet)
Scanare automată completă	Activați scanările automate complete
Actualizări automate	Activați actualizările automate
Interval de verificare a actualizării	Cât de des trebuie actualizate aplicația și baza sa de date (viruși / cod deteriorat)
Protecția aplicațiilor	Activați scanarea automată a aplicațiilor
Protecția cardului SD	Activați scanarea automată a cardului SD
Actualizare numai Wi-Fi	Atunci când este activat, actualizările vor fi aplicate numai atunci când dispozitivul este conectat cu succes la o rețea Wi-Fi

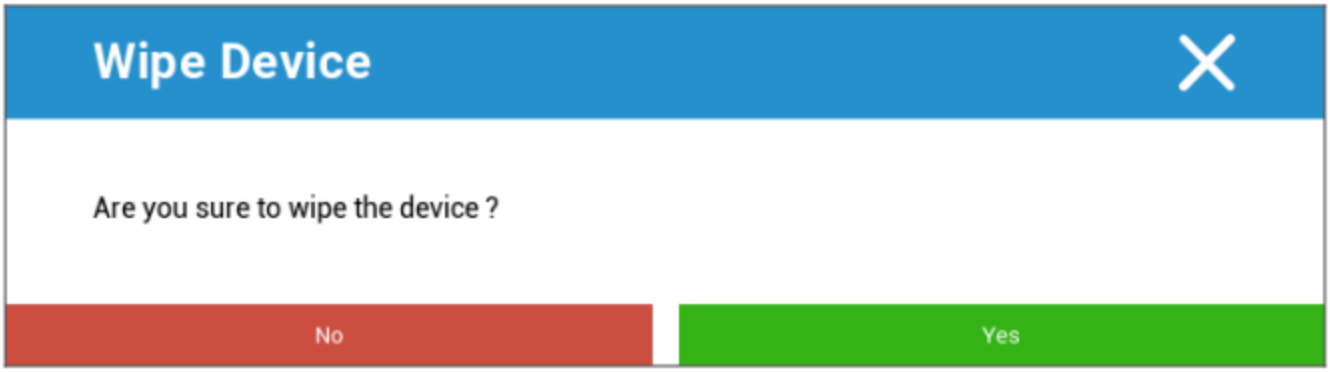
Sfârșitul duratei de viață (numai la nivel de dispozitiv)

Ștergere (numai la nivel de dispozitiv)

Sub "Ștergere", puteți readuce dispozitivul la setările din fabrică (numai în cazul profilului de lucru îmbunătățit).

Aici, atât datele corporative, cât și cele private vor fi șterse de pe dispozitivul utilizatorului final.

La un clic pe "Simbolul minus" primiți următorul mesaj:



Cu "Da" puteți efectua ștergerea.

Sub "Raport ștergere" pot fi afișate următoarele elemente

Șters de	Istoricul persoanei care a efectuat ștergerea
Data	Data
Statut	Stare (de exemplu, dacă ștergerea a fost efectuată cu succes)

Setări de restricționare

Restricții

Aici, pot fi restricționate și blocate o varietate de lucruri.

Aplicarea conformității	Mode Prompt User - Utilizatorul va fi rugat să efectueze acțiunile necesare. Modul Lock-Down Container - Ascundeți toate aplicațiile până când toate cerințele sunt îndeplinite
Politica de autorizare în timpul rulării	Invitați utilizatorul să solicite noi permisiuni Întotdeauna acordați noi cereri de permisiune noi Refuzați întotdeauna noile cereri de permisiune Atenție: Unele aplicații au probleme cu recunoașterea permisiunilor dacă acestea sunt setate automat. Dacă acordați întotdeauna permisiuni și întâmpinați probleme cu aplicațiile care spun că lipsesc permisiunile, setați acest lucru la "prompt user" și reinstalați aplicația
Permiteți scoaterea clipboard-ului	Permite copierea și lipirea din interiorul containerului în exterior
Permiteți rezoluția ID-ului apelantului	Afișează numele pentru un apel primit pe baza contactelor din container
Permiteți rezolvarea căutării contactelor	Permite căutarea numelor în contactele din container atunci când efectuați apeluri
Permiteți partajarea contactelor Bluetooth	Permite accesul la contactul containerului în mașină
Interzice ieșirea fasciculului NFC	Dezactivează NFC pentru container
Permiteți surse necunoscute	Dacă este activată, utilizatorii pot încărca aplicații prin instalarea unui fișier .apk.
Permite depanarea USB	Dacă este activată, utilizatorii pot activa depanarea USB.
Interzicerea modificării contului	Interzice crearea, ștergerea și modificarea conturilor din container Rețineți că unele aplicații trebuie să creeze sau să modifice conturi pentru a funcționa conform așteptărilor

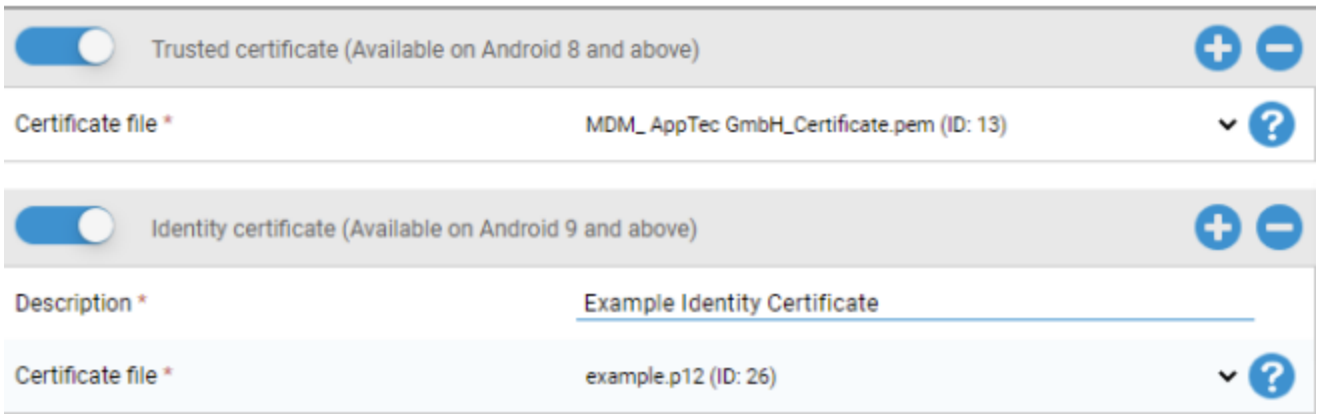
Restricții privind profilul de lucru. Disponibil numai pe dispozitivele Android 11 și versiunile ulterioare, cu profil de lucru îmbunătățit

Interziceți camera	Specifică dacă camera nu este permisă în profilul de lucru.
Interziceți Bluetooth	Specifică dacă bluetooth nu este permis în profilul de lucru.
Activarea protecției la resetarea din fabrică	Activați această opțiune pentru a anula protecția la resetarea din fabrică a Android pentru contul Google definit în "Setări generale" → "Configurare Android" → "Android Enterprise" → "Protecție la resetarea din fabrică" Dacă această opțiune este activată și resetați dispozitivul, va trebui să furnizați contul Google configurat pentru a configura din nou dispozitivul.
Actualizarea sistemului de operare Control	Activați această opțiune pentru a seta comportamentul de actualizare la automat, în fereastră sau amânat.
Politica de actualizare	Automat: Instalați automat imediat ce este disponibilă o actualizare. Fereastrată: Se instalează automat în cadrul unei ferestre de întreținere zilnică. De asemenea, această opțiune configurează aplicațiile Play pentru a fi actualizate în cadrul ferestrei. Acest lucru este foarte recomandat pentru dispozitivele chioșc, deoarece acesta este singurul mod în care aplicațiile fixate în mod persistent în prim-plan pot fi actualizate de Play. Amână: Amână instalarea automată până la un maxim de 30 de zile.

Restricții privind profilul personal. Disponibil numai pe dispozitivele Android 11 și mai recente, cu Profil de lucru îmbunătățit	
Interziceți camera	Specifică dacă camera nu este permisă în profilul personal.
Interziceți Bluetooth	Specifică dacă bluetooth nu este permis în profilul personal.
Permiteți surse necunoscute	Dacă este activat, utilizatorii profilului de lucru pot încărca aplicații prin instalarea unui fișier .apk.

Managementul certificatelor

Aici puteți distribui certificate de încredere și certificate de identitate dispozitivelor dvs. Android 8 sau o versiune mai recentă este necesar pentru a distribui certificate de încredere, iar Android 9 sau o versiune mai recentă este necesar pentru a distribui certificate de identitate.



Cu "+" puteți adăuga mai multe certificate.

Certificatele de încredere trebuie să fie în format PEM.

Certificatele de identitate trebuie să fie în format PKCS12.

Gestionarea conexiunilor

Wifi

Pentru această setare, efectuați preconfigurarea dispozitivelor utilizatorului final, pentru accesul la punctele interne Access

Identificatorul setului de servicii (SSID)	SSID pentru rețeaua care urmează să fie conectată
Rețea ascunsă	Activare, în cazul în care AP nu transmite SSID-ul

Tip de securitate

Stabilirea tipului de securitate al AP

WEP

Parolă	Parolă pentru AP

WPA/WPA2

Parolă	Parolă pentru AP

802.1x EAP

Metoda EAP

PWD	Identitate	Identitate
	Parolă	Parolă

PEAP	Protocolul de autentificare faza 2	niciunul	Fără protocol suplimentar
		MSCHAPV2	Protocolul MSCHAPV2
		GTC	Protocolul GTC
	Certificat CA	Certificat CA	
	Identitate	Identitate	
	Identitate anonimă	Identitate anonimă	
	Parolă	Parolă	

TTLS	Protocolul de autentificare faza 2	niciunul	Fără protocol suplimentar
		PAP	Protocolul PAP
		MSCHAP	Protocolul MSCHAP
		MSCHAPV2	Protocolul MSCHAPV2
		GTC	Protocolul GTC
	Certificat CA	Certificat CA	
	Identitate	Identitate	
	Identitate anonimă	Identitate anonimă	
	Parolă	Parolă	

TLS	Certificat CA	Certificat CA
	Identitate	Identitate
	Parolă	Parolă

VPN

Nume conexiune	Numele conexiunii VPN

Tip VPN

VPN

Client VPN

Client VPN AppTec	
Configurarea gateway-ului	Selectați configurația Gateway VPN (consultați **Setări generale > Gateway universal > Setări VPN**)
VPN Always On	Activați blocarea nativă
Activarea blocării AppTec	Activarea blocării AppTec

Integrat (disponibil numai pe dispozitivele Samsung)			
Tip de conexiune	PPTP	Server	Server
		Activați criptarea PPTP	Activați criptarea PPTP
	L2TP / IPSec PSK	Server	Server
		Cheie IPSec precompartimentată	Cheie IPSec precompartimentată
		Activați L2TP Secret	Activați L2TP Secret
		Secret L2TP	Secret L2TP
	IPSec XAuth PSK	Server	Server
		Identificator IPSec	Identificator IPSec
		Cheie IPSec precompartimentată	Cheie IPSec precompartimentată
DNS Căutare Domenii	DNS Căutare Domenii		
Setări expert	Servere DNS	Servere DNS	
	Redirecționarea rutelor	Redirecționarea rutelor	

VPN deschis		
Server	Server	
Profil OpenVPN	Profil OpenVPN	
Aplicație OpenVPN	OpenVPN pentru Android (recomandat)	
	Conectare OpenVPN	
Setări expert	Servere DNS	Servere DNS
	Redirecționarea rutelor	Redirecționarea rutelor

Samsung / Lebădă puternică			
Tip de conexiune	PPTP	Server	Server
		Nume utilizator	Nume utilizator
		Parolă	Parolă
		Activați criptarea PPTP	Activați criptarea PPTP
	L2TP / IPSec PSK	Server	Server
		Cheie IPSec precompartimentată	Cheie IPSec precompartimentată
		Nume utilizator	Nume utilizator
		Parolă	Parolă
		Activați L2TP Secret	Secret L2TP
	IPSec XAuth PSK	Server	Server
		Identificator IPSec	Identificator IPSec
		Cheie IPSec precompartimentată	Cheie IPSec precompartimentată
		Nume utilizator	Nume utilizator
		Parolă	Parolă
Setări expert	Servere DNS	Servere DNS	
	Redirecționarea rutelor	Redirecționarea rutelor	

Cisco Any Connect		
Server	Server	
Mod certificat	Dezactivat	Dezactivat
	Automată	Automată
Setări expert	Servere DNS	Servere DNS
	Redirecționarea rutelor	Redirecționarea rutelor

VPN per aplicație

Client VPN

Client VPN AppTec		
Configurarea gateway-ului	Selectați configurația Gateway VPN (consultați **Setări generale > Gateway universal > Setări VPN**)	
Aplicații VPN	Aplicații VPN	
VPN Always On	Activați blocarea nativă	VPN Always On
Activarea blocării AppTec	Activarea blocării AppTec	

Samsung / Lebădă puternică			
Tip de conexiune	PPTP	Server	Server
		Aplicații VPN	Aplicații VPN
		Nume utilizator	Nume utilizator
		Parolă	Parolă
		Activați criptarea PPTP	Activați criptarea PPTP
	L2TP / IPSec PSK	Server	Server
		Aplicații VPN	Aplicații VPN
		Cheie IPSec precompartimentată	Cheie IPSec precompartimentată
		Nume utilizator	Nume utilizator
		Parolă	Parolă
		Activați L2TP Secret	Secret L2TP
	IPSec XAuth PSK	Server	Server
		Aplicații VPN	Aplicații VPN
		Identificator IPSec	Identificator IPSec
		Cheie IPSec precompartimentată	Cheie IPSec precompartimentată
		Nume utilizator	Nume utilizator
		Parolă	Parolă
Setări expert	Servere DNS	Servere DNS	
	Redirecționarea rutelor	Redirecționarea rutelor	

Restricții

Aici puteți seta restricțiile, în ceea ce privește gestionarea conexiunii

Permiteți roamingul de date	Permiteți datele mobile în roaming
Forțați roamingul de date	Dacă este activat, roamingul pentru date mobile este activat permanent (nu este recomandat!) Această setare suprascrie setarea "Allow Data Roaming"!
Utilizați serverul proxy http al sistemului	Utilizarea unui server proxy HTTP, care este furnizat de setările sistemului în setări, depinde de rețeaua conectată (WiFi sau APN)

Gestionarea PIM

Gmail Exchange

Info: Această configurare va fi aplicată aplicației Gmail. Deci trebuie să aprobați și să instalați Gmail.

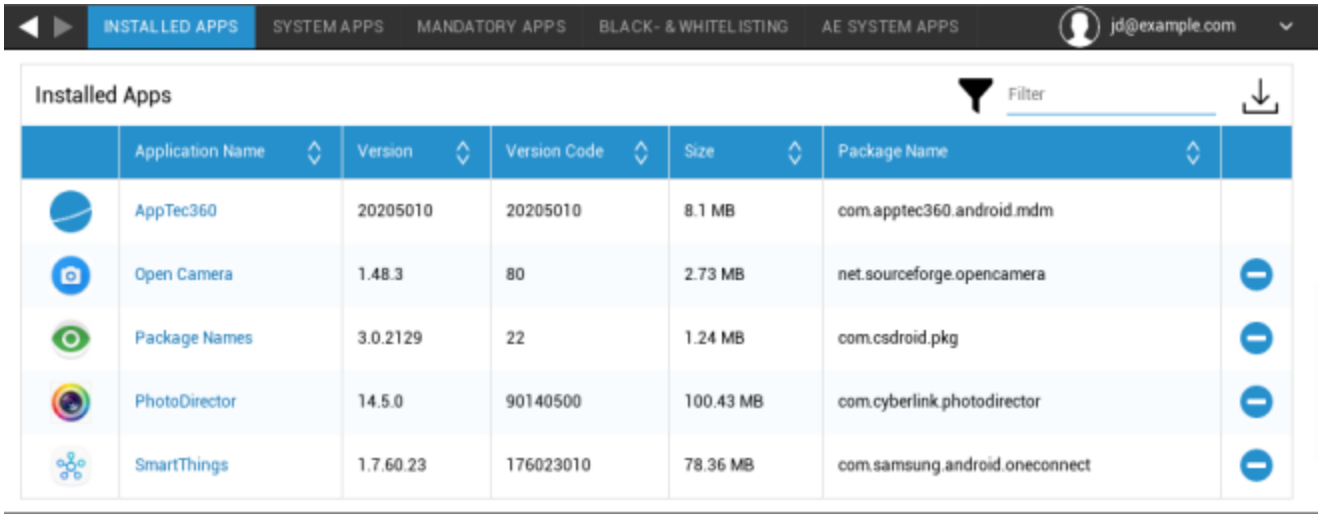
Adresa eMail	Adresa de e-mail a utilizatorului furnizat Vă rugăm să rețineți "Placeholders", pe care le puteți utiliza pentru a lucra cu acreditările și nu efectuați modificări manual pe fiecare dispozitiv Cu un clic pe le puteți afișa pentru tine
Nume gazdă server	Adresa de server a serverelor Exchange
Nume de utilizator	Numele de autentificare pentru dispozitivul respectiv al utilizatorului final, vă rugăm să rețineți și "Placeholders here
Semnătura	Se poate atașa o semnătură (Indicație: Unele dispozitive necesită formatare HTML pentru semnătură)
Numărul de zile anterioare pentru sincronizare	Numărul de zile, care determină momentul în care e-mailurile sunt sincronizate înapoi
Identificatorul dispozitivului	Ein String der die EAS DeviceID enthält. Dies ist Teil des EAS Protokols und wird in einigen Umgebungen benötigt
Utilizați Secure Sockets Layer (SSL)	Utilizați o conexiune SSL
Acceptați toate certificatele	Toate certificatele sunt acceptate. Vă rugăm să selectați această opțiune, dacă Exchange Server utilizează un certificat auto-semnat
Permiteți conturile negestionate	Permiteți utilizatorilor să adauge sau să elimine orice cont Exchange, altul decât contul specificat în această configurație gestionată. Dacă această setare este activată, nu puteți împiedica utilizatorii să adauge alte conturi Exchange la Gmail. De asemenea, nu puteți controla partajarea datelor între alte aplicații și conturile Exchange adăugate de utilizatori. Această setare trebuie activată numai dacă utilizatorii trebuie să mențină mai mult de un cont Exchange de lucru în Gmail.
Certificat de client	Certificat client. Necesar numai dacă serverul dvs. de e-mail se așteaptă ca acesta să fie prezent.

Gestionarea aplicațiilor

Enterprise App Manager

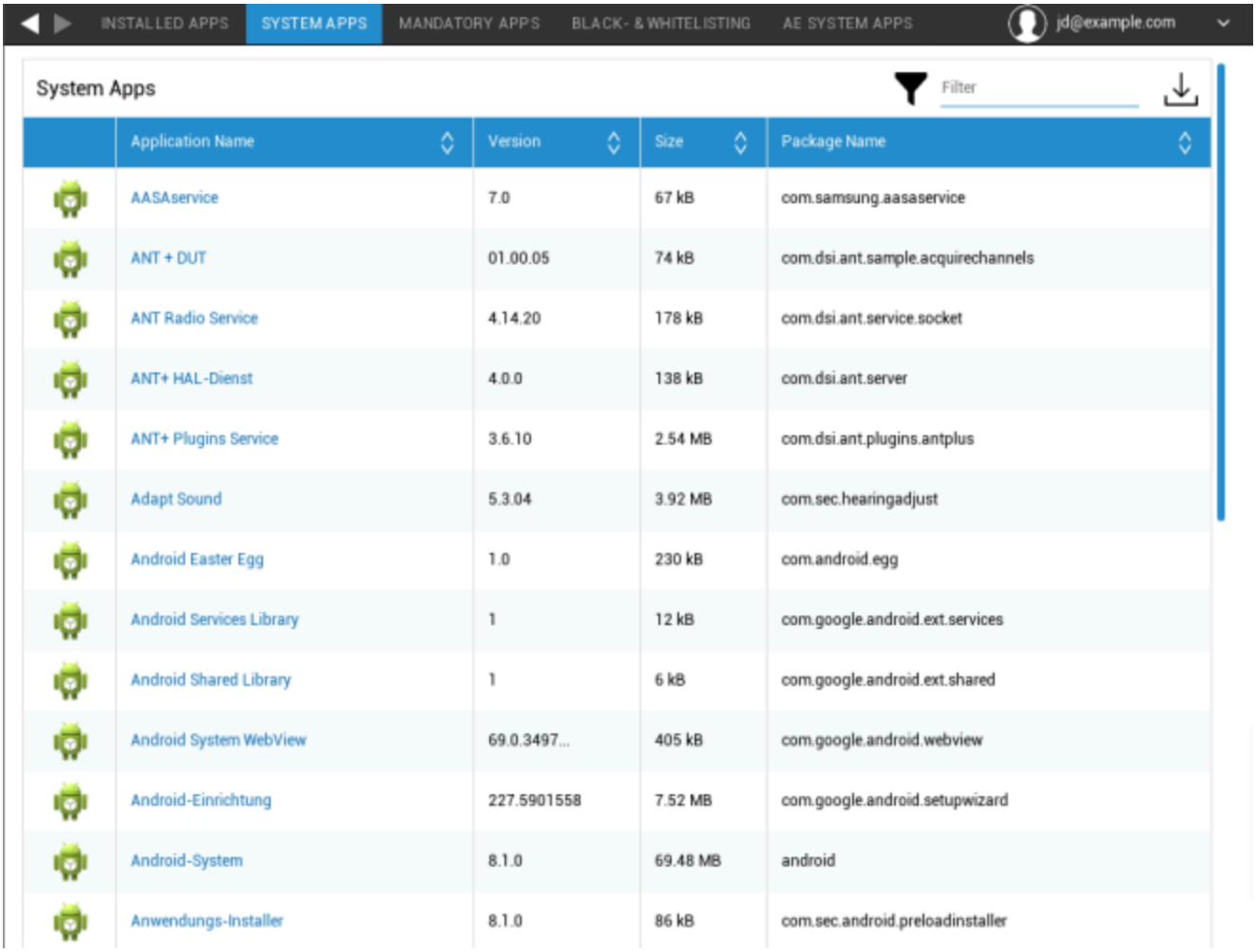
Aplicații instalate (numai la nivel de dispozitiv)

Aici vor fi afișate toate aplicațiile care sunt instalate în container.



Aplicații de sistem (numai la nivel de dispozitiv)

Sub "Aplicații de sistem", toate aplicațiile și serviciile care au fost deja instalate pe dispozitivul utilizatorului final de către producătorul dispozitivului vor fi listate pentru dvs.

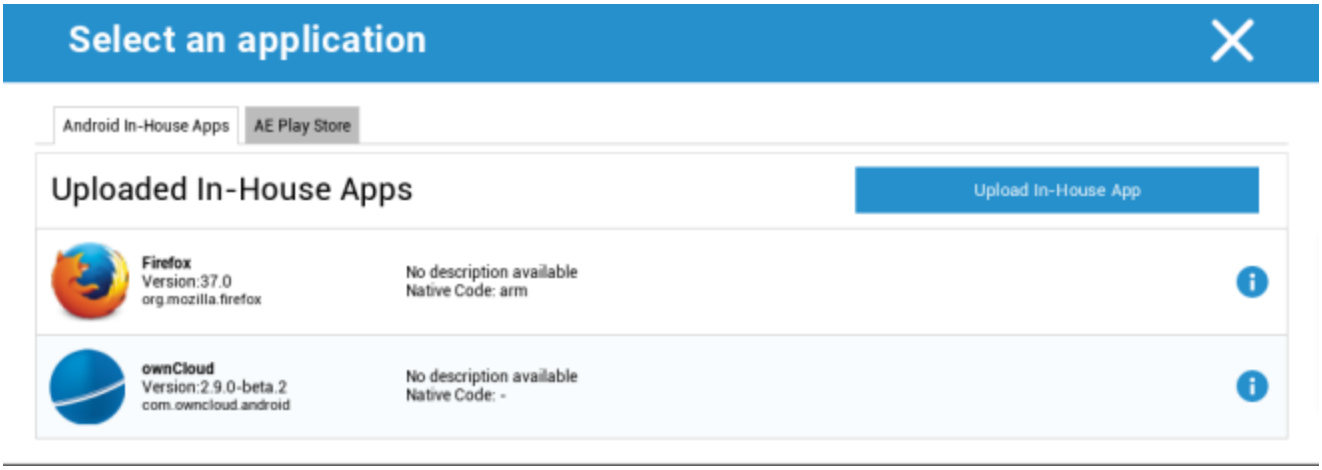


Aplicații obligatorii

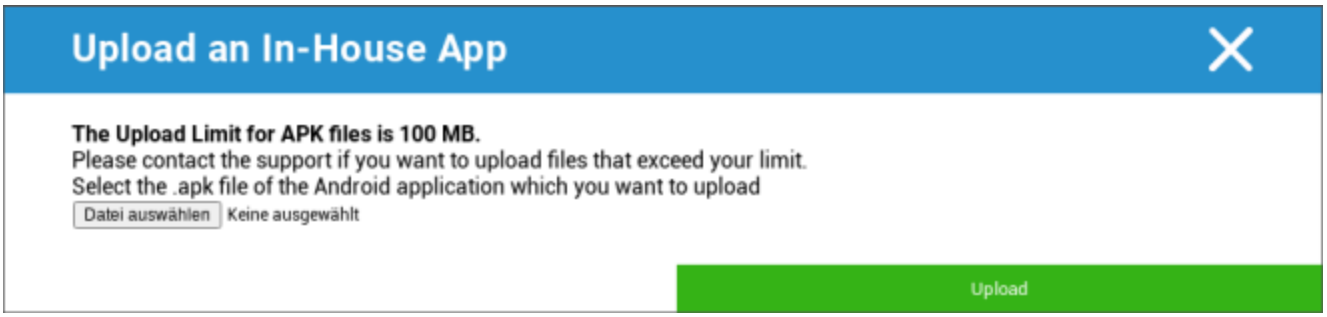
Sub Aplicații obligatorii, puteți stabili aplicațiile obligatorii obligatorii. Utilizatorului i se va solicita în mod continuu să instaleze această aplicație desemnată, dacă este o aplicație InHouse. Aplicațiile Play Store vor fi instalate automat.

Prin intermediul , poate fi definită aplicația obligatorie obligatorie.

Aceasta poate fi o aplicație internă din "Aplicații interne Android", pe care ați încărcat-o în Setări generale.

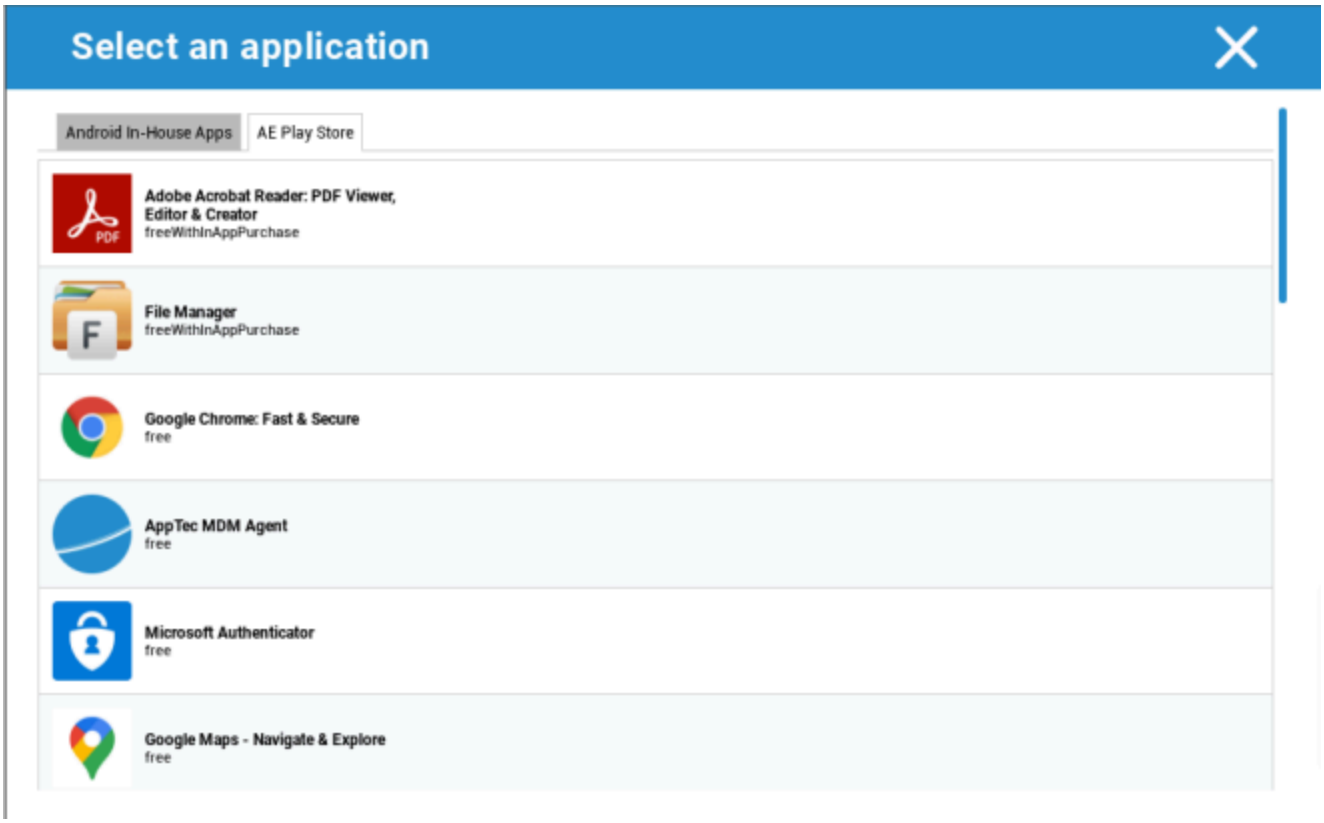


De asemenea, puteți selecta și încărca direct un fișier apk cu "Încărcare aplicație internă".



Dacă instalați o aplicație In-House, veți avea posibilitatea de a activa "Păstrați la zi". Dacă aceasta este activată și ați definit o versiune mai nouă în baza de date a aplicației In-House, aplicația va fi actualizată pe dispozitiv.

Sau poate fi o aplicație "AE Play Store" din Google Work Play Store.



Doar "AE Play Store Apps" aprobate vor fi afișate în această filă.

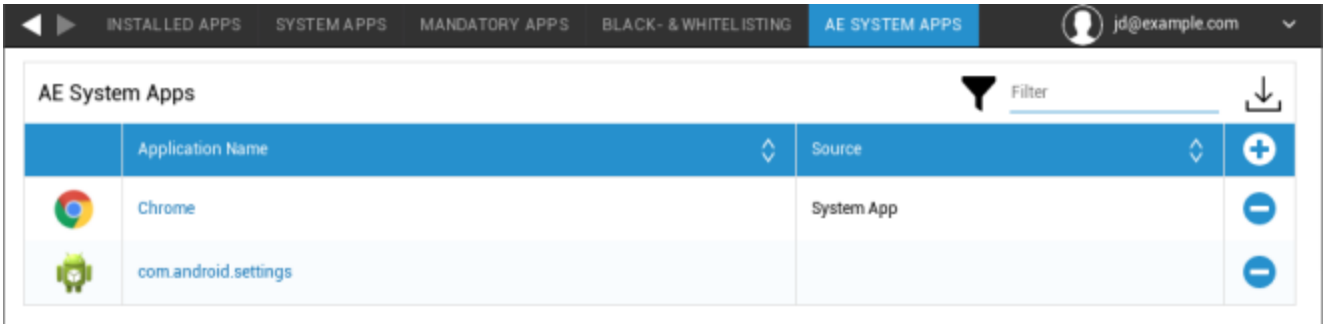
Pentru a aproba o "AE Play Store App", accesați "Setări generale" > "Administrare aplicații" > "AE Play

Store" și adăugați o aplicație prin intermediul butonului care vă va redirecționa către fila "Play Store Apps" (sau puteți merge direct la fila "Play Store Apps").

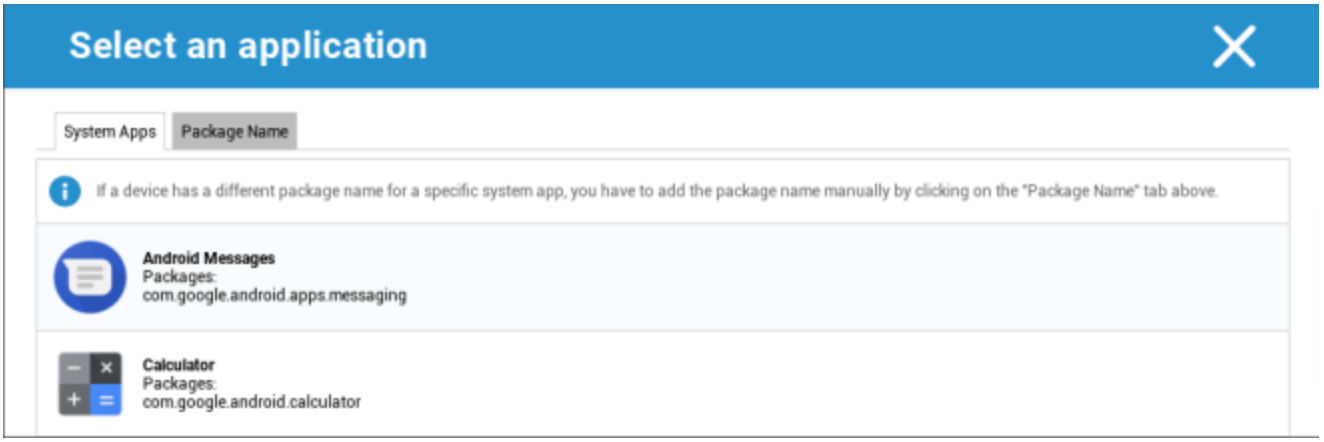
În fila "Aplicații Play Store" puteți căuta aplicații. Când faceți clic pe o aplicație, se deschide pagina aplicației și aici puteți aproba aplicația făcând clic pe "Aprobă".

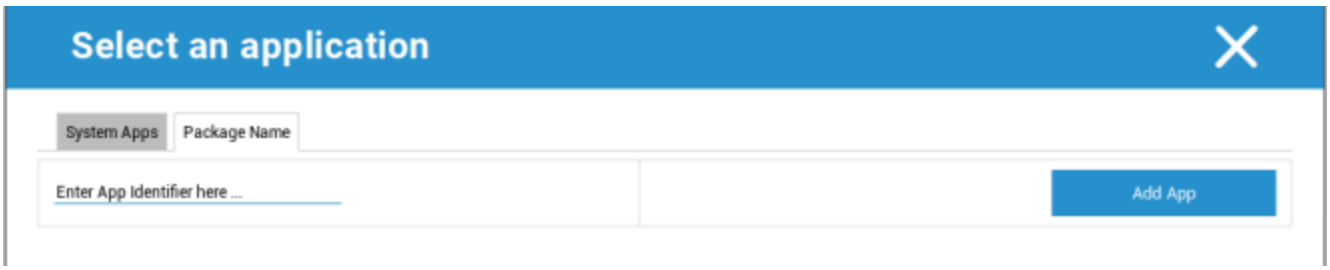
Aplicații de sistem AE

Aici puteți defini o listă care conține aplicații de sistem specifice care ar trebui să fie activate pe dispozitive.



Dacă faceți clic pe buton, puteți alege dintr-o listă de aplicații de sistem posibile furnizate de Google sau puteți introduce direct numele pachetului unei aplicații de sistem care trebuie activată.





Vă rugăm să rețineți că aplicațiile de sistem din lista furnizată de Google sunt doar aplicații care pot fi aplicații de sistem, dar nu trebuie neapărat să fie aplicații de sistem pe dispozitivele dvs.

Cu toate acestea, această listă afectează numai aplicațiile care sunt deja preinstalate.

Adăugarea de aplicații care nu sunt preinstalate pe dispozitivele dvs. nu va afecta dispozitivele, indiferent dacă aplicația este din lista furnizată de Google sau dacă numele pachetului de aplicații este introdus direct.

Restricții și setări

Setări de gestionare a aplicațiilor

Aici puteți configura comportamentul dispozitivului în ceea ce privește actualizările aplicațiilor.

Frecvența verificărilor de actualizare	Specificați intervalul în care clientul AppTec va căuta actualizări pentru aplicații. Valoarea implicită este de 24 de ore.
Prag Wi-Fi	Aplicațiile care sunt mai mari decât dimensiunea specificată vor fi descărcate prin Wi-Fi. Dacă este selectat "Doar Wi-Fi", toate aplicațiile vor fi descărcate prin Wi-Fi.

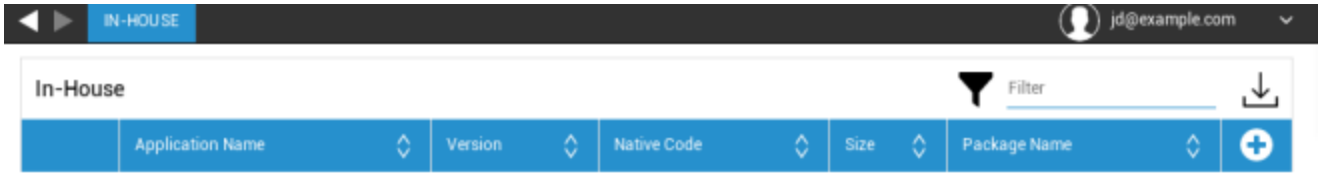
Magazin de aplicații pentru întreprinderi

In-House

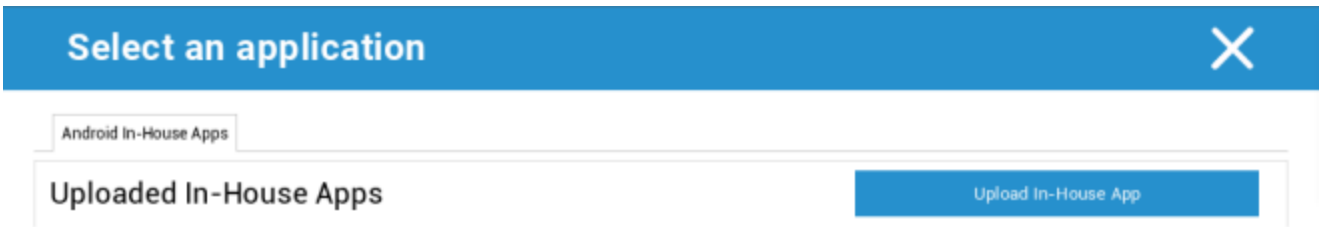
Sub punctul "In-House", puteți încărca și distribui aplicații dezvoltate intern.

Cu ajutorul simbolului, puteți distribui aplicații In-House suplimentare.

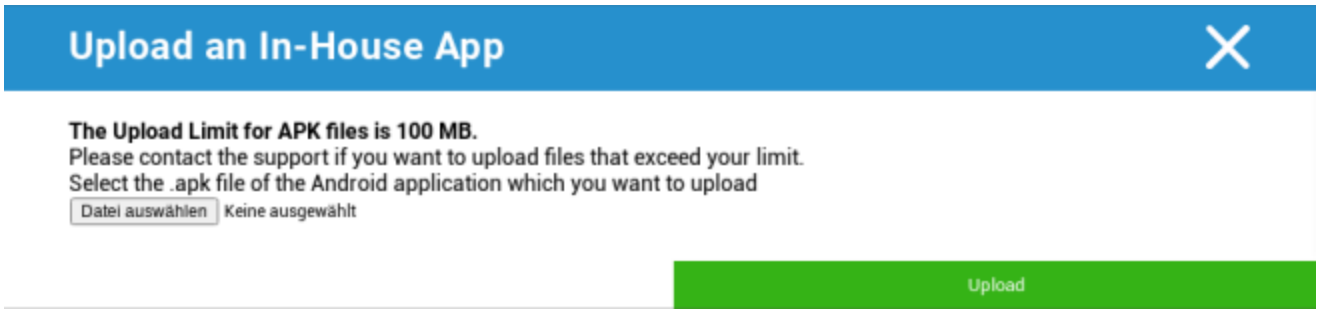
Dacă instalați o aplicație In-House, veți avea posibilitatea de a activa "Păstrați la zi". Dacă aceasta este activată și ați definit o versiune mai nouă în baza de date a aplicației In-House, aplicația va fi actualizată pe dispozitiv.



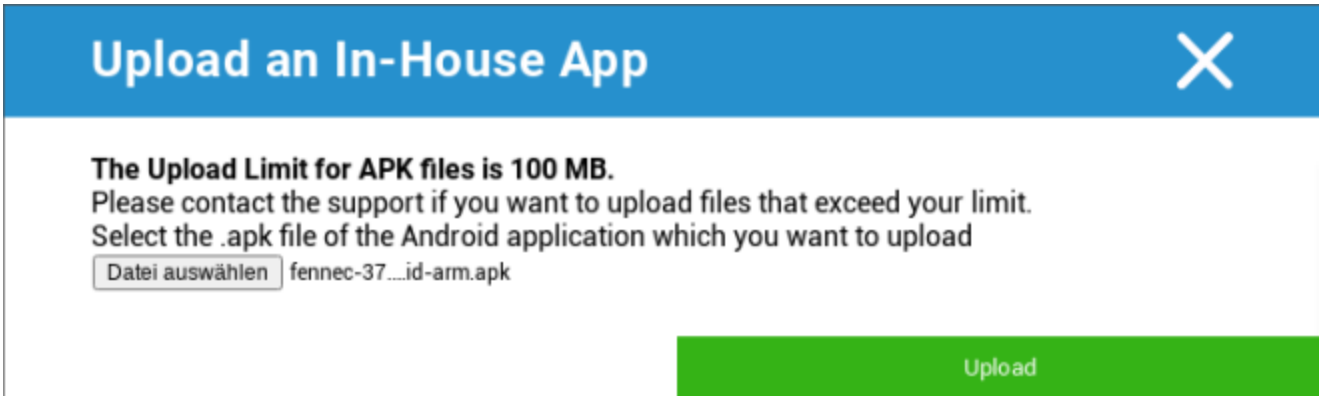
Dacă nu ați distribuit aplicații In-House, veți primi următoarea prezentare generală:



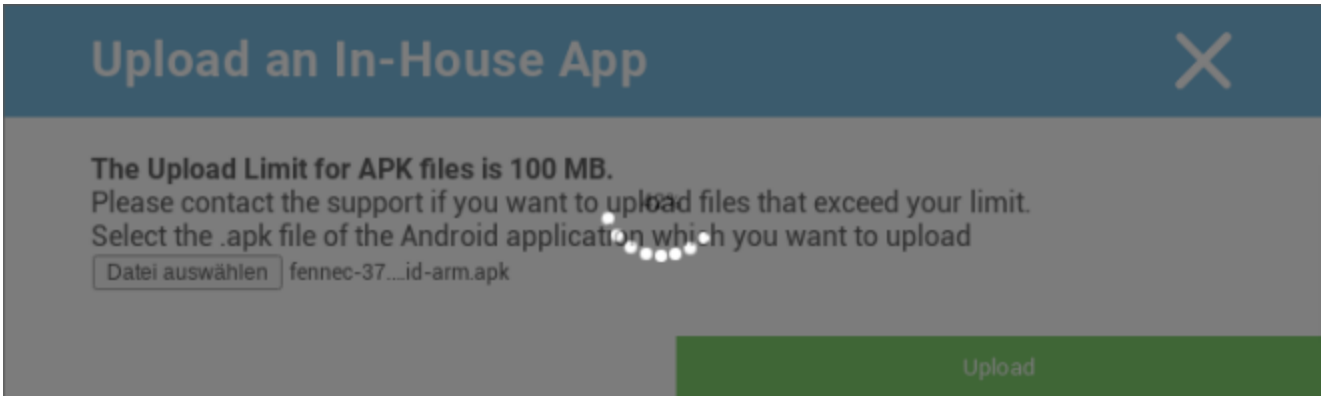
Pentru aceasta, faceți clic pe "Upload In-House App", apoi veți primi următoarea prezentare generală:



Acum, alegeți cu "Căutare..." un fișier .apk și apoi faceți clic pe "Încărcare".



Aplicația dvs. va fi acum încărcată, în mijlocul cercului veți vedea un indicator procentual, care arată cât de mult din aplicație a fost deja încărcată.



În cazul în care încărcarea aplicației dvs. In-House a avut succes, puteți găsi aplicația încărcată în Catalogul de aplicații.

Utilizatorul are acum opțiunea de a vedea și instala această aplicație în AppTec Store pe dispozitivul utilizatorului final, la categoria "In-House".

Datorită faptului că aceasta nu implică o aplicație Google PlayStore, utilizatorul nu are nevoie de un ID Google stocat pe dispozitivul utilizatorului final respectiv.

Magazin Play pentru întreprinderi

AE Magazin Play

Aici puteți adăuga aplicații la Android Enterprise Playstore. Vă rugăm să rețineți că trebuie să aprobați aplicațiile cu ajutorul contului de administrator AE înainte de a le putea adăuga.

Pentru aprobarea unei aplicații, vă rugăm să consultați instrucțiunile din Aplicații obligatorii.

Gestionarea conținutului

ContentBox

Aici puteți activa ContentBox.

De îndată ce comutați "Enable ContentBox" la "On", o aplicație ContentBox separată va fi instalată automat pe dispozitivul utilizatorului final.

Browser securizat

Aici puteți configura setările pentru AppTec Secure Browser.

De îndată ce comutați secțiunea "Browser securizat" la "Activat", o aplicație browser separată va fi instalată automat pe dispozitivul utilizatorului final.

Solicitare parolă	Cereți utilizatorului să configureze și să utilizeze o parolă pentru a accesa browserul.
Lungimea minimă necesară a parolei	Setați numărul necesar de caractere pentru parolă
Calitatea parolei necesare	Setați calitatea parolei necesare
Restricționați descărcările / Deschideți în	
Restricționarea încărcărilor	
Încărcați lista albă	O listă de URL-uri pentru care încărcarea va fi permisă întotdeauna.
Permiteți copierea	Permiteți copierea, tăierea sau partajarea textului din paginile web.
Permiteți capturarea ecranului	Permiteți capturarea de capturi de ecran.
Frecvența curățării datelor	Selectați frecvența cu care TOATE datele utilizatorului (istoric, cache etc.) ar trebui eliminate automat.
Marcaje companie	Marcajele vor apărea în folderul "Marcaje companie" din marcajele browserului. Acestea nu sunt editabile de către utilizator.
Ascundeți bara de adrese	
Lista albă în browser (fără Universal Gateway)	Activează lista albă URL pe partea de client. • Marcajele companiei sunt întotdeauna pe lista albă • Suportat numai pentru 100 de URL-uri • Vă rugăm să utilizați Universal Gateway pentru Black- și Whitelisting nelimitat
URL-uri pe lista albă	O listă de URL-uri permise.
Liste negre și albe bazate pe gateway	Lista neagră are următoarele cerințe:

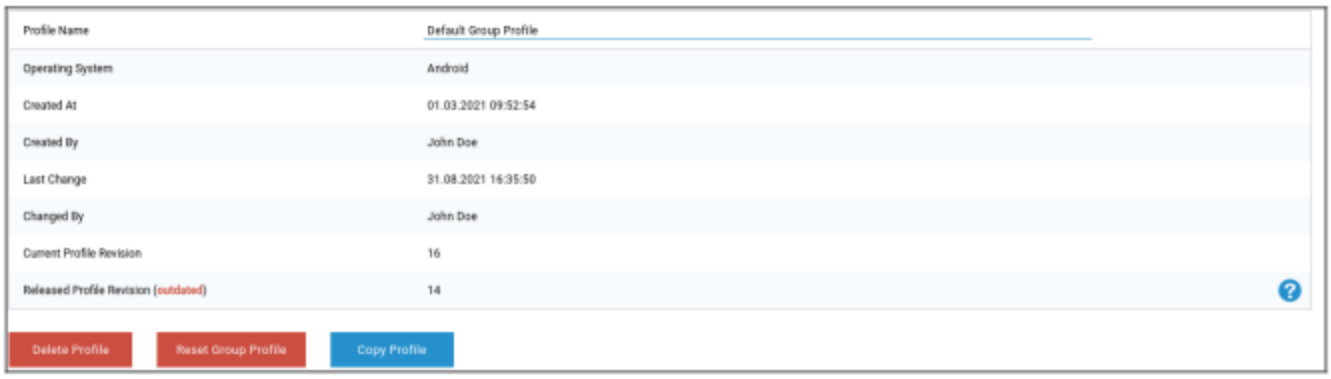
	• Un Gateway universal AppTec funcțional ("Setări generale" → "Gateway universal") • O configurație VPN funcțională cu un server DNS specificat ("Setări generale" → "Universal Gateway" → "Setări VPN") • O configurare a listei negre ("Setări generale" → "Universal Gateway" → "Lista neagră a domeniului") • O conexiune VPN validă în profil ("Gestionarea conexiunii" → "VPN")

Configurare Android

Generalități

Prezentare generală a profilului grupului (numai la nivel de grup)

Atunci când deschideți un profil de grup, veți obține o prezentare generală rapidă a profilului.



Nume profil	Numele profilului (poate fi modificat aici)
Sistem de operare	Sistemul de operare pentru care este creat profilul
Creat la	Momentul creației
Creat de	Creatorul profilului
Ultima schimbare	Ora ultimei modificări a profilului
Schimbat de	Contul care a efectuat ultimele modificări
Revizuirea actuală a profilului	Revizuirea stării profilului salvat
Revizuire profil eliberată	Revizuirea profilului atribuit ("Atribuie acum"). Dacă eticheta afișează "(învechit)" în spatele textului, înseamnă că ați salvat profilul, dar nu l-ați atribuit încă, astfel încât dispozitivele vor primi în continuare o versiune mai veche.

Prezentare generală a dispozitivului (numai la nivel de dispozitiv)

Dacă vă aflați pe un dispozitiv, veți primi o recapitulare generală a dispozitivului selectat, care conține următoarele informații:

Numele dispozitivului	Numele dispozitivului
Ultima locație cunoscută	Ultimele coordonate GPS cunoscute
Număr de telefon	Număr de telefon
Aplicații obligatorii atribuite	Numărul de aplicații obligatorii alocate
Versiunea sistemului de operare	Versiunea sistemului de operare al dispozitivului
Sistem de operare	Sistem de operare (Android / iOS / Windows Phone)
Numărul de serie	Numărul de serie al dispozitivului
Proprietatea dispozitivului	Dispozitiv corporativ sau privat
Tip dispozitiv	Telefon sau tabletă
Înrădăcinat	Stare, indicând dacă dispozitivul a fost rădăcinat
Conform	În conformitate cu liniile directoare
Adresa IP	Adresa IP
Văzut ultima dată	Momentul în care dispozitivul s-a conectat ultima dată la AppTec
Ultimul impuls	Moment în timp, când serverul a trimis un push către dispozitiv
Atribuirea utilizatorului	Un dropdown pentru a atribui dispozitivul altui utilizator

Revizuirea configurației (numai la nivel de dispozitiv)

Aici veți primi o prezentare generală a profilului de grup care este atribuit dispozitivului.

Dacă faceți clic pe profilul grupului, veți accesa direct profilul și veți putea efectua setările.

Cu ajutorul simbolului, puteți readuce aplicațiile alocate la setările profilului de grup.

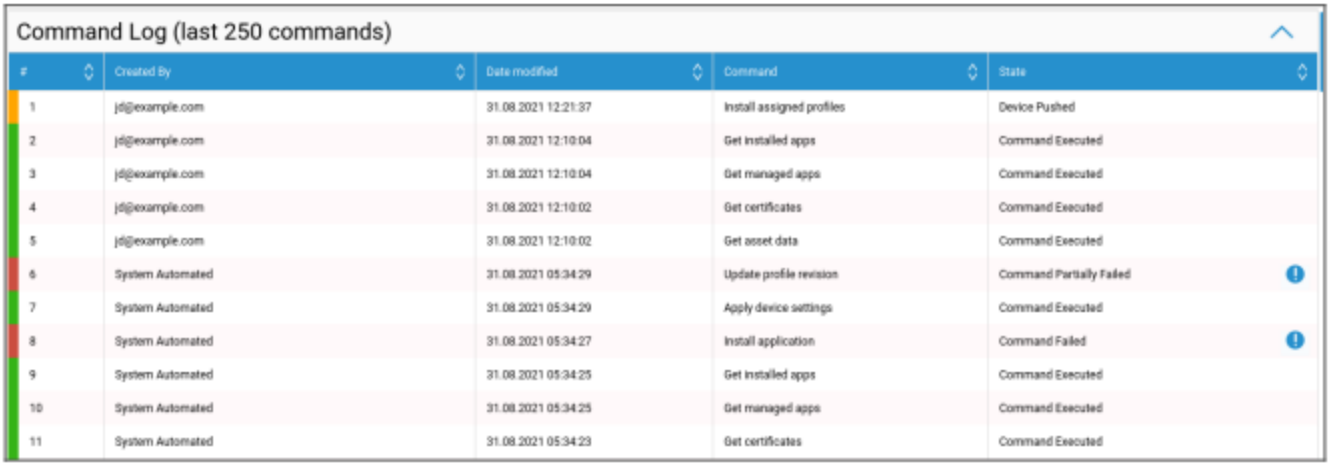
Cu ajutorul simbolului, puteți reseta profilul dispozitivului pentru a nu avea niciun fel de setări.

"Newer Revision available" indică faptul că profilul grupului a fost modificat și salvat, dar nu a fost atribuit. Profilul de grup trebuie să fie atribuit cu "Assign now" la nivel de grup pentru a aplica modificările dispozitivelor.

Jurnalul dispozitivului (numai la nivel de dispozitiv)

Jurnal de comandă

Aici puteți vedea ce comenzi au fost emise pentru dispozitiv și care este starea lor.



Comenzile create de "System Automated" sunt create automat de sistem.

Stări posibile ale comenzii

Dispozitiv împins	O solicitare push a fost trimisă către serviciul push (de exemplu, APNS) pentru a indica dispozitivului să se conecteze din nou la serverul EMM.
Comandă creată	Comanda a fost creată în sistem.
Comandă trimisă	Comanda a fost trimisă către dispozitiv după ce acesta s-a conectat la server.
Comandă executată	Comanda a fost executată cu succes.
Comandă eșuată	Comanda a eșuat. *
Comandă eșuată parțial	În funcție de sistemul de operare al dispozitivului, unele comenzi pot fi grupate împreună. În acest caz, unele părți ale acestui grup de comandă au eșuat. *
Comandă executată, eventual eșuată	Comanda a fost executată, dar poate că nu a fost.
Comanda Repushed	Comanda a fost respinsă de un utilizator.
Aruncată	Comanda a fost eliminată. De exemplu, pentru că a fost înlocuită de o altă comandă sau pentru că dispozitivul a fost înrolat din nou și comenzile vechi au fost eliminate

*Dacă există un semn al exclamării în spatele mesajului, puteți obține mai multe informații trecând cu cursorul peste pictogramă.

Setări dispozitiv

Configurare client

Aici puteți efectua următoarele configurații pe dispozitivul Android:

Mesaj de avertizare după dezactivarea gestionării dispozitivelor	Mesaj de avertizare stabilit după dezactivarea gestionării dispozitivelor
Timp de neconformitate	Limita de timp după care se va efectua "Acțiunea de executare după conformitate", dacă dispozitivul nu este conform. Min. 1 minut Max. 24 de ore
Acțiune de punere în aplicare după expirarea termenului de conformitate	Acțiunea care trebuie întreprinsă imediat ce un dispozitiv devine neconform. • nu faceți nimic = nicio acțiune • Dispozitiv de blocare = dispozitiv de blocare • Ștergere dispozitiv = dispozitivul va fi restaurat la setările din fabrică
Frecvența colectării datelor	Frecvența cu care trebuie colectate informațiile despre dispozitiv/GPS
Frecvența bătăilor inimii dispozitivului	Intervalul în care dispozitivul trebuie să contacteze serverul AppTec360 Min. 1 minut Max. 24 de ore
Activați actualizările locației	Dacă este activat, dispozitivul trimite actualizări ale locației către serverul AppTec360
Locație Ora actualizării	Determină în ce intervale de timp dispozitivul trimite actualizări ale locației către AppTec
Utilizați Google Location Accuracy pentru actualizarea locației	Dacă este activată, precizia locației Google (cunoscută anterior ca locație de rețea) va fi utilizată pentru actualizările locației (dacă aceasta a fost dezactivată la "Restricții", atunci această setare nu va afecta nimic)
Utilizați locația GPS pentru actualizarea locației	Dacă este activat, GPS-ul va fi utilizat pentru actualizarea locației

Permiteți locații fictive (false)	Permite falsificarea informațiilor de localizare prin intermediul aplicațiilor terță parte
Acțiune de pierdere a conexiunii	Vă permite să setați o anumită acțiune care va fi efectuată după un anumit număr de bătăi de inimă eșuate
Modul de aplicare a politicii	Definește gradul de agresivitate cu care clientul AppTec360 solicită utilizatorului să efectueze anumite acțiuni care necesită introducerea datelor de către utilizator. Interval (implicit) = solicită în intervale, astfel încât utilizatorul să poată pune acest lucru în fundal pentru un timp. Nicio alertă = nicio fereastră pop-up pentru orice interacțiune necesară. Trebuie să deschideți manual clientul AppTec360 pentru a verifica dacă există o acțiune necesară Alertă constantă = Utilizatorul poate efectua numai acțiunea necesară. Clientul AppTec360 se va impune în prim-plan dacă utilizatorul încearcă să îl evite
Blocarea versiunii AppTec360	Vă permite să definiți o versiune a Clientului AppTec360 care este versiunea maximă la care se actualizează clientul.

Wallpaper

Aici puteți defini un tapet personalizat.

"Specify a Color" vă permite să definiți o culoare în format hexazecimal (de exemplu, #000000). Numai valorile hexagonale sunt permise.

"Setați imaginea ca fundal" vă permite să încărcați o imagine. Vă rugăm să fiți conștienți de faptul că diferite dispozitive cu diferite lansatoare și versiuni ale sistemului de operare funcționează diferit. Nu există o linie directoare generală pentru dimensiune și raport, deoarece acestea depind de dispozitiv.

Utilizați JPG (sau JPEG) sau PNG pentru formatul de fișier.

Gestionarea activelor (numai la nivel de dispozitiv)

Gestionarea activelor

Informații despre dispozitiv

Model	**Denumirea modelului dispozitivului**
Sistem de operare	SO
Versiunea sistemului de operare	Versiunea sistemului de operare
Sprijin AE	Suport pentru Android Enterprise (container și complet gestionat)
Numărul de serie	Numărul de serie
Numele dispozitivului	Numele dispozitivului
Starea bateriei	Starea bateriei
Memorie liberă / totală	Memorie liberă / totală
Samsung KNOX	Nivelul API Samsung KNOX
Card SD disponibil	Card SD disponibil
Card SD emulat	Card SD emulat
Card SD detașabil	Card SD detașabil
SD Memorie liberă / totală	SD Liber / Total memorie card SD

Wi-Fi

Adresa IP	Adresa IP a dispozitivului
WiFi MAC	Adresa MAC WiFi

Celulare

Statut	Stare (cartela SIM instalată)
Număr de telefon	Număr de telefon
Roaming (voce / date)	Roaming pentru voce / date
Starea de roaming	Starea curentă de roaming
Adresa IP	Adresa IP
Operator/Carrier	Operator/Carrier
Tehnologie celulară	Tehnologie celulară
IMEI	Numărul IMEI
ICCID	Acesta este ID-ul cartelei SIM, de multe ori și un Smartcard sau o cartelă cu circuit integrat (ICC)
IMSI	Identitatea internațională a abonatului mobil (IMSI) oferă în rețelele mobile GSM și UMTS o identificare definitivă a utilizatorilor rețelei IMSI este compus din maximum 15 cifre și este configurat în felul următor: • Codul țării mobile (MCC), 3 cifre • Codul rețelei mobile (MNC), 2 sau 3 cifre • Numărul de identificare a abonatului mobil (MSIN), 1-10 cifre
Actual MCC/MNC	Consultați "SIM MCC/MNC"
SIM MCC/MNC	Codul țării mobile este un identificator de țară stabilit de ITU conform standardului E.212. Acesta funcționează împreună cu codul rețelei mobile (MNC) pentru identificarea rețelei mobile. Înseamnă țara/codul rețelei mobile a cartelei SIM. Dacă vă deplasați într-o altă rețea mobilă, atunci, în mod logic, "MCC/MNC curent" și "SIM MCC/MNC" vor fi diferite.

Bluetooth

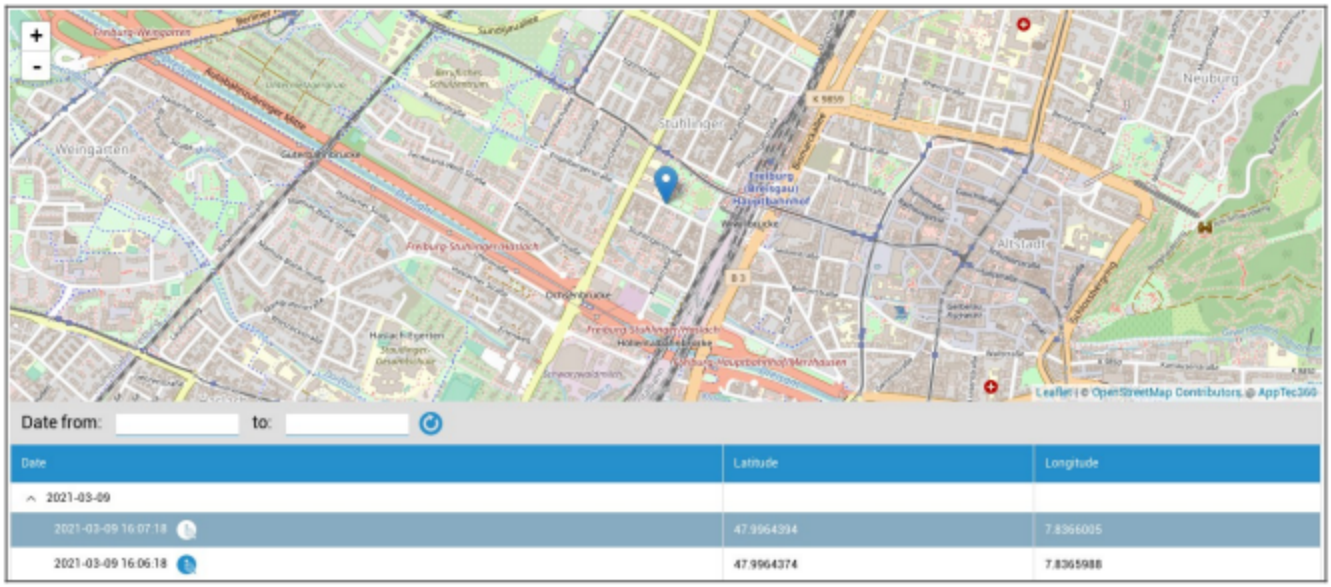
Bluetooth MAC	Adresa MAC Bluetooth

Managementul securității

Anti-furt (numai la nivel de dispozitiv)

Informații GPS (numai la nivelul dispozitivului)

Aici puteți stabili locația curentă/ultima a dispozitivului. Localizarea poate fi protejată cu una sau chiar două parole - Consultați: Setări generale - Confidențialitate - Acces GPS



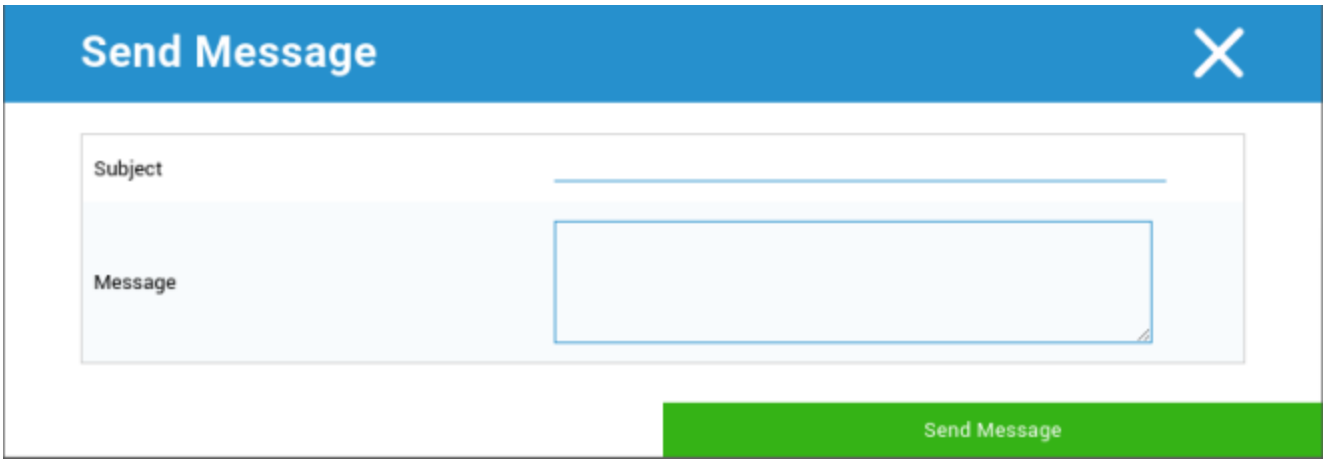
Ștergere și blocare (numai la nivel de dispozitiv)

Sub "Ștergere și blocare", puteți efectua următoarele trei acțiuni:

Ștergere completă	Dispozitivul este readus la setările din fabrică (datele corporative, precum și cele personale sunt șterse)
Ștergere Enterprise	Doar datele corporative sunt eliminate de pe dispozitivul utilizatorului final (toate aplicațiile, datele, etc. care au fost furnizate de AppTec360)
Ecran de blocare	Blocarea ecranului este activată, este suficient să deblocați dispozitivul cu ajutorul parolei dispozitivului/PIN

Mesaj (numai la nivel de dispozitiv)

Puteți completa subiectul și un mesaj și să îl trimiteți unui dispozitiv al utilizatorului final. Acest mesaj va fi afișat în clientul AppTec360.



Configurația de securitate

Codul de acces

Sub "Cod de acces" puteți trimite o parolă pentru dispozitiv, fiind disponibile următoarele opțiuni de setare

Lungimea minimă a parolei	Stabilește numărul minim de simboluri pe care trebuie să le aibă o parolă
Calitatea parolei	Puterea parolei Nespecificat = nespecificat Fiecare parolă este ok = fiecare parolă este acceptabilă cel puțin caractere numerice = trebuie să conțină cel puțin caractere numerice cel puțin caractere complexe = trebuie să conțină cel puțin caractere speciale cel puțin caractere alfanumerice = trebuie să conțină cel puțin caractere alfanumerice cel puțin caractere alfabetice = trebuie să conțină cel puțin caractere alfabetice
Timp maxim de inactivitate blocare	Timeout maxim al ecranului. Aceasta configurează doar valoarea maximă care poate fi selectată de utilizator
Minimum de litere minuscule necesare în parolă	Minimum de litere minuscule necesare în parolă
Minimum de litere majuscule necesare în parolă	Minimum de litere majuscule necesare în parolă
Numărul minim de caractere din afara literelor necesare în parolă	Numărul minim de caractere din afara literelor necesare în parolă
Minimum de cifre numerice necesare în parolă	Minimum de cifre numerice necesare în parolă
Simboluri minime necesare în parolă	Simboluri minime necesare în parolă
Timpul de expirare a parolei	Se stabilește, interval de timp după care parola expiră și trebuie emisă o nouă parolă
Restricționarea istoricului parolelor	Numărul de parole utilizate anterior care nu sunt permise
Numărul maxim de încercări de parole eșuate	Stabilește de câte ori o parolă poate fi introdusă incorect, înainte de a se efectua o ștergere completă a dispozitivului

Criptare

În acest punct, puteți cripta memoria internă a dispozitivului, precum și memoria cardului SD.

Cereți criptarea stocării	Dacă această setare este activată, memoria dispozitivului va fi criptată, atâta timp cât dispozitivul acceptă această funcționalitate. Odată ce memoria dispozitivului a fost criptată pentru prima dată, nu mai este posibilă desecretizarea acesteia. De asemenea, Politica privind parola va fi schimbată automat la 6 simboluri alfanumerice
Necesită criptarea cardului SD	Această setare se aplică numai dispozitivelor Samsung! Dacă această setare este activată, cardul SD extern poate fi criptat și poate fi decriptat manual numai pe dispozitivul utilizatorului final. De asemenea, Politica privind parola va fi schimbată automat la 6 simboluri alfanumerice

AntiVirus

Activarea AntiVirus va instala Ikarus pe dispozitive. Vă rugăm să rețineți că acest lucru necesită o licență separată care poate fi introdusă în Setări generale → Gestionare aplicații → Aplicații terțe.

Scanare automată	Definește dacă Ikarus scanează sau nu automat și cât de des efectuează această scanare Activarea "Scanare automată completă" va efectua o scanare completă. În caz contrar, va fi efectuată o scanare rapidă
Actualizări automate	Activează actualizările automate ale bazei de date a virușilor și stabilește frecvența acestora
Protecția aplicațiilor	Permite scanarea aplicațiilor în plus față de scanarea obișnuită care scanează doar fișierele
Protecția cardului SD	Activează protecția cardului SD. Fără aceasta, scanarea este limitată la spațiul de stocare local
Actualizare numai Wi-Fi	Limitează actualizarea la Wi-Fi

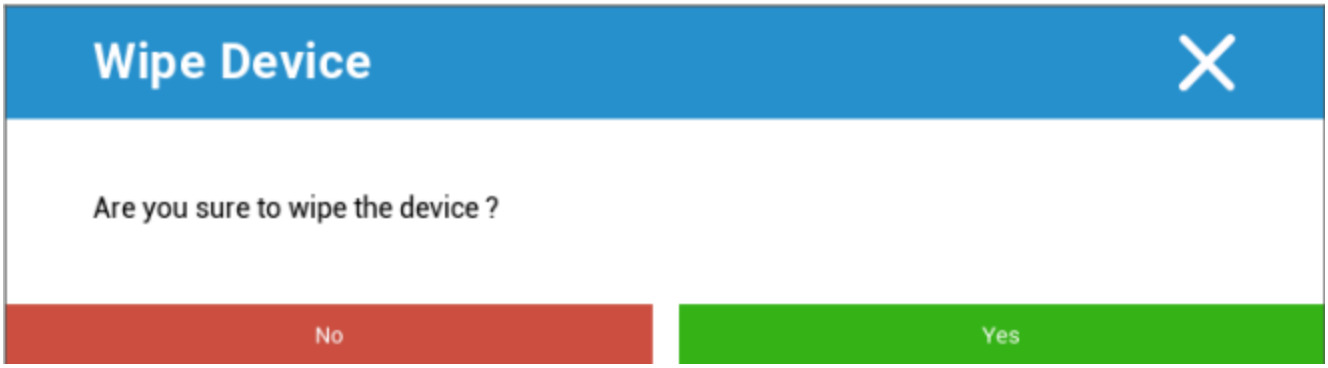
Sfârșitul duratei de viață (numai la nivel de dispozitiv)

Ștergere (numai la nivel de dispozitiv)

Sub "Ștergere", puteți readuce dispozitivul la setările din fabrică. Aici, atât datele corporative, cât și cele private vor fi șterse de pe dispozitivul utilizatorului final.

Cu un clic pe "Simbolul minus" ar trebui să primiți următorul mesaj

Ștergeți și cardul SD?	Memoria cardului SD va fi, de asemenea, ștearsă



Cu "Da" puteți efectua ștergerea.

Sub "Raport ștergere" pot fi afișate următoarele elemente

Șters de	Istoricul persoanei care a efectuat ștergerea
Data	Data
Statut	Stare (de exemplu, dacă ștergerea a fost efectuată cu succes)

Setări de restricționare

Restricții

Aici, pot fi restricționate și blocate o varietate de lucruri.

Activați camera	Permiteți utilizarea camerei
Forțați sincronizarea automată	Se referă la interfața "Sync" Pornit = sincronizarea este activată permanent Oprit = sincronizarea este dezactivată permanent Alegerea utilizatorului = selectat de către utilizator
Forța Bluetooth	Pornit = Bluetooth este activat permanent Oprit = Bluetooth este dezactivat permanent Alegerea utilizatorului = selectat de către utilizator
Forța GPS	Pornit = GPS-ul este activat permanent Oprit = GPS este dezactivat permanent Alegerea utilizatorului = selectat de către utilizator
Forțați acuratețea locației Google	On = Localizare permanentă pe internet Oprit = Dezactivarea permanentă a localizării pe internet Alegerea utilizatorului = selectat de către utilizator

Pentru dispozitivele Samsung cu interfața KNOX 1.0 sau superioară, sunt disponibile următoarele opțiuni de configurare.

Permiteți cardul SD	Permiteți cardul SD
Permiteți scrierea pe cardul SD	Permiteți "scrierea" pe cardul SD
Permiteți capturarea ecranului	Permiteți capturarea ecranului
Permiteți Clipboard	Permiteți clipboard
Copierea de rezervă a setărilor și a datelor aplicației în Google Cloud	Oprit = dezactivarea Google Backup Activat = activați Google Backup Alegerea utilizatorului = selectat de către utilizator
Permite depanarea USB	Permite depanarea USB (este utilizată, de exemplu, pentru crearea jurnalelor dispozitivului (ADB))
Permiteți Google Crash Report	Permiteți ca Google Crash Report să fie trimis din aplicații
Permiteți resetarea din fabrică	Permite utilizatorului să readucă dispozitivul la setările din fabrică
Permiteți actualizarea OTA	Permiteți actualizările "prin aer"
Permiteți stocare gazdă USB	Dacă este activată, memoria USB, sub forma unui HD sau a unui cititor de carduri SD, poate fi conectată
Permiteți USB Media Player (MTP,PTP)	Permiteți USB Media Player (MTP,PTP)
Permiteți microfonul	Activat = permite microfonul pentru aplicații terță parte Dezactivat = blocarea microfonului pentru aplicațiile terță parte Alegerea utilizatorului = utilizatorii pot selecta, dacă aplicația terță parte are acces la microfon
Permiteți NFC (Near Field Communication)	Permiteți NFC
Permiteți surse necunoscute (APK Sideloading)	Dacă este activată, este permisă încărcarea laterală a aplicațiilor (fișiere APK). Odată ce această setare este dezactivată, utilizatorul trebuie să o activeze manual atunci când permiteți din nou instalarea APK-urilor din surse necunoscute.
Permiteți crearea de utilizatori	Permite crearea de utilizatori multipli

Proprietar dispozitiv AE

(Dispozitivul trebuie să fie în modul Android Enterprise Device Owner) Se recomandă crearea dispozitivelor ca dispozitive "Android Enterprise" și nu ca dispozitive "Android".

Securitate	
Interziceți locația de partajare	Specifică dacă unui utilizator nu i se permite să activeze partajarea locației.
Interziceți Safe Boot	Specifică dacă utilizatorului nu i se permite să repornească dispozitivul în modul de pornire sigură.
Nu permite resetarea rețelei	Specifică dacă unui utilizator nu i se permite să reseteze setările de rețea din Setări.
Nu permite resetarea din fabrică	Specifică dacă unui utilizator îi este interzisă resetarea dispozitivului.
Activează ADB	Permite conectarea la un PC prin ADB
Dezactivați cheia de protecție	Dezactivează Keyguard
Proprietar dispozitiv Informații privind ecranul de blocare	Setează informațiile despre proprietarul dispozitivului care urmează să fie afișate pe ecranul de blocare.
Aplicarea conformității	Mode Prompt User - Utilizatorul va fi rugat să efectueze acțiunile necesare. Modul Lock-Down Container - Ascundeți toate aplicațiile până când toate cerințele sunt îndeplinite

Gestionarea aplicațiilor	
Permiteți legarea aplicațiilor între profiluri	Permite aplicațiilor din profilul părinte să gestioneze linkurile web din profilul gestionat.
Interziceți controlul aplicațiilor	Specifică dacă unui utilizator nu i se permite să modifice aplicații în Setări sau lansatoare.
Interziceți instalarea aplicației	Specifică dacă unui utilizator îi este interzisă instalarea de aplicații.
Interziceți dezinstalarea aplicațiilor	Specifică dacă unui utilizator nu i se permite să dezinstaleze aplicații.
Politica de autorizare în timpul rulării	Specifică modul în care vor fi gestionate noile cereri de permisiune din partea aplicațiilor.
Permiteți surse necunoscute	Dacă este activată, utilizatorii pot încărca aplicații prin instalarea unui fișier .apk.

Conectivitate	
Interziceți configurarea rețelei mobile	Specifică dacă unui utilizator îi este interzisă configurarea rețelelor mobile.
Interziceți configurația Tethering	Specifică dacă unui utilizator nu i se permite să configureze Tethering și hotspoturi portabile.
Interziceți configurația VPN	Specifică dacă unui utilizator îi este interzisă configurarea unui VPN.
Interziceți configurarea Wifi	Specifică dacă unui utilizator nu i se permite să schimbe punctele de acces WiFi.
Interzice ieșirea fasciculului NFC	Specifică dacă utilizatorului nu i se permite să utilizeze NFC pentru a transmite date din aplicații.
Blocare configurare WiFi	Această setare controlează dacă configurațiile WiFi create de o aplicație a proprietarului dispozitivului ar trebui să fie blocate (adică să fie editabile sau detașabile numai de aplicația proprietarului dispozitivului, nu și de aplicația Setări).
Activarea roamingului de date	Activează roamingul de date

Bluetooth	
Interziceți Bluetooth	Specifică dacă bluetooth nu este permis pe dispozitiv. Necesită Android 8.0
Interziceți partajarea Bluetooth	Specifică dacă partajarea bluetooth de ieșire nu este permisă pe dispozitiv. Necesită Android 8.0
Interziceți configurarea Bluetooth	Specifică dacă unui utilizator îi este interzisă configurarea bluetooth.

Gestionarea conturilor	
Interzice adăugarea profilului gestionat	Specifică dacă unui utilizator nu i se permite să adauge profiluri gestionate. Necesită Android 8.0
Interzicerea adăugării de utilizatori	Specifică dacă unui utilizator îi este interzis să adauge noi utilizatori.
Interziceți eliminarea profilului gestionat	Specifică dacă profilurile gestionate ale acestui utilizator pot fi eliminate, altfel decât de către proprietarul profilului său. Necesită Android 8.0
Interzicerea modificării contului	Specifică dacă unui utilizator îi este interzis să adauge și să elimine conturi, cu excepția cazului în care acestea sunt adăugate programatic de Authenticator.

Telefonie	
Interzicerea apelurilor de ieșire	Specifică faptul că utilizatorului nu i se permite să efectueze apeluri telefonice externe.
Interzicere SMS	Specifică faptul că utilizatorului nu i se permite să trimită sau să primească mesaje SMS.

Sistemul	
Interzicerea creării ferestrelor	Specifică că ferestrele în afară de ferestrele aplicației nu trebuie create.
Interzicerea setului User Icon	Specifică dacă unui utilizator nu i se permite să își schimbe pictograma.
Interziceți Set Wallpaper	Restricție utilizator pentru a nu permite setarea unui tapet de fundal.
Dezactivați bara de stare	Dezactivarea barei de stare blochează notificările, setările rapide și alte suprapuneri de ecran care permit evadarea de pe un dispozitiv de unică folosință.
Activați timpul automat	Setează automat ora.
Activați fusul orar automat	Setează automat fusul orar.
Rămâne pornit în timp ce este conectat la priză	Dispozitivul va rămâne activ în timp ce este conectat la o sursă de alimentare.

Depozitare	
Interziceți dezactivarea	Specifică dacă unui utilizator nu i se permite să dezactiveze verificarea aplicațiilor.

verificării aplicației	
Interziceți montarea suporturilor fizice	Specifică dacă unui utilizator nu i se permite să monteze suporturi externe fizice.
Activați serviciul de backup	Serviciul de backup gestionează toate mecanismele de backup și restaurare de pe dispozitiv. Dacă setați acest lucru la fals, datele nu vor mai putea fi salvate sau restaurate. Serviciul de backup este dezactivat în mod implicit. Necesită Android 8.0
Activare stocare în masă USB	Permite utilizarea USB Mass Storage.

Tastatură	
Interziceți completarea automată	Specifică dacă unui utilizator nu i se permite să utilizeze serviciile de completare automată. Necesită Android 8.0
Interzicerea copierii și lipirii între profiluri	Specifică dacă ceea ce este copiat în clipboard-ul acestui profil poate fi lipit în profilurile conexe.

Sunet	
Neadmiterea ajustării volumului	Specifică dacă unui utilizator îi este interzisă ajustarea volumului principal.
Dezactivare Dezactivare microfon	Specifică dacă unui utilizator nu i se permite să regleze volumul microfonului.
Dispozitiv mut	Dispozitiv mut.

Politica de actualizare a sistemului	
Controlați actualizările sistemului de operare	Activați această opțiune pentru a seta comportamentul de actualizare la automat, în fereastră sau amânat.

Container BYOD

Android Enterprise

Android Enterprise

Activați Android Enterprise	Activați Android Enterprise (AE). AE este acceptat începând cu Android 5.1 și versiunile ulterioare.
Aplicarea conformității	Mode Prompt User - Utilizatorul va fi rugat să efectueze acțiunile necesare. Modul Lock-Down Container - Ascundeți toate aplicațiile până când toate cerințele sunt îndeplinite
Politica de autorizare în timpul rulării	Invitați utilizatorul să solicite noi permisiuni Întotdeauna acordați noi cereri de permisiune noi Refuzați întotdeauna noile cereri de permisiune Atenție: Unele aplicații au probleme cu recunoașterea permisiunilor dacă acestea sunt setate automat. Dacă acordați întotdeauna permisiuni și întâmpinați probleme cu aplicațiile care spun că lipsesc permisiunile, setați acest lucru la "prompt user" și reinstalați aplicația
Permiteți scoaterea clipboard-ului	Permite copierea și lipirea din interiorul containerului în exterior
Permiteți rezoluția ID-ului apelantului	Afișează numele pentru un apel primit pe baza contactelor din container
Permiteți rezolvarea căutării contactelor	Permite căutarea numelor în contactele din container atunci când efectuați apeluri
Permiteți partajarea contactelor Bluetooth	Permite accesul la contactul containerului în mașină
Interzice ieșirea fasciculului NFC	Dezactivează NFC pentru container
Permiteți surse necunoscute	Dacă este activată, utilizatorii pot încărca aplicații prin instalarea unui fișier .apk.
Permite depanarea USB	Dacă este activată, utilizatorii pot activa depanarea USB.
Interzicerea modificării contului	Interzice crearea, ștergerea și modificarea conturilor din container Rețineți că unele aplicații trebuie să creeze sau să modifice conturi pentru a funcționa conform așteptărilor

Gmail Exchange

Vă permite să configurați Gmail în container. Vă rugăm să rețineți că activarea acestei configurații nu instalează automat aplicația. Trebuie în continuare să adăugați această aplicație ca aplicație obligatorie.

Adresa de e-mail	Adresa de e-mail
Nume gazdă server	Nume gazdă server
Nume de utilizator	Nume de utilizator
Semnătura	Semnătura
Numărul de zile anterioare pentru sincronizare	Numărul de zile anterioare pentru sincronizare.
Identificatorul dispozitivului	Identificator EAS. Păstrați acest câmp gol dacă mediul dvs. nu necesită acest lucru
Utilizați Secure Sockets Layer (SSL)	Activează utilizarea SSL. Dezactivarea acestei opțiuni poate reduce securitatea
Acceptați toate certificatele	Acceptă toate certificatele. Activarea acestei opțiuni poate reduce securitatea
Permiteți conturile negestionate	Permite utilizatorului să adauge conturi suplimentare
Certificat de client	Încărcați certificatul clientului dacă serverul Exchange necesită acest lucru

Aplicații de sistem AE

Aici puteți activa aplicațiile de sistem pentru Android Enterprise Container. Vă rugăm să rețineți că aplicația specificată trebuie să se afle în spațiul de stocare al sistemului, altfel nu se întâmplă nimic.

Codul de acces al containerului

Numai pentru Android 7.0 sau mai mare

Vă permite să setați o cerință specifică privind parola pentru container.

Lungimea minimă a parolei	Stabilește numărul minim de simboluri pe care trebuie să le aibă o parolă
Calitatea parolei	Puterea parolei Nespecificat = nespecificat Fiecare parolă este ok = fiecare parolă este acceptabilă cel puțin caractere numerice = trebuie să conțină cel puțin caractere numerice cel puțin caractere complexe = trebuie să conțină cel puțin caractere speciale cel puțin caractere alfanumerice = trebuie să conțină cel puțin caractere alfanumerice cel puțin caractere alfabetice = trebuie să conțină cel puțin caractere alfabetice
Timp maxim de inactivitate blocare	Timpul maxim până când containerul este blocat. Aceasta configurează doar valoarea maximă care poate fi selectată de utilizator
Minimum de litere minuscule necesare în parolă	Minimum de litere minuscule necesare în parolă
Minimum de litere majuscule necesare în parolă	Minimum de litere majuscule necesare în parolă
Numărul minim de caractere din afara literelor necesare în parolă	Numărul minim de caractere din afara literelor necesare în parolă
Minimum de cifre numerice necesare în parolă	Minimum de cifre numerice necesare în parolă
Simboluri minime necesare în parolă	Simboluri minime necesare în parolă
Timpul de expirare a parolei	Se stabilește, interval de timp după care parola expiră și trebuie emisă o nouă parolă
Restricționarea istoricului parolelor	Numărul de parole utilizate anterior care nu sunt permise
Numărul maxim de încercări de parole eșuate	Stabilește de câte ori o parolă poate fi introdusă incorect, înainte ca recipientul să fie șters

Samsung KNOX

Activare

Aici puteți activa containerul Samsung KNOX. Vă rugăm să rețineți că acesta nu mai este acceptat de Samsung pe Android 10 sau o versiune ulterioară. Utilizați containerul Android Enterprise pe Android 10 sau o versiune ulterioară

Codul de acces Knox

Stabiliți liniile directoare care se referă la setările parolei dispozitivului

Lungimea minimă a parolei	Stabilește câte simboluri trebuie să aibă parola
Calitatea parolei	Puterea parolei Fiecare parolă este ok = Fiecare parolă este ok Cel puțin caractere numerice = Caractere numerice minime trebuie să fie prezente Cel puțin caractere complexe = Caracterele speciale minime trebuie să fie prezente Cel puțin caractere alfanumerice = Minimum de caractere alfanumerice trebuie să fie prezente Cel puțin caractere alfabetice = Minimum de caractere alfabetice trebuie să fie prezente
Minim de caractere complexe necesare	Trebuie să fie prezente minimum caractere complexe
Timeout maxim de inactivitate	Timp maxim de inactivitate a utilizatorului, înainte de blocarea tastaturii
Permiteți autentificarea amprentei digitale	Permiteți autentificarea prin amprentă digitală
Permiteți autentificarea Iris	Permiteți autentificarea prin recunoașterea irisului
Vârsta maximă a parolei	Stabilește după cât timp expiră parola și trebuie emisă o nouă parolă
Istoric parolă stocată	Numărul de parole anterioare care nu sunt permise
Numărul maxim de încercări de parole eșuate	Stabilește de câte ori parola poate fi introdusă incorect, înainte de a avea loc o ștergere completă a dispozitivului

Knox Securitate

Limitarea funcționalităților specifice ale dispozitivului

Activați camera	Permiteți utilizarea camerei
Permiteți Samsung KNOX App Store	Permiteți utilizarea magazinului de aplicații Samsung KNOX

Permiteți serviciile Google Play	Permiteți serviciile Google Play
Permiteți browserul	Permiteți utilizarea browserului nativ
Permiteți capturi de ecran	Permiteți crearea de capturi de ecran
Permiteți importul de contacte	Dacă este activat, este permis accesul la contactele dispozitivului din containerul KNOX
Permiteți exportul contactelor	Dacă este activat, este permis accesul la contactele KNOX de pe dispozitiv
Permiteți importul calendarului	Dacă este activat, este permis accesul la calendarul dispozitivului din containerul KNOX
Permiteți exportul calendarului	Dacă este activat, este permis accesul la calendarul KNOX de pe dispozitiv
Permiteți tastatură nesecurizată	Permiteți utilizarea unei tastaturi nesecurizate
Activarea importului de fișiere	Activarea importului de fișiere în containerul KNOX
Activarea exportului de fișiere	Activarea exportului de fișiere din containerul KNOX

Knox Exchange

Aici puteți configura profilul Exchange pentru containerul KNOX

Adresa eMail	Adresa de e-mail a utilizatorului furnizat Vă rugăm să rețineți "Placeholders", pe care le puteți utiliza pentru a lucra cu acreditările și nu efectuați modificări manual pe fiecare dispozitiv Făcând clic pe **Afișarea marcajelor de poziție**, le puteți afișa pentru dvs.
Nume gazdă server	Adresa de server a serverelor Exchange
Nume de utilizator	Numele de autentificare pentru dispozitivul respectiv al utilizatorului final, vă rugăm să rețineți și "Placeholders" aici
Domeniu	Adresa domeniului
Parolă (numai la nivel de dispozitiv)	Opțional, unui dispozitiv individual i se poate furniza o parolă; dacă aceasta rămâne goală, utilizatorului i se va solicita să introducă parola Exchange
Numărul de zile anterioare pentru sincronizare	Numărul de zile, care determină momentul în care e-mailurile sunt sincronizate înapoi
Semnătura	Poate fi atașată o semnătură
Cont implicit	Stabilește că acest cont de e-mail este contul standard
Utilizați Secure Sockets Layer (SSL)	Utilizați o conexiune SSL
Utilizați securitatea stratului de transport (TLS)	Utilizați o conexiune TLS
Acceptați toate certificatele	Toate certificatele sunt acceptate. Vă rugăm să selectați această opțiune, dacă Exchange Server utilizează un certificat auto-semnat

Knox eMail

Adresa eMail	Adresa de e-mail a utilizatorului furnizat Vă rugăm să rețineți "Placeholders", pe care le puteți utiliza pentru a lucra cu acreditările și nu efectuați modificări manual pe fiecare dispozitiv Făcând clic pe **Afișarea marcajelor de poziție**, le puteți afișa pentru dvs.
Protocol server de intrare	Protocol server de intrare IMAP sau POP
Adresa serverului de intrare	Adresa serverului de intrare
Portul serverului de intrare	Portul serverului de intrare
Autentificare/utilizator server de intrare	Autentificare/utilizator server de intrare
Parola serverului de intrare	Parola serverului de intrare
Serverul de intrare utilizează SSL	Serverul de intrare utilizează SSL
Serverul de intrare utilizează TLS	Serverul de intrare utilizează TLS
Serverul de intrare acceptă toate certificatele	Serverul de intrare acceptă toate tipurile de certificate
Protocolul serverului de ieșire	Protocolul serverului de ieșire SMTP
Portul serverului de ieșire	Portul serverului de ieșire
Serverul de ieșire utilizează credențiale suplimentare	Credențiale suplimentare pentru serverul de ieșire. Dacă acest lucru este setat la "off", atunci vor fi utilizate setările serverului de intrare
Autentificare/utilizator server de ieșire	Autentificare/utilizator server de ieșire
Parola serverului de ieșire	Parola serverului de ieșire
Serverul de ieșire utilizează SSL	Serverul de ieșire utilizează SSL
Serverul de ieșire utilizează TLS	Serverul de ieșire utilizează TLS
Serverul de ieșire acceptă toate certificatele	Serverul de ieșire acceptă toate tipurile de certificate
Semnătura	Aici poate fi atașată o semnătură
Notificarea utilizatorului cu privire la primirea unui nou e-mail	Notificarea utilizatorului cu privire la primirea unui nou e-mail

Aplicații Knox

Stabiliți aici aplicațiile pe care doriți să le distribuiți dispozitivelor utilizatorilor finali. Acestea vor fi apoi disponibile în KNOX-Container. Pentru a adăuga o aplicație, procedați ca în meniul Aplicații obligatorii

Numele aplicației	Numele aplicației
Obligatoriu deoarece	Moment în timp, când a fost adăugată aplicația
Sursa	Sursa aplicației (Play Store | In-House)

Făcând clic pe simbol, aplicația respectivă poate fi eliminată din nou

Gestionarea conexiunilor

Wifi

Pentru această setare, efectuați preconfigurarea dispozitivelor utilizatorului final, pentru accesul la punctele de acces interne

Identificatorul setului de servicii (SSID)	SSID pentru rețeaua care urmează să fie conectată
Rețea ascunsă	Activare, în cazul în care AP nu transmite SSID-ul
Tip de securitate	Stabilirea tipului de securitate al AP

Tip de securitate

WEP

Parolă	Parolă pentru AP

WPA/WPA2

Parolă	Parolă pentru AP

802.1x EAP

Metoda EAP	

PWD	Identitate	Identitate
	Parolă	Parolă

PEAP	Protocolul de autentificare faza 2	niciunul	Fără protocol suplimentar
		MSCHAPV2	Protocolul MSCHAPV2
		GTC	Protocolul GTC
	Certificat CA	Certificat CA	
	Identitate	Identitate	
	Identitate anonimă	Identitate anonimă	
	Parolă	Parolă	

Metoda EAP	

TTLS	Protocolul de autentificare faza 2	niciunul	Fără protocol suplimentar
		PAP	Protocolul PAP
		MSCHAP	Protocolul MSCHAP
		MSCHAPV2	Protocolul MSCHAPV2
		GTC	Protocolul GTC
	Certificat CA	Certificat CA	
	Identitate	Identitate	
	Identitate anonimă	Identitate anonimă	
	Parolă	Parolă	

TLS	Certificat CA	Certificat CA
	Identitate	Identitate
	Parolă	Parolă

VPN

Tip de conexiune	**Stabilirea tipului de conexiune VPN**

Dacă selectați "Per-App VPN" ca Tip VPN, Clienții VPN disponibili se vor schimba. Per-App VPN limitează VPN-ul la anumite aplicații și pornește automat conexiunea VPN dacă este pornită o anumită aplicație.

Client VPN AppTec360	Folosește AppTec360 VPN Client în combinație cu Universal Gateway
Nume conexiune	Numele conexiunii VPN
Configurarea gateway-ului	Selectați configurația VPN a Universal Gateway
Întotdeauna pe VPN	Forțează VPN-ul să fie întotdeauna activ, astfel încât întregul trafic să treacă prin VPN.
Activați blocarea nativă	Blochează toate rețelele atunci când dispozitivul nu este conectat la VPN. Utilizați această opțiune cu atenție, deoarece poate cauza pierderea completă a conexiunii dacă nu este configurată corespunzător. Numai pentru Android Enterprise pe Android 7 sau o versiune ulterioară
Activați Lockdown AppTec360	Blochează utilizarea tuturor aplicațiilor până la pornirea conexiunii VPN

Cisco AnyConnect	
Nume conexiune	Numele conexiunii VPN
Server	Adresa serverului
Mod certificat	Dezactivat = dezactivat Automat = automat

L2TP (numai KNOX)	Disponibil numai pe dispozitivele Samsung
Nume conexiune	Numele conexiunii
Server	Adresa serverului
Activați L2TP Secret	
DNS Căutare Domenii	Domenii de căutare DNS

Tip de conexiune	**Stabilirea tipului de conexiune VPN**

PPTP (numai KNOX)	Disponibil numai pe dispozitivele Samsung
Nume conexiune	Numele conexiunii VPN
Server	Adresa serverului
Activați criptarea	Activați criptarea
DNS Căutare Domenii	Domenii de căutare DNS

L2TP / IPSec PSK (numai KNOX)	Disponibil numai pe dispozitivele Samsung
Nume conexiune	Numele conexiunii VPN
Server	Adresa serverului
Cheie IPSec precompartimentată	Cheie prepartajată pentru autentificare
Activați L2TP Secret	
Secret L2TP	
DNS Căutare Domenii	Domenii de căutare DNS

IPSec XAuth PSK (numai KNOX)	Disponibil numai pe dispozitivele Samsung
Nume conexiune	Numele conexiunii VPN
Server	Adresa serverului
Identificator IPSec	Numele de utilizator pentru conexiune
Cheie IPSec precompartimentată	Parolă pentru conexiune
DNS Căutare Domenii	Domenii de căutare DNS

OpenVPN	

Nume conexiune	Numele conexiunii
Profil OpenVPN	Aici este locul unde va fi copiat conținutul fișierului .ovpn
Aplicație OpenVPN	Există două aplicații diferite pentru utilizarea OpenVPN Vă recomandăm aplicația "OpenVPN pentru Android". Dar, în mod alternativ, poate fi utilizată aplicația "OpenVPN Connect"

Restricții

Aici puteți seta restricțiile legate de gestionarea conexiunilor.

Permiteți roamingul de date	Permiteți datele mobile în roaming
Forțați roamingul de date	Dacă este activat, roamingul pentru date mobile este activat permanent (nu este recomandat!) Această setare suprascrie setarea "Allow Data Roaming"!
Următoarele setări sunt disponibile numai pe Samsung KNOX 2.0 sau o versiune superioară	
Permiteți numai apelurile de urgență	Permiteți numai apelurile de urgență
Permiteți WiFi	Permiteți WiFi
Nivelul minim de securitate al rețelei WiFi	Nivelul minim de securitate al rețelei WiFi Deschis = toate tipurile de WiFi sunt permise
Interziceți utilizatorului să adauge rețele WiFi	Utilizatorul nu poate adăuga singur o rețea WiFi Această setare este posibilă numai dacă a fost definit un profil WiFi în "Gestionarea conexiunii"
Permiteți SMS & MMS	Toate = Tot traficul SMS și MMS este permis Incoming SMS Only = Sunt permise numai mesajele SMS primite Outgoing SMS Only = Sunt permise numai mesajele SMS de ieșire Niciunul = Nu este permis traficul SMS / MMS
Permiteți sincronizarea în timpul roaming-ului	Permiteți sincronizarea în timpul roaming-ului Pornit = activat Oprit = dezactivat Alegerea utilizatorului = alegerea utilizatorului
Permiteți roamingul vocal	Permiteți roamingul vocal Pornit = activat Oprit = dezactivat Alegerea utilizatorului = alegerea utilizatorului
Utilizați serverul proxy http al sistemului	Utilizarea unui server proxy HTTP, care este furnizat de setările sistemului în setări, depinde de rețeaua conectată (WiFi sau APN)

APN

Următoarele setări sunt disponibile numai pe Samsung SAFE 2.0 sau versiune superioară!

Nume de afișare APN	Nume de afișare APN	
Nume punct de acces	Numele APN	
Protocolul serverului de ieșire	Nu este setat	
	Niciuna	
	PAP	Protocolul PAP
	CHAP	Protocolul CHAP
	PAP sau CHAP	Protocolul PAP sau CHAP
MCC - Codul țării mobile	MCC este introdus aici, lăsați acest câmp gol, dacă trebuie utilizat MCC-ul cartelei SIM introduse	
MNC - Codul rețelei mobile	MNC este introdus aici, lăsați acest câmp gol, dacă trebuie utilizat MCC-ul cartelei SIM introduse	
Adresa serverului	Adresa serverului	
Numărul portului serverului	Numărul portului serverului	
Adresa proxy a serverului	Adresa proxy a serverului	
Adresa serverului MMS	Adresa serverului MMS, pentru Standard vă rugăm să lăsați în alb	
Numărul portului MMS	Numărul portului MMS	
Adresa proxy MMS	Adresa proxy MMS	
Numele utilizatorului	Numele utilizatorului	
Parolă	Parolă	
Tip punct de acces	Tipurile permise sunt: "default", "mms", "supl" Dacă acest câmp este lăsat gol, atunci se va utiliza "default,supl,mms"	
APN preferat	APN este de preferat	

Bluetooth

Aici pot fi efectuate o serie de setări Bluetooth.

Următoarele setări sunt disponibile numai pe Samsung KNOX 1.0 sau o versiune mai recentă!

Permiteți descoperirea dispozitivului prin Bluetooth	Permiteți descoperirea dispozitivului prin Bluetooth
Permiteți împerecherea Bluetooth	Permiteți asocierea Bluetooth
Permiteți dispozitivele Bluetooth Headset	Permiteți dispozitivele Bluetooth Headset
Permiteți utilizarea dispozitivelor Bluetooth Hands-free	Permiteți utilizarea dispozitivelor Bluetooth Hands-free
Permiteți dispozitive Bluetooth A2DP	Permiteți streamingul audio Bluetooth A2DP între dispozitive
Permiteți apelurile efectuate	Permiteți efectuarea de apeluri prinBT
Permiteți transferul de date prin Bluetooth	Permiteți transferul de date prin Bluetooth
Permiteți Tethering Bluetooth	Permite utilizarea dispozitivului ca modem (conexiune Bluetooth la internet)
Permiteți conectarea la computer prin Bluetooth	Permiteți conectarea la computer prin Bluetooth

Gestionarea PIM

Schimb

Disponibil numai pentru Samsung KNOX 1.0 sau superior!

Adresa eMail	Adresa de e-mail a utilizatorului furnizat Vă rugăm să rețineți "Placeholders", pe care le puteți utiliza pentru a lucra cu acreditările și nu efectuați modificări manual pe fiecare dispozitiv Făcând clic pe **Afișarea marcajelor de poziție**, le puteți afișa pentru dvs.
Nume gazdă server	Adresa de server a serverelor Exchange
Nume de utilizator	Numele de autentificare pentru dispozitivul respectiv al utilizatorului final, vă rugăm să rețineți și "Placeholders here
Domeniu	Adresa domeniului
Parolă (numai la nivel de dispozitiv)	Opțional, unui dispozitiv individual i se poate furniza o parolă; în cazul în care aceasta rămâne goală, utilizatorului i se va solicita să își introducă parola Exchange
Numărul de zile anterioare pentru sincronizare	Numărul de zile, care determină momentul în care e-mailurile sunt sincronizate înapoi
Semnătura	Se poate atașa o semnătură (Indicație: Unele dispozitive necesită formatare HTML pentru semnătură)
Cont implicit	Stabilește că acest cont de e-mail este contul standard
Utilizați Secure Sockets Layer (SSL)	Utilizați o conexiune SSL
Utilizați securitatea stratului de transport (TLS)	Utilizați o conexiune TLS
Acceptați toate certificatele	Toate certificatele sunt acceptate. Vă rugăm să selectați această opțiune, dacă Exchange Server utilizează un certificat auto-semnat

eMail

Aici, puteți distribui conturile IMAP și POP către dispozitivele respective ale utilizatorului final.

Următoarele setări sunt disponibile numai pe Samsung KNOX 1.0 sau o versiune mai recentă!		
Adresa eMail	Adresa de e-mail a utilizatorului furnizat Vă rugăm să rețineți "Placeholders", pe care le puteți utiliza pentru a lucra cu acreditările și nu efectuați modificări manual pe fiecare dispozitiv Făcând clic pe **Afișarea marcajelor de poziție**, le puteți afișa pentru dvs.	
Protocol server de intrare	Protocol server de intrare	IMAP sau POP
Adresa serverului de intrare	Adresa serverului de intrare	
Portul serverului de intrare	Portul serverului de intrare	
Autentificare/utilizator server de intrare	Autentificare/utilizator server de intrare	
Parola serverului de intrare (numai la nivel de dispozitiv)	Parola serverului de intrare (numai la nivel de dispozitiv)	
Serverul de intrare utilizează SSL	Serverul de intrare utilizează SSL	
Serverul de intrare utilizează TLS	Serverul de intrare utilizează TLS	
Serverul de intrare acceptă toate certificatele	Serverul de intrare acceptă toate tipurile de certificate	
Protocolul serverului de ieșire	Protocolul serverului de ieșire	SMTP
Portul serverului de ieșire	Portul serverului de ieșire	
Serverul de ieșire utilizează credențiale suplimentare	Acreditări suplimentare pentru serverul de ieșire. Dacă acest lucru este setat la "off", atunci se vor utiliza setările serverului de intrare	
Autentificare/utilizator server de ieșire	Autentificare/utilizator server de ieșire	
Parola serverului de ieșire (numai la nivel de dispozitiv)	Parola serverului de ieșire	
Serverul de ieșire utilizează SSL	Serverul de ieșire utilizează SSL	
Serverul de ieșire utilizează TLS	Serverul de ieșire utilizează TLS	

Serverul de ieșire acceptă toate certificatele	Serverul de ieșire acceptă toate tipurile de certificate
Semnătură	O semnătură poate fi atașată aici (Indicație: Unele dispozitive necesită formatare HTML pentru semnătură)
Notificarea utilizatorului cu privire la primirea unui nou e-mail	Notifică utilizatorul cu privire la primirea unui e-mail nou

AE Gmail Exchange

Info: Această configurare va fi aplicată aplicației Gmail. Deci trebuie să aprobați și să instalați Gmail.

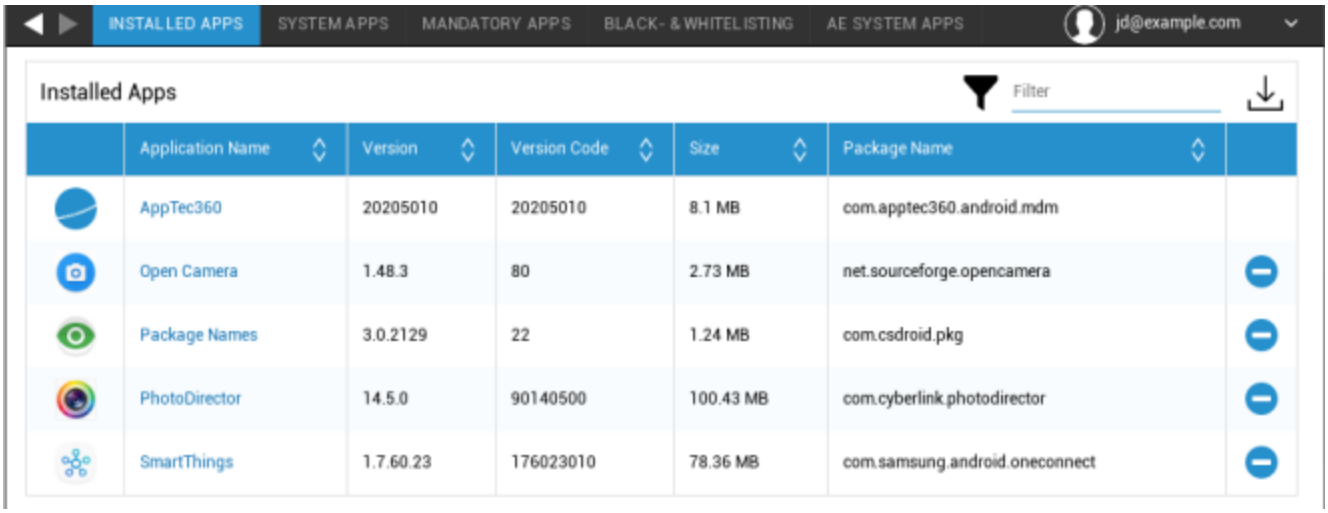
Adresa eMail	Adresa de e-mail a utilizatorului furnizat Vă rugăm să rețineți "Placeholders", pe care le puteți utiliza pentru a lucra cu acreditările și nu efectuați modificări manual pe fiecare dispozitiv Făcând clic pe Afișarea marcajelor de poziție, le puteți afișa pentru dvs.
Nume gazdă server	Adresa de server a serverelor Exchange
Nume de utilizator	Numele de autentificare pentru dispozitivul respectiv al utilizatorului final, vă rugăm să rețineți și "Placeholders here
Semnătura	Se poate atașa o semnătură (Indicație: Unele dispozitive necesită formatare HTML pentru semnătură)
Numărul de zile anterioare pentru sincronizare	Numărul de zile, care determină momentul în care e-mailurile sunt sincronizate înapoi
Identificatorul dispozitivului	Identificator EAS. Păstrați acest câmp gol dacă mediul dvs. nu necesită acest lucru
Utilizați Secure Sockets Layer (SSL)	Utilizați o conexiune SSL
Acceptați toate certificatele	Toate certificatele sunt acceptate. Vă rugăm să selectați această opțiune, dacă Exchange Server utilizează un certificat auto-semnat
Permiteți conturile negestionate	Permite utilizatorului să adauge conturi suplimentare
Certificat de client	Încărcați certificatul clientului dacă serverul Exchange necesită acest lucru

Gestionarea aplicațiilor

Enterprise App Manager

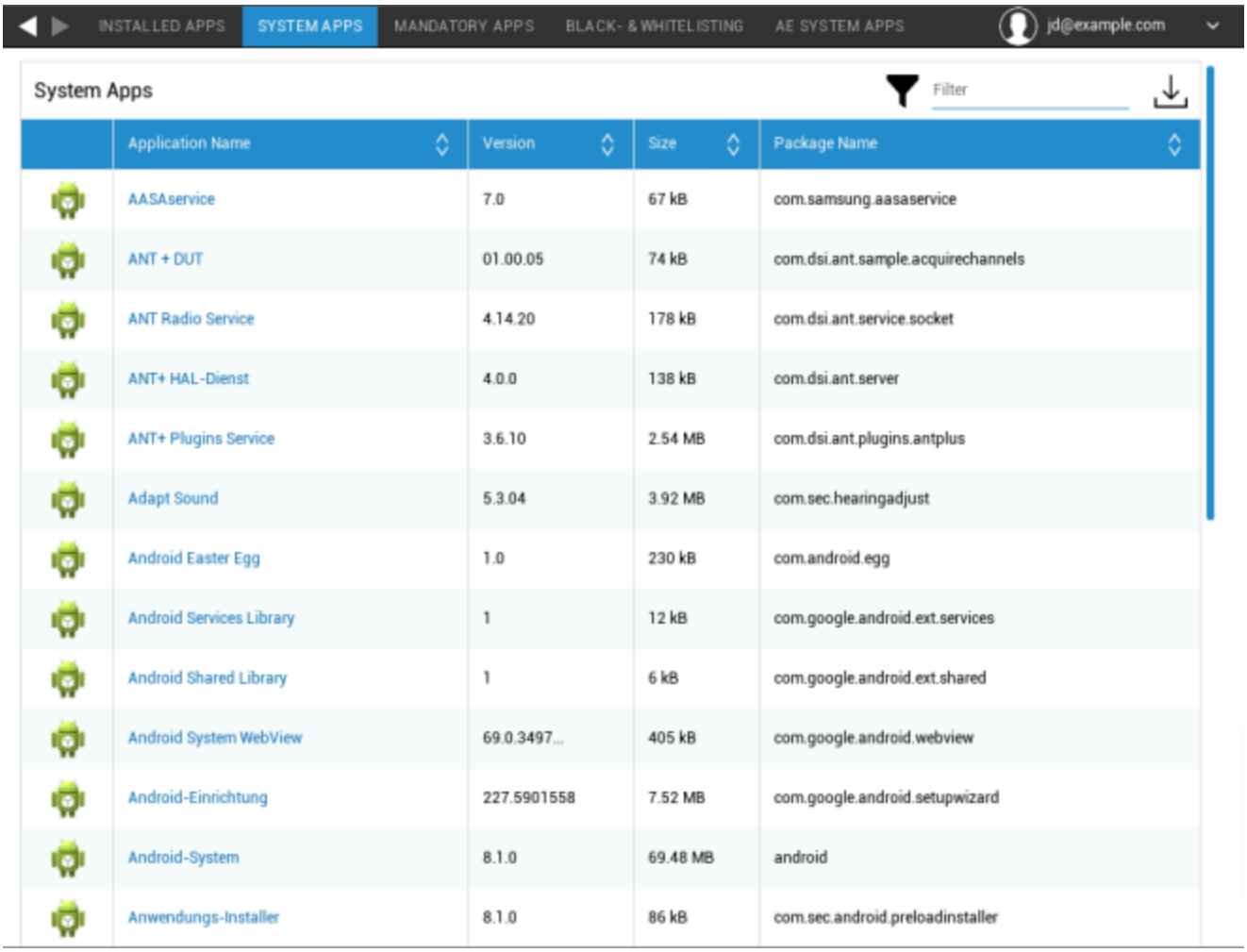
Aplicații instalate (numai la nivel de dispozitiv)

Aici vor fi afișate toate aplicațiile care sunt instalate în prezent pe dispozitivul utilizatorului final.


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

Aplicații de sistem (numai la nivel de dispozitiv)

Sub "Aplicații de sistem", toate sistemele preinstalate vor fi listate cu numele și versiunea pachetului.



Aplicații obligatorii

În Aplicații obligatorii puteți defini aplicațiile care trebuie instalate pe dispozitiv. În funcție de configurație și de dispozitiv, aplicația va fi instalată automat sau utilizatorului i se va solicita să o instaleze.

Vă rugăm să rețineți că este recomandat să utilizați Android Enterprise pentru gestionarea ușoară a aplicațiilor.

Scenariile sunt enumerate mai jos:

Aplicații normale Play Store

Instalarea aplicațiilor Playstore necesită întotdeauna interacțiunea utilizatorului. În plus, un cont Google trebuie să fie configurat pe dispozitiv.

Instalarea aplicației InHouse

Pe dispozitivele Samsung, aceste aplicații vor fi instalate silențios. Singura excepție este containerul, unde utilizatorul trebuie să confirme instalarea.

În orice alt scenariu, utilizatorul trebuie să confirme instalarea aplicației.

Android Enterprise Play Store Aplicații

Aceste aplicații vor fi întotdeauna instalate silențios, fără interacțiunea utilizatorului.

Pentru a adăuga o aplicație obligatorie, faceți clic pe "+" și selectați aplicația dorită din listă. Vă rugăm să rețineți că nu puteți instala aplicații din fila "Magazin Google Play", dacă dispozitivul este configurat cu Android Enterprise fie ca complet gestionat, fie ca container.

Dacă utilizați Android Enterprise, selectați aplicațiile din secțiunea "AE Play Store". Pentru a face aplicațiile disponibile aici, confirmați-le în magazinul Google Enterprise Play accesând Setări generale → AE Play Store → Aplicații Play Store.

Atunci când eliminați o aplicație obligatorie, aceasta va fi dezinstalată și de pe dispozitiv.

Puteți să faceți clic pe numele unei aplicații din lista de aplicații obligatorii și să mergeți la fila "configurare" pentru a configura o aplicație. Acest lucru necesită utilizarea Android Enterprise, iar aplicația trebuie să suporte acest lucru. Prin urmare, opțiunile disponibile depind de aplicația selectată.

Aplicații de sistem AE

Aici puteți activa aplicațiile de sistem pentru dispozitivele Android Enterprise. Vă rugăm să rețineți că aplicația specificată trebuie să se afle în spațiul de stocare al sistemului, altfel nu se întâmplă nimic.

296

Restricții și setări

Lista neagră și lista albă

Aici puteți defini o listă neagră sau o listă albă. Toate aplicațiile de pe lista neagră vor fi blocate. Toate aplicațiile care nu sunt în lista albă vor fi blocate. O listă neagră goală nu blochează nimic, în timp ce o listă albă goală blochează totul*

**Toate aplicațiile obligatorii și aplicațiile din Enterprise App Store vor fi incluse automat pe lista albă. Nu trebuie să le adăugați manual*

Când faceți clic pe "+", puteți fie să căutați o aplicație pe care doriți să o adăugați la lista neagră sau albă, fie să introduceți manual numele unui pachet.

Restricții aplicații sistem

Sub "Restricții aplicații sistem" puteți, printre altele, să blocați aplicațiile și serviciile preinstalate, după cum doriți.

Dezactivați browserul	Dezactivați browserul standard
Dezactivați calendarul	Dezactivați calendarul nativ
Dezactivarea calculatorului	Dezactivați calculatorul
Dezactivați browserul Chrome	Dezactivați browserul Chrome
Dezactivarea ceasului	Dezactivați ceasul
Dezactivarea contactelor	Dezactivarea contactelor
Dezactivați Dialer	Dezactivați dialerul nativ
Dezactivați eMail	Dezactivați e-mailul
Dezactivați Exchange	Dezactivați conturile Exchange
Dezactivați Facebook	Dezactivați aplicația Facebook
Dezactivați galeria	Dezactivați aplicația nativă Galerie
Dezactivați Gmail	Dezactivați Gmail
Dezactivați Google Books	Dezactivați Google Books
Dezactivați Google Play Kiosk	Dezactivați Google Play Kiosk
Dezactivați Google Maps	Dezactivați Google Maps
Dezactivați Google Music	Dezactivați Google Music
Dezactivați Google Movies	Dezactivați Google Movies
Dezactivați Magazinul Google Play	Dezactivați Google Play Store (App Store public)
Dezactivați Google Plus	Dezactivați Google Plus
Dezactivați căutarea Google	Dezactivați căutarea Google
Dezactivați Google Talk / Google Hangouts	Dezactivați Google Talk / Google Hangouts
Dezactivați playerul de muzică	Dezactivați aplicația nativă de redare a muzicii
Dezactivați setările	Dezactivați setările dispozitivului
Dezactivați Sim Toolkit	Dezactivați serviciile Sim Toolkit
Dezactivare SMS / MMS	Dezactivare SMS / MMS
Dezactivați Street View	Dezactivați serviciile Street View
Dezactivați Youtube	Dezactivați Youtube

Aplicații Samsung

Sub "Aplicații Samsung", puteți defini setări și/sau restricții suplimentare pentru dispozitivele Samsung.

Dezactivați AllShare Play / Samsung Link	Dezactivați AllShare Play / Samsung Link
Dezactivați ChatON	Dezactivați ChatON
Dezactivați Game Hub	Dezactivați Game Hub
Dezactivați jocul în grup	Dezactivați jocul în grup
Dezactivați ajutorul	Dezactivați Ajutor Samsung
Dezactivați KNOX	Dezactivați Samsung KNOX Container
Dezactivați Memo	Dezactivați Memo vocal
Dezactivați fișierele mele	Dezactivați fișierele mele
Dezactivați cititorul optic	Dezactivați cititorul optic
Dezactivați Polaris Office	Dezactivați Polaris Office
Dezactivați Readers Hub / Samsung Books	Dezactivați Readers Hub / Samsung Books
Dezactivați S Memo	Dezactivați aplicația Samsung Memo
Dezactivați S Translator	Dezactivați aplicația Samsung Translator
Dezactivați S Voice	Dezactivați asistentul vocal S
Dezactivați aplicațiile Samsung	Dezactivați Samsung App Store
Dezactivați Samsung Hub	Dezactivați magazinele de divertisment Samsung
Dezactivați playerul video	Dezactivați playerul video
Dezactivarea înregistratorului de voce	Dezactivarea înregistratorului de voce
Dezactivați WatchON	Dezactivați WatchON (simulează o telecomandă)

Aplicații Huawei

Sub "Aplicații Huawei", puteți defini setări și/sau restricții suplimentare pe dispozitivul Huawei.

Dezactivați DLNA	Dezactivați DLNA
Dezactivați instalatorul de aplicații	Dezactivați instalatorul de aplicații
Dezactivați Managerul de fișiere	Dezactivați Managerul de fișiere
Dezactivați Managerul de backup	Dezactivați Managerul de backup
Dezactivați actualizatorul de sistem	Dezactivați actualizatorul de sistem
Dezactivați caseta de instrumente	Dezactivați caseta de instrumente
Dezactivați vremea	Dezactivați vremea
Dezactivați radioul FM	Dezactivați radioul FM

Setări de gestionare a aplicațiilor

Aici puteți defini comportamentul de actualizare al aplicațiilor InHouse.

Frecvența verificării actualizărilor definește frecvența cu care AppTec360 App caută actualizări pentru aplicațiile InHouse. Odată ce este detectată o versiune nouă, aceasta va fi descărcată și instalată.

Pragul Wi-Fi definește dacă descărcarea ar trebui să fie limitată la conexiunile Wi-Fi în cazul în care aplicația este mai mare decât pragul configurat. Dacă este mai mică sau nu definiți un prag, aplicația va fi descărcată în Wi-Fi și într-o rețea celulară.

Magazin de aplicații pentru întreprinderi

Vă rugăm să rețineți că adăugarea aplicațiilor aici (Enterprise App Store) NU va face ca acestea să fie instalate automat pe dispozitiv(e). Utilizatorul trebuie să deschidă Enterprise App Store pe dispozitiv și să instaleze manual aplicația.

Dacă doriți să instalați automat aplicații pe dispozitiv, accesați "App Management" → "Enterprise App Manager" → "Mandatory Apps" și adăugați acolo aplicațiile dorite.

În acest punct, puteți distribui utilizatorilor dvs. aplicații opționale.

Playstore

Faceți clic pe "+" pentru a adăuga o aplicație Play Store la magazin. Dacă utilizați Android Enterprise, vă rugăm să mergeți la "App Management Enterprise Play Store". De asemenea, rețineți că un cont Google trebuie să fie configurat pe → dispozitiv pentru a instala aplicațiile definite aici.

In-House

Sub punctul "In-House", puteți încărca și distribui aplicații dezvoltate intern.

Faceți clic pe "+" pentru a adăuga o aplicație InHouse la magazinul de aplicații al întreprinderii, care poate fi apoi instalată de utilizator. În acest dialog puteți încărca, de asemenea, o nouă aplicație InHouse.

Magazin Play pentru întreprinderi

Vă rugăm să rețineți că adăugarea aplicațiilor aici (Enterprise Play Store) NU va face ca acestea să fie instalate automat pe dispozitiv(e). Utilizatorul trebuie să deschidă Play Store pe dispozitiv și să instaleze manual aplicația.

Dacă doriți să instalați automat aplicații pe dispozitiv, accesați "App Management" → "Enterprise App Manager" → "Mandatory Apps" și adăugați acolo aplicațiile dorite.

În acest punct, puteți distribui utilizatorilor dvs. aplicații opționale.

Aici puteți adăuga aplicații la Android Enterprise Playstore. Rețineți că trebuie să aprobați aplicațiile în Setări generale → AE Play Store → Aplicații Play Store. Aceste aplicații vor fi adăugate în magazinul Google Play normal.

De asemenea, trebuie să știți că mai întâi trebuie să definiți un aspect cu aplicații în Setări generale → Gestionarea aplicațiilor → AE Play Store → Aspectul magazinului.

Aplicațiile trebuie să fie într-un Layout înainte de a le putea adăuga cu succes în magazin.

Mod chioșc și lansator

Modul Kiosk

Modul Kiosk vă permite să predefiniți o aplicație sau un URL. Apoi va fi posibil să rulați/vizitați exclusiv această aplicație și/sau URL.

De asemenea, diverse butoane hardware pot fi dezactivate în diverse moduri Kiosk.

Start automat	Pornește automat modul Kiosk, de îndată ce profilul ajunge pe dispozitivul utilizatorului final
Modul Kiosk programat?	Puteți planifica o oră pentru modul Kiosk, care va începe și se va încheia automat, la ora stabilită de dvs.
Ora de începere	Ora de începere
Timp în minute	Timp în minute, după care modul Kiosk ar trebui să se încheie din nou

Tip de aplicație

Aplicație unică	Dacă doriți să porniți aplicația în modul chioșc, selectați Pachet" la "Tip aplicație"
Aplicație kiosk	Faceți clic aici, pentru a selecta o aplicație care ar trebui să fie pornită în modul Kiosk Veți găsi prezentarea generală obișnuită a gestionării aplicațiilor Puteți selecta între "Magazin Google Play", "Aplicații interne Android" și "Nume de pachet"

Tip de aplicație	
URL	Dacă doriți să lansați un URL în modul chioșc, selectați "URL" la "Tip aplicație" Apoi definiți adresa URL dorită
Ștergeți browserul după inactivitate	Aici puteți defini un interval de timp în minute, după care modul Kiosk ar trebui să fie relansat
Ștergeți cache-ul web și modulele cookie	Dacă activați această funcție, după o repornire a modului Kiosk, cache-ul web (cookie-uri și imagini în cache) va fi șters
Politica privind aceeași origine	Dacă această funcție este activă, atunci utilizatorul poate naviga numai pe subpaginile unui URL definit De exemplu, ați definit următoarea adresă URL:www.mypage.com Apoi, utilizatorul poate naviga pe: www.mypage.com/subpage
URL-uri pe lista albă	Aici puteți menține o listă albă, toate aceste URL-uri sunt permise Maximum 1 URL pe linie O adresă URL trebuie să înceapă cu http:/ sau https://
URL-uri pe lista neagră	Aici puteți menține o listă neagră, toate aceste URL-uri nu sunt permise Maximum 1 URL pe linie O adresă URL trebuie să înceapă cu http:/ sau https://
Orientarea ecranului	Această setare se referă la ajustările ecranului Automat = automat Portret = format vertical Peisaj = modul peisaj

Aplicație multiplă	Dacă selectați modul chioșc "Multi App", va fi impusă utilizarea lansatorului AppTec360.
Aplicații	Aplicație: Selectați o aplicație Playstore sau o aplicație internă ca aplicație pentru chioșc. De asemenea, este posibil să introduceți un nume de pachet. Aplicația de chioșc selectată trebuie să fie instalată pe dispozitiv. Nu uitați să setați aplicația de chioșc ca fiind obligatorie. Comandă rapidă pe ecranul de pornire: Dacă este setat la "Activat", va fi creată o comandă rapidă pe ecranul de pornire. Dacă este setată la "Off", aplicația va apărea în continuare în lista de aplicații.

Parola de ieșire activată	Dacă activați această funcție, atunci este posibil ca utilizatorul să încheie modul Kiosk cu o parolă predefinită de dvs.
Parola de ieșire	Aceasta este parola, care a fost predefinită de dvs.
Auto Collapse Status Bar	Dacă această opțiune este activată, bara de stare va fi automat colpasată. Cu această opțiune, utilizatorii pot vedea informațiile din bara de stare, dar nu pot accesa funcțiile acesteia
Dezactivați bara de stare	Bara de stare conține notificări, comenzi rapide și informații. Disponibil numai pentru dispozitivele Samsung cu KNOX 1.0 sau mai mare.
Dezactivarea tastelor de volum	Dezactivați tastele de volum (disponibil numai pe dispozitivele Samsung cu KNOX 1.0 sau superior)
Dezactivați comutatorul pornit / oprit	Dezactivați comutatorul Pornit / Oprit (disponibil numai pe dispozitivele Samsung cu KNOX 1.0 sau superior)
Dezactivați butonul Acasă	Dezactivarea butonului Acasă. Dacă această funcție a fost activată, atunci modul Kiosk poate fi oprit numai în consola AppTec360 (disponibil numai pe dispozitivele Samsung cu KNOX 1.0 sau versiune superioară)
Dezactivați bara de navigare	Cu aceasta puteți dezactiva bara de navigare (Înapoi / Meniu) În cazul în care această funcție a fost activată, modul Kiosk poate fi oprit numai în consola AppTec360 (disponibil numai pe dispozitivele Samsung cu KNOX 1.0 sau versiune superioară)

Setări actualizare aplicație	
Permiteți actualizările aplicației	Utilizatorilor li se va solicita să efectueze actualizări ale aplicațiilor chiar și atunci când modul Kiosk este activ. Pe dispozitivele cu Samsung KNOX, aplicațiile vor fi actualizate silențios.
Fereastra de actualizare	Setați un interval în care utilizatorilor li se va cere să instaleze actualizările aplicației.

TeamViewer	
Activați accesul nesupravegheat	Dacă este activată, administratorii pot controla dispozitivul de la distanță fără interacțiunea utilizatorului. Aplicația TeamViewer Host trebuie să fie instalată pe dispozitiv.

Lansator AppTec360

Activați lansatorul AppTec360	Pornit: Activează lansatorul AppTec360. Utilizatorul trebuie să îl seteze o singură dată ca lansator implicit. Notă: Dacă modul chioșc este activat, iar modul chioșc este setat la "Multi App", va fi impusă utilizarea lansatorului AppTec360.
Icoane mari	Pornit: Afișează o versiune mai mare a pictogramelor aplicației în lansator
Ascundeți pictograma AppTec360 App	Pornit: Ascunde complet aplicația AppTec360
Ascundeți pictograma magazinului AppTec360	Pornit: Ascunde complet AppTec360 Enterprise AppStore

Setări AppTec360

Activați AppTec360 Settings App	AppTec360 Settings App oferă control asupra conexiunilor WiFi și Bluetooth
Activați setările în Multi App Modul Kiosk	Dacă este activat, utilizatorii pot accesa AppTec360 Settings App în timp ce modul Multi App Kiosk este activ

Telecomandă

Splashtop

Afișează starea curentă a configurării Splashtop. Aici veți vedea pașii pe care trebuie să îi efectuați pentru a accesa dispozitivul de la distanță prin Splashtop. Aici trebuie, de asemenea, să introduceți codul de implementare pe care îl puteți obține de pe site-ul Splashtop. Codul de distribuire este necesar pentru a vă conecta la dispozitiv.

Teamviewer

Afișează starea curentă a configurării Teamviewer. Aici veți vedea pașii pe care trebuie să îi efectuați pentru a accesa dispozitivul de la distanță prin Teamviewer.

Gestionarea conținutului

Caseta de conținut

Aici puteți activa Contentbox pentru acest dispozitiv. Odată activată, aplicația Contentbox va fi instalată pe dispozitiv.

Browser securizat

Aici puteți activa browserul securizat pentru acest dispozitiv. Odată activată, aplicația Secure Browser va fi instalată pe dispozitiv. Acest browser poate fi configurat pentru a oferi un browser web pe dispozitiv care este limitat la nevoile dumneavoastră.

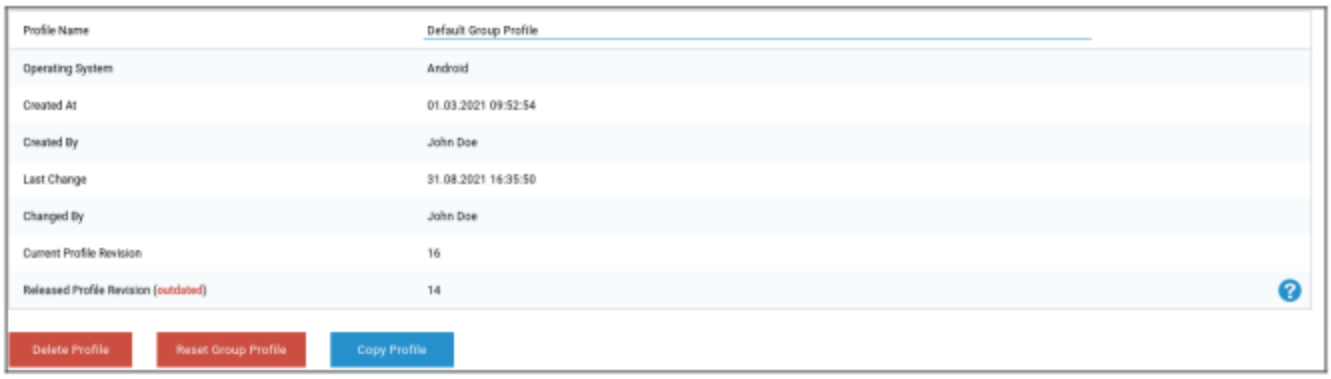
Solicitare parolă	Cereți utilizatorului să configureze și să utilizeze o parolă pentru a accesa browserul.
Restricționați descărcările / Deschideți în	Blochează descărcările de pe site-uri web
Restricționarea încărcărilor	Restricționează încărcările la anumite URL-uri. Nu furnizați niciun URL pentru a bloca încărcarea în întregime
Permiteți copierea	Permiteți copierea, tăierea sau partajarea textului din paginile web.
Permiteți capturarea ecranului	Permiteți capturarea de capturi de ecran.
Frecvența curățării datelor	Selectați frecvența cu care TOATE datele utilizatorului (istoric, cache etc.) ar trebui eliminate automat.
Marcaje companie	Marcajele vor apărea în folderul "Marcaje companie" din marcajele browserului. Acestea nu sunt editabile de către utilizator.
Ascundeți bara de adrese	Ascunde bara de adrese astfel încât utilizatorul să nu vadă URL-ul pe care îl vizitează
Lista albă în browser (fără Universal Gateway)	Permite lista albă a URL-urilor pe partea clientului. - Bookmark-urile companiei sunt întotdeauna pe lista albă - Compatibil doar pentru 100 de URL-uri - Vă rugăm să utilizați Universal Gateway pentru Black- și Whitelisting nelimitat
Liste negre și albe bazate pe gateway	Blacklisting are următoarele cerințe: - O configurație VPN funcțională cu un server DNS specificat ("General Settings" → "Universal Gateway" → "VPN Settings") - O configurație Blacklist ("General Settings" → "Universal Gateway" → "Domain Blacklist") - O conexiune VPN validă în profil ("Connection Management" → "VPN")

Configurare Windows 10 PC

Generalități

Prezentare generală a profilului grupului (numai la nivel de grup)

Atunci când deschideți un profil de grup, veți obține o prezentare generală rapidă a profilului.



Nume profil	Numele profilului (poate fi modificat aici)
Sistem de operare	Sistemul de operare pentru care este creat profilul
Creat la	Momentul creației
Creat de	Creatorul profilului
Ultima schimbare	Ora ultimei modificări a profilului
Schimbat de	Contul care a efectuat ultimele modificări
Revizuirea actuală a profilului	Revizuirea stării profilului salvat
Revizuire profil eliberată	Revizuirea profilului atribuit ("Atribuie acum"). Dacă eticheta afișează "(învechit)" în spatele textului, înseamnă că ați salvat profilul, dar nu l-ați atribuit încă, astfel încât dispozitivele vor primi în continuare o versiune mai veche.

Prezentare generală a dispozitivului (numai la nivel de dispozitiv)

Prezentare generală sumară a dispozitivului, care conține următoarele:

Nume PC	Numele PC-ului
Client	Dispozitivele de tip Windows
Ultima locație cunoscută	Latitudinea și longitudinea ultimei locații cunoscute a dispozitivului
Aplicații obligatorii atribuite	Numărul de aplicații obligatorii atribuite dispozitivului
PC UID	UID al PC-ului
Ediția OS	Afișează ediția Windows
Versiunea sistemului de operare	Versiunea Windows instalată în prezent
Construire sistem de operare	Windows Build curent
Sistem de operare	Sistemul de operare instalat în prezent
Numărul de serie	Numărul de serie al dispozitivului
Proprietatea dispozitivului	Tipul de proprietate configurat
Tip dispozitiv	Tipul de dispozitiv
Înrădăcinat	Arată dacă dispozitivul este înrădăcinat
Conform	Arată dacă dispozitivul este conform
Văzut ultima dată	Data și ora la care au fost efectuate modificările la profil
Atribuirea utilizatorului	Afișează utilizatorul sau grupul căruia îi este atribuit în prezent acest dispozitiv. Puteți muta dispozitivul selectând un alt utilizator sau grup din lista derulantă.

Setări

Permiteți actualizarea automată	Permiteți sau nu permiteți actualizările automate ale sistemului de operare.

Revizuirea configurației (numai la nivel de dispozitiv)

Aici veți primi o prezentare generală a profilului de grup care este atribuit dispozitivului.

Dacă faceți clic pe profilul grupului, veți accesa direct profilul și veți putea efectua setările.

Cu ajutorul simbolului, puteți readuce aplicațiile alocate la setările profilului de grup.

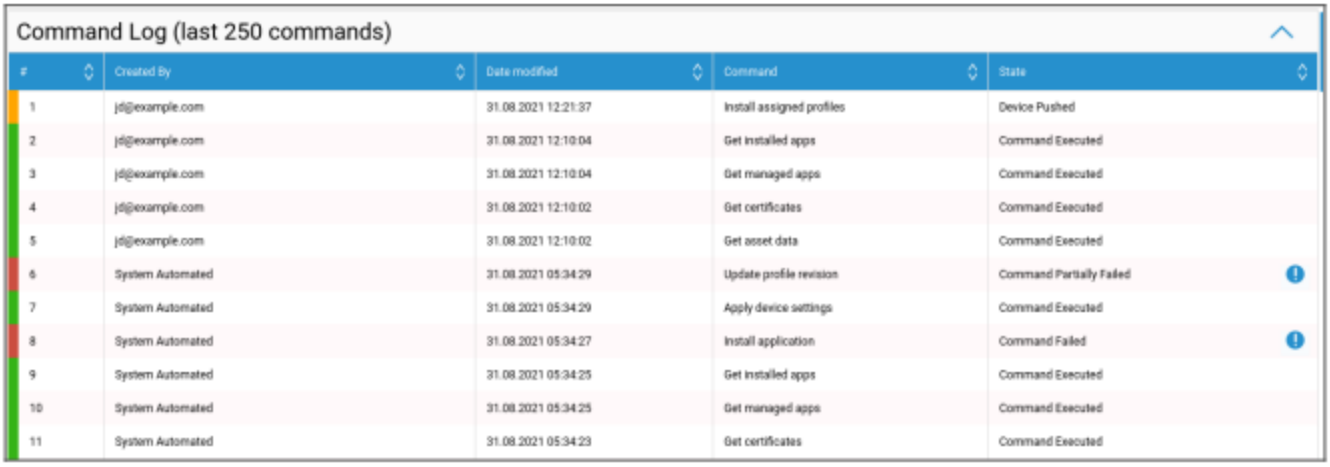
Cu ajutorul simbolului, puteți reseta profilul dispozitivului pentru a nu avea niciun fel de setări.

"Newer Revision available" indică faptul că profilul grupului a fost modificat și salvat, dar nu a fost atribuit. Profilul de grup trebuie să fie atribuit cu "Assign now" la nivel de grup pentru a aplica modificările dispozitivelor.

Jurnalul dispozitivului (numai la nivel de dispozitiv)

Jurnal de comandă

Aici puteți vedea ce comenzi au fost emise pentru dispozitiv și care este starea lor.



Comenzile create de "System Automated" sunt create automat de sistem.

Stări posibile ale comenzii

Dispozitiv împins	O solicitare push a fost trimisă către serviciul push (de exemplu, APNS) pentru a indica dispozitivului să se conecteze din nou la serverul EMM.
Comandă creată	Comanda a fost creată în sistem.
Comandă trimisă	Comanda a fost trimisă către dispozitiv după ce acesta s-a conectat la server.
Comandă executată	Comanda a fost executată cu succes.
Comandă eșuată	Comanda a eșuat. *
Comandă eșuată parțial	În funcție de sistemul de operare al dispozitivului, unele comenzi pot fi grupate împreună. În acest caz, unele părți ale acestui grup de comandă au eșuat. *
Comandă executată, eventual eșuată	Comanda a fost executată, dar poate că nu a fost.
Comanda Repushed	Comanda a fost respinsă de un utilizator.
Aruncată	Comanda a fost eliminată. De exemplu, pentru că a fost înlocuită de o altă comandă sau pentru că dispozitivul a fost înrolat din nou și comenzile vechi au fost eliminate

*Dacă există un semn al exclamării în spatele mesajului, puteți obține mai multe informații trecând cu cursorul peste pictogramă.

Gestionarea activelor (numai la nivel de dispozitiv)

Informații despre dispozitiv

Producător	Producător de dispozitive
Model	Model de dispozitiv
Numărul modelului	Numărul modelului
Sistem de operare	Sistemul de operare
Versiunea sistemului de operare	Versiunea sistemului de operare
Numărul de serie	Numărul de serie
ExchangeID	ExchangeID
Total RAM	Total RAM
Rezoluția ecranului	Rezoluția ecranului
Limba telefonului	Limba dispozitivului
Versiunea firmware	Versiunea firmware
Versiunea clientului DM	Versiunea Device Management Client
Versiunea hardware	Versiunea hardware a dispozitivului
Arhitectura CPU	Arhitectura CPU (tipul procesorului)

Celulare

Rețea SIM Carrier	Rețea de transportatori
Număr de telefon	Număr de telefon
Starea de roaming	Starea de roaming
IMEI	IMEI
IMSI	IMSI
Firmware modem	Firmware modem

Informații despre sincronizare

Conexiune DM instantanee	Dispozitivul ar trebui să creeze imediat o conexiune la AppTec
Timp inițial de rescriere	Timpul inițial de încercare pentru această primă conexiune
Reîncercări ale conexiunii	Numărul de noi încercări de conectare, după o deconectare de la managerul de conexiuni sau o eroare la nivel WinInet
Timp maxim de somn	Timpul maxim de așteptare după o eroare de trimitere a pachetului
Prima încercare de sincronizare	Timpul pentru prima etapă după înscriere
Primul interval de reîncercare	Timpul pentru prima etapă după înscriere
A doua încercare de sincronizare	Timpul pentru a doua etapă după înscriere
Al doilea interval de reîncercare	Timpul pentru a doua etapă după înscriere
Reîncercări regulate de sincronizare	Timpul pentru etapele suplimentare după înscriere
Interval regulat de reîncercare	Timpul pentru etapele suplimentare după înscriere

Managementul securității

Anti-furt (numai la nivel de dispozitiv)

Informații GPS (numai la nivelul dispozitivului)

Aici puteți stabili locația curentă/ultima a dispozitivului. Localizarea poate fi protejată cu una sau chiar două parole - Consultați: "Setări generale" > "Confidențialitate" > "Acces GPS"

Setări GPS

Activarea urmăririi GPS	Activați sincronizarea regulată a informațiilor GPS.
Interval de urmărire	Setați intervalul de sincronizare a informațiilor GPS.

Configurația de securitate

Codul de acces

Lungimea minimă a parolei	Lungimea minimă a parolei	
Compoziția parolei	Specifică numărul de caractere specifice pe care trebuie să le conțină parola Acestea sunt compuse din litere majuscule, litere minuscule, numere și simboluri speciale	
Calitatea parolei	Aici puteți seta calitatea parolei	
	Alfanumeric	Numai numere și litere
	Numeric	Numai numere
	Numeric sau alfanumeric	Numere sau numere și litere
Timp maxim de inactivitate Blocare	Numărul de minute de inactivitate a utilizatorului pe dispozitiv, după care dispozitivul va fi blocat. Utilizatorul trebuie să deblocheze dispozitivul după această perioadă, introducând parola acestuia.	
Expirarea parolei	Setați timpul până când trebuie setată o nouă parolă	
Restricționarea istoricului parolelor	Numărul de parole utilizate anterior, care nu sunt permise	
Numărul maxim de încercări de parole eșuate	Numărul de ori în care parola poate fi introdusă incorect, înainte de a se efectua o ștergere completă a dispozitivului	

Antivirus

Setări antivirus - Setare configurare scanare	
Tip de scanare	Selectează dacă să efectuați o scanare rapidă sau o scanare completă
Setați începutul scanării	Selectează ora din zi la care Windows Defender va începe scanarea
Frecvența de scanare	Selectează ziua în care ar trebui să ruleze scanarea Windows Defender
Frecvența actualizării semnăturii	Speciefies intervalul în ore care va fi utilizat pentru verificarea semnăturilor

Configurați tipul de fișiere pentru scanare	
Permiteți scanarea fișierelor de arhivă	Permiteți sau nu permiteți scanarea arhivelor (cum ar fi .zip) atunci când sunt accesate.
Permiteți scanarea scripturilor	Permite sau nu permite funcționalitatea Windows Defender Script Scanning.
Permiteți scanarea e-mailurilor	Permiteți sau nu permiteți scanarea e-mailurilor.
Permiteți scanarea fișierelor de rețea	Permiteți sau nu permiteți scanarea fișierelor de rețea.
Permiteți scanarea completă a unităților de rețea mapate	Permiteți sau nu permiteți scanarea unităților de rețea mapate (activată numai atunci când scanarea completă este activată).
Controlul scanării bidirecționale	Controlează ce seturi de fișiere ar trebui monitorizate.
Permiteți scanarea completă a unităților amovibile	Permiteți sau nu permiteți scanarea completă a unităților amovibile. Numai în timpul scanării complete este inițiată.

Tipul de fișiere care urmează să fie excluse din scanare	
Ignorați tipurile de fișiere pentru scanare	Definiți un set de tipuri de extensii de fișiere. Fiecare extensie de fișier pentru fiecare câmp.
Ignorarea căilor directoarelor	Definiți un set de căi de directoare pentru a nu le scana. O cale per câmp. Exemple: "C:\Example", "C:\Windows" sau "C:\Users".
Excluderea proceselor din scanare	Excludeți fișierele care au fost deschise de anumite procese din scanările Microsoft Defender Antivirus. . O cale per câmp. Exemple: "C:\myFile.exe", "C:\Windows\myProcess.exe", "C:\myScript.bat

Setări suplimentare	
Permiteți monitorizarea în timp real	Permiteți sau nu permiteți funcționalitatea Windows Defender Realtime Monitoring
Permiteți monitorizarea comportamentului	Permiteți sau nu permiteți funcționalitatea Windows Behavior Monitoring
Permiteți protecția în cloud	Permiteți sau nu permiteți Windows Defender să trimită informații către Microsoft despre orice problemă pe care o găsește. Microsoft va analiza aceste informații, va afla mai multe despre problema care afectează dispozitivul și va oferi soluții îmbunătățite
	Comportamentul pentru trimiterea eșantioanelor
Permiteți protecția IOAV a Windows Defender	Permiteți sau nu permiteți protecția IOAV Windows Defender
Permiteți accesul la interfața "Protecție la acces" a Defenders	
Factor mediu de încărcare CPU	Reprezintă factorul mediu de încărcare a CPU pentru scanarea Windows Defender (în procente)

Gestionarea programelor malware	
Severitate scăzută	Puteți defini pentru fiecare nivel de severitate modul în care dispozitivul gestionează programele malware. Opțiunile disponibile sunt: • Curat • Carantină • Eliminați • Permiteți • Definit de utilizator • Bloc
Severitate moderată	
Severitate ridicată	
Severitate severă	
Zile pentru păstrarea malware-ului curățat	Perioada de timp în zile în care fișierele/articolele din carantină vor fi stocate pe sistem. Valoarea implicită este 0, care păstrează elementele în carantină și nu le elimină automat. Valoarea maximă este 90.

Centrul de securitate

Centrul de securitate Windows - Setări pentru securitatea Windows	
Dezactivați interfața de protecție împotriva virușilor și amenințărilor	
Ascundeți Ransomware Data Recovery UI	
Dezactivați protecția contului UI	
Dezactivați Firewall și protecția rețelei UI	
Dezactivați interfața de control pentru aplicații și browser	
Interziceți modificările la protecția împotriva exploatării	Interziceți utilizatorului să facă modificări la setările de protecție împotriva exploatării
Dezactivați interfața de securitate a dispozitivului	
Ascundeți depanarea TPM	Ascundeți setările de depanare TPM
Dezactivați butonul Clear TPM	
Dezactivați performanța dispozitivului și interfața de sănătate	
Dezactivați interfața cu opțiuni pentru familie	

Personalizați toasturile	
Activați informații de asistență personalizate	Activați afișarea informațiilor de contact de asistență personalizate pentru compania dvs. în partea din dreapta jos a aplicației Security Center.
Adresa de e-mail	Setați adresa de e-mail a companiei
Numele companiei	Setați numele companiei
Telefonul companiei	Setați telefonul companiei
URL ajutor	Setați URL-ul de ajutor al companiei

Setări suplimentare	
Dezactivați notificările	Dezactivați afișarea notificărilor Centrului de securitate Windows Defender.
Ascundeți recomandările de actualizare a firmware-ului TPM	Ascundeți recomandarea de a actualiza TPM Firmware atunci când este detectat un firmware vulnerabil.
Afișați numele companiei și opțiunile de contact	Afișați numele companiei dvs. și opțiunile de contact într-un card de contact în Centrul de securitate Windows Defender.
Ascundeți Secure Boot	Ascundeți zona de boot de securitate.
Ascundeți controlul zonei de notificare de securitate	Ascundeți controlul zonei de notificare Windows Security.

Configurarea firewall-ului

Configurarea firewall-ului - Setări globale	
Ignorarea setului de autentificare	Ignorați întregul set de autentificare dacă acestea nu acceptă toate suitele de autentificare specificate în set
Tipul de așteptare a pachetelor	Specifică modul în care scalarea pentru software-ul de pe partea de recepție este activată atât pentru recepția criptată, cât și pentru calea de expediere clară pentru scenariul IPsec tunnel gateway.
Dezactivați efectuarea filtrării FTP cu stare	Dacă este dezactivat, nu va efectua filtrarea FTP (File Transfer Protocol) pentru a permite conexiuni secundare
Timpul de inactivitate al asociației de securitate	Acest câmp configurează timpul de inactivitate al asociației de securitate, în secunde. Asociațiile de securitate sunt șterse după ce traficul de rețea nu este observat pentru această perioadă de timp specificată.
Codificarea cheii partajate	Setați codarea cheii precomparate
Excepții IPSec	Configurarea excepțiilor protocolului Internet
Verificarea listei de revocare a certificatelor	

Profiluri Firewall (Profil de domeniu / Profil privat / Profil public)	
Activați Firewall pentru acest profil	
Dezactivați notificările	Dezactivați afișarea notificării către utilizator atunci când o aplicație este blocată de la ascultarea pe un port.
Blocarea răspunsurilor unicast la difuzările multicast	
Aplicarea regulilor firewall pentru aplicații autorizate	Dacă nu este aplicată, regulile firewall ale aplicațiilor autorizate din magazinul local sunt ignorate și nu sunt aplicate
Aplicarea regulilor firewall globale pentru porturi	Dacă nu este aplicată, regulile firewall pentru portul global din stocul local sunt ignorate și nu sunt aplicate. Setarea are sens numai dacă este setată sau enumerată în depozitul de politici de grup sau dacă este enumerată din depozitul GroupPolicyRSoPStore
Aplicarea regulilor firewall	Dacă nu este aplicată, regulile firewall din magazinul local sunt ignorate și nu sunt aplicate
Aplicarea regulilor de securitate a conexiunilor	Dacă nu este aplicată, regulile de securitate a conexiunii din magazinul local sunt ignorate și nu sunt aplicate
Acțiune implicită de ieșire	Acțiunea pe care firewall-ul o efectuează în mod implicit la conexiunile de ieșire
Acțiune de intrare implicită	Acțiunea pe care firewall-ul o efectuează în mod implicit la conexiunile de intrare
Dezactivați modul Stealth	Modul Stealth este un mecanism din Windows Firewall care ajută la prevenirea descoperirii de către utilizatorii rău intenționați a informațiilor despre computerele din rețea și serviciile pe care acestea le rulează.
Dezactivați prevenirea răspunsului la traficul nesolicitat	Dacă sunt dezactivate, regulile de mod stealth ale firewall-ului nu trebuie să împiedice computerul gazdă să răspundă la traficul de rețea nesolicitat dacă traficul respectiv este securizat prin IPsec

Reguli Firewall

Reguli Firewall	
Nume și prenume	Denumirea regulii
Descriere	Descrierea normei
Acțiune	Specificați dacă această regulă va bloca traficul sau îl va permite. Vă rugăm să luați în considerare faptul că opțiunea Block ar putea bloca și traficul (în funcție de restul configurației) între serverul MDM și dispozitiv
Direcție	
Enable Edge traversal (Activare traversare margine) (Disponibil numai când **Direcția** este setată la **trafic de intrare**)	Indică faptul că traficul de intrare specific este permis să treacă prin tunelurile NAT și alte dispozitive de margine utilizând tehnologia de tunelare Teredo.

Programe și servicii	
Definiți aplicațiile, toate altfel	Dacă nu este activat, atunci se vor lua în considerare toate cererile
Nume familie pachet	Numele familiei de pachete la care se va aplica regula.
Calea de fișier a aplicației	Aplicația completă, cum ar fi C:\Windows\System\Notepad.exe, la care se va aplica regula
Nume binar complet calificat	Fully Qualified Binary Name (Nume binar complet calificat) la care se va aplica regula. O FQBN este un șir în următoarea formă: {Publisher\Product\Filename,Version}
Numele serviciului	Introduceți numele unui serviciu (de exemplu, "EventLog"). Puteți obține o listă de nume de servicii în Powershell executând comanda "Get-Service".

Protocoale și porturi				
Protocol	Protocolul utilizat de regulă.			
	Valori disponibile: - Orice - Personalizat - HOPORT - ICMPv4 - IGMP - TCP - UDP - IPv6 - Rută IPv6 - IPv6-Frag - GRE - ICMPv6 - IPv6-NoNxt - IPv6-Opts - VRRP - PGM - L2TP	Când este setat la Personalizat	Introduceți un număr de protocol între 0 și 255	Numărul protocolului
		Când este setat la TCP sau UDP	Specificați porturile locale, în caz contrar vor fi utilizate toate	Porturile locale pe care regula le va utiliza; sunt permise și porturile de interval
			Port local	Un singur port sau un interval de porturi. De exemplu, 100-120, 200, 300-320.
			Specificați porturile de la distanță; în caz contrar, toate vor fi utilizate	Porturile de la distanță pe care regula le va utiliza; sunt permise și porturile de interval
			Port la distanță	Un singur port sau un interval de porturi. De exemplu, 100-120, 200, 300-320.

Domeniul de aplicare	
Specificați IP-uri locale, orice IP în caz contrar	Set de IP-uri locale, poate fi și un interval de IP-uri separate prin -
Adresa IP locală	Set de IP-uri unice sau un interval de IP-uri separate prin -
Specificați IP-urile de la distanță, în caz contrar orice IP de la distanță	Specificați un set de IP-uri la distanță, poate fi și un interval de IP-uri separate prin "-".
Adresa IP la distanță	Specificați IP-uri unice sau un interval de IP-uri
Jetoane	Token-uri care pot fi setate împreună cu adresele la distanță. Tokens Intranet, RmtIntranet și Ply2Renders sunt acceptate în Windows 10, versiunea 1809 și ulterioare.

Setări avansate

Specificați profilurile, în caz contrar toate vor fi utilizate	Dacă este dezactivat, vor fi utilizate toate profilurile
Domeniu	Profilul domeniului
Privat	Profil privat
Public	Profil public
Specificați interfețele, în caz contrar vor fi utilizate toate interfețele	Dacă este dezactivat, vor fi utilizate toate interfețele
Rețea locală	Interfață de rețea locală
Acces la distanță	Interfață de acces la distanță
Fără fir	Interfață fără fir

Directorii locali	
Adăugați utilizatori locali autorizați	Permiteți adăugarea unei liste de utilizatori locali care vor utiliza această regulă
Utilizatori autorizați	Lista utilizatorilor locali autorizați pentru această regulă. Utilizatorul trebuie să fie în format SDDL (Security Description Definition Language), de exemplu PC_NAME\USERNAME. Acest câmp nu trebuie completat dacă un nume de serviciu este setat să utilizeze această regulă

Setări de restricționare

Funcționalitatea dispozitivului

Permiteți cardul SD	Permiteți utilizarea unui card SD
Permiteți camera	Permiteți utilizarea camerei
Permiteți serviciul de localizare	Permiteți serviciul de localizare a dispozitivului
Permiteți Sideloading-ul aplicației	Permiteți instalarea de aplicații din surse necunoscute
Permiteți modul dezvoltator	Permite modul dezvoltator
Permiteți roamingul de date celulare	Permiteți roamingul de date celulare
Permiteți Cortana	Permiteți asistentului vocal Cortana
Permiteți căutării să utilizeze locația	Permiteți căutării să utilizeze locația
Permiteți adăugarea unui cont de e-mail care nu este Microsoft	Specificați dacă utilizatorului i se permite să adauge alte conturi de e-mail decât MSA.
Permiteți conectarea la contul Microsoft	Specificați dacă permiteți utilizarea contului MSA pentru autentificarea și serviciile de conectare care nu sunt legate de e-mail.
Permiteți sincronizarea setărilor mele	Permite sincronizarea setărilor pe întregul dispozitiv
Nume de domenii protejate pentru întreprinderi	Specifică numele domeniului întreprinderii separate prin ";".
Permiteți utilizatorului să dezactiveze	Permite utilizatorului să dezactiveze Restaurarea sistemului. **AVERTISMENT!**

restaurarea sistemului	Această caracteristică trebuie utilizată numai pe dispozitive care sunt deținute sau furnizate de compania sau organizația întreprinderii sau pe un dispozitiv deținut de utilizator, în cazul în care utilizatorul permite ca dispozitivul să fie gestionat integral de compania întreprinderii. Dacă dezactivați această setare de politică, Restaurarea sistemului este dezactivată, iar Asistentul pentru restaurarea sistemului nu poate fi accesat. Opțiunea de a configura Restaurarea sistemului sau de a crea un punct de restaurare prin Protecția sistemului este, de asemenea, dezactivată.
Permiteți dezînscrierea utilizatorului	Permite utilizatorului să elimine partea corporativă de pe dispozitiv și astfel să se deconecteze de la serverele AppTec360. Dacă acest lucru se întâmplă, nu va mai fi posibilă gestionarea dispozitivului **AVERTISMENT!** Această caracteristică trebuie utilizată numai pe dispozitive care sunt deținute sau furnizate de compania sau organizația întreprinderii sau pe un dispozitiv deținut de utilizator, în cazul în care utilizatorul permite ca dispozitivul să fie gestionat integral de compania întreprinderii. Dacă dezactivați această setare de politică, utilizatorii nu vor putea să elimine înscrierile MDM. Specificați dacă utilizatorului i se permite să șteargă contul de la locul de muncă prin intermediul panoului de control al locului de muncă. Serverul MDM poate șterge întotdeauna contul de la distanță.

BitLocker

Configurarea BitLocker

Setări generale	
Cer criptarea dispozitivelor	Invitați utilizatorii să activeze criptarea dispozitivului.În funcție de ediția Windows și de configurația sistemului, utilizatorii pot fi invitați: - Pentru a confirma că criptarea de la un alt furnizor nu este activată. - Pentru a dezactiva BitLocker Drive Encryption și apoi pentru a activa BitLocker din nou.
Metode de criptare	
Metodă de criptare pentru unitățile sistemului de operare	
Metodă de criptare pentru unitățile fixe de stocare a datelor	
Metodă de criptare pentru unități de date amovibile	
Dezactivați avertizarea cu privire la criptarea discurilor de către terți	Dezactivați solicitarea de avertizare cu privire la un serviciu terț de criptare a discurilor utilizat pe dispozitiv. Începând cu Windows 10, versiunea 1803, această setare este acceptată numai pentru dispozitivele conectate la Azure Active Directory.
Permiteți rularea criptării în timp ce utilizatorul non-administrator este conectat	Compatibil numai pentru dispozitivele conectate la Azure Active Directory

Extensii AppTec360		
Criptare silențioasă		Dacă este selectat împreună cu "Necesită criptarea dispozitivului", serviciul de administrare AppTec360 va executa criptarea automată silențioasă a unităților dispozitivului.
	Generarea automată a acreditărilor de utilizator	Unitatea sistemului de operare criptată va fi protejată cu credențiale de utilizator generate automat. Fie un PIN TPM, atunci când este disponibil un TPM, fie o parolă textuală cu 6 cifre. Acreditările generate sunt trimise la adresa de e-mail înregistrată pentru dispozitivul respectiv. Dacă această opțiune este dezactivată, singura protecție posibilă pentru criptarea silențioasă este utilizarea TPM. În acest caz, pentru dispozitivele fără TPM, criptarea silențioasă va eșua.
	Criptarea unităților fixe	Toate unitățile de date fixe disponibile vor fi, de asemenea, criptate și protejate cu "deblocare automată" utilizând o cheie stocată pe unitatea sistemului de operare.

Setări unitate OS		
Necesitatea unei autentificări suplimentare la pornire		Această setare vă permite să configurați dacă BitLocker necesită o autentificare de fiecare dată când computerul pornește. Această setare este aplicată în timpul configurării BitLocker. Dacă activați această setare, utilizatorii pot configura opțiuni avansate de pornire în expertul de configurare BitLocker.
	Blocați BitLocker fără un TPM compatibil	
	Numai TPM	
	TPM și PIN	
	TPM și cheie	
	TPM, cheie și PIN	Dacă doriți să solicitați utilizarea unui cod PIN și a unei unități flash USB (cheie), utilizatorul trebuie să configureze BitLocker utilizând instrumentul din linia de comandă "manage-bde" în locul asistentului de configurare BitLocker Drive Encryption.

Solicită lungimea minimă a PIN-ului	
	Caractere minime

Configurați mesajul și URL-ul de recuperare înainte de pornire	Configurați întregul mesaj de recuperare sau înlocuiți URL-ul existent care este afișat pe ecranul de recuperare a cheii înainte de pornire atunci când unitatea sistemului de operare este blocată. Notă: Nu toate caracterele și limbile sunt acceptate în pre-boot. Vă recomandăm insistent să verificați dacă caracterele pe care le utilizați apar corect pe ecranul de recuperare înainte de pornire.
	Opțiunea mesajului de recuperare înainte de pornire
	Mesaj de recuperare personalizat
	URL de recuperare personalizat

Opțiuni de recuperare a unității OS		Această setare vă permite să controlați modul în care unitățile sistemului de operare protejate prin BitLocker sunt recuperate în absența acreditărilor necesare. Această setare este aplicată în timpul configurării BitLocker. În mod implicit, este permis un agent de recuperare a datelor bazat pe certificat, opțiunile de recuperare pot fi specificate de către utilizator, inclusiv parola și cheia de recuperare, iar informațiile de recuperare nu sunt salvate în AD DS.
	Agent de recuperare a datelor bazat pe certificate de bloc	Specificați dacă un agent de recuperare a datelor poate fi utilizat cu unități ale sistemului de operare protejate de BitLocker. Înainte de a putea fi utilizat, un agent de recuperare a datelor trebuie adăugat de la elementul Politici privind cheile publice, fie în Consola de gestionare a politicilor de grup, fie în Editorul local de politici de grup. Consultați BitLocker Drive Encryption Deployment Guide de pe Microsoft TechNet pentru mai multe informații despre adăugarea agenților de recuperare a datelor.
	Setări pentru parola de recuperare BitLocker	
	Setări cheie de recuperare BitLocker	
	Salvați informațiile de recuperare BitLocker în Active Directory Domain Services	
	Configurarea stocării de recuperare AD DS BitLocker	Stocarea pachetului de chei permite recuperarea datelor de pe o unitate care a fost deteriorată fizic.
	Necesitatea stocării datelor de recuperare în AD DS	Împiedicați utilizatorii să activeze BitLocker, cu excepția cazului în care computerul este conectat la domeniu și

Setări fixe ale acționării	
Opțiuni de recuperare a unităților fixe	Această setare vă permite să controlați modul în care unitățile fixe protejate prin BitLocker sunt recuperate în absența acreditărilor necesare. Această setare este aplicată în timpul configurării BitLocker. În mod implicit, este permis un agent de recuperare a datelor bazat pe certificat, opțiunile de recuperare pot fi specificate de către utilizator, inclusiv parola și cheia de recuperare, iar informațiile de recuperare nu sunt salvate în AD DS.
Agent de recuperare a datelor bazat pe certificate de bloc	
Setări pentru parola de recuperare BitLocker	
Setări cheie de recuperare BitLocker	
Salvați informațiile de recuperare BitLocker în Active Directory Domain Services	
Configurarea stocării de recuperare AD DS BitLocker	Stocarea pachetului de chei permite recuperarea datelor de pe o unitate care a fost deteriorată fizic.
Necesitatea stocării datelor de recuperare în AD DS	Împiedicați utilizatorii să activeze BitLocker, cu excepția cazului în care computerul este conectat la domeniu și copia de rezervă a informațiilor de recuperare BitLocker în AD DS reușește. Notă: Parola de recuperare este generată automat.
Refuzați accesul în scris la unități fixe neprotejate	

Setări unitate amovibilă	
Refuzați accesul în scris la unități amovibile neprotejate	Refuzați accesul în scris la unitățile de date amovibile care nu sunt protejate de Bitlocker. Notă: Dacă opțiunea "Removable Disks: Deny write access" este activată în politica de grup, această setare de politică va fi ignorată.
Refuzarea accesului în scris la dispozitivele configurate într-o altă organizație	Numai unitățile cu câmpuri de identificare care corespund câmpurilor de identificare ale computerului vor primi acces în scris. Aceste câmpuri sunt definite prin setarea de politică de grup "Furnizați identificatorii unici pentru organizația dvs.".

Starea BitLocker

Aici puteți vedea starea curentă a unităților criptate BitLocker

C [OS Drive]
Stare criptare
Criptate (%)
Statutul de protecție
Metoda de criptare
Protectori de chei
Recuperare parolă

Cu un clic pe butonul "Rotiți parola de recuperare" puteți roti parola de recuperare BitLocker.

Managementul certificatelor

Lista certificatelor

Iată o listă a certificatelor care sunt instalate pe dispozitivul afișat.

Configurarea certificatului

Aici puteți configura certificatele și modul în care acestea vor fi instalate pe dispozitiv.

Certificat de încredere	
Descriere	Descrierea certificatului
Domeniul de aplicare	Domeniul de aplicare al implementării certificatului: Utilizator curent vs Dispozitiv
Magazin de certificate	"Certificate neîncrezătoare" este disponibilă numai începând cu Windows 10, versiunea 1803
Fișier de certificat	Încărcați un fișier PKCS#1

Certificat de identitate			
Descriere	Descrierea certificatului		
Domeniul de aplicare	Domeniul de aplicare al implementării certificatului: Utilizator curent vs Dispozitiv		
Locație cheie	Furnizorul de stocare a cheilor pentru instalarea cheii private.		
		TPM. Eșuează dacă nu este prezent niciun TPM	
	TPM. Dacă nu există TPM, se revine la Software KSP		
	Software Key Storage Provider		Marcați cheia privată ca fiind exportabilă
	Windows Hello pentru afaceri	Denumirea recipientului	Specifică numele recipientului Windows Hello for Business (cunoscut anterior ca Microsoft Passport for Work).
		Text prompt PIN	Specifică textul personalizat care se afișează la solicitarea PIN-ului Windows Hello for Business în timpul înregistrării certificatului.
Acreditare	Încărcați un fișier PKCS#12		

SCEP

Descriere	Descrierea serverului SCEP		
Domeniul de aplicare al implementării	Domeniul de aplicare al implementării certificatului: Dispozitiv curent vs Utilizator		
URL-uri ale serverului SCEP	Unul sau mai multe servere care emit certificate prin SCEP		
Subiect	Reprezentarea unui nume X.500. De exemplu, "C=US, O=Microsoft Corporation, CN=foo, 1.2.5.3=bar"		
Nume alternative ale subiectului	Tip	Adresa de e-mail	
		DNS	
		URI	
		Nume principal utilizator (UPN)	
Amprenta digitală CA	Amprenta SHA1 a certificatului autorității de certificare. E.g. 31:8F:1E:78:5C:D5:12:9F:7E:3B:AD:F3:1C:C0:19:03:96:43:A9:E5		
Perioada de valabilitate unități	Zile, luni sau ani		
Perioada de valabilitate			
Provocare	Utilizat ca secret partajat în prealabil pentru înscrierea automată		
Reîncercări	Numărul de încercări pe care dispozitivul trebuie să le facă din nou dacă serverul trimite un răspuns PENDING. Valoarea implicită este 5. Valoarea maximă este 30.		
Întârziere reluare	Numărul de minute de așteptat înainte de reluarea încercării. Valoarea implicită este 5. Valoarea minimă este 1.		
Dimensiunea cheii	Dimensiunea cheii în biți		
Algoritmul Hash	Familia de algoritmi Hash		
Utilizare cheie	Extensia privind utilizarea cheii definește scopul (de exemplu, cifrare, semnătură) cheii conținute în certificat. Trebuie selectată cel puțin una dintre opțiunile "Digital signature" sau "Key encipherment".		
Utilizarea extinsă a cheilor	Specifică utilizarea cheilor extinse. sub rezerva configurației serverului SCEP. Specificați lista de OID-uri corespunzătoare, de exemplu 1.3.6.1.5.5.7.3.2		

	(Autentificare client)		
Locație cheie	Furnizorul de stocare a cheilor pentru instalarea cheii private.		
		TPM. Eșuează dacă nu este prezent niciun TPM	
	TPM. Dacă nu există TPM, se revine la Software KSP		
	Software Key Storage Provider		
	Windows Hello pentru afaceri	Denumirea recipientului	Specifică numele recipientului Windows Hello for Business (cunoscut anterior ca Microsoft Passport for Work).
		Text prompt PIN	Specifică textul personalizat care se afișează la solicitarea PIN-ului Windows Hello for Business în timpul înregistrării certificatului.

Gestionarea conexiunilor

Wifi

La această setare, efectuați preconfigurarea dispozitivelor utilizatorului final pentru accesul la punctele de acces interne

Identificatorul setului de servicii (SSID)	SSID pentru rețeaua la care va fi stabilită conexiunea
Auto Join	Activați conectarea automată la rețea
Rețea ascunsă	Activare, în cazul în care AP nu transmite SSID-ul

Tip de securitate

Stabilirea tipului de securitate AP

Sistem deschis WEP	
Parolă	Parolă pentru AP

WPA PSK	
Parolă	Parolă pentru AP

WPA EAP	
Tip de autentificare	Tip de autentificare, posibil numai cu "PEAP-MSCAHPv2"
Reconectare rapidă	Dispozitivele pot comuta între punctele de acces, fără a fi nevoie să se autentifice din nou
Accesul oaspeților	Utilizatorul nu are un cont și, prin urmare, trebuie să se înregistreze ca invitat
Verificări de carantină	Clientul trebuie să efectueze verificări NAP (Network Access Protection) și să partajeze rezultatele cu sistemul, care decide apoi dacă clientul se poate conecta
Necesită Crypto Binding	Autentificarea este posibilă numai prin Crypto Binding
Validarea serverului	Clientul verifică dacă certificatul serverului este valabil. Dacă acesta este cazul, se va stabili o conexiune
Prompt pentru certificate	Permite utilizatorului să accepte certificate care nu sunt de încredere
Nume server	Oferă opțiunea de a afișa numele serverului RADIUS, care oferă autentificarea și autorizarea în rețea

WPA2-PSK	
Parolă	Parolă AP

WPA2 EAP	
Tip de autentificare	Tip de autentificare, posibil numai cu "PEAP-MSCAHPv2"
Reconectare rapidă	
Accesul oaspeților	
Verificări de carantină	Activează protecția accesului la rețea NAP
Necesită Crypto Binding	Autentificarea este posibilă numai prin Crypto Binding
Validarea serverului	
Prompt pentru certificate	Solicită un certificat de server validat, un nume sau un certificat rădăcină de autentificare (CA)
Nume server	Lista serverelor care ar trebui să fie de încredere pentru dispozitive
Niciuna	Nu există securitate stabilită
Utilizați serverul proxy	Utilizarea unui server proxy
Adresa serverului	Adresa serverului proxy
Port server	Portul serverului serverului proxy

Utilizați serverul proxy

Activați utilizarea serverului proxy.

Adresa serverului	Adresa serverului proxy utilizat de această rețea.
Port server	Portul serverului proxy utilizat de această rețea.

Restricții Wifi

Aici puteți defini diverse restricții Wifi.

Permiteți WiFi	Permiteți/refuzați WiFi
Permiteți partajarea pe Internet	Permiteți utilizarea unui Hotspot
Permiteți conectarea automată la WiFi Sense Hot Spots	Permiteți conectarea automată la WiFi Sense Hot Spots
Permiteți configurarea manuală WiFi	Permite utilizatorului să se conecteze la rețele WiFi, care nu au fost definite de AppTec
Frecvența de scanare WLAN	Stabilește intervalul WLAN-Scan. Aici, o valoare mai mare crește capacitatea de a recunoaște rețelele WIFI.

VPN

Efectuați setările corespunzătoare aici, pentru a configura conexiunile VPN

Nume conexiune	Numele conexiunii indicate		
Tip VPN	O conexiune VPN Per-App este utilizată pentru a securiza traficul anumitor aplicații.		
	VPN	Întotdeauna pornit	Acest lucru va conecta automat VPN-ul la autentificare și va rămâne conectat până când utilizatorul se deconectează manual.
	VPN per aplicație	Aplicații VPN	Definiți aplicațiile care utilizează această conexiune VPN
		Blocare pe aplicație	Per-App Lockdown face ca aplicațiile selectate să aibă conectivitate numai prin această conexiune VPN. Această caracteristică depinde de Windows Defender Firewall.
	Profil WIP	Domeniu WIP pentru această conexiune	Enterprise ID, care este necesar pentru conectarea acestui profil VPN la o politică de protecție a informațiilor Windows (WIP)

Tip de conexiune

AppTec360 VPN	
Pentru "AppTec360 VPN" este necesar ca încărcarea laterală a aplicațiilor să fie permisă. Vă rugăm să activați "Allow App Sideloading" în "Security Management" → "Restriction Settings" → "Device Functionality".	
Configurarea gateway-ului	Pentru a configura o conexiune VPN cu lista neagră, vă rugăm să selectați o configurație VPN cu un server DNS specificat. Puteți seta o configurație VPN în "Setări generale" → "Universal Gateway" → "Setări VPN".

IKEv2		
Servere	Lista de servere VPN	
Tunel dispozitiv	Activarea conexiunii înainte de conectarea utilizatorului.	
Metoda de autentificare	EAP	EAP XML
	Certificate de mașină	
Algoritm de criptare		
Algoritm de verificare a integrității		
Grupul Diffie-Hellman		
Algoritm de transformare a cifrului		
Algoritm de transformare a autentificării		
Grupul PFS (Perfect forward secrecy)		

PPTP		
Servere	Lista de servere VPN	
Metoda de autentificare	EAP	EAP XML

L2TP		
Servere	Lista de servere VPN	
Metoda de autentificare	EAP	EAP XML
Algoritm de criptare		
Algoritm de verificare a integrității		
Grupul Diffie-Hellman		
Algoritm de transformare a cifrului		
Algoritm de transformare a autentificării		
Grupul PFS (Perfect forward secrecy)		

Automată		
Servere	Lista de servere VPN	
Metoda de autentificare	EAP	EAP XML

Configurații VPN generice

Rețineți datele de identificare la fiecare conectare	
Înregistrarea adreselor IP cu DNS intern	
Reguli de filtrare a traficului de rețea	Limitați conexiunea VPN la setul de reguli definit.
Lista de căutare a sufixelor DNS	Sufixe DNS de adăugat la lista de căutare DNS pentru rutarea numelor scurte.
Reguli NRPT (Name Resolution Policy Table)	Regulile tabelului de politici de rezolvare a numelor (NRPT) definesc modul în care DNS rezolvă numele atunci când este conectat la VPN.
Detectarea rețelelor de încredere	Lista de sufixe DNS pentru identificarea rețelei de încredere.
Tunelare divizată	Tunelarea divizată înseamnă că traficul poate trece prin orice interfață determinată de stiva de rețea.
Rute de tunelare divizate	Lista de rute care urmează să fie adăugate la tabela de rutare pentru interfața VPN.
Configurare proxy	Configurează Proxy-ul utilizat cu această rețea
Adresă proxy	Adresa serverului proxy sub forma unui nume de gazdă complet calificat sau a unei adrese IP.
Port	Portul serverului proxy.
Proxy Auto-Config URL	URL pentru a prelua automat setările proxy.

Restricții VPN

Aici puteți defini diverse restricții VPN.

Permiteți setările VPN	Acest ghid permite/interzice utilizatorului să dezactiveze și să schimbe setările VPN
Permiteți VPN pe celular	Permite/nepermite dispozitivului să stabilească o conexiune VPN, dacă dispozitivul utilizează date mobile
Permiteți roamingul VPN prin rețeaua celulară	Permite/interzice dispozitivului să stabilească o conexiune VPN, dacă dispozitivul este în roaming

Bluetooth

Aici puteți stabili dacă Bluetooth ar trebui să fie permis/interzis.

Permiteți Bluetooth	Activarea/dezactivarea Bluetooth

Gestionarea PIM

Exchange Active Sync

Configurarea contului ActiveSync pe dispozitivul utilizatorului final

Numele contului	Numele contului de e-mail
Nume gazdă server	Adresa serverului/FQDN
Numele domeniului	Domeniul serverului
Adresa de e-mail	Adresa de e-mail
Nume utilizator	Numele utilizatorului
Parolă utilizator	Opțional, puteți atașa deja o parolă utilizatorului aici
Utilizați SSL	Utilizați conexiunea SSL
Interval de sincronizare	Aici poate fi stabilit intervalul de sincronizare Sincronizare manuală = Utilizatorul trebuie să își descarce e-mailurile și să efectueze o sincronizare manuală
Filtru de vârstă a corespondenței	Perioada de timp până când e-mailurile ar trebui să fie sincronizate Fără filtru = nelimitat
Nivelul jurnalului	Stabilirea nivelurilor de logare pentru traficul ActiveSync
Sincronizare e-mail	Activat = e-mailurile sunt sincronizate
Sincronizarea contactelor	Activat = contactele sunt sincronizate
Sincronizarea calendarului	Activat = calendarul este sincronizat
Sincronizarea sarcinilor	Activat = sarcinile sunt sincronizate

eMail

Crearea de conturi POP3/IMAP4 pe dispozitivul utilizatorului final.

Descrierea contului	Numele contului de e-mail
Numele expeditorului	Numele expeditorului afișat
Numele domeniului	Numele de domeniu pentru contul de e-mail
Adresa de e-mail	Adresa de e-mail a utilizatorului
Nume utilizator	Numele utilizatorului
Parolă utilizator	Opțional, puteți atașa deja o parolă utilizatorului aici
Autentificări alternative ale serverului de ieșire	Aici se poate defini, dacă sunt necesare alte acreditări pentru serverul de ieșire
Nume de domeniu de ieșire	Numele domeniului de ieșire
Numele de utilizator al serverului de ieșire	Numele de utilizator al serverului de ieșire
Parola serverului de ieșire	Parola serverului de ieșire
Protocolul de e-mail	POP3 sau IMAP4, poate fi utilizat ca protocol
Nume gazdă server de poștă electronică de intrare	Numele gazdei serverului de e-mail de intrare
Utilizați SSL pentru e-mailurile primite	Utilizați SSL pentru e-mailurile primite
Numele gazdei serverului de corespondență de ieșire	Numele gazdei serverului de e-mail de ieșire
Utilizați SSL pentru e-mailurile de ieșire	Utilizați SSL pentru e-mailurile de ieșire
Autentificarea serverului de ieșire	Este necesară o autentificare a serverului de ieșire
Interval de sincronizare	Aici poate fi stabilit intervalul de sincronizare Sincronizare manuală = Utilizatorul trebuie să își descarce e-mailurile și să efectueze o sincronizare manuală
Filtru de vârstă a corespondenței	Perioada de timp până când e-mailurile ar trebui să fie sincronizate Fără filtru = nelimitat

Gestionarea aplicațiilor

Enterprise App Manager

Aplicații instalate

Iată o listă a aplicațiilor care sunt instalate în prezent pe dispozitivul afișat.

Aplicații obligatorii

Aici puteți configura o listă de aplicații care sunt obligatorii pe dispozitiv.

Această listă va fi verificată de fiecare dată când dispozitivul se conectează la MDM și va instala toate aplicațiile de pe această listă care se întâmplă să nu fie instalate pe dispozitiv, indiferent dacă aplicația a fost dezinstalată sau nu a fost niciodată instalată înainte.

Puteți încărca Windows 10 In-House Apps și apoi să le adăugați în această listă sau puteți adăuga configurații Microsoft Office care trebuie să fie configurate în prealabil în "Setări generale" > "Administrare aplicații" > "Microsoft Office".

Restricții aplicații sistem

Aplicații Inbox
Permiteți alarme și ceas
Calculator Allow
Permiteți camera
Permiteți Contact Suport
Permiteți Cortana
Permiteți Explorer fișier
Permiteți începerea
Permiteți muzica Groove
Permiteți hărți
Permiteți mesageria
Permiteți Microsoft Edge
Permiteți filme și TV
Permiteți bani
Allow News
Permiteți OneDrive
Permiteți OneNote
Permiteți Outlook Calendar și Mail
Permiteți oamenilor
Permiteți telefonul
Permiteți fotografii
Permiteți Powerpoint
Permiteți setările
Permiteți Skype
Permiteți Sport
Permiteți Magazin
Permiteți Recorder de voce
Permiteți portofelul
Permiteți vremea

Permiteți Windows Feedback Hub
Permiteți cuvântul
Permiteți Xbox

Setarea paginilor
Permiteți conturile Locul de muncă
Permiteți informații avansate
Permiteți colțul aplicațiilor
Permiteți blocarea și filtrarea
Permiteți profilul de culoare
Permiteți modul de conducere
Permiteți e-mail și conturi
Permiteți Egalizator
Permiteți tastatură
Permiteți bara de navigare
Permiteți modul avion al rețelei
Permiteți partajarea internetului în rețea
Permiteți serviciile de rețea
Permite rețea Wi-Fi
Permiteți sistemului PC Bluetooth
Permiteți evaluarea dispozitivului dvs.
Permiteți restaurarea actualizării
Permiteți partajarea
Permiteți începerea
Permiteți timp Limba
Timp permis Regiune
Permiteți ecranul de blocare implicit al Windows
Permiteți munca sau contul școlar

Lista neagră și lista albă

Sub "Listă albă și neagră", puteți alege între modul "Listă albă" și modul "Listă neagră".

Lista albă	Numai aplicațiile și serviciile care sunt adăugate la listă pot fi instalate pe dispozitivul utilizatorului final. Dacă acestea sunt deja preinstalate pe dispozitivul utilizatorului final, ele vor fi activate și setate, astfel încât utilizatorul să le poată rula.
	Toate celelalte aplicații care nu sunt adăugate la listă nu pot fi instalate pe dispozitivul utilizatorului final. Dacă acestea sunt deja preinstalate pe dispozitivul utilizatorului final, ele vor fi dezactivate și setate, astfel încât utilizatorul să nu le poată rula.
Lista neagră	Aplicațiile și serviciile care sunt adăugate la listă nu pot fi instalate pe dispozitivul utilizatorului final. Dacă acestea sunt deja preinstalate pe dispozitivul utilizatorului final, ele vor fi dezactivate și setate astfel încât utilizatorul să nu le poată rula.
	Toate celelalte aplicații care nu sunt adăugate la listă pot fi instalate pe dispozitivul utilizatorului final. Dacă acestea sunt deja preinstalate pe dispozitivul utilizatorului final, ele vor fi activate și setate, astfel încât utilizatorul să le poată rula.

Prin intermediul , adăugați aplicații sau servicii suplimentare la lista utilizată în prezent.

Cu ajutorul butonului , adăugați aplicații sau servicii suplimentare la lista inactivă în prezent.

Puteți adăuga o aplicație din "Magazinul de aplicații Windows" sau puteți introduce direct un "Identificator de aplicație" pentru a o adăuga pe lista neagră sau albă.

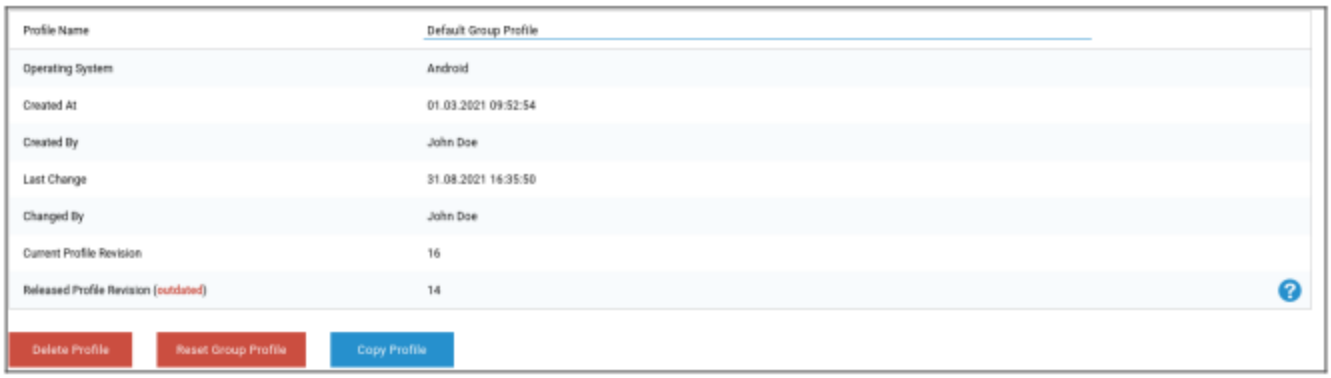
Configurație MacOS

În funcție de faptul că ați selectat un profil sau un dispozitiv, afișajul și subpunctele sale sunt diferite - vă rugăm să acordați o atenție deosebită acestui aspect!

Generalități

Prezentare generală a profilului grupului (numai la nivel de grup)

Atunci când deschideți un profil de grup, veți obține o prezentare generală rapidă a profilului.



Nume profil	Numele profilului (poate fi modificat aici)
Sistem de operare	Sistemul de operare pentru care este creat profilul
Creat la	Momentul creației
Creat de	Creatorul profilului
Ultima schimbare	Ora ultimei modificări a profilului
Schimbat de	Contul care a efectuat ultimele modificări
Revizuirea actuală a profilului	Revizuirea stării profilului salvat
Revizuire profil eliberată	Revizuirea profilului atribuit ("Atribuie acum"). Dacă eticheta afișează "(învechit)" în spatele textului, înseamnă că ați salvat profilul, dar nu l-ați atribuit încă, astfel încât dispozitivele vor primi în continuare o versiune mai veche.

Prezentare generală a dispozitivului (numai la nivel de dispozitiv)

Prezentare generală sumară a dispozitivului.

Numele dispozitivului	Numele dispozitivului
Model	Model
Sistem de operare	Sistem de operare
Numărul de serie	Numărul de serie al dispozitivului
Proprietatea dispozitivului	Tipul de proprietate configurat
Tip dispozitiv	Tipul de dispozitiv
Conform	Arată dacă dispozitivul este conform
Adresa IP	Adresa IP de la care dispozitivul s-a conectat la server
Văzut ultima dată	Ora ultimei conexiuni de la dispozitiv
Ultimul impuls	Ora ultimului push trimis către dispozitiv
Atribuire	Aici puteți muta dispozitivul la un alt utilizator sau grup

Revizuirea configurației (numai la nivel de dispozitiv)

Aici veți primi o prezentare generală a profilului de grup care este atribuit dispozitivului.

Dacă faceți clic pe profilul grupului, veți accesa direct profilul și veți putea efectua setările.

Cu ajutorul simbolului, puteți readuce aplicațiile alocate la setările profilului de grup.

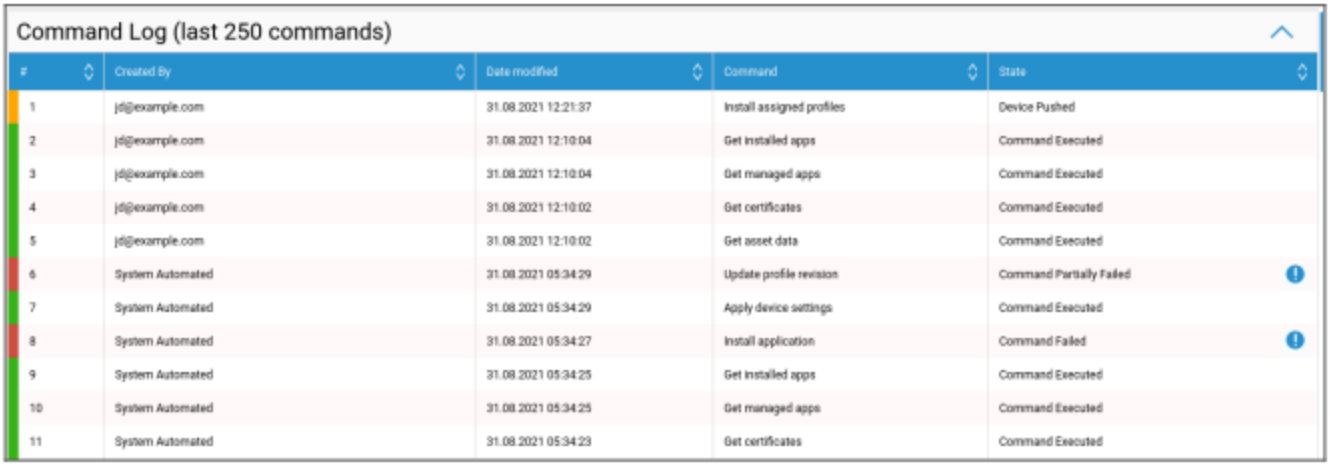
Cu ajutorul simbolului, puteți reseta profilul dispozitivului pentru a nu avea niciun fel de setări.

"Newer Revision available" indică faptul că profilul grupului a fost modificat și salvat, dar nu a fost atribuit. Profilul de grup trebuie să fie atribuit cu "Assign now" la nivel de grup pentru a aplica modificările dispozitivelor.

Jurnalul dispozitivului (numai la nivel de dispozitiv)

Jurnal de comandă

Aici puteți vedea ce comenzi au fost emise pentru dispozitiv și care este starea lor.



Comenzile create de "System Automated" sunt create automat de sistem.

Stări posibile ale comenzii

Dispozitiv împins	O solicitare push a fost trimisă către serviciul push (de exemplu, APNS) pentru a indica dispozitivului să se conecteze din nou la serverul EMM.
Comandă creată	Comanda a fost creată în sistem.
Comandă trimisă	Comanda a fost trimisă către dispozitiv după ce acesta s-a conectat la server.
Comandă executată	Comanda a fost executată cu succes.
Comandă eșuată	Comanda a eșuat. *
Comandă eșuată parțial	În funcție de sistemul de operare al dispozitivului, unele comenzi pot fi grupate împreună. În acest caz, unele părți ale acestui grup de comandă au eșuat. *
Comandă executată, eventual eșuată	Comanda a fost executată, dar poate că nu a fost.
Comanda Repushed	Comanda a fost respinsă de un utilizator.
Aruncată	Comanda a fost eliminată. De exemplu, pentru că a fost înlocuită de o altă comandă sau pentru că dispozitivul a fost înrolat din nou și comenzile vechi au fost eliminate

*Dacă există un semn al exclamării în spatele mesajului, puteți obține mai multe informații trecând cu cursorul peste pictogramă.

Gestionarea activelor (numai la nivel de dispozitiv)

Informații despre dispozitiv

Numărul modelului	Numărul modelului
Nume gazdă	Nume gazdă
Nume gazdă local	Nume gazdă local
Sistem de operare	Sistemul de operare
Versiunea sistemului de operare	Versiunea sistemului de operare
UDID	UDID
Memorie liberă / totală	Memorie liberă / totală

WiFi

Adresa IP	Adresa IP
WiFi MAC	WiFi MAC

Celulare

Număr de telefon	Număr de telefon
Starea de roaming	Starea de roaming
Roaming (voce / date)	Roaming (voce / date)
Adresa IP	Adresa IP
Operator/Carrier	Operator/Carrier
Rețea SIM Carrier	Rețea de transportatori
Versiunea de transport	Versiunea de transport
ICCID	ICCID
Actual MCC/MNC	Actual MCC/MNC
SIM MCC/MNC	SIM MCC/MNC

Bluetooth

Bluetooth MAC	Bluetooth MAC

Gestionarea actualizărilor (numai la nivel de dispozitiv)

Informații actualizate

Această filă prezintă informații despre setările de actualizare a sistemului de pe dispozitiv.

Autocheck activat	Dacă sistemul verifică automat actualizarea.
Actualizarea automată a aplicațiilor activată	Dacă sistemul va instala automat actualizările aplicațiilor.
Actualizări automate ale sistemului de operare activate	Dacă sistemul va instala automat actualizările OS.
Actualizări automate de securitate activate	Dacă sistemul va instala automat actualizările de securitate.
Actualizarea aplicației Descărcare în fundal activată	Dacă sistemul va descărca actualizări ale aplicațiilor în fundal.
Catalog URL	Adresa URL a catalogului de actualizări software pe care îl utilizează clientul.
Este catalogul implicit	Dacă "da", Catalogul este catalogul implicit.
Efectuați verificări periodice	Dacă "da", începeți o nouă scanare.
Data scanării anterioare	Data ultimei scanări a actualizării software.
Rezultatul scanării anterioare	Codul rezultat al ultimei scanări de actualizare a software-ului.

Managementul securității

Anti-furt

Ștergeți și blocați

Ștergere completă	Trimiteți o comandă pentru resetarea din fabrică a dispozitivului
Ștergere Enterprise	Îndepărtați MDM de pe dispozitiv și eliminați toate datele MDM (de exemplu, conturi, aplicații)
Ecran de blocare	Faceți dispozitivul să revină la ecranul de blocare

Configurația de securitate

Codul de acces

Dezactivarea codului este permisă	Determină dacă utilizatorul este obligat să seteze un cod PIN. Simpla setare a acestei valori (și nu a altor valori) obligă utilizatorul să introducă un cod de acces, fără a impune o lungime sau o calitate.
Permiteți o valoare simplă	Permiteți utilizatorului să utilizeze aceleași șiruri de numere, crescătoare și reducătoare (ex. 1234, 1111)
Necesită valoare alfanumerică	Parolele trebuie să conțină cel puțin o literă
Lungimea minimă a codului de acces	Lungimea minimă a parolei
Numărul minim de caractere complexe	Numărul minim de simboluri alfanumerice din parolă
Vârsta maximă a codului de acces	Numărul de zile, după care parola trebuie schimbată
Blocare automată maximă	Timpul maxim după care dispozitivul este blocat
Perioada maximă de grație pentru blocarea dispozitivului	Perioada de timp în care dispozitivul poate fi blocat fără solicitarea codului de acces la deblocare
Vârsta maximă a codului de acces (1-730 de zile sau niciuna)	Zile după care codul de acces trebuie schimbat
Istoricul codurilor de acces (1-50 de coduri de acces sau niciunul)	Numărul de coduri de acces unice înainte de reutilizare

Certificat

PKCS#1	
Descriere	Introduceți o descriere pentru certificat
Acreditare	Încărcați un fișier pkcs1

PKCS#12	
Descriere	Introduceți o descriere pentru certificat
Acreditare	Încărcați un fișier pkcs12

Setări de restricționare

Funcționalitatea dispozitivului

Permiteți camera	Permiteți utilizarea camerei
Permiteți Game Center	Când este fals, Game Center este dezactivat și pictograma acestuia este eliminată din ecranul de pornire.
Permite jocuri multiplayer	Când este fals, interzice jocurile multiplayer.
Permite adăugarea de prieteni Game Center	Când este fals, interzice adăugarea prietenilor în Game Center.
Permiteți Biblioteca foto iCloud	Dacă este setat la false, dezactivează Biblioteca foto iCloud. Fotografiile care nu au fost descărcate complet din Biblioteca foto iCloud pe dispozitiv vor fi eliminate din spațiul de stocare local.
Permiteți Touch ID	Dacă este fals, împiedică Touch ID să deblocheze un dispozitiv.

iCloud

Blocați anumite funcționalități în timpul împerecherii iCloud

Permiteți sincronizarea documentelor	Permiteți sincronizarea documentelor
Permiteți sincronizarea cu iCloud Keychain	Permiteți sincronizarea cu iCloud Keychain
Permiteți notele iCloud	Atunci când este fals, nu permite serviciile MacOS iCloud Notes
Permiteți iCloud BTMM	Când este fals, nu permite serviciul MacOS Back to My Mac iCloud.
Permiteți iCloud FMM	Dacă este fals, nu permite serviciul iCloud Găsirea Macului meu din MacOS.
Permiteți marcajele iCloud	Când este fals, nu permite sincronizarea cu MacOS iCloud Bookmark.
Permiteți iCloud Mail	Dacă este fals, nu permite accesul la serviciile MacOS Mail iCloud.
Permiteți Calendarul iCloud	Dacă este fals, nu permite serviciile MacOS Cloud iCloud.

Permiteți memento-urile iCloud	În cazul în care este fals, dezactivează serviciile iCloud Reminder.
Permiteți Addressbook iCloud	Dacă este fals, nu permite serviciile Agendă iCloud MacOS.

Management media

Ejectare la deconectare	Ejectați toate suporturile amovibile la deconectare
Permite rețea	Permiteți accesul mediilor de rețea
Permiteți disc intern	Permite accesul pentru discul intern.
Necesită autentificare	Necesită autentificare pentru utilizarea acestui mediu
Numai citire	Utilizatorul poate doar să citească date de pe suport
Permiteți disc extern	Permiteți accesul pentru discul extern.
Necesită autentificare	Necesită autentificare pentru utilizarea acestui mediu
Numai citire	Utilizatorul poate doar să citească date de pe suport
Permiteți utilizarea imaginilor de disc	Permiteți accesul pentru imagini.
Necesită autentificare	Necesită autentificare pentru utilizarea acestui mediu
Numai citire	Utilizatorul poate doar să citească date de pe suport
Permiteți utilizarea DVD-RAM-urilor	Permiteți accesul pentru discul DVD-RAM.
Necesită autentificare	Necesită autentificare pentru utilizarea acestui mediu
Numai citire	Utilizatorul poate doar să citească date de pe suport
Permiteți utilizarea DVD-urilor	Permiteți accesul pentru discul DVD.
Necesită autentificare	Necesită autentificare pentru utilizarea acestui mediu
Permiteți utilizarea de CD-uri	Permite accesul pentru discul CD.
Necesită autentificare	Necesită autentificare pentru utilizarea acestui mediu

Gestionarea conexiunilor

Wi-Fi

Aici puteți adăuga și configura conexiuni Wi-Fi

Identificatorul setului de servicii (SSID)	SSID al rețelei la care va fi stabilită conexiunea
Auto Join	Activați aderarea automată pentru rețea
Rețea ascunsă	Activare, în cazul în care AP nu transmite SSID
Configurare proxy	Configurarea unui proxy pentru fiecare punct de acces
Niciuna	Nu utilizați un server proxy
Manual	Stabilirea unui proxy manual
URL server proxy	Adresa pentru accesarea setărilor proxy
Port	Stabiliți portul pentru Proxy
Autentificare	Numele de utilizator pentru autentificarea pe Proxy
Parolă	Parolă pentru autentificarea pe Proxy
Automată	Stabiliți automat un proxy
URL server proxy	URL pentru fișierul de setări proxy
Tip de securitate	Stabilirea tipului de securitate pentru AP
WEP	
Parolă	Parolă pentru AP
WPA/WPA2	
Parolă	Parolă pentru AP
WEP Enterprise - WPA / WPA2 Enterprise / Orice întreprindere	A se vedea tabelul Error: Sursa de referință nu a fost găsită mai jos
Niciuna	Nu stabiliți nicio securitate
Dezactivați randomizarea adresei MAC	Dezactivează randomizarea adresei MAC pentru rețeaua Wi-Fi respectivă în timpul asocierii cu rețeaua. Acest lucru afișează, de asemenea, un avertisment de confidențialitate în Setări care indică faptul că rețeaua are protecții reduse de confidențialitate.

Configurarea Wi-Fi pentru întreprinderi

Notă: Disponibil numai atunci când "Tipul de securitate" este setat la un tip de întreprindere.

Protocoale	Protocol de autentificare acceptat în rețeaua țintă
TLS	Activare / Dezactivare Utilizare
TTLS	Activare / Dezactivare Utilizare
Autentificări interne	Protocolul de autentificare care ar trebui utilizat: PAP, CHAP, MSCHAP, MSCHAPv2
LEAP	Activare / Dezactivare Utilizare
PEAP	Activare / Dezactivare Utilizare
EAP-FAST	Activare / Dezactivare Utilizare
EAP-SIM	Activare / Dezactivare Utilizare
Utilizați PAC	Utilizarea PAC (Protected Access Control)
Dispoziție PAC	Configurarea PAC Provision
Furnizați PAC în mod anonim	Furnizarea anonimă de PAC
Autentificare	
Nume utilizator	Nume utilizator de autentificare
Nu utilizați Per-conexiune Parolă	Nu utilizați parola per-conectare
Parolă	Parola de utilizat
Certificat de identitate	Încărcați/selectați certificatul de autentificare
Identitate exterioară	Identitate care poate fi văzută în exterior
Încredere	
Certificat de încredere 1	Încărcați primul certificat de încredere
Certificat de încredere 2	Încărcați al doilea certificat de încredere
Certificat de încredere 3	Încărcați al treilea certificat de încredere
Server de încredere Nume certificate	Numele certificatelor de server așteptate (într-o listă separată prin virgulă)

VPN

În funcție de tipul de conexiune selectat, pot fi vizibile câmpuri diferite.

Nume conexiune	Numele profilului VPN
Tip VPN	
VPN	Tot traficul de rețea al dispozitivului va fi direcționat printr-o conexiune VPN.
Tip de conexiune	Stabilirea tipului de conexiune VPN
IPsec (cisco)	Protocolul IPsec de cisco
L2TP	Protocolul L2TP
SSL personalizat	Conexiune prin SSL personalizat
IKEv2	Protocolul IKEv2
Configurare proxy	Configurarea unui proxy pentru conexiunea VPN
Niciuna	Nu stabiliți niciun Proxy
Manual	Stabilirea manuală a unui Proxy
URL server proxy	Adresa pentru accesul la setările proxy
Port	Stabiliți portul pentru Proxy
Autentificare	Nume de utilizator pentru autentificarea la Proxy
Parolă	Parolă pentru autentificarea la Proxy
Automată	Stabiliți automat un proxy
URL server proxy	URL pentru accesul la setările Proxy

Proxy HTTP

Tip Proxy	
Manual	Stabiliți manual un Proxy
URL server proxy	Adresa pentru accesul la setările proxy
Port	Stabilirea portului Proxy
Autentificare	Nume de utilizator pentru autentificarea la Proxy
Parolă	Parolă pentru autentificarea la Proxy
Automată	Stabiliți automat un proxy
URL proxy PAC	URL proxy PAC
Permiteți conexiunea directă dacă PAC este inaccesibil	Permiteți conexiunea directă (fără VPN), dacă PAC este inaccesibil
Permite ocolirea proxy-ului pentru a accesa rețele captive	Permiteți ocolirea proxy-ului pentru a accesa rețele interne captive

AirPrint

Adresa IP	Adresa IP a imprimantei
Calea resurselor	Cale definită către dispozitivul AirPrint

AirPlay

Numele dispozitivului	Numele dispozitivului
Parolă	Parolă de împerechere
Lista albă	Definiți o listă de dispozitive, cu care dispozitivul se poate împerechea exclusiv

Gestionarea PIM

Exchange Active Sync

Numele contului	Denumirea contului.
Adresa eMail	Adresa contului (de exemplu, max@company.com)
Nume gazdă server	Nume de gazdă intern
Nume de utilizator	"Domain" și "Login Name" trebuie să fie goale pentru ca dispozitivul să solicite numele utilizatorului.
Domeniu	"Domain" și "Login Name" trebuie să fie goale pentru ca dispozitivul să solicite numele utilizatorului. Dacă este activată o configurare ACL Gateway și câmpul Domain nu este gol, AppTec360 Universal Gateway va autentifica dispozitivul cu următorul nume "Domain\Login Name"
Parolă	Parola pentru cont (de exemplu, secretUserPassword)
Zilele trecute ale Mail to Sync	Numărul de e-mailuri din ultimele zile de sincronizat
Utilizați SSL	Utilizați SSL pentru gazda Exchange internă
Opțiune avansată	Afișare opțiuni avansate
Port server	Port intern
Calea serverului	Cale internă
Nume de gazdă extern	Gazdă externă
Port extern	Port extern
Cale externă	Cale externă
Utilizați SSL pentru extern Gazdă de schimb	Utilizați SSL pentru gazda Exchange externă

eMail

Configurarea conturilor POP3 / IMAP pe dispozitivul utilizatorului final

Descrierea contului	Nume des Conturi de e-mail
Tip de cont	
IMAP	
Prefixul căii	Prefixul căii pentru folderele speciale
POP	
Nume afișare utilizator	Numele de afișare al utilizatorului
Adresa de e-mail	Adresa de e-mail a utilizatorului

Poșta de intrare	Setări server de intrare
Adresa serverului de poștă electronică	Adresa serverului de poștă electronică
Portul serverului de e-mail	Portul serverului de poștă electronică
Nume utilizator	Numele utilizatorului respectiv
Tip de autentificare	Tip de autentificare
Niciuna	Niciun tip de autentificare
Parolă (numai la nivel de dispozitiv)	Solicitare parolă
MDM provocare-răspuns	
NTLM	Autentificare NTLM
HTTP MD5 Digest	
Utilizați SSL	Utilizați SSL, dacă este necesar

Poșta de ieșire	Setări server de ieșire
Adresa serverului de poștă electronică	Adresa serverului de poștă electronică
Portul serverului de e-mail	Portul serverului de e-mail
Nume utilizator	Numele utilizatorului respectiv
Tip de autentificare	
Niciuna	Nicio metodă de autentificare
Parolă (numai la nivel de dispozitiv)	Solicitare parolă
MDM provocare-răspuns	
NTLM	Autentificare NTLM
HTTP MD5 Digest	
Utilizați SSL	Utilizați SSL, dacă este necesar
Parola de ieșire este aceeași cu cea de intrare	Parola de ieșire este aceeași cu cea de intrare
Utilizați numai în poștă	Activați, dacă toate e-mailurile de ieșire vor fi trimise prin intermediul aplicației Mail-App

CalDav

Configurați înființarea și distribuirea unui cont CalDav

Descrierea contului	Numele de afișare al contului
Nume gazdă	Nume gazdă și/sau adresă IP
Port	Port al contului CalDav
URL principal	URL-ul principal al contului
Nume utilizator	Numele de utilizator CalDav respectiv
Parolă (numai la nivel de dispozitiv)	Respectiva parolă CalDav
Utilizați SSL	Utilizați SSL, dacă este necesar

CardDav

Configurați înființarea și distribuirea unui cont CardDav

Descrierea contului	Numele de afișare al contului
Nume gazdă	Nume gazdă și/sau adresă IP
Port	Portul contului CardDav
URL principal	URL-ul principal al contului
Nume utilizator	Numele de utilizator CardDav respectiv
Parolă (numai la nivel de dispozitiv)	Parolă CardDav corespunzătoare
Utilizați SSL	Utilizați SSL, dacă este necesar

LDAP

În această zonă, configurați o conexiune LDAP, pentru a permite un schimb dinamic de certificate între dispozitivul utilizatorului final și Active Directory.

Vă rugăm să rețineți că utilizatorul selectat are nevoie de permisiunea respectivă de citire.

Descrierea contului	Descrierea contului
Nume utilizator cont	Utilizator pentru acces LDAP
Parolă cont	Parolă pentru accesul LDAP
Nume gazdă cont	Nume gazdă/adresa IP a serverului LDAP
Utilizați SSL	Utilizați SSL, dacă este necesar

În a doua parte, puteți defini filtre individuale pentru căutarea în registrul LDAP.

Descriere	Domeniul de aplicare	Baza de căutare
Descrierea filtrului	Nivelul de căutare în registrul LDAP	Definirea filtrului individual

Tablou de bord și raportare

Setări tablou de bord

Aici puteți vedea ce tablouri de bord există, le puteți edita sau crea unele noi. Fiecare tablou de bord are propriul set de date de afișat și propria configurație grafică.

Control setări tablou de bord

Public	Setează tabloul de bord public, astfel încât alți utilizatori să poată vedea tabloul de bord. Bineînțeles, utilizatorii trebuie să se poată conecta și să vadă tablourile de bord. Dacă "Public" nu este activat, numai creatorul îl poate vedea.
Implicit	Setează tabloul de bord ca fiind implicit, astfel încât acesta să se deschidă automat data viitoare când accesați vizualizarea Tablou de bord.
	Afișați tabloul de bord și graficele sale
	Ștergeți tabloul de bord
	Modificați numele și setările tabloului de bord
	Faceți o copie a tabloului de bord
	Adăugați un tablou de bord complet nou

Vizualizare tablou de bord

Aceasta afișează datele și graficele tabloului de bord selectat și vă permite, de asemenea, să le modificați.

Control tablou de bord

	Vă permite să definiți ce date sunt afișate în tabloul de bord, cantitatea de date care urmează să fie afișate și dimensiunea în care urmează să fie afișate aceste date
	Vă aduce înapoi la Tabloul de bord Prezentare generală
	Resetează tabloul de bord deschis în prezent la setările implicite
	Salvează toate modificările pe care le-ați făcut în tabloul de bord deschis în prezent (de exemplu, ce date să afișați)
	Schimbarea tipului de grafic în grafic de piloni
	Schimbați tipul graficului la graficul plăcintă
	Schimbați tipul graficului la graficul gogoașă
	Schimbarea tipului de diagramă în diagramă a zonei polare
	Modificarea ordinii de sortare

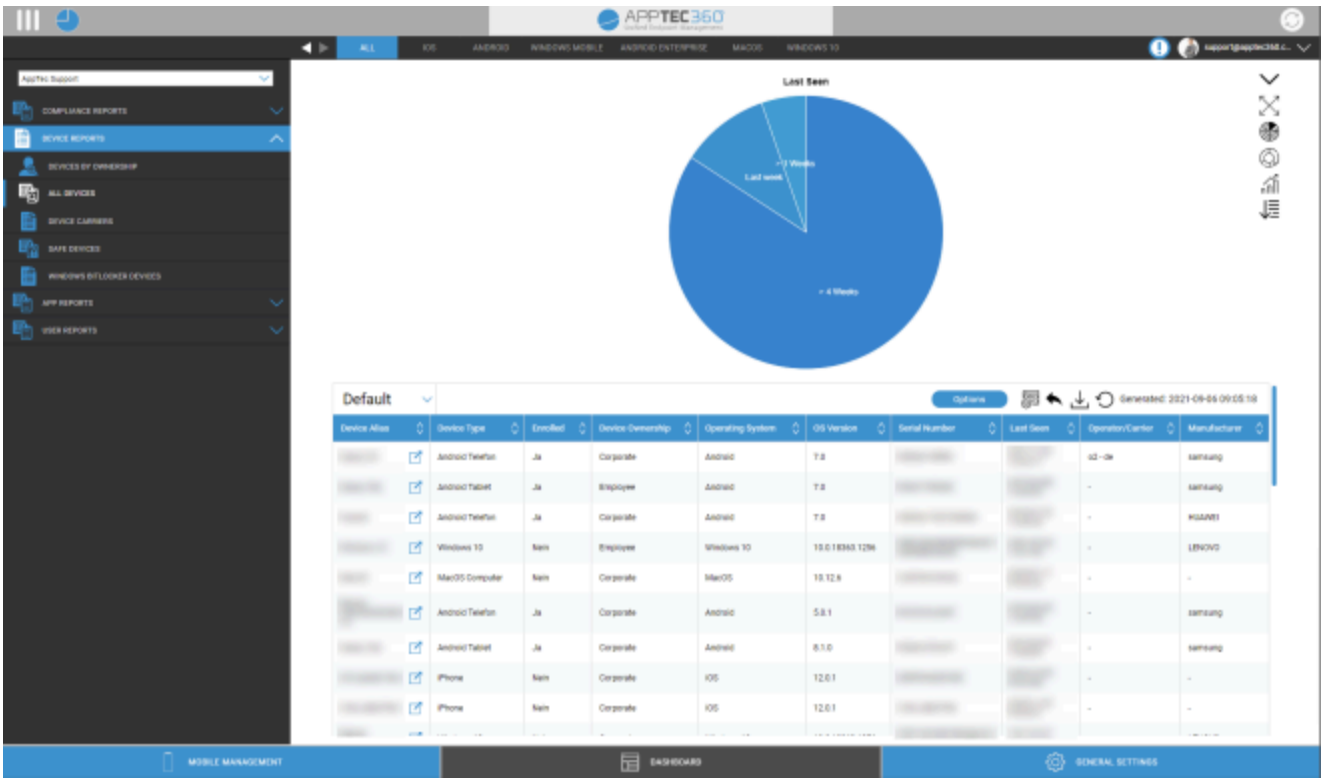
Raportare extinsă

"Raportare extinsă" oferă imagini de ansamblu și grafice detaliate cu privire la informațiile despre dispozitive și utilizatori.

Există câteva rapoarte implicite, dar toate pot fi modificate manual pentru a adăuga sau a elimina date de afișat.

Vă rugăm să rețineți că puteți modifica doar manual datele care sunt afișate. Categoria de raport selectată definește datele pe care se bazează aceasta. De exemplu, nu veți putea vedea niciodată dispozitive Android în raportul iOS în Rapoarte dispozitive Toate dispozitivele iOS

În stânga sus, puteți limita datele raportului la un anumit grup (și la toate subgrupurile acestuia). În mod implicit, acesta este setat la nodul rădăcină, astfel încât se iau în considerare TOATE dispozitivele și utilizatorii.



Control extins al raportării

În fiecare prezentare generală puteți utiliza următoarele funcții pentru a modifica raportul în orice mod doriți:

	Ascundeți graficul (dacă graficul este afișat)
	Afișați graficul (dacă graficul este ascuns)
	Extindeți graficul (dacă graficul este colapsat)
	Închideți graficul (dacă graficul este extins)
	Schimbarea tipului de grafic în grafic de piloni
	Schimbați tipul graficului la graficul plăcintă
	Schimbați tipul graficului la graficul gogoașă
	Schimbarea tipului de diagramă în diagramă a zonei polare
	Modificarea ordinii de sortare
	Modificați următoarele părți ale imaginii de ansamblu afișate: • Adăugare/eliminare coloane • Specificați ordinea în care sunt afișate coloanele • Afișați/ascundeți graficul de deasupra tabelului • Selectați coloana care este utilizată pentru grafic • Filtrați datele din tabelul dvs.
	Deschideți managerul de configurare pentru a salva și încărca diferite rapoarte
	Resetează raportul deschis în prezent la valoarea implicită
	Exportați raportul curent ca fișier .csv
	Regenerarea datelor și reîncărcarea raportului curent

Puteți găsi o listă a tuturor rapoartelor implicite pe paginile următoare.

Rapoarte de conformitate

Dispozitive înrădăcinate

Prezentare generală a dispozitivelor care au fost rootate/ jailbroken.

Coloanele implicite ale acestui raport:

Alias dispozitiv
Proprietarul dispozitivului
E-mail
Sistem de operare
Număr de telefon
Văzut ultima dată
Producător

Dispozitive Roaming

Prezentare generală a tuturor dispozitivelor care sunt în roaming

Coloanele implicite ale acestui raport:

Alias dispozitiv
Proprietarul dispozitivului
E-mail
Tip dispozitiv
Sistem de operare
Număr de telefon
Văzut ultima dată

Dispozitive cu roaming activat

Prezentare generală a tuturor dispozitivelor care au activat roamingul, dar care nu sunt neapărat în roaming în prezent.

Coloanele implicite ale acestui raport:

Alias dispozitiv
Proprietarul dispozitivului
E-mail
Tip dispozitiv
Sistem de operare
Număr de telefon
Văzut ultima dată

Dispozitive supravegheate

Prezentare generală a tuturor dispozitivelor care sunt supravegheate în modul supravegheat (numai iOS)

Coloanele implicite ale acestui raport:

Alias dispozitiv
Proprietarul dispozitivului
E-mail
Tip dispozitiv
Văzut ultima dată

Dispozitive inactive

Prezentare generală a tuturor dispozitivelor care nu s-au conectat la server în ultimele 7 zile

Coloanele implicite ale acestui raport:

Alias dispozitiv
Proprietarul dispozitivului
E-mail
Tip dispozitiv
Sistem de operare
Văzut ultima dată

Rapoarte dispozitiv

Dispozitive în funcție de proprietar

Aici puteți vedea câte dispozitive au fost implementate în prezent ca dispozitive corporate (dispozitive corporative) și dispozitive ale angajaților (dispozitive private).

Coloanele implicite ale acestui raport:

Alias dispozitiv
Proprietarul dispozitivului
Tip dispozitiv
Proprietatea dispozitivului
Sistem de operare

Toate dispozitivele

Aici puteți vedea o prezentare generală a tuturor dispozitivelor cu cele mai importante informații.

Coloanele implicite ale acestui raport:

Alias dispozitiv
Tip dispozitiv
Înscris
Proprietatea dispozitivului
Sistem de operare
Versiunea sistemului de operare
Numărul de serie
Văzut ultima dată
Operator/Carrier
Producător

Purtători de dispozitive

Aici puteți vedea o prezentare generală privind operatorul (furnizorul de telefonie mobilă).

Coloanele implicite ale acestui raport:

Alias dispozitiv
Proprietarul dispozitivului
E-mail
Sistem de operare
Versiunea sistemului de operare
Operator/Carrier

Dispozitive SAFE

Aici puteți vedea o prezentare generală a dispozitivelor care utilizează versiunea SAFE.

Deoarece prezentarea generală și/sau SAFE este disponibilă numai pentru dispozitivele Samsung, nu veți vedea filele obișnuite sub acest punct.

Coloanele implicite ale acestui raport:

Alias dispozitiv
Proprietarul dispozitivului
E-mail
Tip dispozitiv
Văzut ultima dată
Versiunea SAFE

Dispozitive Windows BitLocker

Aici puteți vedea o prezentare generală a dispozitivelor Windows care utilizează BitLocker.

Coloanele implicite ale acestui raport:

Alias dispozitiv
Proprietarul dispozitivului
E-mail

Starea BitLocker

Rapoarte aplicații

Aici veți obține o varietate de imagini de ansamblu în ceea ce privește aplicațiile. În toate aceste rapoarte puteți face clic pe o intrare pentru a vedea în continuare ce versiuni sunt instalate pe dispozitive și cât de des. În această vizualizare, puteți face clic din nou pe o versiune specifică pentru a vedea ce dispozitive au instalată această versiune specifică.

Notă: Poate dura ceva timp până când sistemul primește informații actualizate de la dispozitiv. În plus, rapoartele nu sunt actualizate în fiecare minut. Este posibil să trebuiască să aveți răbdare pentru a vedea starea actuală dacă tocmai ați atribuit o nouă aplicație sau versiune. Reîncărcarea manuală a raportului va forța raportul să afișeze cele mai recente date disponibile

Aplicații instalate

Aici veți obține o prezentare generală a tuturor aplicațiilor instalate.

Coloanele implicite ale acestui raport:

Nume și prenume	Numele aplicației și/sau serviciului respectiv
Identificator	ID aplicație/serviciu definit
Număr total	Cât de des a fost instalată această aplicație/serviciu pe dispozitivele utilizatorului final

Cele mai instalate aplicații

Aici veți obține o prezentare generală a aplicațiilor care au fost instalate cel mai mult.

Coloanele implicite ale acestui raport:

Nume și prenume	Numele aplicației și/sau serviciului respectiv
Identificator	ID aplicație/serviciu definit
Număr total	Cât de des a fost instalată această aplicație/serviciu pe dispozitivele utilizatorului final

Aplicații obligatorii

Aici veți obține o prezentare generală a aplicațiilor obligatorii (obligatorii prin mandat).

Coloanele implicite ale acestui raport:

Nume și prenume	Numele aplicației și/sau serviciului respectiv
Identificator	ID aplicație/serviciu definit
Sursa aplicației	Care AppStore este implicat: • Google PlayStore (Android) • iTunes AppStore (iOS)
SO	Sistem de operare

Aplicații pe lista neagră

Aici veți obține o prezentare generală a tuturor aplicațiilor definite pe lista neagră.

Coloanele implicite ale acestui raport:

Nume și prenume	Numele aplicației și/sau serviciului respectiv
Identificator	ID aplicație/serviciu definit
Sursa aplicației	Care AppStore este implicat: • Google PlayStore (Android) • iTunes AppStore (iOS)
SO	Sistem de operare

Rapoarte ale utilizatorilor

Tariful

Aici veți obține o prezentare generală a tarifelor de telefonie și a cartelelor SIM ale utilizatorilor.

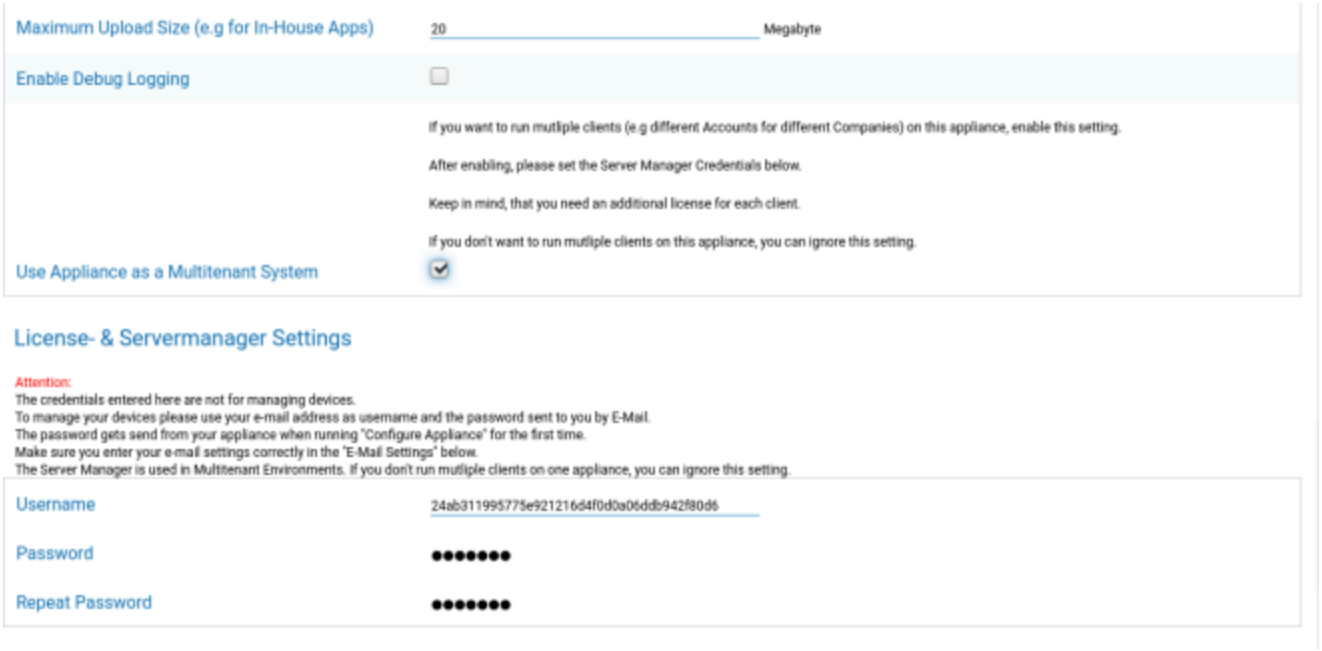
Coloanele implicite ale acestui raport:

E-mail
Nume și prenume
Numărul de telefon
transportator
tarif
opțiune
preț
contractCancelat
contractStart
în timpulTime
mobileAndData
dateVolum
multiSIM
tip
simCardSerial1
simCardSerial2
simCardSerial3
pin1
pin2
puk1
puk2
notă

Managementul multitenant

AppTec360 EMM este capabil să găzduiască mai mulți chiriași separați, fiecare cu proprii utilizatori și grupuri, permisiuni și setări globale.

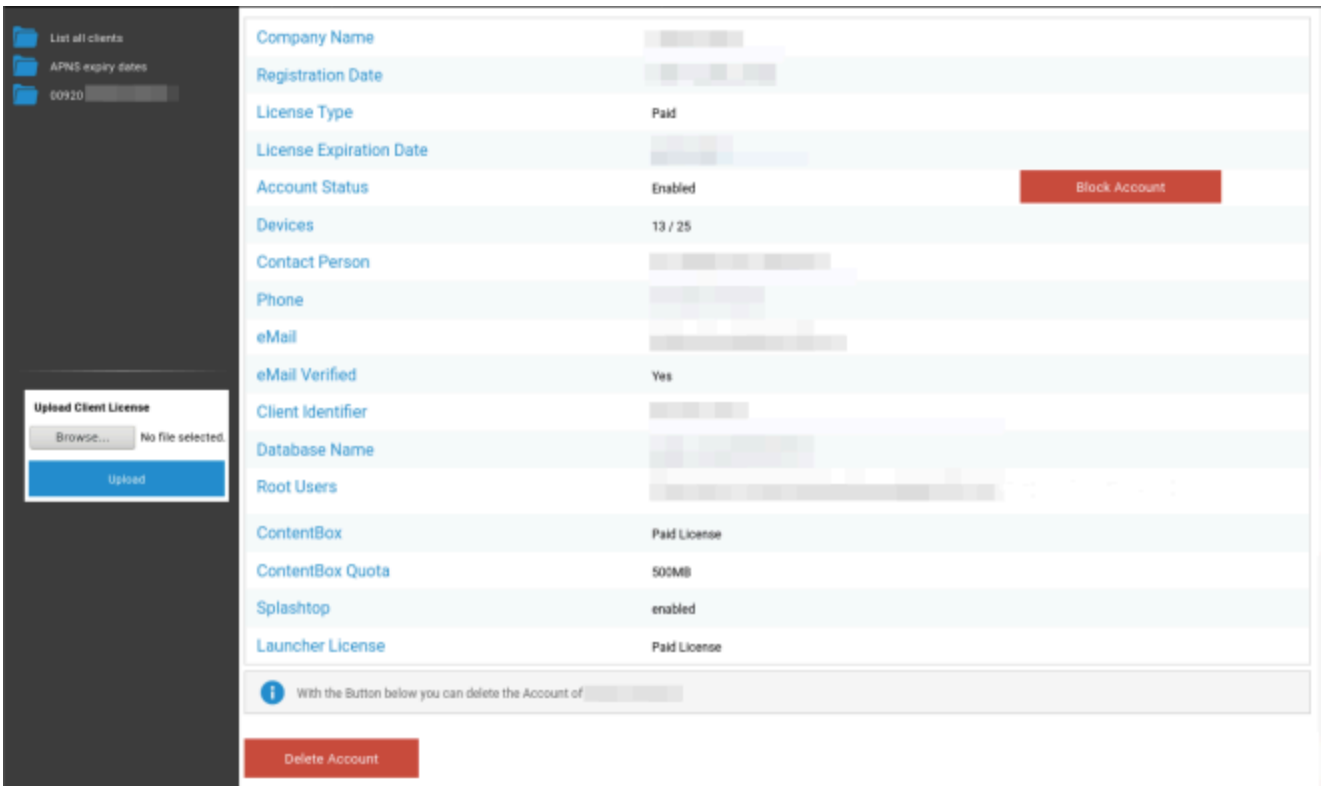
Pentru a activa capabilitățile Multitenant, trebuie să le activați în interfața de configurare a dispozitivului în "Pasul trei - Setări server".



În noul meniu, setați un nume de utilizator și o parolă pentru Servermanager. Salvați setările și rulați "Configure Appliance" în "Pasul cinci - Acordul de licență" pentru a aplica setările.

Când configurația este finalizată, vă puteți conecta cu datele de identificare stabilite prin interfața normală de gestionare a telefoanelor mobile.

După autentificare, puteți vedea următoarea vizualizare.



În stânga puteți vedea toți chiriașii (în acest caz doar unul cu ID 920), iar în dreapta informațiile despre acest client. De asemenea, aveți opțiunea de a bloca accesul la cont, precum și de a șterge clientul (ATENȚIE: acest lucru va elimina toate datele referitoare la clientul respectiv).

În partea stângă puteți încărca o nouă licență de client, care poate fi fie o actualizare de licență pentru un client existent, fie o licență nouă care creează automat un client nou. Atunci când se creează un client nou, un e-mail care conține parola de conectare este trimis automat la adresa de e-mail pentru care a fost emisă licența.

Pentru a obține o licență client nouă sau actualizată (de exemplu, în cazul în care aveți nevoie de mai multe licențe pentru dispozitive), contactați reprezentantul dvs. de vânzări.

Vederi suplimentare

Lista tuturor clienților

Afișează o prezentare generală a tuturor clienților din sistem.

ID client	ID client
Identificator	Identificator client
Baza de date	Baza de date
Numele companiei	Numele companiei
eMail	Persoana de contact eMail
Verificat	Dacă eMail-ul persoanei de contact este verificat sau nu
Țara	Țara
Dispozitive	Numărul de dispozitive înregistrate
Data înregistrării	Momentul atribuirii licenței
Ultima autentificare	Ultima autentificare în contul de administrator
Licență	Afișarea tipului de licență (Free|Paid)
Licență CB	Tipul de licență ContentBox (Free|Paid)
Statut	Starea actuală a AppTec-Client
Expirat	Afișează, dacă licența a expirat
iOS	Numărul de dispozitive iOS
Android	Numărul de dispozitive Android
Windows Mobile	Numărul de dispozitive Windows Mobile
MacOS	Numărul de dispozitive MacOS
Windows 10	Numărul de dispozitive Windows 10
Android Enterprise	Numărul de dispozitive Android pentru întreprinderi
IOS BYOD (Înscrierea utilizatorului)	Numărul de dispozitive IOS BYOD (înscrierea utilizatorilor)
IoT	Numărul de dispozitive IoT

Datele de expirare APNS

Afișează o prezentare generală a tuturor datelor de expirare a certificatelor APNS ale tuturor clienților.

ID client	ID client
Numele companiei	Numele companiei
Data expirării	Data expirării certificatului Apple APNS
Info	Informații privind expirarea

Persoană de contact

Întrebări suplimentare? Pur și simplu contactați-ne sub:

Pentru întrebări tehnice generale

support@apptec360.com

+41 61 511 3210

Pentru întrebări legate de instalarea unui dispozitiv virtual

consulting@apptec360.com

+41 61 511 3214

Disclaimer