AppTec360 Enterprise Mobile Manager & ContentBox

Príručka pre správu | Verzia 5.0 (202110)

Obsah

- Zariadenie na vypnutie
- Reštartovanie zariadenia
- Alarm a stratový režim | Zakázať stratový režim
- Odstrániť zariadenie
- Zariadenie na utieranie
- Vyčistenie podniku | Odstrániť MDM
- Odoslať správu
- Vzdialené ovládanie TeamViewer
- Odoslať žiadosť o zápis

Android

- Upraviť zariadenie
- Vymazanie prístupového kódu
- Zariadenie na uzamknutie
- Odstrániť zariadenie
- Zariadenie na utieranie
- Odstránenie MDM
- Odoslať správu
- Transformácia do režimu COPE
- Odoslať žiadosť o zápis
- Migrácia staršieho zariadenia

Windows

- Upraviť zariadenie
- Odstrániť zariadenie
- Vyčistenie podniku | Odstrániť MDM
- Vzdialené ovládanie TeamViewer
- Odoslať žiadosť o zápis

Správa obsahu

- Skupinové súbory
- Prieskumník súborov
- Audítorská stopa
- Odpadky
- Externé úložisko

Protokol o audite

Konfigurácia systému iOS

- Zabezpečenie SecurePIM
- Prehliadač SecurePIM
- Výmena

Správa pripojenia

- Wi-Fi
  - Nastavenie servera proxy
  - Typ zabezpečenia
- VPN
  - Typ VPN
    - VPN
    - Sieť VPN pre jednotlivé aplikácie
  - Nastavenie servera proxy
- APN
- Cellular
- Proxy server HTTP
- AirPrint
- AirPlay

Správa PIM

- Exchange Active Sync
- E-mail
  - Prichádzajúca pošta
  - Odchádzajúca pošta
- CalDav
- Odhlásené kalendáre
- LDAP

Správa webu

- Webové klipy
- Filter webového obsahu

Správa aplikácií

- Správca podnikových aplikácií
  - Nainštalované aplikácie (len na úrovni zariadenia)
  - Povinné aplikácie
    - Možnosti inštalácie
  - Webové aplikácie

- Obmedzenie a nastavenia
  - Aplikácie na čiernej / bielej listine
  - Obmedzenia aplikácie SysApp
  - App-VPN
  - Nastavenia aplikácie
- Obchod s podnikovými aplikáciami
  - Aplikácie iTunes
  - Vnútorná stránka
- Režim kiosku
  - Typ aplikácie
    - Balík
    - ADRESA URL
  - Nastavenia režimu kiosku

Android Enterprise – Plne spravovaná konfigurácia zariadenia

Všeobecné

- Prehľad profilu skupiny (len na úrovni skupiny)
- Prehľad zariadení (len na úrovni zariadenia)
- Revízia konfigurácie (len na úrovni zariadenia)
- Protokol zariadenia (len na úrovni zariadenia)
  - Denník príkazov
  - Možné stavy príkazov
- Nastavenia zariadenia
  - Konfigurácia klienta
  - Tapety

Správa aktív (len na úrovni zariadenia)

- Informácie o zariadení
  - Wi-Fi
- Cellular
- Bluetooth

Riadenie bezpečnosti

- Ochrana proti krádeži (len na úrovni zariadenia)
  - Informácie GPS (len na úrovni zariadenia)
  - Vyčistiť a uzamknúť (len na úrovni zariadenia)
  - Správa (len na úrovni zariadenia)

- Tapety

Správa aktív (len na úrovni zariadenia)

- Informácie o zariadení
  - Wi-Fi
- Cellular
- Bluetooth

Riadenie bezpečnosti

- Ochrana proti krádeži (len na úrovni zariadenia)
  - Informácie GPS (len na úrovni zariadenia)
  - Vyčistiť a uzamknúť (len na úrovni zariadenia)
  - Správa (len na úrovni zariadenia)
- Konfigurácia zabezpečenia
  - Prístupový kód zariadenia
  - Prístupový kód kontajnera
  - AntiVirus
- Koniec životnosti (len na úrovni zariadenia)
  - Vyčistiť (len na úrovni zariadenia)
- Nastavenia obmedzenia
  - Obmedzenia
- Správa certifikátov

Správa pripojenia

- Wifi
  - Typ zabezpečenia
    - WEP
    - WPA/WPA2
    - 802.1x EAP
- VPN
  - Typ VPN
    - VPN
    - Sieť VPN pre jednotlivé aplikácie
- Obmedzenia

Správa PIM

- Výmena Gmail

Správa aplikácií

- Správca podnikových aplikácií

- Správa (len na úrovni zariadenia)
- Konfigurácia zabezpečenia
  - Prístupový kód
  - Šifrovanie
  - AntiVirus
- Koniec životnosti (len na úrovni zariadenia)
  - Vyčistiť (len na úrovni zariadenia)
- Nastavenia obmedzenia
  - Obmedzenia
  - Vlastník zariadenia AE

Kontajner BYOD

- Android Enterprise
  - Android Enterprise
  - Výmena Gmail
  - Aplikácie systému AE
  - Prístupový kód kontajnera
- Samsung KNOX
  - Aktivácia
  - Prístupový kód Knox
  - Knox Security
  - Výmenník Knox Exchange
  - Knox eMail
  - Aplikácie Knox

Správa pripojenia

- Wifi
  - Typ zabezpečenia
    - WEP
    - WPA/WPA2
    - 802.1x EAP
- VPN
- Obmedzenia
- APN
- Bluetooth

Správa PIM

- Výmena

- Wi-Fi
  - Konfigurácia podnikovej siete Wi-Fi
- VPN
- Proxy server HTTP
- AirPrint
- AirPlay

Správa PIM

- Exchange Active Sync
- E-mail
- CalDav
- CardDav
- LDAP

Prístrojový panel a podávanie správ

Nastavenia prístrojovej dosky

Zobrazenie prístrojovej dosky

Rozšírené podávanie správ

- Správy o dodržiavaní predpisov
  - Zakorenené zariadenia
  - Roamingové zariadenia
  - Zariadenia s povoleným roamingom
  - Zariadenia pod dohľadom
  - Neaktívne zariadenia
- Správy o zariadení
  - Zariadenia podľa vlastníctva
  - Všetky zariadenia
  - Nosiče zariadení
  - Zariadenia SAFE
  - Zariadenia so systémom Windows BitLocker
- Správy o aplikáciách
  - Nainštalované aplikácie
  - Najviac nainštalovaných aplikácií
  - Povinné aplikácie
  - Aplikácie na čiernej listine
- Správy používateľov

Všeobecný prehľad

Úvod do AppTec360

Riešenie AppTec Enterprise-Mobile-Management-Solution ponúka možnosť spravovať a konfigurovať všetky mobilné zariadenia pomocou intuitívnej konzoly na správu. V tomto scenári môže byť server EMM spustený buď vo vašom vlastnom prostredí, alebo môžete využiť naše cloudové riešenie.

Aj pokiaľ ide o centrálnu inštaláciu podnikových aplikácií do smartfónov, ste na správnom mieste. Pomocou nástroja Enterprise Mobile Manager môžete v priebehu niekoľkých sekúnd distribuovať podnikové aplikácie a dokumenty do zariadení alebo blokovať nežiaduce aplikácie pomocou bielej/ čiernej listiny.

Používanie súkromných zariadení vo firmách predstavuje novú výzvu pre zabezpečenie smartfónov a tabletov. Vzhľadom na to, že zamestnanci chcú čoraz viac používať svoje smartfóny, musia správcovia IT chrániť veľké množstvo rôznych typov zariadení. Pomôžeme vám zabezpečiť všetky zariadenia a citlivé údaje, ktoré sú v nich uložené, a spravovať ich z intuitívnej konzoly.

Podporované operačné systémy zariadení

AppTec360 ponúka podporu pre zariadenia iOS, Android a Windows. Upozorňujeme, že kapacita funkcií uvedených platforiem sa môže v jednotlivých operačných systémoch líšiť.

- Apple iOS 11.0 alebo vyššia verzia*
- Apple macOS 10.11 alebo vyššia verzia
- Google Android 4.4 alebo vyššia verzia** v cloudovej verzii
- Systém Google Android 4.1 alebo novší** vo verzii OnPrem
- MS Windows 10 alebo novší*** (stolný počítač, notebook a tablet)

** Upozorňujeme, že zariadenia so systémom iOS 10 alebo starším nie je možné zaregistrovať z dôvodu drastických zmien, ktoré spoločnosť Apple vykonala v procese registrácie.*

***Zariadenia je možné pripojiť a nakonfigurovať, aj keď používajú verziu, ktorá už nie je podporovaná výrobcom. Upozorňujeme, že niektoré funkcie môžu vyžadovať určitú verziu systému Android. V prípadoch podpory sa riadime oficiálnou podporou výrobcu. V prípade problémov alebo chýb spôsobených zastaranou verziou, ktorá už nie je podporovaná výrobcom, si vyhradzujeme právo poskytnúť len obmedzenú podporu.*

****Domáca verzia systému Windows nie je podporovaná z dôvodu obmedzení operačného systému. Dôrazne odporúčame používať verziu operačného systému, ktorú výrobca stále podporuje. Nielen z dôvodu kompatibility, ale aj z bezpečnostných dôvodov. Preto odporúčame iOS 12 alebo novší a Android 9 alebo novší.*

Podporované adresáre LDAP

- Microsoft Active Directory
- Otvoriť LDAP

Aktuálne informácie o "Podporovaných operačných systémoch zariadení" a "Podporovaných adresároch LDAP" nájdete tu:

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

Vysvetlenie „režimu pod dohľadom“ v zariadeniach Apple

Režim pod dohľadom predstavuje rozšírené rozhranie pre zariadenia so systémom iOS.

Na príslušne nakonfigurovanom zariadení sa môžu uplatniť ďalšie obmedzenia, ktoré sa týkajú funkčnosti zariadenia koncového používateľa. Tieto sú tiež uvedené v príručke pre administratívu a sú označené bannerom.

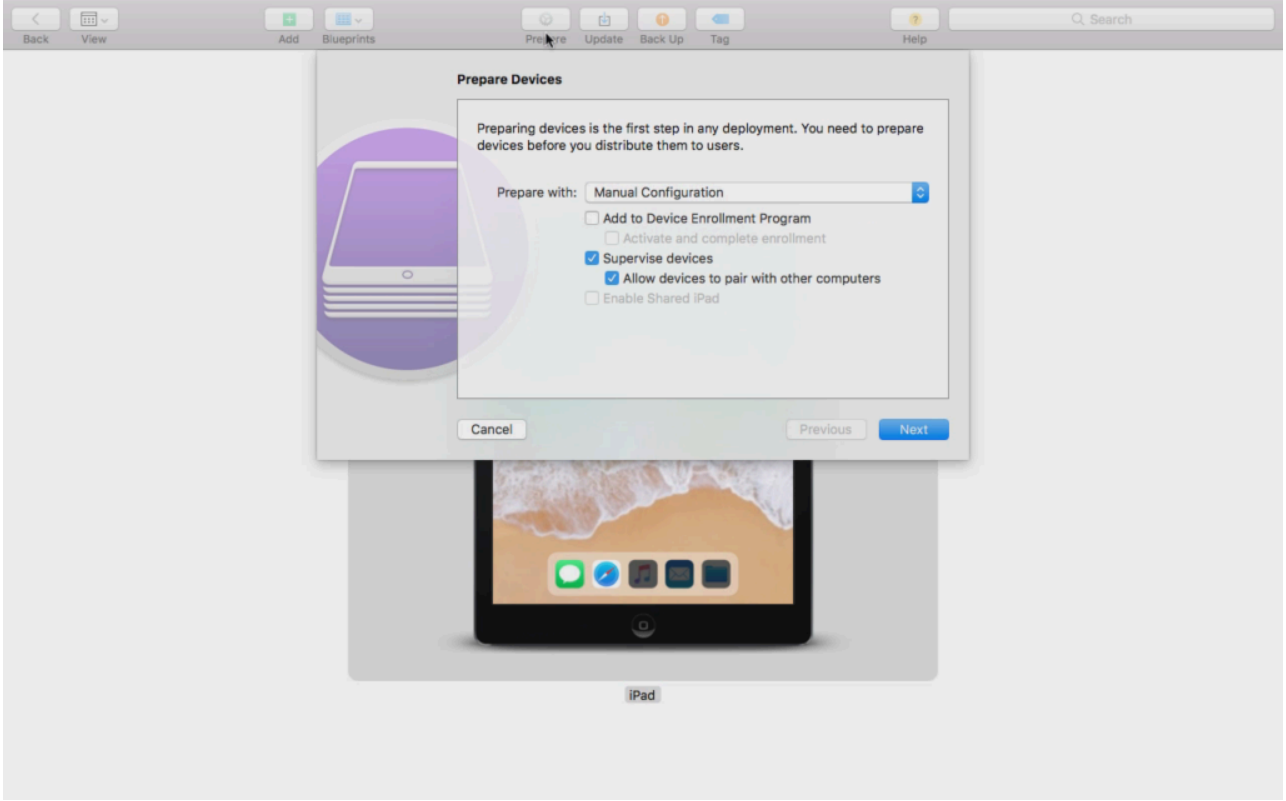
K dispozícii v režime pod dohľadom

Režim "Supervised-Mode" môžete aktivovať pomocou programu "Apple Configurator". Apple Configurator môže nastaviť predvolené nastavenia nových zariadení iOS ako konfiguračný nástroj (cez rozhranie USB).

Nástroj dokáže nainštalovať nielen konfiguračné profily, ale aj aplikácie. Je bezplatná, ale vyžaduje počítač Mac.

Aktivácia režimu pod dohľadom

1. Otvorenie aplikácie Apple Configurator



2. Kliknite na zariadenie a vyberte položku "Pripraviť".
3. Vyberte "Manuálna konfigurácia" a "Dohľad nad zariadeniami".
4. Kliknite na "Ďalej".
5. (voliteľné) Teraz môžete pridať server MDM, na ktorom bude zariadenie zaregistrované. Prepojenie na tento účel nájdete v časti "Všeobecné nastavenia - Konfigurácia iOS - Konfigurátor a URL" Vyberte si svoju organizáciu alebo vytvorte novú.
6. Vyberte si svoju organizáciu alebo vytvorte novú
7. Vyberte, ktoré kroky sa majú pri úvodnom nastavení preskočiť, a kliknite na "Next" (POZOR: Pokračovaním sa zariadenie vymaže!)

Teraz sa vaše zariadenie prepne do režimu pod dohľadom. Môže to trvať niekoľko minút. Po dokončení sa zariadenie reštartuje.

Teraz je vaše zariadenie pod dohľadom!

Pridanie zariadenia do DEP

Zariadenia môžete do DEP (Device Enrollment Programm) pridať aj pomocou konfigurátora Apple, ak sú vaše zariadenia v systéme iOS 11 alebo novšom.

Viac informácií o DEP: https: //www.apple.com/business/dep/

Postupujte rovnako ako pri dohľade nad zariadením a navyše začiarknite položku "Add to Device Enrollment Programm". Ak ste sa ešte nikdy neprihlásili do DEP pomocou programu Apple Configurator, budete požiadaní o prihlasovacie údaje do DEP.

Po dokončení procesu sa zariadenie nachádza na serveri DEP "Devices Added by Apple Configurator 2". Teraz môžete použiť tento server a pripojiť ho ku konzole na správu alebo preniesť zariadenie na už existujúci server.

Teraz ste úspešne pridali zariadenie do DEP!

Vysvetlenie systému Android Enterprise

Čo je Android Enterprise?

Android Enterprise ponúka lepšiu kontrolu nad pracovnými zariadeniami, ktoré sú spravované pomocou MDM. Správcovia tak môžu mať buď úplnú kontrolu nad zariadeniami so systémom Android, alebo oddeliť firemné údaje od súkromných údajov v kontajnerových zariadeniach. Okrem toho Android Enterprise umožňuje jednoduchšiu registráciu zariadení a jednoduchú distribúciu aplikácií.

Aké sú požiadavky na používanie systému Android Enterprise?.

Službu Android Enterprise môže bezplatne používať každý. Na aktiváciu všetkých funkcií Android Enterprise stačí pripojiť konto Google k MDM. Viac informácií o tom nájdete v časti Android Enterprise.

Android Enterprise možno používať na zariadeniach so systémom Android 5.1 alebo vyšším, s výnimkou rozšíreného pracovného profilu (pozri nižšie). Odporúčame aspoň Android 7 alebo vyšší pre jednoduchšiu registráciu alebo Android 11 pre využitie všetkých dostupných funkcií.

Aké režimy sú k dispozícii v systéme Android Enterprise?

Pri používaní systému Android Enterprise môžete používať 3 rôzne režimy.

AE Plne spravované zariadenie (Work Managed): Plne spravované zariadenie, ktoré sa používa len na prácu. To umožňuje správcovi plnú kontrolu nad zariadením. Neumožňuje to súkromné používanie zariadenia. Ak chcete zaregistrovať zariadenia v tomto režime, je potrebné zariadenia resetovať a zaregistrovať pomocou kódu QR (pozrite si časť Registrácia AE) alebo zaregistrovať prostredníctvom funkcie Knox Enrollment alebo Zero Touch.

AE BYOD Container: Kontajner BYOD (bring your own device) umožňuje používateľom prístup k firemným údajom na ich súkromnom telefóne v samostatnom kontajneri. V tomto režime súkromné aplikácie nemôžu vidieť firemné údaje a aplikácie a naopak. Na registráciu zariadení v tomto režime je potrebné stiahnuť aplikáciu AppTec a naskenovať kód QR. Vytvorte zariadenie v konzole a ako typ zariadenia vyberte "AE Container (BYOD & Enahnced Work Profile)". Kliknutím na QR kód na novo vytvorenom zariadení získajte QR kód a nastavte prvý prepínač na "Legacy & BYOD".

Rozšírený pracovný profil AE: (vyžaduje systém Android 11 alebo novší) Zatiaľ čo vyššie uvedený kontajner BYOD prináša firemné údaje na súkromné zariadenie, rozšírený pracovný profil robí to isté, ale pre zariadenie vo vlastníctve spoločnosti. Vytvára rovnaký kontajner, ale dáva správcovi trochu väčšiu kontrolu nad zariadením, takže používateľ nemôže jednoducho odstrániť MDM zo zariadenia. Vytvorte zariadenie v konzole a ako typ zariadenia vyberte "AE Container (BYOD & Enahnced Work Profile)". Kliknutím na QR kód na novovytvorenom zariadení získajte QR kód a nastavte prvý prepínač

na "Enhanced Work Profile". Tento QR kód môžete naskenovať po resetovaní zariadenia a 6-krát ťuknúť na obrazovku, ako je vysvetlené v Metóde 1 v časti Registrácia AE.

Ako môžem priradiť aplikácie k zariadeniam so systémom Android Enterprise?

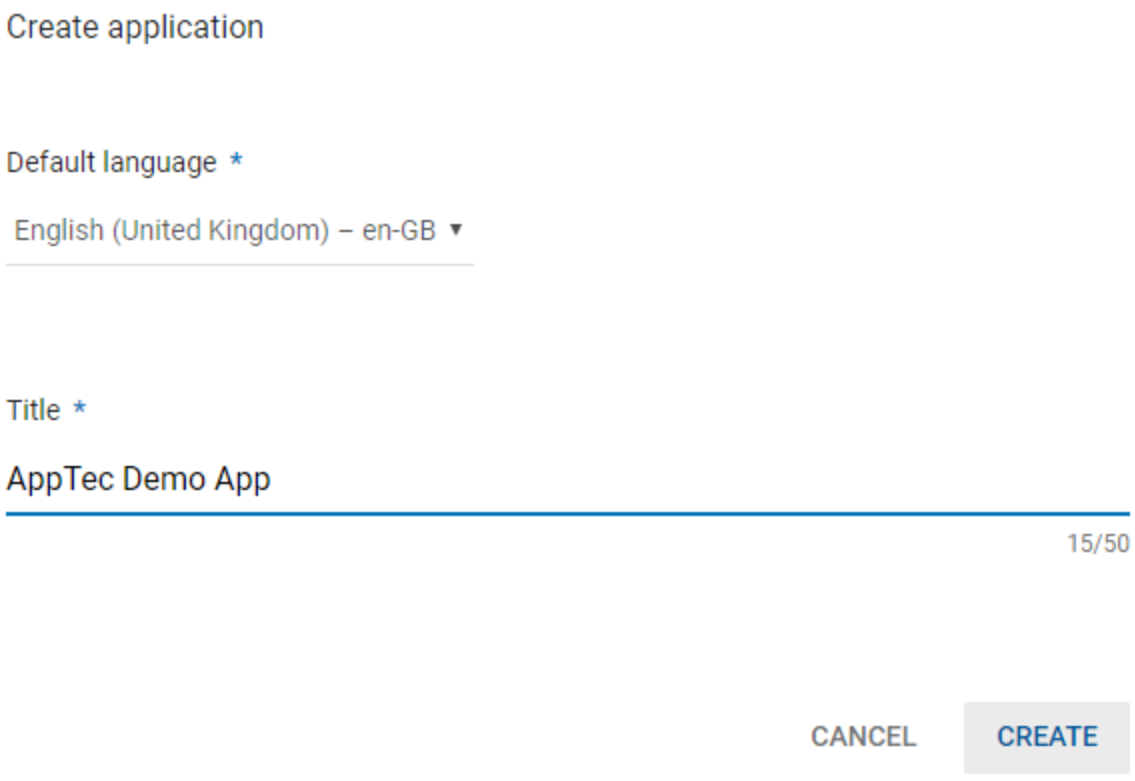
Najprv musíte schváliť aplikácie, ktoré chcete používať, v časti Všeobecné nastavenia → Správa aplikácií → Obchod AE Play → Aplikácie obchodu Play. Po schválení aplikácie ich môžete priradiť do zoznamu povinných aplikácií → svojho profilu kliknutím na "+" a výberom aplikácie na karte "AE Play Store". Tým sa aplikácia automaticky stiahne a nainštaluje. V zariadení nie je potrebné žiadne konto Google a používateľ to nemusí potvrdzovať ani povoľovať.

Nahrávanie vlastných aplikácií do obchodu Google Play

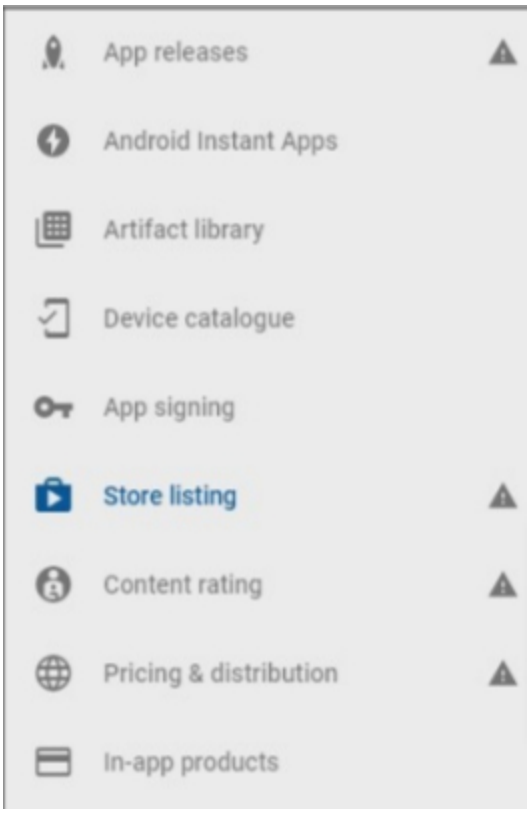
Do obchodu Google Play je možné nahrať vlastné aplikácie. Týmto spôsobom môžete využívať rôzne výhody, ako je napríklad mechanizmus aktualizácie obchodu Play.

Na to potrebujete vývojárske konto Google. Prihláste sa pomocou služby Google Play Console(https://play.google.com/apps/publish).

Kliknite na "Vytvoriť aplikáciu". Vyberte predvolený jazyk a názov aplikácie.



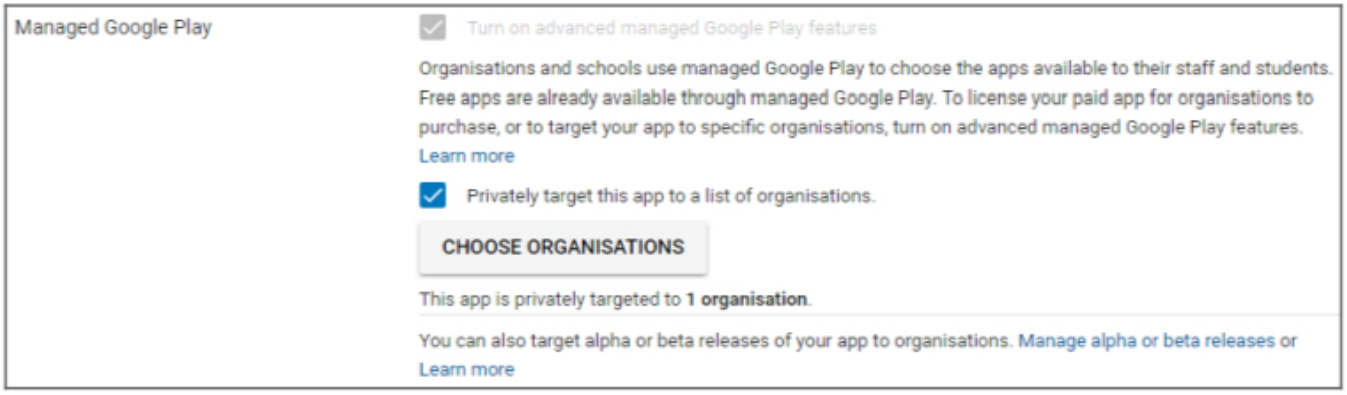
Na nasledujúcej stránke budete požiadaní o zadanie rôznych údajov o vašej aplikácii.



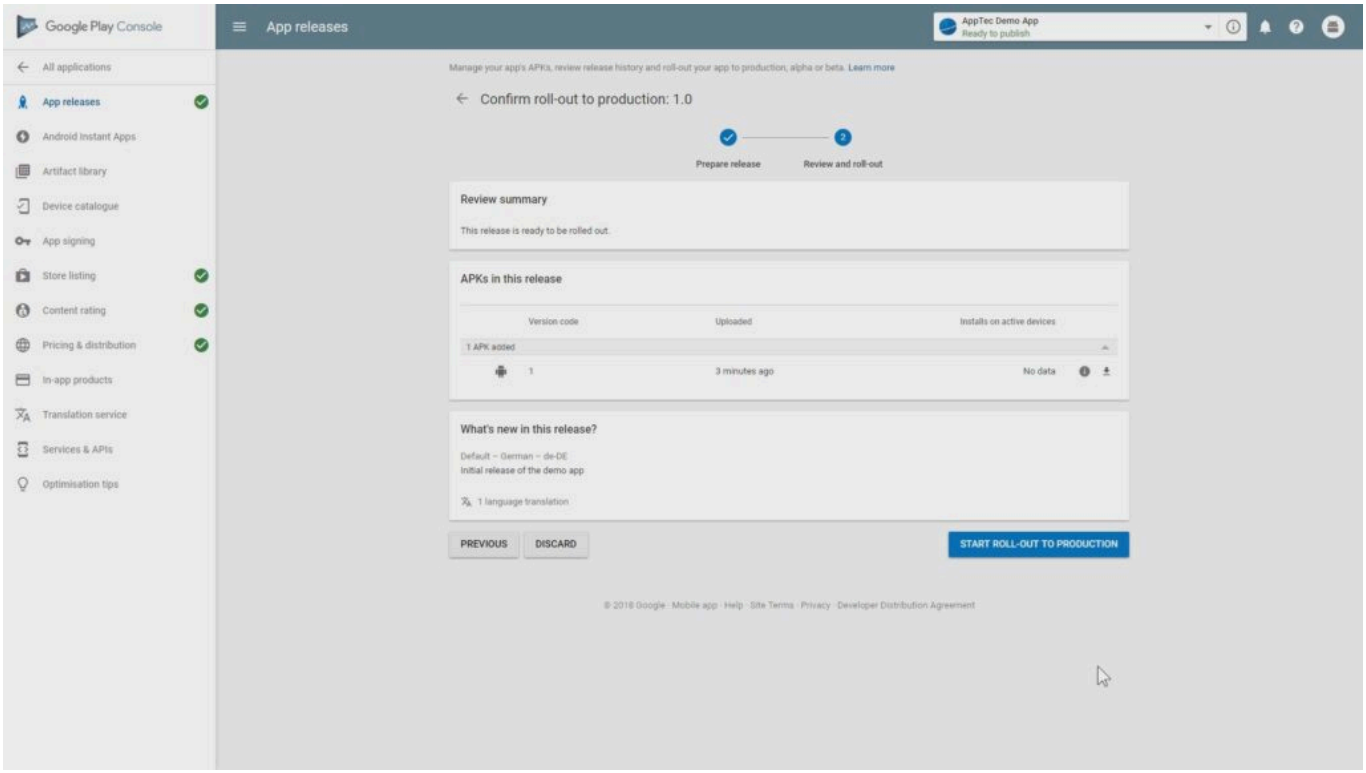
Po zadaní všetkých údajov sa na ľavej strane zobrazia rôzne nápovedné symboly.

Prejdite nad ne, aby ste videli, ktoré kroky zostávajú, a postupujte podľa nich v ľubovoľnom poradí.

Poznámka: Nezabudnite zaškrtnúť dve zaškrtávacie políčka v časti "Spravované služby Google Play" v časti "Ceny a distribúcia". V opačnom prípade bude aplikácia verejná a bude k nej mať prístup každý. Tiež sa uistite, že ste si vybrali krajinu pre distribúciu.



Po dokončení všetkých krokov môžete prejsť na "Vydanie aplikácie". Kliknutím na "Review" (Preskúmať) a "Start Roll-Out to Production" (Spustiť roll-out do výroby) dokončíte návrh a zverejníte aplikáciu.



Kým bude aplikácia dostupná v obchode Play, potrvá to nejaký čas. Po dokončení procesu môžete svoju aplikáciu vyhľadať v obchode Play for Work a schváliť ju. Potom môžete aplikáciu jednoducho priradiť k zariadeniam pomocou konzoly EMM rovnako, ako to robíte s inými aplikáciami.

Požiadavky a inštalácia

Požiadavky

Systémové požiadavky

Virtuálne zariadenie je k dispozícii vo formáte Open Virtualization Format (VMWare, VirtualBox, Citrix Xen Server) a ako komprimovaný súbor .vhdx (Hyper-V)*.

*Poznámka: Pri používaní Hyper-V musí byť počítač vytvorený s generáciou 1.

Virtuálny disk má cieľovú veľkosť 20 GB a počítač vyžaduje 4 GB pamäte RAM.

Zariadenie je založené na Debiane 9 64bit

Aktualizujte importovaný počítač na najnovšiu kompatibilitu (napr. vo VMWare) a uistite sa, že typ operačného systému počítača je vo vašom hypervízore nastavený správne.

Licenčný kľúč

Na úspešnú aktiváciu a inštaláciu servera potrebujete platný licenčný súbor. Môžete ho získať priamo od spoločnosti AppTec360 a/alebo od príslušného predajcu.

Rozlíšenie IP adries a DNS

Zariadenie AppTec360 musí byť dosiahnuteľné zariadením, ktoré používa názov hostiteľa, pre ktorý je licencia vydaná.

Ak chcete zaregistrovať zariadenia so systémom Windows 10, musíte tiež nastaviť ďalšiu subdoménu v podobe "enterpriseenrollment.", ktorá bude smerovať na zariadenie.

Certifikát SSL

Keďže všetky pripojenia k zariadeniam a zo zariadení musia byť zabezpečené pomocou protokolu SSL, potrebujete platný certifikát pre názov hostiteľa vydaný certifikačnou autoritou, ktorej zariadenie dôveruje. Súkromný kľúč pre certifikát musí byť nahraný bez ochrany heslom. Vo väčšine prípadov je potrebný sprostredkovateľský certifikát pre certifikačnú autoritu, aby zariadenia rozpoznali certifikát servera.

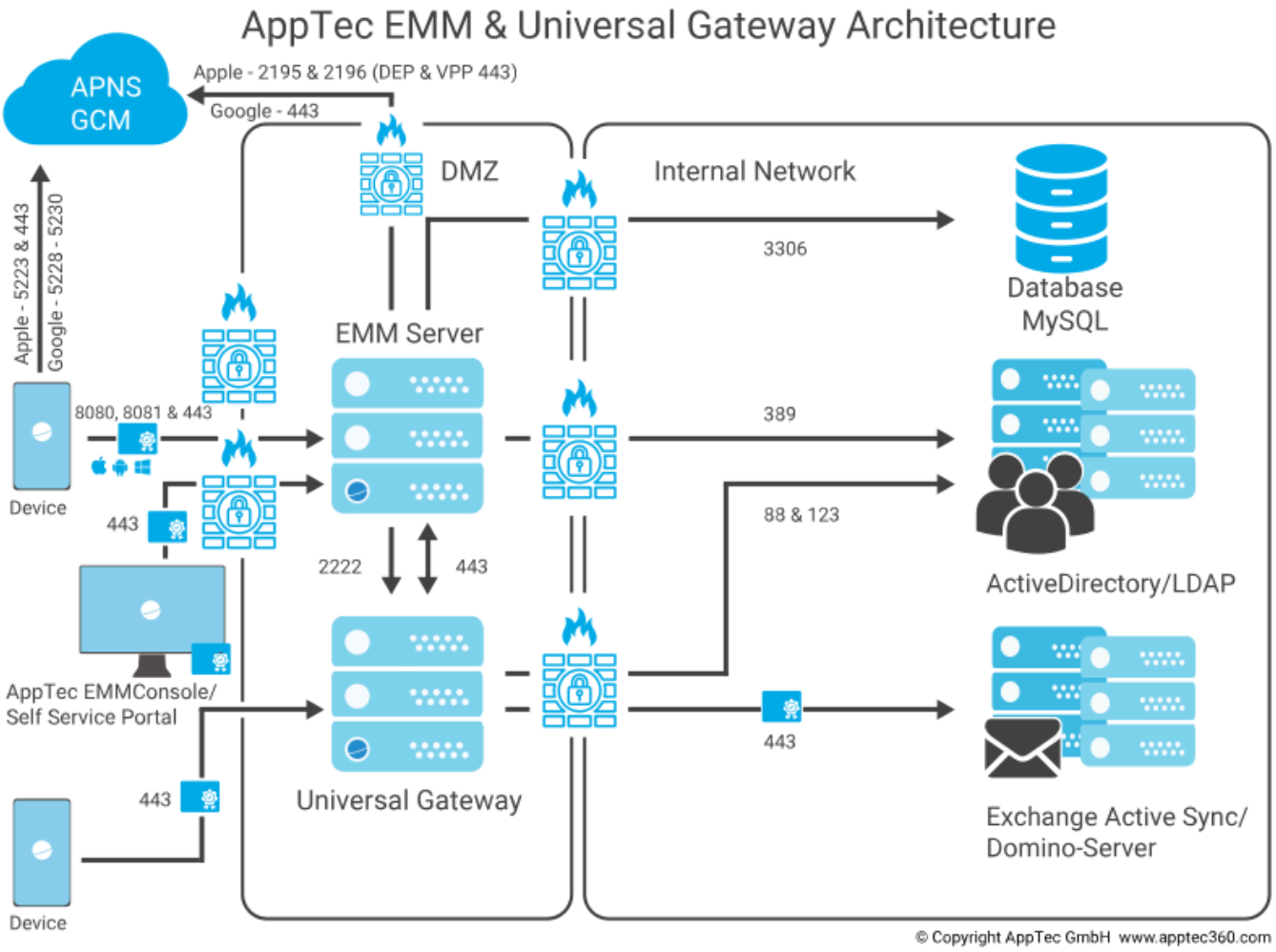
Zariadenia so systémom Windows 10 budú vyžadovať špecifický certifikát pre vašu podnikovú subdoménu.

Od verzie zariadenia 202104 môžete používať aj certifikáty Let's Encrypt, ktoré sa generujú automaticky (popísané v druhom kroku - Certifikát SSL).

Server SMTP

Na to, aby AppTec360 EMM mohol odosielať e-maily (napr. na registráciu zariadenia a overenie účtu), je potrebný e-mailový server a/alebo e-mailová relé.

Pravidlá brány firewall



Tento diagram ukazuje, ktoré pripojenie je potrebné v závislosti od toho, aké služby chcete používať.

Podrobnejší opis nájdete v tabuľke na nasledujúcej strane.

Akékoľvek (externé/zariadenia)	→	**AppTec360 Appliance / emmconsole.com**
Porty	443	Správa, podnikový obchod s aplikáciami a komunikácia so systémom Windows Phone
	8080	Komunikácia so systémom Android a iOS
	80	Prvé nastavenie aplikácie Let´s Encrypt. Potom používa 443.
Akékoľvek (zariadenia)	→	**ľubovoľný (externý)**
Porty	5223, 443	Služba Apple Push Service, musí byť dostupná bez proxy servera, 443 ako Fallback, pozri https://support.apple.com/en-us/HT203609
	5228-5230	Služba Android Push Service (FCM), musí byť dostupná bez proxy servera
Zariadenie AppTec360	→	**Radič domény**
Porty	389, (LDAPS 636)	Synchronizácia používateľov s LDAP
Zariadenie AppTec360	→	**Akékoľvek**
Prístav	443	Používa sa pre službu Android Push Service (GCM) Vyhľadávanie v AppStore / Obchode Play
Zariadenie AppTec360	→	**emmconsole.com**
Porty	443	Aktualizácie zariadenia AppTec360, generovanie certifikátov APNS
Zariadenie AppTec360	→	**Sieť Apple (17.0.0.0/8)**
Porty	2195, 2196	Služba Apple Push Service & Feedback Service
	443	DEP A VPP

Aktualizácie zabezpečenia

Operačný systém Debian by sa mal pravidelne aktualizovať, aby ste získali najnovšie bezpečnostné opravy. Uistite sa však, že na novšiu hlavnú verziu Debianu neaktualizujete ručne. Keď bude AppTec360 EMM kompatibilný s novšou hlavnou verziou, pridáme spôsob aktualizácie v aktualizácii zariadenia.

Predvolené heslá virtuálneho zariadenia

Prihlásenie používateľa (Prihlásenie koreňového systému je zakázané. Na administračné úlohy použite "sudo")

apptec

Prihlasovacie heslo

apptec

Koreňový používateľ MySQL

root

Heslo koreňového servera MySQL

apptec

Predvolený používateľ MySQL

AppTec

Predvolené heslo používateľa MySQL

AppTec

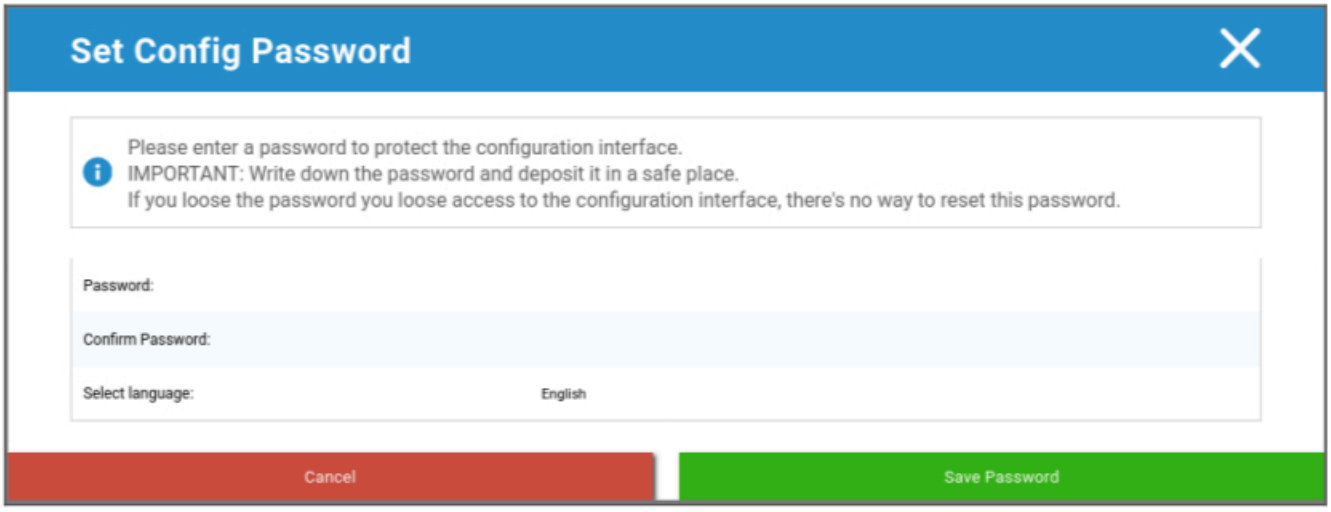
Konfigurácia virtuálneho zariadenia

Dôležité: Pred začatím konfigurácie virtuálneho zariadenia by malo byť rozlíšenie displeja nastavené aspoň na 1280 x 800 pixelov.

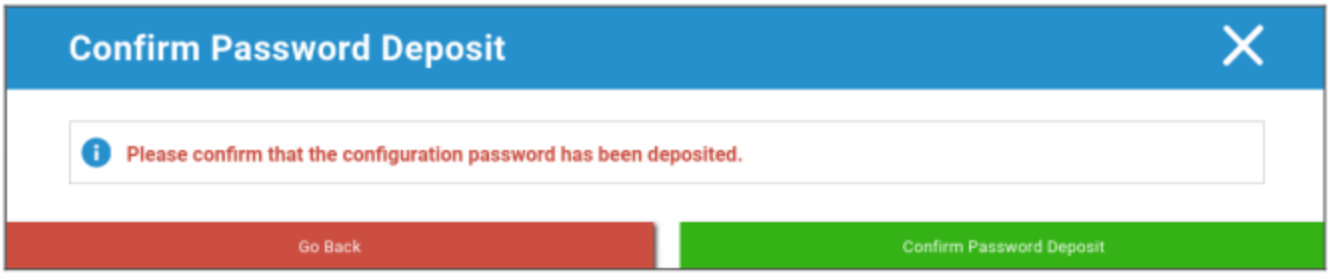
Po dlhom prihlásení do zariadenia by sa mal automaticky spustiť prehliadač Firefox a zobraziť konfiguračné rozhranie.

Príprava

Najprv je potrebné zadať heslo pre konfiguračné rozhranie. Toto heslo sa používa na šifrovanie všetkých informácií a súborov zadaných v konfiguračnom rozhraní. Tu môžete tiež nastaviť jazyk, v ktorom sa má rozhranie zobrazovať (možno ho zmeniť neskôr).

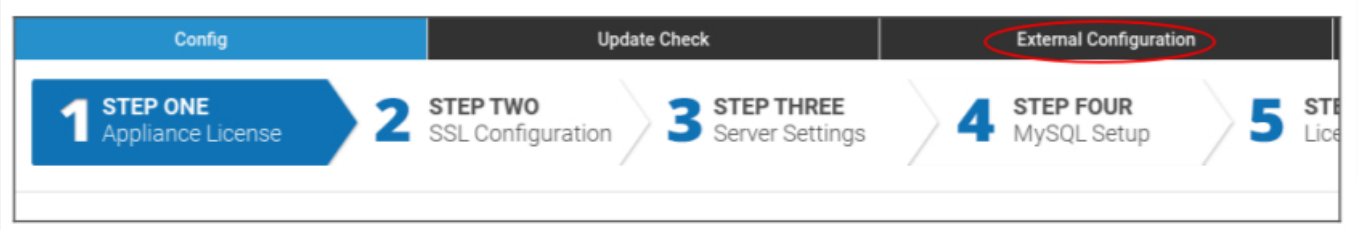


Heslo môže resetovať iba podpora AppTec360, preto si ho uložte na bezpečné miesto a potvrďte nadchádzajúce vyskakovacie okno.



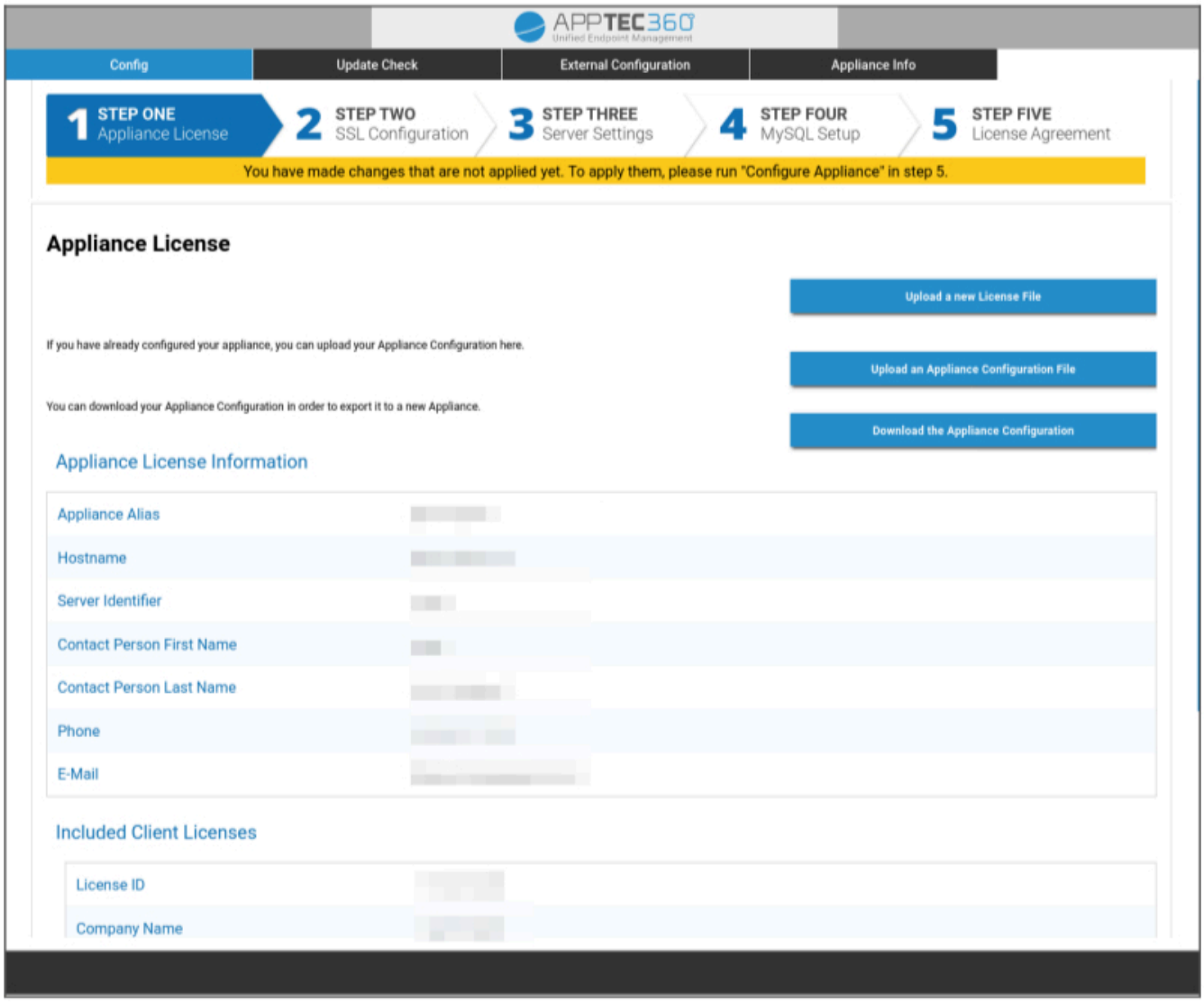
Konfigurácia z externého hostiteľa

Ak chcete uľahčiť proces nastavenia, môžete stránku konfigurácie sprístupniť zo vzdialeného prístupu. Postupujte podľa krokov uvedených v časti "Konfigurácia z externého hostiteľa".



Prvý krok – Licencia spotrebiča

1. Nahrajte licenčný súbor, ktorý ste dostali od spoločnosti AppTec.
2. Ak bol licenčný súbor úspešne nahraný, môžete vidieť informácie o licencii spotrebiča, ako na nasledujúcej snímke obrazovky.



Druhý krok – certifikát SSL

Môžete použiť automatické nastavenie certifikátov pomocou služby Let's Encrypt alebo si certifikáty zabezpečiť sami (viac informácií nájdete v časti SSL-Certifikát).

Automatické

Certifikát sa automaticky vygeneruje pomocou služby Let's Encrypt.

AppTec360 EMM používa na overenie domény výzvu HTTP-01, čo znamená, že pri prvej žiadosti o certifikát musí byť otvorený port HTTP z internetu. Následné žiadosti o obnovenie môžu byť overené prostredníctvom HTTPS.

Prepnite prepínače na možnosť "Automatic (Let's Encrypt)" a stlačte tlačidlo "SAVE VALUES". Certifikát bude automaticky vyžiadaný pri použití konfigurácie v piatom kroku - Licenčná zmluva. Certifikát sa v prípade potreby automaticky obnoví a v prípade blížiaceho sa vypršania platnosti certifikátu (čo znamená, že obnovenie mohlo zlyhať) dostanete e-mail.

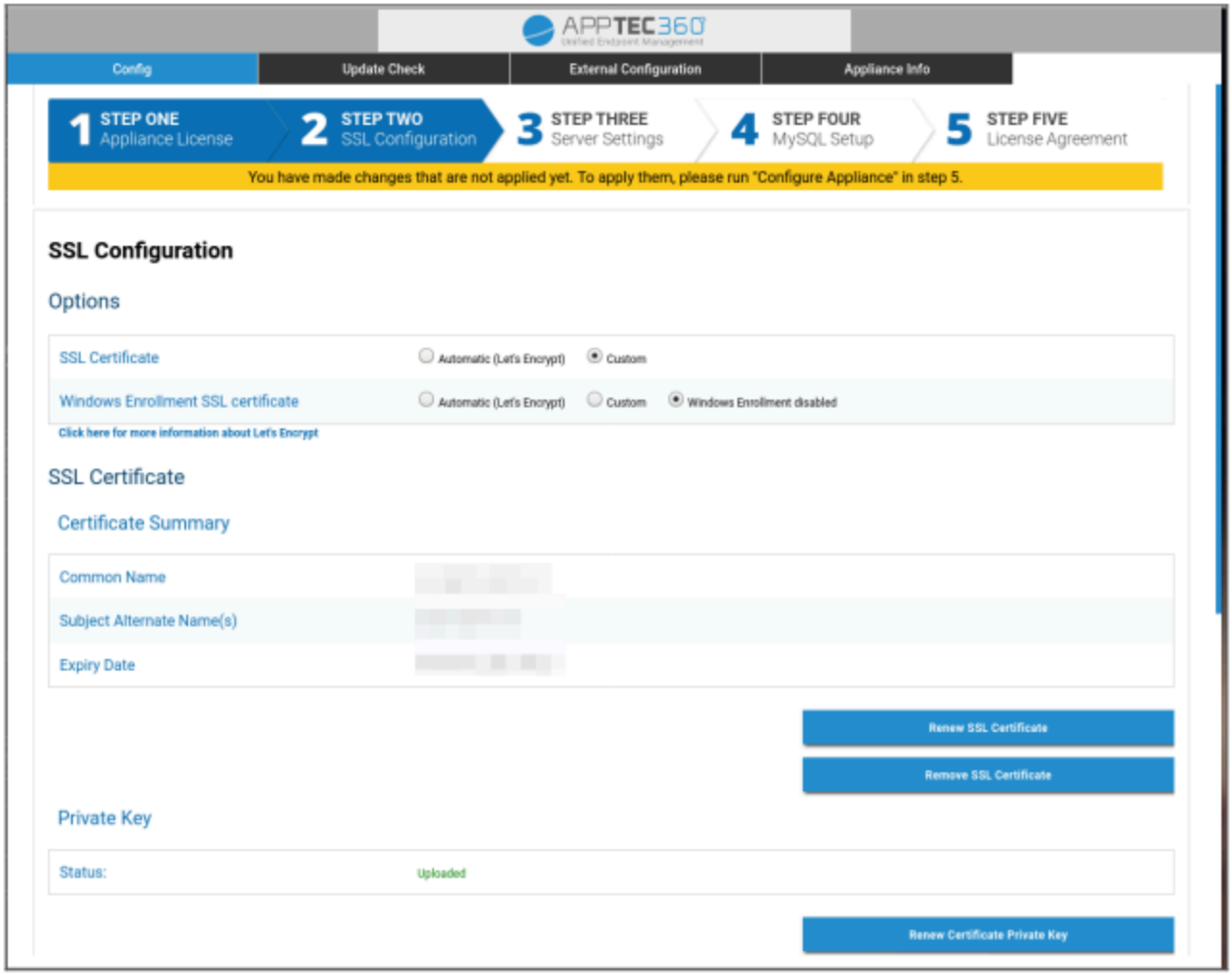
Vlastné

1. Nahrajte certifikát SSL pre vaše licencované hostiteľské meno. Názov hostiteľa si môžete pozrieť v prvom kroku - Licencia spotrebiča.

2. Nahrajte aj súkromný kľúč k certifikátu a v prípade potreby aj sprostredkovateľský certifikát.

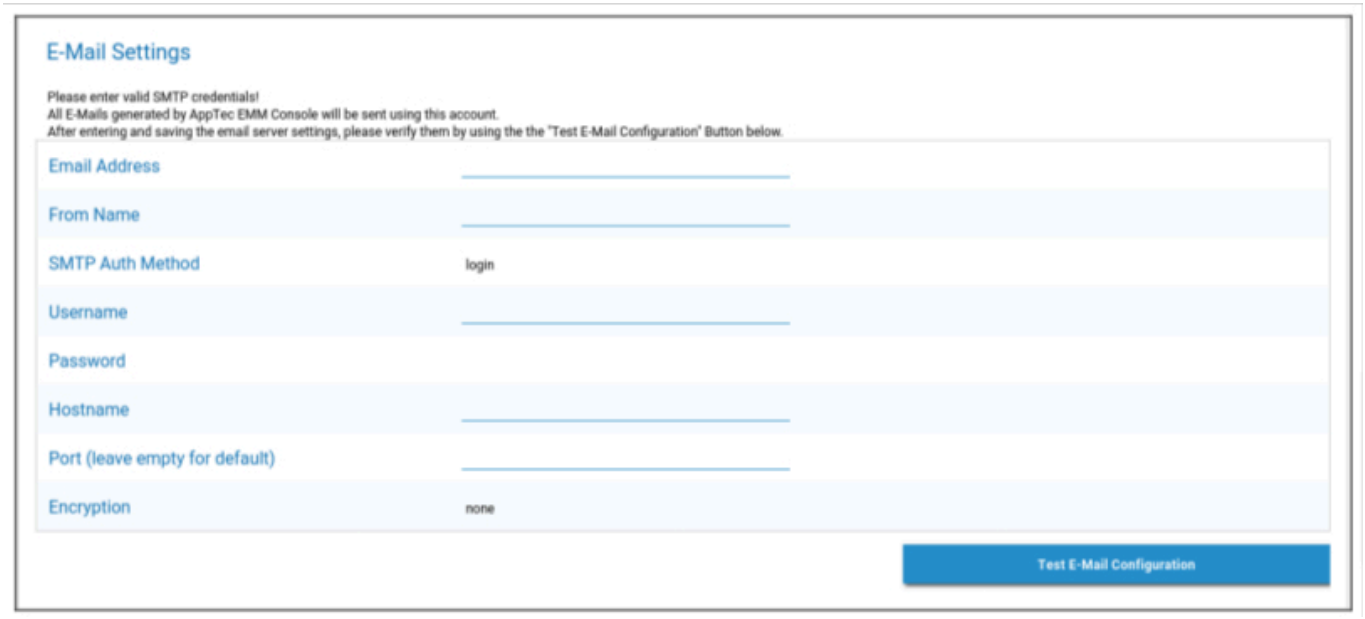
Dôležité: Kľúč nesmie byť chránený heslom. Ak je, pred odoslaním odstráňte heslo.

Tip: Ak chcete používať aj zariadenia so systémom Windows 10, musíte povoliť funkciu "Certifikát Windows Enrollment SSL" a nahrať certifikát, súkromný kľúč a sprostredkovateľský certifikát pre vašu subdoménu (opísané v časti Nahrávanie IP adresy a rozlíšenie DNS) v dolnej časti stránky.



Tretí krok – Nastavenia servera

1. Zadajte globálnu e-mailovú adresu podpory. Táto adresa sa bude používať v e-mailoch pre vašich používateľov, aby vedeli, na koho sa majú obrátiť v prípade akýchkoľvek problémov týkajúcich sa ich zariadenia.
2. Zadajte nastavenia elektronickej pošty, ktoré má systém používať na odosielanie e-mailov. Tieto nastavenia sa použijú na odosielanie e-mailov používateľovi a tiež na odosielanie hlásení o chybách a požiadaviek na funkcie na adresu"support@apptec360.com". Po uložení nastavení e-mailu je potrebné ich overiť kliknutím na "Test E-Mail Configuration" (Otestovať konfiguráciu e-mailu) a postupovať podľa pokynov.



Štvrtý krok – Nastavenie MySQL

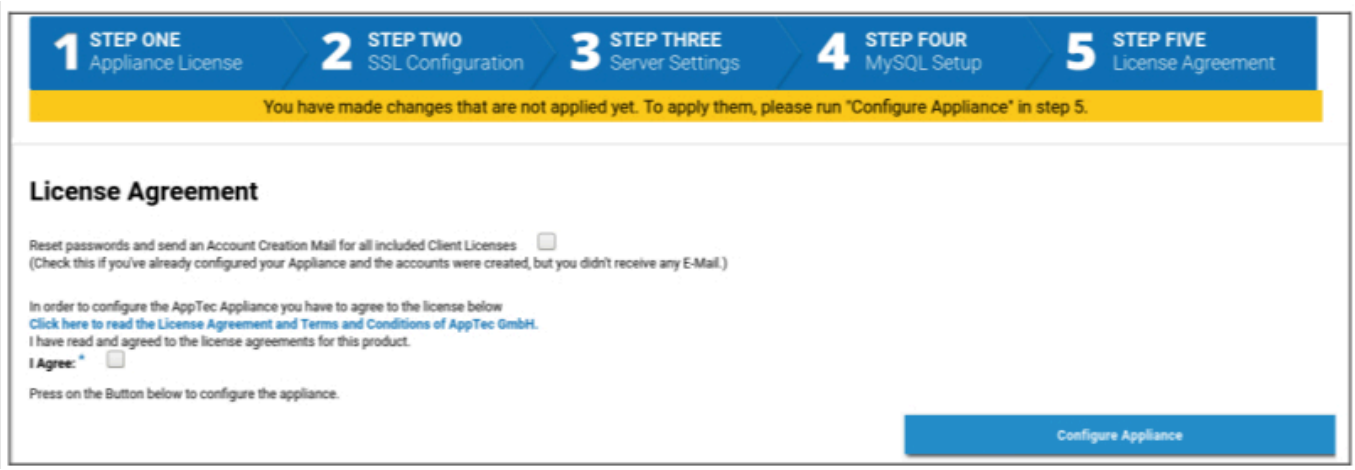
1. Ak chcete používať internú databázu, môžete tento krok preskočiť. V opačnom prípade môžete zadať informácie o pripojení k externému databázovému serveru.


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)

Piaty krok – Licenčná zmluva

1. Prečítajte si licenčnú zmluvu.
2. Začiarknite políčko "I Agree" (Súhlasím) a stlačte tlačidlo "Configure Appliance" (Konfigurovať spotrebič), aby ste použili nastavenia.

Tip: Pri každej zmene nastavení v 5 krokoch je potrebné spustiť funkciu "Konfigurácia zariadenia", aby sa nastavenia použili.



Gratulujeme!

Dokončili ste konfiguráciu virtuálneho zariadenia.

Na adresu, ktorú ste uviedli pre licenciu (viditeľnú v časti "Zahrnuté klientske licencie" v prvom kroku - Licencia spotrebiča), bol odoslaný e-mail vrátane hesla.

Teraz sa môžete prihlásiť do konzoly pomocou tohto hesla a e-mailovej adresy, na ktorú ste ho dostali.

Ak sa chcete prihlásiť do konzoly, zadajte názov hostiteľa konzoly do adresného riadka prehliadača.

Názov hostiteľa vášho spotrebiča nájdete v prvom kroku - Licencia spotrebiča.

Riešenie problémov

1. Pri konfigurácii spotrebiča v piatom kroku - Licenčná zmluva - ste nedostali e-mail:

Skontrolujte, či sú nastavenia e-mailu v treťom kroku - Nastavenia servera správne. Pre opätovné odoslanie hesla zaškrtnite "Resetovať heslá a odoslať mail o vytvorení účtu pre všetky zahrnuté klientské licencie" v piatom kroku - Licenčná zmluva pred opätovným spustením "Konfigurácia zariadenia".

2. Počas konfigurácie v piatom kroku - Licenčná zmluva - ste dostali chybu týkajúcu sa služby Let's Encrypt:

Uistite sa, že je zariadenie dosiahnuteľné pomocou názvu domény na porte 80. Let's encrypt tiež zapisuje protokol do "/var/log/letsencrypt", ktorý môže pomôcť pri ďalšom riešení problémov.

Bezpečnostné odporúčania

Na zabezpečenie zariadenia AppTec360 sa odporúča vykonať nasledujúce kroky.

Toto nie je úplný súbor pokynov, je to len odporúčanie pre základnú konfiguráciu.

- Zmena hesla pre používateľa AppTec360
- Zmeňte heslo pre používateľov MySQL "root" a "AppTec" a aktualizujte štvrtý krok - Nastavenie MySQL
- Zmena predvoleného portu servera SSH
- V konzole zablokujte port 80 a zakážte prichádzajúcu prevádzku HTTP, používajte len HTTPS. Po konfigurácii je možná aj externá konfigurácia cez HTTPS.
- Obmedzenie prístupu k rozhraniu správy len na určité IPS v dolnej časti tretieho kroku - Nastavenia servera
- Konfigurácia brány firewall

Všeobecné nastavenia

Prehľad účtov

Informácie o účte

Prehľad

Tu si môžete pozrieť prehľad svojho účtu AppTec360.

Názov spoločnosti	Názov vašej spoločnosti
Dátum vytvorenia	Dátum vytvorenia vášho účtu
Typ licencie	Paid = platená licencia Bezplatná = neplatená licencia Poznámka: Účty v zariadení OnPremise sa z technických dôvodov vždy zobrazujú ako zaplatené.
Identifikátor klienta	Identifikátor vášho účtu (toto NIE je vaše zákaznícke číslo)
Dátum skončenia platnosti licencie	Dátum skončenia platnosti vašej licencie AppTec360
Licencia ContentBox	Free = bezplatná licencia pre 25 zariadení Platené = platená licencia pre x zariadení
Spúšťač	Zobrazuje, či môžete používať vlastný spúšťač pre Android
Zariadenia	Počet aktuálne používaných / celkový počet licencií
Kontaktná osoba	Poskytnutá kontaktná osoba
Telefón	Poskytnuté telefónne číslo
eMail*	Poskytnutá e-mailová adresa
Používateľ koreňového systému	Používatelia koreňového systému, ktorí sa môžu prihlásiť
Verzia softvéru	Aktuálna verzia softvéru

**Poznámka: Tu uvedená e-mailová adresa je tá, ktorú ste zadali pri registrácii konta. Na jej základe sa v strome používateľov/zariadení vytvorí používateľ, ktorého je možné upraviť. Úpravou tohto používateľa sa zmení e-mailová adresa, ktorú musíte použiť na prihlásenie, ale nie informácie v prehľade účtov .*

Správa o chybe

Hlásenie o chybe môžete poslať priamo na podporu a nahlásiť problémy alebo chyby, ktoré obsahujú informácie a protokoly o vašom účte a nastavení.

Predmet	Predmet hlásenia chyby. Uveďte číslo hlásenia, ak ho chcete pridať k existujúcemu hláseniu podpory.
Očakávané správanie	Podrobne opíšte, čo ste urobili a čo ste očakávali, že sa stane
Skutočné správanie	Podrobne opíšte, čo sa presne stalo. Presne uveďte chybové hlásenia. Pomôže tiež, ak do prílohy pridáte snímky obrazovky.
V akom čase ste zaznamenali tento problém?	Uveďte presný čas, kedy ste dostali konkrétnu chybovú správu/problém. V najlepšom prípade uveďte aj sekundy, napr. 18:55:27
Dá sa tento problém zopakovať? Ak áno, ako (podrobne)?	Podrobne popíšte, ako môžete problém reprodukovať.
Fungovala táto funkcia predtým tak, ako ste očakávali? Ak áno, dokedy?	Ak neviete, nechajte prázdne.
Boli pred objavením tohto problému vykonané v systéme nejaké konkrétne zmeny? Ak áno, aké zmeny (podrobne)?	Vždy uveďte, aká bola vaša posledná zmena alebo činnosť pred objavením sa problému, aj keď si myslíte, že je to nepodstatné.
Ak sa uplatňuje: Ktorých modelov zariadení a verzií operačného systému sa to týka?	Vždy uveďte presný názov verzie operačného systému (napr. iOS 14.7.1 alebo Android 11)
Ak sa uplatňuje: Aká je verejná IP adresa a/alebo sériové číslo zariadenia?	Uveďte aspoň jedno, aj keď sa to týka všetkých zariadení.
Zahrnúť súbory denníka	Začiarknite túto možnosť, ak chcete odoslať súbor denníka s hlásením chyby. Odporúča sa to urobiť.
Získanie aktuálneho stavu VPP od spoločnosti Apple a zahrnutie do hlásenia o chybe	Obsahuje informácie o pridelení licencií VPP. Aktivujte ju len vtedy, ak vás o to požiada podpora alebo ak sa váš problém týka VPP.
Príloha	Priložte akýkoľvek súbor, ktorý by mohol byť užitočný (napr. snímky obrazovky s chybovou správou).

Žiadosť o funkciu

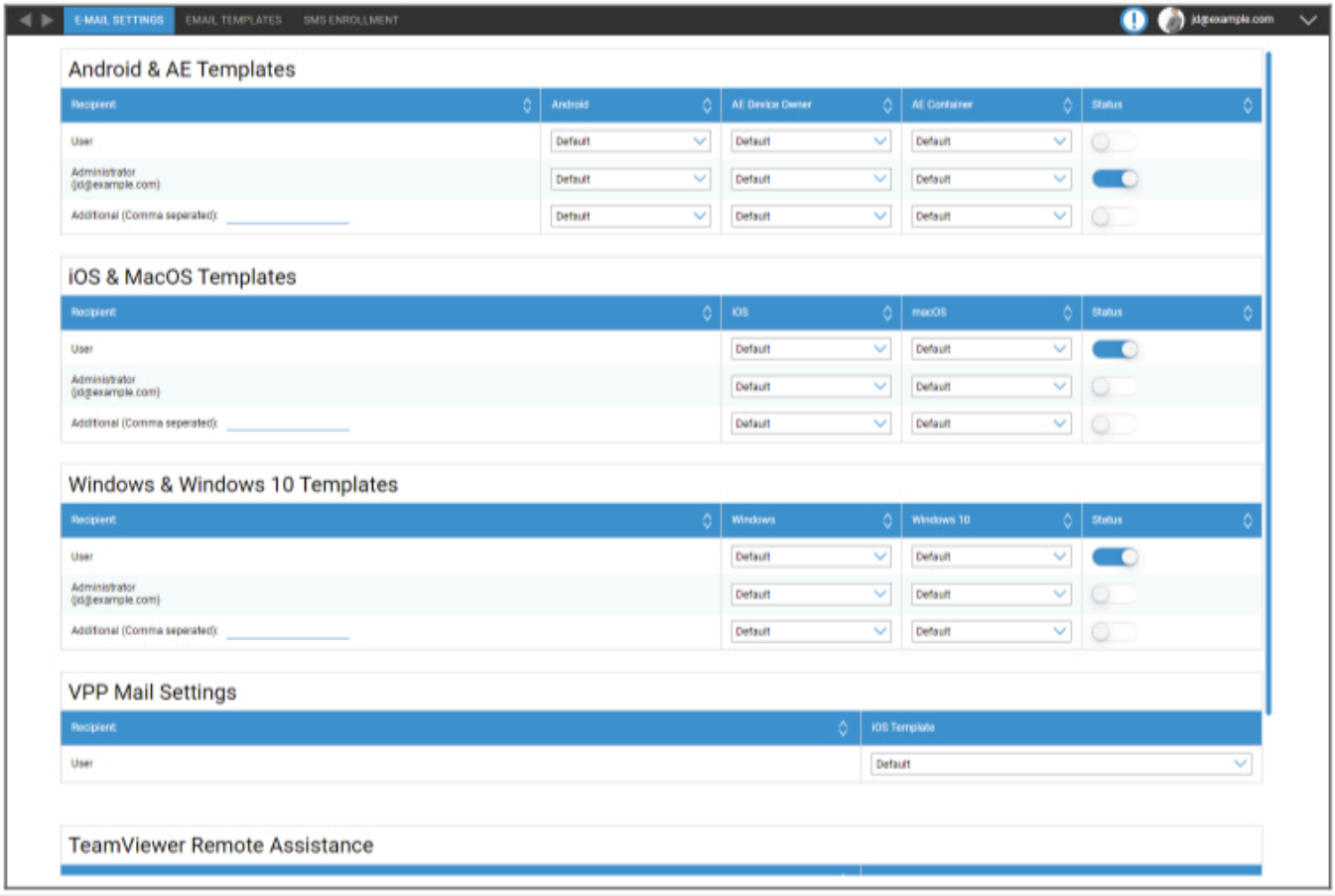
Žiadosť o funkciu môžete poslať priamo na podporu. Môže obsahovať požiadavku na konkrétnu funkciu alebo vylepšenie pre

Zhrnutie	Stručné zhrnutie vášho problému
Popis	Podrobný opis vášho problému, buďte čo najkonkrétnejší.
Príloha	Pripojenie súborov k správe o chybe

Globálna konfigurácia

Nastavenia elektronickej pošty

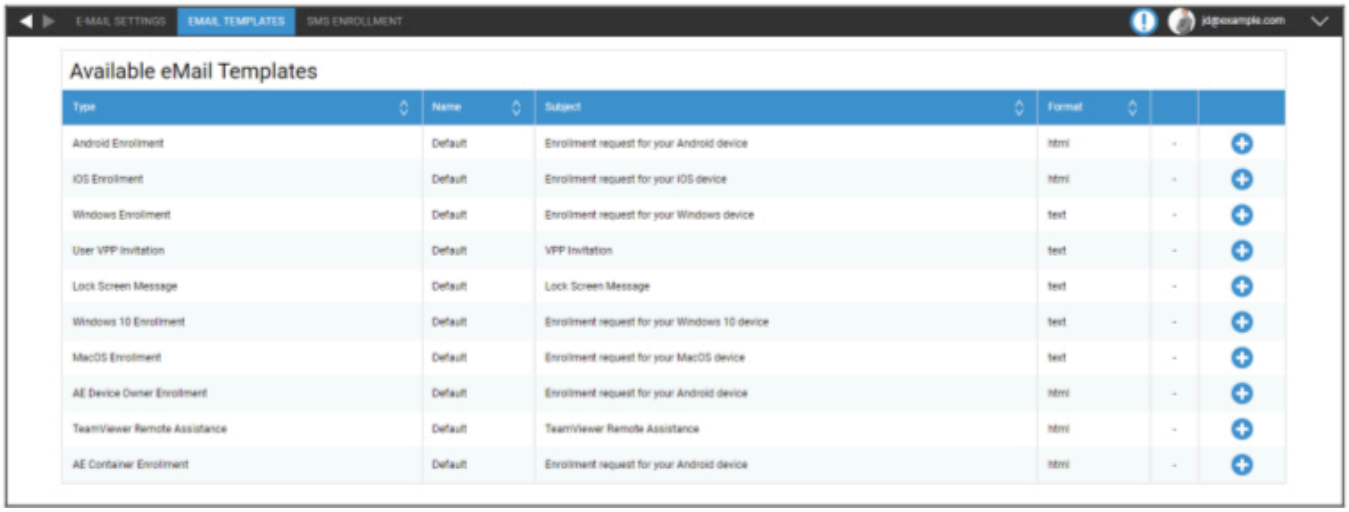
Tu môžete definovať, kto dostane e-mail, keď sa vygeneruje žiadosť o registráciu, a aká textová šablóna sa pre tento e-mail použije.



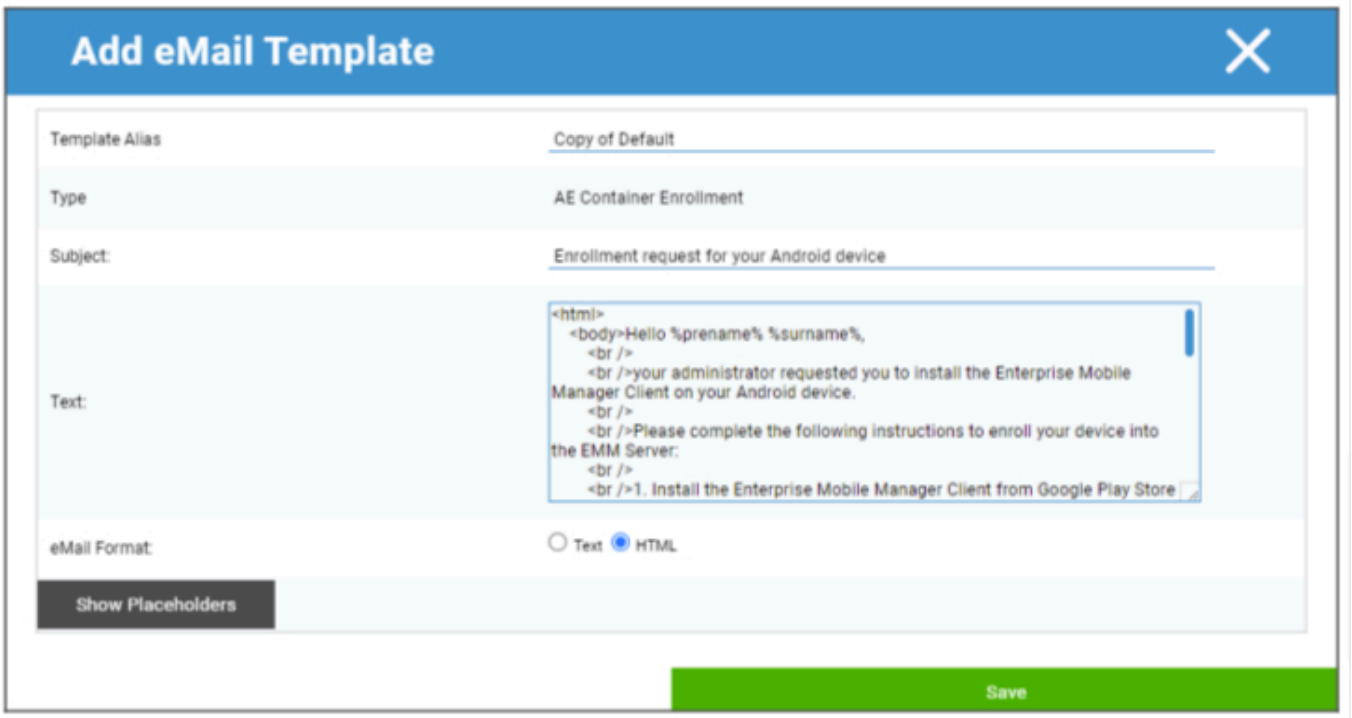
Šablóny elektronickej pošty

Tu môžete vytvárať a upravovať šablóny pre rôzne scenáre. Tie môžu byť v normálnej textovej forme alebo v HTML. V HTML môžete lepšie kontrolovať formátovanie textu.

Predvolené šablóny nie je možné upraviť ani vymazať.



Ako premennú môžete použiť aj zástupné znaky, ktoré budú automaticky nahradené. Ak chcete zobraziť dostupné zástupné symboly, kliknite počas úprav na "Zobraziť zástupné symboly". Rôzne kategórie majú rôzne Placeholdery.



Zápis SMS

Tu môžete deaktivovať proces registrácie SMS.

(Predvolené nastavenie: deaktivované)

Zobrazí sa aj informácia o tom, koľko SMS kreditov je ešte k dispozícii.

SMS kredity je potrebné zakúpiť samostatne.

Ochrana osobných údajov

Prístup GPS

Tu môžete chrániť zobrazenie GPS pre každé zariadenie pomocou 1 alebo 2 hesiel (princíp štyroch očí). Pri každom pokuse o prístup k polohe zariadenia budete vyzvaní na zadanie hesla (hesiel).

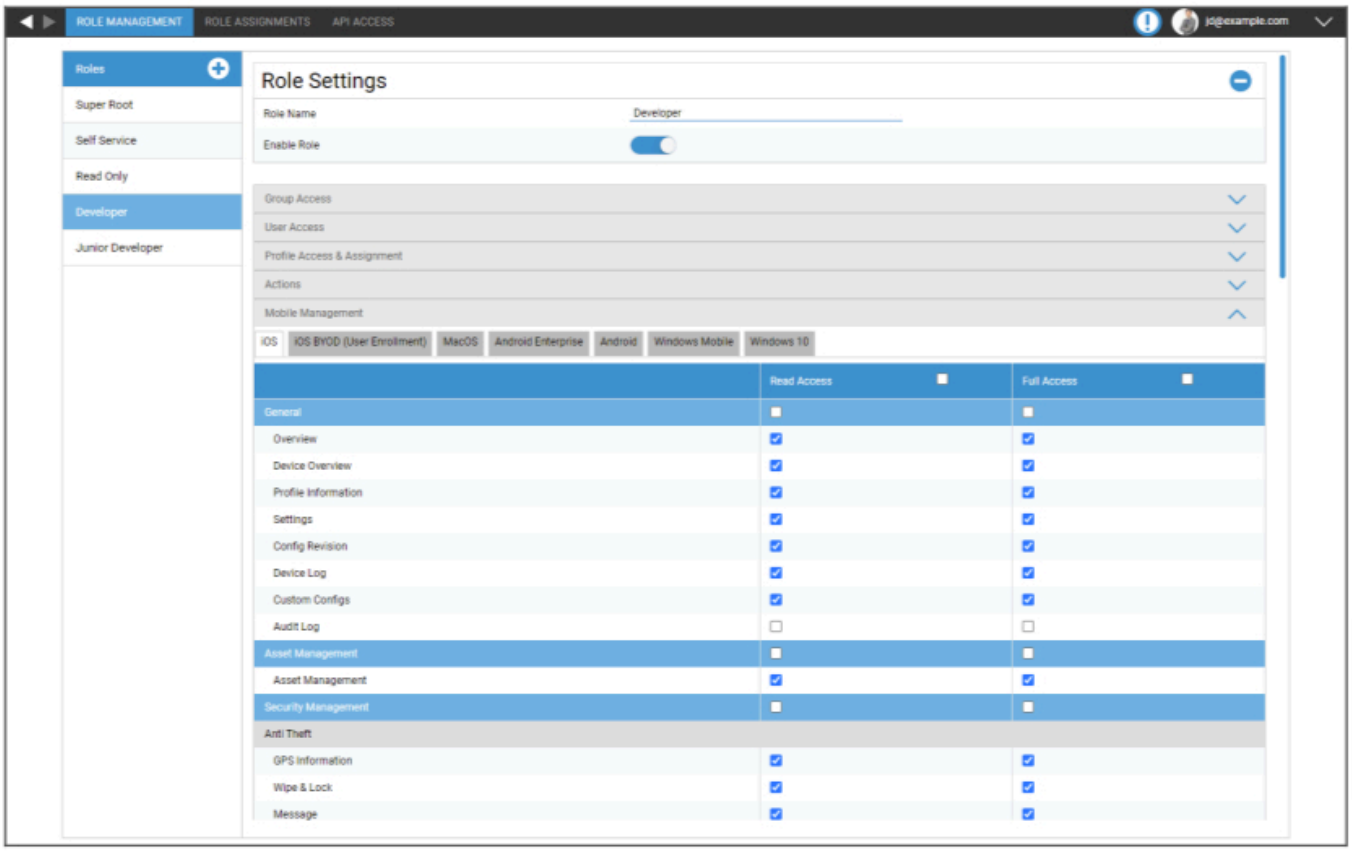
Obmedzenie prístupu k nastaveniam GPS	Vypnuté = funkcia je vypnutá a na lokalizáciu sa nevyžaduje heslo
	Zapnuté = funkcia je zapnutá a na lokalizáciu sa vyžaduje heslo
Metóda ochrany	Použiť jedno heslo = použiť jedno heslo na lokalizáciu
	Použiť dve heslá = použiť dve heslá na lokalizáciu
Zadajte heslo (1)	Zadajte zvolené heslo
Opakovanie hesla (1)	Opätovné zadanie zvoleného hesla
voliteľné: Zadajte heslo 2	Zadajte druhé zvolené heslo
voliteľné: Opakujte heslo 2	Opätovné zadanie druhého zvoleného hesla

Poznámka: Po nastavení prístupového kódu (kódov) ho musíte zadať ešte raz, kým sa úplne aktivuje.

Prístup na základe rolí

Riadenie rolí

Roly definujú, čo môže používateľ vidieť a robiť, keď sa prihlási do konzoly na správu. To vám umožní vytvoriť používateľov, ktorí sa môžu prihlásiť, ale majú obmedzené funkcie.



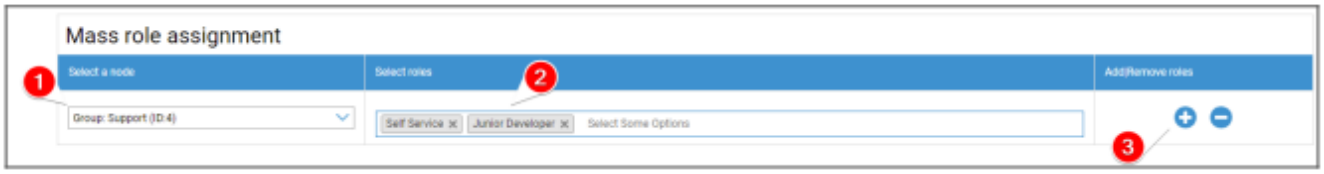
Rola Super Root je predvolená rola, ktorá má vždy možnosť vidieť a meniť všetko. Nemožno ju zmeniť ani odstrániť. Samoobslužná rola je schopná vidieť len svojho vlastného používateľa a zariadenia. Môžete skombinovať samoobslužnú rolu a vlastnú rolu, aby ste napr. umožnili používateľom prihlasovať sa a registrovať zariadenia samostatne a len pre svojho používateľa.

Vlastné roly je možné manuálne povoliť alebo zakázať. Nové roly sú predvolene vypnuté. Používatelia s vypnutou rolou pracujú, ako keby túto rolu nemali. To umožňuje napr. dočasne obmedziť danú rolu v jej činnostiach.

Všetky oprávnenia sú rozdelené medzi "Prístup na čítanie" a "Úplný prístup". Pridelenie Prístupu na čítanie roly umožňuje vidieť konkrétnu časť konzoly. Udelenie Úplného prístupu umožňuje Role vidieť a meniť konkrétnu časť konzoly.

Pridelenie úloh

Tu získate prehľad o všetkých používateľoch, ktorí majú rolu, a uvidíte, ktorú z nich majú. Môžete tu tiež priradiť rolu používateľom alebo celým skupinám:

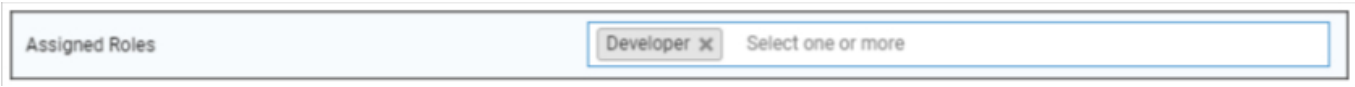


1. Vyberte, pre ktorú skupinu alebo používateľa chcete pridať alebo odstrániť roly. Môžete vybrať jedného používateľa alebo skupinu. Pri výbere skupiny sa vaša zmena dotkne všetkých používateľov v rámci tejto skupiny a všetkých používateľov podskupín vo vybranej skupine.
2. Vyberte úlohu, ktorú chcete pridať alebo odstrániť. Môžete vybrať jednu alebo viacero rolí.
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. Uložením proces ukončíte. Používatelia, ktorí predtým nemali žiadnu rolu a možnosť "Môže sa prihlásiť" bola zakázaná, automaticky dostanú e-mail s odkazom na nastavenie hesla.

Pod priradením hromadnej roly nájdete prehľad priradených rolí. Môžete tam tiež ručne zmeniť roly pre konkrétnych používateľov.

Pridelenie úlohy

Ak chcete priradiť rolu používateľovi, musíte prejsť do správy mobilných zariadení, kde nájdete strom skupín, používateľov a zariadení. Upravte používateľa a priraďte mu úlohu. Prípadne môžete použiť vyššie uvedený spôsob aj len pre jednotlivých používateľov.



Prístup k API

Prístup k API REST AppTec360

Rozhranie AppTec360 REST API vyžaduje autentifikačný token (kľúč API) a súkromný kľúč, ktoré je potrebné vygenerovať v konzole na správu.

Ak to chcete urobiť, prihláste sa do systému AppTec360 EMM a prejdite na

Všeobecné nastavenia → Prístup na základe rolí → Prístup k API a pridajte nový kľúč.

Musíte vybrať používateľa, ktorého oprávnenia sa budú vzťahovať na kľúč API.

Súkromný kľúč je možné prevziať len raz. Po začatí sťahovania sa kľúč vymaže a tlačidlo "Stiahnuť" zmizne.

Ak stratíte súkromný kľúč, musíte si vygenerovať nový kľúč API.

Všeobecné pravidlá

- Rozhranie REST API je k dispozícii pod základnou adresou URL:

/public/external/api

- Všetky požiadavky sa musia posielať prostredníctvom POST.
- Rozhranie REST API podporuje len požiadavky cez protokol HTTPS.
- Žiadosti musia obsahovať tieto hlavičky:

Názov hlavičky	Hodnota záhlavia	Popis
Typ obsahu	application/json	pevné
auth	123...xyz	Kľúč API z karty "Prístup k API"
podpis	Podpis v kóde Base64	Podpis užitočného zaťaženia vygenerovaného pomocou súkromný kľúč z karty "Prístup k rozhraniu API"

- Telo požiadavky musí byť objekt zakódovaný v tvare json, ktorý musí obsahovať nasledujúce hodnoty:

Pole	Príklad poľa Hodnota	Popis
api	v2/device/listdevices	Názov rozhrania API
čas	1529662725	Časová značka Unix (UTC) klientskeho počítača. Maximálny povolený časový rozdiel medzi klientom a serverom je 30 minút.

- V prípade úspechu API vráti požadované údaje (pozri nižšie uvedené dotazy) a stavový kód HTTP 200.
- Ak sa vyskytne chyba, stavový kód HTTP bude v závislosti od chyby 4xx až 5xx a objekt odpovede bude obsahovať pole s kľúčom "errors", ktoré obsahuje zoznam ľudsky čitateľných chybových správ.
- Ak pre zariadenie neexistujú žiadne zodpovedajúce údaje, vráti sa prázdne pole.
- Ak identifikátor zariadenia neexistuje, jeho návratové údaje budú nulové.

Príklad žiadosti

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]}}

Dotazy

Zoznam všetkých zariadení

Funkčnosť:
API URI: v2/device/listdevices
Povinné parametre: žiadne
Voliteľné parametre: žiadne

Príklad tela žiadosti

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

Príklad tela odpovede

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

Získanie zoznamu pozícií (GPS)

Funkčnosť:
URI API: v2/device/listposition
Povinné parametre: "ids" - pole ID zariadení
Voliteľné parametre: žiadne

Príklad tela žiadosti


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


Príklad tela odpovede


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

Získať mapu aktív

Funkcionalita:
Vráti zoznam všetkých uložených možných aktív, ktoré sa majú vyžiadať pomocou funkcie Get any asset data.
Na vyžiadanie údajov môžete použiť buď ľudsky čitateľný formulár, alebo značku aktíva.
URI API: v2/device/getassetmap
Povinné parametre: žiadne
Voliteľné parametre: žiadne

Príklad tela žiadosti


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


Príklad tela odpovede

Táto odpoveď bola kvôli zrozumiteľnosti skrátená.


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

Získanie akýchkoľvek údajov o aktívach

Funkčnosť:
URI API: v2/device/getassetdata
Povinné parametre:
"Voliteľné parametre:
"assetkeys" - kľúče údajov o aktívach, ktoré sa majú vrátiť. Ak nie sú uvedené, vrátia sa všetky dostupné údaje o aktívach
. Zoznam kľúčov aktív môžete získať pomocou funkcie Get asset map.

Príklad tela žiadosti


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


Príklad tela odpovede


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

Príklad kódu v jazyku 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)
```

Konfigurácia Apple

Certifikát APNS

Tu môžete nahrať certifikát APNS. Ten je potrebný na správu zariadení so systémami iOS a MacOS.

Poznámka: Certifikát APNS je platný len jeden rok. Pred uplynutím jeho platnosti je potrebné ho obnoviť. Proces obnovenia je totožný s procesom vytvorenia (pozri nižšie) a trvá len niekoľko krátkych minút.

Ak by ste si ho zabudli včas obnoviť, nemôžete vykonať zmeny v už zaregistrovaných zariadeniach. **a musíte všetky zariadenia zaregistrovať znova.**.

Krok 1

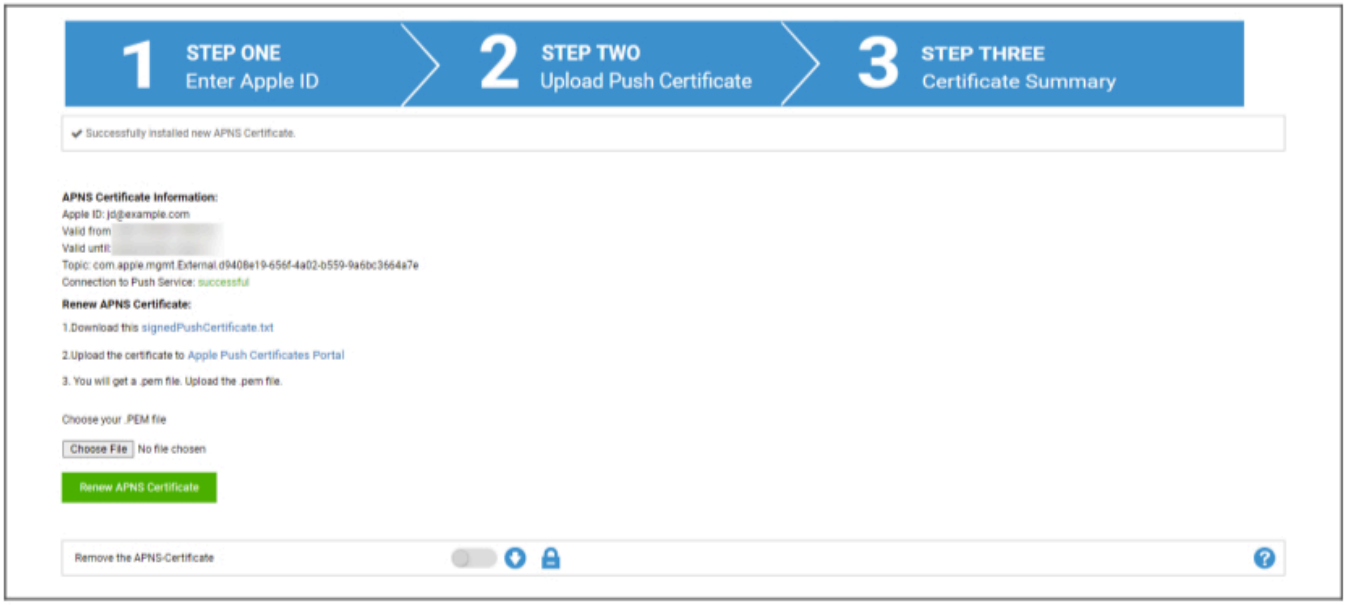
- Najprv zadajte svoje Apple ID, ktoré chcete použiť na vytvorenie certifikátu APNS.

Poznámka: Toto Apple ID sa používa len na vytvorenie certifikátu APNS. Toto Apple ID nemá nič spoločné so zariadeniami a zariadenia o ňom nebudú vedieť. Okrem toho potrebujete prístup k tomuto Apple ID aj na obnovenie certifikátu APNS. Preto sa odporúča použiť nejaké všeobecné Apple ID a zdokumentovať prihlasovacie údaje. Pred vypršaním platnosti certifikátu APNS sa na používanú poštovú adresu Apple ID odošle pripomienka.

- Ak chcete pokračovať, kliknite na "Ďalší krok".
- (voliteľné) Ak ste omylom vymazali predtým vymazaný certifikát APNS, môžete ho tiež obnoviť.

Krok 2

- Stiahnite si súbor signedPushCertificate.txt
- Prejdite na stránku https://identity.apple.com/pushcert/ a prihláste sa pomocou Apple ID z kroku 1
- Kliknite na "Vytvoriť certifikát"
- (nepovinné) zadajte poznámku. Môže to byť užitočné, ak spravujete viacero nájomcov, aby ste ich mohli ľahko identifikovať.
- Kliknutím na "Choose File" vyberte predtým stiahnutý súbor signedPushCertificate.txt
- Kliknite na "Nahrať".
- Teraz sa zobrazí potvrdenie, že ste vytvorili certifikát APNS.
- Kliknite na "Stiahnuť" a uložte ho.
- Vráťte sa do konzoly na správu.
- Kliknite na "Choose File" a vyberte certifikát APNS, ktorý chcete nahrať.
- Kliknite na "Nahrať"



Krok 3

Teraz ste úspešne nastavili certifikát APNS a môžete spravovať zariadenia so systémami iOS a MacOS.

V kroku 3 sa zobrazí prehľad aktuálne používaných certifikátov APNS.

Taktiež máte možnosť obnoviť certifikát APNS podľa krokov zobrazených na obrazovke. Nezabudnite ho obnoviť pred uplynutím jeho platnosti.

Pri obnovovaní certifikátu APNS nezabudnite, že sa musíte prihlásiť pomocou Apple ID uvedeného v kroku 3 a tiež obnoviť predtým použitý certifikát, a NIE vytvoriť nový. "Téma" certifikátu APNS sa zobrazí v kroku 3 a po kliknutí na "i" na portáli Apple Push Certificate. Ide o jedinečné ID, ktoré identifikuje certifikát. To vám pomôže identifikovať správny a obnoviť správny.

Keď sa zobrazí správa "Chyba: To znamená, že ste obnovili iný certifikát alebo ste vytvorili nový.

Ak chcete nahrať nový certifikát, napr. ak už nemáte prístup k predtým používanému Apple ID, musíte najprv odstrániť aktuálne nahraný certifikát.

Vymazanie certifikátu APNS znamená, že už nemôžete vykonávať zmeny v aktuálne zaregistrovaných zariadeniach, kým ich znova nezaregistrujete. Preto sa uistite, že ste na to pripravení, a odstráňte certifikát, len ak nie je iná možnosť.

Spravovaný prístup

Tu môžete povoliť registráciu používateľov pre zariadenia so systémom iOS a zdieľaný iPad pre zariadenia so systémom iOS.

Registrácia používateľov

"Zápis používateľa" umožňuje špeciálny režim pre zariadenia BYOD.

Pre každého používateľa je potrebné vytvoriť spravované Apple-ID na portáli Apple Business Portal.

Počas procesu registrácie budú používatelia požiadaní o svoje poverenia Apple-ID.

"Zápis používateľa" zaručuje maximálnu bezpečnosť používateľa, pretože umožňuje konfigurovať len obmedzený súbor nastavení a obmedzení zo strany MDM.

Spravovaná doména:

Doména použitá na mapovanie e-mailovej adresy používateľa na jeho spravované Apple-ID (musí byť vo formáte: "@appleid.company.com").Napr. john.doe@example.com bude mapovaná na john.doe@appleid.company.com.

V aplikácii Apple Business Manager si môžete pozrieť svoju spravovanú doménu

Spoločný iPad

Zdieľaný iPad je zariadenie DEP nakonfigurované so špeciálnym profilom DEP.

To umožňuje viacerým používateľom prihlásiť sa do zariadenia pomocou ich spravovaného Apple-ID.

Spravované Apple-ID musí byť vytvorené v Apple Business Portal alebo v Apple School Manager.

Používatelia, ktorí sa prihlásia do zdieľaného iPadu, sú požiadaní o svoje spravované poverenia Apple-ID.

Spravovaná doména:

Doména použitá na mapovanie e-mailovej adresy používateľa na jeho spravované Apple-ID (musí byť vo formáte: "@appleid.company.com").Napr. john.doe@example.com bude mapovaná na john.doe@appleid.company.com.

V aplikácii Apple Business Manager si môžete pozrieť svoju spravovanú doménu

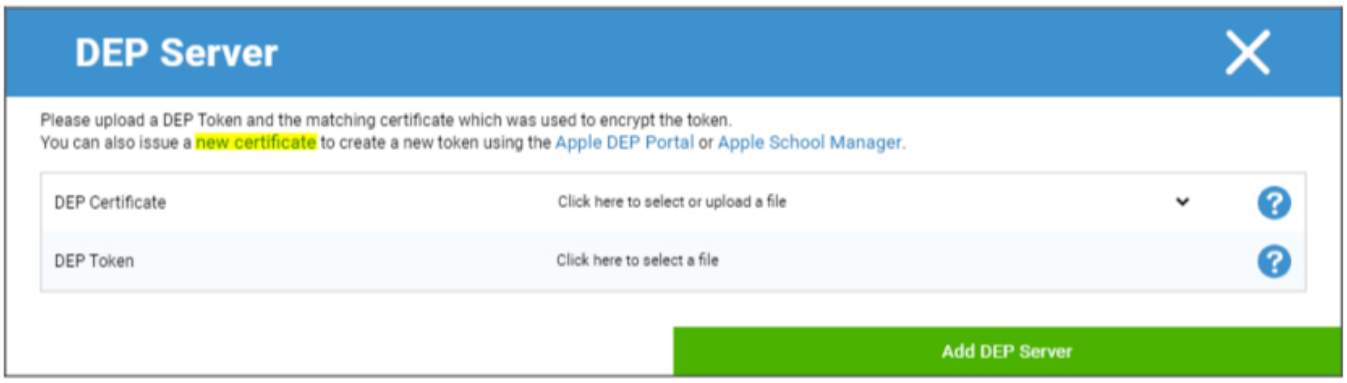
DEP

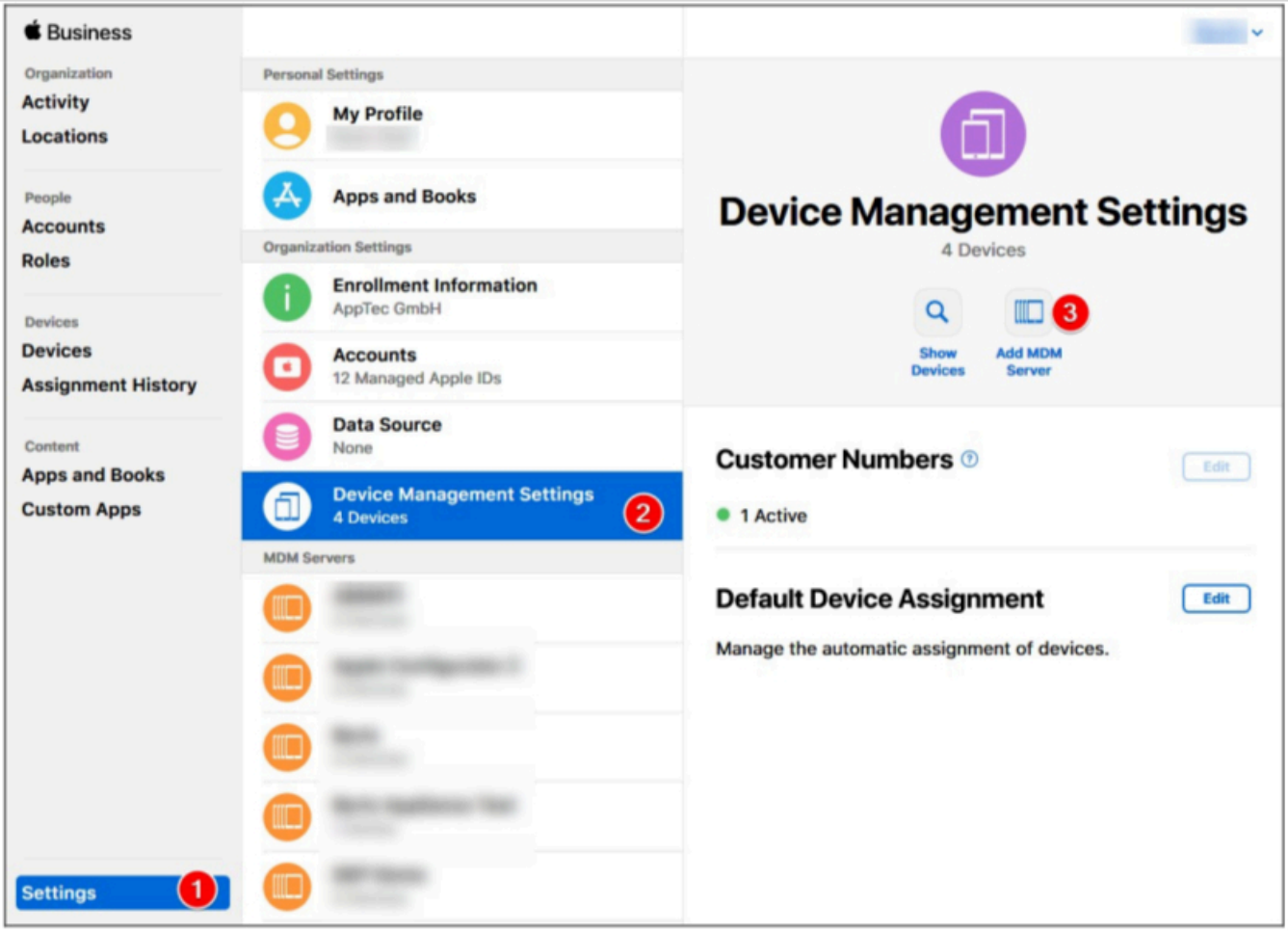
DEP (Device Enrollment Program) umožňuje jednoduchú registráciu zariadení do MDM. Pri používaní DEP sa zariadenia pri nastavovaní zariadenia automaticky pripoja k MDM. Môžete tiež preskočiť takmer všetky kroky nastavenia, ktoré sú v systéme iOS zvyčajne povinné.

Nezabudnite, že zariadenia musíte kúpiť od predajcu, ktorý podporuje DEP. Ďalšie informácie vám poskytne predajca alebo spoločnosť Apple.

Viac informácií o DEP: https: //www.apple.com/business/dep/

Kliknutím na "+" pridajte token DEP. Vo vyskakovacom okne kliknite na "nový certifikát" v texte (na obrázku nižšie označený žltou farbou). Tým sa vygeneruje a stiahne certifikát DEP. Potom prejdite do aplikácie Apple Business Manager(https://business.apple.com/) alebo Apple School Manager(https://school.apple.com/).

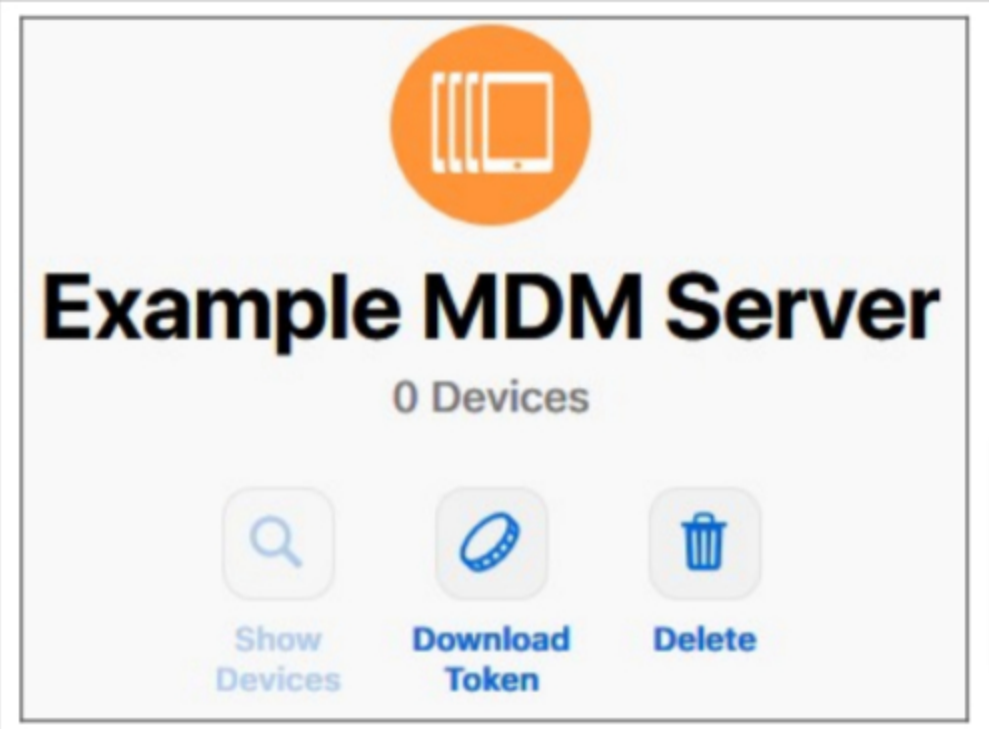




V aplikácii Apple Business Manager postupujte podľa pokynov na obrázku vyššie. Nastavenia → Nastavenia správy zariadení → Pridať server MDM.

Server nazvite ľubovoľne a nahrajte predtým stiahnutý certifikát DEP v časti Nastavenia servera MDM → Nahrať verejný kľúč a kliknite na "Uložiť".

Teraz sa zobrazí možnosť "Stiahnuť token". Kliknite na ňu a uložte ju. Token je platný len 1 rok. Stačí však opäť kliknúť na "Download Token" (Stiahnuť token), čím získate nový token, ktorého obnovenie je veľmi jednoduché.



Teraz sa môžete vrátiť do MDM, odkiaľ ste predtým prevzali certifikát DEP. Ak ste kartu nezatvorili, vyskakovacie okno pre pridanie DEP servera by malo byť stále otvorené a DEP certifikát by už mal byť vybraný. Teraz môžete nahrať svoj Token do poľa "DEP Token" a kliknúť na DEP Server.

V stĺpci "**Zariadenia**" uvidíte počet zariadení, ktoré sú priradené k tomuto serveru DEP. Zariadenia pridané k tomuto DEP serveru sa automaticky vytvoria v DEP poole v Mobile Management.

Kliknutím na toto číslo získate prehľad o všetkých zariadeniach DEP a ich stave.

Poznámka: V závislosti od pracovného postupu alebo konfigurácie v Business Manager môže byť potrebné tieto zariadenia priradiť k DEP Serveru manuálne. V aplikácii Apple Business Manager môžete pre nové zariadenia nastaviť aj predvolený DEP Server.

V stĺpci "**Profily**" sa zobrazí počet profilov DEP, ktoré máte. Kliknutím na toto číslo môžete tiež zobraziť podrobnosti o svojich DEP profiloch a môžete tu vymazať staré/nepoužívané profily. V súčasnosti ich nie je možné zmeniť. Ak chcete vykonať zmenu, musíte si vytvoriť nový.

V stĺpci "**Posledná synchronizácia**" môžete manuálne synchronizovať server DEP (napr. ak ste práve pridali nové zariadenie do DEP) a vidieť dátum poslednej úspešnej synchronizácie.

V stĺpci "**Automatický profil**" môžete nastaviť profil DEP ako automatický predvolený. Tento profil sa automaticky priradí novým zariadeniam. Ak nenastavíte automatický profil, musíte profil novým zariadeniam priradiť zakaždým ručne.

V stĺpci "**Pridať profil**" môžete pridať nový profil DEP. Zariadenie ho dostane na začiatku nastavenia zariadenia. Profil DEP definuje spôsob nastavenia zariadenia a určuje, ktoré kroky nastavenia budú preskočené.

Poznámka: po zaregistrovaní zariadenia je možné tieto nastavenia zmeniť len vykonaním obnovenia výrobných nastavení a zaregistrovaním zariadenia s novým profilom. Týka sa to najmä položiek "**Odstrániteľné**" a "**Povoliť párovanie**". V prípade "**Allow pairing" (Povoliť párovanie)**sa odporúča zapnúť túto funkciu, pretože ju možno vypnúť prostredníctvom obmedzení MDM, ale nemožno ju znova zapnúť, ak je vypnutá v profile DEP.

V stĺpci "**Upraviť**" môžete nahrať nový token, napr. pri obnove tokenu.

Konfigurátor a adresa URL

URL adresy pre zápis do bazéna

Tu môžete vytvoriť adresu URL pre zápis a QR kód pre zápis, ktorý je platný po určitú dobu zápisu a do určitého dátumu. To vám umožní zaregistrovať viacero zariadení, ktoré stačí zaregistrovať pomocou jedného odkazu alebo QR kódu.

Zariadenia zaregistrované pomocou tejto adresy URL alebo kódu QR budú v skupine v správe mobilných zariadení a následne ich musíte manuálne priradiť k skupine alebo používateľovi.

Poznámka: toto sa týka len manuálneho zápisu. Túto adresu URL nepoužívajte, ak registrujete zariadenia prostredníctvom aplikácie Apple Configurator

Profil MDM – Konfigurátor Apple

Tu môžete získať adresu URL, ktorú potrebujete pri registrácii zariadení prostredníctvom aplikácie Apple Configurator. Pri príprave zariadení pomocou nástroja Apple Configurator môžete v tom istom procese pridať zariadenia do MDM. Aplikácia Apple Configurator na to vyžaduje túto adresu URL.

Zariadenia pridané prostredníctvom nástroja Apple Configurator budú v skupine v správe mobilných zariadení a následne ich musíte manuálne priradiť skupine alebo používateľovi.

Nájdete tu aj súbor .mobileconfig, ktorý môžete použiť na registráciu zariadení prostredníctvom aplikácie Apple Configurator. Každopádne sa odporúča použiť túto adresu URL.

Konfigurácia systému Android

Konfigurácia systému Android

Odinštalovanie ochrany	Ak je táto funkcia aktivovaná, používateľ nemôže deaktivovať správcu zariadenia bez zadania hesla nastaveného správcom MDM. Heslo sa nastavuje počas registrácie, takže zariadenia sa musia opätovne zaregistrovať, aby sa heslo aktualizovalo. Existujú dve možnosti odstránenia správcov zariadenia: 1. Ručne v zariadení ◦ Otvorenie aplikácie EMM v zariadení ◦ Prepnutie na kartu Stav ◦ Ťuknite na položku "Odinštalovať ochranu". ◦ Zadanie hesla Správne heslo môžete získať pomocou funkcie Revision (Revízia) z položky "Password History" (História hesiel) v konzole. ◦ Prejdite nadol a ťuknite na novo pridaný bod, "Ťuknutím odinštalujete aplikáciu AppTec360 MDM" (na vykonanie tejto úlohy máte 20 sekúnd) ◦ Potvrďte dialóg "Odinštalovať aplikáciu AppTec360 MDM" tlačidlom "ok". Tým sa zariadenie odhlási z konzoly. ◦ Ak chcete odstrániť aplikáciu zo zariadenia, potvrďte dialóg "AppTec360 MDM bude odinštalovaný" pomocou "UNINSTALL". 2. automatický (konzola) ◦ Vyberte zariadenie v konzole ◦ Kliknite na modrú ikonu ozubeného kolesa a vyberte položku "Enterprise Wipe". Poznámka: K dispozícii len v systéme Android 4.x a nižších verziách alebo v zariadeniach s rozhraním KNOX API (zariadenia Samsung).

Odinštalovanie hesla (revízia x)	Stanovené heslo, pomocou ktorého môže používateľ odstrániť správcu zariadenia Revízia x = počítadlo, ako často už bolo heslo zmenené Je dôležité, ktoré heslo používateľ potrebuje, pretože je možné, že zariadenie ešte nekomunikovalo so serverom AppTec360, a preto ešte nebolo odoslané najnovšie heslo.
História hesiel	Po kliknutí na modré tlačidlo ("Zobraziť históriu") si môžete prezrieť predtým vytvorené heslá.
Rozšírená ochrana pred odinštalovaním	Táto možnosť ponúka ochranu pred zariadeniami, ktoré nie sú v systéme SAFE. Pokiaľ je toto nastavenie aktivované, nie je možné správcu zariadenia jednoducho deaktivovať.
Vyzvať používateľa, aby odinštaloval zablokované aplikácie?	Ak je to možné, zablokované aplikácie sa nielen zablokujú, ale aj automaticky odinštalujú. Ak nie je možné zablokované Aplikácie automaticky odinštalovať, používateľ bude vyzvaný, aby ich odinštaloval.
Blokovanie aplikácií inteligentného systému	Ak je zapnutá biela listina, klient Android MDM zablokuje všetky aplikácie nainštalované používateľom. Ak toto nastavenie povolíte, zablokujete všetky spustiteľné systémové aplikácie v režime Whitelisting.

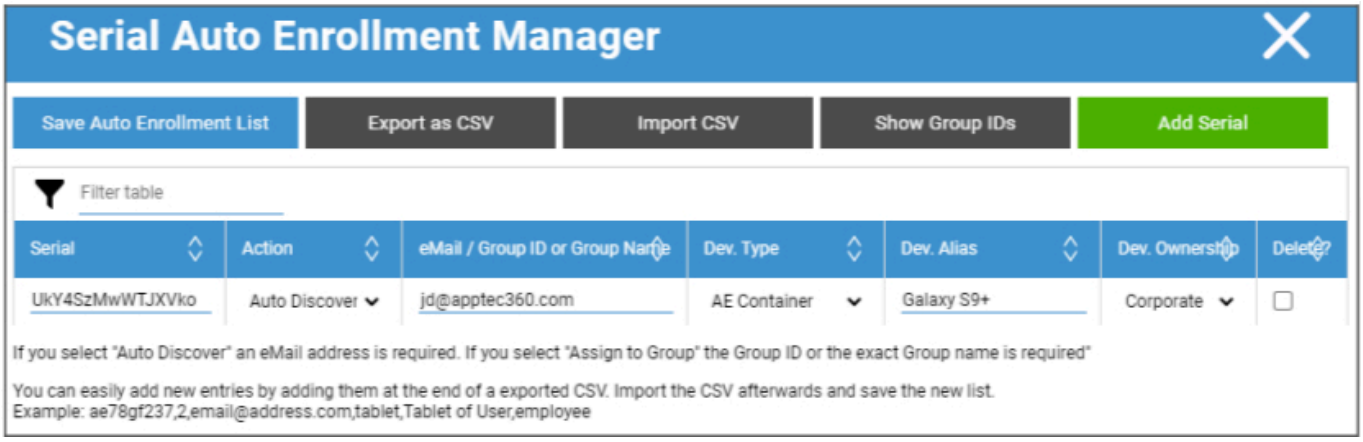
Automatický zápis

Tu môžete povoliť funkciu automatického zápisu, aby sa vaše zariadenia zaregistrovali automaticky po otvorení klienta AppTec360 MDM na zariadení.

Dôležité: Táto metóda zápisu je zastaraná a v systéme Android 10 alebo novšom už nefunguje. Každopádne pri používaní systému Android 7 alebo vyššieho by ste mali zariadenia zaregistrovať ako plne spravované zariadenia Android Enterprise. Ak chcete používať kontajner Android Enterprise BYOD a používate systém Android 10 alebo vyšší, musíte zariadenie zaregistrovať ručne prostredníctvom poverovacích údajov, kódu QR alebo SMS. Každopádne zoznam automatického zápisu sa stále používa na automatizáciu procesu zápisu napr. pre AE Enrollment, Knox Enrollment atď.

Každopádne, zoznam automatického zápisu sa stále používa na automatizáciu procesu zápisu, napr. pri zápise AE, zápise Knox atď.

Kliknutím na položku "Serial Manager" alebo "IMEI Manager" môžete pridať sériové alebo IMEI zariadenia. Nie je potrebné, aby ste pre svoje zariadenia urobili obidve, stačí len jedno.



Akcia definuje, či budú zariadenia zapísané do fondu, používateľa alebo skupiny.

Môžete tiež exportovať a importovať súbor .csv a filtrovať záznamy podľa kľúčových slov.

Android Enterprise

Tu môžete nastaviť systém Android Enterprise. Je to potrebné na používanie všetkých funkcií Android Enterprise.

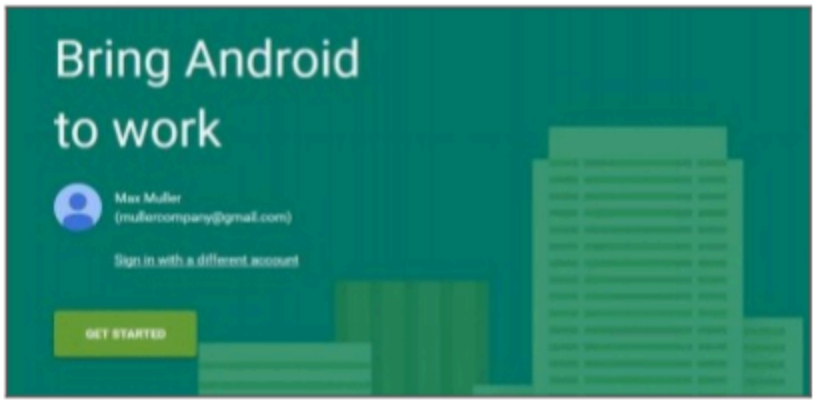
Prvá metóda: Podnikový účet Android (účet Google)

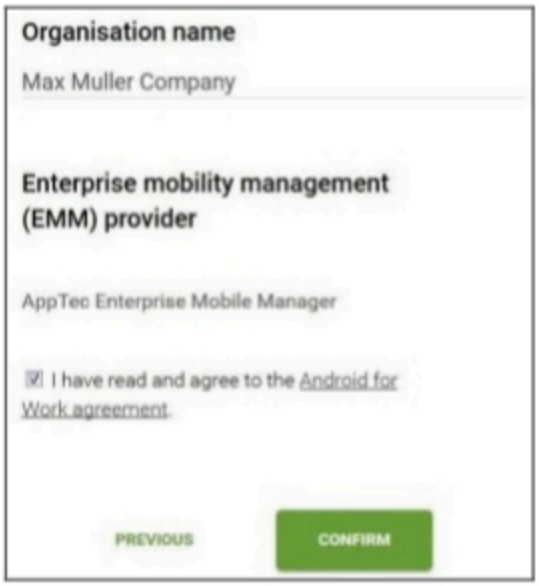
Najprv stlačte tlačidlo "Prepare Setup" (Pripraviť nastavenie) a po chvíli by sa malo objaviť tlačidlo "Start Setup" (Spustiť nastavenie).

Tým sa dostanete na stránku nastavenia systému Android Enterprise spoločnosti Google.

Ak ešte nie ste prihlásení, prihláste sa pomocou konta Google, ktoré chcete používať, a stlačte tlačidlo "Začať".

Teraz môžete zadať názov svojej spoločnosti. Potom začiarknite políčko a stlačte tlačidlo "Potvrdiť".





V poslednom kroku môžete dokončiť registráciu a mali by ste sa vrátiť do konzoly. Ak všetko fungovalo, malo by to vyzerať takto:

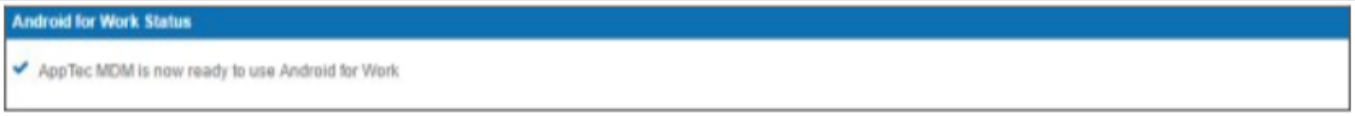
Teraz môžete začať konfigurovať kontajner Android Enterprise Container.

Druhá metóda: Účet G-Suite

Stlačte tlačidlo "Použiť G-Suite" a prihláste sa do svojho konta správcu Google. Tam prejdite do časti "Zabezpečenie" -> "Zobraziť viac" -> "Spravovať poskytovateľa EMM pre Android" a vygenerujte token. Poznámka: Ak vo svojom účte G-Suite nevidíte nastavenia Android Enterprise Settings, musíte prejsť na "Získať ďalšie aplikácie a služby" a pridať správu zariadení Android. Teraz zadajte Token a svoju primárnu doménu v našej konzole a kliknite na "Uložiť zmeny". Keď ste hotoví, kliknite na "Použiť účet Android Enterprise".

Teraz by sa malo zobraziť tlačidlo "Vytvoriť servisné konto". Kliknite naň. Tento proces môže trvať niekoľko okamihov.

Ak všetko fungovalo, malo by to vyzerať takto:



Teraz môžete začať konfigurovať kontajner Android Enterprise Container.

Ochrana pred obnovením továrenského nastavenia

Pomocou ochrany pred obnovením továrenských nastavení môžete zariadenie zviazať s účtom Google podľa vlastného výberu, čím sa zruší aj akékoľvek existujúce viazanie na účet Google. Ak chcete používať ochranu pred obnovením výrobných nastavení, musíte ju najprv nastaviť tu a potom ju aktivovať vo svojich profiloch.

Ak chcete nastaviť ochranu pred obnovením výrobných nastavení, kliknite na položku "FRP Setup" a postupujte podľa pokynov na obrazovke.

POZNÁMKA: Pozorne si prečítajte a vykonajte tieto kroky. Odporúčame to vykonať v novom okne prehliadača inkognito, aby ste sa vyhli automatickému prihláseniu do nesprávneho konta Google. Ak by ste zadali nesprávne ID alebo by ste stratili prístup k používanému kontu Google, môžete sa úplne zablokovať zo zariadenia!

Zápis do AE

Tu môžete aktivovať Android Enterprise Ernollment. Použitím tejto metódy zapíšete svoje zariadenia do režimu vlastníka zariadenia Android Enterprise. V tomto režime budete mať plnú kontrolu nad zariadením.

Povolenie zápisu do AE	Aktivuje AE Enrollment Caution: Ak zakážete funkciu AE Enrollment, existujúce kódy QR a už nakonfigurované zariadenia NFC programátora prestanú fungovať. Ak AE Enrollment opäť povolíte, budete musieť znovu odoslať konfigurácie NFC push / vygenerovať nové QR kódy.
Povolenie automatického objavovania	Keď sa zariadenie zaregistruje prostredníctvom funkcie "AE Enrollment", systém sa ho pokúsi priradiť k používateľovi na základe informácií nastavených v zozname bielych čísiel ("General Settings" > "Android Configuration" > "Auto Enrollment").
Blokovanie neznámych zariadení	Zapísať sa môžu len zariadenia, ktoré boli zaradené do bielej listiny sériových zariadení / IMEI ("Všeobecné nastavenia" > "Konfigurácia systému Android" > "Automatický zápis").

Poznámka k metóde 1 a 2: "Uvítacia obrazovka" sa vzťahuje na prvú obrazovku, ktorá sa zobrazí po obnovení výrobných nastavení. Tá môže vyzerať rôzne v závislosti od verzie systému Android a/alebo modelu zariadenia, ktoré používate.

Metóda 1: Zápis kódu QR

(vyžaduje systém Android 7.0 alebo vyšší) Ak používate systém Android 7 alebo vyšší, odporúčame vždy použiť túto metódu.

1. Obnovenie továrenského nastavenia zariadenia
2. Vygenerujte kód QR pre zápis pomocou jednej z nasledujúcich dvoch metód:
    - Kliknite v časti "Všeobecné nastavenia -> Konfigurácia systému Android -> Zápis do AE" na položku "Generovať kód QR". Vyberte, či chcete preskočiť šifrovanie úložiska a/alebo či sa majú odstrániť všetky systémové aplikácie.
    - (prípadne) Vyberte existujúce zariadenie. V "Prehľade zariadení" kliknite na zobrazený QR kód. Vyberte, či chcete preskočiť šifrovanie úložiska a/alebo či sa majú odstrániť všetky systémové aplikácie.
3. Teraz ťuknite 6-krát na uvítaciu obrazovku zariadenia. Tým by sa mal spustiť režim zápisu QR.
4. Teraz sa pripojte k bezdrôtovej sieti a krátko počkajte, kým sa nainštaluje čítačka QR kódov.
5. Teraz naskenujte kód QR
6. To je všetko. Vaše zariadenie je teraz zaregistrované v režime zariadenia Android Enterprise.
    - a. Ak ste použili QR kód vo "Všeobecných nastaveniach", môžete nájsť svoje zariadenie v "Bazéne -> Zariadenia vlastníka AE". (Tip: Je možné, že budete musieť znovu načítať

stránku, aby ste videli zariadenia). Ak ste zaškrtli "Zapnúť automatické vyhľadávanie", nájdete ho v rámci používateľa automatického vyhľadávania.

- Ak ste použili QR kód existujúceho profilu zariadenia, zariadenie bude zaregistrované do tohto profilu.

Metóda 2: Registrácia NFC

(vyžaduje NFC a systém Android 6.0 alebo vyšší)

Príprava: Zadajte svoje údaje o WiFi v časti "Všeobecné nastavenia -> Konfigurácia Androidu -> Zápis do AE -> Údaje pre zabezpečenie NFC". Teraz pomocou položky "NFC Device" vyhľadajte zariadenie, ktoré sa stane programátorom. Toto zariadenie sa bude používať na odosielanie informácií o zápise do ostatných zariadení prostredníctvom NFC.

1. Obnovenie továrenského nastavenia zariadenia
2. Otvorte aplikáciu na párovanie NFC z AppTec360 na svojom programátore
3. Vyberte, či chcete vynechať šifrovanie úložiska a/alebo či sa majú odstrániť všetky systémové aplikácie.
4. Držte obe zariadenia chrbtom k sebe
5. Teraz by mal byť Android Enterprise Enrollment výrazne
6. Teraz nájdete svoje zariadenie v konzole
    - a. Ak ste v bazéne nenakonfigurovali funkciu Auto Discover
    - b. V rámci používateľa, ktorého ste nakonfigurovali pre funkciu Auto Discover
    - c. Tip: Je možné, že budete musieť znovu načítať stránku, aby ste videli zariadenia.

Metóda 3: Konto Google

(vyžaduje systém Android 5.1 alebo vyšší)

(Poznámka: Ak používate túto metódu, zariadenie nebude automaticky zaregistrované. Namiesto toho ho musíte zaregistrovať ručne alebo proces zautomatizovať pomocou funkcie Automatická registrácia.)

1. Obnovenie továrenského nastavenia zariadenia
2. Prejdite krokmi nastavenia, kým sa nebudete môcť prihlásiť pomocou konta Google
3. Ako používateľské meno/mail zadajte "afw#apptec"
4. Ťuknite na položku "Next".
5. Vaše zariadenie je teraz zariadenie so systémom Android Enterprise

Zápis do spoločnosti KNOX

Tu môžete aktivovať registráciu KNOX a nájsť informácie potrebné na vytvorenie profilu registrácie KNOX na portáli nasadenia KNOX. Na konfiguráciu a používanie potrebujete konto na portáli KNOX Deployment Portal.

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

Povolenie zápisu do systému KNOX	Aktivuje funkciu KNOX Enrollment. Upozornenie: Ak zakážete registráciu KNOX, existujúce profily MDM prestanú fungovať. Ak opäť povolíte funkciu KNOX Enrollment, budete musieť aktualizovať pole "Vlastné údaje JSON" svojho profilu MDM.
Povolenie automatického objavovania	Keď sa zariadenie zaregistruje prostredníctvom funkcie "KNOX Enrollment", systém sa ho pokúsi priradiť k používateľovi na základe informácií nastavených v zozname bielych čísiel ("Všeobecné nastavenia" > "Konfigurácia systému Android" > "Automatická registrácia").

1. Prihláste sa na portál Samsung KNOX Mobile Enrollment Portal https://eukme.samsungknox.com/itadmin
2. Prejdite na "Profily MDM"
3. Kliknite na "Pridať"
4. Vyberte možnosť "Server URI sa pre moje MDM nevyžaduje" a kliknite na "Ďalej".
5. Teraz vytvorte profil s informáciami zobrazenými v konzole pre správu

Tento profil registrácie KNOX môže teraz do zariadenia nainštalovať priamo spoločnosť Samsung, ak zariadenie získate priamo od spoločnosti Samsung.

Prípadne si môžete stiahnuť aplikáciu KNOX Deployment App, prihlásiť sa pomocou účtu KNOX Deployment Account a poslať profil KNOX Enrollment Profile prostredníctvom NFC do iných zariadení.

Ak má zariadenie nainštalovaný profil registrácie KNOX, stiahne si našu aplikáciu a zaregistruje zariadenie, ak má funkčné internetové pripojenie.

Registráciu zariadení prostredníctvom funkcie KNOX Enrollment nájdete v ponuke "Pool -> KNOX Enrollment" alebo v rámci používateľa, ktorého ste zadali v službe Auto Discover.

Zero-Touch

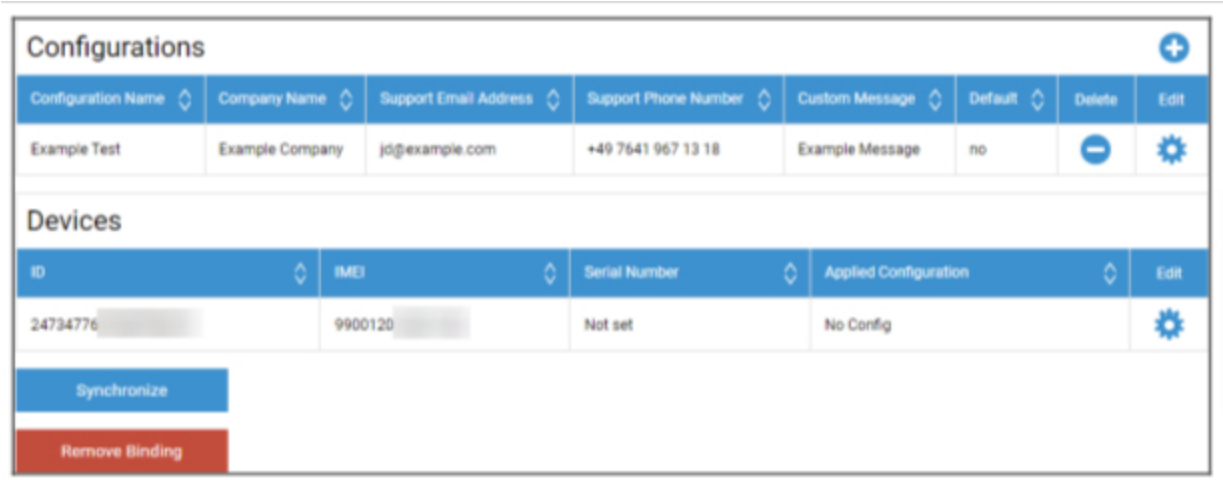
Pomocou funkcie Zero-Touch môžete jednoducho zaregistrovať svoje zariadenia bez toho, aby ste sa ich museli dotknúť alebo čokoľvek konfigurovať na samotnom zariadení. Stačí ho zapnúť, pokračovať v konfigurácii ako zvyčajne a zariadenie dostane všetky informácie o nastavení a pripojení k MDM úplne automaticky.

Ak chcete používať funkciu Zero-Touch, musíte si zakúpiť zariadenia od predajcu, ktorý podporuje funkciu Zero-Touch. Ten istý predajca pre vás vytvorí aj konto na portáli Zero-Touch. Ak chcete získať ďalšie informácie o postupe alebo ak máte problémy pri prístupe na portál Zero-Touch, obráťte sa na svojho predajcu.

Kliknutím na "Start Setup" (Spustiť nastavenie) spustite nastavenie. Budete presmerovaní na prihlasovaciu stránku, kde musíte vybrať svoje konto Google, ktoré má prístup k portálu Zero-Touch.

POZNÁMKA: Je možné vybrať ľubovoľné konto. Preto sa uistite, že ste v tomto kroku vybrali správne konto. Ak nevidíte svoje zariadenia/konfigurácie, vysoko pravdepodobne ste použili nesprávne Konto.

Po dokončení prihlásenia to bude vyzerať takto:



Kliknutím na tlačidlo "+" pridajte konfiguráciu a vyplňte polia tak, ako sú zobrazené na obrazovke. Ak konfiguráciu povolíte ako predvolenú konfiguráciu, bude automaticky priradená novým zariadeniam. Vytvorenie alebo nastavenie predvolenej konfigurácie ju nepriradí k už existujúcim zariadeniam.

Ak zariadenie nemá priradenú žiadnu konfiguráciu, nastaví sa ako bežné zariadenie a nepripojí sa k MDM. Preto sa uistite, že vaše zariadenia majú priradenú Konfiguráciu.

Po pripojení konta, keď sú vaše zariadenia viditeľné a máte k nim priradenú konfiguráciu, môžete začať nastavovať zariadenia.

Zariadenia môžete pridať do zoznamu automatického zápisu, aby sa automaticky zapísali do určenej skupiny alebo používateľa. Ak ste v zozname Automatický zápis nič nenakonfigurovali, zariadenia budú zapísané do skupiny.

Konfigurácia systému Windows

Konfigurácia systému Windows

Tu máte možnosť povoliť nasledujúce konfigurácie v počítači so systémom Windows 10:

Okamžité pripojenie DM	
Počiatočný čas opakovania	nadviaže prvý pokus o pripojenie k zariadeniu, táto hodnota sa exponenciálne zvyšuje
Opakovanie pripojenia	Udáva, koľko pokusov o pripojenie má klient DM vykonať počas chyby pripojenia.
Maximálny čas spánku	Udáva maximálny čas spánku po chybe pripojenia
Prvé opakovanie synchronizácie	Intervaly, v ktorých má zariadenie komunikovať so serverom po prvom spojení
Interval prvého opakovania	Vzťahuje sa na "Prvé opakovanie synchronizácie" Tu sú časy uvedené v minútach Napríklad v položke "First Sync Retries" (Prvé opakovanie synchronizácie) je uvedená hodnota "2" a v položke "First Retry Interval" (Interval prvého opakovania) je uvedená hodnota "4 Minutes" (4 minúty), čím zariadenie komunikuje 2-krát každé 4 minúty po prvom spojení.
Druhé opakovanie synchronizácie	Intervaly, v ktorých má zariadenie komunikovať so serverom po dokončení "Prvých opakovaných pokusov o synchronizáciu"
Druhý interval opakovania	Rovnaký princíp ako v prípade "First Retry Interval" - len tu platí pre "Second Sync Retries".
Pravidelné opakovanie synchronizácie	Intervaly, ako často má zariadenie v budúcnosti komunikovať so serverom Predvolené nastavenie: "Nekonečné" Odporúčame túto hodnotu nemeniť, pretože ak zadáte "10", zariadenie bude so serverom komunikovať 10x a potom prestane Preto sa komunikácia so serverom AppTec360 preruší!
Pravidelný interval opakovania	Rovnaký princíp ako v prípade "First/Second Retry Interval" - len tu platí nastavenie pre budúcnosť
Pravidelný interval opakovania	Rovnaký princíp ako v prípade "First/Second Retry Interval" - len tu platí nastavenie pre budúcnosť

ContentBox

Konfigurácia

Tu môžete nakonfigurovať pole ContentBox. Do ContentBoxu môžete umiestniť súbory pre skupiny, ku ktorým môžete pristupovať pomocou aplikácie ContentBox v zariadení.

Povolenie okna ContentBox	Povoľte ContentBox. Ak ContentBox nepoužívate, jeho vypnutím môžete ušetriť prostriedky na počítačoch OnPremise.
Použitie externej inštalácie ContentBox	ContentBox je možné prevádzkovať aj pomocou vlastného Nextcloudu.
ADRESA URL	Úplná adresa URL subjektu Nextcloud
Používateľ koreňového systému	Koreňový používateľ účtu Nextcloud
Heslo koreňového systému	Koreňové heslo konta Nextcloud
Predvolené oprávnenia priečinkov skupiny	Predvolené skupinové oprávnenia priečinkov, ktoré možno individuálne upraviť podľa skupiny (v správe mobilných zariadení)
Zdieľanie priečinka skupiny s podskupinami	Ak je aktívna, každá podskupina môže čítať všetky priečinky hlavnej skupiny, možno ju tiež individuálne nakonfigurovať pre každú skupinu (správa mobilných zariadení).
Oprávnenia pre podskupiny	Oprávnenia pre podskupiny možno individuálne konfigurovať pre každú skupinu (správa mobilných zariadení)
Povoľte zdieľanie	Umožňuje používateľovi zdieľať obsah prostredníctvom odkazov, môže byť individuálne nakonfigurovaný pre každú skupinu
Maximálna veľkosť nahraného súboru v MB	Maximálna veľkosť súboru Štandard: 512 MB Maximálna konfigurácia: 2048
Splnomocnenia WebDAV	
Adresa URL WebDAV	ContentBox môžete otvoriť aj pomocou WebDAV. V žiadnom prípade neodstraňujte nasledujúce priečinky: /apptecgroups /apptecgroups/AppTecGroup-X
Používateľ koreňového systému	Názov koreňových používateľov

Heslo	Heslo koreňových používateľov

Synchronizácia s rámčekom ContentBox sa uskutočňuje automaticky. Môžete však vykonať manuálnu synchronizáciu pomocou funkcie "Synchronizovať ContentBox".

Okrem toho tu môžete aktivovať/deaktivovať ContentBox na každom jednotlivom zariadení.

Toto je relevantné len vtedy, ak ste si ContentBox dodatočne nelicencovali, potom máte stále prístup k 25 zariadeniam, s ktorými môžete ContentBox testovať - tu to môžete aktivovať pre príslušné zariadenia.

Konfigurácia LDAP

Prehľad LDAP

Tu môžete vytvoriť spojenie so službou Active Directory prostredníctvom LDAP a hromadne importovať používateľov a skupiny. Synchronizácia sa musí vykonať ručne. Môžete nakonfigurovať viacero pripojení LDAP k rôznym systémom alebo s rôznymi konfiguráciami/filtrami.

Názov servera	Zobrazovaný názov servera
Typ	V súčasnosti sú podporované len adresáre Active Directories, ktoré podporujú LDAP
Doména LDAP	Primárna doména LDAP (napr. example.com)
Hostiteľ LDAP	Potrebné len vtedy, ak hostiteľ LDAP nie je dosiahnuteľný pod danou doménou LDAP.
Prístav	Ak chcete použiť štandardný port (389 alebo 636 pre SSL), nechajte prázdny.
Používateľské meno	Napr. CN=John,OU=Users,DC=EXAMPLE,DC=COM Poznámka: Väčšina systémov vyžaduje meno používateľa v tomto formáte a neakceptuje "John" ako meno používateľa.
Heslo	
Potvrdenie hesla	
Zabezpečenie pripojenia	Poznámka: pri použití protokolu SSL alebo TLS sa skontroluje certifikát služby Active Directory. Ak je podpísaný vlastným podpisom, musíte pridať koreňovú certifikačnú autoritu do úložiska dôveryhodnosti počítača OnPremise. Ak ste v Cloude, Active Directory musí poskytnúť dôveryhodný certifikát, inak bude pripojenie fungovať len bez šifrovania
Automatická synchronizácia.	Povolí automatickú synchronizáciu adresára LDAP v časovom intervale určenom vo všeobecných nastaveniach LDAP.
Základná DN	Ak nechcete synchronizovať celý adresár, môžete tu zadať OU.Napr. OU=AndroidUsers,OU=Users,DC=EXAMPLE,DC=COM
Člen	Všetci importovaní používatelia budú pridaní do vybranej skupiny
Iba aktivovaní používatelia?	Ak je zapnutý, bude sa brať do úvahy atribút userAccountControl, používatelia bez tohto atribútu nebudú importovaní.
Filter LDAP	Pomocou filtra LDAP môžete filtrovať, ktorí používatelia sa importujú
Filter regexu	Na filtrovanie používateľov, ktorí sa importujú, môžete použiť filter Regex

Testovacie pripojenie	Testuje pripojenie pri ukladaní konfigurácie
Obnovenie adresárovej štruktúry pri synchronizácii?	Ak je to pravda, všetky položky LDAP sa presunú späť na svoje pôvodné miesto v strome LDAP. Odporúča sa zapnúť.
Opätovný import odstránených používateľov a skupín?	Ak je táto funkcia povolená, vymazaní používatelia a skupiny sa znovu vytvoria. Odporúča sa zapnúť.
Synchronizácia vymazaní?	Ak je táto možnosť povolená, skupiny a používatelia sa odstránia, keď sa odstránia na serveri LDAP. Vymažú sa aj zariadenia vymazaných používateľov.

Pod zoznamom vašich konfigurácií LDAP môžete definovať obdobie, v ktorom sa systém automaticky synchronizuje. Na automatickú synchronizáciu sa používajú len tie Konfigurácie LDAP, ktoré majú aktivovanú príslušnú možnosť.

Správa aplikácií

Vnútorná aplikácia DB

Android

Tu môžete nahrať aplikácie pre Android, ktoré vaša spoločnosť vyvinula, a neskôr ich distribuovať v správe mobilných zariadení v profiloch zariadení alebo skupín.

Upozorňujeme, že týmto spôsobom odporúčame distribuovať iba aplikácie, ktoré nie sú dostupné v obchode Google Play.

Kliknutím na "+" nahrajte súbor APK aplikácie, ktorú chcete nahrať. V súčasnosti je podporovaný iba formát APK.

Limit odosielania na zariadeniach OnPremise môžete zvýšiť v kroku 3 konfigurácie zariadenia. Ak chcete zvýšiť limit nahrávania v cloude, obráťte sa na podporu, ktorá vám poskytne ďalšie informácie.

Upozorňujeme, že súbory APK sú zvyčajne o niečo menšie ako ich obsah. Je možné, že sa odoslanie z tohto dôvodu nepodarí, pretože APK sa v procese rozbalí. Napr. je možné, že 95 MB APK zlyhá pri 100 MB limite na odosielanie. V takom prípade zvýšte limit nahrávania, ako je uvedené vyššie.

Odporúčame tiež najprv ručne presunúť súbor APK do jedného testovacieho zariadenia (napr. cez USB) a skúsiť ho nainštalovať ručne pomocou aplikácie Súbory v zariadení. Ak to z nejakého dôvodu nebude fungovať, nepodarí sa to ani cez MDM.

Cieľová aktualizácia

Pomocou funkcie "Update Target" môžete vybrať, ktorá verzia aplikácie sa má nainštalovať alebo na ktorú verziu sa má aplikácia aktualizovať, ak ste pre aplikáciu aktivovali funkciu "Keep up to date".

Ak ste nevybrali cieľ aktualizácie, použije sa najvyššia verzia.

Majte na pamäti, že systém Android nemôže znížiť úroveň aplikácií. Tiež si uvedomte, že "Kód verzie" určuje, či je verzia vyššia, nižšia alebo rovnaká. Pri vytváraní aktualizácie sa preto uistite, že ste túto verziu v aplikácii správne zvýšili.

iOS

Tu môžete nahrať aplikácie pre iOS, ktoré ste vyvinuli, a neskôr ich distribuovať v mobilnej správe v profile zariadenia alebo skupiny.

Kliknutím na "+" nahrajte IPA aplikácie, ktorú chcete nahrať. Zatiaľ je podporovaný len formát IPA.

Limit odosielania na zariadeniach OnPremise môžete zvýšiť v kroku 3 konfigurácie zariadenia. Ak chcete zvýšiť limit nahrávania v cloude, obráťte sa na podporu, ktorá vám poskytne ďalšie informácie.

Cieľová aktualizácia

Pomocou funkcie "Update Target" môžete vybrať, ktorá verzia aplikácie sa má nainštalovať alebo na ktorú verziu sa má aplikácia aktualizovať, ak ste pre aplikáciu aktivovali funkciu "Keep up to date".

Ak ste nevybrali cieľ aktualizácie, použije sa najvyššia verzia.

MacOS

Tu môžete nahrať aplikácie pre MacOS, ktoré ste vyvinuli, a neskôr ich distribuovať v mobilnej správe v profile zariadenia alebo skupiny.

Kliknutím na "+" nahrajte PKG aplikácie, ktorú chcete nahrať. Zatiaľ je podporovaný len formát PKG.

Limit odosielania na zariadeniach OnPremise môžete zvýšiť v kroku 3 konfigurácie zariadenia. Ak chcete zvýšiť limit nahrávania v cloude, obráťte sa na podporu, ktorá vám poskytne ďalšie informácie.

Cieľová aktualizácia

Pomocou funkcie "Update Target" môžete vybrať, ktorá verzia aplikácie sa má nainštalovať alebo na ktorú verziu sa má aplikácia aktualizovať, ak ste pre aplikáciu aktivovali funkciu "Keep up to date".

Ak ste nevybrali cieľ aktualizácie, použije sa najvyššia verzia.

Windows 10

Tu môžete nahrať aplikácie Windows 10 a neskôr ich distribuovať v správe mobilných zariadení v profile zariadenia alebo skupiny.

Kliknutím na "+" nahrajte APPX, APPXBUNDLE alebo MSI aplikácie, ktorú chcete nahrať. Zatiaľ je podporovaný len formát APPX, APPXBUNDLE alebo MSI.

Môžete tiež nahrať a definovať Závislosti pre aplikáciu, ktoré budú automaticky distribuované a nainštalované pred inštaláciou požadovanej aplikácie.

Limit odosielania na zariadeniach OnPremise môžete zvýšiť v kroku 3 konfigurácie zariadenia. Ak chcete zvýšiť limit nahrávania v cloude, obráťte sa na podporu, ktorá vám poskytne ďalšie informácie.

Cieľová aktualizácia

Pomocou funkcie "Update Target" môžete vybrať, ktorá verzia aplikácie sa má nainštalovať alebo na ktorú verziu sa má aplikácia aktualizovať, ak ste pre aplikáciu aktivovali funkciu "Keep up to date".

Ak ste nevybrali cieľ aktualizácie, použije sa najvyššia verzia.

Balík Win32 (.exe)

Do zariadení môžete distribuovať aj súbory .exe/inštalačné programy.

Názov balíka	Názov, ktorý sa zobrazí v MDM
Popis	Popis uvedený v MDM
Súbor balíka	Povolené sú len súbory .zip. Umiestnite súbory, ktoré chcete nasadiť, do tohto zip súboru.
Kontext nasadenia	**Systém**: Príkaz inštalácie sa spustí so systémovými oprávneniami, ktoré sú vyššie ako "Používateľ". Taktiež pri použití "System" proces nemá používateľské rozhranie, takže bude tichý a profil používateľa, napr. premenné prostredia ako %AppDat%, nie je prístupný. **User (Používateľ)**: Príkaz inštalácie má prístup k profilu používateľa a v prípade potreby môže zobraziť používateľské rozhranie. Poznámka: Niektoré procesy môžu pracovať len v jednom kontexte. Napr. ak sa softvér nainštaluje do AppData, bude fungovať len pri výbere "User" (Používateľ).
Inštalácia príkazu	Príkaz použitý na inštaláciu programu. Napríklad inštalačný príkaz pre súbor zip obsahujúci v koreni súbor "setup.exe", ktorý podporuje parameter "/s" pre tichú inštaláciu, by bol príkaz "setup.exe /s". Uvedomte si, že rôzne softvéry môžu mať rôzne parametre.
Príkaz na odinštalovanie	Príkaz, ktorý sa má spustiť na odinštalovanie softvéru prostredníctvom MDM. Zvyčajne ukazuje na odinštalátor. Napríklad "C:\Program Files\ExampleSoftware\uninstall.exe".
Požiadavky	
Poznámka: Aby sa softvér nainštaloval, musia byť splnené všetky stanovené požiadavky. V opačnom prípade sa nenainštaluje. Niektoré polia môžu byť povinné. Ak pre požiadavku nie je nastavená žiadna hodnota, požiadavka sa bude ignorovať.	
Architektúra operačného systému	Architektúra operačného systému
Min. verzia OS	Min. verzia OS
Min. voľné miesto na disku (MB)	Min. voľné miesto na disku (MB)
Min. fyzická pamäť (MB)	Min. fyzická pamäť (MB)
Minimálny počet logických procesorov	Minimálny počet logických procesorov

Min. rýchlosť CPU (MHz)	Min. rýchlosť CPU (MHz)
Ďalšie požiadavky	Ak chcete, môžete tu tiež ručne definovať pravidlá alebo nahrať skript na vykonanie ďalších kontrol požiadaviek.
Pravidlá detekcie	
Metóda detekcie	Tu môžete definovať spôsob zisťovania, či je aplikácia v zariadení nainštalovaná. Príkazy na inštaláciu sa spustia len vtedy, keď tieto pravidlá zistia, že aplikácia NIE JE nainštalovaná. Príkazy na odinštalovanie sa spustia len vtedy, keď tieto pravidlá zistia, že aplikácia nie je nainštalovaná. **Ručne definujte pravidlá**: Umožňuje ručne definovať jedno alebo viac pravidiel, ktoré napríklad kontrolujú prítomnosť určitého súboru, priečinka, kľúča MSI alebo kľúča registra. Ak sú všetky zadané pravidlá detekcie pravdivé, aplikácia sa bude považovať za prítomnú. **Použiť skript**: Nahrajte vlastný skript s vlastnými kontrolami. Ak skript vráti "$TRUE", aplikácia sa bude považovať za prítomnú.
Pravidlá detekcie	

Nastavenia aplikácie

Nastavenia aplikácie iOS

Tu môžete definovať predvolené nastavenia pre pridanie aplikácie do povinného obchodu s aplikáciami alebo do podnikového obchodu s aplikáciami.

Poznámka: Týmto sa nastaví len to, čo je predvolene vybrané pri pridávaní aplikácií. NEMENÍ to existujúce nastavenia pre aplikácie, ktoré sú už pridané v povinných aplikáciách alebo v podnikovom obchode s aplikáciami.

Udržujte aktuálny stav	Automaticky aktualizuje aplikáciu. Upozorňujeme, že aktualizácia aplikácie môže trvať až 7 dní od vydania aktualizácie.
Predbiehanie, keď nie je riadené	Ak je aplikácia už nainštalovaná ako nespravovaná (používateľom), bude prevzatá a spravovaná systémom MDM.
Odstránenie aplikácie po odstránení profilu MDM	Odinštaluje aplikáciu po odstránení MDM.
Zabránenie zálohovaniu údajov aplikácie	Zabraňuje zálohovaniu údajov aplikácie.

Nastavenia aplikácie Android

Tu môžete definovať predvolené nastavenia pre pridanie aplikácie do povinného obchodu s aplikáciami alebo do podnikového obchodu s aplikáciami.

Poznámka: Týmto sa nastaví len to, čo je predvolene vybrané pri pridávaní. NEMENÍ to nastavenia pre aplikácie, ktoré sú už pridané v povinných aplikáciách alebo v obchode s podnikovými aplikáciami.

Udržujte aktuálny stav	Automaticky aktualizuje aplikáciu. K dispozícii len pre aplikácie InHouse.
Riadená aktualizácia klienta EMM AppTec360	Ak je táto možnosť povolená, administrátori môžu určiť cieľ aktualizácie pre klienta AppTec360 EMM. Zoznam všetkých dostupných verzií AppTec360 EMM Client sa zobrazí v časti "Všeobecné nastavenia" → "Správa aplikácií" → "Vnútorná databáza aplikácií" → "Android".

Aplikácie tretích strán

Android

Tu môžete nastaviť aktivačný kód pre Ikarus.

Nastavte túto možnosť na "Použiť aktivačný kód" a zadajte tu svoj aktivačný kód.

Poznámka: Po zadaní kódu a uložení sa kód ešte nepridá do profilu, ktorý sa odošle do zariadenia. Musíte vykonať akúkoľvek zmenu v profile, aby sa kód pridal do profilu. Napr. zmeňte ľubovoľný prepínač v profile z vypnuté → zapnuté → vypnuté - Uložiť → Priradiť teraz.

iOS

Tu môžete zadať svoju licenciu SecurePIM. Po zadaní licencie stlačte "Uložiť zmeny" a môžete používať možnosti SecurePIM.

VPP / KNOX Premium

Program Apples Volume Purchase Program (VPP) vám umožňuje jednoducho distribuovať platené a bezplatné aplikácie do vašich zariadení. Tento spôsob sa veľmi odporúča, pretože v zariadeniach nepotrebujete Apple ID, používatelia nemusia potvrdzovať inštaláciu (pod dohľadom), používatelia nebudú musieť zadávať heslo Apple ID a môžete ľahko distribuovať platené aplikácie bez toho, aby ste ich museli kupovať na každé zariadenie znova.

Ak chcete používať VPP, musíte sa zaregistrovať v aplikácii Apple Business Manager.

Licencie VPP

Tu môžete získať prehľad o svojich aplikáciách VPP, o tom, koľko licencií sa používa a koľko ich je k dispozícii.

Kliknutím na koliesko uvidíte, ktoré zariadenia majú priradenú licenciu a aký je stav tohto priradenia.

Kliknutím na obnovíte vyrovnávaciu pamäť VPP, ktorá porovnáva licencie pridelené v systéme MDM s licenciami pridelenými na strane Applu. To môže v niektorých prípadoch vyriešiť problémy s licenciami.

Token VPP

Tu môžete nahrať svoj token VPP, ktorý nájdete v aplikácii Apple Business Manager v časti Nastavenia → Aplikácie a knihy. Môžete nahrať viacero tokenov VPP.

Token môžete obnoviť tak, že si jednoducho stiahnete nový v aplikácii Apple Business Manager, kliknete na koliesko "Upraviť" a nahráte nový.

Režim VPP rozhoduje o tom, ako sa bude postupovať pri prideľovaní licencií. V závislosti od scenára musíte použiť rôzne režimy:

"Device based" sa musí použiť pri registrácii zariadení prostredníctvom QR kódu, odkazu, konfigurátora Apple alebo DEP.

"Na základe používateľa" sa vyžaduje, ak sú Zariadenia zaregistrované s Registráciou používateľa alebo ako zdieľaný iPad.

Ak povolíte funkciu "Automatizovaná správa licencií", používateľom presunutým z jednej skupiny do druhej budú automaticky pridelené licencie Apple VPP na základe profilu skupiny, do ktorej boli presunutí.

Existujúce licencie Apple VPP zo skupiny, z ktorej sa presunuli, nebudú zrušené.

Novým používateľom pridaným do skupiny budú automaticky pridelené licencie Apple VPP na základe príslušného profilu skupiny.

Kľúč KNOX Premium

Tu môžete zadať svoj kľúč KNOX Premium Key na používanie kontajnera Samsung KNOX.

Upozorňujeme, že táto funkcia už nie je podporovaná od systému Android 10. Namiesto toho použite kontajner Android Enterprise.

Nastavenia obchodu s aplikáciami

Región a jazyk

Tu môžete nastaviť predvolený jazyk a oblasť pre vyhľadávanie aplikácií v správe aplikácií.

Upozorňujeme, že nastavenie pre iTunes určuje aj spôsob, akým systém získava informácie o určitých aplikáciách. Ak sa v zoznamoch stretnete s aplikáciami, ktoré sa zobrazujú zvláštnym spôsobom (napr. chýbajúca ikona), možno ste nastavili oblasť, v ktorej konkrétna aplikácia nie je dostupná.

Obchod AE Play

Tu nájdete všetky možnosti obchodu Play pre podnikové zariadenia so systémom Android na schvaľovanie aplikácií, nahrávanie vlastných aplikácií do obchodu Play alebo vytváranie vlastných webových aplikácií.

Schválené aplikácie

Tu môžete získať prehľad o všetkých schválených aplikáciách.

Aplikácie v Obchode Play

Tým sa načíta iFrame zobrazujúci Obchod Play. Vyhľadajte ľubovoľnú aplikáciu, kliknite na ňu a potvrďte ju. Pri schvaľovaní aplikácie môžete tiež definovať, že schválenie sa zruší, ak sa zmenia požadované oprávnenia. Pri schvaľovaní aplikácií odporúčame ponechať tieto nastavenia predvolené.

Po schválení aplikácie ju môžete pridať do svojich profilov.

Tlačidlo "Schváliť" sa po schválení zmení na "Odvolať schválenie", takže aplikácie môžete kedykoľvek odstrániť, ak ich už nepotrebujete.

Súkromné aplikácie

Tu môžete nahrať vlastnú aplikáciu ako súkromnú aplikáciu do obchodu Google Play. To vám umožní distribuovať aplikáciu prostredníctvom služieb spoločnosti Google a aktualizovať ju prostredníctvom nich. Výhodou je aj to, že vaše vlastné Aplikácie sa môžu inštalovať bez potvrdenia používateľom, ktoré je zvyčajne potrebné.

Webové aplikácie

Tu môžete vytvárať webové aplikácie, čo sú odkazy na určité webové stránky, ktoré možno priradiť ako aplikácie.

Tejto ikone môžete tiež priradiť vlastnú ikonu a ďalej definovať, ako presne sa má zobrazovať.

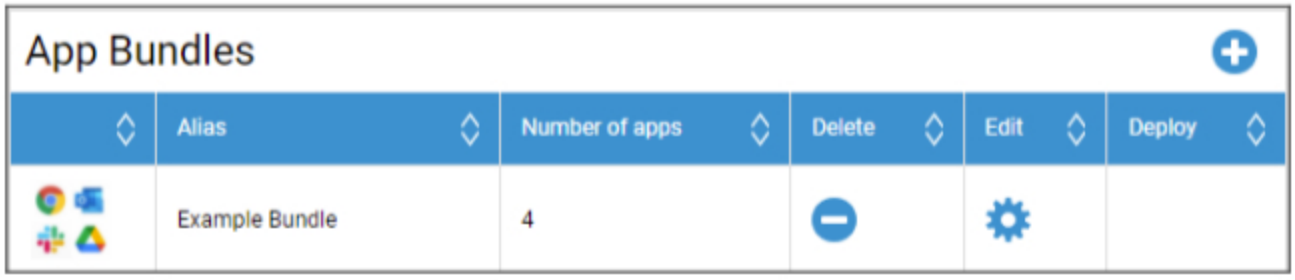
Rozloženie obchodu

Rozloženie obchodu určuje, ako sa aplikácie zobrazujú v Obchode Play alebo či sa vôbec zobrazujú.

Majte na pamäti, že ak chcete zobraziť aplikácie v Obchode Play, ktoré si používateľ môže manuálne nainštalovať, je potrebné ich pridať sem do rozvrhnutia. **A .** v profile do podnikového obchodu Play. Ak pridáte aplikáciu len do jednej z nich, nebude sa zobrazovať.

Balík aplikácií

Pomocou balíkov aplikácií môžete definovať skupiny aplikácií, ktoré možno jedným kliknutím priradiť k profilom zariadenia alebo skupiny.



Kliknutím na "+" vytvorte nový balík aplikácií. Po vytvorení balíka aplikácií môžete kliknutím na "Upraviť" pridať do balíka aplikácie z rôznych zdrojov.

Balík je možné pridávať do profilov ako všetky ostatné aplikácie. Pri pridávaní aplikácií sa vám zobrazí ďalšia karta s názvom "App Bundles" (Balíky aplikácií), kde máte svoje Balíky.

Ak vykonáte akúkoľvek zmenu v balíku aplikácií, zobrazí sa tlačidlo v stĺpci "Deploy". To vám umožní poslať tieto zmeny do všetkých profilov obsahujúcich tento Bundle. Majte preto na pamäti, že po pridaní alebo odstránení aplikácií v Bundle to musíte urobiť ručne.

Diaľkové ovládanie

TeamViewer

Konektor TeamViewer

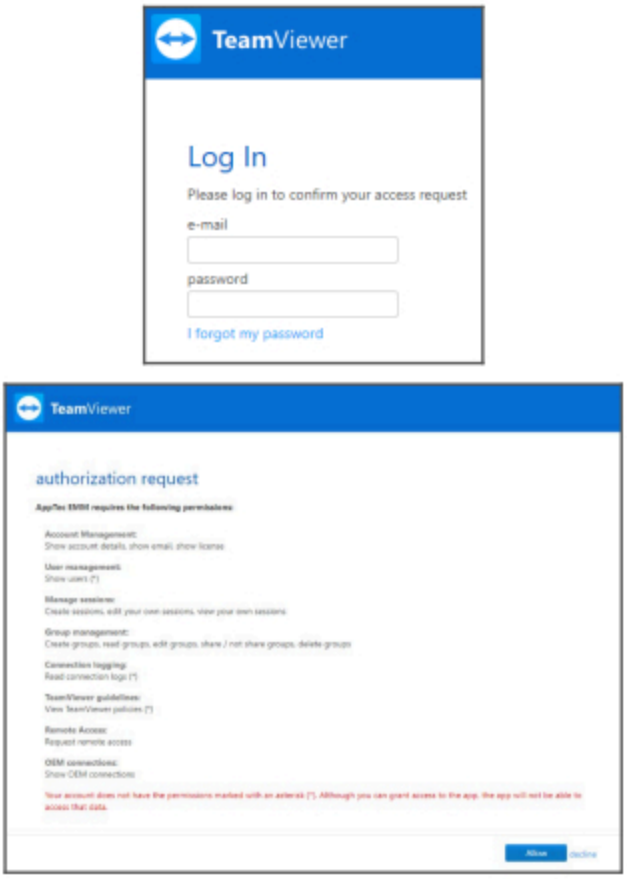
Poznámka: V bezplatnej skúšobnej verzii našej cloudovej aplikácie nemôžete pripojiť svoje konto TeamViewer. Namiesto toho budete mať automaticky pripojený bezplatný demo účet.

Prejdite na Všeobecné nastavenia -> Vzdialené ovládanie -> TeamViewer. Tu môžete prepojiť svoje konto TeamViewer s konzolou alebo si pozrieť informácie o aktuálne pripojenom konte. Taktiež máte možnosť zobraziť všetky aktuálne aktívne relácie, ak prejdete do časti "Aktívne relácie".

Ak chcete prepojiť svoje konto, kliknite na "Spustiť nastavenie".

Tým sa dostanete na novú stránku, kde sa musíte prihlásiť pomocou svojho konta TeamViewer.

Po prihlásení ste autorizovali AppTec360 MDM na používanie tohto účtu. Po potvrdení musíte počkať niekoľko sekúnd a účet je pripojený.


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

Inštalácia aplikácie TeamViewer QuickSupport

Pridajte aplikáciu "TeamViewer QuickSupport" do povinných aplikácií profilu zariadenia alebo profilu skupiny a kliknite na "Priradiť teraz". Počkajte, kým sa aplikácia nainštaluje do zariadenia.

Ak sa pokúsite získať prístup k zariadeniu, v ktorom aplikácia nie je nainštalovaná, v závislosti od konfigurácie zariadenia sa nainštaluje alebo sa zobrazí výzva na jej inštaláciu.

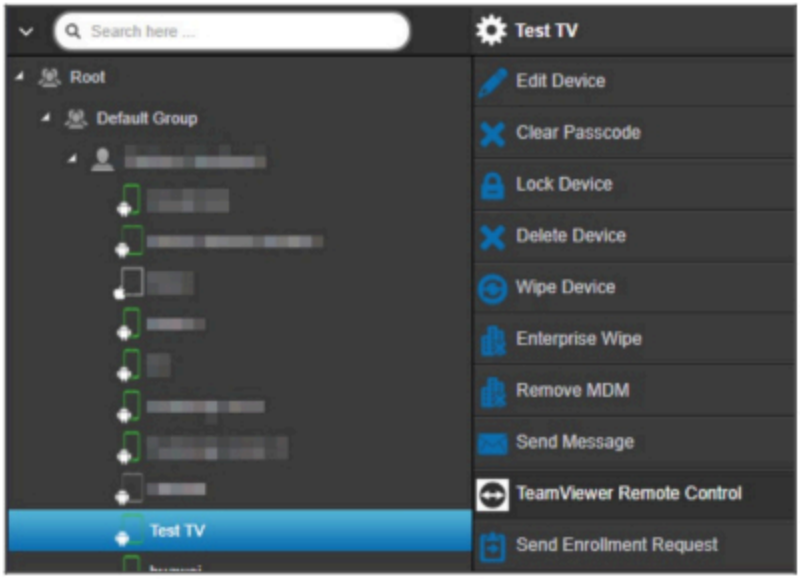
Diaľkové ovládanie zariadenia

Ak chcete zariadenie ovládať na diaľku, vyberte zariadenie, kliknite na koliesko a vyberte položku "TeamViewer Remote Control".

Ak už existuje aktívna relácia, môžete použiť starú reláciu alebo vytvoriť novú.

Potvrďte, že chcete vytvoriť novú reláciu TeamViewer.

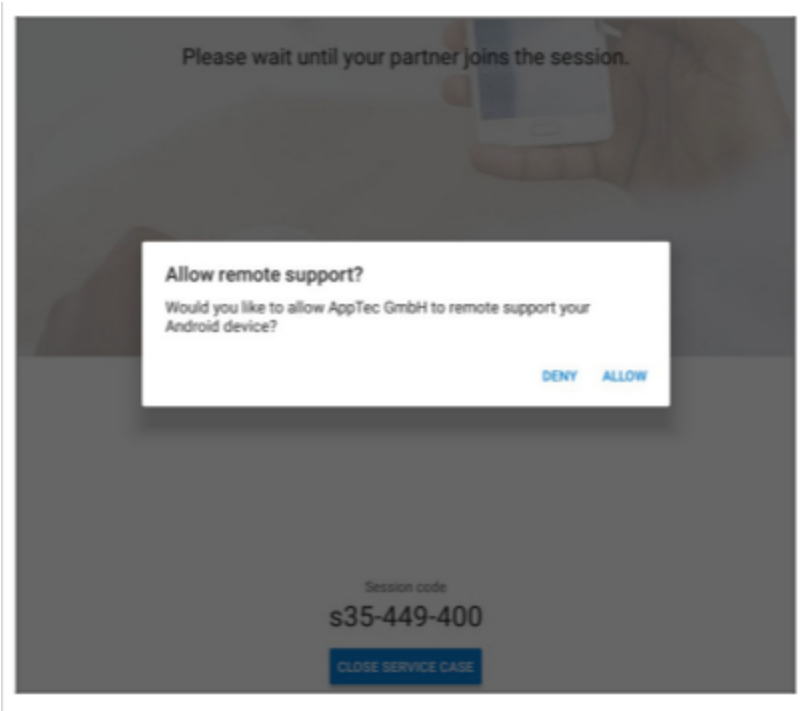
Po niekoľkých sekundách sa zobrazí odkaz na reláciu TeamViewer. Kliknutím na "Start" (Spustiť) otvoríte tento odkaz v novom okne.


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

Toto prepojenie otvorí nainštalovaný program TeamViewer a pripojí vás k zariadeniu.

Teraz musíte potvrdiť pripojenie na samotnom zariadení, aby ste ho mohli diaľkovo ovládať.

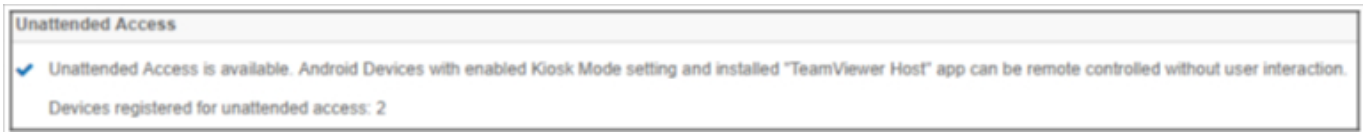


Ak používate iOS, v klientovi AppTec360 MDM sa zobrazí správa. Pomocou tohto odkazu sa zariadenie pripojí k vzdialenej relácii. V závislosti od nastavení oznámení zariadenia je možné, že oznámenie nedostanete a budete musieť otvoriť AppTec360 MDM Client manuálne.

Na niektorých zariadeniach so systémom Android (napr. Samsung) je potrebné nainštalovať ďalšiu aplikáciu ako doplnok. Aplikácia TeamViewer v zariadení vás o tom bude informovať, ak je to vo vašom zariadení potrebné.

Prístup bez dozoru

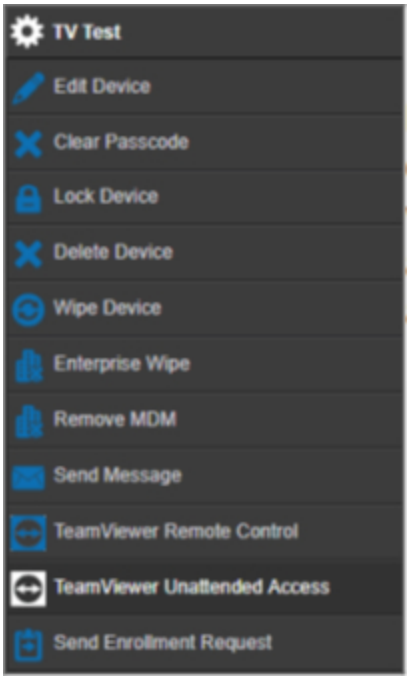
Poznámka: Bezobslužný prístup je možný len na zariadeniach so systémom Android.



K zariadeniam sa môžete pripojiť bez toho, aby ste prijali pripojenie na zariadení, len ak vaše konto TeamViewer používa licenciu "Tensor" alebo "Corporate".

Po prepojení účtu to môžete skontrolovať v časti "Všeobecné nastavenia".

Ak chcete používať bezobslužný prístup, musíte si nainštalovať aplikáciu "TeamViewer Host" a aktivovať "Enable Unattended Access" (Povoliť bezobslužný prístup) v časti "Kiosk Mode & Launcher" (Režim kiosku a spúšťač) vo svojom profile. Upozorňujeme, že je to možné len vtedy, ak používate režim Kiosk Mode.



Teraz môžete vybrať bezobslužný prístup, ak vyberiete zariadenie a kliknete na koliesko. Tým sa pripojíte k svojmu zariadeniu bez potreby potvrdenia na samotnom zariadení. Upozorňujeme, že môže chvíľu trvať, kým sa zobrazí Odkaz na prístup k vášmu zariadeniu.

Splashtop

Ak povolíte možnosť Splashtop, v profiloch sa zobrazia možnosti konfigurácie Splashtop.

Ak chcete používať Splashtop, musíte vo svojom profile nastaviť Splashtop Streamer (com.splashtop.streamer.csrs) ako povinnú aplikáciu. Potom môžete vo svojom profile v časti "Vzdialené ovládanie" povoliť konfiguráciu Splashtop. Jej povolením sa nakonfiguruje aplikácia Splashtop Streamer. Ak používate aplikáciu Splashtop Streamer, ale nie v kombinácii s MDM, mali by ste túto možnosť nechať vypnutú.

Vo svojom profile v časti "Diaľkové ovládanie" musíte nastaviť aj kód nasadenia. Prejdite na stránku https://my.splashtop.com a prihláste sa do svojho účtu Splashtop. Kliknite na "Add Computer" (Pridať počítač) a na výslednej stránke skopírujte 12-miestny deploy kód.

Bez kódu Deploy Code nie je diaľkové ovládanie možné.

Potom môžete kliknúť pravým tlačidlom myši na svoje zariadenie a spustiť vzdialenú reláciu kliknutím na "Splashtop Remote Control".

Správa sim kariet

Hromadný import CSV

Zobrazí sa prehľad priradených SIM kariet a všetky informácie o nich. Pomôže vám to mať všetky informácie nielen o vašich zariadeniach, ale aj o vašich SIM kartách v jednom systéme.

POZNÁMKA: Toto je manuálne riadenie/dokumentácia. Tieto údaje nie je možné získať automaticky zo zariadení z dôvodu ochrany súkromia/bezpečnostných mechanizmov operačných systémov.

Tento zoznam môžete tiež ex- a importovať ako CSV.

Prepravca a tarifa

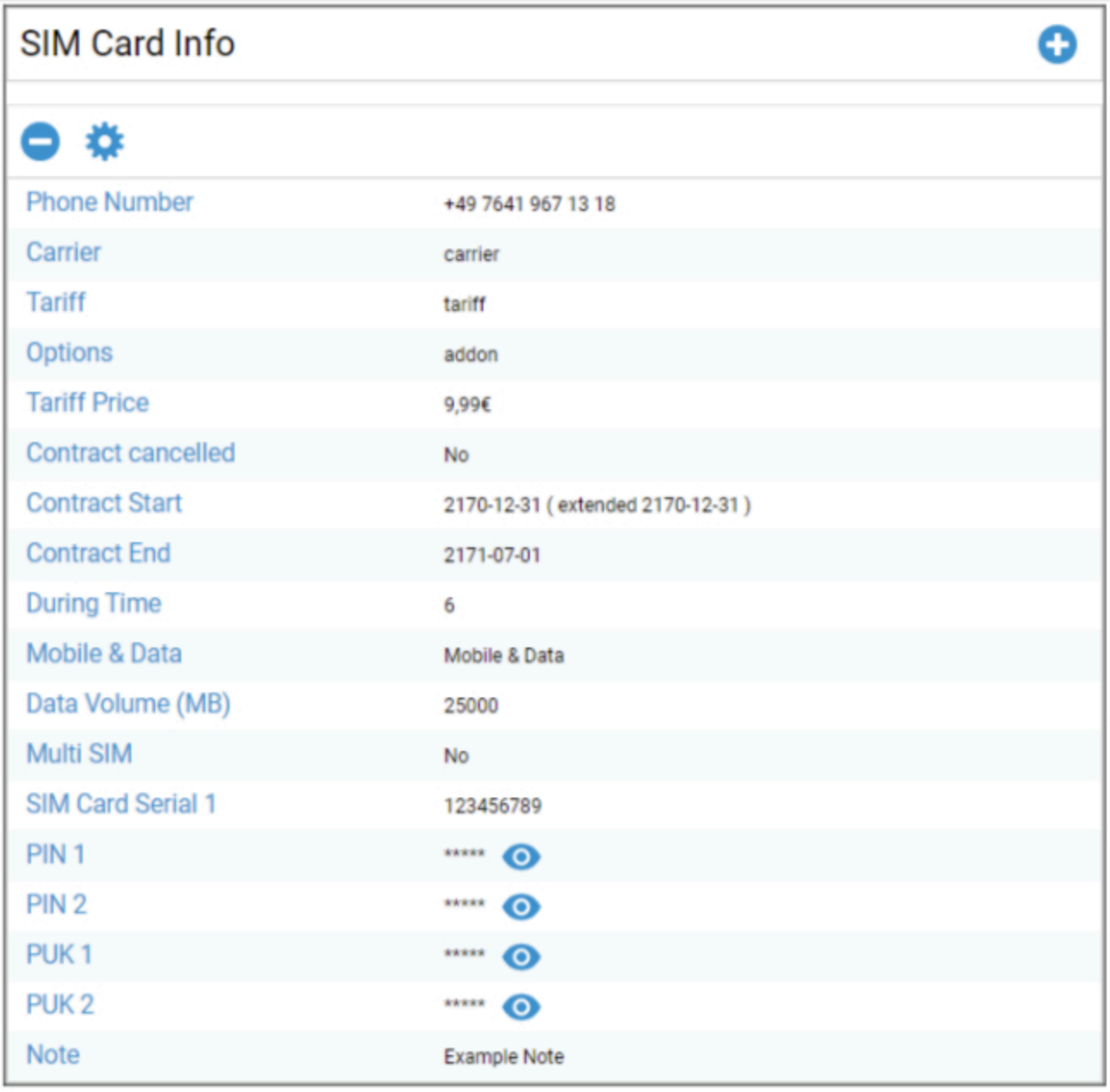
Ak chcete pridať SIM kartu, najprv kliknite na tlačidlo Pridať jedného alebo viacerých operátorov.

Potom kliknite na "+" v časti "Informácie o tarife" a pridajte tarifu k dopravcovi.

Voliteľne môžete pridať voliteľné doplnky nižšie, ak máte niečo podobné.

Pripravené je všetko potrebné na pridanie skutočnej karty Sim. SIM karty sú v súčasnosti priradené k Používateľovi. Prejdite preto do Správy mobilných zariadení, vyberte Používateľa a prejdite na položku Prehľad SIM kariet.

Tu vidíte SIM karty týchto používateľov. Ak tu nejaká je, môžete ju upraviť alebo odstrániť. Používatelia môžu mať viacero SIM kariet.

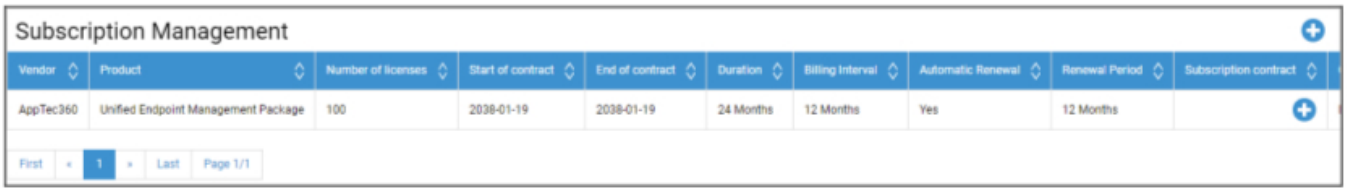


Kliknutím na "+" pridajte kartu Sim a pridajte všetky potrebné informácie. Tieto Sim karty budú tiež uvedené v zozname všetkých vašich Sim kariet v časti Všeobecné nastavenia → Správa Sim kariet.

Správa predplatného

Správa predplatného

Tu môžete dokumentovať prebiehajúce predplatné, jeho podrobnosti a tiež ukladať rôzne súbory, napr. podpísanú zmluvu, výpoveď zmluvy atď. Môžete tiež nastaviť pripomienky, ktoré vám pred ukončením predplatného pripomínajú per mail a možno ho automaticky predlžujú.



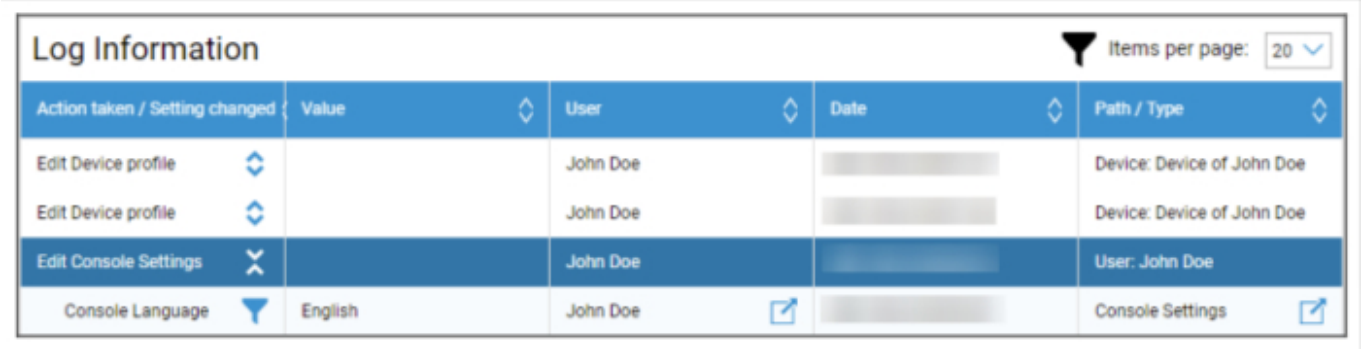
Ak chcete pridať predplatné, kliknite na "+" v hornej časti. Môžete pridať toľko odberov, koľko chcete.

Ak chcete nahrať súbory týkajúce sa tohto predplatného, kliknite na "+" v rôznych poliach. Technicky môžete nahrať akýkoľvek typ súboru, ale majte na pamäti, že nie každý typ súboru je možné zobraziť v prehliadači.

Všeobecný denník auditu

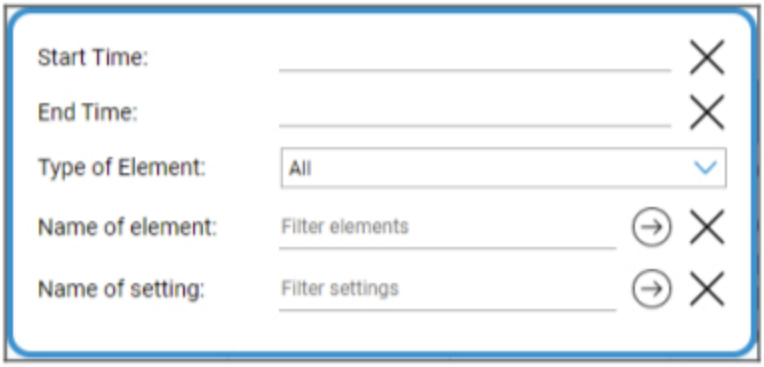
Protokol o audite

Tu sa nachádza všeobecný protokol auditu, v ktorom sú zobrazené všetky vykonané zmeny. Zatiaľ čo v denníku auditu u používateľa alebo skupiny sa zobrazujú len zmeny podľa tohto používateľa alebo skupiny, v tomto denníku sa zobrazuje KAŽDÁ zmena vykonaná kdekoľvek v konzole.



Môžete si pozrieť, čo, kto, kedy a kde zmenil. V niektorých prípadoch môžete záznam rozšíriť a zobraziť ďalšie podrobnosti.

Kliknutím na používateľa alebo na položku v poli "Cesta / Typ" sa dostanete na miesto, kde bola vykonaná zmena.



V pravom hornom rohu môžete tiež definovať filter, ktorý môže pomôcť nájsť určité zmeny v prostredí, v ktorom dochádza k mnohým zmenám.

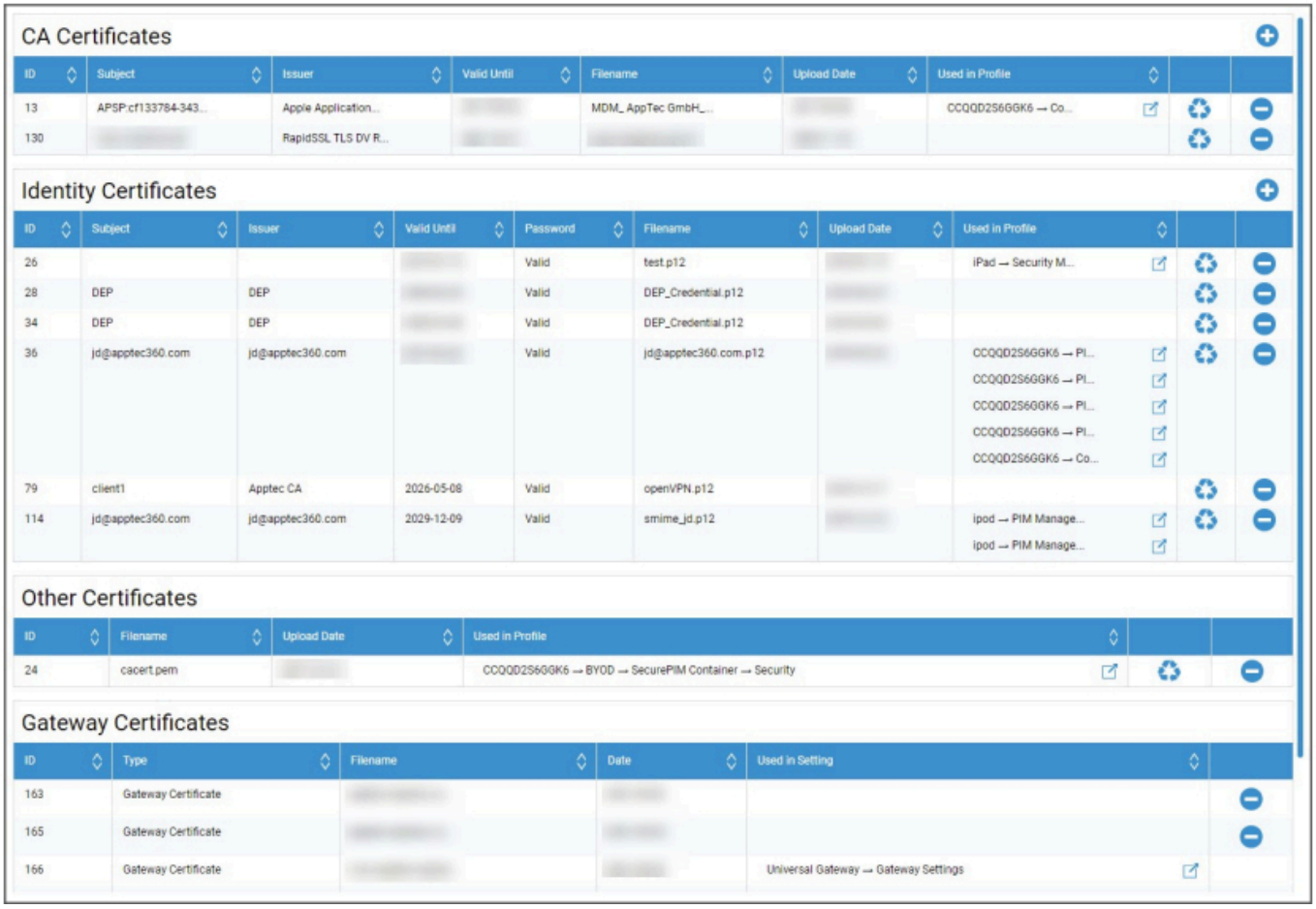
Nastavenia protokolu auditu

"Doba uchovávania denníka auditu" definuje, ako dlho by sa mali denníky auditu uchovávať pred vymazaním.

Správa certifikátov

Tu získate prehľad o všetkých certifikátoch nahraných a použitých v konzole. Toto je len prehľad. Skutočná konfigurácia napr. certifikátov Wi-Fi sa stále vykonáva v profile na príslušnom mieste.

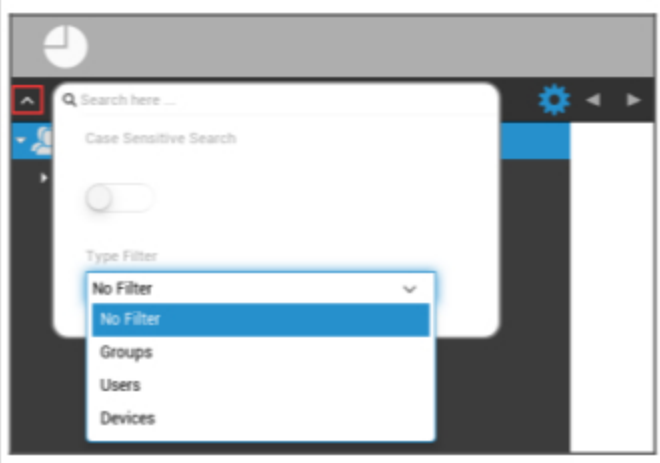
Tu môžete tiež odstrániť alebo aktualizovať certifikáty, čo sa automaticky premietne do dotknutých profilov. Kliknutím na informácie v časti "Použité v profile" zistíte, kde presne je ešte priradený nejaký certifikát.



Správa mobilných zariadení

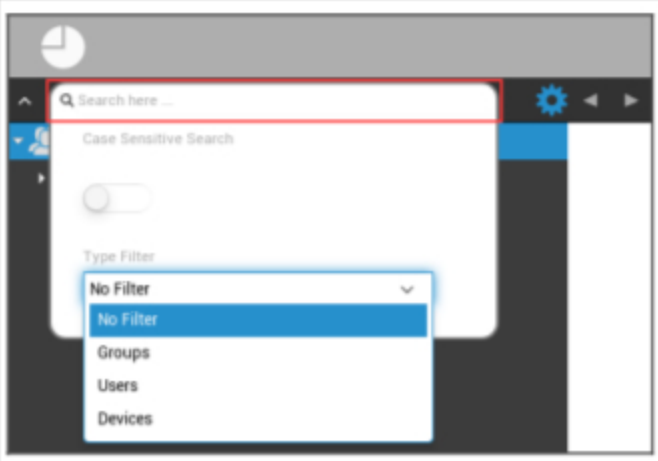
Obrazovka správy mobilných zariadení

Filter zariadenia



Kliknutím v ľavom hornom rohu obrazovky nájdete rôzne filtre na zobrazenie zariadení.

Vyhľadávacie okno



Okno vyhľadávania umožňuje vyhľadávať všetky zariadenia a/alebo používateľov s konkrétnym kľúčovým slovom.

Možnosť voľby zariadenia

Po kliknutí na príslušný symbol sa zobrazí zoznam možností, ktoré máte k dispozícii.

Tie sa menia s každým aktuálnym oknom a sú vysvetlené v príslušných kapitolách.

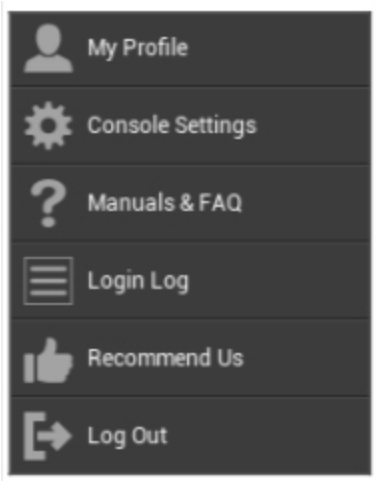
Navigačné šípky

Kliknutím na šípku vľavo sa dostanete na predchádzajúcu stránku.

Potom sa kliknutím na šípku doprava dostanete na stránku, ktorú ste práve opustili.

Nastavenia účtu pre správu

Kliknutím na e-mailovú adresu, ako je vidieť vyššie, sa zobrazí nasledujúca ponuka:



Môj profil	Úprava údajov konta administrátora
Nastavenia konzoly	Konfigurácia nastavení konzoly pre konto Admins
Príručky a často kladené otázky	Zobrazenie stránky "Manuály a často kladené otázky" v časti "Všeobecné nastavenia"
Prihlasovací protokol	Prístup k "Prihlasovaciemu protokolu"
Odporúčajte nás	Zobrazenie stránky "Odporúčajte nás" v časti "Všeobecné nastavenia"
Odhlásenie	Odhlásenie z konzoly MDM

Informácie o používateľovi

Tu môžete upraviť údaje o účte aktuálne prihláseného správcu.

Používateľské meno	Používateľské meno a/alebo e-mailová adresa účtu
Názov	Krstné meno správcov
Priezvisko	Priezvisko správcov
Prihlasovacie meno	Prihlasovacie meno správcov
E-mailová adresa	E-mailová adresa správcov
Alternatívna e-mailová adresa	Náhradná e-mailová adresa správcov
Obrázok	Profilový obrázok
Telefónne číslo	Telefónne číslo správcov
Mobilné číslo	Mobilné číslo správcov
Predĺženie telefónu	Predĺženie telefónu
Umiestnenie	Umiestnenie
Pozícia	Pozícia v spoločnosti
Skupina používateľov	Vyberte, do ktorej skupiny používateľov chcete priradiť konto správcu
Komentár	Zadajte komentár
Zadajte nové heslo	Zadajte heslo pre zmenu hesla
Opakovanie nového hesla	Zopakujte nové heslo na potvrdenie

Upozorňujeme, že administrátorský prístup môže byť v hierarchickej štruktúre podaný aj ako lokálny používateľský účet. Bez založenia ďalšieho administrátora by sa tento nemal vymazať!

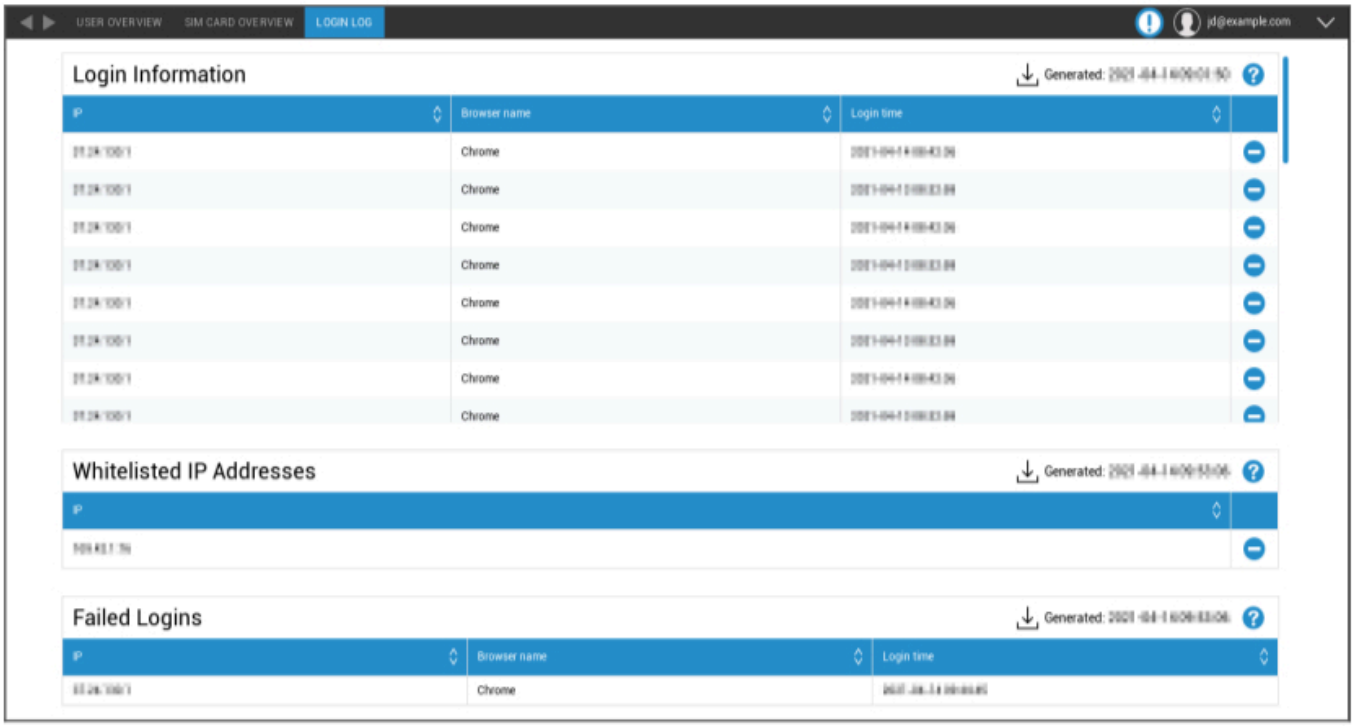
Nastavenia konzoly

Tu môžete nakonfigurovať nasledujúce nastavenia konzoly pre účet Admins:

Možnosti zobrazenia používateľa adresára	Definovanie spôsobu označovania používateľov v strome
Možnosti zobrazenia adresárového zariadenia	Definovanie spôsobu označovania zariadení v strome
Časový limit relácie	Ak používateľ v určenom čase nič neurobí, bude odhlásený. Predvolená hodnota je 60 minút. Po zmene tohto nastavenia sa odhláste a znovu prihláste.
Časové pásmo	Výber používaného časového pásma
Formát času	Vyberte, ako sa majú zobrazovať časové značky
Jazyk konzoly	Vyberte jazyk, v ktorom sa má konzola zobrazovať. K dispozícii sú angličtina a nemčina.
Hlavná farba	Môžete nastaviť farbu, ktorá sa použije ako základ pre farebnú schému konzoly. Môžete použiť výber farby alebo zadať farbu v HTML HEX notácii. Fungujú aj formátory RGB ako "ružová", "žltá".
Uložiť príkaz	Kombinácia klávesov na spustenie ukladania bez stlačenia tlačidla "Uložiť".
Používanie dvojfaktorového overovania	Povoľte používanie dvojfaktorového overovania pri prihlasovaní. Po prihlásení dostanete e-mail s kódom, ktorý musíte zadať na prihlásenie.
Časový limit dvojfaktorového overovania	Nastavte časové obdobie, počas ktorého nebudete požiadaní o dvojfaktorové overenie po už úspešnom overení.
Odoslať overovací kód prostredníctvom	Overovací kód bude odoslaný na vybrané možnosti. Správa o zariadení sa zobrazí v aplikácii AppTec360 MDM na všetkých zariadeniach so systémom Android a iOS, ktoré vám patria.
Odoslanie prihlasovacej správy po prihlásení	Ak je táto možnosť povolená, pri každom prihlásení z IP adresy, ktorá nie je uvedená na bielej listine, sa odošle e-mail. E-mail obsahuje informácie o prihlásení (napr. IP, prehliadač).

Prihlasovací protokol

Tu môžete vidieť informácie o prihláseniach aktuálne prihláseného administrátorského účtu.



Prihlasovacie údaje	Zoznam obsahujúci prihlásenia aktuálne prihláseného účtu správcu, ktoré boli zaznamenané konzolou. V tomto zozname sa zobrazujú všetky vaše úspešné prihlásenia za posledných 30 dní.
IP adresy na bielej listine	Toto je zoznam všetkých vašich IP adries na bielej listine. Ak sa prihlásite z IP adresy, ktorá je uvedená v tomto zozname, nedostanete správu o prihlásení. IP adresu môžete do tohto zoznamu pridať kliknutím na tlačidlo vedľa položky v zozname "Prihlasovacie údaje" vyššie. Adresu IP môžete z tohto zoznamu odstrániť kliknutím na tlačidlo vedľa položky v tomto zozname alebo v zozname "Prihlasovacie údaje" vyššie.
Neúspešné prihlásenia	Toto je zoznam všetkých neúspešných pokusov o prihlásenie za posledných 30 dní. Ak sa vám nepodarilo zadať správne heslo aspoň trikrát za 20 minút, v tomto zozname sa objaví položka. O neúspešných pokusoch o prihlásenie budete informovaní aj e-mailom.

Podniková správa (koreňový uzol) v mobilnej správe

Po dosiahnutí koreňového uzla (prvej skupiny) môžete vykonať rôzne nastavenia pre vašu spoločnosť, pokiaľ ide o správu mobilných zariadení.

Vytvorenie podskupiny	Vytvorenie podskupiny
Premenovanie koreňového uzla	premenovanie koreňového uzla (napr. názov vašej spoločnosti)
Hromadný zápis	Registrácia viacerých zariadení/užívateľov súčasne
Hromadné pridelenie	Priradenie profilu pre príslušné skupiny s jedným pohľadom
Rýchla správa aplikácií	Odosielanie (ne)požiadaviek na inštaláciu aplikácie príslušným skupinám zariadení
Import používateľa CSV	Import používateľov z CSV do príslušnej skupiny

Vytvorenie podskupiny

Pomocou funkcie "Vytvoriť podskupinu" môžete vytvoriť ďalšiu podskupinu.

Môžete určiť, do ktorej skupiny sa má podskupina priradiť.

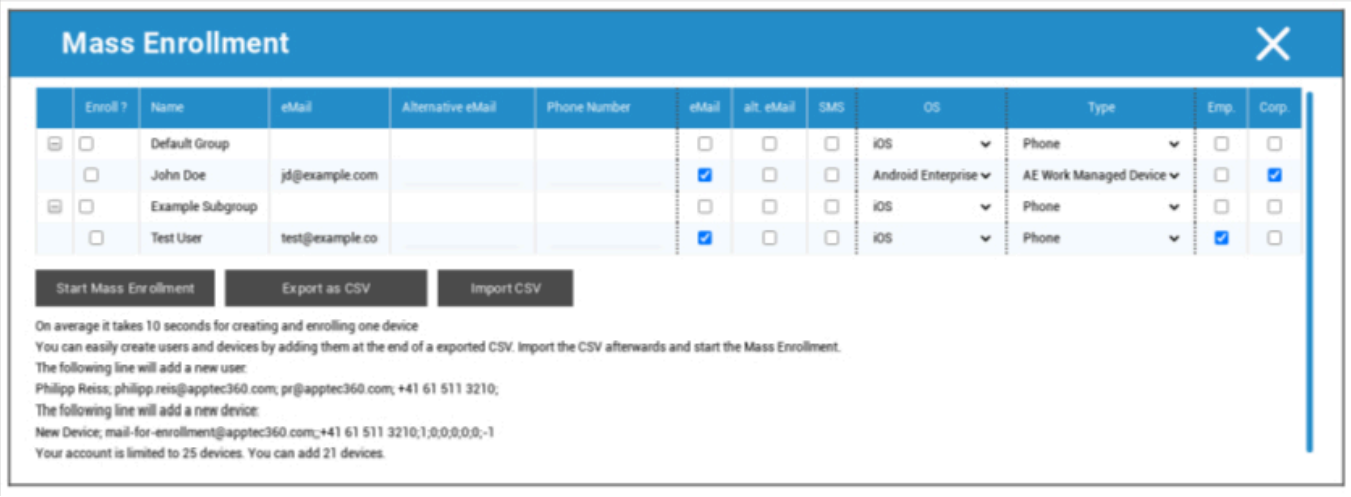
(V predvolenom nastavení sa vytvorí nová skupina, ktorá je priradená ako podskupina v koreňovom uzle)

Premenovanie koreňového uzla

Tu môžete premenovať svoje koreňové meno. Je bežné, že sa v tomto prípade používa názov spoločnosti.

Hromadný zápis

Pomocou funkcie "Hromadný zápis" môžete zaregistrovať viacero zariadení a používateľov.



Môžete priamo vybrať, akým spôsobom má používateľ dostať registráciu (eMail; alternatívny eMail; SMS)

V závislosti od toho, ktoré zariadenie používateľ dostane (iOS, Android, Windows Phone), môžete to tu priamo označiť.

Tu je možné nakonfigurovať aj rozlíšenie, či ide o smartfón alebo tablet, ktoré je potrebné správne zaškrtnúť.

V poslednom kroku môžete zistiť, či je príslušné zariadenie firemné alebo súkromné (BYOD).

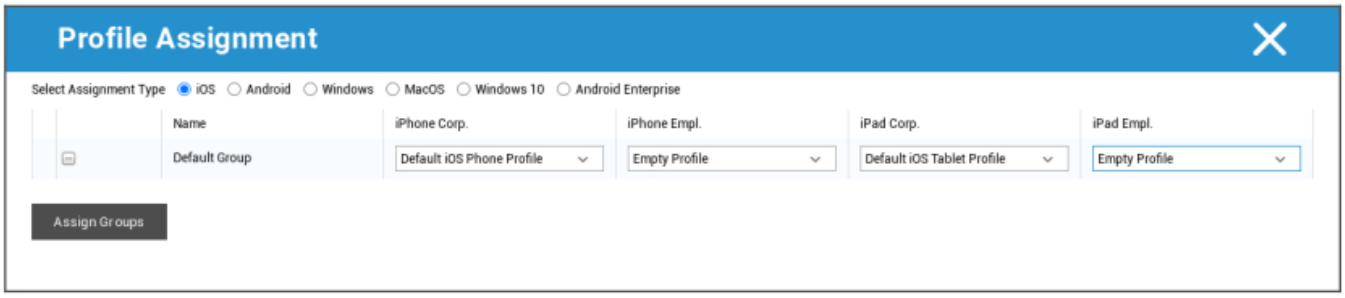
Pomocou položky "Exportovať ako CSV" môžete informácie exportovať ako dátový súbor CSV. Na oplátku môžete tiež importovať dátový súbor CSV pomocou "Import CSV", súbor by mal vyzerať ako v

nasledujúcom príklade:

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

Hromadné pridelenie

V časti Hromadné priradenie môžete priradiť profil všetkým skupinám, ktoré sú rozdelené na iOS - Android - Windows - MacOS - Windows 10 - Android Enterprise

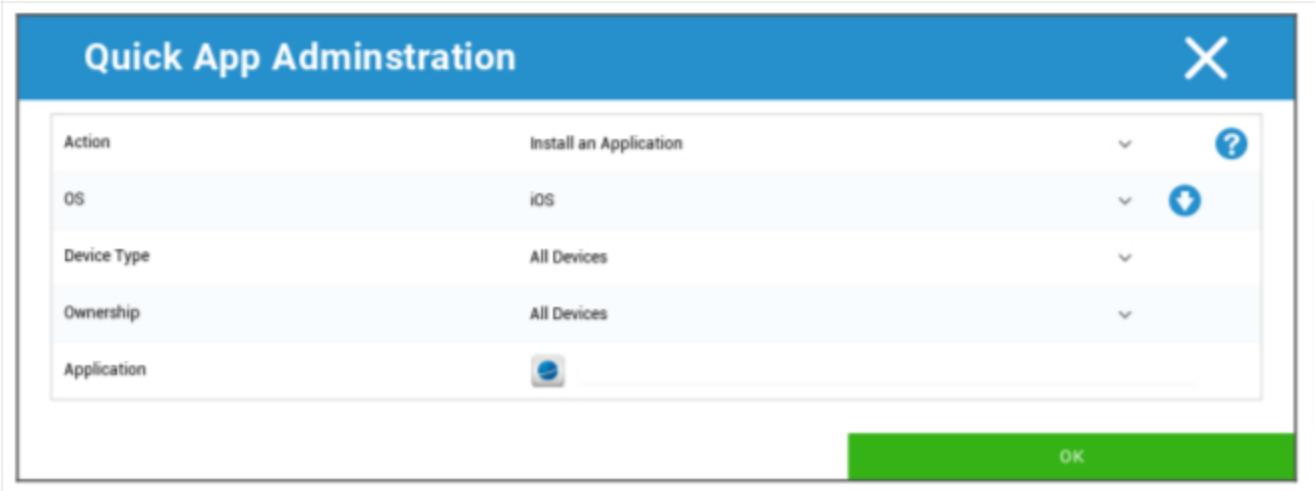


Windows - MacOS - Windows 10 - Android Enterprise

Rýchla správa aplikácií

V časti Rýchla správa aplikácií môžete odosielať požiadavky na inštaláciu alebo odinštalovanie zadanej aplikácie do vybraného operačného systému.

Môžete tiež definovať, či sa má požiadavka odoslať všetkým typom zariadení vybraného operačného systému alebo len konkrétnemu typu zariadenia.



Import používateľa CSV

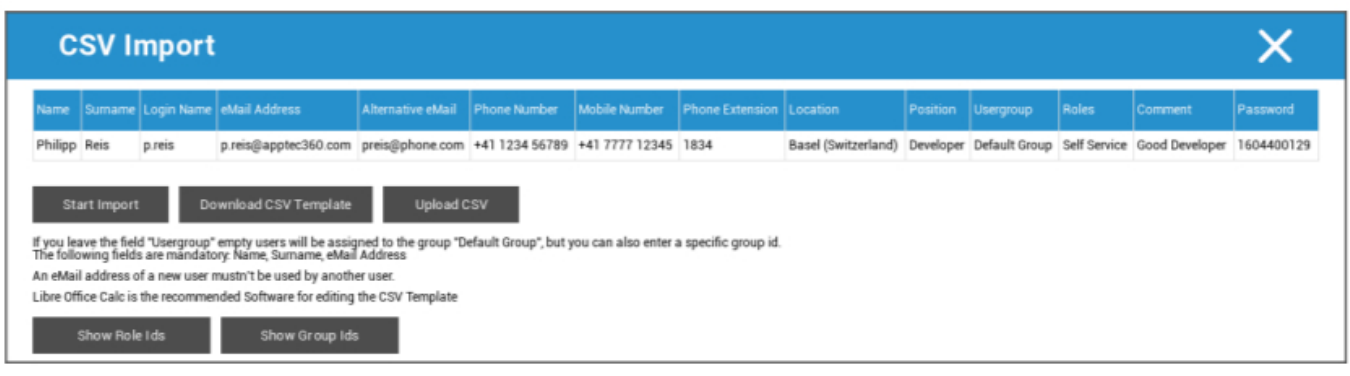
Import používateľov z CSV do príslušnej skupiny.

Pomocou funkcie "Stiahnuť šablónu CSV" môžete exportovať súbor šablóny CSV, ktorý môžete vyplniť (alebo ho môžete použiť ako referenciu).

Na vytvorenie vlastného súboru CSV môžete ako odkaz použiť aj možnosti "Zobraziť identifikátory rolí" a "Zobraziť identifikátory skupín".

Súbor CSV môžete nahrať do MDM pomocou funkcie "Nahrať CSV".

V poslednom kroku môžete spustiť import kliknutím na "Spustiť import".



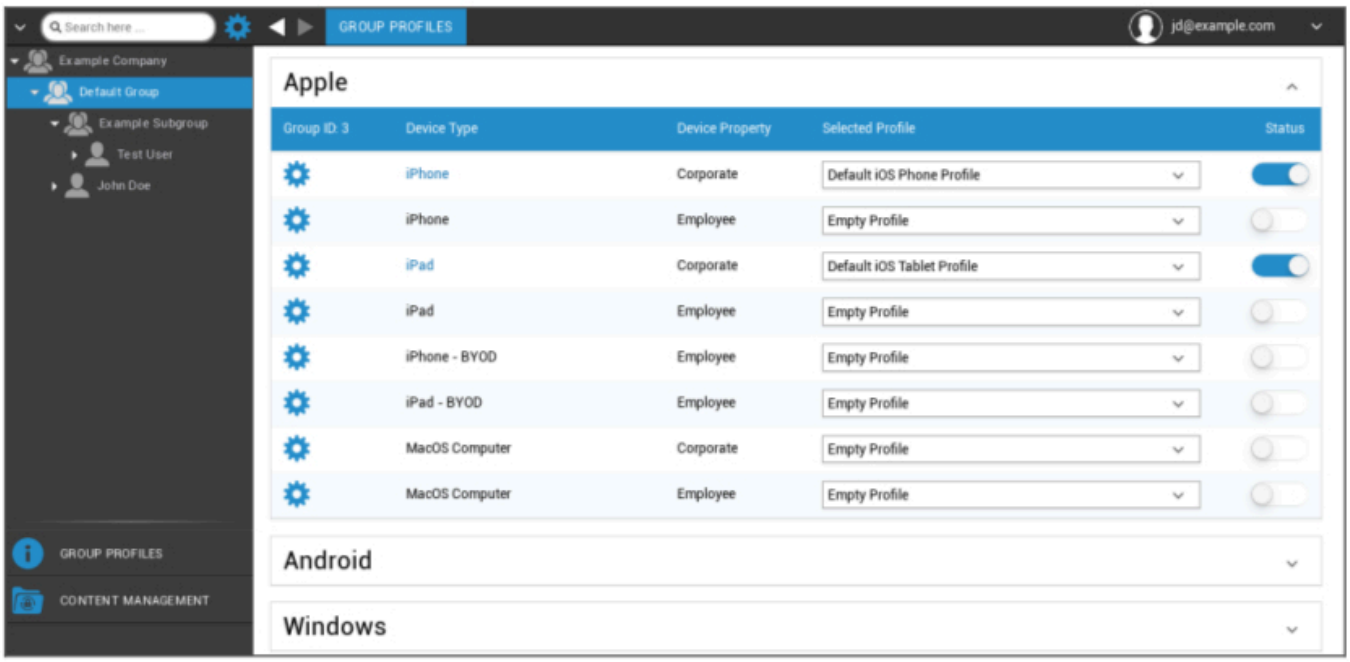
Správa skupín v mobilnej správe

Jedným kliknutím na prehľad sa zobrazia rôzne konfiguračné profily pre príslušné platformy.

Jeden profil obsahuje všetky možnosti nastavenia, ktoré je možné vopred vytvoriť pomocou AppTec360 v zariadení koncového používateľa. Na každej platforme môžete vytvoriť profily pre firemné zariadenia (Corporate) alebo zariadenia Bring-Your-Own-Device (Employee).

Na rozlíšenie konfigurácií skupín zariadení, napríklad na základe umiestnenia alebo funkcie, sa odporúča vytvoriť niekoľko podskupín.

Upozorňujeme na správu profilov v mobilnej správe



V ponuke prevodovky môžete nastaviť rôzne nastavenia pre príslušnú (pod)skupinu.

Vytvorenie podskupiny	Vytvorenie podskupiny pre príslušnú (pod)skupinu
Upraviť vybranú skupinu	Upraviť vybranú skupinu
Odstránenie vybranej skupiny	Odstránenie vybranej skupiny
Hromadný zápis	Zaregistrovanie mnohých zariadení/užívateľov naraz pre vybraný profil
Hromadné pridelenie	Priradenie profilov k aktuálne vybranej skupine
Vytvorenie podskupiny	Vytvorenie podskupiny pre príslušnú (pod)skupinu

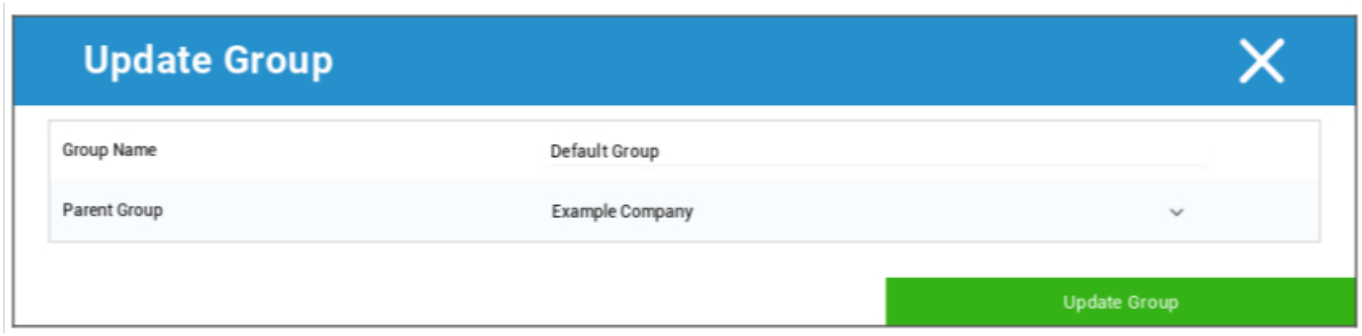
Vytvorenie používateľa	Vytvorenie používateľa pre príslušnú (pod)skupinu

Vytvorenie podskupiny

Pomocou funkcie "Vytvoriť podskupinu" môžete vytvoriť ďalšiu podskupinu.

Môžete určiť, pod ktorú skupinu sa má podskupina priradiť (predvolene sa podskupina priradí do skupiny, ktorá je aktuálne vybraná).

Upraviť vybranú skupinu



Tu môžete upraviť profil - sú tu možné nasledujúce nastavenia:

- Názov skupiny je možné zmeniť
- Rodičovskú skupinu možno zmeniť

Odstránenie vybranej skupiny

V časti "Odstrániť vybranú skupinu" sa zobrazí zoznam všetkých používateľov a zariadení, ktorí sú v príslušnej skupine. Tu máte možnosť ich vymazať.

Pre jedného používateľa môžete vykonať nasledujúce príkazy na odstránenie:

Odstrániť používateľa	Používateľ je vymazaný
Presunúť používateľa do skupiny:	Používateľa môžete presunúť do inej skupiny (nasledujúci stĺpec, napr. "Admins")

Pre jedno zariadenie môžete vykonať nasledujúce príkazy na odstránenie:

Vymazať a odstrániť	Vymazanie a odstránenie zariadenia
Odstrániť zo systému	Odstránenie zariadenia len z aplikácie AppTec

Odkaz: Hromadný zápis

Odkaz: Hromadné zadanie

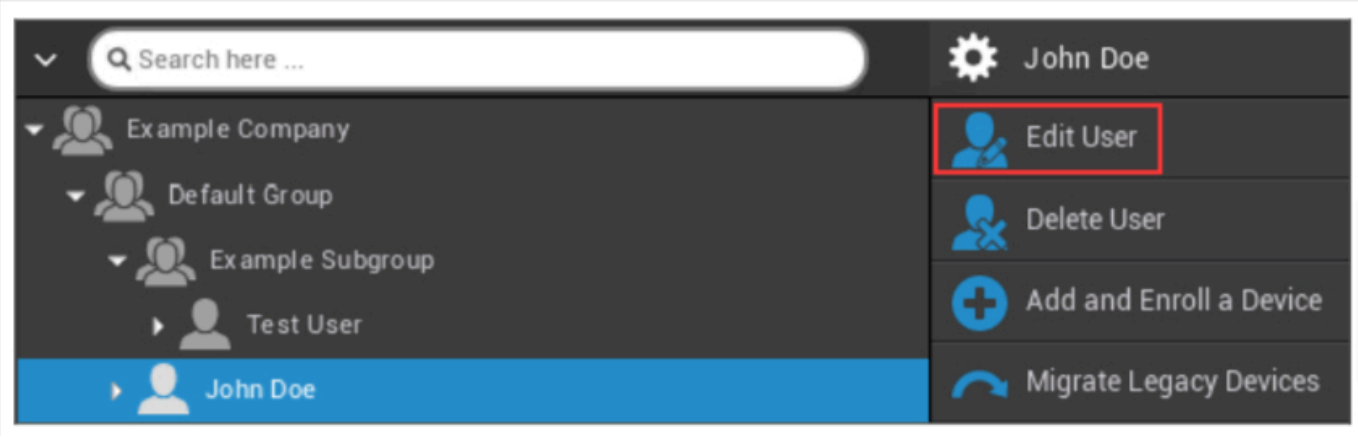
Vytvorenie používateľa

Pomocou položky "Vytvoriť používateľa" môžete pridať nového používateľa.

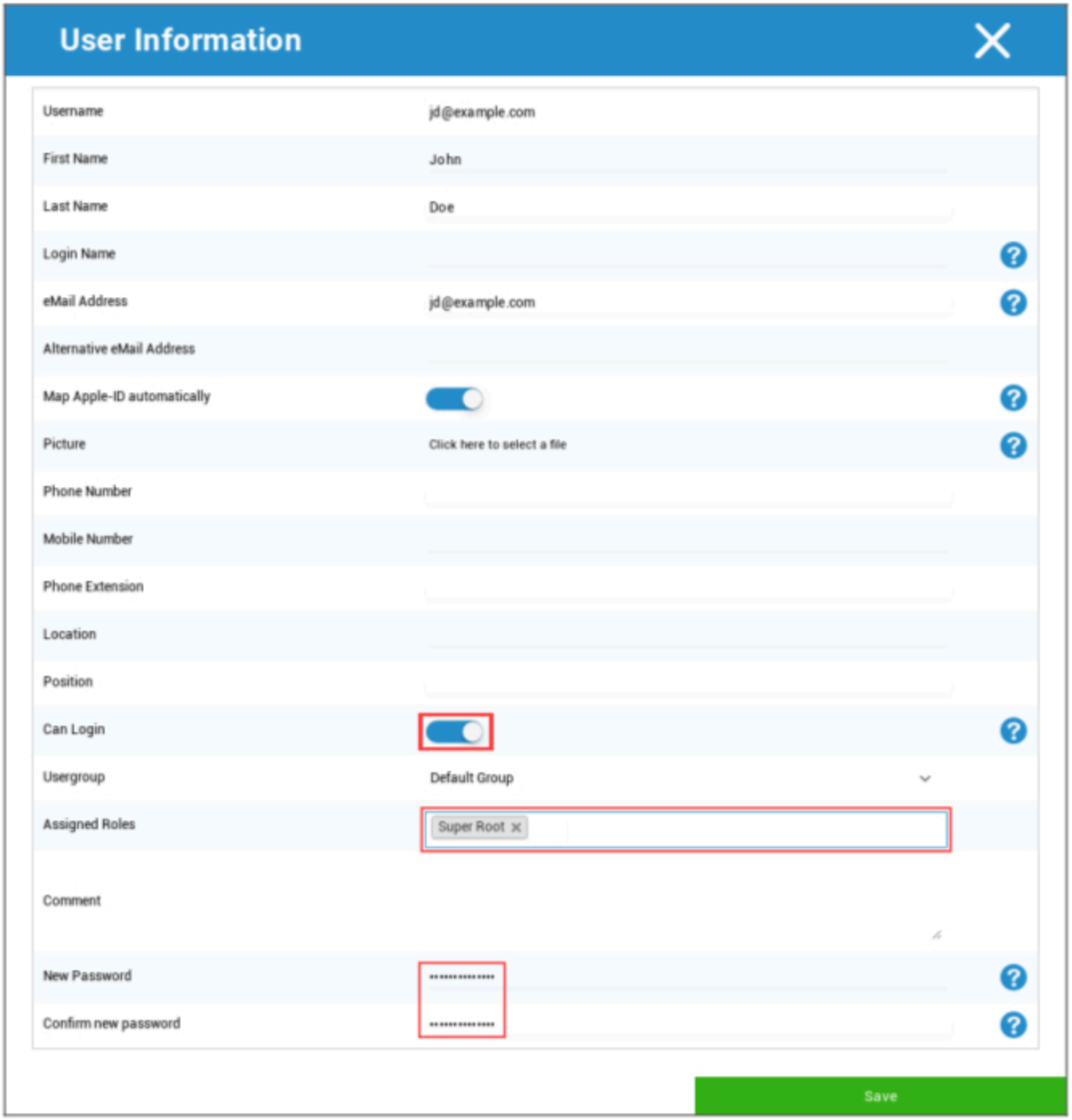
Vytvorenie nového administrátorského používateľa

Používateľa môžete nastaviť ako administrátora. Tým mu dáte oprávnenia na prihlásenie do konzoly a tiež na zmenu používateľov/skupín/zariadení.

Vytvorte bežného používateľa alebo použite existujúceho používateľa. Vyberte User (Používateľa), ktorému chcete udeliť administrátorské oprávnenia, kliknite na koliesko a vyberte "Edit User" (Upraviť používateľa):



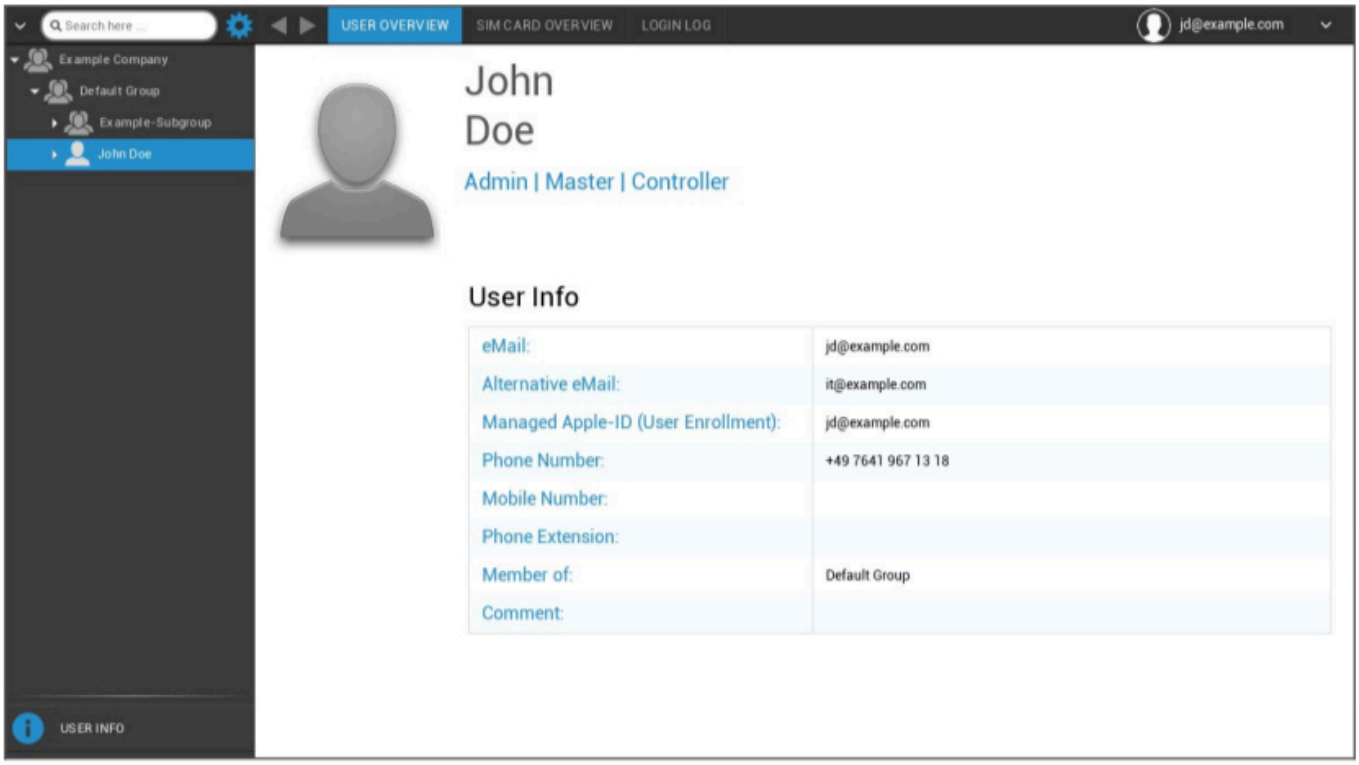
Aktivujte prepínač "Can Login", priraďte používateľovi rolu "Super-Root" a nastavte heslo.



Uložte to a používateľ sa teraz môže prihlásiť pomocou používateľského mena a hesla.

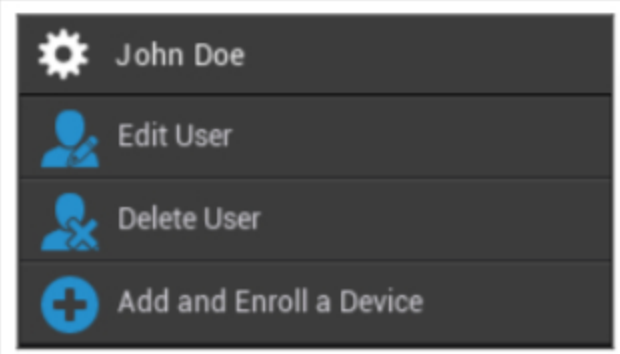
Správa používateľov v mobilnej správe

Keď vyberiete určitého používateľa, zobrazí sa nasledujúci prehľad:



Zobrazí sa prehľad všetkých informácií, ktoré ste predtým zadali v časti "Vytvoriť používateľa".

Pomocou zariadenia, ktoré je nainštalované v hornej časti, môžete vykonať nasledujúce konfigurácie:



Meno používateľa	Používateľské meno vybraného používateľa
Upraviť používateľa	Úprava informácií o používateľovi
Odstránenie používateľa	Odstránenie používateľa • Odstrániť zo systému = zariadenie bude odstránené z AppTec

	• Wipe & Delete = zariadenie sa obnoví do továrenských nastavení a odstráni sa z AppTecu
Pridanie a registrácia zariadenia	Zapísať zariadenie pre vybraného používateľa

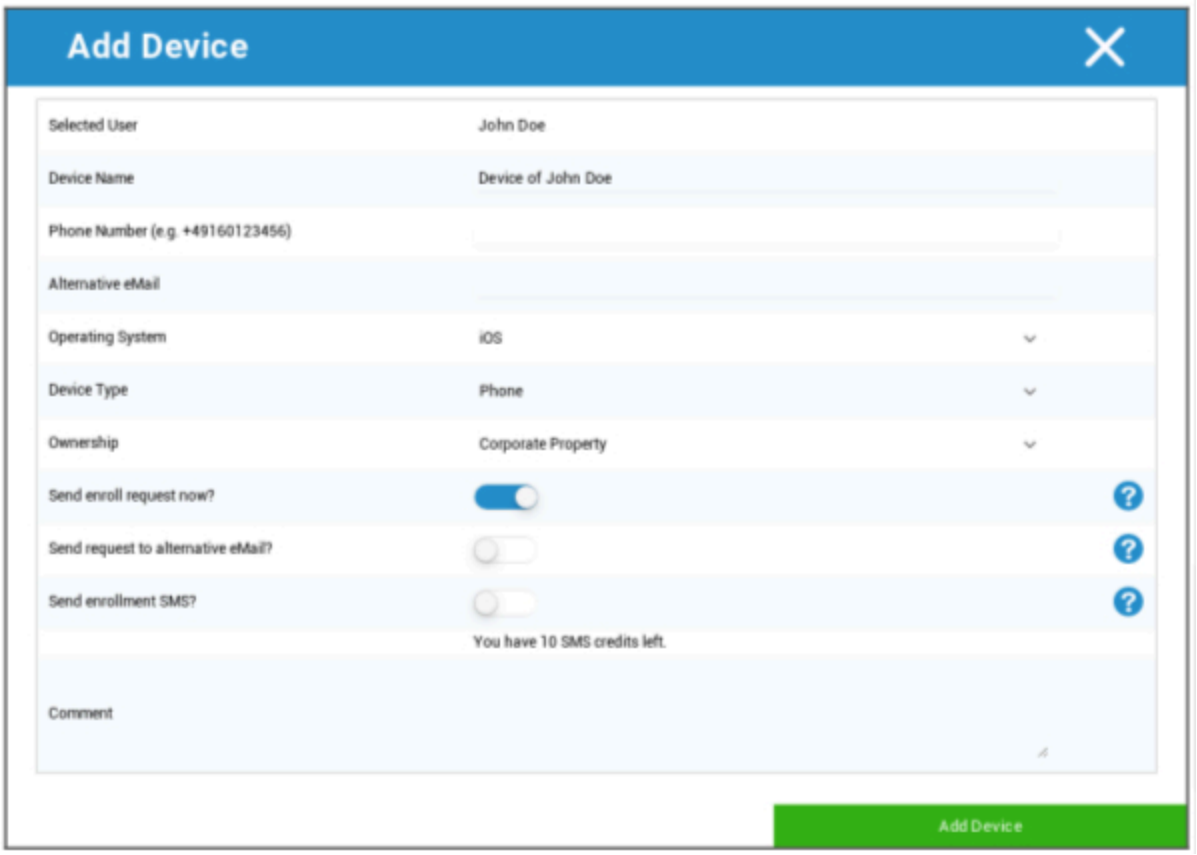
Upozorňujeme, že administrátorský prístup môže byť v hierarchickej štruktúre podaný aj ako lokálny používateľský účet. Bez založenia ďalšieho administrátora by sa tento nemal vymazať!

Pridanie a registrácia zariadenia

Tu môžete vybrať zariadenie pre vybrané použitie.

Prípadne môžete zariadenia do skupiny zaregistrovať priamo. Ak to chcete urobiť, kliknite na skupinu, kliknite na koliesko a vyberte možnosť "Pridať a zapísať zariadenie".

Mal by sa zobraziť nasledujúci prehľad:



V závislosti od druhu zariadenia, ktoré chcete zaregistrovať, musíte vykonať nasledujúce konfigurácie:

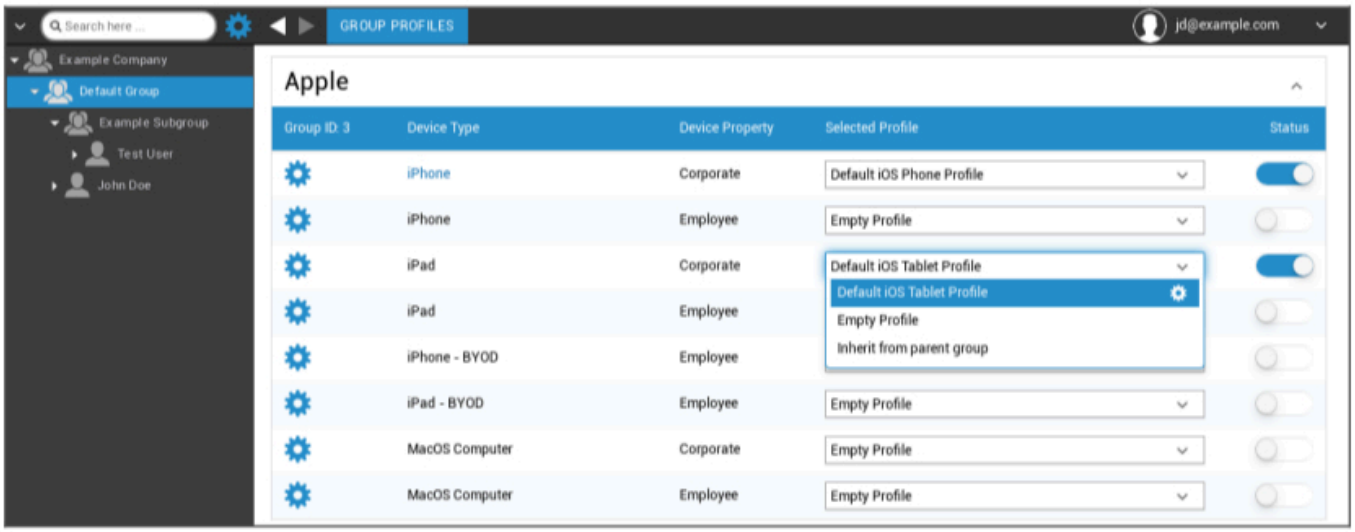
Vybraný používateľ	Vybraný používateľ (vyplní sa automaticky)
Názov zariadenia	Vyplní sa automaticky (zariadenie pre "meno používateľa") - možno ho však zmeniť
Telefónne číslo	Telefónne číslo sa vyplní automaticky (pokiaľ ho používateľ zadal) - tu ho však môžete pridať alebo zmeniť.
Alternatívna elektronická pošta	Alternatívny e-mail, vyplní sa automaticky (pokiaľ ho zadal používateľ) - tu ho však môžete pridať alebo zmeniť
Vlastník zariadenia	Firemný majetok = firemné zariadenie Majetok zamestnanca = zariadenie BYOD
Zvoľte systém prevádzky	Tu si môžete vybrať z nasledujúcich operačných systémov: • iOS • iOS BYOD (registrácia používateľov) • MacOS • Android Enterprise • Android • Windows Mobile • Windows 10
Odoslať žiadosť o zápis?	E-mail sa okamžite odošle na hlavnú e-mailovú adresu a používateľ je vyzvaný, aby pripojil svoje zariadenie.
Odoslať žiadosť na alternatívny e-mail?	Odoslať e-mail dodatočne alebo výlučne (v prípade, že možnosť "Odoslať žiadosť o zápis?" bola deaktivovaná) na alternatívnu e-mailovú adresu (e-mail sa líši od "normálneho" e-mailu so žiadosťou o zápis)
Odoslať registračnú SMS?	Odoslanie žiadosti o registráciu prostredníctvom SMS (je potrebné zadať "telefónne číslo")

Po odoslaní žiadosti o registráciu sa zariadenie ihneď zobrazí (označené červenou farbou).

Hneď po úspešnom pripojení sa zariadenie označí zelenou farbou, čím je pripravené na prijímanie obmedzení, aplikácií atď.

Správa profilov v mobilnej správe

Po kliknutí na skupinu sa zobrazí prehľad všetkých platforiem zariadení, ktoré sa majú konfigurovať, a príslušných priradených profilov.



	Vykonanie konfigurácie pre vybraný profil
Typ zariadenia	Typ a/alebo model zariadenia
Vlastnosť zariadenia	Vlastník zariadenia (firemný = majetok firmy, zamestnanec = súkromné zariadenie zamestnanca)
Vybraný profil	Vybraný profil (ozubené koliesko otvorí dialóg konfigurácie profilu)
Stav	Zapnuté/vypnuté (profil je aktivovaný/deaktivovaný)

Po výbere prevodovky sa zobrazia tieto možnosti:

Vytvorenie profilu

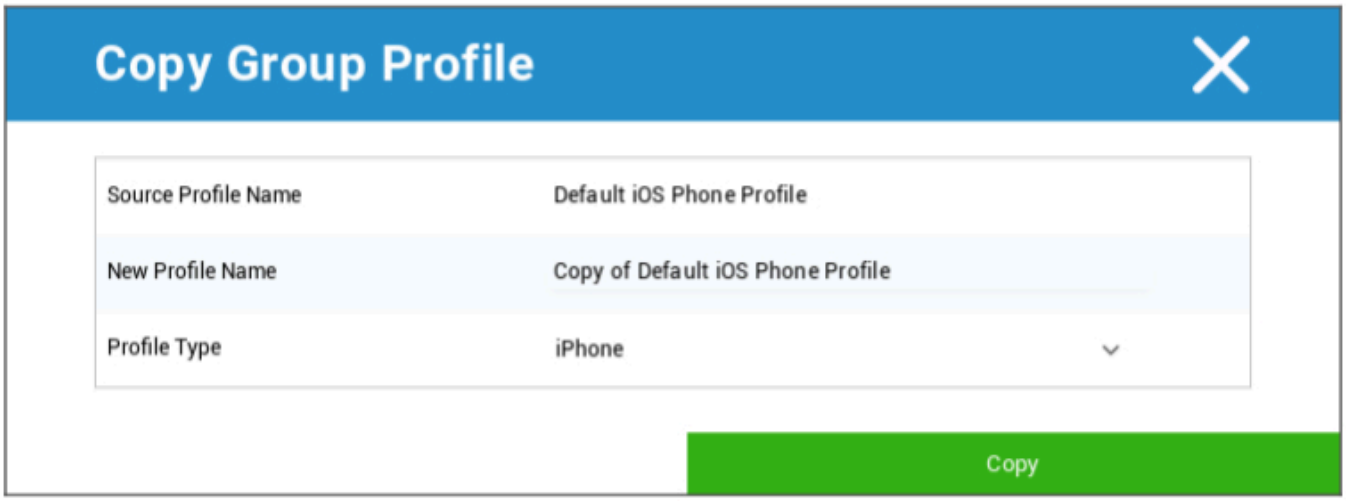
Pre každú položku a/alebo platformu môžete vytvoriť a nakonfigurovať nový profil. Po kliknutí na tento podbod sa profil okamžite vytvorí a môžete hneď začať s konfiguráciou pre iOS, Android a Windows Phone.

Upraviť profil

Po kliknutí na "Upraviť profil" sa zobrazí konfigurácia príslušného profilu, kde môžete nastaviť konfigurácie.

Kopírovať profil

Pomocou funkcie "Kopírovať profil" môžete skopírovať nastavenia/konfigurácie z už existujúceho profilu a pridať ich do nového profilu.

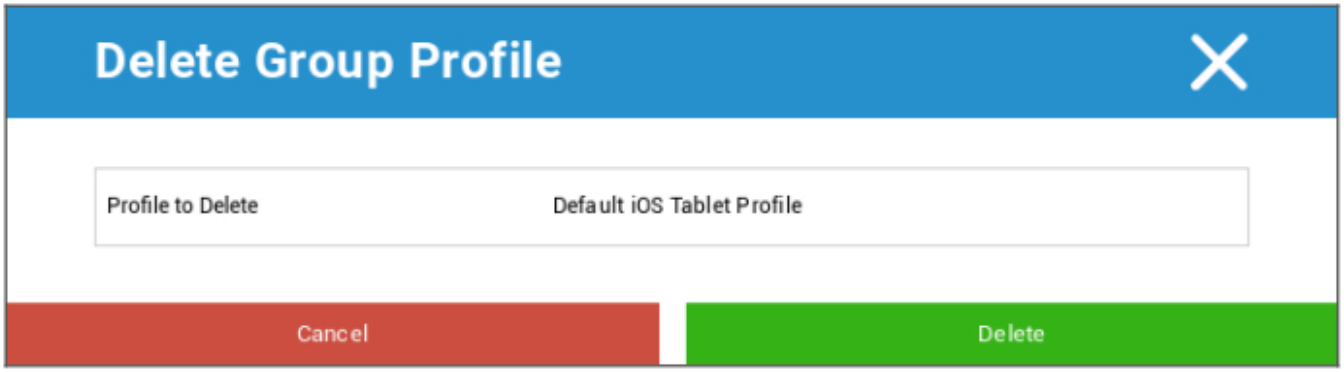


Názov profilu zdroja	Názov profilu, ktorý sa má skopírovať
Nový názov profilu	Názov nového profilu
Typ profilu	Typ profilu (telefón/tablet)

Po kliknutí na "Kopírovať" sa profil vytvorí a teraz ho môžete priradiť skupine.

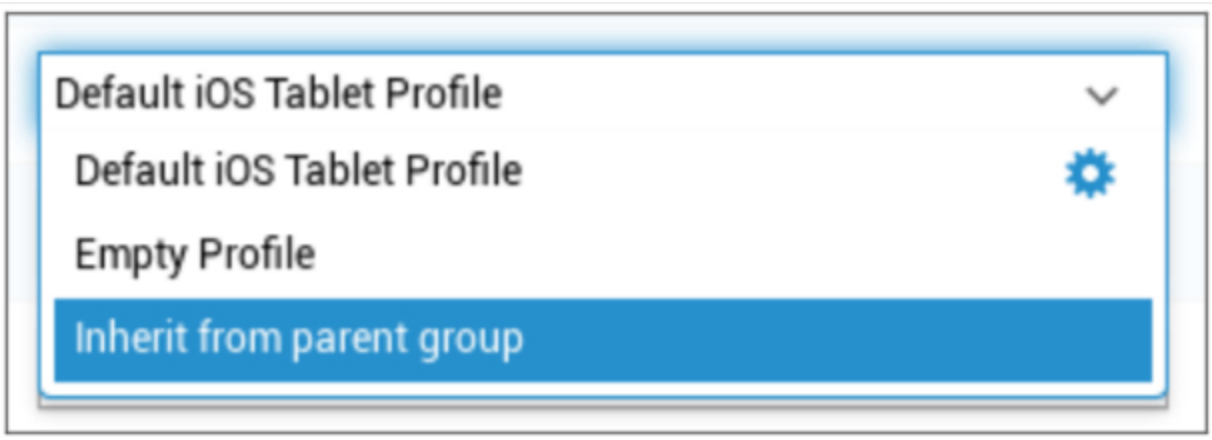
Odstránenie profilu

Tu môžete profil natrvalo vymazať. Upozorňujeme, že počas procesu vymazania a nasledujúceho procesu "Priradiť teraz" pre profil zmizne konfigurácia na príslušných zariadeniach dotknutej skupiny a nebude možné ju obnoviť!


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

Dedenie profilov

Počas výberu profilov je k dispozícii možnosť "Zdediť z nadradenej skupiny".



Po aktivácii profilu sa pre vybrané zariadenie (a príslušný typ zariadenia) použije profil nadradenej skupiny. Upozorňujeme tiež, že zmeny tohto profilu môžu mať vplyv na viaceré skupiny.

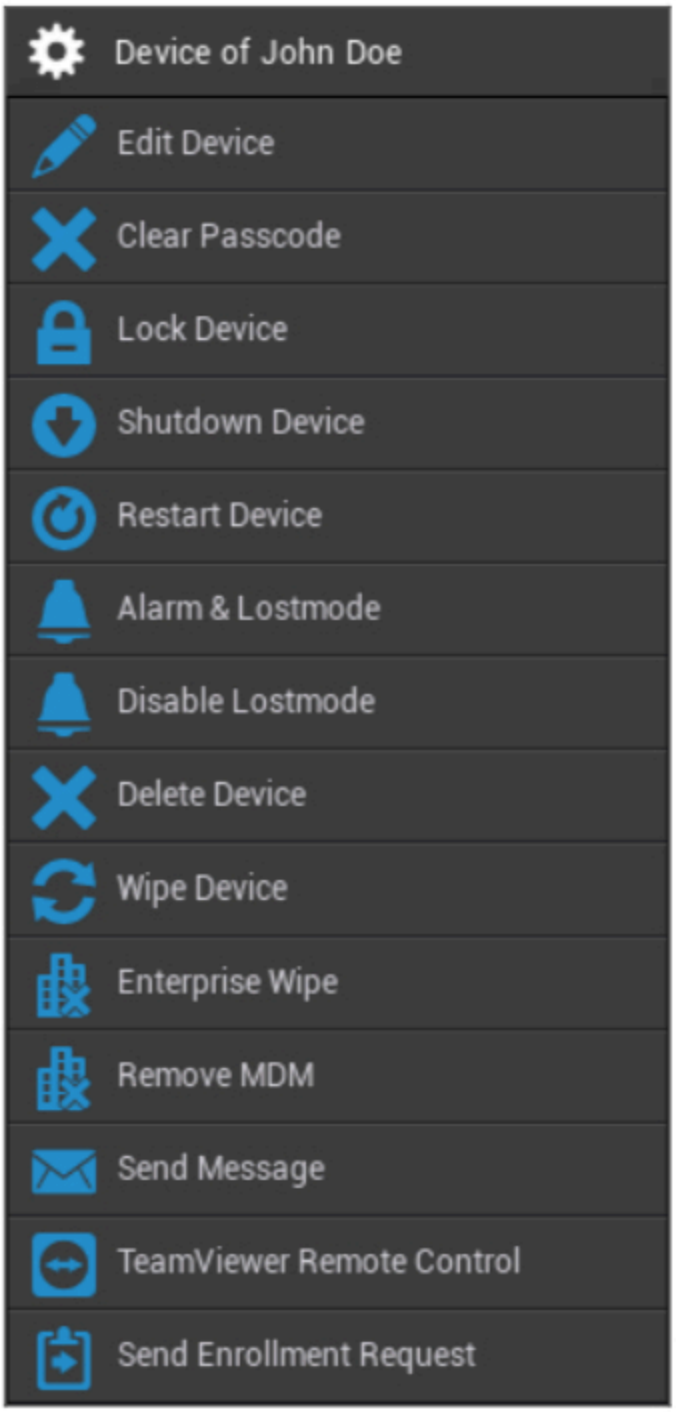
Táto konfigurácia sa nastaví ako predvolená hodnota pri vytvorení novej podskupiny.

K dispozícii je aj konfigurácia "Prázdny profil", ktorá zodpovedá prázdnemu profilu, čo znamená, že na zariadení koncového používateľa sa nakoniec nevykonajú žiadne nové konfigurácie.

Správa zariadení v mobilnej správe

Keď vyberiete zariadenie, môžete prostredníctvom "ozubeného kolesa" vykonávať rôzne úlohy. Tie sa líšia v závislosti od platforiem operačného systému (iOS, Android Enterprise, Android, Windows Mobile, Windows 10).

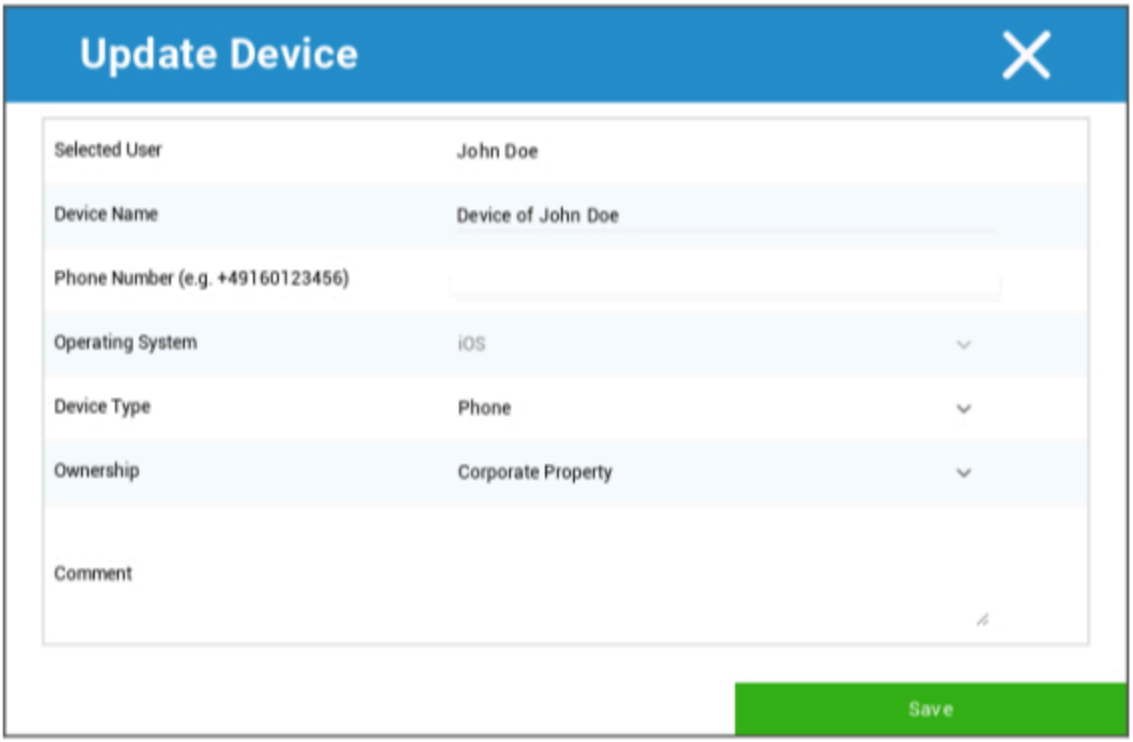
IOS



Upraviť zariadenie	Upraviť zariadenie
Vymazanie prístupového kódu	Prístupový kód zariadenia sa vymaže
Zariadenie na uzamknutie	Uzamknutie zariadenia (uzamknutie obrazovky)

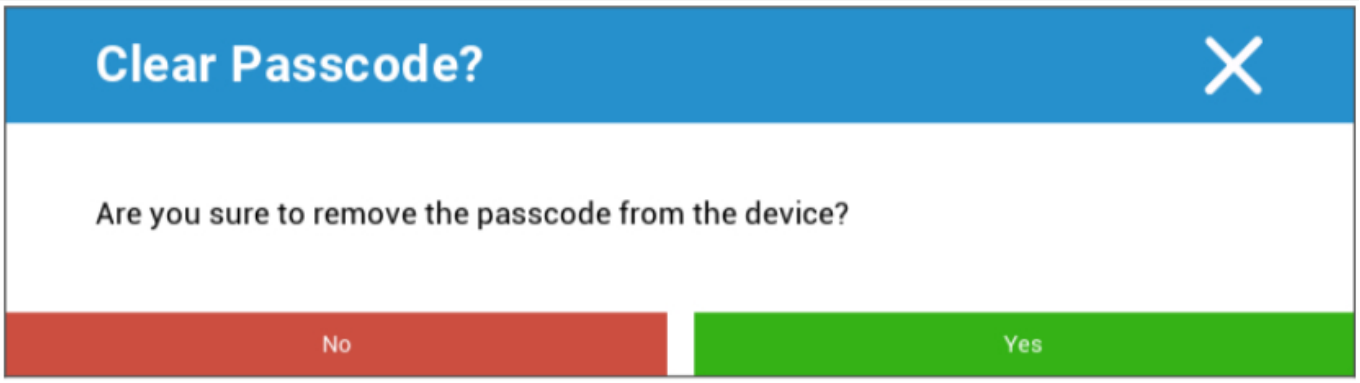
Zariadenie na vypnutie	Zariadenie na vypnutie
Reštartovanie zariadenia	Reštartovanie zariadenia
Alarm & Lostmode	Spustenie alarmu a režimu Lostmode
Zakázanie režimu Lostmode	Zakázanie režimu Lostmode
Odstrániť zariadenie	Odstránenie zariadenia z aplikácie AppTec
Zariadenie na utieranie	Obnovenie výrobných nastavení zariadenia
Podnik Wipe	Informácie, aplikácie a profily poskytnuté AppTec360 sú vymazané (zariadenie je oddelené od MDM)
Odstránenie MDM	
Odoslať správu	Odosielanie oznámení Push do zariadenia Správa sa zobrazí v aplikácii AppTec360 (karta Správa)
Vzdialené ovládanie TeamViewer	Spustenie relácie vzdialeného ovládania pomocou programu TeamViewer
Odoslať žiadosť o zápis	Odoslanie (opakovanej) žiadosti o zápis

Upraviť zariadenie



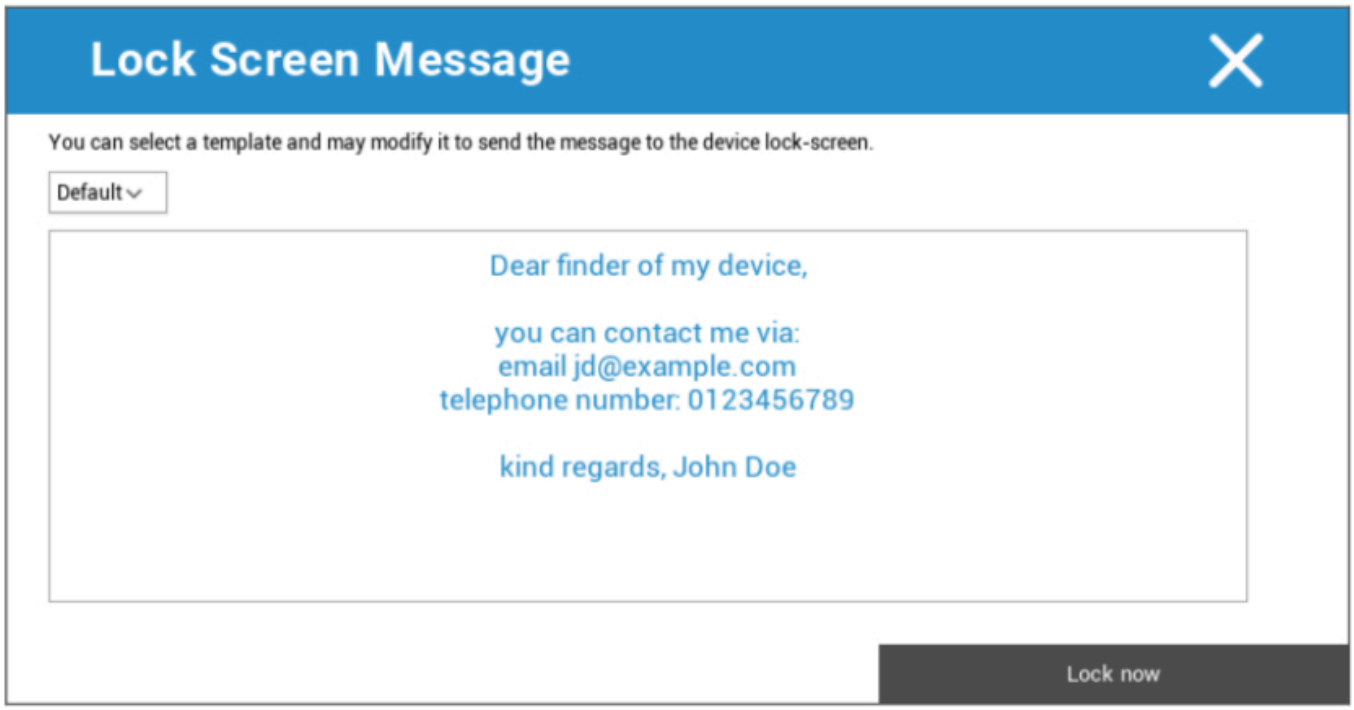
Tu môžete aktualizovať rôzne informácie o zariadení.

Vymazanie prístupového kódu



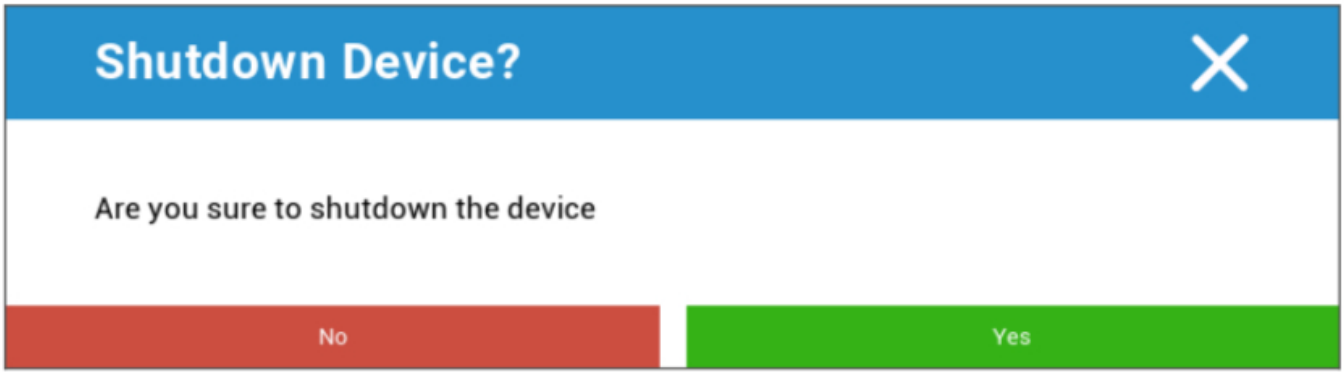
V časti "Vymazať prístupový kód" môžete na diaľku odstrániť prístupový kód zo zariadenia. Následne bude používateľ vyzvaný na zadanie nového hesla (v závislosti od pokynov pre prístupový kód).

Zariadenie na uzamknutie



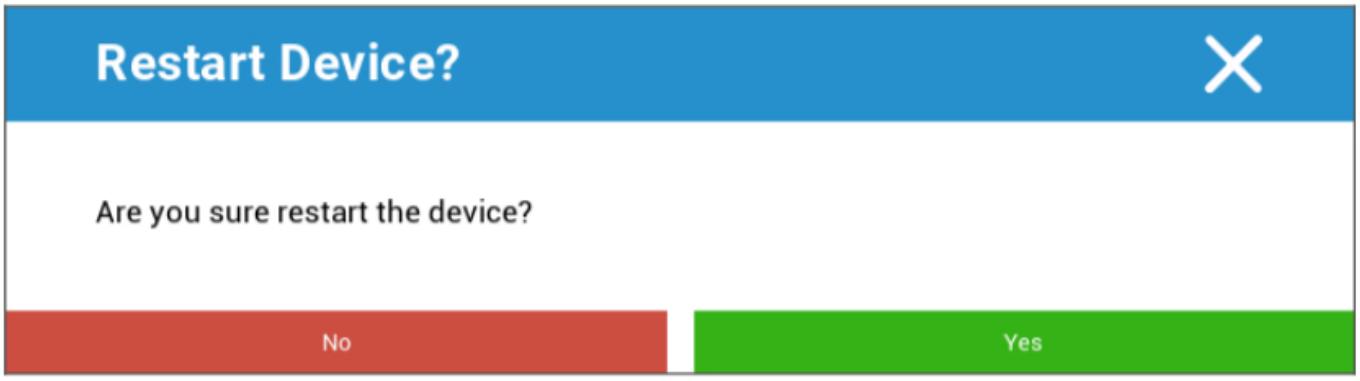
V tomto prípade sa do koncového používateľského zariadenia (uzamknutá obrazovka) odošle príkaz na uzamknutie.

Zariadenie na vypnutie



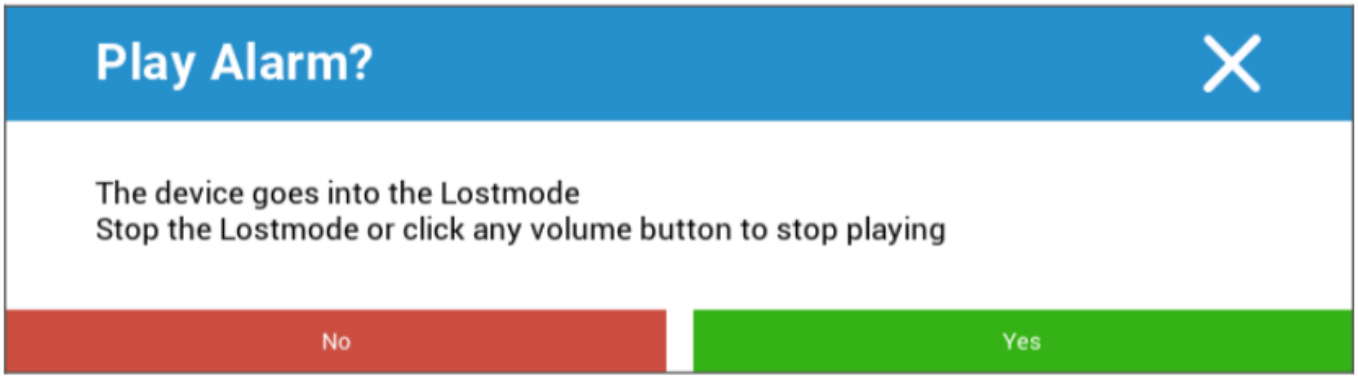
Tu sa koncovému používateľskému zariadeniu odošle príkaz na vypnutie.

Reštartovanie zariadenia

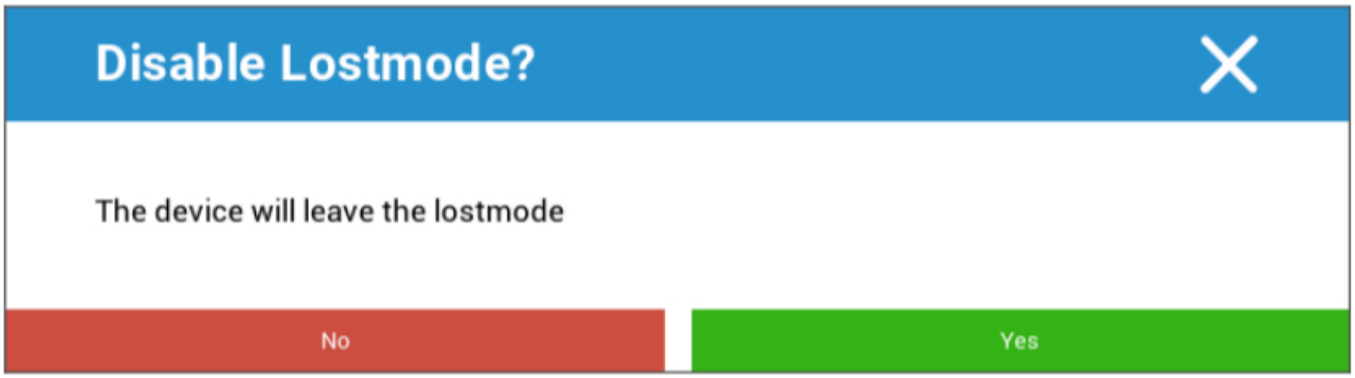


Tu sa koncovému používateľskému zariadeniu odošle príkaz na reštart.

Alarm a stratový režim | Zakázať stratový režim



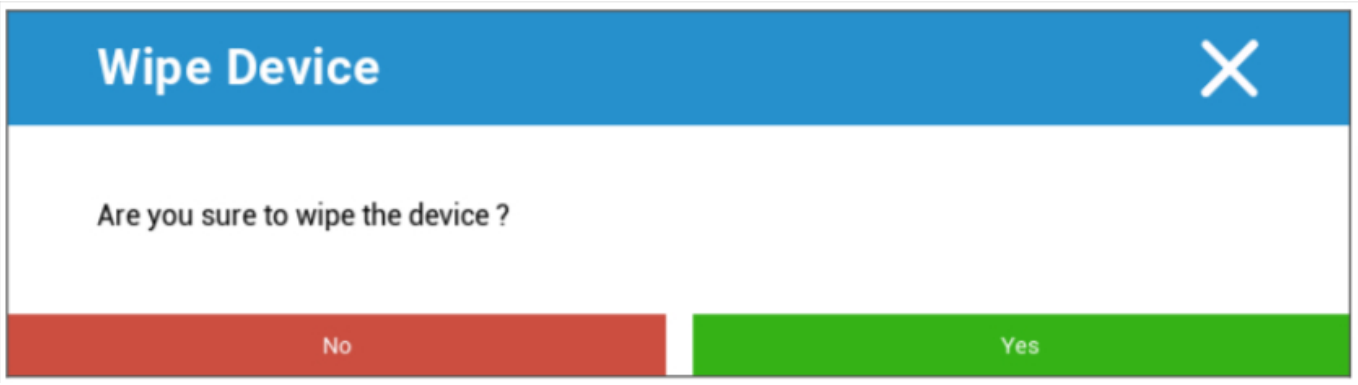
Tu môžete zariadenie nastaviť do režimu Lostmode, ktorý nastaví zariadenie na neustále prehrávanie zvuku budíka. Režim Lostmode možno zastaviť stlačením ľubovoľného tlačidla hlasitosti zariadenia alebo na diaľku kliknutím na položku "Disable Lostmode" (Zakázať režim Lostmode):



Odstrániť zariadenie

Tu je možné vykonať príkaz na odstránenie. Opäť sa môžete rozhodnúť, či má byť zariadenie odstránené len z AppTec360 ("Delete from System") alebo či má byť zariadenie odstránené z AppTec360 a zároveň obnovené do továrenského nastavenia ("Wipe & Delete").

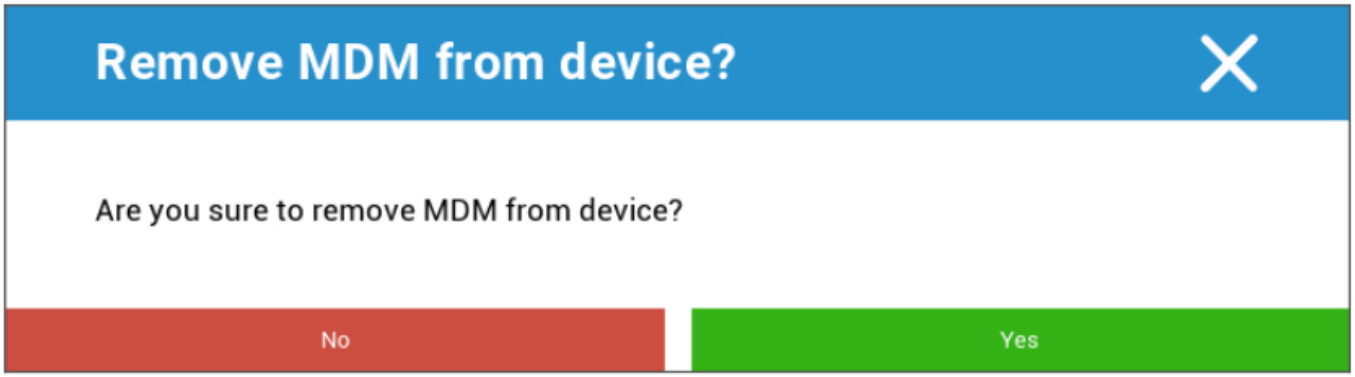
Zariadenie na utieranie



V časti "Vymazať zariadenie" môžete vykonať úplné vymazanie zariadenia. Zariadenie sa obnoví na svoje výrobné nastavenia.

Vyčistenie podniku | Odstrániť MDM

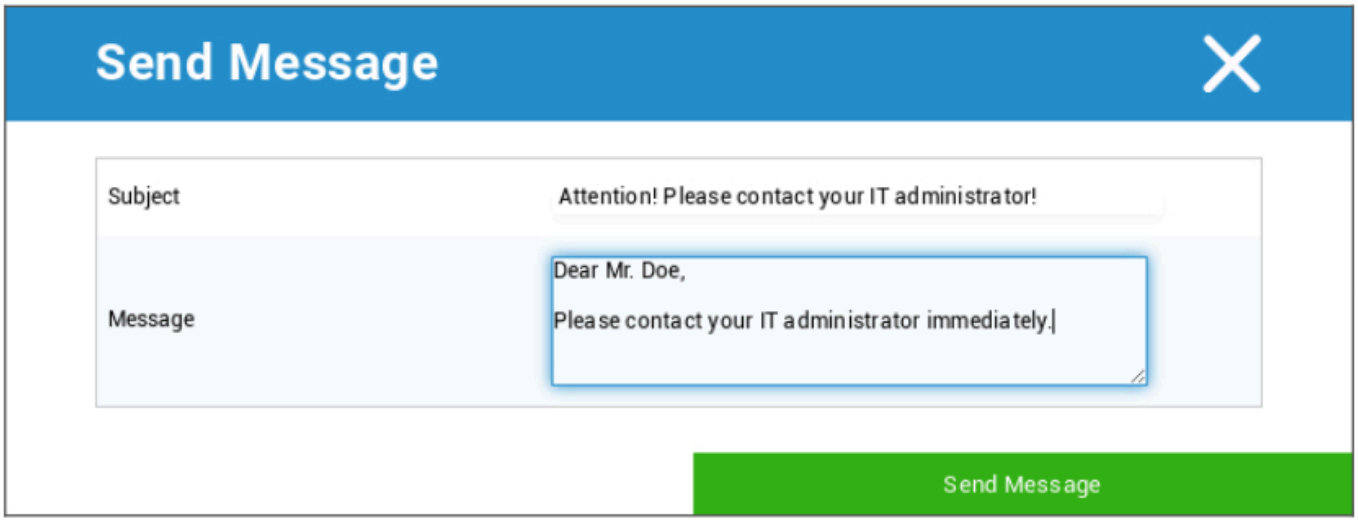
Vymazané sú len informácie, aplikácie a profily poskytnuté spoločnosťou AppTec360. Týmto spôsobom už nebudú podnikové údaje dostupné v zariadení koncového používateľa. Súkromná oblasť nie je ovplyvnená a naďalej zostáva v zariadení koncového používateľa.



Pomocou funkcie "Odstrániť MDM" môžete odstrániť profil MDM na zariadení koncového používateľa a všetky ostatné položky poskytnuté spoločnosťou AppTec.

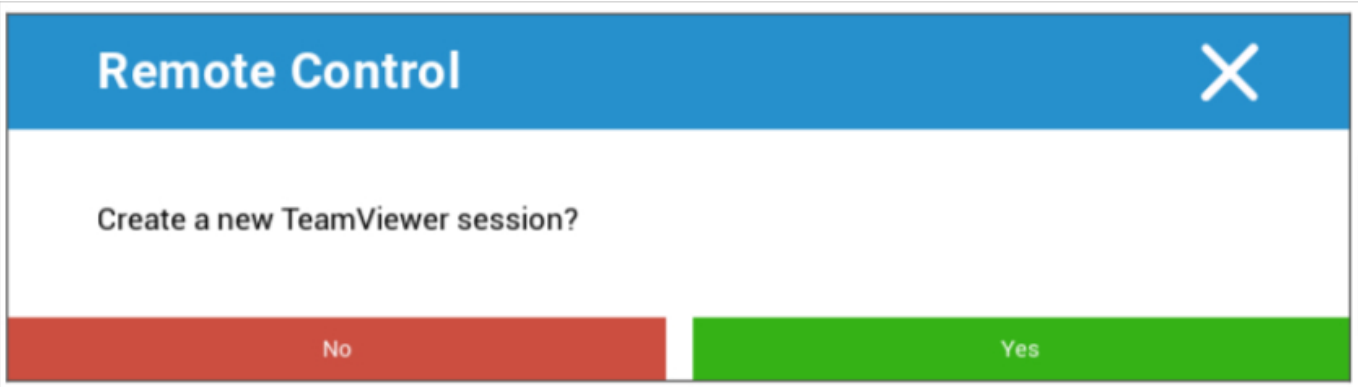
Tento príkaz vykoná rovnakú akciu ako príkaz "Enterprise Wipe".

Odoslať správu



Tu môžete poslať oznámenie Push do príslušného zariadenia.

Vzdialené ovládanie TeamViewer



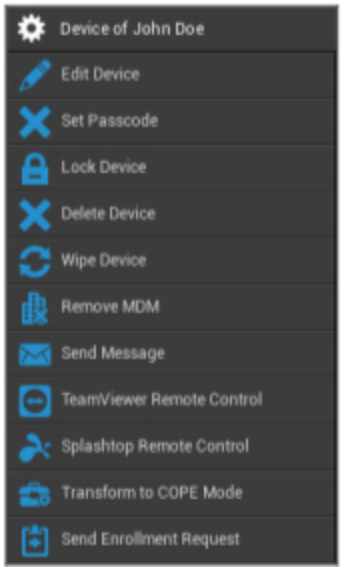
Tu môžete spustiť reláciu vzdialeného ovládania programu Teamviewer.

Odoslať žiadosť o zápis

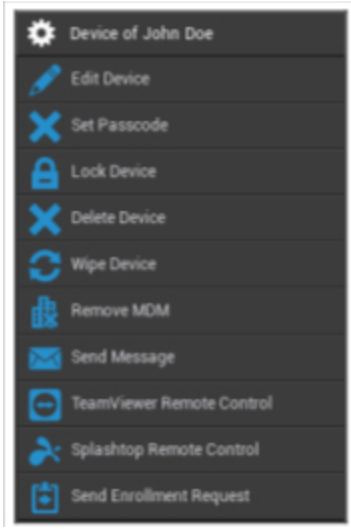
Pomocou položky "Odoslať žiadosť o registráciu" môžete príslušnému používateľovi (opäť) odoslať žiadosť o registráciu.

Android

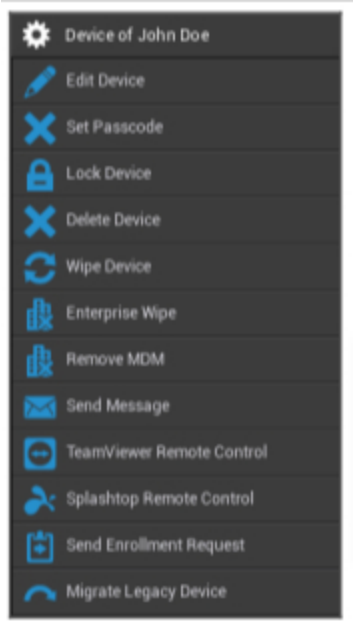
AE Plne spravované zariadenie (Work Managed)



Pracovný profil AE (kontajner)



Telefón so systémom Android | Tablet

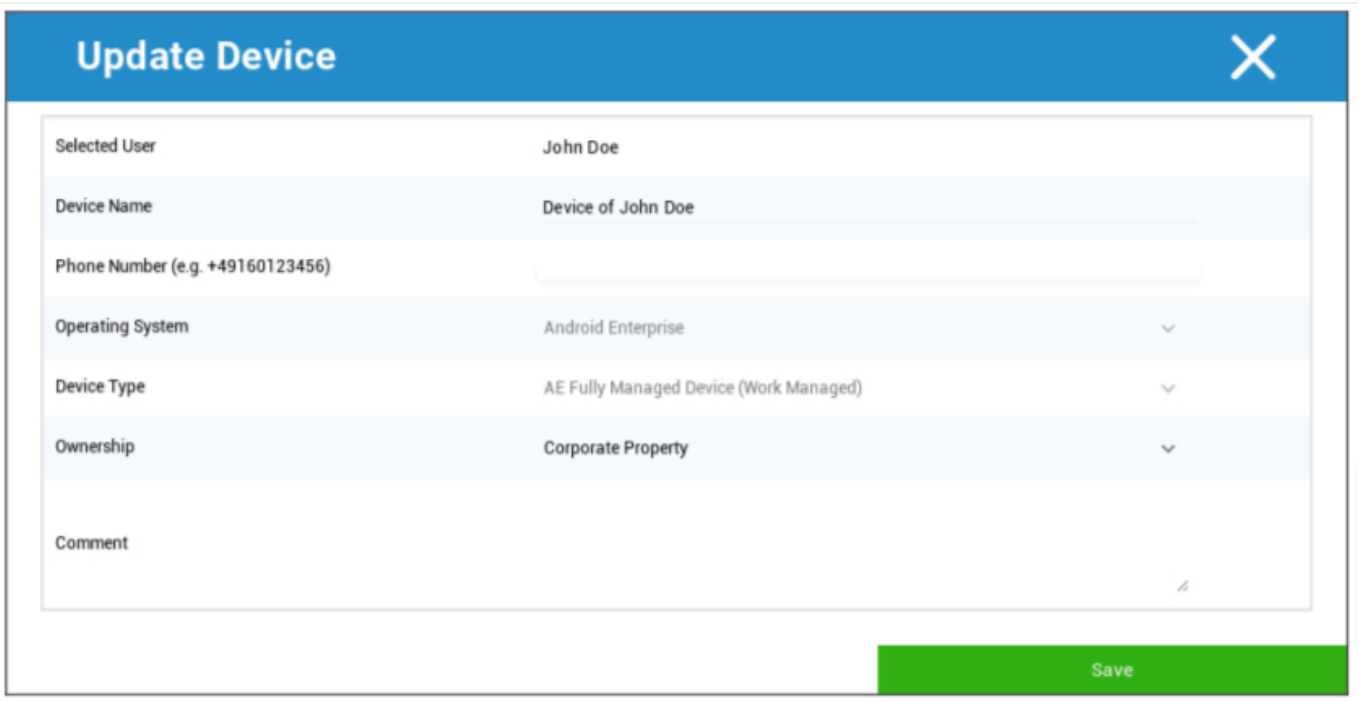


Upraviť zariadenie	Úprava informácií o zariadení
Nastavenie prístupového kódu	Nastavenie prístupového kódu zariadenia
Zariadenie na uzamknutie	Uzamknutie zariadenia (uzamknutie obrazovky)
Odstrániť zariadenie	Odstránenie zariadenia z AppTec
Zariadenie na utieranie	Obnovenie výrobných nastavení zariadenia
Podnik Wipe	Informácie, aplikácie, profily, ktoré poskytuje AppTec360, sú vymazané (zariadenie bude oddelené od MDM)
Odstránenie MDM	
Odoslať správu	Odosielanie oznámení Push do zariadenia Správa sa zobrazí v aplikácii AppTec360 (karta Správa)
Vzdialené ovládanie TeamViewer	Spustenie relácie vzdialeného ovládania pre toto zariadenie pomocou aplikácie TeamViewer
Diaľkové ovládanie Splashtop	Spustenie relácie diaľkového ovládania pre toto zariadenie pomocou aplikácie Splashtop
Transformácia do režimu COPE (iba v plne spravovanom zariadení AE (Work Managed))	Vytvorenie pracovného profilu na tomto plne spravovanom zariadení AE (Work Managed)

Odoslať žiadosť o zápis	Odoslanie (opakovanej) žiadosti o zápis
Migrácia staršieho zariadenia (iba v prípade telefónu/tabletu so systémom Android, ak je zaregistrovaný pomocou funkcie Device Owner Mode Provisioning)	Migrácia profilu telefónu/tabletu so systémom Android do profilu plne spravovaného zariadenia AE (pracovný profil)

Upraviť zariadenie

Tu môžete aktualizovať rôzne informácie o zariadení.



Vybraný používateľ	Používateľ zariadenia
Názov zariadenia	Názov zariadenia
Telefónne číslo	Telefónne číslo zariadenia
Operačný systém	Android Enterprise Android
Typ zariadenia	Android Enterprise: • AE Plne spravované zariadenie (Work Managed) • Režim pracovného profilu AE (iba kontajner) • AE Plne spravované zariadenie s pracovným profilom (COPE) Android: • Telefón • Tablet
Vlastníctvo	Corporate = majetok spoločnosti

	Employee = vlastnosť zamestnanca
Komentár	Ďalšie popisy zariadenia

Vymazanie prístupového kódu

Tu môžete odstrániť prístupový kód zariadenia na vybranom zariadení. V predvolenom nastavení systému Android je prístupový kód nastavený na hodnotu "123456" - používateľ ho môže a mal by ho neskôr zmeniť.

Zariadenie na uzamknutie

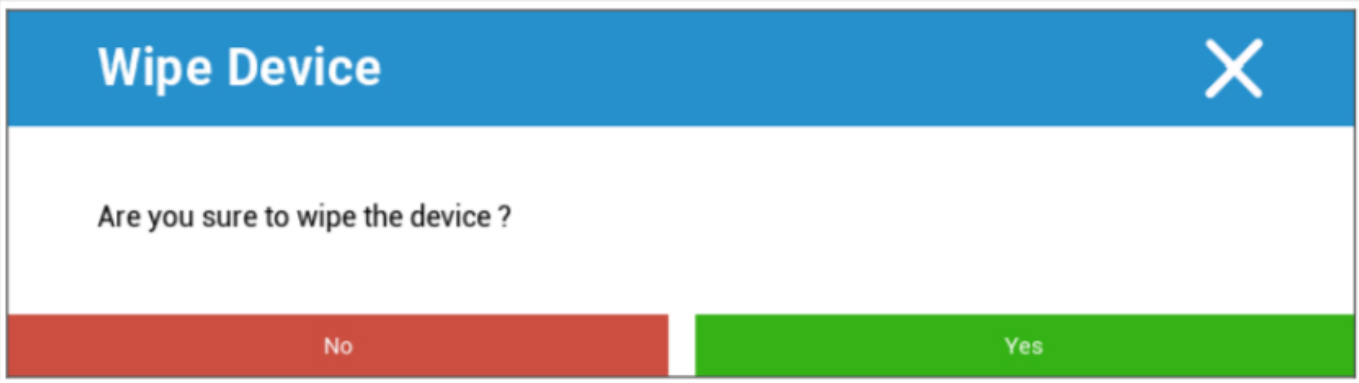
Tu sa do zariadenia odošle príkaz na uzamknutie zariadenia (uzamknutie obrazovky).

Odstrániť zariadenie

Tu je možné vykonať príkaz na vymazanie. Opäť sa môžete rozhodnúť, či sa má zariadenie odstrániť len z AppTec360 ("Odstrániť zo systému"), alebo či sa má zariadenie odstrániť z AppTec360 a dodatočne obnoviť na výrobné nastavenia ("Vymazať a odstrániť").

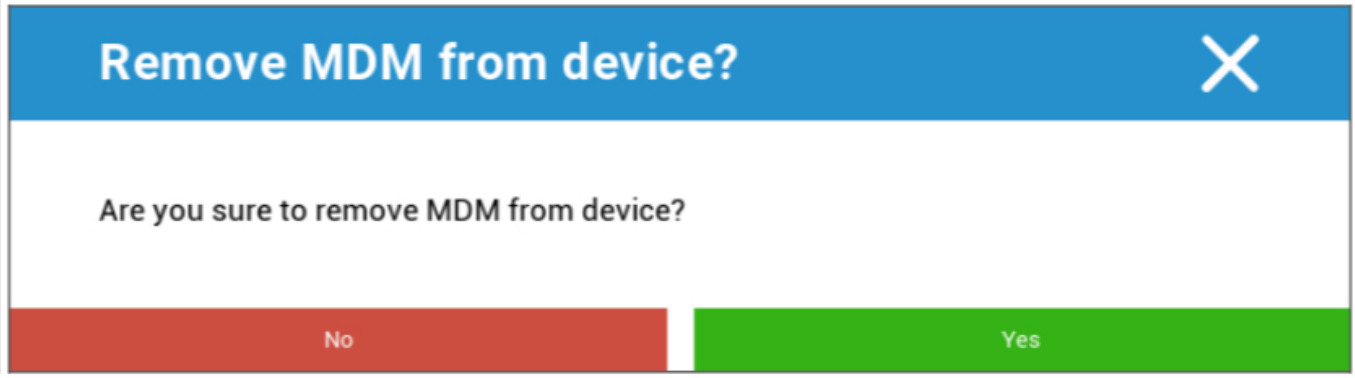
Zariadenie na utieranie

V časti "Vymazať zariadenie" môžete vykonať úplné vymazanie zariadenia. Zariadenie sa potom obnoví do továrenských nastavení.



Okrem toho, ak zariadenie obsahuje kartu SD, môžete kartu SD vymazať. Môžete to dosiahnuť nastavením položky "Wipe SD Card too? " na možnosť "Zapnuté".

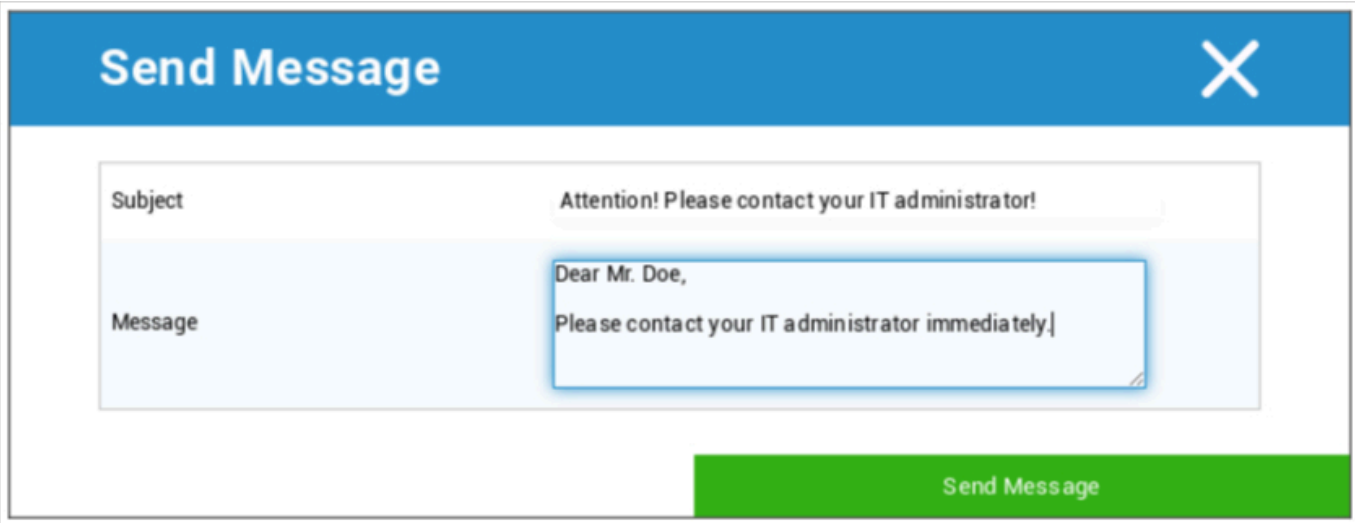
Odstránenie MDM



Toto je odporúčaná metóda na vytvorenie oddelenia od MDM.

Vymažú sa len informácie, aplikácie a profily poskytnuté spoločnosťou AppTec360, čo znamená, že všetky firemné údaje už nebudú v zariadení koncového používateľa k dispozícii. Súkromná sféra však nie je ovplyvnená a naďalej zostáva v zariadení koncového používateľa.

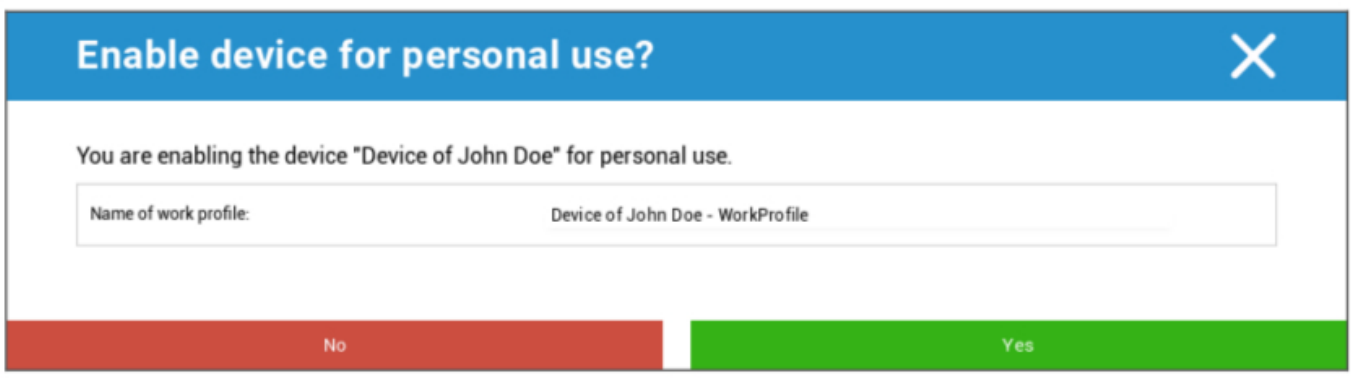
Odoslať správu



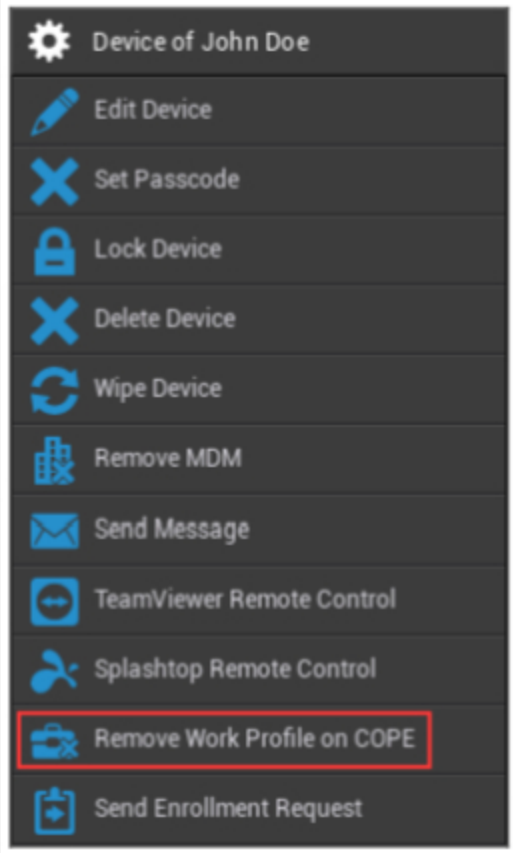
Tu môžete odoslať oznámenie Push do príslušného zariadenia koncového používateľa.

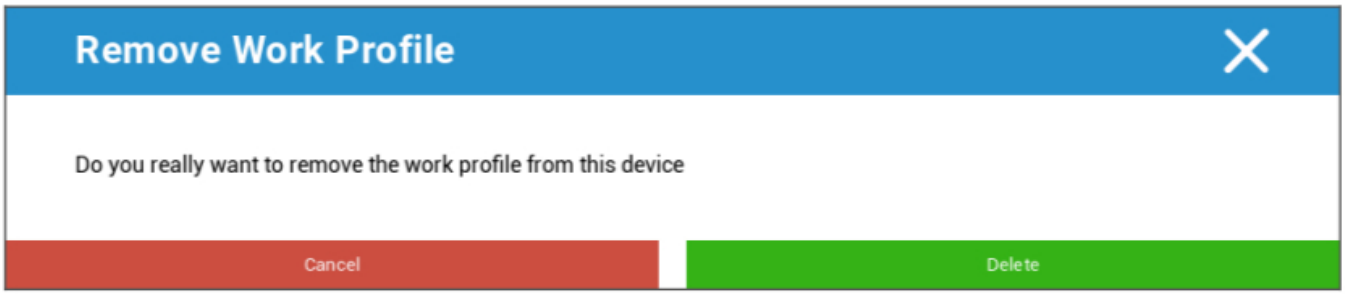
Transformácia do režimu COPE

Vytvorenie pracovného profilu na tomto plne spravovanom zariadení AE (Work Managed)



Po transformácii zariadenia do režimu COPE môžete pracovný profil odstrániť kliknutím na možnosť **Odstrániť pracovný profil na COPE**:




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

Odoslať žiadosť o zápis

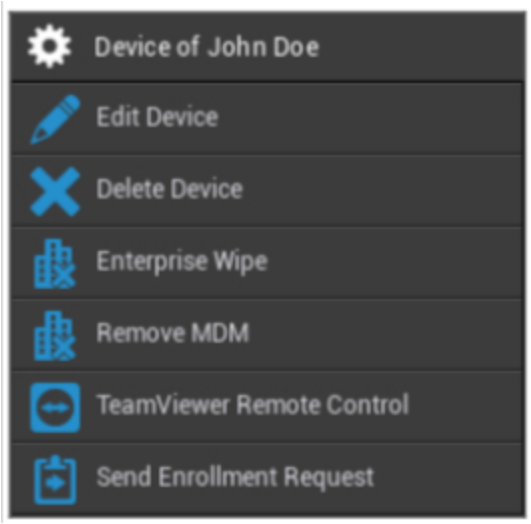
Pomocou položky "Odoslať žiadosť o registráciu" môžete príslušnému používateľovi (opäť) odoslať žiadosť o registráciu.

Upozorňujeme, že platná je len najnovšia žiadosť o zápis.

Migrácia staršieho zariadenia

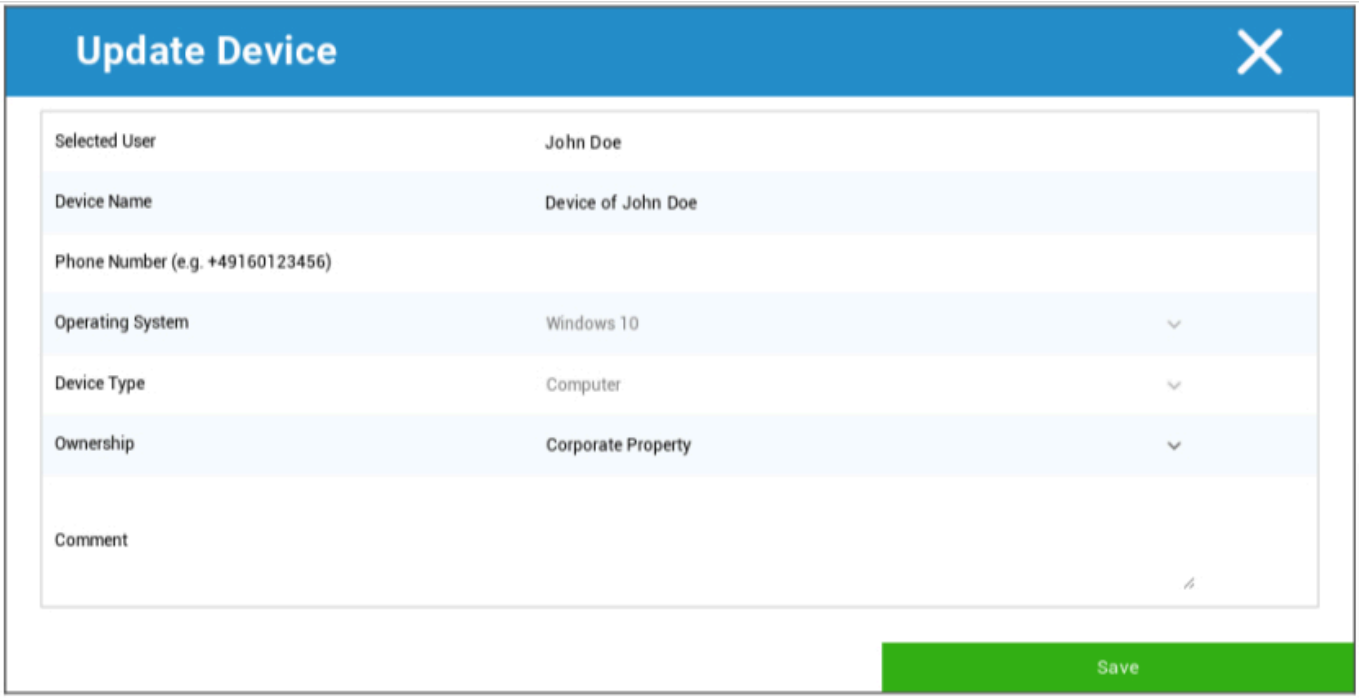
Migrácia profilu telefónu/tabletu so systémom Android do profilu plne spravovaného zariadenia AE (pracovný profil)

Windows



Názov zariadenia	Názov vybraného zariadenia
Upraviť zariadenie	Upraviť zariadenie
Odstrániť zariadenie	Odstránenie zariadenia z aplikácie AppTec
Podnik Wipe	Informácie, aplikácie a profil poskytované spoločnosťou AppTec360 sú vymazané
Odstránenie MDM	
Vzdialené ovládanie TeamViewer	Vzdialené ovládanie zariadenia pomocou aplikácie TeamViewer
Odoslať žiadosť o zápis	Odoslanie žiadosti o registráciu (znova)

Upraviť zariadenie

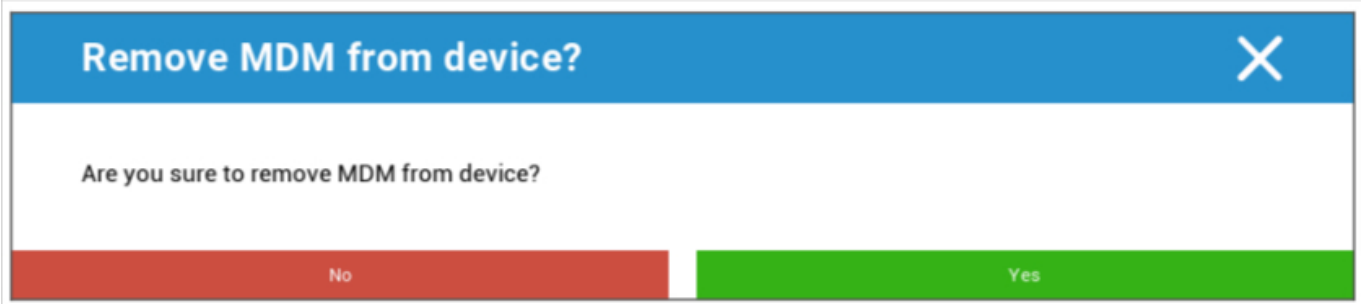


Tu môžete aktualizovať rôzne informácie o zariadení.

Odstrániť zariadenie

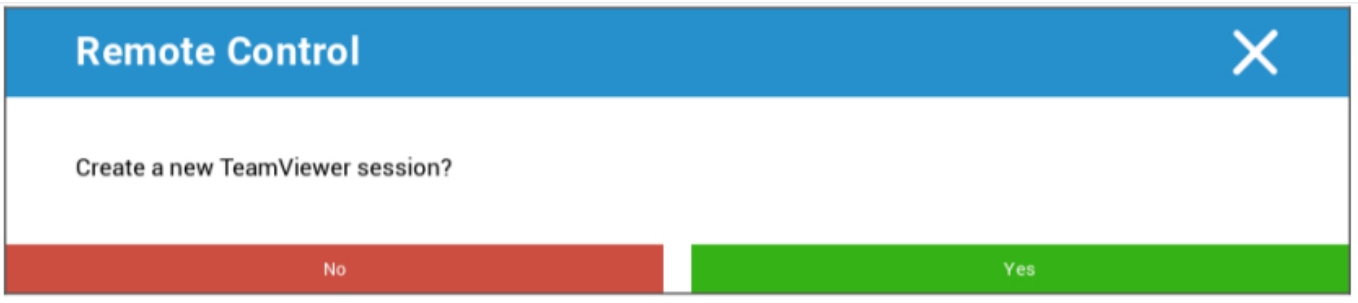
Tu je možné vykonať príkaz na odstránenie, ktorý iba odstráni zariadenie z AppTec360.

Vyčistenie podniku | Odstrániť MDM



Vymazané sú len informácie, aplikácie a profily poskytnuté spoločnosťou AppTec360. Týmto spôsobom už nebudú podnikové údaje dostupné v zariadení koncového používateľa. Súkromná oblasť nie je ovplyvnená a naďalej zostáva v zariadení koncového používateľa.

Vzdialené ovládanie TeamViewer



Tu môžete spustiť reláciu vzdialeného ovládania TeamViewer pre toto zariadenie.

Odoslať žiadosť o zápis

Pomocou položky "Odoslať žiadosť o registráciu" môžete príslušnému používateľovi (opäť) odoslať žiadosť o registráciu.

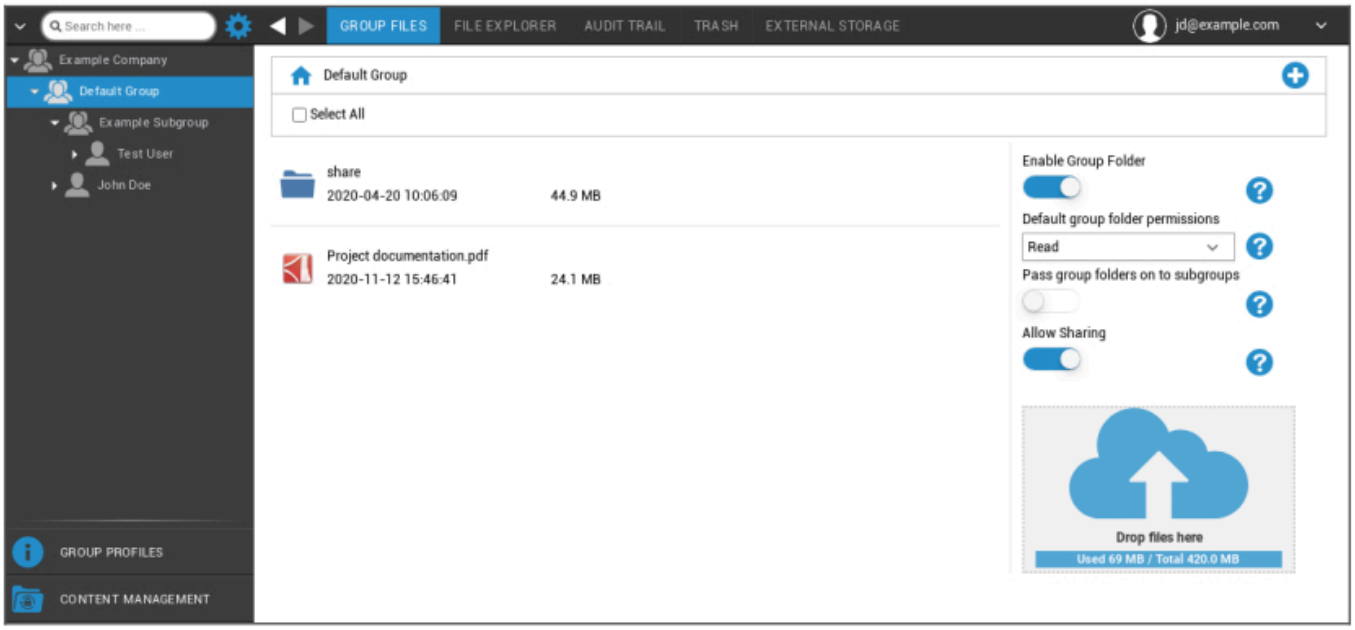
Správa obsahu

Keď ste v skupine, môžete spravovať aplikáciu AppTec ContentBox pomocou funkcie "Správa obsahu".

Pomocou Content Boxu môžete bezpečne distribuovať dokumenty a iné podnikové údaje do zariadení koncových používateľov.

Skupinové súbory

"Skupinové súbory" predstavujú základnú časť ContentBox. Tu môžete vytvárať nastavenia, nahrávať dokumenty, vytvárať nové priečinky atď.



Pomocou symbolu v pravom hornom rohu môžete vytvárať nové priečinky, ktoré sú určené do príslušnej skupiny pomocou "Pridať priečinok".

Pomocou symbolu v pravom hornom rohu môžete vytvoriť nový priečinok prostredníctvom položky "Pridať priečinok", ktorý by mal byť priradený k príslušnej skupine.

Priečinok môžete pomenovať ľubovoľne.

Prostredníctvom položky "Nahrať súbory" môžete nahrať údaje. Tu sa otvorí váš prehliadač Standard-Explorer. Tieto dve akcie môžete samozrejme vykonať v každom (pod)priečinku.

Pomocou symbolu v ľavom hornom rohu sa môžete vrátiť do hlavnej ponuky.

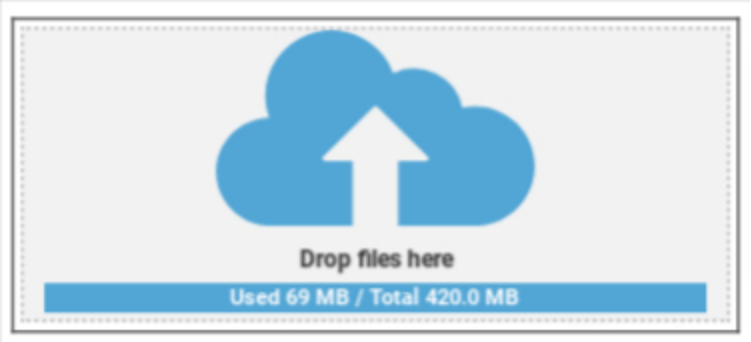
Môžete vybrať niekoľko priečinkov a súborov a stiahnuť ich pomocou "Download" (Stiahnuť) alebo ich môžete vymazať kliknutím na "Delete" (Odstrániť).

Môžete tiež vybrať všetky súbory a priečinky a vykonať príkazy "Stiahnuť" a "Odstrániť".

Keď prejdete myšou na priečinok alebo súbor, zobrazí sa nasledujúci prehľad:

- Pomocou funkcie "Premenovať" môžete premenovať priečinok/súbor
- Pomocou položky "Stiahnuť" môžete stiahnuť priečinok/súbor
- Pomocou "Delete" môžete priečinok/súbor vymazať

Povolenie priečinka skupiny	Ak je aktivovaná, všetci členovia skupiny majú prístup k príslušnému priečinku
Predvolené oprávnenia priečinkov skupiny	Oprávnenia používateľov vo vybranej skupine: Čítať = povolenie len na čítanie Aktualizovať = povolenie aktualizovať Vytvoriť = oprávnenie na vytvorenie Vymazať = povolenie na vymazanie
Odovzdávanie skupinových priečinkov podskupinám	Ak je aktivovaná, príslušné podskupiny môžu mať prístup k nadradeným dátovým súborom
Oprávnenia pre podskupiny	Oprávnenia používateľov vo vybranej podskupine: Čítať = povolenie len na čítanie Aktualizácia = povolenie aktualizácie Vytvoriť = oprávnenie na vytvorenie Vymazať = povolenie na vymazanie
Povoliť zdieľanie	Ak je aktivovaná, používateľ môže zdieľať súbory prostredníctvom odkazu



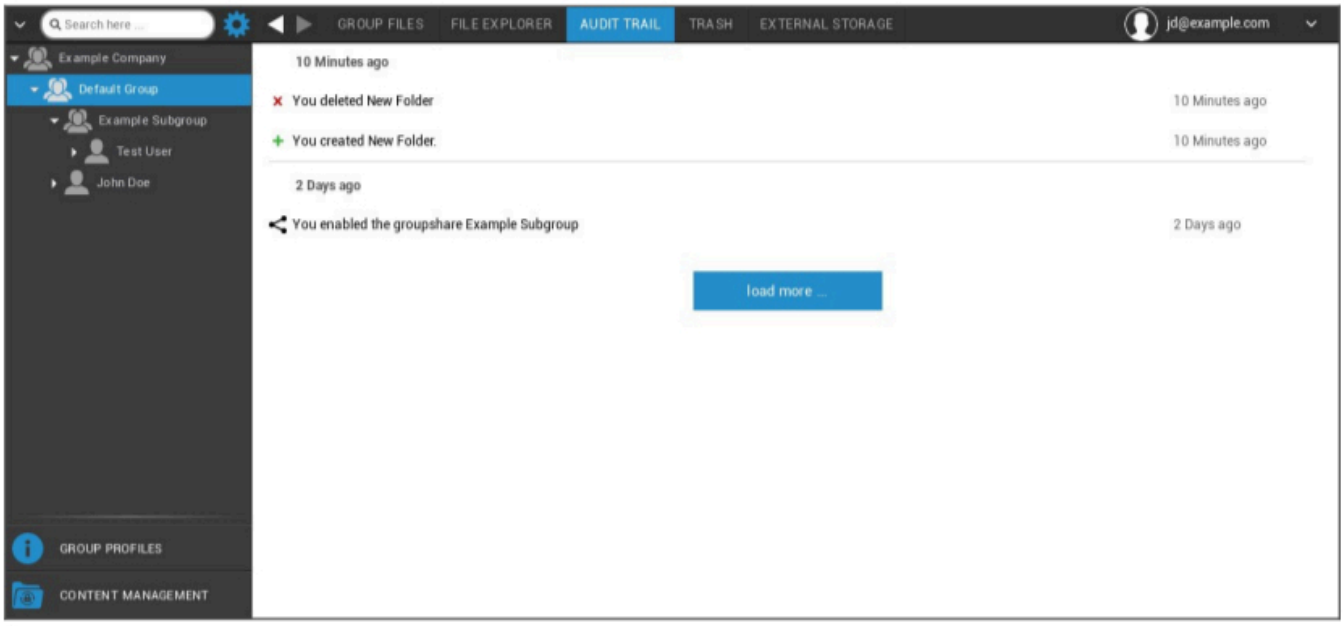
Ak chcete nahrať súbory, môžete toto pole použiť tak, že do tohto okna vytiahnete súbor pomocou funkcie Drag & Drop. Na toto pole môžete tiež kliknúť, aby ste vybrali a nahrali súbor pomocou programu Internet Explorer.

Prieskumník súborov

Pomocou Prieskumníka súborov môžete spravovať všetky priečinky a súbory bez ohľadu na skupinu, v ktorej sú uložené.

Nájdete tu aj nastavenia a tlačidlá, o ktorých ste sa dozvedeli v časti "Skupinové súbory".

Audítorská stopa



V časti "Audit Trail" môžete z histórie zistiť, ktorý používateľ čo vytvoril, vymazal alebo zdieľal. Takto môžete kedykoľvek zistiť, čo bolo vykonané s podnikovými údajmi.

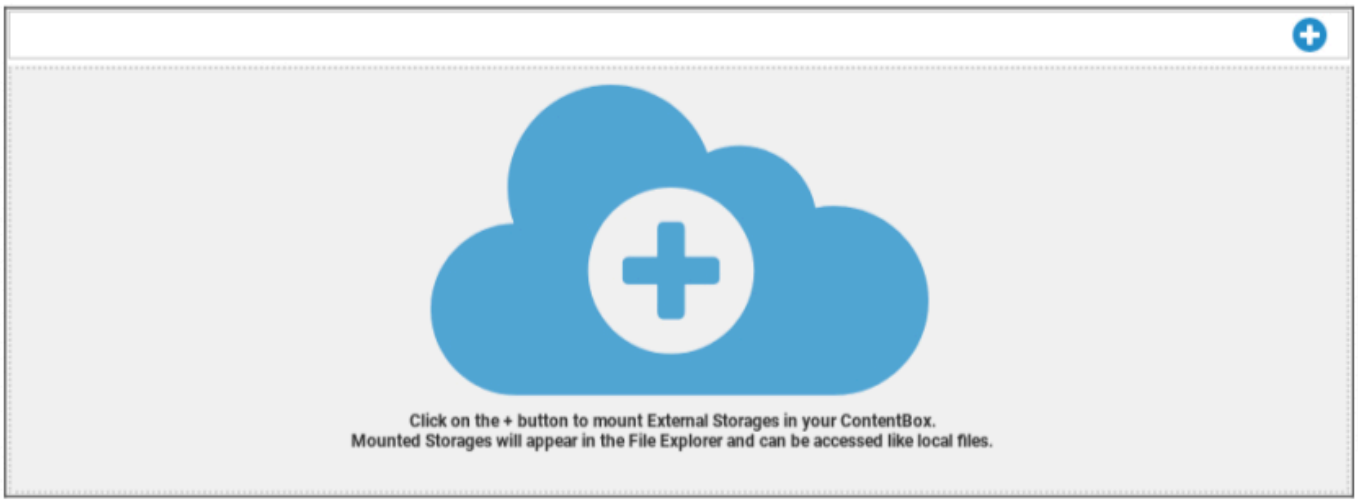
Odpadky

Ak ste niečo vymazali (omylom), môžete si prezrieť priečinky a súbory v časti Kôš a obnoviť ich podľa svojich predstáv.

- Pomocou funkcie "Undelete" môžete obnoviť údaje/priečinok.
- Pomocou príkazu "Delete" (Odstrániť) môžete údaje/priečinok natrvalo vymazať - príkaz Delete (Vymazať) musíte ešte raz potvrdiť.

Upozorňujeme, že kapacita úložiska, ktorá sa využíva v koši, znižuje celkový dostupný priestor - ide o požiadavku služby ownCloud.

Externé úložisko



V časti "Externé úložisko" môžete pripojiť externé úložisko.

Pomocou symbolu je možné pridať (ďalšie) úložisko.

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

Amazon S3	
Zobrazenie názvu	Zobrazenie názvu
Prístupový kľúč	Prístupový kľúč
Tajný kľúč	Bezpečnostný kľúč
Vedro	Definitívna identita podpriečinka, ktorý vám bol pridelený
Názov hostiteľa (voliteľné)	Názov hostiteľa (voliteľné)
Port (voliteľné)	Port (voliteľné)
Región	Región (voliteľné)
Povolenie protokolu SSL	Povolenie protokolu SSL
Povolenie štýlu cesty	Vymazať adresu cesty, ktorá vám bola pridelená

FTP	
Zobrazenie názvu	Zobrazenie názvu
Hostiteľ	Adresa hostiteľa
Používateľské meno	Používateľské meno
Heslo	Heslo
Koreň	Hlavné menu
Zabezpečené ftps://	

SFTP	
Zobrazenie názvu	Zobrazenie názvu
Hostiteľ	Adresa hostiteľa
Používateľské meno	Meno používateľa
Heslo	Heslo
Koreň	Hlavné menu

ownCloud	
Zobrazenie názvu	Zobrazenie názvu
ADRESA URL	URL adresa služby ownCloud
Používateľské meno	Používateľské meno
Heslo	Heslo
Vzdialený podpriečinok	Štandardný priečinok
Zabezpečiť https://	

WebDAV	
Zobrazenie názvu	Zobrazenie názvu
ADRESA URL	Adresa URL WebDAV
Používateľské meno	Meno používateľa
Heslo	Heslo
Koreň	Hlavné menu
Zabezpečiť https://	
Zdieľanie systému Windows	Podpora pre Windows Share bude k dispozícii čoskoro
SharePoint	Podpora pre Microsoft SharePoint bude k dispozícii čoskoro

Protokol o audite

Tu nájdete protokol, ktorý zaznamenáva informácie o akciách vykonaných v konzole MDM.

Pomocou ikony filtra môžete na zobrazený zoznam použiť filtre.

Pomocou rozbaľovacieho menu **Položky na stránku**: môžete vybrať množstvo položiek, ktoré sa majú zobraziť na jednej stránke zoznamu.

Prijaté opatrenie / zmena nastavenia	Akcia, ktorá bola vykonaná / Nastavenie, ktoré bolo zmenené
Hodnota	Hodnota vykonanej akcie/zmeneného nastavenia
Používateľ	Meno používateľa, ktorý vykonal akciu/zmenil nastavenie
Dátum	Časová značka, kedy bola táto akcia vykonaná / toto nastavenie zmenené
Cesta / typ	Cesta k miestu, kde bola vykonaná táto akcia / zmenené toto nastavenie

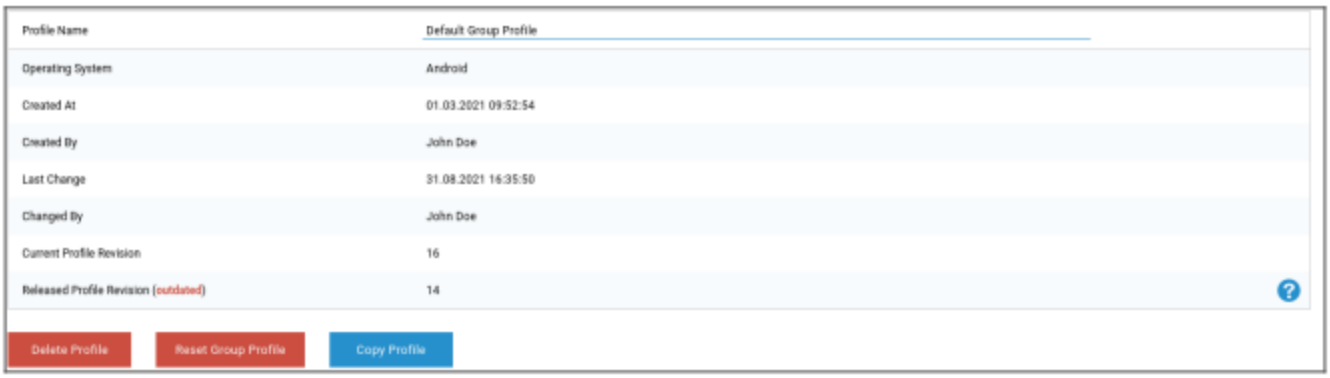
Konfigurácia systému iOS

Všeobecné

V závislosti od toho, či ste aktuálne vybrali skupinu alebo zariadenie, sa zobrazenie a jeho podbody líšia - venujte tomu zvýšenú pozornosť!

Prehľad profilu skupiny (len na úrovni skupiny)

Po otvorení profilu skupiny sa zobrazí rýchly prehľad profilu.



Názov profilu	Názov profilu (tu sa dá zmeniť)
Operačný systém	Operačný systém, pre ktorý je profil určený
Vytvorené v	Čas vytvorenia
Vytvoril	Tvorca profilu
Posledná zmena	Čas poslednej zmeny profilu
Zmenené podľa	Účet, ktorý vykonal posledné zmeny
Aktuálna revízia profilu	Revízia uloženého stavu profilu
Vydaná revízia profilu	Priradená revízia profilu ("Priradiť teraz"). Ak sa za textom na štítku zobrazí " (zastaraný)", znamená to, že ste profil uložili, ale ešte ste ho nepriradili, takže zariadenia budú stále dostávať staršiu verziu.

Všeobecné informácie

Ak sa nachádzate priamo v zariadení, zobrazí sa stručný prehľad vybraného zariadenia.

Názov zariadenia	Názov zariadenia
Telefónne číslo	Telefónne číslo zariadenia
Model	Číslo modelu
Operačný systém	OS
Sériové číslo	Sériové číslo zariadenia
Vlastníctvo zariadenia	Firemné alebo súkromné zariadenie Corporate = firemné zariadenie Zamestnanec = súkromné zariadenie
Typ zariadenia	Typ zariadenia (tablet alebo telefón)
Jailbroken	Ak je v zariadení útek z väzenia
Pod dohľadom	Označuje, či ide o zariadenie pod dohľadom
V súlade s	Ak boli porušené nejaké usmernenia
Naposledy videné	Stav, kedy zariadenie naposledy komunikovalo so serverom AppTec360

Nastavenia

Tieto nastavenia obsahujú názov zariadenia a preddefinované pozadie.

Názov zariadenia na názov systému	Názov, ktorý bude vydaný v konzole AppTec360 (v ľavej hierarchickej štruktúre), bude rovnaký ako na príslušnom zariadení koncového používateľa (možno zobraziť v nastaveniach zariadenia)
Používanie vlastnej tapety (iba zariadenia pod dohľadom)	Tu môžete vopred definovať pozadie, ktoré sa má zobrazovať na zariadení koncového používateľa (napr. pre typ firemnej značky zariadenia) Je k dispozícii len v režime pod dohľadom!
Automatické aktualizácie operačného systému	Vynúti aktualizácie operačného systému, ak sú k dispozícii. Len pre zariadenia DEP v režime pod dohľadom.
Vlastné písma	Tu môžete pridať vlastné písma.
Názov	Voliteľné. Používateľsky viditeľný názov písma. Toto pole sa po inštalácii nahradí skutočným názvom písma.
Písmo	Nahrajte súbor písma (.otf alebo .ttf).

Revízia konfigurácie

Tu získate prehľad o tom, ktorý skupinový profil je určený pre zariadenie.

Ak kliknete na profil skupiny, získate priamy prístup k profilu a môžete vykonať nastavenia.

Pomocou symbolu môžete vrátiť priradené aplikácie do nastavení skupinového profilu.

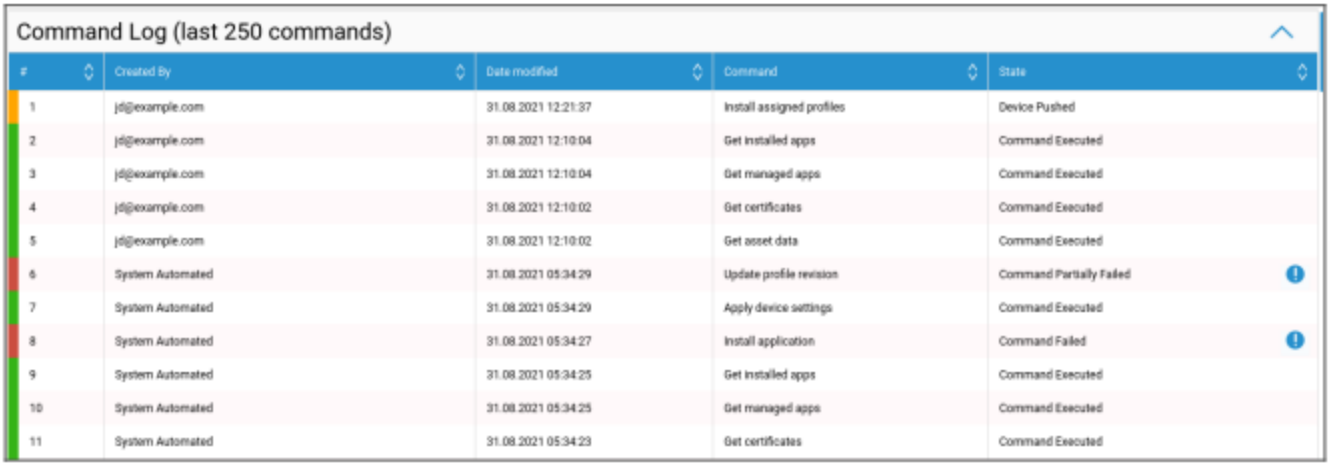
Pomocou symbolu môžete obnoviť profil zariadenia tak, aby nemal žiadne nastavenia.

"K dispozícii je novšia revízia" znamená, že profil skupiny bol zmenený a uložený, ale nie je priradený. Profil skupiny sa musí priradiť pomocou "Priradiť teraz" na úrovni skupiny, aby sa zmeny uplatnili na zariadeniach.

Protokol zariadenia (len na úrovni zariadenia)

Denník príkazov

Tu môžete vidieť, ktoré príkazy boli pre zariadenie vydané a aký je ich stav.



Príkazy vytvorené pomocou "System Automated" sú automaticky vytvorené systémom.

Možné stavy príkazov

Stlačené zariadenie	Do služby push (napr. APNS) bola odoslaná požiadavka na pripojenie, aby sa zariadenie pripojilo späť k serveru EMM.
Vytvorený príkaz	Príkaz bol vytvorený v systéme.
Odoslaný príkaz	Príkaz sa odoslal do zariadenia po jeho pripojení k serveru.
Vykonaný príkaz	Príkaz bol úspešne vykonaný.
Príkaz zlyhal	Príkaz zlyhal. *
Príkaz čiastočne zlyhal	V závislosti od operačného systému zariadenia môžu byť niektoré príkazy zoskupené. V tejto časti tejto skupiny príkazov zlyhali niektoré časti. *
Príkaz vykonaný, prípadne neúspešný	Príkaz bol vykonaný, ale možno nebol.
Príkaz Repushed	Príkaz bol opätovne odoslaný používateľom.
Vyradené	Príkaz bol zamietnutý. Napríklad preto, že bol nahradený iným príkazom alebo zariadenie bolo znovu zaregistrované a staré príkazy boli odstránené.

Ak sa za správou nachádza výkričník, môžete získať ďalšie informácie tak, že kurzorom prejdete nad ikonu.

Správa aktív (len na úrovni zariadenia)

Správa aktív (len na úrovni zariadenia)

Informácie o zariadení

Model	Číslo modelu zariadenia
Operačný systém	OS
Verzia operačného systému	Verzia operačného systému
Sériové číslo	Sériové číslo
UDID	Identifikátor UDID zariadenia
Názov zariadenia	Názov zariadenia
Pod dohľadom	Zobrazuje, či je zariadenie pod dohľadom
Stav batérie	Stav batérie

Wi-Fi

IP adresa	Adresa IP zariadenia
WiFi MAC	Adresa MAC WiFi

Cellular

Stav	Stav (karta SIM je prítomná)
Telefónne číslo	Telefónne číslo
Stav roamingu	Aktuálny stav roamingu
Roaming (hlas/údaj)	Stav roamingu pre hlasové/dátové služby
IP adresa	IP adresa
IMEI	Číslo IMEI
Prevádzkovateľ/prepravca	Poskytovateľ mobilných služieb
Sieť operátora SIM	Sieť operátora SIM
Verzia nosiča	Verzia nosiča
Firmvér modemu	Firmvér modemu
Súčasné MCC/MNC	Pozri "SIM MCC/MNC".
SIM MCC/MNC	Kód mobilnej krajiny je identifikácia krajiny stanovená ITU podľa normy E.212, ktorá sa v spojení s kódom mobilnej siete (MNC) používa na identifikáciu mobilnej siete (=kód krajiny). Keď prejdete do inej mobilnej siete, "Current MCC/MNC" a "SIM MCC/MNC" sú preto odlišné.

Bluetooth

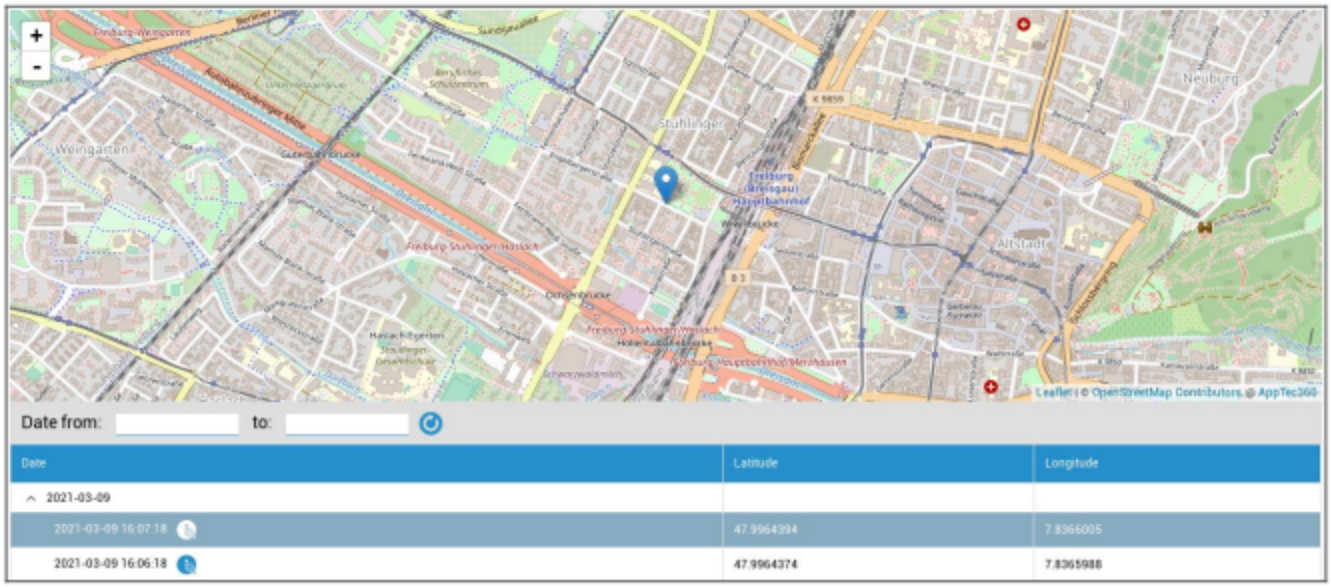
Bluetooth MAC	Adresa MAC Bluetooth

Riadenie bezpečnosti

Ochrana proti krádeži (len na úrovni zariadenia)

Informácie GPS (len na úrovni zariadenia)

Tu môžete vyhodnotiť aktuálnu/poslednú polohu zariadenia. Lokalizácia môže byť chránená buď jedným, alebo dokonca dvoma heslami - pozrite si: Všeobecné nastavenia - Súkromie - Prístup k GPS



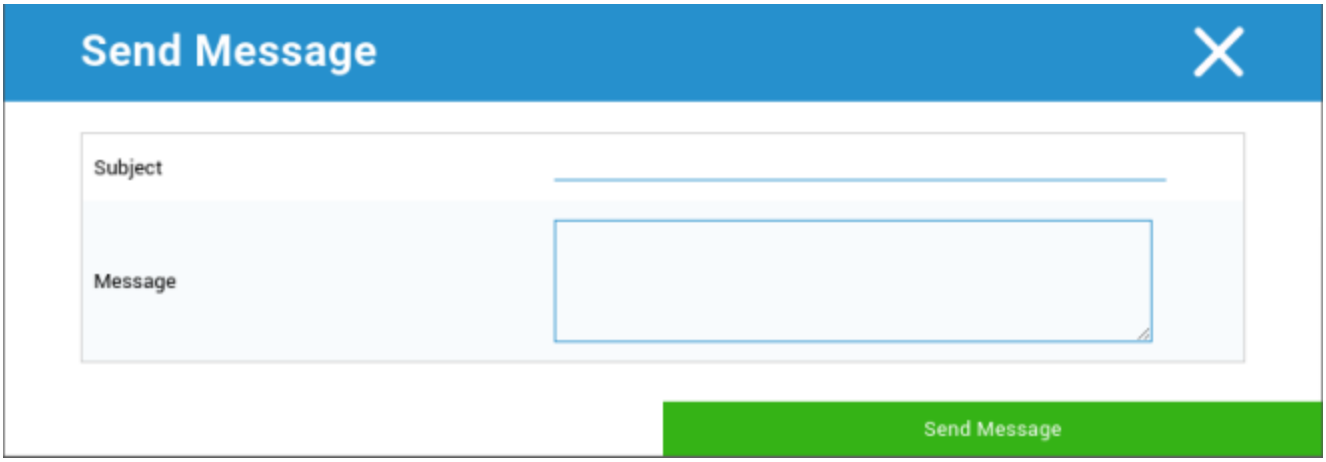
Vyčistiť a uzamknúť (len na úrovni zariadenia)

V časti "Vyčistiť a uzamknúť" môžete vykonať nasledujúce tri akcie:

Úplné utretie	Zariadenie sa obnoví do továrenského nastavenia (vymažú sa firemné aj osobné údaje).
Podnik Wipe	Zo zariadenia koncového používateľa sa odstránia len firemné údaje (všetky aplikácie, údaje atď., ktoré poskytla spoločnosť AppTec)
Uzamknutie obrazovky	Ak je aktivovaný zámok obrazovky, stačí zariadenie odomknúť pomocou hesla zariadenia/PIN kódu.
Forenzné uzamknutie (len pre zariadenia pod dohľadom)	Ak sa táto funkcia aktivuje pomocou symbolu  , zariadenie sa uzamkne zobrazením správy, ktorú nie je možné zatvoriť. Zamestnanec tiež nemôže zariadenie odomknúť. Zariadenie môže odomknúť iba správca v konzole pomocou symbolu odomknutia  .
Povoliť blokovanie aktivácie (len pre zariadenia pod dohľadom)	Ak je táto funkcia aktivovaná , zariadenie sa uzamkne, akonáhle je v nastaveniach iCloudu aktivovaná funkcia "Nájsť môj iPhone".

Správa (len na úrovni zariadenia)

V nasledujúcom okne môžete vyplniť predmet a správu a odoslať ju koncovému používateľskému zariadeniu:



Konfigurácia zabezpečenia

Prístupový kód

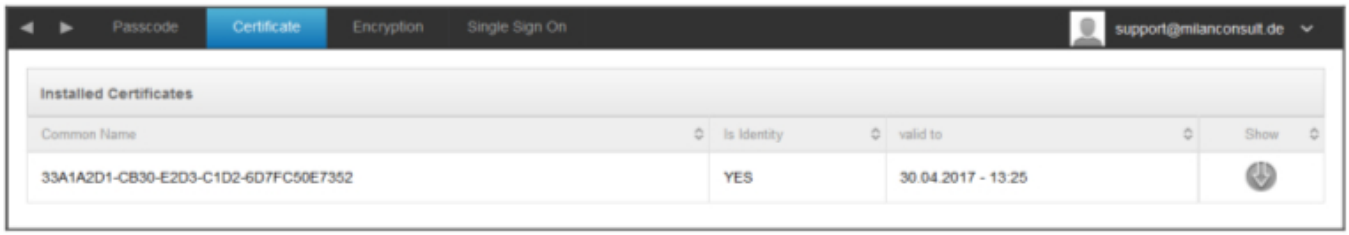
Tu môžete nastaviť heslo zariadenia

Povolená deaktivácia kódu	Keď je toto nastavenie aktivované, nezobrazí sa výzva na zadanie hesla. Hneď ako je heslo vytvorené, nie je možné ho deaktivovať.
Povolenie jednoduchej hodnoty	Umožniť používateľovi používať rovnaké, stupňujúce sa a znižujúce sa číselné reťazce (napr. 1234, 1111)
Vyžadovať alfanumerickú hodnotu	Heslá musia obsahovať aspoň jedno písmeno
Minimálna dĺžka prístupového kódu	Minimálna dĺžka hesla
Minimálny počet zložených znakov	Minimálny počet alfanumerických symbolov v hesle
Maximálny vek prístupového kódu	Počet dní, po ktorých sa musí heslo zmeniť
Maximálny automatický zámok	Maximálny čas, po uplynutí ktorého sa zariadenie uzamkne
Maximálna doba odkladu na zablokovanie zariadenia	čas, po ktorom zariadenie prejde do uzamknutého režimu Stand-By
Maximálny počet neúspešných pokusov	stanovuje, ako často môže byť heslo zadané nesprávne, kým sa vykoná úplné vymazanie zariadenia
Maximálny vek prístupového kódu (1-730 dní)	Maximálny vek hesla
História prístupových kódov (1-50 prístupových kódov)	Po tomto čísle je povolené používať staré heslo

Kliknutím na kôš sa otvorí dialógové okno Obnovenie hesla, pomocou ktorého možno vymazať zabudnuté heslo zariadenia.

Certifikát (len na úrovni zariadenia)

Zobrazí certifikáty, ktoré sú k dispozícii v zariadení


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

Šifrovanie

Vyžadovať šifrovanie úložiska	Aktivácia funkcie šifrovania nainštalovaného zariadenia

Jednotné prihlásenie

V bode "Single Sign-On" môžete nakonfigurovať overovanie Kerberos.

Tu môžete nastaviť prístupové údaje a príslušné adresy URL / aplikácie, ktoré môžu používať tokeny Kerberos.

K dispozícii v režime s dohľadom	
Názov účtu	Názov účtu
Hlavné meno	Jedinečná identita, na ktorú možno distribuovať lístky Kerberos
Ríša	Vaša doména Kerberos, ktorá sa má používať (napr. vaša doména)

Pomocou symbolu môžete vytvoriť ďalšie adresy URL.

Vzor URL použitý na obmedzenie tohto účtu	Určia sa adresy URL, na ktoré sa môžu distribuovať lístky Kerberos

Pomocou symbolu môžete vytvoriť ďalšie aplikácie.

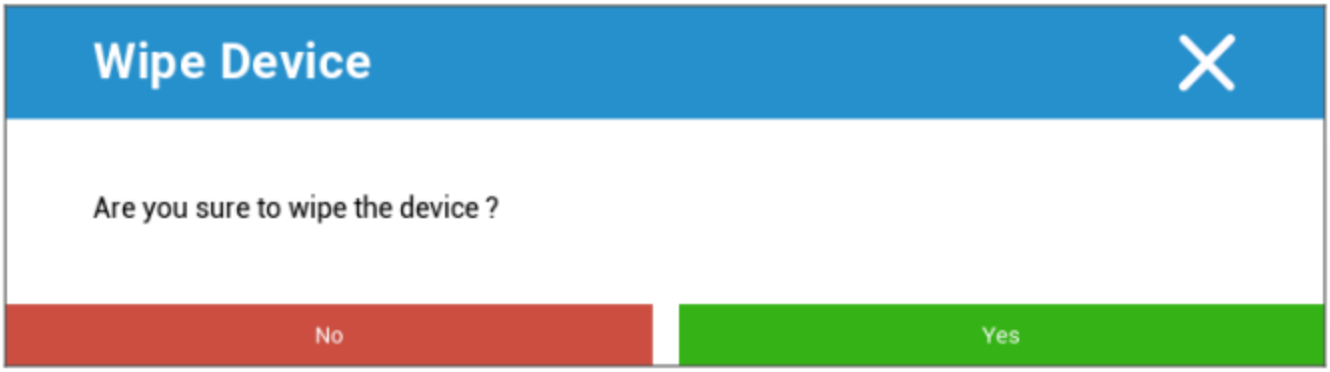
Aplikácie na obmedzenie tohto účtu	Určí sa Aplikácie, ktorým možno distribuovať vstupenky Kerberos

Koniec životnosti (len na úrovni zariadenia)

Vyčistiť (len na úrovni zariadenia)

V časti "Vymazať" môžete obnoviť výrobné nastavenia zariadenia. Tu sa odstránia firemné, ako aj súkromné údaje v zariadení koncového používateľa.

Po kliknutí na symbol "Mínus" by sa mala zobraziť nasledujúca správa



Pomocou možnosti "Áno" môžete vykonať vymazanie.

V časti "Wipe Report" sa môžu zobraziť tieto položky

Zotreté	História toho, kto vykonal utretie
Dátum	Dátum
Stav	Stav (napr. či bolo vymazanie vykonané úspešne)

Nastavenia obmedzenia

Funkčnosť zariadenia

Tu môžete zablokovať jednotlivé funkcie koncového zariadenia používateľa

Povolenie inštalácie aplikácií	Povolenie inštalácie aplikácií
Povoliť kameru	Povolenie používania fotoaparátu
Povolenie FaceTime	Povolenie FaceTime
Povolenie snímania obrazovky	Povolenie snímania obrazovky
Povolenie automatickej synchronizácie počas roamingu	Povolenie automatickej synchronizácie počas roamingu
Povoľte Siri	Povoľte Siri
Povolenie hlasového vytáčania	Povolenie hlasového vytáčania
Povolenie nákupu v aplikácii	Povolenie nákupu v aplikácii
Vyžadovanie hesla iTunes Store pre všetky nákupy	Vyžadovanie hesla iTunes Store pre všetky nákupy
Umožniť hranie pre viacerých hráčov	Umožniť hranie pre viacerých hráčov
Povolenie pridávania priateľov do služby Game Center	Povolenie pridávania priateľov do služby Game Center
Povolenie otvorenia zo spravovaného do nespravovaného	Povolenie otvárania obsahu spravovaných aplikácií v nespravovaných aplikáciách
Povolenie otvorenia z nespravovaných na spravované	Povolenie otvárania obsahu nespravovaných aplikácií v spravovaných aplikáciách
Povolenie dnešného zobrazenia na uzamknutej obrazovke	Keď je toto nastavenie aktívne, zobrazenie "Dnes" sa zobrazí v Centre oznámení na uzamknutej obrazovke.
Povolenie ovládacieho centra na uzamknutej obrazovke	Povolenie Ovládacieho centra na uzamknutej obrazovke
Povolenie funkcie TouchID	Povolenie funkcie TouchID
Povolenie aktualizácií PKI over-the-air	Povolenie aktualizácií PKI over-the-air

Povolenie zablokovania vkladnej knižky	Povolenie passbooku, keď je zariadenie uzamknuté
Obmedzenie sledovania reklám	Táto funkcia deaktivuje sledovanie reklám (napr. inzerenti nemôžu používať sledovanie reklám na šírenie personalizovaných reklám).
Povolenie odovzdávania	Povolenie odovzdávania
Povoľte internetové výsledky v centre pozornosti	Povolenie internetových výsledkov v centre pozornosti (napr. Bing alebo Wikipedia)
Vyžadovanie prístupového kódu pri prvom párovaní AirPlay	Vyžadovanie prístupového kódu pri prvom párovaní AirPlay
Ochrana zápästia hodiniek Force Watch	Ak je aktivovaná, hodinky Apple Watch sú nútené používať "Ochranu zápästia" (rozpoznávanie zápästia).
Povolenie knižnice fotografií iCloud	Umožňuje používať knižnicu iCloud Photo Library. Ak to nie je povolené, všetky obrázky, ktoré neboli úplne stiahnuté z iCloudu, sa vymažú z miestneho úložiska.
K dispozícii v režime pod dohľadom	
Povolenie úpravy účtu	Povolenie úpravy "pošta, kontakty, kalendár"
Povolenie služby AirDrop	Povolenie služby AirDrop
Povolenie úpravy aplikácie Cellular	Toto nastavenie blokuje nastavenie, pre ktoré aplikácie je povolené používať mobilné dáta. Toto nastavenie možno napríklad manuálne nastaviť na zariadení koncového používateľa a potom toto obmedzenie aktivovať.
Povolenie vyhľadávania obsahu vytvoreného používateľom z webu v aplikácii Siri	Webové vyhľadávanie na niektorých webových stránkach je zablokované, napr. na Wikipédii, pretože každý môže robiť zmeny podľa vlastného uváženia
Povolenie filtra vulgarizmov Siri	Profanácia namierená na Siri je cenzurovaná
Povolenie obchodu iBook Store	Povolenie obchodu iBook Store
Povoliť iBook Store Erotika	Povoliť iBook Store Erotika
Povolenie úpravy nastavení služby Nájsť mojich priateľov	Povolenie úpravy nastavení služby Nájsť mojich priateľov
Povolenie služby Game Center	Povolenie služby Game Center
Povolenie párovania hostiteľov	Párovanie riadiaceho počítača
Povolenie inštalácie konfiguračných profilov	Povolenie inštalácie konfiguračných profilov

Povolenie odstránenia aplikácie	Odstránenie kontrolných aplikácií
Povolenie iMessage	Povolenie iMessage
Povolenie vymazania všetkého obsahu a nastavení	Umožniť vymazanie všetkého obsahu a nastavení
Umožniť konfiguráciu obmedzení	Umožniť konfiguráciu obmedzení
Povoliť podcast	Povoliť podcast
Povoliť vyhľadávanie definícií	Povolenie vyhľadávania definícií
Povolenie prediktívnej klávesnice	Povolenie prediktívnej klávesnice
Povolenie automatickej korekcie	Povolenie automatickej korekcie
Povolenie inštalácie aplikácie používateľského rozhrania	Ak je deaktivovaný, nie je možné inštalovať žiadne aplikácie z verejného AppStore (ikona sa už nebude zobrazovať). Aplikácie je však stále možné inštalovať prostredníctvom iTunes a konfigurátora
Povolenie klávesových skratiek	Povolenie klávesových skratiek, ak je zariadenie pripojené k fyzickej klávesnici
Povolenie párovania s hodinkami Apple Watch	Zakáže párovanie medzi zariadením a hodinkami Apple Watch, existujúce spojenia sa ukončia
Povolenie úpravy prístupového kódu	Ak nie je povolené, nie je možné pridať, zmeniť ani odstrániť žiadne heslo zariadenia.
Povolenie úpravy názvu zariadenia	Usmernenie na určenie, či je možné zmeniť názov zariadenia
Povolenie úpravy tapety	Usmernenie na určenie, či je možné zmeniť tapetu
Povolenie automatického sťahovania aplikácií	Ak je zakúpená aplikácia deaktivovaná, nebude sa automaticky inštalovať do iných zariadení. Nevzťahuje sa na aktualizácie existujúcich aplikácií
Povoliť správy	Povolenie správ v zariadení iOS
Povolenie dôveryhodnosti podnikových aplikácií	Ak je nastavená na hodnotu false, zabraňuje dôverovaniu podnikovým aplikáciám.

iCloud

Blokovanie určitých funkcií počas párovania iCloud

Povolenie zálohovania	Povolenie zálohovania
Povolenie synchronizácie dokumentov	Povolenie synchronizácie dokumentov
Povoliť prúd fotografií	Povoliť prúd fotografií
Povolenie zdieľaného prúdu fotografií	Povolenie zdieľaného prúdu fotografií
Povolenie cloudovej synchronizácie kľúčenky	Povolenie cloudovej synchronizácie kľúčenky
Povolenie spravovaným aplikáciám ukladať údaje	Povolenie spravovaným aplikáciám ukladať údaje
Povolenie synchronizácie poznámok a zvýraznení pre podnikové knihy	Povolenie synchronizácie poznámok a zvýraznení pre podnikové knihy
Umožniť zálohovanie podnikových kníh	Umožniť zálohovanie podnikových kníh

Bezpečnosť a ochrana osobných údajov

Blokovanie týchto funkcií spojených s diagnostickými údajmi

Povolenie odosielania diagnostických údajov do spoločnosti Apple	Povolenie odosielania diagnostických údajov do spoločnosti Apple
Povolenie používateľovi akceptovať nedôveryhodné certifikáty TLS	Povoliť používateľovi, aby akceptoval nedôveryhodné certifikáty TLS
Vynútenie šifrovaných záloh	Vynútenie šifrovaných záloh

BYOD

Zabudované zabezpečenie iOS (kontajner)

iOS vždy dokázal rozlišovať medzi spravovaným (obchodným) a nespravovaným (súkromným). Všetko, čo pochádza zo systému MDM, sa považuje za spravované. Ak napríklad nainštalujete aplikáciu prostredníctvom MDM oder nakonfigurujete konto Exchange, bude sa to v systéme iOS považovať za spravované.

Všetko ostatné, čo sa v zariadení nakonfiguruje/inštaluje ručne, sa bude považovať za nespravované. Napríklad ak si používateľ sám nainštaluje aplikáciu WhatsApp alebo ak pridáva konto Exchange. Toto oddelenie však nikdy neovplyvnilo kontakty. Od verzie iOS 11.3 (a vyššej) však bolo toto oddelenie pridané aj pre kontakty.

Keďže ide o základnú funkciu operačného systému, nemusíte nič inštalovať ani nastavovať špeciálny kontajner.

Aktivujte vstavanú funkciu na oddelenie súkromných a pracovných aplikácií/informácií/súborov. Toto nastavenie tiež deaktivuje niektoré ďalšie funkcie, ktoré by inak mohli omylom vypnúť časti tohto oddelenia.

Aktivácia

Aktivácia kontajnerových riešení, ktoré podporuje AppTec360

Povolenie kontajnera Google Divide	Povolenie kontajnera Google Divide
Povolenie kontajnera SecurePIM	Povolenie kontajnera SecurePIM

Ak ste aktivovali SecurePIM Container, v časti "Aktivácia" nájdete aj nasledujúci bod. Okrem toho sa hneď otvoria ďalšie štyri karty, ktoré sú popísané nižšie.

E-mailová adresa podpory	E-mailová adresa podpory, na ktorú sa používateľ môže obrátiť s problémami

Heslo SecurePIM

V časti "Heslo SecurePIM" môžete nastaviť pokyny pre silu zabezpečenia hesla.

Časový limit relácie	Tu môžete nastaviť, po koľkých minútach sa musí znovu zadať nové heslo, keď SecurePIM beží na pozadí.
Dĺžka hesla	Dĺžka hesla pre prístup do kontajnera SecurePIM
Veľké písmená	Minimálny počet veľkých písmen
Znaky malých písmen	Minimálny počet malých písmen
Špeciálne znaky	Minimálny počet špeciálnych znakov
Číslice	Minimálne číslice
Aplikácia stierania	Počet prípadov, kedy je možné nesprávne zadať heslo, než sa obsah SecurePIM vymaže (Aplikácia však stále zostáva v zariadení koncového používateľa)

Zabezpečenie SecurePIM

V časti "SecurePIM Security" môžete nastaviť rôzne bezpečnostné nastavenia.

Zisťovanie zariadení s Jailbreakom	Ak je toto nastavenie aktivované, prístup do kontajnera SecurePIM sa zablokuje, akonáhle sa zariadenie rozpozná ako jailbreaknuté.
Zabezpečené textové polia	Obsah polí na odoslanie bude zašifrovaný, do operačného systému (iOS) sa nedostanú žiadne informácie. Poznámka: Pokiaľ je toto nastavenie aktívne, automatická oprava už nie je k dispozícii.
Exportovanie údajov o kontaktoch do zariadenia	Ak je toto nastavenie aktivované, používateľ môže exportovať kontakty Exchange do svojho lokálneho zariadenia. Poznámka: Exportuje sa len meno a telefónne číslo.
Ukážte miesto podujatia	Ak je toto nastavenie aktivované, miesto nadchádzajúcich udalostí sa zobrazí v paneli oznámení.
Zobraziť názov podujatia	Ak je toto nastavenie aktivované, v paneli oznámení sa zobrazí umiestnenie názvu nadchádzajúcej udalosti.

Prehliadač SecurePIM

Tu môžete nakonfigurovať prehliadač SecurePIM.

Pomocou symbolu môžete definovať novú adresu URL.

Pomocou symbolu môžete definovanú adresu URL opäť odstrániť.

"Adresy URL na bielej listine" sú adresy URL, ktoré možno načítať.

"Adresy URL na čiernej listine" sú adresy URL, ktoré nie je možné načítať, a preto sú blokované.

Upozorňujeme, že položky bielej listiny majú vyššiu prioritu ako položky čiernej listiny. V časti "Bookmark Title" (Názov záložky) môžete vydať názov. Pomocou položky "Bookmark URL" (URL záložky) môžete priradiť URL adresu k názvu záložky - týmto spôsobom môžete príslušným používateľom distribuovať individualizované záložky.

Výmena

V časti Exchange môžete nakonfigurovať konto Exchange.

E-mailová adresa ActiveSync	E-mailová adresa Exchange (všimnite si "zástupné znaky")
Prihlásenie do služby ActiveSync Exchange	Výmena používateľských mien (všimnite si "zástupné znaky")
Server Exchange ActiveSync	Adresa servera Exchange (FQDN)
Doména Exchange ActiveSync	Adresa domény Exchange
Certifikát používateľa	Certifikát používateľa
Overovanie na základe certifikátu	Používateľ sa overí pomocou certifikátu
Povolenie šifrovania S/MIME	Umožňuje používateľovi šifrovať poštu
Povolenie podpisovania S/MIME	Umožňuje používateľovi podpísať svoju poštu
Kontrola CRL	Ak je aktívny, súkromný certifikát sa porovná so zoznamom CRL (Certificate Revocation List).

Správa pripojenia

Wi-Fi

Identifikátor súboru služieb (SSID)	SSID siete, ktorá sa má pripojiť
Automatické pripojenie	Aktivácia automatického pripojenia pri vstupe do siete
Skrytá sieť	Aktivácia v prípade, že prístupový bod nevysiela identifikátor SSID

Nastavenie servera proxy

Konfigurácia proxy servera pre každý prístupový bod

Žiadne	Zriadenie bez splnomocnenia
Manuálne	Zriadenie manuálneho zástupcu
Adresa URL servera proxy	Adresa pre prístup k nastaveniam proxy servera
Prístav	Nastavenie portu pre proxy server
Overovanie	Meno používateľa pre overovanie na serveri Proxy
Heslo	Heslo pre overovanie na serveri Proxy
Automatické	Automatické vytvorenie proxy servera
Adresa URL servera proxy	URL adresa pre prístup k nastaveniam proxy servera

Typ zabezpečenia

Vytvorenie typu zabezpečenia pre prístupový bod

WEP	
Heslo	Heslo pre AP

WPA/WPA2	
Heslo	Heslo pre AP

WEP Enterprise - WPA / WPA2 Enterprise - Any Enterprise			
	Protokoly		
	TLS	Aktivácia/deaktivácia	
	TTLS	Aktivácia/deaktivácia	
	LEAP	Aktivácia/deaktivácia	
	PEAP	Aktivácia/deaktivácia	
	EAP-FAST	Aktivácia/deaktivácia	
	EAP-SIM	Aktivácia/deaktivácia	
	Používanie PAC		Používanie PAC (Protected Access Controll)
	Ustanovenie PAC	Konfigurácia Provision PAC	
	Anonymné poskytovanie PAC	Anonymné poskytovanie PAC	
	Vnútorné overovanie	Autentifikačný protokol, ktorý sa má použiť: PAP, CHAP, MSCHAP, MSCHAPv2	
	Používateľské meno	Používateľské meno na overovanie	
	Nepoužívajte heslo na pripojenie	Nepoužívajte heslo na pripojenie	
	Certifikát totožnosti	Nahratie/výber certifikátu overenia	
	Vonkajšia identita	Identita, ktorá je viditeľná navonok	
	Trust		
	Dôveryhodný certifikát 1	Nahratie prvého dôveryhodného certifikátu	
	Dôveryhodný certifikát 2	Nahratie druhého dôveryhodného certifikátu	
	Dôveryhodný certifikát 3	Nahratie tretieho dôveryhodného certifikátu	
	Názvy certifikátov dôveryhodných serverov	Názvy očakávaných certifikátov servera (v zozname oddelenom čiarkou)	

Žiadne	Nezaviesť žiadnu bezpečnosť

VPN

Názov pripojenia	Názov profilu VPN

Typ VPN

VPN

Všetka sieťová prevádzka zariadenia bude smerovaná cez pripojenie VPN.

Typ pripojenia	Vytvorenie typu pripojenia VPN
IPsec (cisco)	Protokol IPsec od spoločnosti cisco
PPTP	Protokol PPTP
L2TP	Protokol L2TP
Cisco AnyConnect	Protokol AnyConnect
Juniper SSL	Protokol Juniper SSL
F5 SSL	Protokol F5 SSL
SonicWall mConnect	SonicWall mobile Connect
Aruba VIA	Protokol Aruba VIA
Vlastné SSL	Pripojenie prostredníctvom vlastného protokolu SSL
OpenVPN	Protokol OpenVPN

Sieť VPN pre jednotlivé aplikácie

Pri otvorení určitej aplikácie sa vytvorí pripojenie VPN

Automatické spustenie pripojenia VPN pre jednotlivé aplikácie		Automatické spustenie pripojenia VPN pre jednotlivé aplikácie
Typ pripojenia		Vytvorenie typu pripojenia VPN
	Cisco AnyConnect	Protokol AnyConnect
	Juniper SSL	Protokol Juniper SSL
	F5 SSL	Protokol F5 SSL
	SonicWall mConnect	SonicWall mobile Connect
	Aruba VIA	Protokol Aruba VIA
	Vlastné SSL	Pripojenie prostredníctvom vlastného protokolu SSL
	OpenVPN	Protokol OpenVPN

Nastavenie servera proxy

Konfigurácia proxy servera pre pripojenie VPN

Žiadne	Zriadenie bez splnomocnenia
Manuálne	Ručné vytvorenie servera Proxy
Adresa URL servera proxy	Adresa pre prístup k nastaveniam proxy servera
Prístav	Nastavenie portu pre proxy server
Overovanie	Používateľské meno pre overovanie na serveri Proxy
Heslo	Heslo pre overovanie na serveri Proxy
Automatické	Automatické vytvorenie proxy servera
Adresa URL servera proxy	URL adresa pre prístup k nastaveniam proxy servera

Zobraziť zástupné symboly	Zobrazí všetky dostupné používateľské premenné, ktoré môže AppTec360 používať

APN

Názov prístupového bodu	Názov prístupového bodu
Používateľské meno prístupového bodu	Používateľské meno prístupového bodu
Heslo prístupového bodu	Heslo prístupového bodu
Proxy server	Adresa servera proxy
Prístav	Príslušný port proxy servera

Cellular

Povolenie dátového roamingu	Povolenie dátového roamingu
Povolenie hlasového roamingu	Povolenie hlasového roamingu
Povolenie hotspotu	Povolenie hotspotu

Proxy server HTTP

Typ proxy servera	
Manuálne	Zriadenie proxy servera manuálne
Adresa URL servera proxy	Adresa pre prístup k nastaveniam proxy servera
Prístav	Zriadenie portu proxy servera
Overovanie	Používateľské meno pre overovanie na serveri Proxy
Heslo	Heslo pre overovanie na serveri Proxy
Automatické	Automatické vytvorenie proxy servera
Adresa URL proxy servera PAC	Adresa URL proxy servera PAC
Povolenie priameho pripojenia, ak je PAC nedostupný	Povolenie priameho pripojenia (bez VPN), ak je PAC nedostupný
Umožnenie obchádzania proxy servera na prístup k vlastným sieťam	Umožniť obídenie proxy servera na prístup k interným sieťam

AirPrint

IP adresa	IP adresa tlačiarne
Cesta k zdroju	Definitívna cesta k zariadeniu AirPrint

AirPlay

Názov zariadenia	Názov zariadenia
Heslo	Heslo párovania
Biela listina	Definovanie zoznamu zariadení, s ktorými sa zariadenie môže výlučne spárovať

Správa PIM

Exchange Active Sync

Názov účtu	Názov e-mailového konta
Hostiteľ Exchange ActiveSync	Adresa/FQDN servera
Povoliť presun	Umožniť presúvanie e-mailov
Používajte len v pošte	Interakcie sa môžu vyskytovať len v natívnej aplikácii Mail
Používanie protokolu SSL	Používanie šifrovania SSL
Doména	Doména servera
Používateľ	Používateľské meno
E-mailová adresa	e-mailová adresa (len na úrovni zariadenia)
Heslo (len na úrovni zariadenia)	Heslo používateľa
Certifikát totožnosti	Vyberte príslušný certifikát na overenie na serveri
Minulé dni služby Mail to Sync	Počet dní, do ktorých by sa mali e-maily synchronizovať späť. Bez limitu = neobmedzené
Povolenie S/MIME	Povolenie šifrovania S/MIME
Podpisový certifikát	Nahratie príslušného podpisového certifikátu
Šifrovací certifikát	Odoslanie príslušného šifrovacieho certifikátu

E-mail

Nastavenie účtov POP3 / IMAP na zariadení koncového používateľa

Popis účtu	Názov des E-mailové kontá		
Typ účtu	IMAP	Prefix cesty	Prefix cesty pre špeciálne priečinky
	POP		
Zobrazované meno používateľa	Zobrazované meno používateľa		
E-mailová adresa	E-mailová adresa používateľa		
Povoliť presun	Umožniť presúvanie e-mailov		
Povolenie S/MIME	Povolenie šifrovania S/MIME		
Podpisový certifikát	Nahratie príslušného podpisového certifikátu		
Šifrovací certifikát	Odoslanie príslušného šifrovacieho certifikátu		

Prichádzajúca pošta

Nastavenia prichádzajúceho servera

Adresa poštového servera	Adresa poštového servera
Port poštového servera	Port poštového servera
Meno používateľa	Príslušné meno používateľa
Typ overovania	Typ overovania
Žiadne	Žiadny typ overovania
Heslo (len na úrovni zariadenia)	Výzva na zadanie hesla
MDM Challenge-Response	
NTLM	Overovanie NTLM
HTTP MD5 Digest	
Používanie protokolu SSL	V prípade potreby použite protokol SSL

Odchádzajúca pošta

Nastavenia odchádzajúceho servera

Adresa poštového servera	Adresa poštového servera
Port poštového servera	Port poštového servera
Meno používateľa	Príslušné meno používateľa
Typ overovania	
Žiadne	Žiadna metóda overovania
Heslo (len na úrovni zariadenia)	Výzva na zadanie hesla
MDM Challenge-Response	
NTLM	Overovanie NTLM
HTTP MD5 Digest	
Používanie protokolu SSL	V prípade potreby použite protokol SSL
Odchádzajúce heslo rovnaké ako prichádzajúce	Odchádzajúce heslo rovnaké ako prichádzajúce
Používajte len v pošte	Aktivácia, ak sa majú všetky odchádzajúce e-maily odosielať prostredníctvom aplikácie Mail-App

CalDav

Konfigurácia nastavenia a distribúcie účtu CalDav

Popis účtu	Zobrazovaný názov účtu
Názov hostiteľa	Názov hostiteľa a/alebo IP adresa
Prístav	Prístav účtu CalDav
Hlavná adresa URL	Hlavná adresa URL účtu
Používateľské meno	Príslušné používateľské meno CalDav
Heslo (len na úrovni zariadenia)	Príslušné heslo CalDav
Používanie protokolu SSL	V prípade potreby použite protokol SSL

Odhlásené kalendáre

Nastavenie a distribúcia prihlásených kalendárov

Popis	Zobrazovaný názov účtu
ADRESA URL	URL adresa databázy kalendára
Používateľské meno	Používateľské meno predplatného kalendára
Heslo (len na úrovni zariadenia)	Heslo predplatného kalendára
Používanie protokolu SSL	V prípade potreby použite protokol SSL

LDAP

V tejto oblasti nastavte pripojenie LDAP, aby ste umožnili dynamickú výmenu certifikátov medzi koncovým používateľským zariadením a adresárom Active Directory.

Upozorňujeme, že vybraný používateľ vyžaduje príslušné oprávnenie na čítanie.

Popis účtu	Popis účtu
Používateľské meno účtu	Používateľ pre prístup k LDAP
Heslo účtu	Heslo pre prístup k LDAP
Názov hostiteľa účtu	Názov hostiteľa/IP adresa servera LDAP
Používanie protokolu SSL	V prípade potreby použite protokol SSL

V druhej časti môžete definovať jednotlivé filtre na vyhľadávanie v registri LDAP.

Popis	Rozsah pôsobnosti	Vyhľadávacia základňa
Popis filtra	Úroveň vyhľadávania v registri LDAP	Definovanie jednotlivých filtrov

Správa webu

Webové klipy

Na tomto mieste definujte záložky s odkazmi na webové stránky, intranetové portály atď., ktoré budú viditeľné ako aplikácia na zariadení koncového používateľa.

Štítok	Názov pripojenia v zariadení koncového používateľa
ADRESA URL	Odkaz na príslušnú webovú lokalitu
Odnímateľný	Ak je aktivovaný, používateľ môže odstrániť webový klip
Ikona	Prostredníctvom tohto dialógu nahrajte logo pripojenia: Rozmery 180x180, formát png
Predkomponovaná ikona	Ak je aktivovaná, na ikone sa nezobrazia žiadne ďalšie efekty (tieň, odraz).
Na celú obrazovku	Pri otváraní webových klipov sa prehliadač otvára v režime celej obrazovky

Filter webového obsahu

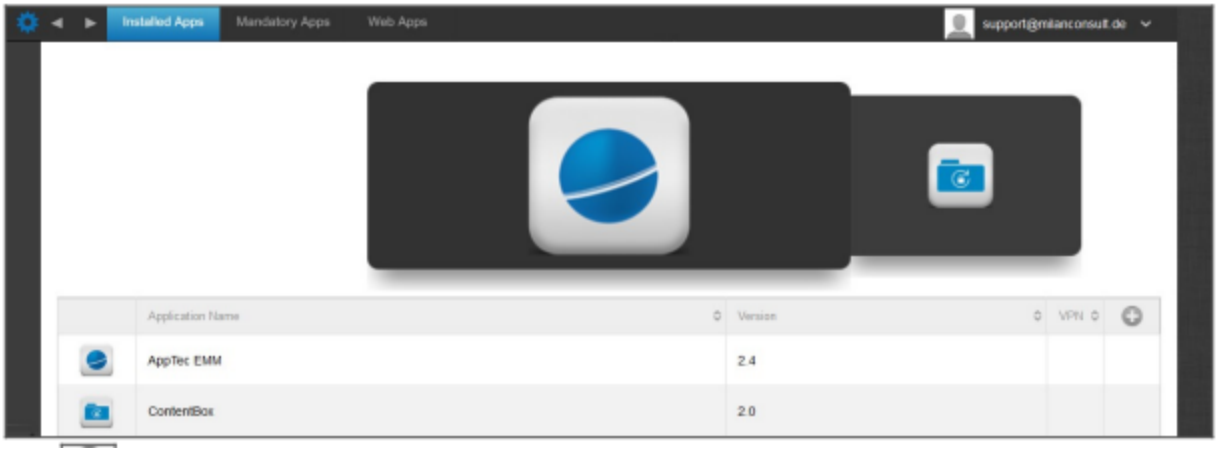
Filter webového obsahu umožňuje obmedziť prístup na konkrétne internetové stránky.

Povolené webové lokality	
Obmedzenie obsahu pre dospelých	Webový filter sa automaticky aplikuje na obsah pre dospelých
Povolené adresy URL	Pomocou symbolu + pridajte povolené stránky
Adresy URL na čiernej listine	Pomocou symbolu + pridajte blokované stránky
Len špecifické webové lokality	Zobrazovať sa môže len špecifický obsah, ktorý môžete pridať pomocou symbolu +.

Správa aplikácií

Správca podnikových aplikácií

Nainštalované aplikácie (len na úrovni zariadenia)



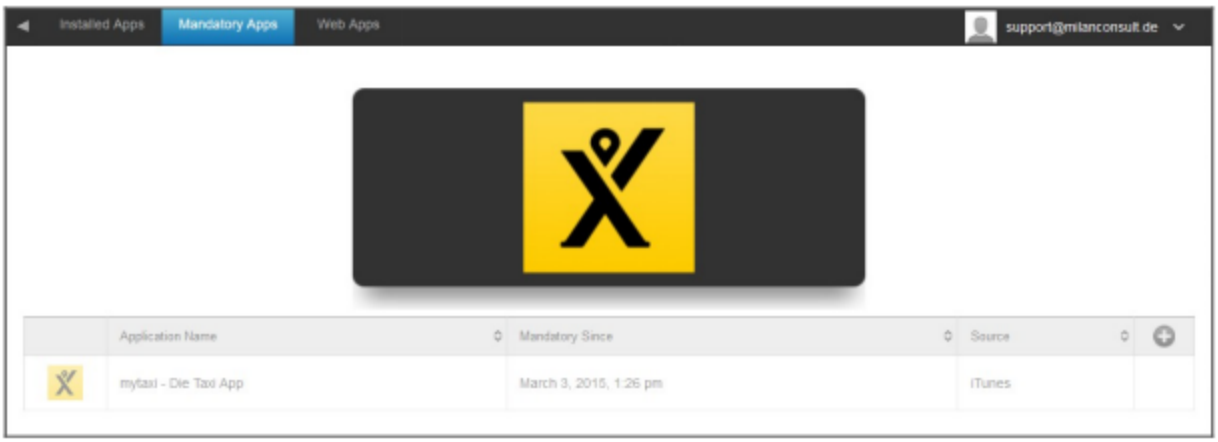
Tu môžete vidieť Aplikácie, ktoré sú aktuálne nainštalované v zariadení.

Povinné aplikácie

V časti Povinné aplikácie môžete nariadiť potrebné aplikácie.

Používateľovi bude neustále pripomínať, aby si nainštaloval túto aplikáciu.

Prostredníctvom , možno definovať mandátnu aplikáciu.



Môže ísť o aplikáciu v obchode Apple App Store, ale aj o internú aplikáciu.

Ak ide o zariadenie pod dohľadom, aplikácia sa nainštaluje automaticky.

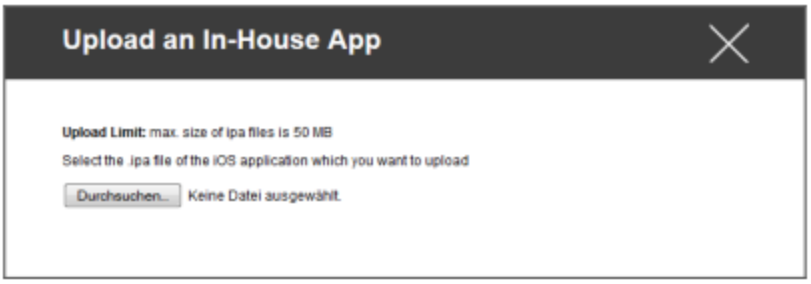
Do zariadenia môžete presunúť aplikáciu z verejného obchodu Apple AppStore, ako aj interne vyvinutú aplikáciu.

Alebo si môžete vybrať z kategórie "iOS In-House Apps" a vybrať In-House App, ktorú ste nahrali v časti Všeobecné nastavenia.

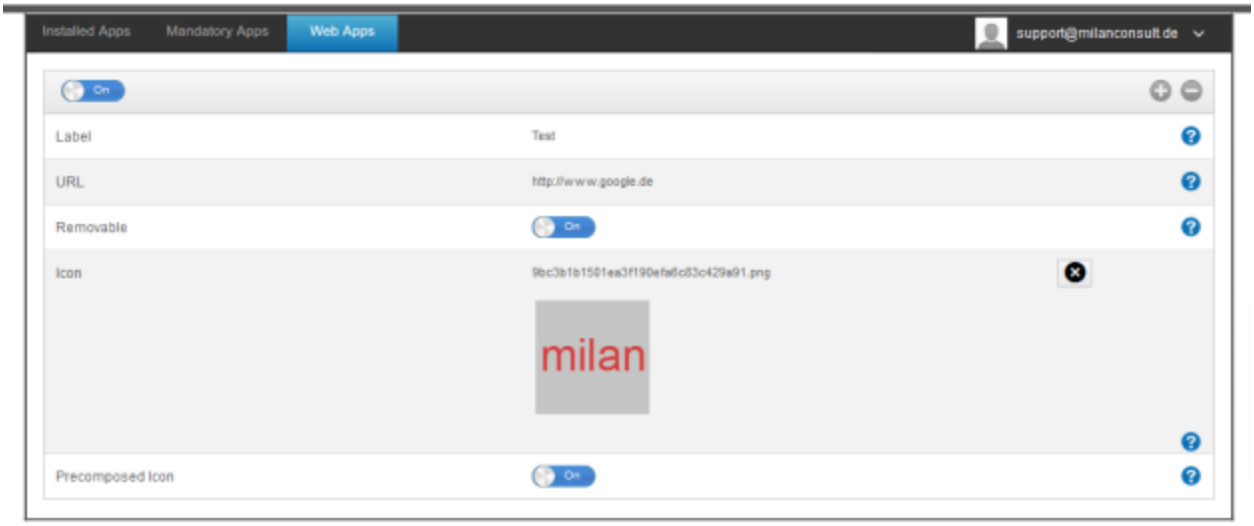
Možnosti inštalácie

Aktualizovať (podporované len pre VPP na zariadenie)	Raz týždenne sa určí, či je k dispozícii aktualizácia aplikácie. Ak áno, táto aktualizácia sa nainštaluje Pre interné aplikácie sa na proces aktualizácie použije cieľ aktualizácie, ktorý ste nakonfigurovali vo všeobecných nastaveniach.
Predbiehanie, keď nie je riadené	Ak je aplikácia už nainštalovaná, MDM prevezme aplikáciu a bude ju spravovať
Odstránenie aplikácie po odstránení profilu MDM	V prípade odstránenia správy zariadenia sa aplikácia odinštaluje
Zabránenie zálohovaniu údajov aplikácie	Záloha údajov špecifických pre aplikáciu sa nevytvorí
Nastavenie aplikácie	V časti "Nastavenia aplikácie" môžete aplikácii priradiť určité hodnoty do popredia (pokiaľ to aplikácia podporuje, v prípade potreby sa opýtajte vývojára aplikácie).

Môžete tiež priamo vybrať a nahrať súbor ipa prostredníctvom položky "Nahrať vlastnú aplikáciu".



Webové aplikácie



V rámci bodu "Web Apps" môžete podobne ako v prípade "Web Clips" posielať internetové stránky alebo intranetové portály ako aplikácie do zariadenia koncového používateľa v oblasti správy webu. Webové aplikácie sa štandardne zobrazujú v režime celej obrazovky, ktorý je možné nakonfigurovať v časti Webové klipy.

Štítok	Názov pripojenia v zariadení koncového používateľa
ADRESA URL	Prepojenie na príslušnú webovú lokalitu
Odnímateľný	Ak je aktivovaný, používateľ môže odstrániť webový klip
Ikona	Prostredníctvom tohto dialógu nahrajte logo pripojenia: Rozmery 180x180, formát png
Predkomponovaná ikona	Ak je aktivovaná, na ikone sa nezobrazia žiadne ďalšie efekty (tieň, odraz).

Obmedzenie a nastavenia

Aplikácie na čiernej / bielej listine

Tu môžete nastaviť aplikácie, ktoré sú blokované (alebo povolené) v závislosti od nastavení v časti "Všeobecné nastavenia". Po kliknutí sa zobrazí vyhľadávanie známych aplikácií. Tam môžete vyhľadať aplikácie, ktoré chcete pridať.

Upozorňujeme, že pre túto funkciu je potrebné zariadenie pod dohľadom

Obmedzenia aplikácie SysApp

Blokovanie konkrétnych aplikácií alebo funkcií zariadenia

Povolenie používania služby YouTube	Povolenie používania služby YouTube
Povolenie používania obchodu iTunes Store	Povolenie používania obchodu iTunes Store
Povolenie používania prehliadača Safari	Povolenie používania prehliadača Safari
Povolenie automatického vypĺňania	Umožňuje automatické vypĺňanie
Varovanie pred podvodmi	Vynúti upozornenie na podvod
Povolenie jazyka JavScript	Umožňuje používať JavaScript
Blokovanie vyskakovacích okien	Blokuje všetky druhy šteniatok
Povoliť súbory cookie	Výber, kedy bude Safari prijímať súbory cookie

App-VPN

Prostredníctvom tohto symbolu môžete definovať aplikácie, ktoré sa automaticky spustia pri spustení vybraného pripojenia VPN.

Nastavenia aplikácie

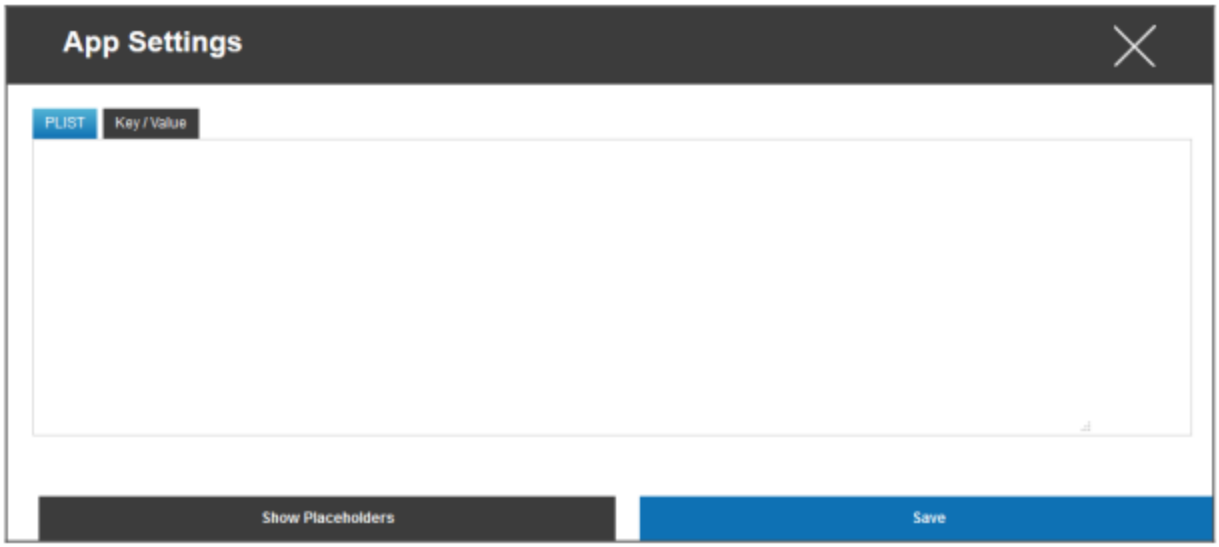
V časti "Nastavenia aplikácie" môžete aplikácii priradiť určité hodnoty do popredia (pokiaľ to aplikácia podporuje, v prípade potreby sa opýtajte vývojára aplikácie).

Prostredníctvom symbolu pridáte (ďalšiu) aplikáciu. Opäť nájdete známe zobrazenie AppTec360 App-Import.

Vyhľadajte tu aplikáciu, ktorú chcete nakonfigurovať, a vyberte ju. Nastavenia sa budú vzťahovať len na spravované aplikácie.

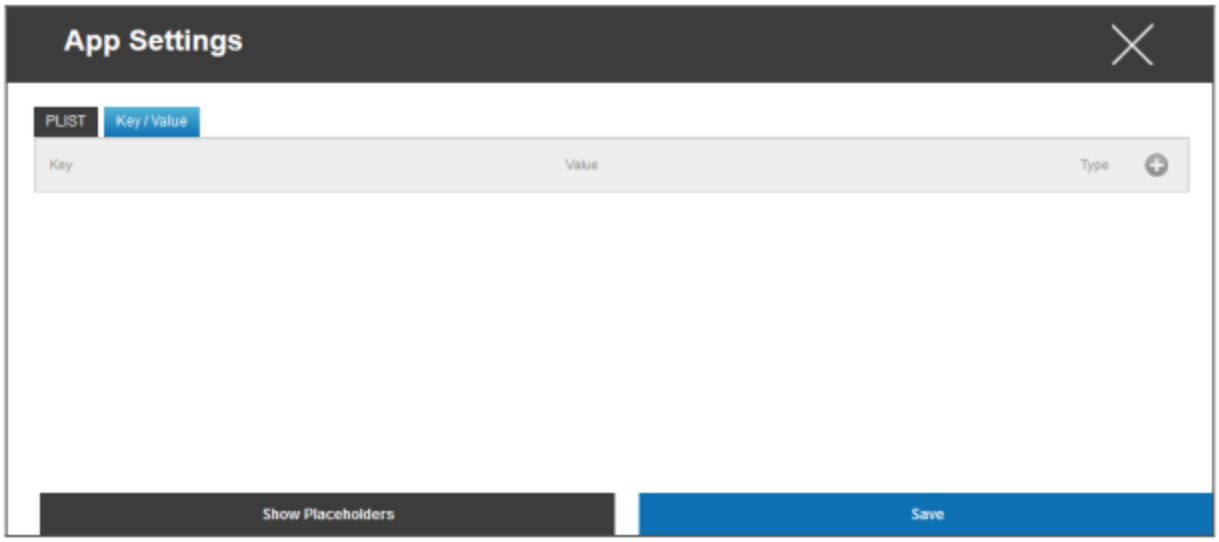
Ak by bol import úspešný, zobrazí sa nasledujúce zobrazenie:

Teraz môžete kliknutím na tlačidlo , vykonať rôzne konfigurácie. Potom sa zobrazí nasledujúci prehľad:

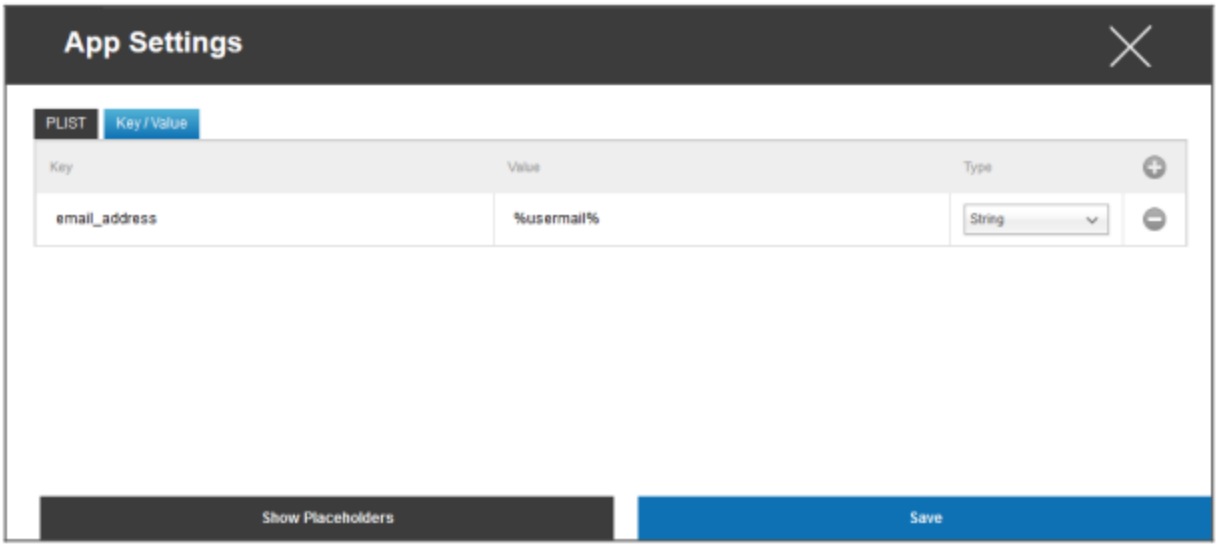


Ak už máte PLIST (zdrojový text konfigurácie), môžete ho sem pridať a všetko uložiť pomocou "Uložiť".

V časti "Kľúč / hodnota" môžete k aplikácii pripojiť konkrétne konfigurácie



Tu môžete vytvoriť nový kľúč a jeho hodnotu pomocou symbolu.



Samozrejme, k dispozícii máte všetky zástupné prvky AppTec

Vysvetlenie "Type":

String	Text
Boolean	Pravda/nepravda
Číslo	Číslo

Pomocou symbolu môžete aplikáciu opäť odstrániť.

Obchod s podnikovými aplikáciami

Aplikácie iTunes

V tomto bode môžete distribuovať voliteľné aplikácie pre používateľa.

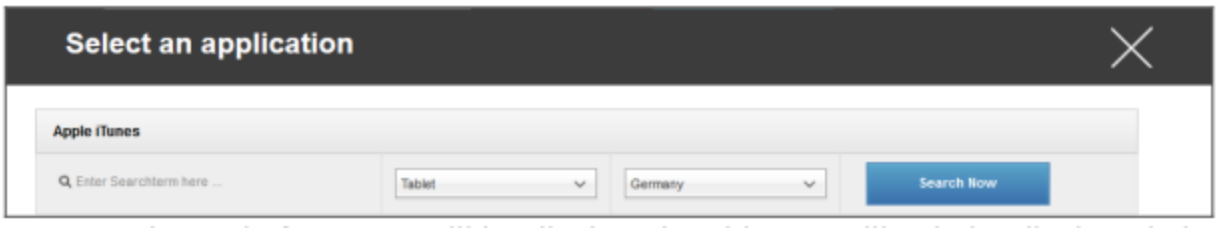
Ak sa tu nachádza aplikácia, automaticky sa nainštaluje do zariadenia koncového používateľa AppTec360 Store.

Sú to len odkazy na oficiálny obchod Apple App Store. Z tohto dôvodu musí byť každé zariadenie koncového používateľa vybavené Apple ID.

V tejto chvíli odporúčame, aby mal každý používateľ svoje vlastné Apple ID.

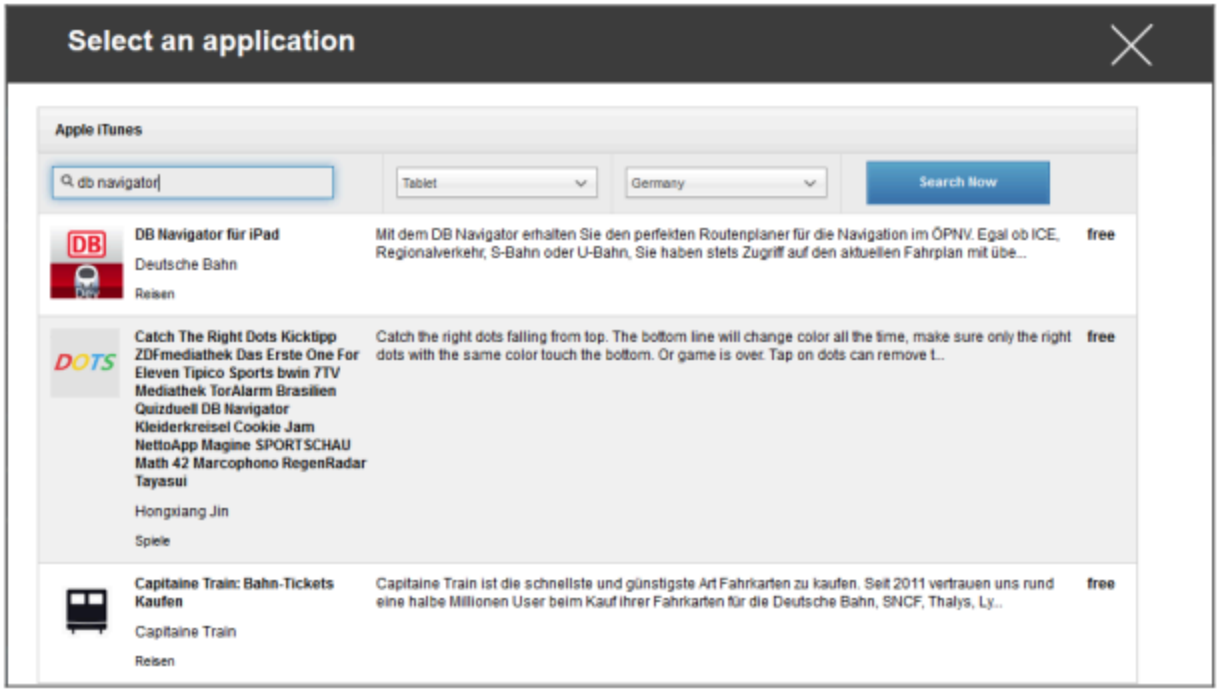
Pomocou symbolu môžete pridať ďalšie aplikácie.

Potom by sa malo otvoriť okno s nasledujúcim prehľadom.



Upozorňujeme, že sa zobrazia len bezplatné aplikácie, platené aplikácie sa zobrazia len cez VPN.

V časti "Zadajte tu hľadaný výraz..." môžete vyhľadať aplikáciu, ktorá sa nachádza v obchode Apple App Store.



Po kliknutí na ikonu alebo na názov aplikácie budete opäť vyzvaní na vykonanie ďalších konfigurácií.

Udržujte aktuálny stav	Raz týždenne sa určí, či je k dispozícii aktualizácia aplikácie. Ak áno, táto aktualizácia sa nainštaluje
Odstránenie aplikácie po odstránení profilu MDM	V prípade odstránenia správy zariadenia sa aplikácia odinštaluje
Zabránenie zálohovaniu údajov aplikácie	Záloha údajov špecifických pre aplikáciu sa nevytvorí
App-VPN	Vyberte pripojenie VPN, ktoré sa spustí po otvorení aplikácie

Po kliknutí na tlačidlo "Inštalovať" sa aplikácia pridá do podnikového obchodu s aplikáciami a následne sa môže nainštalovať do zariadenia koncového používateľa prostredníctvom AppTec360 AppStore.

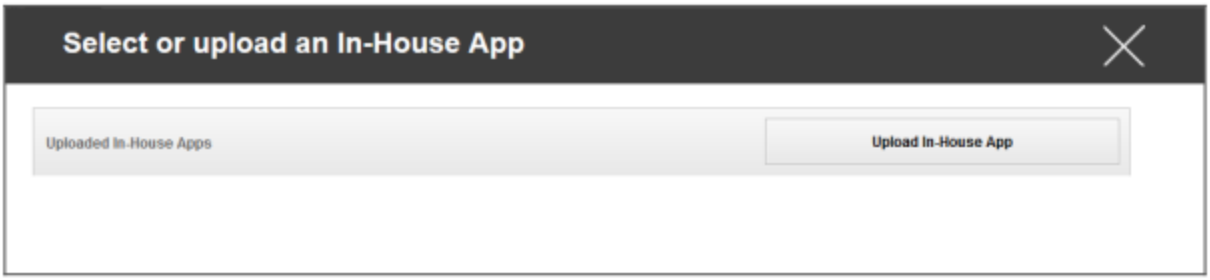
Ak bol import do App-Store úspešný, zobrazí sa nasledujúci prehľad:

Vnútorná stránka

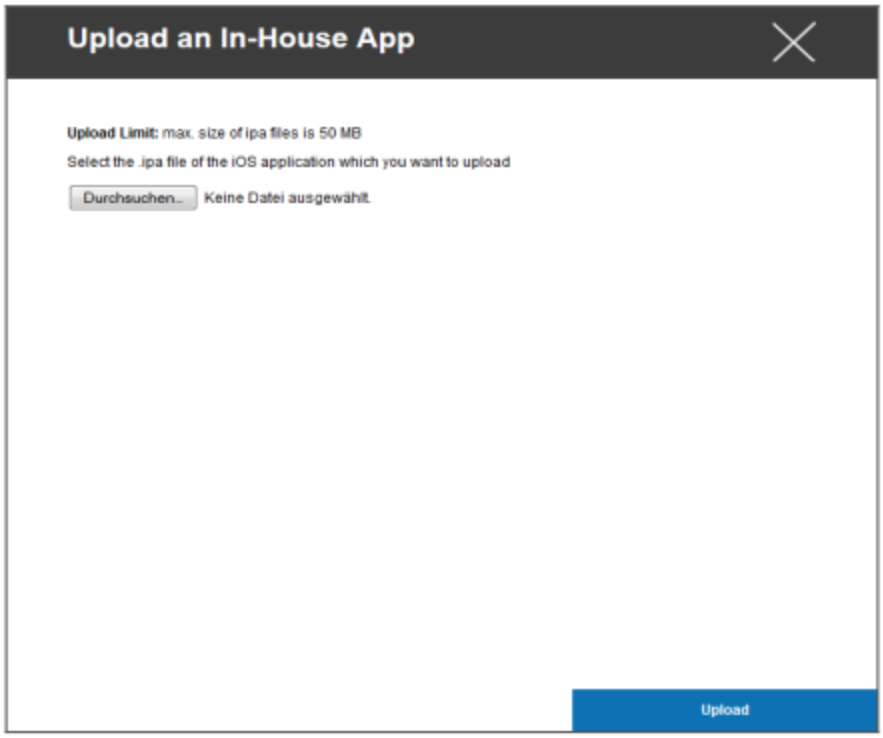
V bode "In-House" môžete nahrať interne vyvinuté aplikácie a distribuovať ich.

Pomocou tohto symbolu môžete distribuovať ďalšie aplikácie In-House.

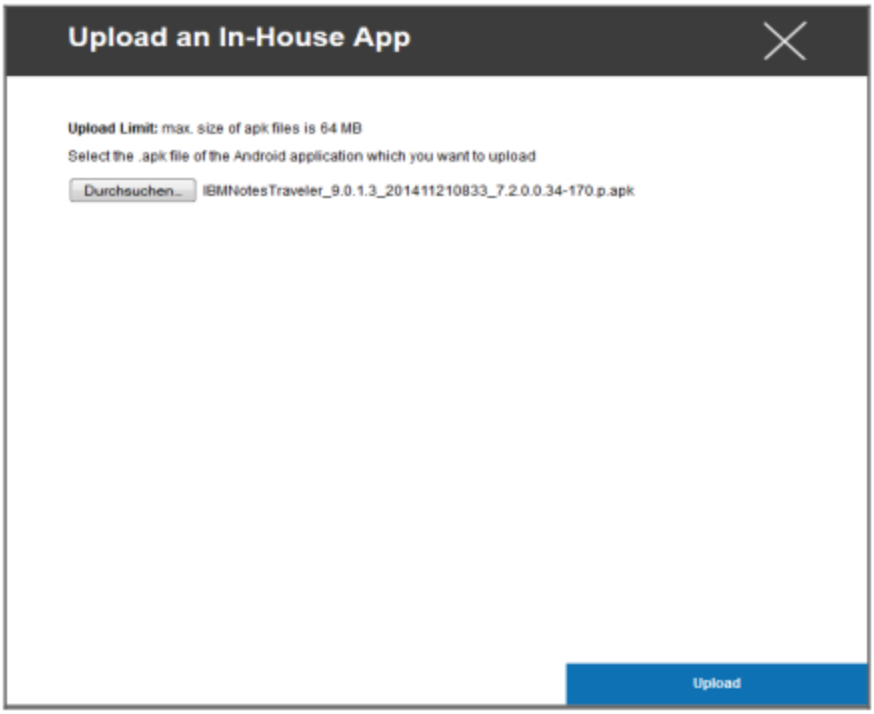
Ak ste nikdy nedistribuovali aplikáciu In-House, dostanete nasledujúci prehľad:



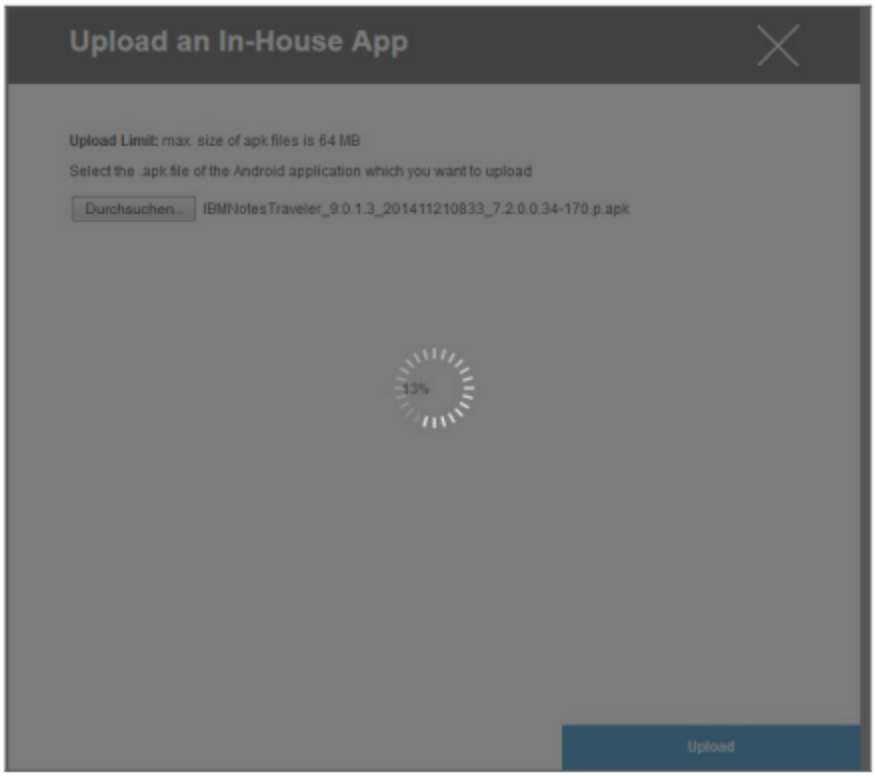
Na tento účel kliknite na položku "Upload In-House App", potom sa zobrazí nasledujúci prehľad:



Teraz vyberte pomocou "Search..." súbor .ipa a potom kliknite na "Upload".



Vaša aplikácia sa teraz nahrá. V strede kruhu môžete vidieť percentuálny údaj o tom, aká veľká časť vašej aplikácie už bola nahraná.



Ak sa odoslanie internej aplikácie úspešne vykonalo, uvidíte novo nahranú aplikáciu vo svojom Katalógu aplikácií.

Používateľ má teraz možnosť zobraziť a nainštalovať túto aplikáciu v obchode AppTec360 na zariadení koncového používateľa v kategórii "In-House".

Vzhľadom na to, že nejde o verejnú aplikáciu Apple AppStore, používateľ nepotrebuje uložené Apple ID v koncovom zariadení používateľa.

Režim kiosku

Režim iOS Kiosk je k dispozícii len v režime pod dohľadom

Režim Kiosk umožňuje vopred definovať aplikáciu alebo adresu URL tak, aby bolo možné spúšťať/navštevovať výlučne túto aplikáciu/URL.

Okrem toho môžete v režime Kiosk deaktivovať rôzne hardvérové tlačidlá.

Typ aplikácie

Balík

Ak chcete aplikáciu spustiť v režime kiosku, vyberte možnosť "Package" v časti "Application Type".

Aplikácia kiosku	Kliknite sem, aby ste vybrali aplikáciu, ktorá sa má spustiť v režime kiosku. Aktuálny prehľad správy aplikácií nájdete Môžete si vybrať medzi "Apple iTunes Apps" a "iOS In-House Apps".

ADRESA URL

Ak chcete v režime kiosku spustiť adresu URL, vyberte položku "URL" v časti "Typ aplikácie".

ADRESA URL	Teraz definujte požadovanú adresu URL
Politika rovnakého pôvodu	Ak je táto funkcia aktívna, používateľ môže surfovať len na podstránkach preddefinovanej adresy URL Ak ste napríklad definovali nasledujúcu adresu URL: www.mypage.com, potom môže používateľ surfovať na stránke www.mypage.com/subpage.
Adresy URL na bielej listine	Tu môžete udržiavať bielu listinu, všetky tieto adresy URL sú povolené Maximálne 1 adresa URL na riadok Adresa URL musí začínať http:/ alebo https://
Adresy URL na čiernej listine	Tu môžete udržiavať čiernu listinu, všetky tieto adresy URL sú zakázané. Maximálne 1 adresa URL na riadok Adresa URL musí začínať http:/ alebo https://
Vyčistiť prehliadač po nečinnosti	Po nečinnosti sa vyrovnávacia pamäť prehliadača vyprázdni
Povolené heslo pre ukončenie	Ak aktivujete túto funkciu, používateľ má možnosť ukončiť režim Kiosk pomocou hesla, ktoré ste vopred definovali.
Heslo pre ukončenie	Toto je vami preddefinované heslo.

Nastavenia režimu kiosku

Plánovaný režim kiosku	Na základe denného času môžete nastaviť režim kiosku tak, aby sa režim automaticky spustil a ukončil vo vopred určenom čase.
Čas začiatku	Čas začiatku
Čas v minútach	Čas v minútach, po ktorom sa má režim Kiosk opäť ukončiť
Zakázať dotykové ovládanie	Ak je aktivovaný, dotykový displej je deaktivovaný
Zakázanie otáčania zariadenia	Ak je aktivovaná, automatické prispôsobenie obrazovky je deaktivované
Vypnutie prepínača zvonenia	Ak je aktivovaný, prepínač zvonenia sa deaktivuje. Od tohto momentu je správanie závislé od predtým nastavenej funkcie
Zakázanie tlačidiel hlasitosti	Ak je aktivovaná, tlačidlá hlasitosti sa deaktivujú
Zakázanie tlačidla prebudenia v režime spánku	Ak je aktivovaný, vypínač sa deaktivuje
Zakázanie automatického uzamknutia	Ak je aktivovaný, zariadenie sa neprepne do pohotovostného režimu
Povolenie funkcie Voice Over	Ak je aktivovaný, aktivuje sa hlasový asistent
Povolenie zväčšenia	Ak je aktivované, aktivuje sa priblíženie
Povolenie invertovania farieb	Ak je aktivovaný, aktivuje sa režim inverzného zobrazenia
Povolenie asistovaného dotyku	Ak je aktivovaná, aktivuje sa funkcia AssistiveTouch
Povolenie výberu reči	Ak je aktivovaná, aktivuje sa voľba hovoriť
Povolenie mono zvuku	Ak je aktivovaný, aktivuje sa monofónny zvuk
VoiceOver	Ak je aktivovaná, používateľ môže povoliť funkciu VoiceOver
Priblíženie	Ak je aktivovaná, používateľ môže povoliť funkciu Zoom
Invertovanie farieb	Ak je aktivovaná, používateľ môže povoliť inverzné farby
Asistenčný dotyk	Ak je aktivovaná, používateľ môže povoliť asistenčné dotykové

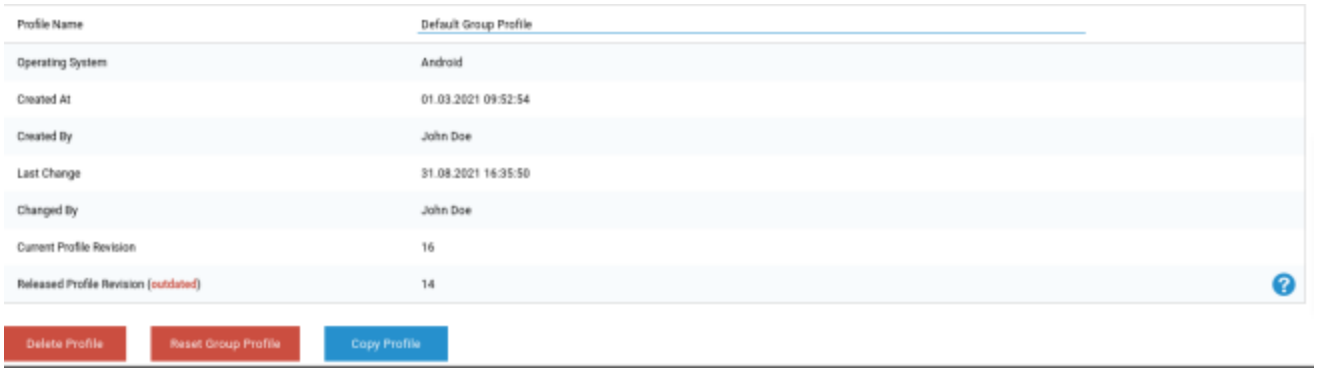
Android Enterprise – Plne spravovaná konfigurácia zariadenia

V závislosti od toho, či ste aktuálne vybrali profil skupiny alebo zariadenie, sa prehľad a jeho podbody líšia - zvážte to pozorne!

Všeobecné

Prehľad profilu skupiny (len na úrovni skupiny)

Po otvorení profilu skupiny sa zobrazí rýchly prehľad profilu.



Názov profilu	Názov profilu (tu sa dá zmeniť)
Operačný systém	Operačný systém, pre ktorý je profil určený
Vytvorené v	Čas vytvorenia
Vytvoril	Tvorca profilu
Posledná zmena	Čas poslednej zmeny profilu
Zmenené podľa	Účet, ktorý vykonal posledné zmeny
Aktuálna revízia profilu	Revízia uloženého stavu profilu
Vydaná revízia profilu	Priradená revízia profilu ("Priradiť teraz"). Ak sa za textom na štítku zobrazí " (zastaraný)", znamená to, že ste profil uložili, ale ešte ste ho nepriradili, takže zariadenia budú stále dostávať staršiu verziu.

Prehľad zariadení (len na úrovni zariadenia)

Ak sa nachádzate na zariadení, zobrazí sa prehľadné zhrnutie vybraného zariadenia, ktoré obsahuje nasledujúce informácie:

Názov zariadenia	Názov zariadenia
Umiestnenie	Súradnice polohy
Telefónne číslo	Telefónne číslo
Priradené povinné aplikácie	Počet pridelených povinných aplikácií
Verzia operačného systému	Verzia operačného systému zariadenia
Operačný systém	Operačný systém (Android Enterprise)
Sériové číslo	Sériové číslo zariadenia
Vlastníctvo zariadenia	Firemné alebo súkromné zariadenie
Typ zariadenia	AE Work Spravované zariadenie
Zakorenené	Stav, ktorý uvádza, či bolo zariadenie rootnuté
V súlade s	V súlade s usmerneniami
IP adresa	IP adresa zariadenia
Naposledy videné	Bod v čase, kedy sa zariadenie naposledy pripojilo k AppTecu
Posledný impulz	Bod v čase, keď bol do zariadenia odoslaný posledný push
Režim vlastníka zariadenia AE	Áno
Priradenie používateľa	Používateľ alebo skupina, ku ktorej je toto zariadenie priradené

Revízia konfigurácie (len na úrovni zariadenia)

Tu získate prehľad o tom, ktorý skupinový profil je priradený k zariadeniu.

Ak kliknete na profil skupiny, získate priamy prístup k tomuto profilu a môžete vykonať nastavenia.

Pomocou tohto symbolu môžete vrátiť distribuované aplikácie do nastavení profilu skupiny.

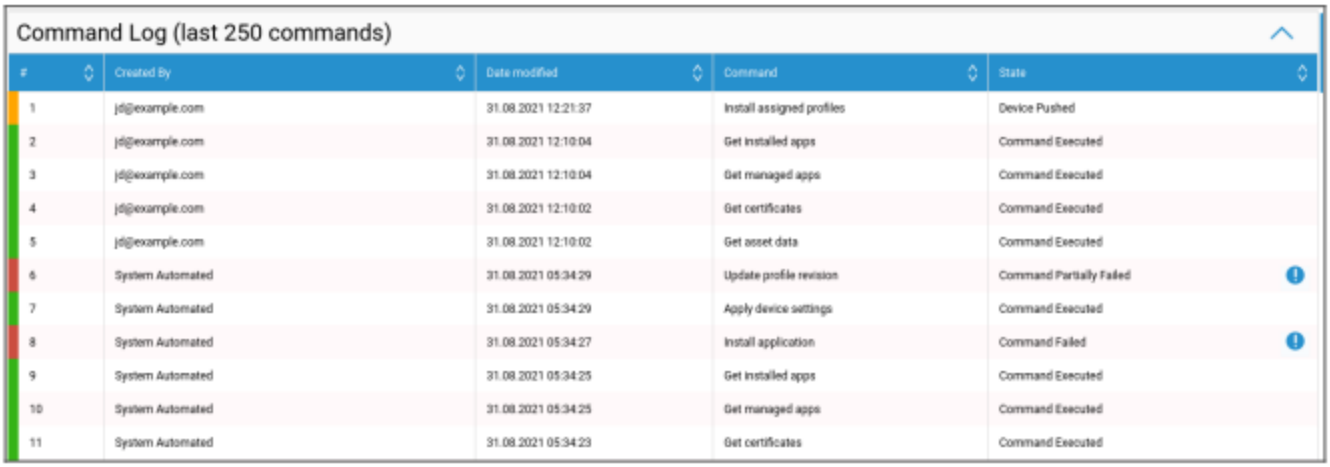
Pomocou tohto symbolu môžete vrátiť všetky používané aplikácie do nastavení skupinového profilu.

"K dispozícii je novšia revízia" znamená, že profil skupiny bol zmenený a uložený, ale nie je priradený. Profil skupiny sa musí priradiť pomocou "Priradiť teraz" na úrovni skupiny, aby sa zmeny uplatnili na zariadeniach.

Protokol zariadenia (len na úrovni zariadenia)

Denník príkazov

Tu môžete vidieť, ktoré príkazy boli pre zariadenie vydané a aký je ich stav.



Príkazy vytvorené pomocou "System Automated" sú automaticky vytvorené systémom.

Možné stavy príkazov

Stlačené zariadenie	Do služby push (napr. APNS) bola odoslaná požiadavka na pripojenie, aby sa zariadenie pripojilo späť k serveru EMM.
Vytvorený príkaz	Príkaz bol vytvorený v systéme.
Odoslaný príkaz	Príkaz sa odoslal do zariadenia po jeho pripojení k serveru.
Vykonaný príkaz	Príkaz bol úspešne vykonaný.
Príkaz zlyhal	Príkaz zlyhal. *
Príkaz čiastočne zlyhal	V závislosti od operačného systému zariadenia môžu byť niektoré príkazy zoskupené. V tejto časti tejto skupiny príkazov zlyhali niektoré časti. *
Príkaz vykonaný, prípadne neúspešný	Príkaz bol vykonaný, ale možno nebol.
Príkaz Repushed	Príkaz bol opätovne odoslaný používateľom.
Vyradené	Príkaz bol zamietnutý. Napríklad preto, že bol nahradený iným príkazom alebo zariadenie bolo znovu zaregistrované a staré príkazy boli odstránené.

Ak sa za správou nachádza výkričník, môžete získať ďalšie informácie tak, že kurzorom prejdete nad ikonu.

Nastavenia zariadenia

Konfigurácia klienta

Tu môžete vykonať nasledujúce konfigurácie zariadenia so systémom Android:

Čas mimo súladu	Časový limit reakcie používateľa, po uplynutí ktorého sa uplatní akcia vynucovania.
Opatrenia na presadzovanie práva po uplynutí lehoty na dosiahnutie súladu	Ak používateľ nevykoná činnosti, ktoré vedú k dosiahnutiu stavu zariadenia, ktoré je v súlade s predpismi, vykoná sa vynucovacia akcia.
Frekvencia zberu údajov	Frekvencia zberu informácií o zariadení/GPS
Frekvencia srdcového tepu zariadenia	Interval, v ktorom má zariadenie kontaktovať server AppTec360 Min. 1 minúta Max. 24 hodín
Povolenie aktualizácií polohy	Ak je aktivované, zariadenie posiela aktualizácie polohy na server AppTec360
Čas aktualizácie polohy	Určuje, v akých časových intervaloch zariadenie odosiela aktualizácie polohy do AppTec360
Používanie služby Google Location Accuracy na aktualizáciu polohy	Ak je aktivovaná, pre aktualizácie polohy sa bude používať sieťová poloha (ak bola deaktivovaná v časti "Obmedzenia", toto nastavenie nebude mať žiadny vplyv).
Používanie polohy GPS na aktualizáciu polohy	Ak je aktivovaná, GPS sa bude používať na aktualizáciu polohy
Povolenie falošných lokalít	Umožňuje falšovanie informácií o polohe prostredníctvom aplikácií tretích strán
Akcia strateného spojenia	Ak je táto možnosť povolená, môžete určiť akciu pre prípad, že zariadenie nezíska spojenie so serverom MDM v intervale srdcového tepu. Napríklad ak má zariadenie čas srdcového tepu 5 minút, pripojí sa k serveru o 10:35. Potom zariadenie opustí dosah siete Wi-Fi. Ďalší srdcový úder o 10:40 sa nepodarí vykonať a vykoná sa zadaná akcia.
Akcia	Opatrenia, ktoré sa majú prijať, akonáhle sa zariadenie stane nevyhovujúcim. • Uzamknúť zariadenie = uzamknúť zariadenie

	• Vymazať zariadenie = zariadenie sa obnoví na výrobné nastavenia • Vymazať zariadenie a kartu SD = zariadenie sa obnoví do továrenských nastavení a úložisko karty SD sa vymaže
Prahová hodnota	Môžete určiť prahový počet zlyhaných srdcových úderov, ktoré sú potrebné na spustenie zadanej akcie.

Režim presadzovania zásad	Predvolené nastavenie:	Používatelia budú pravidelne vyzývaní na vykonanie nevykonaných akcií
	Lenivé presadzovanie zásad:	Používatelia nebudú nikdy vyzvaní na vykonanie nevykonaných akcií. Všetky otvorené akcie sa zobrazia v aplikácii AppTec360 Client
	Agresívne presadzovanie zásad:	Používatelia budú nepretržite vyzývaní na vykonanie nevykonaných akcií
Zámok verzie AppTec360	Ak je táto možnosť povolená, je možné zadať kód verzie klienta AppTec360 MDM. Klient AppTec360 sa aktualizuje len na zadanú verziu. Novšie verzie sa budú ignorovať. Zníženie aktualizácie NIE JE možné.	
Kód verzie	Kód verzie pre klienta AppTec360 MDM, ktorý má byť uzamknutý.	
Zakázanie oznámenia AppTec360	Ak je vypnuté, klient AppTec360 nezobrazí oznámenie v paneli oznámení. Používatelia tak môžu klienta AppTec360 zavrieť prostredníctvom správcu úloh. Ak je klient AppTec360 zatvorený, niekoľko funkcií vrátane režimu Kiosk a čiernej/bielej listiny aplikácií nebude fungovať správne. Zariadenia Samsung ponúkajú ochranný mechanizmus pre klienta AppTec360. V zariadeniach Samsung, ktoré podporujú rozhranie KNOX API, je toto upozornenie predvolene vypnuté. Oznámenie by nemalo byť vypnuté na zariadeniach so systémom Android 8.0 alebo vyšším.	

Tapety

Nastavenie vlastnej tapety	Povolenie/zakázanie vlastnej tapety
Tapety	Nastavenie režimu tapety na použitie farebného kódu alebo obrázka
Zadanie farby	Zadajte farbu pozadia ako hexadecimálnu hodnotu, napr. #000000 pre čiernu alebo #ffffff pre bielu.
Nastavenie obrázka ako tapety	Nahrajte súbor s obrázkom, ktorý chcete použiť ako tapetu

Správa aktív (len na úrovni zariadenia)

Informácie o zariadení

Model	Označenie modelu zariadenia
Operačný systém	OS
Verzia operačného systému	Verzia operačného systému
Sériové číslo	Sériové číslo
Názov zariadenia	Názov zariadenia
Stav batérie	Stav batérie
Voľná / celková pamäť	Voľná / celková pamäť
Samsung Safe	Rozhranie Samsung SAFE, potrebné pre rôzne možnosti nastavenia
K dispozícii je karta SD	K dispozícii je karta SD
Emulovaná karta SD	Emulovaná karta SD
Vymeniteľná karta SD	Vymeniteľná karta SD
SD Voľná / celková pamäť	SD Voľná / Celková pamäť karty SD

Wi-Fi

IP adresa	IP adresa zariadenia
WiFi MAC	Adresa MAC WiFi

Cellular

Stav	Stav (nainštalovaná karta SIM)
Telefónne číslo	Telefónne číslo
Roaming (hlas / dáta)	Roaming pre hlas / dáta
Stav roamingu	Aktuálny stav roamingu
IP adresa	IP adresa
Prevádzkovateľ/prepravca	Prevádzkovateľ/prepravca
Mobilná technológia	Mobilná technológia
IMEI	Číslo IMEI
ICCID	Ide o identifikátor karty SIM, často aj karty Smartcard alebo karty s integrovaným obvodom (ICC).
IMSI	Medzinárodná identita mobilného účastníka (IMSI) poskytuje v mobilných sieťach GSM a UMTS jednoznačnú identifikáciu používateľov siete. IMSI pozostáva z maximálne 15 číslic a konfiguruje sa takto: • Kód mobilnej krajiny (MCC), 3 číslice • Kód mobilnej siete (MNC), 2 alebo 3 číslice • Identifikačné číslo mobilného účastníka (MSIN), 1-10 číslic
Súčasné MCC/MNC	Pozri "SIM MCC/MNC".
SIM MCC/MNC	Kód mobilnej krajiny je zavedený identifikátor krajiny, ktorý stanovila ITU podľa normy E.212. Funguje v spojení s kódom mobilnej siete (MNC) na identifikáciu mobilnej siete. Znamená kód krajiny/mobilnej siete karty SIM. Ak sa pohybujete v inej mobilnej sieti, potom sa logicky budú "Aktuálne MCC/MNC" a "SIM MCC/MNC" líšiť.

Bluetooth

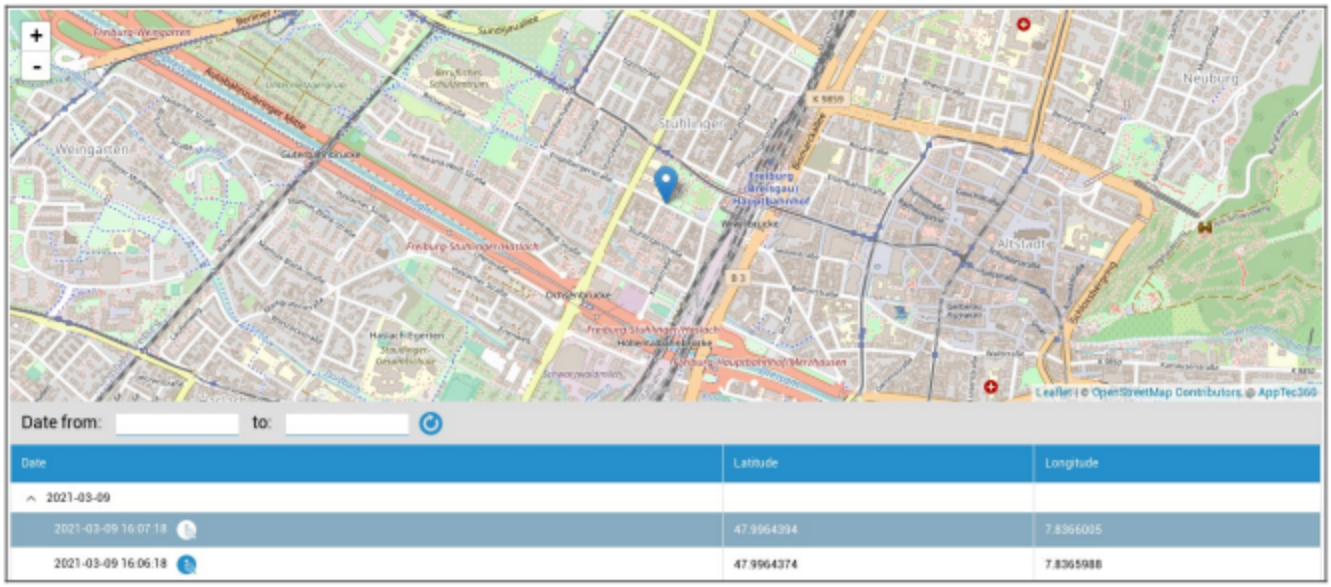
Bluetooth MAC	Adresa MAC Bluetooth

Riadenie bezpečnosti

Ochrana proti krádeži (len na úrovni zariadenia)

Informácie GPS (len na úrovni zariadenia)

Tu môžete určiť aktuálne/posledné umiestnenie zariadenia. Lokalizácia môže byť chránená jedným alebo dokonca dvoma heslami - pozri: Všeobecné nastavenia - Súkromie - Prístup k GPS



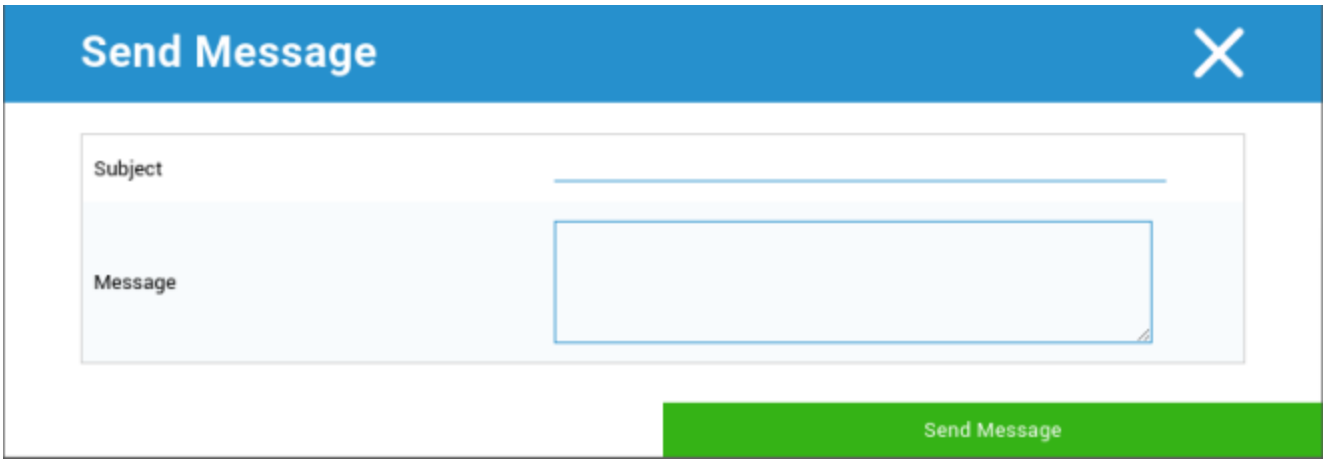
Vyčistiť a uzamknúť (len na úrovni zariadenia)

V časti "Vyčistiť a uzamknúť" môžete vykonať nasledujúce tri akcie:

Úplné utretie	Zariadenie sa obnoví do továrenského nastavenia (vymažú sa firemné aj osobné údaje).
Podnik Wipe	Zo zariadenia koncového používateľa sa odstránia len firemné údaje (všetky aplikácie, údaje atď., ktoré poskytla spoločnosť AppTec360)
Uzamknutie obrazovky	Ak je aktivovaný zámok obrazovky, stačí zariadenie odomknúť pomocou hesla zariadenia/PIN kódu.

Správa (len na úrovni zariadenia)

Tu môžete vyplniť predmet a správu a odoslať ju koncovému používateľskému zariadeniu.



Konfigurácia zabezpečenia

Prístupový kód zariadenia

V časti "Prístupový kód" môžete povoliť heslo zariadenia, pričom máte k dispozícii tieto možnosti nastavenia

Minimálna dĺžka hesla	stanovuje minimálny počet symbolov, ktoré musí heslo obsahovať	
Kvalita hesla	Nešpecifikované	Táto zásada nemá žiadne požiadavky na heslo.
	Biometrické Slabé	Táto politika umožňuje použitie biometrickej technológie rozpoznávania s nízkou úrovňou zabezpečenia. To znamená technológie, ktoré dokážu rozpoznať totožnosť jednotlivca približne na úrovni trojmiestneho PIN kódu (falošná detekcia je menej ako 1 z 1 000).
	Niečo	Táto zásada vyžaduje nastavenie nejakého hesla alebo vzoru, ale nevynucuje žiadne konkrétne pravidlá.
	Abecedné	Používateľ musí zadať heslo obsahujúce aspoň znaky abecedy (alebo iný symbol).
	Alfanumerické	Používateľ musí zadať heslo, ktoré obsahuje aspoň číselné a abecedné (alebo iné znaky).
	Komplex	Používateľ musí štandardne zadať heslo obsahujúce aspoň jedno písmeno, jednu číslicu a špeciálny symbol. Pomocou tejto kvality hesla možno obmedziť, aby heslá obsahovali rôzne sady znakov, napríklad aspoň veľké písmeno atď.
Minimálna dĺžka hesla	Nastavte požadovaný počet znakov pre heslo. Môžete napríklad vyžadovať, aby PIN alebo heslá mali aspoň šesť znakov.	
Minimálne číselné znaky požadované v hesle	Minimálne číselné znaky požadované v hesle	
Minimálny počet malých písmen v hesle	Minimálny počet malých písmen v hesle	
Minimálny počet veľkých písmen v hesle	Minimálny počet veľkých písmen v hesle	

Minimálny počet nepísmenových znakov požadovaných v hesle	Minimálny počet nepísmenových znakov požadovaných v hesle
Minimálne požadované symboly v hesle	Minimálne požadované symboly v hesle

Maximálny čas blokovania nečinnosti	Maximálna nečinnosť používateľa do časového uzamknutia
Časový limit vypršania platnosti hesla	stanovuje, po uplynutí ktorého časového intervalu heslo vyprší a musí sa vydať nové heslo
Obmedzenie histórie hesiel	Počet predtým použitých hesiel, ktoré nie sú povolené
Maximálny počet neúspešných pokusov o zadanie hesla	stanovuje, ako často môže byť heslo zadané nesprávne, kým sa vykoná úplné vymazanie zariadenia
Povolenie biometrického overovania	Umožňuje overovanie pomocou odtlačku prsta alebo skenovania dúhovky. Len pre Samsung KNOX 2.1 a vyššie

AntiVirus

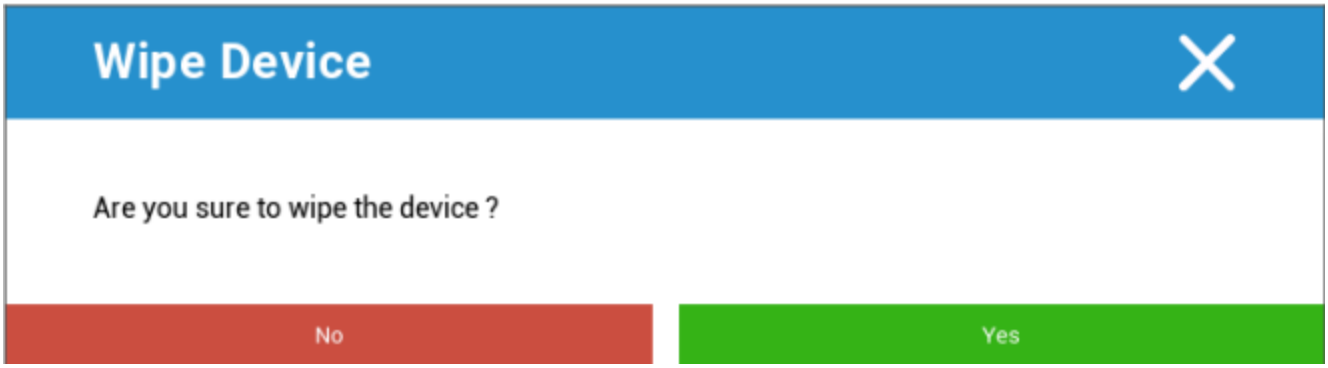
Automatické skenovanie	Povolenie pravidelného automatického skenovania
Interval skenovania	Interval vyšetrenia (rýchly/úplný)
Úplné automatické skenovanie	Povolenie úplného automatického skenovania
Automatické aktualizácie	Povolenie automatických aktualizácií
Interval kontroly aktualizácie	Ako často by sa mala aplikácia a jej databáza aktualizovať (vírusy/poškodený kód)
Ochrana aplikácií	Povolenie automatického skenovania aplikácií
Ochrana karty SD	Povolenie automatického skenovania karty SD
Aktualizácia iba Wi-Fi	Ak je táto možnosť povolená, aktualizácie sa použijú len vtedy, keď je zariadenie úspešne pripojené k sieti Wi-Fi.

Koniec životnosti (len na úrovni zariadenia)

Vyčistiť (len na úrovni zariadenia)

V časti "Vymazať" môžete obnoviť výrobné nastavenia zariadenia. V tomto prípade sa v zariadení koncového používateľa vymažú firemné, ako aj súkromné údaje.

Po kliknutí na symbol mínus sa zobrazí nasledujúca správa:



Pomocou možnosti "Áno" môžete vykonať vymazanie.

V časti "Wipe Report" sa môžu zobraziť tieto položky

Zotreté	História toho, kto vykonal utretie
Dátum	Dátum
Stav	Stav (napr. či bolo vymazanie vykonané úspešne)

Nastavenia obmedzenia

Obmedzenia

Tu je možné obmedziť a zablokovať rôzne veci.

Povolenie kamery	Povolenie používania kamery	
Vynútiť automatickú synchronizáciu	Na stránke	Synchronizácia je trvalo aktivovaná
	Vypnuté	Synchronizácia je trvalo deaktivovaná
	Výber používateľa	Vybral používateľ
Vynútiť Bluetooth	Na stránke	Bluetooth je trvalo aktivované
	Vypnuté	Bluetooth je trvalo deaktivované
	Výber používateľa	Vybral používateľ
Force GPS	Na stránke	GPS je trvalo aktivované
	Vypnuté	GPS je trvalo deaktivované
	Výber používateľa	Vybral používateľ
Umiestnenie siete Force	Na stránke	Trvalá lokalizácia na internete
	Vypnuté	Trvalá deaktivácia lokalizácie internetu
	Výber používateľa	Vybral používateľ

Zabezpečenie		
Zakázať zdieľanie umiestnenia	Určuje, či je používateľovi zakázané zapnúť zdieľanie polohy.	
Zakázať bezpečné spustenie systému	Určuje, či používateľ nesmie reštartovať zariadenie do núdzového režimu.	
Zakázať resetovanie siete	Určuje, či je používateľovi zakázané resetovať sieťové nastavenia z Nastavení.	
Zakázať obnovenie továrenských nastavení	Určuje, či je používateľovi zakázané resetovať zariadenie.	
Povolenie ADB	Umožňuje pripojenie k počítaču prostredníctvom ADB	
Zakázanie funkcie Keyguard	Vypnutie funkcie Keyguard	
Informácie o uzamknutej obrazovke vlastníka zariadenia	Nastavenie informácií o vlastníkovi zariadenia, ktoré sa majú zobrazovať na uzamknutej obrazovke.	
Presadzovanie súladu	Režim Výzva Používateľ	Používateľ bude vyzvaný na vykonanie potrebných úkonov.
	Kontajner s uzamknutým režimom	Skryť všetky aplikácie, kým nie sú splnené všetky požiadavky

Správa aplikácií	
Povolenie prepojenia aplikácií medzi profilmi	Umožňuje aplikáciám v nadradenom profile spracúvať webové odkazy zo spravovaného profilu.
Zakázať ovládanie aplikácií	Určuje, či je používateľovi zakázané upravovať aplikácie v Nastaveniach alebo spúšťacích programoch.
Zakázať inštaláciu aplikácií	Určuje, či je používateľovi zakázané inštalovať aplikácie.
Zakázať odinštalovanie aplikácií	Určuje, či je používateľovi zakázané odinštalovať aplikácie.
Zásady oprávnení počas behu	Určuje, ako sa budú spracovávať nové žiadosti o povolenie od aplikácií.
Povolenie neznámych zdrojov	Ak je táto funkcia povolená, používatelia môžu aplikácie načítavať zboku inštaláciou súboru .apk.

Pripojenie	
Zakázať konfiguráciu mobilnej siete	Určuje, či je používateľovi zakázané konfigurovať mobilné siete.
Zakázať konfiguráciu tetheringu	Určuje, či je používateľovi zakázané konfigurovať Tethering a prenosné hotspoty.
Zakázať konfiguráciu VPN	Určuje, či je používateľovi zakázané konfigurovať sieť VPN.
Zakázať konfiguráciu Wifi	Určuje, či je používateľovi zakázané meniť prístupové body WiFi.
Zakázanie odchádzajúceho lúča NFC	Určuje, či používateľ nesmie používať NFC na prenos údajov z aplikácií.
Konfigurácia uzamknutia WiFi	Toto nastavenie určuje, či majú byť konfigurácie WiFi vytvorené aplikáciou Vlastník zariadenia uzamknuté (t. j. či ich môže upravovať alebo odstraňovať iba aplikácia Vlastník zariadenia, nie však ani aplikácia Nastavenia).
Povolenie dátového roamingu	Aktivácia dátového roamingu

Bluetooth	
Zakázať pripojenie Bluetooth	Určuje, či je v zariadení zakázaný bluetooth. Vyžaduje systém Android 8.0
Zakázanie zdieľania cez Bluetooth	Určuje, či je v zariadení zakázané odchádzajúce zdieľanie cez bluetooth. Vyžaduje systém Android 8.0
Zakázať konfiguráciu Bluetooth	Určuje, či je používateľovi zakázané konfigurovať bluetooth.

Správa účtov	
Zakázať pridávanie spravovaného profilu	Určuje, či je používateľovi zakázané pridávať spravované profily. Vyžaduje Android 8.0
Zakázať pridávanie používateľov	Určuje, či je používateľovi zakázané pridávať nových používateľov.
Zakázať Odstrániť spravovaný profil	Určuje, či spravované profily tohto používateľa môžu byť odstránené inak ako jeho vlastníkom profilu. Vyžaduje Android 8.0
Zakázať úpravu účtu	Určuje, či je používateľovi zakázané pridávať a odstraňovať účty, pokiaľ ich program Authenticator nepridá programovo.

Telefonovanie	
Zakázať odchádzajúce hovory	Určuje, že používateľ nemá povolené uskutočňovať odchádzajúce telefónne hovory.
Zakázať SMS	Určuje, že používateľ nemá povolené odosielať alebo prijímať SMS správy.

Systém	
Zakázať vytváranie okien	Určuje, že okrem okien aplikácie sa nemajú vytvárať žiadne iné okná.
Zakázať nastaviť ikonu používateľa	Určuje, či používateľ nesmie zmeniť svoju ikonu.
Zakázať nastavenie tapety	Obmedzenie používateľa na zakázanie nastavenia tapety.
Zakázanie stavového riadka	Zakázanie stavového riadka blokuje oznámenia, rýchle nastavenia a ďalšie prekrytia obrazovky, ktoré umožňujú únik z jednorazového zariadenia.
Povolenie automatického času	Automaticky nastaví čas.
Povolenie automatického časového pásma	Automaticky nastaví časové pásmo.
Zostať zapnutý, keď je pripojený k sieti	Zariadenie zostane aktívne, kým je pripojené k zdroju napájania.

Úložisko	
Zakázať zakázanie overovania aplikácií	Určuje, či je používateľovi zakázané vypnúť overovanie aplikácie.
Zakázať pripojenie fyzických médií	Určuje, či je používateľovi zakázané pripájať fyzické externé médiá.
Povolenie služby zálohovania	Služba zálohovania spravuje všetky mechanizmy zálohovania a obnovy v zariadení. Nastavenie tejto hodnoty na false zabráni zálohovaniu alebo obnove údajov. Služba zálohovania je v predvolenom nastavení vypnutá. Vyžaduje systém Android 8.0
Povolenie veľkokapacitného úložiska USB	Povolí používanie veľkokapacitného úložiska USB.

Klávesnica	
Zakázať automatické vypĺňanie	Určuje, či používateľ nesmie používať služby automatického vypĺňania. Vyžaduje Android 8.0
Zakázať kopírovanie a vkladanie medzi profilmi	Určuje, či to, čo sa skopíruje do schránky tohto profilu, možno vložiť do súvisiacich profilov.

Zvuk	
Zakázať úpravu objemu	Určuje, či je používateľovi zakázané upravovať hlavnú hlasitosť.
Zakázať vypnutie mikrofónu	Určuje, či je používateľovi zakázané nastavovať hlasitosť mikrofónu.
Zariadenie na stlmenie zvuku	Zariadenie na stlmenie zvuku.

Správa certifikátov

Tu môžete distribuovať dôveryhodné certifikáty a certifikáty identity do svojich zariadení.

Na distribúciu dôveryhodných certifikátov je potrebný systém Android 8 alebo novší a na distribúciu certifikátov identity je potrebný systém Android 9 alebo novší.

Pomocou "+" môžete pridať viacero certifikátov.

Dôveryhodné certifikáty musia byť vo formáte PEM.

Certifikáty totožnosti musia byť vo formáte PKCS12

Správa pripojenia

Wifi

Pre toto nastavenie vykonajte predbežnú konfiguráciu zariadení koncových používateľov pre prístup k interným prístupovým bodom

.

Identifikátor súboru služieb (SSID)	SSID pre sieť, ktorá sa má pripojiť
Skrytá sieť	Aktivácia v prípade, že prístupový bod nevysiela identifikátor SSID

Typ zabezpečenia

Stanovenie typu zabezpečenia prístupového bodu

WEP

Heslo	Heslo pre AP

WPA/WPA2

Heslo	Heslo pre AP

802.1x EAP

Metóda EAP

PWD	Identita	Identita
	Heslo	Heslo

PEAP	Fáza 2 autentifikačného protokolu	žiadne	Žiadny dodatočný protokol
		MSCHAPV2	Protokol MSCHAPV2
		GTC	Protokol GTC
	Certifikát CA	Certifikát CA	
	Identita	Identita	
	Anonymná identita	Anonymná identita	
	Heslo	Heslo	

TTLS	Fáza 2 autentifikačného protokolu	žiadne	Žiadny dodatočný protokol
		PAP	Protokol PAP
		MSCHAP	Protokol MSCHAP
		MSCHAPV2	Protokol MSCHAPV2
		GTC	Protokol GTC
	Certifikát CA	Certifikát CA	
	Identita	Identita	
	Anonymná identita	Anonymná identita	
	Heslo	Heslo	

TLS	Certifikát CA	Certifikát CA
	Identita	Identita
	Heslo	Heslo

VPN

Názov pripojenia	Názov pripojenia VPN

Typ VPN

VPN

Klient VPN

Klient VPN AppTec360	
Konfigurácia brány	Vyberte konfiguráciu brány VPN (pozri **Všeobecné nastavenia > Univerzálna brána > Nastavenia VPN**).
Vždy zapnutá sieť VPN	Povolenie funkcie Native Lockdown
Povolenie uzamknutia AppTec360	Povolenie uzamknutia AppTec360

Zabudované (k dispozícii len v zariadeniach Samsung)			
Typ pripojenia	PPTP	Server	Server
		Povolenie šifrovania PPTP	Povolenie šifrovania PPTP
	L2TP / IPSec PSK	Server	Server
		Predsdieľaný kľúč IPSec	Predsdieľaný kľúč IPSec
		Povolenie funkcie L2TP Secret	Povolenie funkcie L2TP Secret
		Tajomstvo L2TP	Tajomstvo L2TP
	IPSec XAuth PSK	Server	Server
		Identifikátor IPSec	Identifikátor IPSec
		Predsdieľaný kľúč IPSec	Predsdieľaný kľúč IPSec
Vyhľadávanie domén DNS	Vyhľadávanie domén DNS		
Expertné nastavenia	Servery DNS	Servery DNS	
	Trasy preposielania	Trasy preposielania	

Otvorená sieť VPN		
Server	Server	
Profil OpenVPN	Profil OpenVPN	
Aplikácia OpenVPN	OpenVPN pre Android (odporúčané)	
	Pripojenie OpenVPN	
Expertné nastavenia	Servery DNS	Servery DNS
	Trasy preposielania	Trasy preposielania

Samsung / Strong Swan			
Typ pripojenia	PPTP	Server	Server
		Používateľské meno	Používateľské meno
		Heslo	Heslo
		Povolenie šifrovania PPTP	Povolenie šifrovania PPTP
	L2TP / IPSec PSK	Server	Server
		Predsdieľaný kľúč IPSec	Predsdieľaný kľúč IPSec
		Používateľské meno	Používateľské meno
		Heslo	Heslo
		Povolenie funkcie L2TP Secret	Tajomstvo L2TP
	IPSec XAuth PSK	Server	Server
		Identifikátor IPSec	Identifikátor IPSec
		Predsdieľaný kľúč IPSec	Predsdieľaný kľúč IPSec
		Používateľské meno	Používateľské meno
		Heslo	Heslo
Expertné nastavenia	Servery DNS	Servery DNS	
	Trasy preposielania	Trasy preposielania	

Cisco Any Connect		
Server	Server	
Režim certifikátu	Bezbariérový	Bezbariérový
	Automatické	Automatické
Expertné nastavenia	Servery DNS	Servery DNS
	Trasy preposielania	Trasy preposielania

Sieť VPN pre jednotlivé aplikácie

Klient VPN

Klient VPN AppTec360		
Konfigurácia brány	Vyberte konfiguráciu brány VPN (pozri **Všeobecné nastavenia > Univerzálna brána > Nastavenia VPN**).	
Aplikácie VPN	Aplikácie VPN	
Vždy zapnutá sieť VPN	Povolenie funkcie Native Lockdown	Vždy zapnutá sieť VPN
Povolenie uzamknutia AppTec360	Povolenie uzamknutia AppTec360	

Samsung / Strong Swan			
Typ pripojenia	PPTP	Server	Server
		Aplikácie VPN	Aplikácie VPN
		Používateľské meno	Používateľské meno
		Heslo	Heslo
		Povolenie šifrovania PPTP	Povolenie šifrovania PPTP
	L2TP / IPSec PSK	Server	Server
		Aplikácie VPN	Aplikácie VPN
		Predsdieľaný kľúč IPSec	Predsdieľaný kľúč IPSec
		Používateľské meno	Používateľské meno
		Heslo	Heslo
		Povolenie funkcie L2TP Secret	Tajomstvo L2TP
	IPSec XAuth PSK	Server	Server
		Aplikácie VPN	Aplikácie VPN
		Identifikátor IPSec	Identifikátor IPSec
		Predsdieľaný kľúč IPSec	Predsdieľaný kľúč IPSec
		Používateľské meno	Používateľské meno
		Heslo	Heslo
Expertné nastavenia	Servery DNS	Servery DNS	
	Trasy preposielania	Trasy preposielania	

Obmedzenia

Tu môžete nastaviť obmedzenia týkajúce sa správy pripojenia.

Povolenie dátového roamingu	Povolenie mobilných dát počas roamingu
Vynútenie dátového roamingu	Ak je aktivovaný, roaming pre mobilné dáta je trvalo aktivovaný (neodporúča sa!) Toto nastavenie prepíše nastavenie "Povoliť dátový roaming"!
Nasledujúce nastavenia sú k dispozícii len v systéme SAFE 2.x alebo vyššom	
Povoľte len tiesňové volania	Povoľte len tiesňové volania
Povolenie Wi-Fi	Povolenie Wi-Fi
Minimálna úroveň zabezpečenia siete WiFi	Minimálna úroveň zabezpečenia siete WiFi Otvorené = všetky typy WiFi sú povolené
Zakázať používateľovi pridávať siete WiFi	Používateľ nemôže sám pridať sieť WiFi Toto nastavenie je možné len vtedy, ak bol profil WiFi definovaný v časti "Správa pripojenia".
Povolenie SMS a MMS	Všetky = všetka prevádzka SMS a MMS je povolená Len prichádzajúce SMS = povolené sú len prichádzajúce SMS správy Len odchádzajúce SMS = povolené sú len odchádzajúce SMS správy Žiadne = nie je povolená žiadna prevádzka SMS / MMS
Povolenie synchronizácie počas roamingu	Povolenie synchronizácie počas roamingu Zapnuté = aktivované Vypnuté = deaktivované Voľba používateľa = voľba používateľa
Povolenie hlasového roamingu	Povolenie hlasového roamingu Zapnuté = aktivované Vypnuté = deaktivované Voľba používateľa = voľba používateľa
Použitie systémového servera http Proxy	Použitie proxy servera HTTP, ktorý je k dispozícii v nastaveniach systému, závisí od pripojenej siete (WiFi alebo APN).

Správa PIM

Výmena Gmail

Informácie: Táto konfigurácia sa použije pre aplikáciu Gmail. Preto musíte schváliť a nainštalovať aplikáciu Gmail.

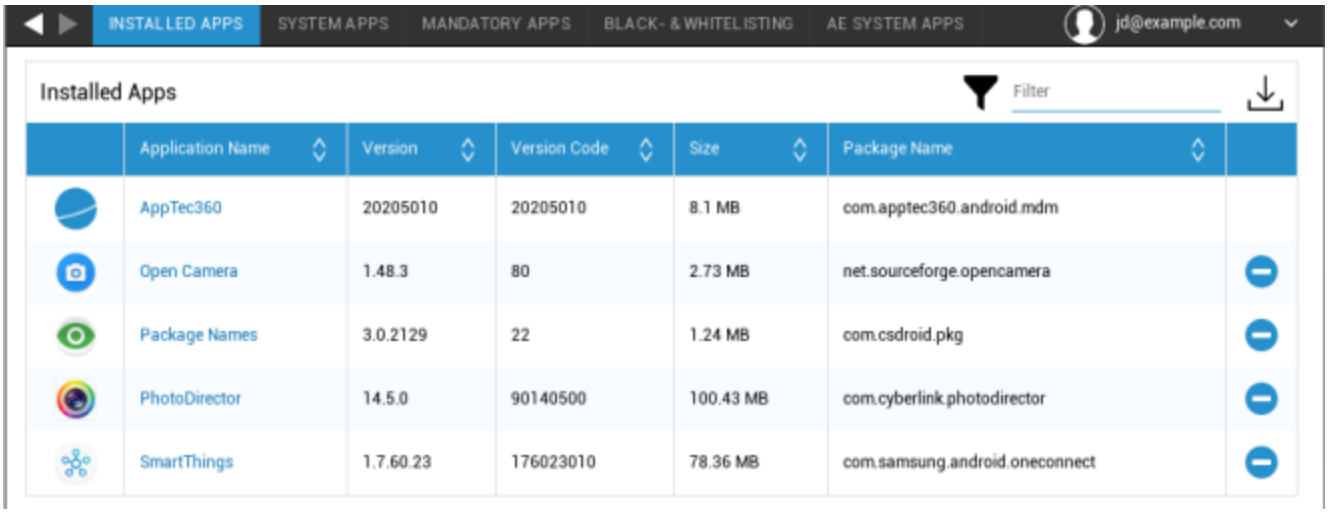
E-mailová adresa	Poskytnutá e-mailová adresa používateľa Všimnite si "zástupné symboly", ktoré môžete použiť na prácu s povereniami a nevykonávate zmeny ručne na každom zariadení. Jedným kliknutím si ich môžete zobraziť sami
Názov hostiteľa servera	Adresa servera vašich serverov Exchange
Prihlasovacie meno	Prihlasovacie meno pre príslušné zariadenie koncového používateľa, všimnite si tiež "Placeholders here".
Podpis	Môžete pripojiť podpis (Tip: Niektoré zariadenia vyžadujú formátovanie podpisu v HTML).
Počet predchádzajúcich dní na synchronizáciu	Počet dní, ktoré určujú, kedy sa e-maily synchronizujú späť
Identifikátor zariadenia	Ein String der die EAS DeviceID enthält. Dies ist Teil des EAS Protokols und wird in einigen Umgebungen benötigt
Používanie Secure Sockets Layer (SSL)	Použitie pripojenia SSL
Prijať všetky certifikáty	Všetky certifikáty sú akceptované. Túto možnosť vyberte, ak váš server Exchange používa certifikát s vlastným podpisom.

Správa aplikácií

Správca podnikových aplikácií

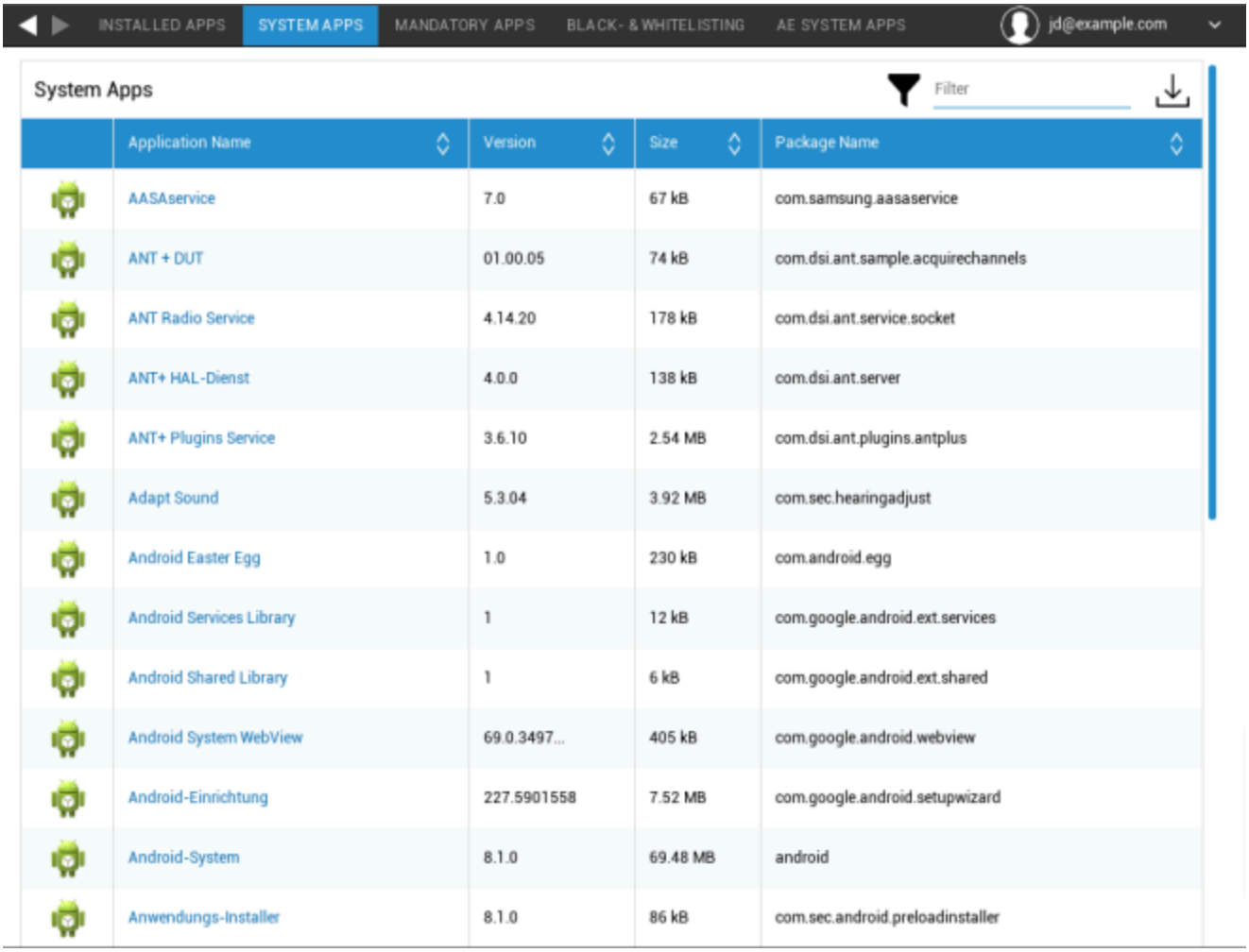
Nainštalované aplikácie (len na úrovni zariadenia)

Tu sa zobrazia všetky aplikácie, ktoré sú aktuálne nainštalované v zariadení koncového používateľa.



Systémové aplikácie (len na úrovni zariadenia)

V časti "Systémové aplikácie" sa zobrazí zoznam všetkých aplikácií a služieb, ktoré už výrobca zariadenia nainštaloval do zariadenia koncového používateľa.

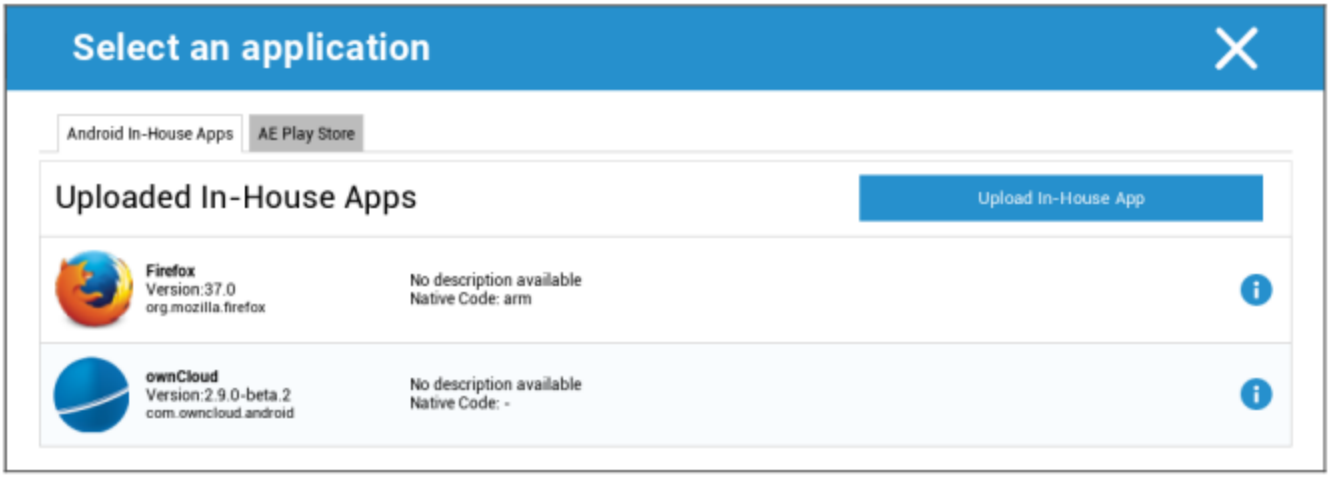


Povinné aplikácie

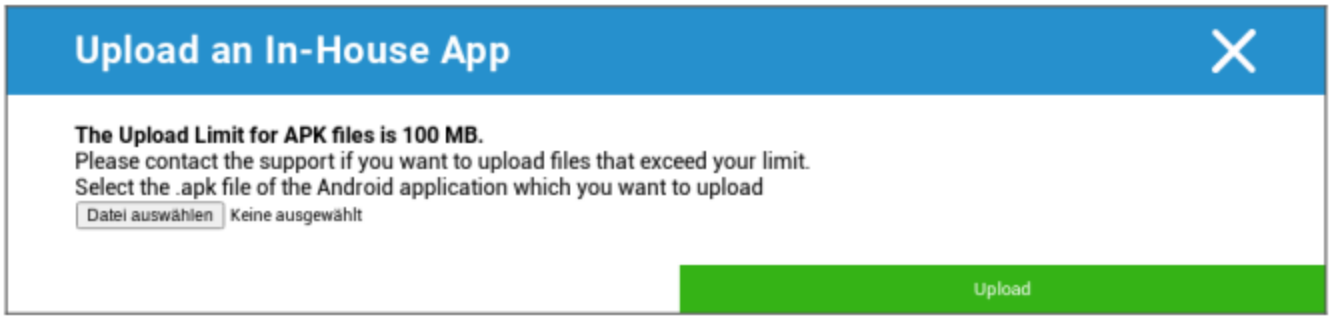
V časti Povinné aplikácie môžete nastaviť povinné požadované aplikácie. Používateľ bude neustále vyzývaný, aby si túto určenú aplikáciu nainštaloval.

Prostredníctvom , možno definovať povinnú požadovanú aplikáciu.

Môže to byť interná aplikácia z "Interných aplikácií pre Android", ktorú ste nahrali vo Všeobecných nastaveniach.

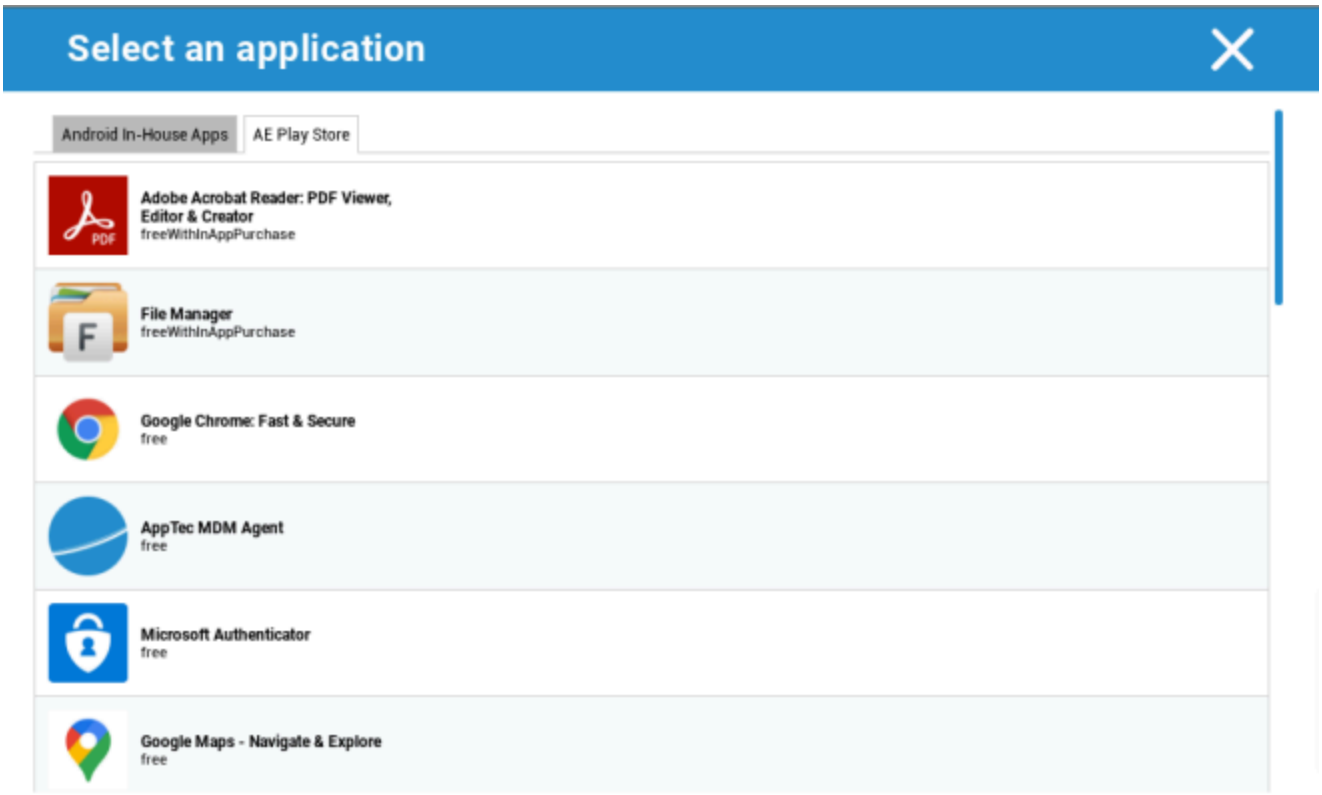


Súbor APK môžete vybrať a nahrať aj priamo pomocou funkcie "Nahrať vlastnú aplikáciu".



Ak inštalujete aplikáciu In-House, budete mať možnosť aktivovať funkciu "Keep up to date". Ak je táto funkcia aktivovaná a v DB aplikácie In-House App ste definovali novšiu verziu, aplikácia sa v zariadení aktualizuje.

Alebo to môže byť aplikácia "AE Play Store" z pracovného obchodu Google Play.



Na tejto karte sa zobrazia len schválené aplikácie "AE Play Store Apps".

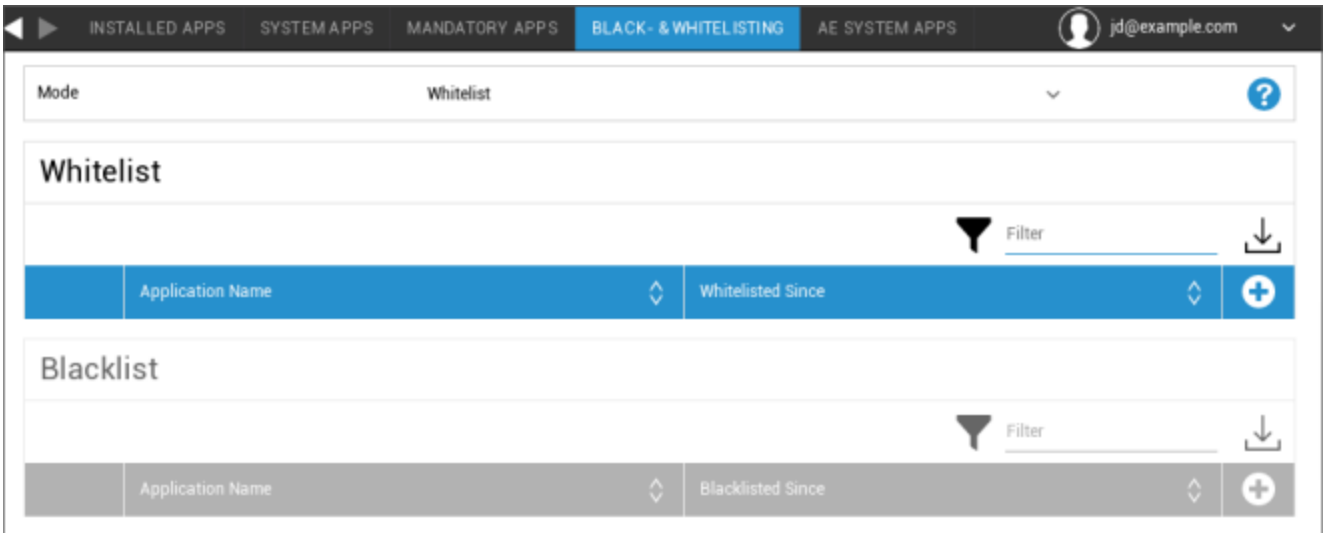
Ak chcete schváliť aplikáciu "AE Play Store", prejdite do časti "Všeobecné nastavenia" > "Správa aplikácií" > "AE Play".

Obchod" a pridajte aplikáciu pomocou tlačidla, ktoré vás presmeruje na kartu "Aplikácie obchodu Play" (alebo môžete
priamo prejsť na kartu "Aplikácie obchodu Play").

Na karte "Aplikácie v Obchode Play" môžete vyhľadávať aplikácie. Po kliknutí na aplikáciu sa otvorí stránka aplikácie
a tu môžete aplikáciu schváliť kliknutím na tlačidlo "Schváliť".

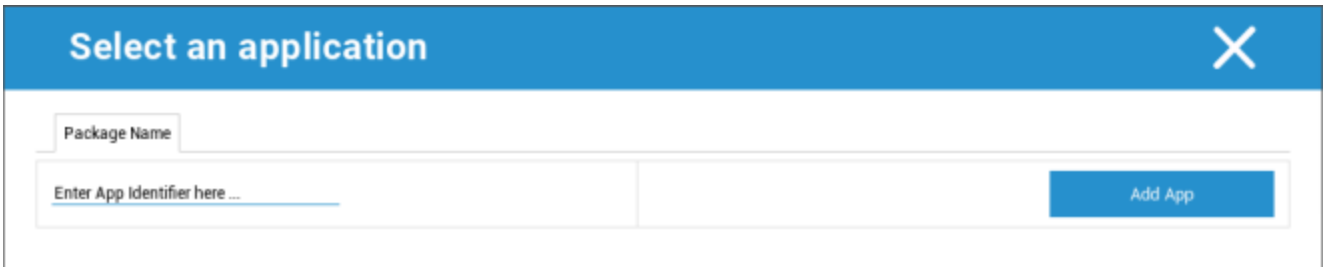
Čierna a biela listina

V časti "Black- & Whitelisting" si môžete vybrať medzi režimom "Whitelist" a režimom "Blacklist".



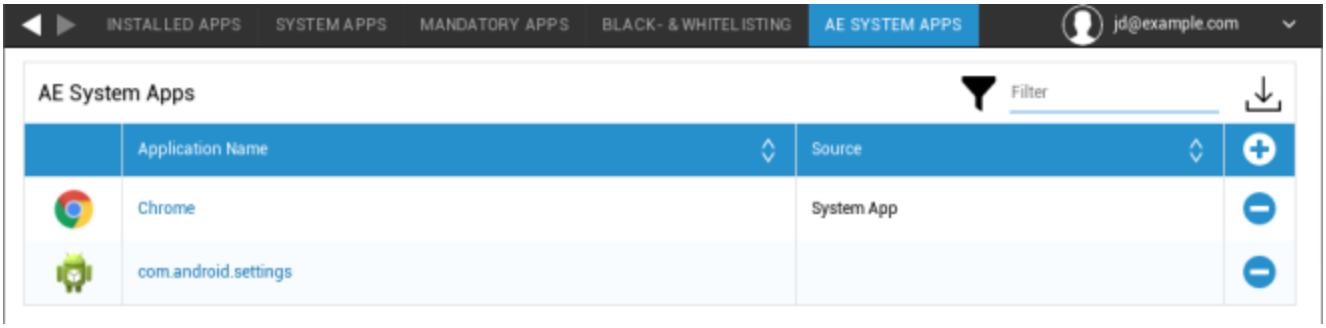
Biela listina	Do zariadenia koncového používateľa je možné nainštalovať iba aplikácie a služby, ktoré sú pridané do zoznamu. Ak sú už v zariadení koncového používateľa predinštalované, budú aktivované a nastavené tak, aby ich používateľ mohol spustiť.
	Všetky ostatné aplikácie, ktoré nie sú pridané do zoznamu, nie je možné nainštalovať do zariadenia koncového používateľa. Ak sú tieto aplikácie už predinštalované v zariadení koncového používateľa, budú deaktivované a nastavené tak, aby ich používateľ nemohol spustiť.
Čierna listina	Aplikácie a služby, ktoré sú pridané do zoznamu, nie je možné nainštalovať do zariadenia koncového používateľa. Ak sú už v zariadení koncového používateľa predinštalované, budú deaktivované a nastavené tak, aby ich používateľ nemohol spustiť.
	Všetky ostatné aplikácie, ktoré nie sú pridané do zoznamu, sa môžu nainštalovať do zariadenia koncového používateľa. Ak sú tieto aplikácie už predinštalované v zariadení koncového používateľa, budú aktivované a nastavené tak, aby ich používateľ mohol spustiť.

Prostredníctvom tlačidla , pridáte ďalšie aplikácie alebo služby do aktuálne používaného zoznamu.
Prostredníctvom tlačidla , pridáte ďalšie aplikácie alebo služby do aktuálne neaktívneho zoznamu.
Môžete definovať "Packagename":

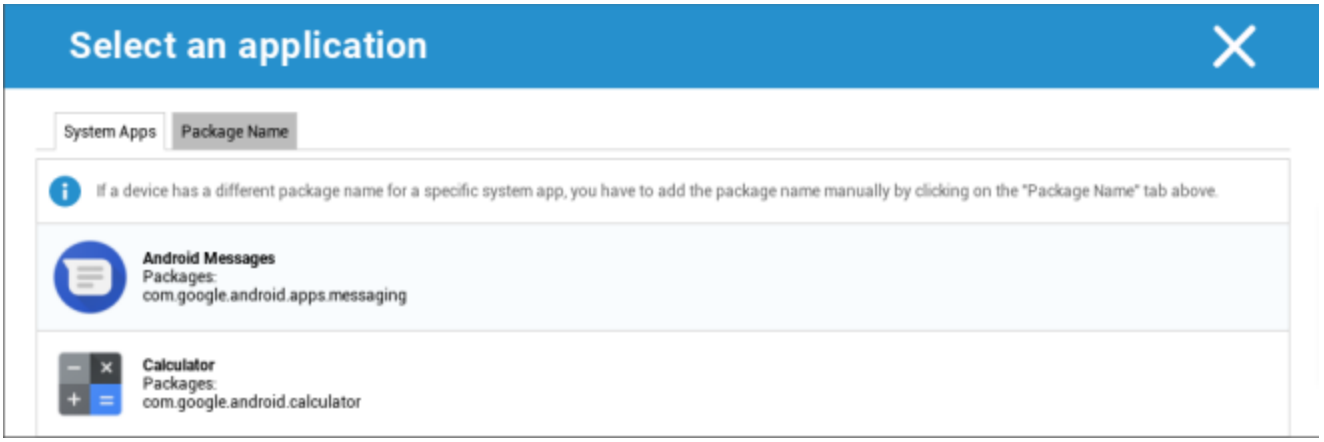

Select an application
Package Name
Enter App Identifier here ...
Add App

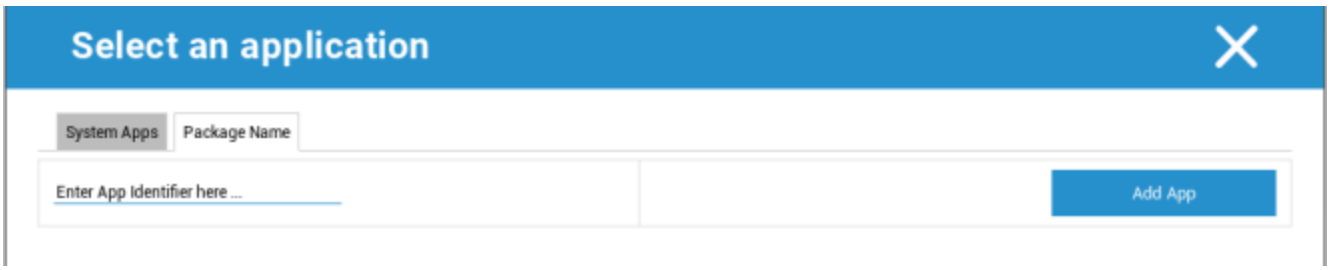
Aplikácie systému AE

Tu môžete definovať zoznam, ktorý obsahuje konkrétne systémové aplikácie, ktoré sa majú aktivovať v zariadeniach.



Po kliknutí na tlačidlo môžete vybrať zo zoznamu možných systémových aplikácií, ktorý poskytuje spoločnosť Google, alebo priamo zadať názov balíka systémovej aplikácie, ktorá sa má aktivovať.





Majte na pamäti, že systémové aplikácie v zozname poskytnutom spoločnosťou Google sú len aplikácie, ktoré môžu byť systémovými aplikáciami, ale nemusia byť nevyhnutne systémovými aplikáciami vo vašich zariadeniach.

Tento zoznam sa však týka len aplikácií, ktoré sú už predinštalované.

Pridanie aplikácií, ktoré nie sú predinštalované vo vašich zariadeniach, nebude mať vplyv na vaše zariadenia bez ohľadu na to, či je aplikácia zo zoznamu poskytnutého spoločnosťou Google alebo je

priamo zadaný názov balíka aplikácie.

Obmedzenia a nastavenia

Nastavenia správy aplikácií

Tu môžete nakonfigurovať správanie zariadenia, pokiaľ ide o aktualizácie aplikácií.

Frekvencia kontroly aktualizácie	Určite, v akom intervale bude klient AppTec360 vyhľadávať aktualizácie aplikácií. Predvolená hodnota je 24 hodín.
Prahová hodnota Wi-Fi	Aplikácie, ktoré sú väčšie ako zadaná veľkosť, sa budú sťahovať cez Wi-Fi. Ak je vybratá možnosť "Iba Wi-Fi", všetky aplikácie sa budú sťahovať cez Wi-Fi.

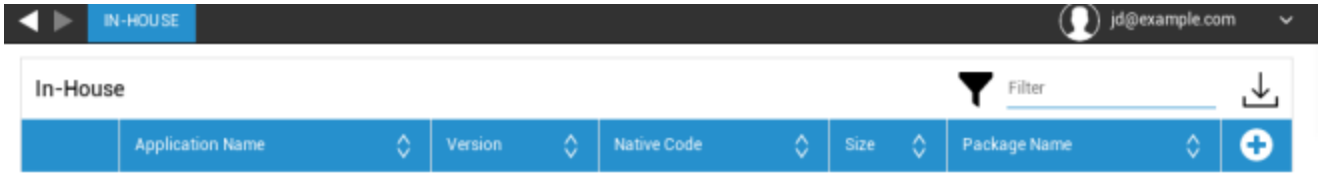
Obchod s podnikovými aplikáciami

Vnútorná stránka

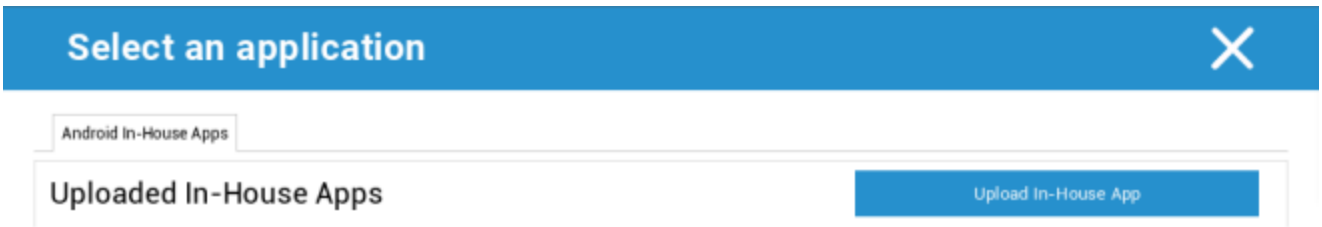
V bode "In-House" môžete nahrať a distribuovať interne vyvinuté aplikácie.

Pomocou tohto symbolu môžete distribuovať ďalšie aplikácie In-House.

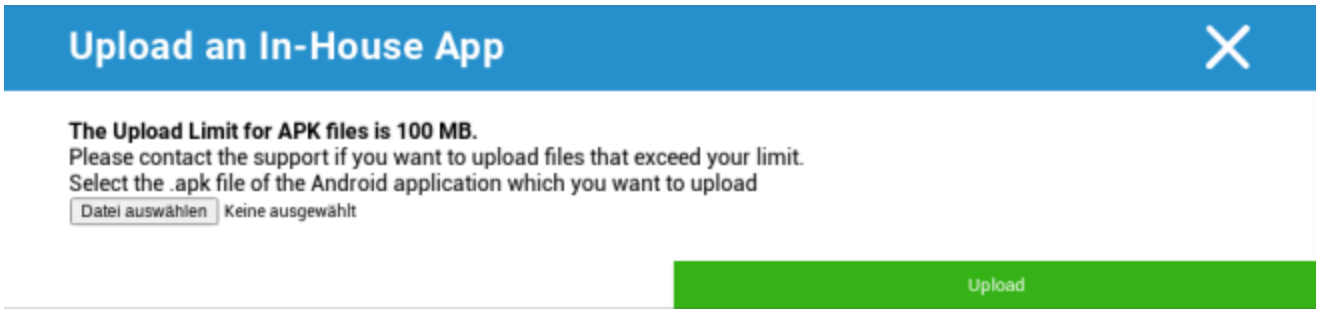
Ak inštalujete aplikáciu In-House, budete mať možnosť aktivovať funkciu "Keep up to date". Ak je táto funkcia aktivovaná na stránke
a v DB aplikácie In-House App ste definovali novšiu verziu, aplikácia sa v zariadení aktualizuje na
.



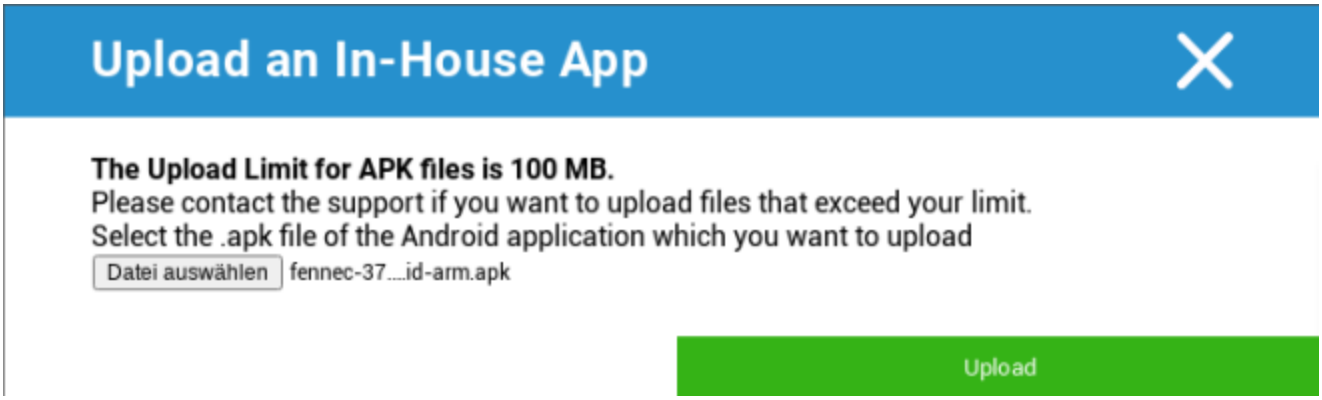
Ak nemáte distribuované aplikácie In-House, dostanete nasledujúci prehľad:



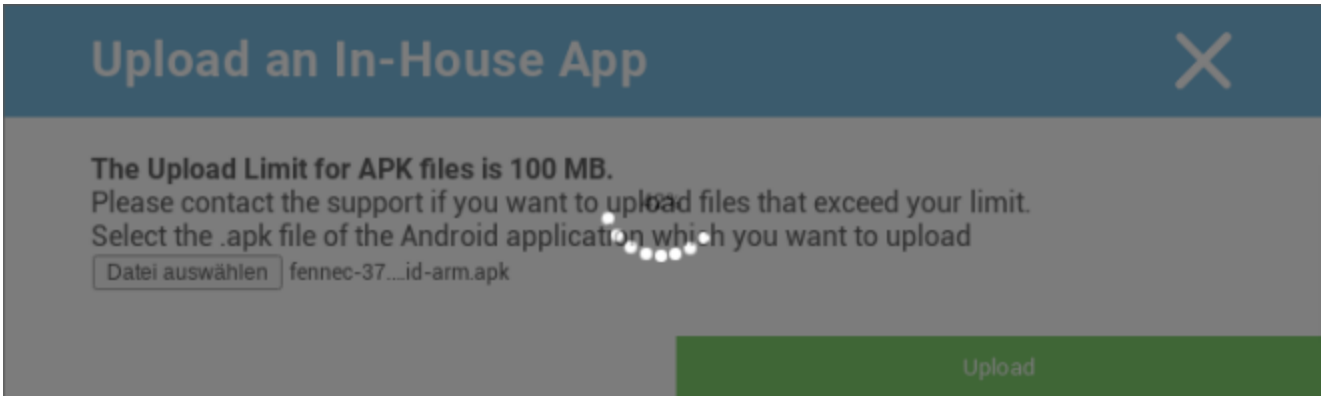
Na tento účel kliknite na položku "Upload In-House App", potom sa zobrazí nasledujúci prehľad:



Teraz vyberte pomocou "Search... "súbor .apk a potom kliknite na "Upload".



Vaša aplikácia bude teraz nahraná, uprostred kruhu sa zobrazí percentuálny ukazovateľ, ukazuje, aká veľká časť vašej aplikácie už bola nahraná.



Ak bolo nahratie vašej internej aplikácie úspešné, nahratú aplikáciu nájdete na stránke
v Katalógu aplikácií.

Používateľ má teraz možnosť zobraziť a nainštalovať túto aplikáciu v obchode AppTec360 na zariadení koncového používateľa
v kategórii "In-House".

Vzhľadom na to, že nejde o aplikáciu Google PlayStore, používateľ nepotrebuje uložené ID Google v príslušnom zariadení koncového používateľa.

Obchod Play pre podniky

Obchod AE Play

Tu môžete pridať aplikácie do obchodu Android Enterprise Playstore. Upozorňujeme, že pred pridaním aplikácií musíte schváliť
Apps pomocou konta správcu AE.

Pokyny na schválenie aplikácie nájdete v časti Povinné aplikácie.

Režim kiosku a spúšťač

Režim kiosku

Režim Kiosk umožňuje vopred definovať aplikáciu alebo adresu URL. Potom bude možné výlučne spustiť/navštíviť túto aplikáciu alebo URL adresu

.

Podobne je možné deaktivovať rôzne hardvérové tlačidlá v režime Kiosk Mode.

Automatický štart	Automatické spustenie režimu Kiosk, hneď ako profil dorazí do zariadenia koncového používateľa.
Plánovaný režim kiosku?	Môžete si naplánovať čas pre režim kiosku, ktorý sa potom začne a skončí automaticky vo vami nastavenom čase.
Čas začiatku	Čas začiatku
Čas v minútach	Čas v minútach, po ktorom by sa mal režim Kiosk opäť ukončiť

Typ aplikácie

Jedna aplikácia	Ak chcete spustiť aplikáciu v režime kiosku, vyberte možnosť Balík" v časti "Typ aplikácie".
Aplikácia kiosku	Kliknite sem, ak chcete vybrať aplikáciu, ktorá sa má spustiť v režime kiosku. Nájdete tu obvyklý prehľad správy aplikácií Môžete si vybrať medzi "Google Play Store", "Android In-House Apps" a "Packagename".

Typ aplikácie	
ADRESA URL	Ak chcete v režime kiosku spustiť adresu URL, vyberte položku "URL" v časti "Typ aplikácie". Potom definujte požadovanú adresu URL
Vymazanie prehliadača po nečinnosti	Tu môžete definovať časový interval v minútach, po ktorom sa má režim kiosku znovu spustiť.
Vymazanie webovej vyrovnávacej pamäte a súborov cookie	Ak túto funkciu aktivujete, po reštarte režimu Kiosk sa vymaže webová vyrovnávacia pamäť (súbory cookie a obrázky v medzipamäti).
Politika rovnakého pôvodu	Ak je táto funkcia aktívna, používateľ môže surfovať iba na podstránkach definovanej adresy URL Napríklad ste definovali nasledujúcu adresu URL:www.mypage.com Potom môže používateľ surfovať na: www.mypage.com/subpage
Adresy URL na bielej listine	Tu môžete udržiavať bielu listinu, všetky tieto adresy URL sú povolené Maximálne 1 adresa URL na riadok Adresa URL musí začínať http:/ alebo https://
Adresy URL na čiernej listine	Tu môžete udržiavať čiernu listinu, všetky tieto adresy URL nie sú povolené. Maximálne 1 adresa URL na riadok Adresa URL musí začínať http:/ alebo https://
Orientácia obrazovky	Toto nastavenie sa týka úprav obrazovky Automatic = automatický Portrét = vertikálny formát Krajina = režim na šírku

Viacnásobná aplikácia	Ak vyberiete režim "Multi App" Kiosk Mode, bude sa vyžadovať používanie spúšťacieho programu AppTec360.
Aplikácie	Použitie: Ako aplikáciu pre kiosk vyberte aplikáciu z obchodu Playstore alebo vlastnú aplikáciu. Je možné zadať aj názov balíka. Vybraná aplikácia Kiosk Application musí byť nainštalovaná v zariadení. Nezabudnite nastaviť Kiosk Application ako povinnú. Skratka na domovskej obrazovke: Ak je nastavená na "Zapnuté", vytvorí sa skratka na domovskej obrazovke. Ak je nastavená na "Off" (Vyp.), aplikácia sa bude stále zobrazovať v zozname aplikácií.

Povolené heslo pre ukončenie	Ak túto funkciu aktivujete, používateľ môže ukončiť režim kiosku pomocou vami vopred definovaného hesla.
Heslo pre ukončenie	Toto je heslo, ktoré ste preddefinovali.
Automatické zbalenie stavového riadku	Ak je táto možnosť povolená, stavový riadok sa automaticky podfarbí. S touto možnosťou môžu používatelia vidieť informácie na stavovom riadku, ale nemajú prístup k jeho funkciám
Zakázanie stavového riadka	Stavový riadok obsahuje Upozornenia, Skratky a Informácie. K dispozícii len pre zariadenia Samsung s verziou SAFE 4.0 alebo vyššou.
Zakázanie tlačidiel hlasitosti	Zakázanie tlačidiel hlasitosti (dostupné len v zariadeniach Samsung s verziou SAFE 3.0 alebo vyššou)
Zakázanie vypínača zapnutia/vypnutia	Vypnutie prepínača zapnutia/vypnutia (dostupné len v zariadeniach Samsung s verziou SAFE 3.0 alebo vyššou)
Zakázanie tlačidla Domov	Zakázanie tlačidla Domov. Ak bola táto funkcia aktivovaná, režim Kiosk je možné ukončiť len v konzole AppTec360. (k dispozícii len v zariadeniach Samsung s verziou SAFE 3.0 alebo vyššou)
Zakázanie navigačného panela	Pomocou tejto funkcie môžete vypnúť navigačný panel (Späť / Menu) Ak bola táto funkcia aktivovaná, režim Kiosk je možné ukončiť len v konzole AppTec360. (k dispozícii len v zariadeniach Samsung s verziou SAFE 3.0 alebo vyššou)

Spúšťač AppTec360

Povolenie AppTec360 Launcher	Na: AppTec360 Launcher. Používateľ ho musí jednorazovo nastaviť ako predvolený spúšťač. Poznámka: Ak je povolený režim kiosku a režim kiosku je nastavený na "Multi App", bude sa vyžadovať používanie spúšťacieho programu AppTec360.
Veľké ikony	Na: Zobrazí väčšiu verziu ikon aplikácií v spúšťači
Skryť ikonu aplikácie AppTec360	Na: Úplne skryje aplikáciu AppTec360
Skryť ikonu obchodu AppTec360	Na: Úplne skryje AppTec360 Enterprise AppStore

Nastavenia aplikácie AppTec360

Povolenie aplikácie AppTec360 Settings	Aplikácia AppTec360 Settings poskytuje kontrolu nad pripojeniami WiFi a Bluetooth
Povolenie nastavení v aplikácii Multi App Režim kiosku	Ak je táto možnosť povolená, používatelia môžu pristupovať k aplikácii AppTec360 Settings, keď je aktívny režim Multi App Kiosk Mode.

Diaľkové ovládanie

Splashtop

Ak chcete spustiť reláciu vzdialeného ovládania pre svoje zariadenie, je potrebné nainštalovať aplikáciu "Splashtop Streamer" do zariadenia pridaním aplikácie do časti **Správa aplikácií** → **Správca podnikových aplikácií** → **Povinné aplikácie**.

Potom nakonfigurujte nasledujúce nastavenia pre Splashtop:

Povolenie funkcie Splashtop	Ak je to povolené, AppTec360 nakonfiguruje aplikáciu Splashtop tak, aby umožňovala vzdialené ovládanie
Nasadenie kódu	Prejdite na stránku https://my.splashtop.com a prihláste sa do svojho konta Splashtop. Kliknite na "Add Computer" (Pridať počítač) a skopírujte 12-miestny kód nasadenia z výslednej stránky.
Nastavenie vlastnej brány nasadenia?	Nasadenie brány
Nasadenie domény brány / hostiteľa	Nasadenie brány
Overenie certifikátu	Overenie certifikátu

Potom môžete použiť možnosť Splashtop Remote Control v kontextovej ponuke (ozubené koleso vedľa vyhľadávacieho panela, keď je zariadenie vybrané, alebo kliknite pravým tlačidlom myši na zariadenie v strome) na spustenie relácie diaľkového ovládania.

TeamViewer

Ak chcete spustiť reláciu vzdialeného ovládania pre svoje zariadenie, je potrebné nainštalovať aplikáciu "TeamViewer QuickSupport" do zariadenia pridaním aplikácie do časti **Správa aplikácií** → **Správca podnikových aplikácií** → **Povinné aplikácie**.

Potom môžete použiť možnosť **TeamViewer Remote Control** v kontextovej ponuke (ozubené koleso vedľa vyhľadávacieho panela, keď je zariadenie vybrané, alebo kliknutie pravým tlačidlom myši na zariadenie v strome) na spustenie relácie vzdialeného ovládania.

Správa obsahu

ContentBox

Tu môžete aktivovať ContentBox.

Hneď ako prepnete možnosť "Enable ContentBox" na "On", do zariadenia koncového používateľa sa automaticky nainštaluje samostatná aplikácia ContentBox

.

Zabezpečený prehliadač

Tu môžete konfigurovať nastavenia pre AppTec360 Secure Browser.

Akonáhle prepnete sekciu v časti "Zabezpečený prehliadač" na "Zapnutý", do zariadenia koncového používateľa sa automaticky nainštaluje samostatná aplikácia prehliadača
.

Vyžadovať heslo	Vyžadovať od používateľa nastavenie a používanie hesla na prístup do prehliadača.
Minimálna požadovaná dĺžka hesla	Nastavenie požadovaného počtu znakov pre heslo
Požadovaná kvalita hesla	Nastavenie požadovanej kvality hesla
Obmedzenie sťahovania / Otvoriť v	
Obmedzenie nahrávania	
Nahrávanie bielej listiny	Zoznam adries URL, pre ktoré bude nahrávanie vždy povolené.
Povoliť kopírovanie	Povoľte kopírovanie, vyrezávanie alebo zdieľanie textu vo vnútri webových stránok.
Povolenie snímania obrazovky	Umožniť zachytávanie snímok obrazovky.
Frekvencia čistenia údajov	Vyberte, s akou frekvenciou sa majú automaticky odstraňovať VŠETKY údaje používateľa (história, vyrovnávacia pamäť atď.).
Záložky spoločnosti	Záložky sa zobrazia v priečinku "Firemné záložky" v záložkách prehliadača. Používateľ ich nemôže upravovať.
Skryť adresný riadok	
Biela listina v prehliadači (bez univerzálnej brány)	Povolí vytváranie bielych zoznamov URL na strane klienta. • Záložky spoločnosti sú vždy zaradené na biely zoznam • Podporované len pre 100 adries URL • Použite univerzálnu bránu na neobmedzené zaradenie do čiernej a bielej listiny
Adresy URL na bielej listine	Zoznam povolených adries URL.

Čierna a biela listina založená na bráne	Čierna listina má tieto požiadavky: • Fungujúca univerzálna brána AppTec360 ("Všeobecné nastavenia" → "Univerzálna brána") • Fungujúca konfigurácia VPN so zadaným serverom DNS ("Všeobecné nastavenia" → "Univerzálna brána" → "Nastavenia VPN") • Konfigurácia čiernej listiny ("Všeobecné nastavenia" → "Univerzálna brána" → "Čierna listina domén") • Platné pripojenie VPN v profile ("Správa pripojení" → "VPN")

Ďalšie API

Samsung KNOX

Obmedzenia

Povolenie karty SD	
Povolenie zápisu na kartu SD	
Povolenie snímania obrazovky	
Povoliť schránku	
Zálohovanie nastavení a údajov aplikácie v službe Google Cloud	
Obnovenie nastavení zo služby Google Cloud pri preinštalovaní aplikácie	
Povolenie ladenia USB	
Povoliť hlásenie o zrážke Google	
Povolenie obnovenia továrenského nastavenia	
Povolenie aktualizácie OTA	
Povolenie ukladania do hostiteľského počítača USB	Ak je táto funkcia povolená, používateľ môže pripojiť ľubovoľnú jednotku typu pen (prenosné úložisko USB), externý pevný disk alebo čítačku kariet Secure Digital (SD), ktorá sa v zariadení pripojí ako úložná jednotka.
Povolenie prehrávača médií USB (MTP,PTP)	
Povoliť mikrofón	Zakázanie mikrofónu pre aplikácie tretích strán
Povolenie NFC (Near Field Communication)	
Povolenie neznámych zdrojov (APK Sideloading)	Ak je povolené vedľajšie načítanie aplikácií (súborov APK), je povolené. Po vypnutí tohto nastavenia ho musí používateľ povoliť ručne, keď opätovne povolíte inštaláciu súborov APK z neznámych zdrojov.

Povolenie vytvárania používateľov	Ak je táto možnosť povolená, používateľ môže v zariadení vytvoriť viacero účtov, napr. účty hostí.

E-mail

E-mailová adresa	
Protokol prichádzajúceho servera	
Adresa prichádzajúceho servera	
Port prichádzajúceho servera	
Prihlasovacie meno/meno používateľa prichádzajúceho servera	
Heslo prichádzajúceho servera	
Prichádzajúci server používa protokol SSL	
Prichádzajúci server používa TLS	
Prichádzajúci server akceptuje všetky certifikáty	
Protokol odchádzajúceho servera	
Adresa odchádzajúceho servera	
Port odchádzajúceho servera	
Odchádzajúci server používa ďalšie poverenia	Ak je vypnuté, systém použije prichádzajúce poverenia aj pre odchádzajúci server.
Prihlasovacie meno/meno používateľa odchádzajúceho servera	
Heslo odchádzajúceho servera	
Odchádzajúci server používa protokol SSL	
Odchádzajúci server používa TLS	
Odchádzajúci server akceptuje všetky certifikáty	
Nastaviť podpis	
Podpis	Poznámka: Pre niektoré zariadenia sa musí podpis zadať vo formáte HTML.
Upozorniť používateľa na prijatie novej elektronickej pošty	

Výmena

E-mailová adresa	
Názov hostiteľa servera	Názov hostiteľa servera Exchange
Prihlasovacie meno	Používateľské meno, ktoré sa používa na prihlásenie na server Exchange
Doména	Ak je povolená konfigurácia brány ACL a pole Domain nie je prázdne, univerzálna brána AppTec360 overí zariadenie s nasledujúcim názvom "Domain\Login Name
Heslo	
Počet predchádzajúcich dní na synchronizáciu	
Frekvencia synchronizácie elektronickej pošty	
Synchronizácia počas roamingu	
Nastaviť podpis	
Podpis	Poznámka: V prípade niektorých zariadení sa musí podpis zadať vo formáte HTML.
Predvolený účet	
Používanie Secure Sockets Layer (SSL)	
Používanie protokolu TLS (Transport Layer Security)	
Prijať všetky certifikáty	

APN

Zobrazovaný názov APN	
Názov prístupového bodu	Názov APN
Protokol odchádzajúceho servera	
MCC - kód mobilnej krajiny	Nechajte prázdne, ak chcete použiť mmc nainštalovanej SIM karty
MNC - Kód mobilnej siete	Nechajte prázdne, ak chcete použiť mnc nainštalovanej SIM karty
Adresa servera	
Číslo portu servera	
Adresa servera proxy	
Adresa servera MMS	Pre predvolené nastavenie nechajte prázdne
Číslo portu MMS	Pre predvolené nastavenie nechajte prázdne
Adresa proxy servera MMS	Pre predvolené nastavenie nechajte prázdne
Používateľské meno	
Heslo	
Typ prístupového bodu	Akceptované typy sú "default", "mms", "supl".
	Ak sa odovzdá null alebo prázdne, predvolene sa použije "default,supl,mms".
	Pre predvolené nastavenie nechajte prázdne.
Uprednostňované APN	

Bluetooth

Povolenie zisťovania zariadenia cez Bluetooth	
Povolenie párovania cez Bluetooth	
Povolenie zariadení s náhlavnou súpravou Bluetooth	
Povolenie zariadení Bluetooth Hands-free	
Povolenie zariadení Bluetooth A2DP	A2DP, profil Advanced Audio Distribution Profile umožňuje streamovanie zvuku medzi zariadeniami
Povolenie odchádzajúcich hovorov	
Povolenie prenosu údajov cez Bluetooth	
Povolenie tetheringu Bluetooth	
Povolenie pripojenia k počítaču cez Bluetooth	

Pripojenie

Povoliť len tiesňové volaniaPovoliť Wi-Fi	
Minimálna úroveň zabezpečenia siete Wi-Fi	
Zákaz používateľovi pridávať siete Wi-Fi	Toto obmedzenie je možné aktivovať len vtedy, ak je v časti Správa pripojenia definovaný aspoň jeden aktívny profil Wi-Fi.
Povolenie SMS a MMS	
Povolenie synchronizácie počas roamingu	
Povolenie hlasového roamingu	

Android Enterprise – Plne spravované zariadenie s pracovným profilom (COPE)

Všeobecné vysvetlenie COPE

COPE je skratka pre **Corporate Owned Personally Enabled**(**osobne vlastnená spoločnosť**).

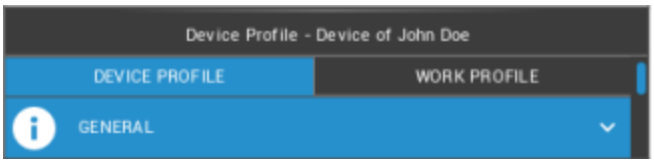
Režim COPE umožňuje zaregistrovať zariadenie so systémom Android ako **zariadenie Android Enterprise - plne spravované zariadenie** s integrovaným profilom **Android Enterprise - Container**.

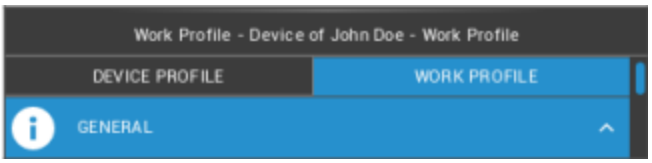
Môže to byť buď zariadenie so systémom Android, ktoré je už zaregistrované ako **Android Enterprise - plne spravované zariadenie** a na ktorom je dodatočne nastavený **Android Enterprise - Container**, alebo novo zaregistrované zariadenie so systémom Android, ktoré je priamo zaregistrované ako **Android Enterprise - plne spravované zariadenie** spolu s **Android Enterprise - Container** na ňom.

Režim COPE je k dispozícii len pre zariadenia so systémom Android 8, 9 a 10

Konfigurácia profilov pre zariadenia COPE

Keďže pre samotný režim COPE neexistuje konfiguračný profil, konfigurácia **Android Enterprise - plne spravované zariadenie** a **Android Enterprise - kontajner** je v rámci profilu COPE rozdelená do dvoch profilov. Medzi týmito dvoma profilmi je možné prepínať konfiguráciu každého profilu kliknutím na príslušné tlačidlo na ľavej strane konzoly:





Oba profily je možné nakonfigurovať tak, ako je to popísané pri jednotlivých profiloch:

Android Enterprise - Plne spravované zariadenie

Android Enterprise - Kontajner

Návrat k plne spravovanému zariadeniu AE

Profil **Android Enterprise - Container** môžete odstrániť podľa opisu v časti **Správa mobilných zariadení**.

Odstránením profilu Container sa profil COPE zmení na profil **Android Enterprise - plne spravované zariadenie**.

Android Enterprise – Konfigurácia kontajnera

V závislosti od toho, či ste aktuálne vybrali profil skupiny alebo zariadenie, sa prehľad a jeho podbody líšia - zvážte to pozorne!

Všeobecné

Prehľad profilu (len na úrovni profilu)

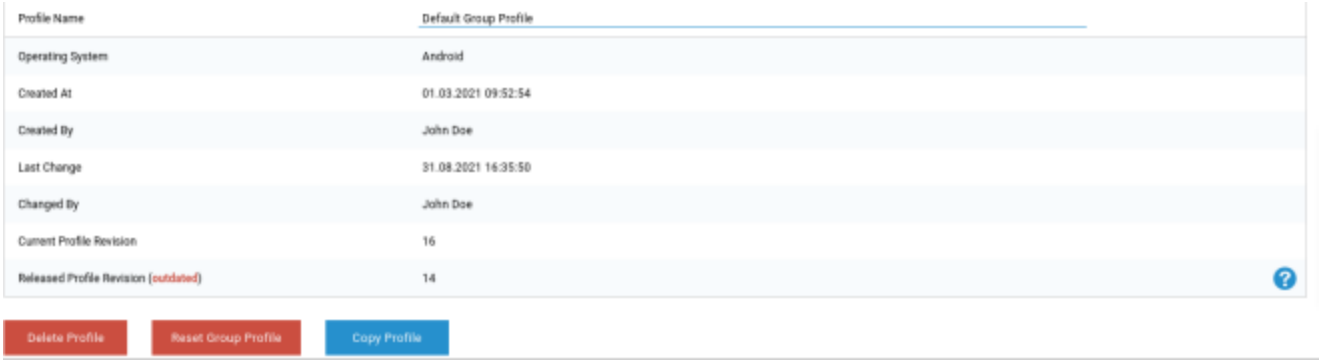
Ak sa nachádzate v profile, zobrazí sa vám stručný prehľad profilu, pokiaľ ide o názov, operačný systém, dátum vytvorenia, autora atď.

Názov profilu	Názov profilu - tu sa dá priamo premenovať
Operačný systém	Platný OS pre profil
Vytvorené v	Dátum vytvorenia
Vytvoril	Vytvoril
Posledná zmena	Dátum poslednej zmeny
Zmenené podľa	Používateľ, ktorý vykonal posledné zmeny v tomto profile
Aktuálna revízia profilu	Počet aktualizácií profilu
Vydaná revízia profilu	Počet aktualizácií profilu, ktorým už boli priradené zariadenia

Odstránenie profilu	Odstránenie profilu
Obnovenie profilu skupiny	Obnovenie profilu skupiny
Kopírovať profil	Kopírovať profil

Prehľad profilu skupiny (len na úrovni skupiny)

Po otvorení profilu skupiny sa zobrazí rýchly prehľad profilu.



Názov profilu	Názov profilu (tu sa dá zmeniť)
Operačný systém	Operačný systém, pre ktorý je profil určený
Vytvorené v	Čas vytvorenia
Vytvoril	Tvorca profilu
Posledná zmena	Čas poslednej zmeny profilu
Zmenené podľa	Účet, ktorý vykonal posledné zmeny
Aktuálna revízia profilu	Revízia uloženého stavu profilu
Vydaná revízia profilu	Priradená revízia profilu ("Priradiť teraz"). Ak sa za textom na štítku zobrazí " (zastaraný)", znamená to, že ste profil uložili, ale ešte ste ho nepriradili, takže zariadenia budú stále dostávať staršiu verziu.

Prehľad zariadení (len na úrovni zariadenia)

Ak sa nachádzate na zariadení, zobrazí sa prehľadné zhrnutie vybraného zariadenia, ktoré obsahuje nasledujúce informácie:

Názov zariadenia	Názov zariadenia
Umiestnenie	Súradnice polohy
Telefónne číslo	Telefónne číslo
Priradené povinné aplikácie	Počet pridelených povinných aplikácií
Verzia operačného systému	Verzia operačného systému zariadenia
Operačný systém	Operačný systém (Android Enterprise)
Sériové číslo	Sériové číslo zariadenia
Vlastníctvo zariadenia	Firemné alebo súkromné zariadenie
Typ zariadenia	AE Work Spravované zariadenie
Zakorenené	Stav, ktorý uvádza, či bolo zariadenie rootnuté
V súlade s	V súlade s usmerneniami
IP adresa	IP adresa zariadenia
Naposledy videné	Bod v čase, kedy sa zariadenie naposledy pripojilo k AppTecu
Posledný impulz	Bod v čase, keď bol do zariadenia odoslaný posledný push
Priradenie používateľa	Používateľ alebo skupina, ku ktorej je toto zariadenie priradené

Revízia konfigurácie

Tu získate prehľad o tom, ktorý skupinový profil je priradený k zariadeniu.

Ak kliknete na profil skupiny, získate priamy prístup k tomuto profilu a môžete vykonať nastavenia.

Pomocou tohto symbolu môžete vrátiť distribuované aplikácie do nastavení profilu skupiny.

Pomocou tohto symbolu môžete vrátiť všetky používané aplikácie do nastavení skupinového profilu.

"K dispozícii je novšia revízia" znamená, že profil skupiny bol zmenený a uložený, ale nie je priradený. Profil skupiny sa musí priradiť pomocou "Priradiť teraz" na úrovni skupiny, aby sa zmeny uplatnili na

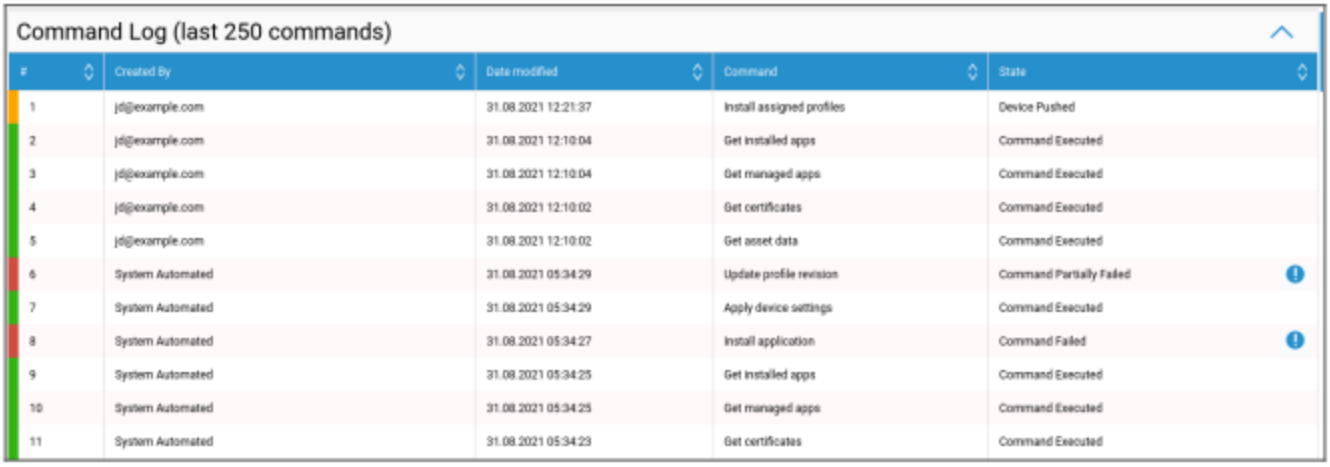
zariadeniach.

Protokol zariadenia (len na úrovni zariadenia)

Tu sa zobrazia rôzne protokoly zariadenia. V prípade potreby tu môžete priamo zistiť príčinu chyby.

Denník príkazov

Tu môžete vidieť, ktoré príkazy boli pre zariadenie vydané a aký je ich stav.



Možné stavy príkazov

Stlačené zariadenie	Do služby push (napr. APNS) bola odoslaná požiadavka na pripojenie, aby sa zariadenie pripojilo späť k serveru EMM.
Vytvorený príkaz	Príkaz bol vytvorený v systéme.
Odoslaný príkaz	Príkaz sa odoslal do zariadenia po jeho pripojení k serveru.
Vykonaný príkaz	Príkaz bol úspešne vykonaný.
Príkaz zlyhal	Príkaz zlyhal. *
Príkaz čiastočne zlyhal	V závislosti od operačného systému zariadenia môžu byť niektoré príkazy zoskupené. V tejto časti tejto skupiny príkazov zlyhali niektoré časti. *
Príkaz vykonaný, prípadne neúspešný	Príkaz bol vykonaný, ale možno nebol.
Príkaz Repushed	Príkaz bol opätovne odoslaný používateľom.
Vyradené	Príkaz bol zamietnutý. Napríklad preto, že bol nahradený iným príkazom alebo zariadenie bolo znovu zaregistrované a staré príkazy boli odstránené.

*Ak je za správou výkričník, môžete získať ďalšie informácie, ak kurzorom prejdete na ikonu.

Nastavenia zariadenia

Konfigurácia klienta

Tu môžete vykonať nasledujúce konfigurácie zariadenia so systémom Android:

Čas mimo súladu	Časový limit reakcie používateľa, po uplynutí ktorého sa uplatní akcia vynucovania.
Opatrenia na presadzovanie práva po uplynutí lehoty na dosiahnutie súladu	Ak používateľ nevykonáva činnosti, ktoré vedú k dosiahnutiu stavu zariadenia, ktoré je v súlade s predpismi
Frekvencia zberu údajov	Frekvencia zberu informácií o zariadení/GPS
Frekvencia srdcového tepu zariadenia	Interval, v ktorom má zariadenie kontaktovať server AppTec Min. 1 minúta Max. 24 hodín
Povolenie aktualizácií polohy	Ak je aktivovaná, zariadenie odosiela aktualizácie polohy na server AppTec
Čas aktualizácie polohy	Určuje, v akých časových intervaloch zariadenie odosiela aktualizácie polohy do aplikácie AppTec.
Používanie služby Google Location Accuracy na aktualizáciu polohy	Ak je aktivovaná, pre aktualizácie polohy sa bude používať sieťová poloha (ak bola deaktivovaná v časti "Obmedzenia", toto nastavenie nebude mať žiadny vplyv).
Používanie polohy GPS na aktualizáciu polohy	Ak je aktivovaná, GPS sa bude používať na aktualizáciu polohy
Povolenie falošných lokalít	Umožňuje falšovanie informácií o polohe prostredníctvom aplikácií tretích strán
Akcia strateného spojenia	Ak je táto možnosť povolená, môžete určiť akciu pre prípad, že zariadenie nezíska spojenie so serverom MDM v intervale srdcového tepu. Napríklad ak má zariadenie čas srdcového tepu 5 minút, pripojí sa k serveru o 10:35. Potom zariadenie opustí dosah siete Wi-Fi. Ďalší srdcový úder o 10:40 sa nepodarí vykonať a vykoná sa zadaná akcia.

Akcia	Opatrenia, ktoré sa majú prijať, akonáhle sa zariadenie stane nevyhovujúcim. • Lock Zariadenie = uzamknúť zariadenie • Vymazať zariadenie = zariadenie sa obnoví na výrobné nastavenia • Vymazať zariadenie a kartu SD = zariadenie sa obnoví do továrenských nastavení a úložisko karty SD sa vymaže
Prahová hodnota	Môžete zadať prahovú hodnotu zlyhaných srdcových úderov, ktoré sú potrebné na spustenie zadanej akcie.

Režim presadzovania zásad	Predvolené nastavenie:	Používatelia budú pravidelne vyzývaní na vykonanie nevykonaných akcií
	Lenivé presadzovanie zásad:	Používatelia nebudú nikdy vyzvaní na vykonanie nevykonaných akcií. Všetky otvorené akcie sa zobrazia v aplikácii AppTec Client
	Agresívne presadzovanie zásad:	Používatelia budú nepretržite vyzývaní na vykonanie nevykonaných akcií
Zámok verzie AppTec	Ak je táto možnosť povolená, je možné zadať kód verzie aplikácie AppTec. Klient AppTec sa aktualizuje len na zadanú verziu. Novšie verzie sa budú ignorovať. Zníženie aktualizácie NIE JE možné.	
Kód verzie	Kód verzie aplikácie AppTec, ktorá má byť uzamknutá.	
Zakázanie oznámenia AppTec	Ak je vypnuté, klient AppTec nezobrazí oznámenie v paneli oznámení. Používatelia tak môžu klienta AppTec zavrieť prostredníctvom správcu úloh. Ak je klient AppTec zatvorený, niekoľko funkcií vrátane režimu Kiosk a čiernej/bielej listiny aplikácií nebude fungovať správne. Zariadenia Samsung ponúkajú ochranný mechanizmus pre klienta AppTec. V zariadeniach Samsung, ktoré podporujú rozhranie KNOX API, je upozornenie predvolene vypnuté. Oznámenie by nemalo byť vypnuté na zariadeniach so systémom Android 8.0 alebo vyšším.	

Tapety

Nastavenie vlastnej tapety	Povolenie/zakázanie vlastnej tapety
Tapety	Nastavenie režimu tapety na použitie farebného kódu alebo obrázka
Zadanie farby	Zadajte farbu pozadia ako hexadecimálnu hodnotu, napr. #000000 ako čiernu alebo #ffffff ako bielu.
Nastavenie obrázka ako tapety	Nahrajte súbor s obrázkom, ktorý chcete použiť ako tapetu

Správa aktív (len na úrovni zariadenia)

Informácie o zariadení

Model	Označenie modelu zariadenia
Operačný systém	OS
Verzia operačného systému	Verzia operačného systému
Sériové číslo	Sériové číslo
Názov zariadenia	Názov zariadenia
Stav batérie	Stav batérie
Voľná / celková pamäť	Voľná / celková pamäť
Samsung Safe	Rozhranie Samsung SAFE, potrebné pre rôzne možnosti nastavenia
K dispozícii je karta SD	K dispozícii je karta SD
Emulovaná karta SD	Emulovaná karta SD
Vymeniteľná karta SD	Vymeniteľná karta SD
SD Voľná / celková pamäť	SD Voľná / Celková pamäť karty SD

Wi-Fi

IP adresa	IP adresa zariadenia
WiFi MAC	Adresa MAC WiFi

Cellular

Stav	Stav (nainštalovaná karta SIM)
Telefónne číslo	Telefónne číslo
Roaming (hlas / dáta)	Roaming pre hlas / dáta
Stav roamingu	Aktuálny stav roamingu
IP adresa	IP adresa
Prevádzkovateľ/prepravca	Prevádzkovateľ/prepravca
Mobilná technológia	Mobilná technológia
IMEI	Číslo IMEI
ICCID	Ide o identifikátor karty SIM, často aj karty Smartcard alebo karty s integrovaným obvodom (ICC).
IMSI	Medzinárodná identita mobilného účastníka (IMSI) poskytuje v mobilných sieťach GSM a UMTS jednoznačnú identifikáciu používateľov siete. IMSI pozostáva z maximálne 15 číslic a konfiguruje sa takto: • Kód mobilnej krajiny (MCC), 3 číslice • Kód mobilnej siete (MNC), 2 alebo 3 číslice • Identifikačné číslo mobilného účastníka (MSIN), 1-10 číslic
Súčasné MCC/MNC	Pozri "SIM MCC/MNC".
SIM MCC/MNC	Kód mobilnej krajiny je zavedený identifikátor krajiny, ktorý stanovila ITU podľa normy E.212. Funguje v spojení s kódom mobilnej siete (MNC) na identifikáciu mobilnej siete. Znamená kód krajiny/mobilnej siete karty SIM. Ak sa pohybujete v inej mobilnej sieti, potom sa logicky budú "Aktuálne MCC/MNC" a "SIM MCC/MNC" líšiť.

Bluetooth

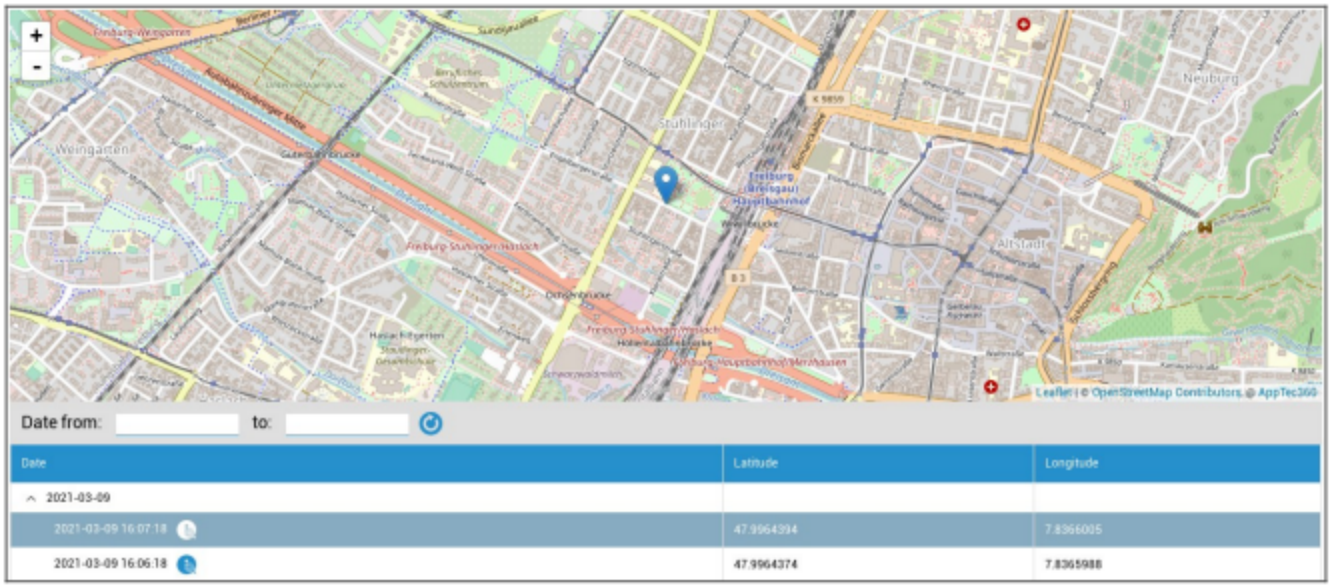
Bluetooth MAC	Adresa MAC Bluetooth

Riadenie bezpečnosti

Ochrana proti krádeži (len na úrovni zariadenia)

Informácie GPS (len na úrovni zariadenia)

Tu môžete určiť aktuálne/posledné umiestnenie zariadenia. Lokalizácia môže byť chránená jedným alebo dokonca dvoma heslami - pozri: Všeobecné nastavenia - Súkromie - Prístup k GPS



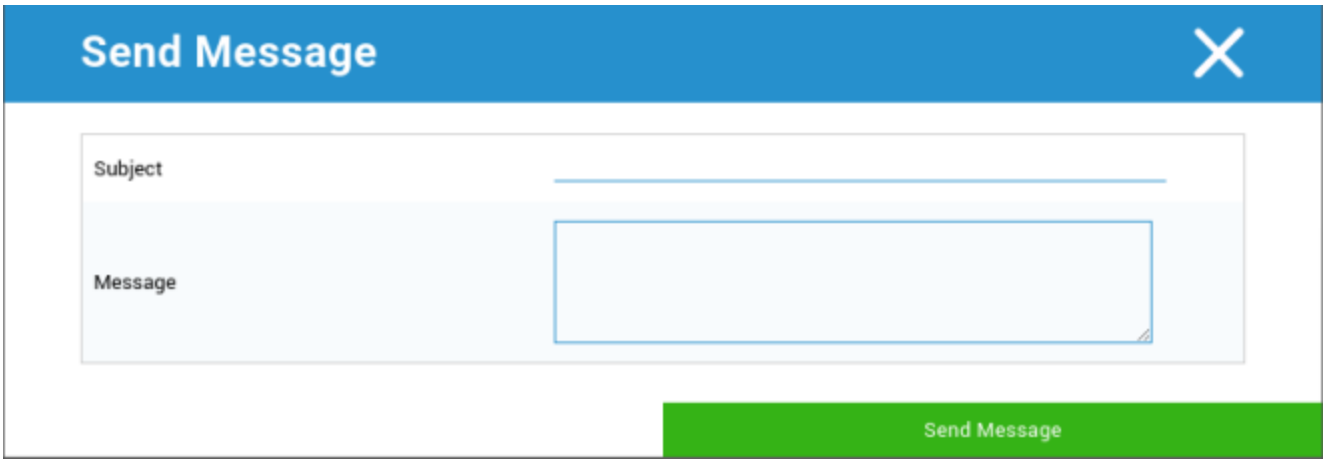
Vyčistiť a uzamknúť (len na úrovni zariadenia)

V časti "Vyčistiť a uzamknúť" môžete vykonať nasledujúce tri akcie:

Úplné utretie	Zariadenie sa obnoví do výrobných nastavení (vymažú sa firemné aj osobné údaje). Funguje len pre rozšírený pracovný profil
Podnik Wipe	Zo zariadenia koncového používateľa sa odstránia len firemné údaje (všetky aplikácie, údaje atď., ktoré poskytla spoločnosť AppTec)
Uzamknutie obrazovky	Ak je aktivovaný zámok obrazovky, stačí zariadenie odomknúť pomocou hesla zariadenia/PIN kódu.

Správa (len na úrovni zariadenia)

Tu môžete vyplniť predmet a správu a odoslať ju koncovému používateľskému zariadeniu.



Konfigurácia zabezpečenia

Prístupový kód zariadenia

V časti "Prístupový kód" môžete povoliť heslo zariadenia, pričom máte k dispozícii tieto možnosti nastavenia

Minimálna dĺžka hesla	stanovuje minimálny počet symbolov, ktoré musí heslo obsahovať	
Kvalita hesla	Nešpecifikované	Táto zásada nemá žiadne požiadavky na heslo.
	Biometrické Slabé	Táto politika umožňuje použitie biometrickej technológie rozpoznávania s nízkou úrovňou zabezpečenia. To znamená technológie, ktoré dokážu rozpoznať totožnosť jednotlivca približne na úrovni trojmiestneho PIN kódu (falošná detekcia je menej ako 1 z 1 000).
	Niečo	Táto zásada vyžaduje nastavenie nejakého hesla alebo vzoru, ale nevynucuje žiadne konkrétne pravidlá.
	Abecedné	Používateľ musí zadať heslo obsahujúce aspoň znaky abecedy (alebo iný symbol).
	Alfanumerické	Používateľ musí zadať heslo, ktoré obsahuje aspoň číselné a abecedné (alebo iné znaky).
	Komplex	Používateľ musí štandardne zadať heslo obsahujúce aspoň jedno písmeno, jednu číslicu a špeciálny symbol. Pomocou tejto kvality hesla možno obmedziť, aby heslá obsahovali rôzne sady znakov, napríklad aspoň veľké písmeno atď.
Minimálna dĺžka hesla	Nastavte požadovaný počet znakov pre heslo. Môžete napríklad vyžadovať, aby PIN alebo heslá mali aspoň šesť znakov.	
Minimálne číselné znaky požadované v hesle	Minimálne číselné znaky požadované v hesle	
Minimálny počet malých písmen v hesle	Minimálny počet malých písmen v hesle	
Minimálny počet veľkých písmen v hesle	Minimálny počet veľkých písmen v hesle	

Minimálny počet nepísmenových znakov požadovaných v hesle	Minimálny počet nepísmenových znakov požadovaných v hesle
Minimálne požadované symboly v hesle	Minimálne požadované symboly v hesle

Maximálny čas blokovania nečinnosti	Maximálna nečinnosť používateľa do časového uzamknutia
Časový limit vypršania platnosti hesla	stanovuje, po uplynutí ktorého časového intervalu heslo vyprší a musí sa vydať nové heslo
Obmedzenie histórie hesiel	Počet predtým použitých hesiel, ktoré nie sú povolené
Maximálny počet neúspešných pokusov o zadanie hesla	stanovuje, ako často môže byť heslo zadané nesprávne, kým sa vykoná úplné vymazanie zariadenia
Povolenie biometrického overovania	Umožňuje overovanie pomocou odtlačku prsta alebo skenovania dúhovky. Len pre Samsung KNOX 2.1 a vyššie

Prístupový kód kontajnera

V časti "Prístupový kód" môžete povoliť heslo kontajnera, pričom máte k dispozícii tieto možnosti nastavenia:

Minimálna dĺžka hesla	stanovuje minimálny počet symbolov, ktoré musí heslo obsahovať	
Kvalita hesla	Nešpecifikované	Táto zásada neobsahuje žiadne požiadavky na heslo.
	Biometrické Slabé	Táto politika umožňuje použitie biometrickej technológie rozpoznávania s nízkou úrovňou zabezpečenia. To znamená technológie, ktoré dokážu rozpoznať totožnosť jednotlivca približne na úrovni trojmiestneho PIN kódu (falošná detekcia je menej ako 1 z 1 000).
	Niečo	Táto zásada vyžaduje nastavenie nejakého hesla alebo vzoru, ale nevynucuje žiadne konkrétne pravidlá.
	Abecedné	Používateľ musí zadať heslo obsahujúce aspoň znaky abecedy (alebo iný symbol).
	Alfanumerické	Používateľ musí zadať heslo, ktoré obsahuje aspoň číselné a abecedné (alebo iné znaky).
	Komplex	Používateľ musí štandardne zadať heslo obsahujúce aspoň jedno písmeno, jednu číslicu a špeciálny symbol. Pomocou tejto kvality hesla možno obmedziť, aby heslá obsahovali rôzne sady znakov, napríklad aspoň veľké písmeno atď.
Minimálna dĺžka hesla	Nastavte požadovaný počet znakov pre heslo. Môžete napríklad vyžadovať, aby PIN alebo heslá mali aspoň šesť znakov.	
Minimálne číselné znaky požadované v hesle	Minimálne číselné znaky požadované v hesle	
Minimálny počet malých písmen v hesle	Minimálny počet malých písmen v hesle	
Minimálny počet veľkých písmen v hesle	Minimálny počet veľkých písmen v hesle	
Minimálny počet nepísmenových znakov požadovaných v hesle	Minimálny počet nepísmenových znakov požadovaných v hesle	

Minimálne požadované symboly v hesle	Minimálne požadované symboly v hesle

Maximálny čas blokovania nečinnosti	Maximálna nečinnosť používateľa do časového uzamknutia
Časový limit vypršania platnosti hesla	stanovuje, po uplynutí ktorého časového intervalu heslo vyprší a musí sa vydať nové heslo
Obmedzenie histórie hesiel	Počet predtým použitých hesiel, ktoré nie sú povolené
Maximálny počet neúspešných pokusov o zadanie hesla	stanovuje, ako často môže byť heslo zadané nesprávne, kým sa vykoná úplné vymazanie zariadenia

AntiVirus

Automatické skenovanie	Povolenie pravidelného automatického skenovania
Interval skenovania	Interval vyšetrenia (rýchly/úplný)
Úplné automatické skenovanie	Povolenie úplného automatického skenovania
Automatické aktualizácie	Povolenie automatických aktualizácií
Interval kontroly aktualizácie	Ako často by sa mala aplikácia a jej databáza aktualizovať (vírusy/poškodený kód)
Ochrana aplikácií	Povolenie automatického skenovania aplikácií
Ochrana karty SD	Povolenie automatického skenovania karty SD
Aktualizácia iba Wi-Fi	Ak je táto možnosť povolená, aktualizácie sa použijú len vtedy, keď je zariadenie úspešne pripojené k sieti Wi-Fi.

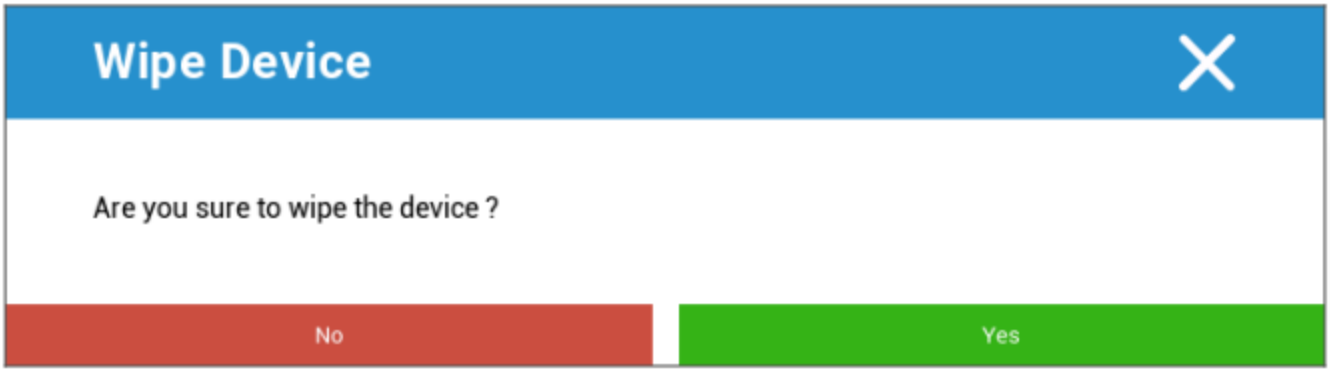
Koniec životnosti (len na úrovni zariadenia)

Vyčistiť (len na úrovni zariadenia)

V časti "Wipe" (Vymazať) môžete obnoviť výrobné nastavenia zariadenia (iba v rozšírenom pracovnom profile).

V tomto prípade sa v zariadení koncového používateľa vymažú firemné, ako aj súkromné údaje.

Po kliknutí na symbol mínus sa zobrazí nasledujúca správa:



Pomocou možnosti "Áno" môžete vykonať vymazanie.

V časti "Wipe Report" sa môžu zobraziť tieto položky

Zotreté	História toho, kto vykonal utretie
Dátum	Dátum
Stav	Stav (napr. či bolo vymazanie vykonané úspešne)

Nastavenia obmedzenia

Obmedzenia

Tu je možné obmedziť a zablokovať rôzne veci.

Presadzovanie súladu	Režim Výzva používateľovi - používateľ bude vyzvaný na vykonanie potrebných činností. Kontajner s uzamknutým režimom - skryje všetky aplikácie, kým nie sú splnené všetky požiadavky
Zásady oprávnení počas behu	Výzva používateľovi na zadanie nových požiadaviek na povolenie Vždy udeľte nové žiadosti o nové povolenie Vždy zamietnuť nové žiadosti o povolenie Varovanie: Niektoré aplikácie majú problémy s rozpoznaním oprávnení, ak sú nastavené automaticky. Ak vždy udeľujete oprávnenia a stretávate sa s problémami s aplikáciami, ktoré tvrdia, že oprávnenia chýbajú, nastavte túto možnosť na "vyzvať používateľa" a znovu nainštalujte aplikáciu.
Povolenie odchádzajúcej schránky	Umožňuje kopírovanie a vkladanie zvnútra kontajnera do vonkajšej časti
Povolenie rozlíšenia ID volajúceho	Zobrazenie názvu prichádzajúceho hovoru na základe kontaktov v kontajneri
Povolenie rozlíšenia vyhľadávania kontaktov	Umožňuje vyhľadávať mená v kontajneri kontaktov pri uskutočňovaní hovorov
Povolenie zdieľania kontaktov cez Bluetooth	Umožňuje prístup ku kontaktu kontajnera v aute
Zakázanie odchádzajúceho lúča NFC	Zakázanie funkcie NFC pre kontajner
Povolenie neznámych zdrojov	Ak je táto funkcia povolená, používatelia môžu aplikácie načítavať zboku inštaláciou súboru .apk.
Povolenie ladenia USB	Ak je táto možnosť povolená, používatelia môžu zapnúť ladenie USB.
Zakázať úpravu účtu	Zakázanie vytvárania, odstraňovania a modifikácie účtov v kontajneri

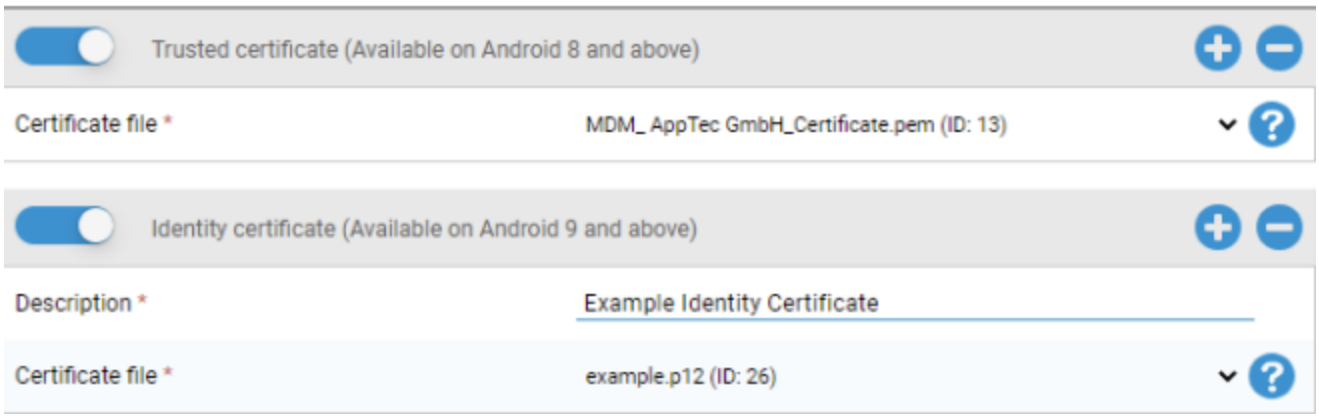
	Majte na pamäti, že niektoré aplikácie potrebujú vytvoriť alebo upraviť kontá, aby fungovali podľa očakávania.

Obmedzenia pracovného profilu. K dispozícii len na zariadeniach so systémom Android 11 a vyšším, s rozšíreným pracovným profilom	
Zakázať fotoaparát	Určuje, či je fotoaparát v pracovnom profile zakázaný.
Zakázať pripojenie Bluetooth	Určuje, či je v pracovnom profile zakázaný bluetooth.
Povolenie ochrany pred obnovením výrobných nastavení	Aktiváciou tejto funkcie prepíšete ochranu pred obnovením výrobných nastavení systému Android na účet Google, ktorý ste definovali v časti "Všeobecné nastavenia" → "Konfigurácia systému Android" → "Android Enterprise" → "Ochrana pred obnovením výrobných nastavení" Ak je táto funkcia aktivovaná a zariadenie resetujete, budete musieť pri opätovnom nastavení zariadenia zadať nakonfigurovaný účet Google.
Aktualizácia riadiaceho systému OS	Ak zapnete túto možnosť, nastavíte správanie aktualizácie na automatické, okenné alebo odložené.
Politika aktualizácie	Automaticky: Inštaluje sa automaticky, hneď ako je k dispozícii aktualizácia. Okná: Inštalácia automaticky v rámci denného okna údržby. Týmto spôsobom sa tiež nakonfigurujú aplikácie Play tak, aby sa aktualizovali v rámci okna. Toto sa dôrazne odporúča pre kioskové zariadenia, pretože je to jediný spôsob, ako môžu byť aplikácie trvalo pripnuté na popredné miesto aktualizované aplikáciou Play. Odložiť: Odložte automatickú inštaláciu maximálne o 30 dní.

Obmedzenia osobného profilu. K dispozícii len na zariadeniach so systémom Android 11 a vyšším, s rozšíreným pracovným profilom	
Zakázať fotoaparát	Určuje, či je fotoaparát v osobnom profile zakázaný.
Zakázať pripojenie Bluetooth	Určuje, či je v osobnom profile zakázaný bluetooth.
Povolenie neznámych zdrojov	Ak je táto funkcia povolená, používatelia pracovného profilu môžu aplikácie načítať zboku nainštalovaním súboru .apk.

Správa certifikátov

Tu môžete distribuovať dôveryhodné certifikáty a certifikáty identity do svojich zariadení. Na distribúciu dôveryhodných certifikátov je potrebný systém Android 8 alebo novší a na distribúciu certifikátov identity je potrebný systém Android 9 alebo novší.



Pomocou "+" môžete pridať viacero certifikátov.

Dôveryhodné certifikáty musia byť vo formáte PEM.

Certifikáty totožnosti musia byť vo formáte PKCS12.

Správa pripojenia

Wifi

Pre toto nastavenie vykonajte predbežnú konfiguráciu zariadení koncových používateľov pre prístup k interným prístupovým bodom

.

Identifikátor súboru služieb (SSID)	SSID pre sieť, ktorá sa má pripojiť
Skrytá sieť	Aktivácia v prípade, že prístupový bod nevysiela identifikátor SSID

Typ zabezpečenia

Stanovenie typu zabezpečenia prístupového bodu

WEP

Heslo	Heslo pre AP

WPA/WPA2

Heslo	Heslo pre AP

802.1x EAP

Metóda EAP

PWD	Identita	Identita
	Heslo	Heslo

PEAP	Fáza 2 autentifikačného protokolu	žiadne	Žiadny dodatočný protokol
		MSCHAPV2	Protokol MSCHAPV2
		GTC	Protokol GTC
	Certifikát CA	Certifikát CA	
	Identita	Identita	
	Anonymná identita	Anonymná identita	
	Heslo	Heslo	

TTLS	Fáza 2 autentifikačného protokolu	žiadne	Žiadny dodatočný protokol
		PAP	Protokol PAP
		MSCHAP	Protokol MSCHAP
		MSCHAPV2	Protokol MSCHAPV2
		GTC	Protokol GTC
	Certifikát CA	Certifikát CA	
	Identita	Identita	
	Anonymná identita	Anonymná identita	
	Heslo	Heslo	

TLS	Certifikát CA	Certifikát CA
	Identita	Identita
	Heslo	Heslo

VPN

Názov pripojenia	Názov pripojenia VPN

Typ VPN

VPN

Klient VPN

Klient VPN AppTec	
Konfigurácia brány	Vyberte konfiguráciu brány VPN (pozri **Všeobecné nastavenia > Univerzálna brána > Nastavenia VPN**).
Vždy zapnutá sieť VPN	Povolenie funkcie Native Lockdown
Povolenie uzamknutia AppTec	Povolenie uzamknutia AppTec

Zabudované (k dispozícii len v zariadeniach Samsung)			
Typ pripojenia	PPTP	Server	Server
		Povolenie šifrovania PPTP	Povolenie šifrovania PPTP
	L2TP / IPSec PSK	Server	Server
		Predsdieľaný kľúč IPSec	Predsdieľaný kľúč IPSec
		Povolenie funkcie L2TP Secret	Povolenie funkcie L2TP Secret
		Tajomstvo L2TP	Tajomstvo L2TP
	IPSec XAuth PSK	Server	Server
		Identifikátor IPSec	Identifikátor IPSec
		Predsdieľaný kľúč IPSec	Predsdieľaný kľúč IPSec
Vyhľadávanie domén DNS	Vyhľadávanie domén DNS		
Expertné nastavenia	Servery DNS	Servery DNS	
	Trasy preposielania	Trasy preposielania	

Otvorená sieť VPN		
Server	Server	
Profil OpenVPN	Profil OpenVPN	
Aplikácia OpenVPN	OpenVPN pre Android (odporúčané)	
	Pripojenie OpenVPN	
Expertné nastavenia	Servery DNS	Servery DNS
	Trasy preposielania	Trasy preposielania

Samsung / Strong Swan			
Typ pripojenia	PPTP	Server	Server
		Používateľské meno	Používateľské meno
		Heslo	Heslo
		Povolenie šifrovania PPTP	Povolenie šifrovania PPTP
	L2TP / IPSec PSK	Server	Server
		Predsdieľaný kľúč IPSec	Predsdieľaný kľúč IPSec
		Používateľské meno	Používateľské meno
		Heslo	Heslo
		Povolenie funkcie L2TP Secret	Tajomstvo L2TP
	IPSec XAuth PSK	Server	Server
		Identifikátor IPSec	Identifikátor IPSec
		Predsdieľaný kľúč IPSec	Predsdieľaný kľúč IPSec
		Používateľské meno	Používateľské meno
		Heslo	Heslo
Expertné nastavenia	Servery DNS	Servery DNS	
	Trasy preposielania	Trasy preposielania	

Cisco Any Connect		
Server	Server	
Režim certifikátu	Bezbariérový	Bezbariérový
	Automatické	Automatické
Expertné nastavenia	Servery DNS	Servery DNS
	Trasy preposielania	Trasy preposielania

Sieť VPN pre jednotlivé aplikácie

Klient VPN

Klient VPN AppTec		
Konfigurácia brány	Vyberte konfiguráciu brány VPN (pozri **Všeobecné nastavenia > Univerzálna brána > Nastavenia VPN**).	
Aplikácie VPN	Aplikácie VPN	
Vždy zapnutá sieť VPN	Povolenie funkcie Native Lockdown	Vždy zapnutá sieť VPN
Povolenie uzamknutia AppTec	Povolenie uzamknutia AppTec	

Samsung / Strong Swan			
Typ pripojenia	PPTP	Server	Server
		Aplikácie VPN	Aplikácie VPN
		Používateľské meno	Používateľské meno
		Heslo	Heslo
		Povolenie šifrovania PPTP	Povolenie šifrovania PPTP
	L2TP / IPSec PSK	Server	Server
		Aplikácie VPN	Aplikácie VPN
		Predsdieľaný kľúč IPSec	Predsdieľaný kľúč IPSec
		Používateľské meno	Používateľské meno
		Heslo	Heslo
		Povolenie funkcie L2TP Secret	Tajomstvo L2TP
	IPSec XAuth PSK	Server	Server
		Aplikácie VPN	Aplikácie VPN
		Identifikátor IPSec	Identifikátor IPSec
		Predsdieľaný kľúč IPSec	Predsdieľaný kľúč IPSec
		Používateľské meno	Používateľské meno
		Heslo	Heslo
Expertné nastavenia	Servery DNS	Servery DNS	
	Trasy preposielania	Trasy preposielania	

Obmedzenia

Tu môžete nastaviť obmedzenia týkajúce sa správy pripojenia

Povolenie dátového roamingu	Povolenie mobilných dát počas roamingu
Vynútenie dátového roamingu	Ak je aktivovaný, roaming pre mobilné dáta je trvalo aktivovaný (neodporúča sa!) Toto nastavenie prepíše nastavenie "Povoliť dátový roaming"!
Použitie systémového servera http Proxy	Použitie proxy servera HTTP, ktorý je k dispozícii v nastaveniach systému, závisí od pripojenej siete (WiFi alebo APN).

Správa PIM

Výmena Gmail

Informácie: Táto konfigurácia sa použije pre aplikáciu Gmail. Preto musíte schváliť a nainštalovať aplikáciu Gmail.

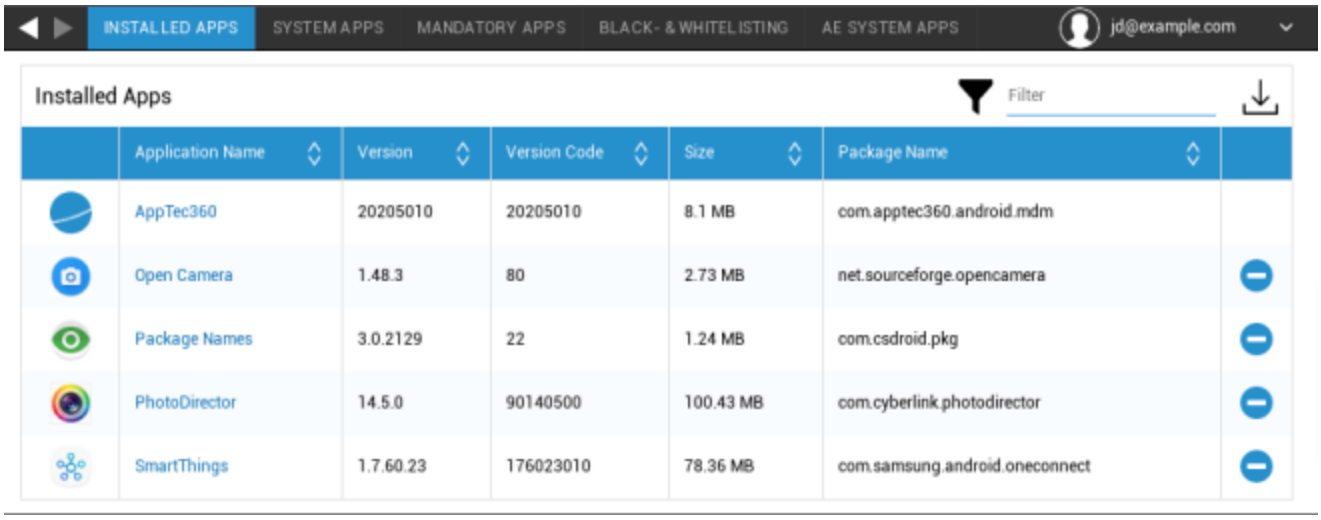
E-mailová adresa	Poskytnutá e-mailová adresa používateľa Všimnite si "zástupné symboly", ktoré môžete použiť na prácu s povereniami a nevykonávate zmeny ručne na každom zariadení. Jedným kliknutím si ich môžete zobraziť sami
Názov hostiteľa servera	Adresa servera vašich serverov Exchange
Prihlasovacie meno	Prihlasovacie meno pre príslušné zariadenie koncového používateľa, všimnite si tiež "Placeholders here".
Podpis	Môžete pripojiť podpis (Tip: Niektoré zariadenia vyžadujú formátovanie podpisu v HTML).
Počet predchádzajúcich dní na synchronizáciu	Počet dní, ktoré určujú, kedy sa e-maily synchronizujú späť
Identifikátor zariadenia	Ein String der die EAS DeviceID enthält. Dies ist Teil des EAS Protokols und wird in einigen Umgebungen benötigt
Používanie Secure Sockets Layer (SSL)	Použitie pripojenia SSL
Prijať všetky certifikáty	Všetky certifikáty sú akceptované. Túto možnosť vyberte, ak váš server Exchange používa certifikát s vlastným podpisom.
Povolenie nespravovaných účtov	Umožniť používateľom pridať alebo odstrániť ľubovoľný účet Exchange okrem účtu uvedeného v tejto spravovanej konfigurácii. Ak je toto nastavenie povolené, nemôžete používateľom zabrániť v pridávaní iných účtov Exchange do služby Gmail. Nemôžete tiež kontrolovať zdieľanie údajov medzi inými aplikáciami a účtami Exchange pridanými používateľmi. Toto nastavenie by malo byť povolené len vtedy, ak vaši používatelia potrebujú v službe Gmail udržiavať viac ako jeden pracovný účet Exchange.
Certifikát klienta	Certifikát klienta. Vyžaduje sa len v prípade, ak ho váš poštový server očakáva.

Správa aplikácií

Správca podnikových aplikácií

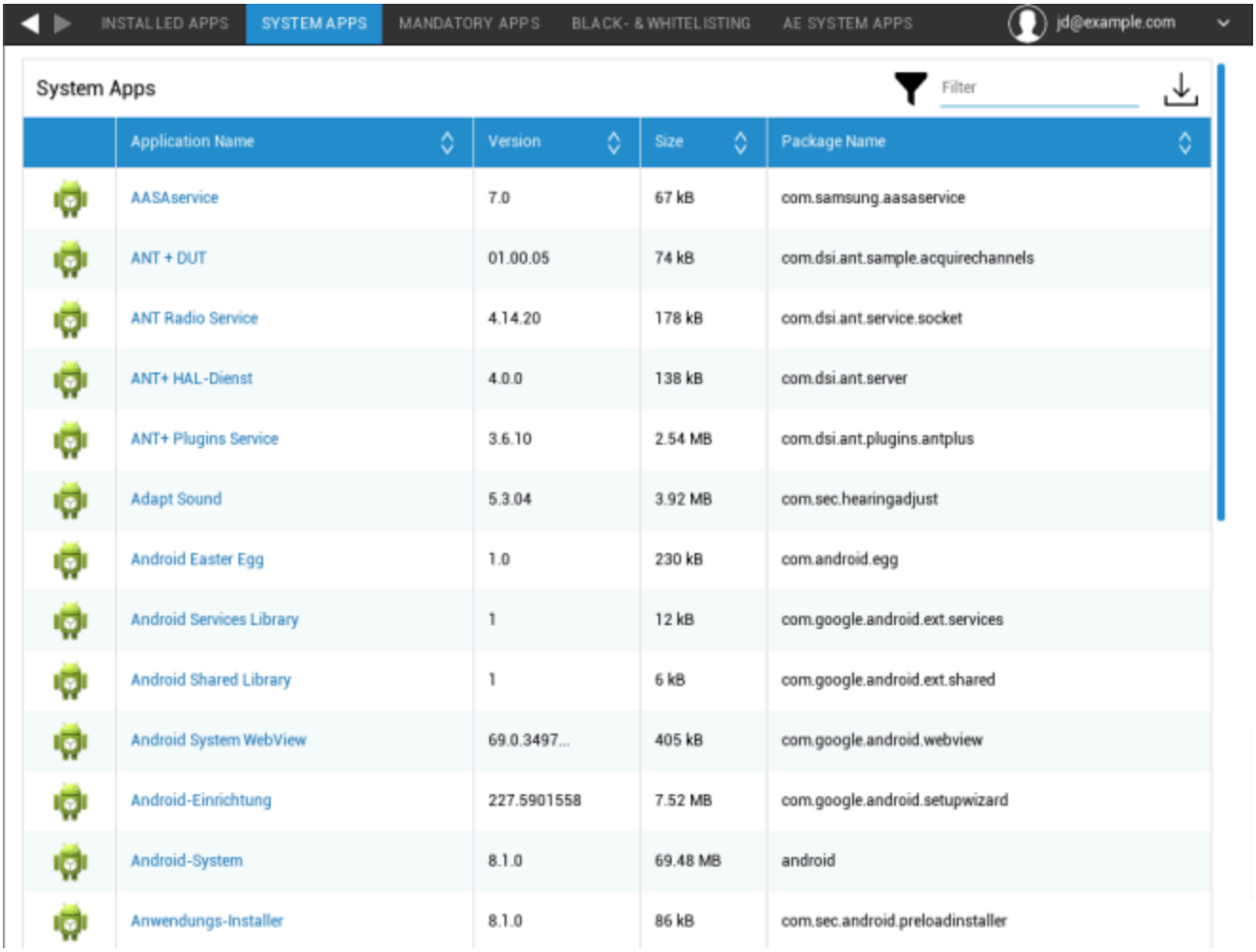
Nainštalované aplikácie (len na úrovni zariadenia)

Tu sa zobrazia všetky aplikácie, ktoré sú v súčasnosti nainštalované v kontajneri.



Systémové aplikácie (len na úrovni zariadenia)

V časti "Systémové aplikácie" sa zobrazí zoznam všetkých aplikácií a služieb, ktoré už výrobca zariadenia nainštaloval do zariadenia koncového používateľa.

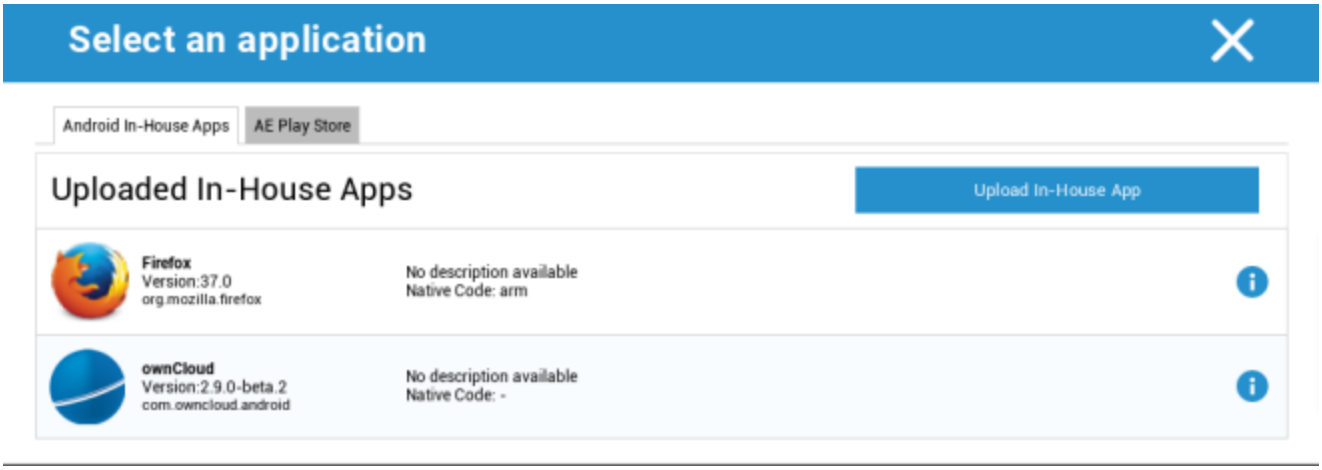


Povinné aplikácie

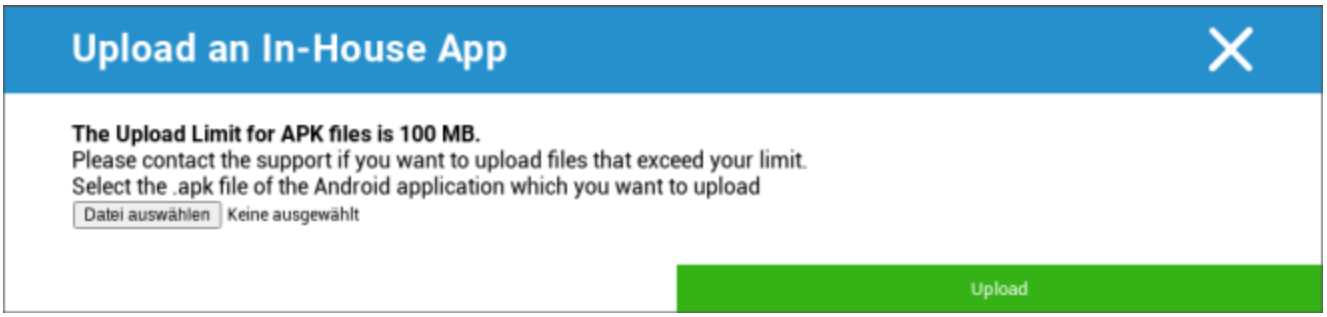
V časti Povinné aplikácie môžete nastaviť povinné požadované aplikácie. Používateľ bude priebežne vyzývaný na inštaláciu tejto určenej aplikácie, ak ide o aplikáciu InHouse. Aplikácie z Obchodu Play sa nainštalujú automaticky.

Prostredníctvom , možno definovať povinnú požadovanú aplikáciu.

Môže to byť interná aplikácia z "Interných aplikácií pre Android", ktorú ste nahrali vo Všeobecných nastaveniach.

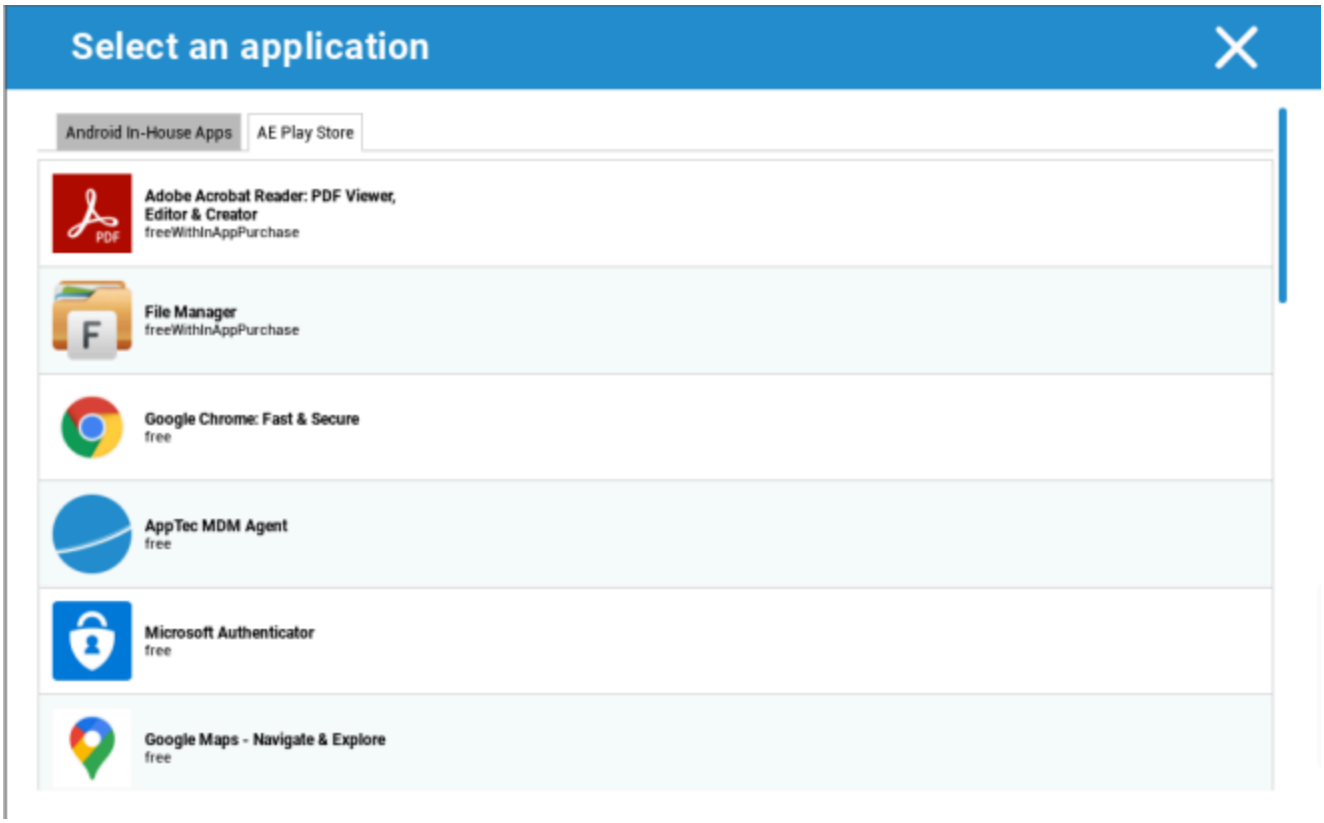


Súbor APK môžete vybrať a nahrať aj priamo pomocou funkcie "Nahrať vlastnú aplikáciu".



Ak inštalujete aplikáciu In-House, budete mať možnosť aktivovať funkciu "Keep up to date". Ak je táto funkcia aktivovaná a v DB aplikácie In-House App ste definovali novšiu verziu, aplikácia sa v zariadení aktualizuje.

Alebo to môže byť aplikácia "AE Play Store" z pracovného obchodu Google Play.



Na tejto karte sa zobrazia len schválené aplikácie "AE Play Store Apps".

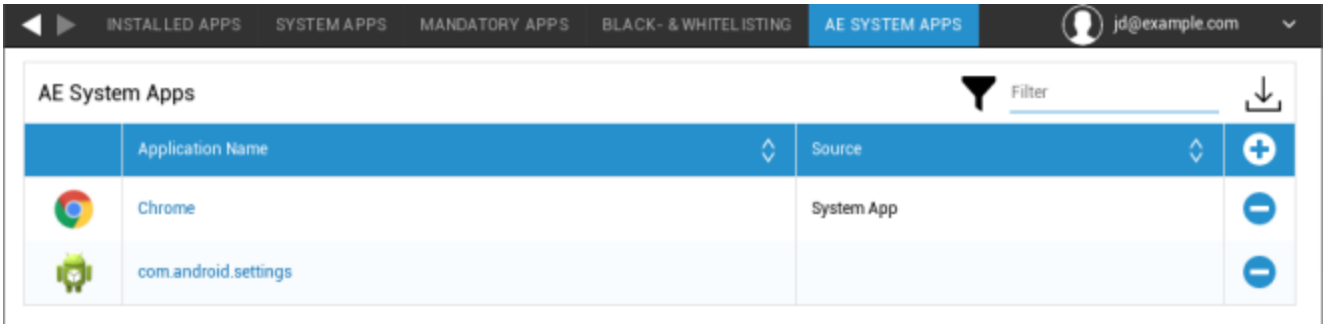
Ak chcete schváliť aplikáciu "AE Play Store", prejdite do časti "Všeobecné nastavenia" > "Správa aplikácií" > "AE Play".

Obchod" a pridajte aplikáciu pomocou tlačidla, ktoré vás presmeruje na kartu "Aplikácie obchodu Play" (alebo môžete priamo prejsť na kartu "Aplikácie obchodu Play").

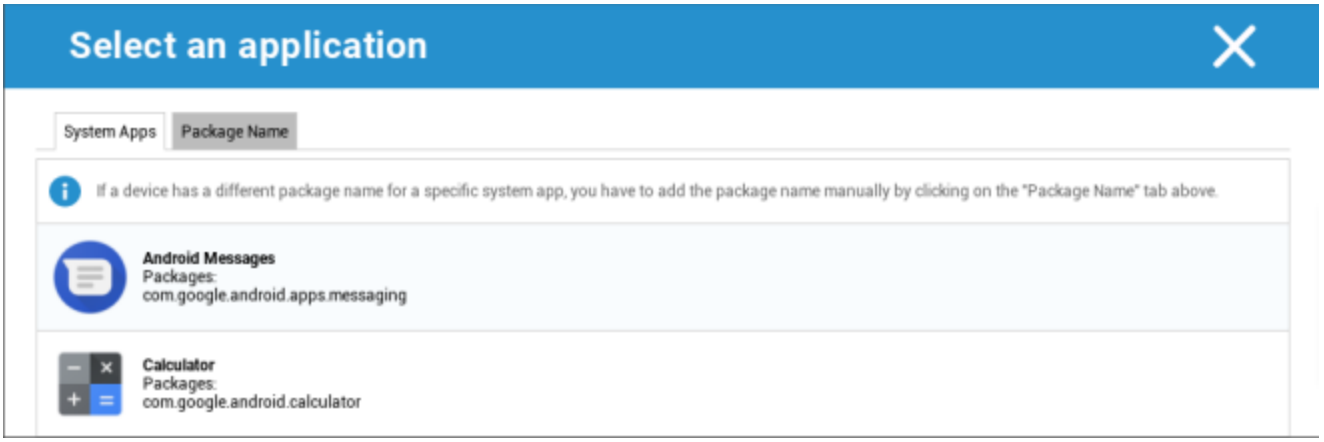
Na karte "Aplikácie v Obchode Play" môžete vyhľadávať aplikácie. Po kliknutí na aplikáciu sa otvorí stránka aplikácie a tu môžete aplikáciu schváliť kliknutím na tlačidlo "Schváliť".

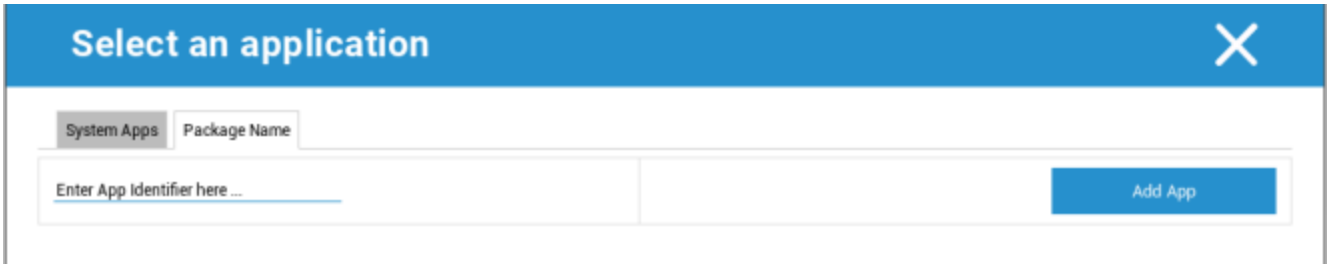
Aplikácie systému AE

Tu môžete definovať zoznam, ktorý obsahuje konkrétne systémové aplikácie, ktoré sa majú aktivovať v zariadeniach.



Po kliknutí na tlačidlo môžete vybrať zo zoznamu možných systémových aplikácií, ktorý poskytuje spoločnosť Google, alebo priamo zadať názov balíka systémovej aplikácie, ktorá sa má aktivovať.





Majte na pamäti, že systémové aplikácie v zozname poskytnutom spoločnosťou Google sú len aplikácie, ktoré môžu byť systémovými aplikáciami, ale nemusia byť nevyhnutne systémovými aplikáciami vo vašich zariadeniach.

Tento zoznam sa však týka len aplikácií, ktoré sú už predinštalované.

Pridanie aplikácií, ktoré nie sú predinštalované vo vašich zariadeniach, nebude mať vplyv na vaše zariadenia bez ohľadu na to, či je aplikácia zo zoznamu poskytnutého spoločnosťou Google alebo je

priamo zadaný názov balíka aplikácie.

Obmedzenia a nastavenia

Nastavenia správy aplikácií

Tu môžete nakonfigurovať správanie zariadenia, pokiaľ ide o aktualizácie aplikácií.

Frekvencia kontroly aktualizácie	Určite, v akom intervale bude klient AppTec vyhľadávať aktualizácie aplikácií. Predvolená hodnota je 24 hodín.
Prahová hodnota Wi-Fi	Aplikácie, ktoré sú väčšie ako zadaná veľkosť, sa budú sťahovať cez Wi-Fi. Ak je vybratá možnosť "Iba Wi-Fi", všetky aplikácie sa budú sťahovať cez Wi-Fi.

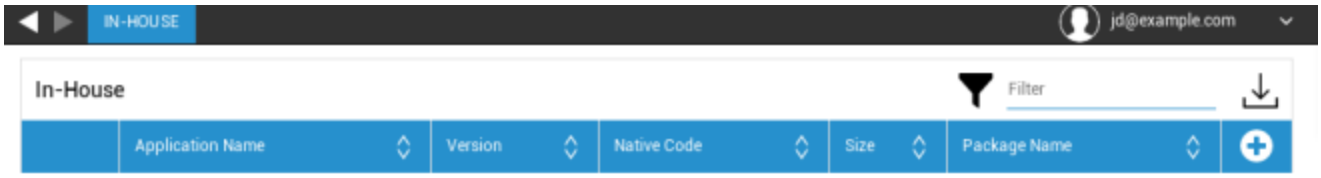
Obchod s podnikovými aplikáciami

Vnútorná stránka

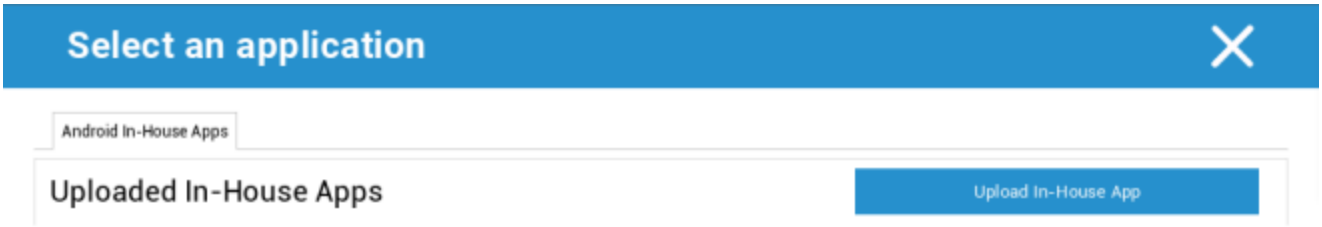
V bode "In-House" môžete nahrať a distribuovať interne vyvinuté aplikácie.

Pomocou tohto symbolu môžete distribuovať ďalšie aplikácie In-House.

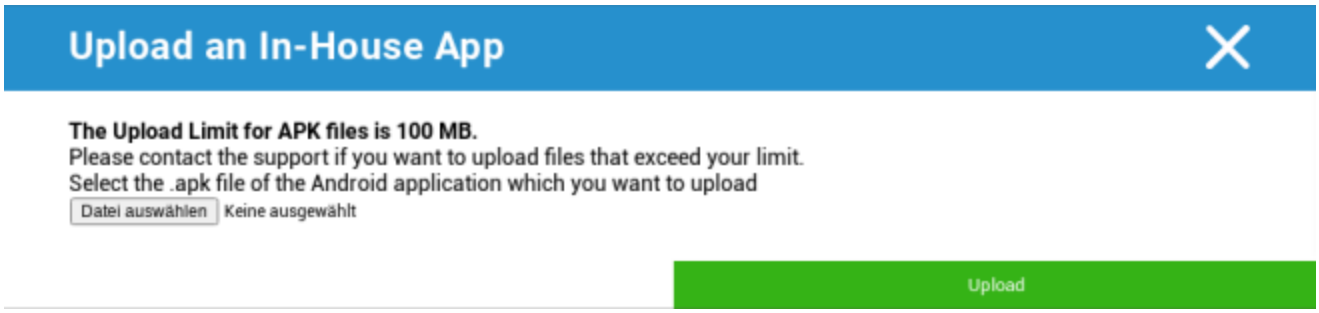
Ak inštalujete aplikáciu In-House, budete mať možnosť aktivovať funkciu "Keep up to date". Ak je táto funkcia aktivovaná a v DB aplikácie In-House App ste definovali novšiu verziu, aplikácia sa v zariadení aktualizuje.



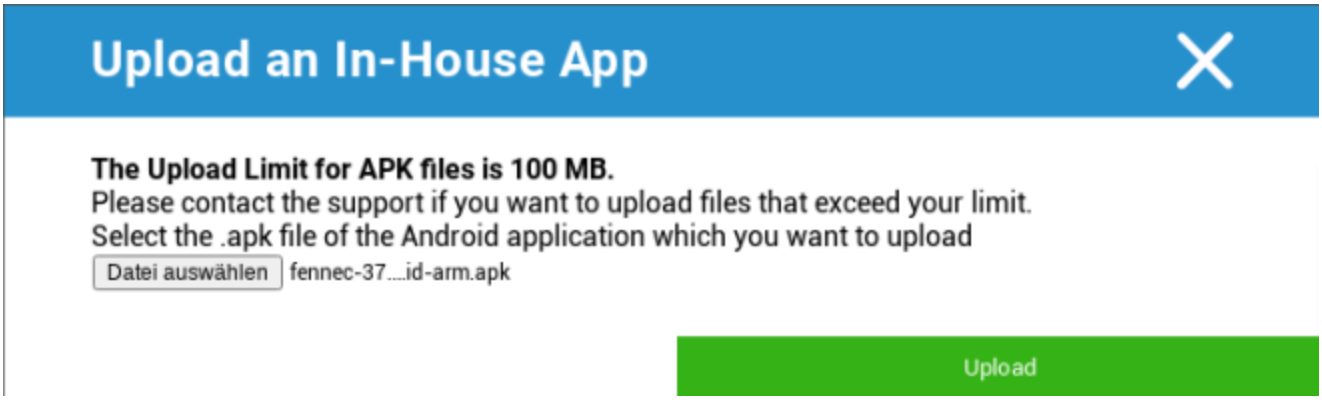
Ak nemáte distribuované aplikácie In-House, dostanete nasledujúci prehľad:



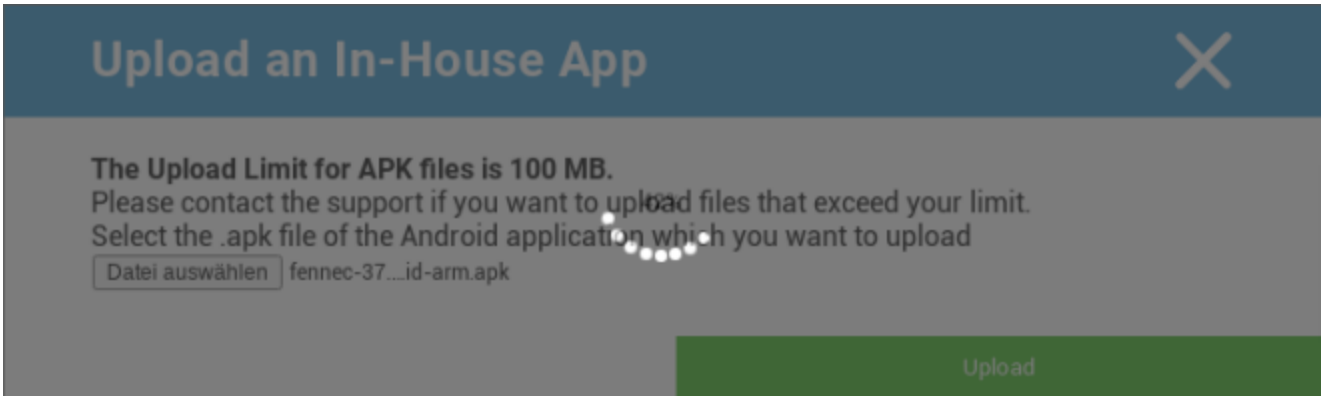
Na tento účel kliknite na položku "Upload In-House App", potom sa zobrazí nasledujúci prehľad:



Teraz vyberte pomocou "Search... "súbor .apk a potom kliknite na "Upload".



Vaša aplikácia sa teraz nahrá, uprostred kruhu sa zobrazí percentuálny ukazovateľ, ktorý ukazuje, aká veľká časť vašej aplikácie už bola nahraná.



Ak bolo odoslanie vašej internej aplikácie úspešné, môžete nahranú aplikáciu nájsť vo svojom Katalógu aplikácií.

Používateľ má teraz možnosť zobraziť a nainštalovať túto aplikáciu v obchode AppTec Store na zariadení koncového používateľa v kategórii "In-House".

Vzhľadom na to, že nejde o aplikáciu Google PlayStore, používateľ nepotrebuje uložené ID Google v príslušnom zariadení koncového používateľa.

Obchod Play pre podniky

Obchod AE Play

Tu môžete pridať aplikácie do obchodu Android Enterprise Playstore. Upozorňujeme, že pred pridaním aplikácií musíte Aplikácie schváliť pomocou konta správcu AE.

Pokyny na schválenie aplikácie nájdete v časti Povinné aplikácie.

Správa obsahu

ContentBox

Tu môžete aktivovať ContentBox.

Hneď ako prepnete možnosť "Enable ContentBox" na "On", do zariadenia koncového používateľa sa automaticky nainštaluje samostatná aplikácia ContentBox.

Zabezpečený prehliadač

Tu môžete konfigurovať nastavenia pre AppTec Secure Browser.

Akonáhle prepnete sekciu "Zabezpečený prehliadač" na "Zapnutý", do zariadenia koncového používateľa sa automaticky nainštaluje samostatná aplikácia prehliadača.

Vyžadovať heslo	Vyžadovať od používateľa nastavenie a používanie hesla na prístup do prehliadača.
Minimálna požadovaná dĺžka hesla	Nastavenie požadovaného počtu znakov pre heslo
Požadovaná kvalita hesla	Nastavenie požadovanej kvality hesla
Obmedzenie sťahovania / Otvoriť v	
Obmedzenie nahrávania	
Nahrávanie bielej listiny	Zoznam adries URL, pre ktoré bude nahrávanie vždy povolené.
Povoliť kopírovanie	Povoľte kopírovanie, vyrezávanie alebo zdieľanie textu vo vnútri webových stránok.
Povolenie snímania obrazovky	Umožniť zachytávanie snímok obrazovky.
Frekvencia čistenia údajov	Vyberte, s akou frekvenciou sa majú automaticky odstraňovať VŠETKY údaje používateľa (história, vyrovnávacia pamäť atď.).
Záložky spoločnosti	Záložky sa zobrazia v priečinku "Firemné záložky" v záložkách prehliadača. Používateľ ich nemôže upravovať.
Skryť adresný riadok	
Biela listina v prehliadači (bez univerzálnej brány)	Povolí vytváranie bielych zoznamov URL na strane klienta. • Záložky spoločnosti sú vždy zaradené na biely zoznam • Podporované len pre 100 adries URL • Použite univerzálnu bránu na neobmedzené zaradenie do čiernej a bielej listiny
Adresy URL na bielej listine	Zoznam povolených adries URL.

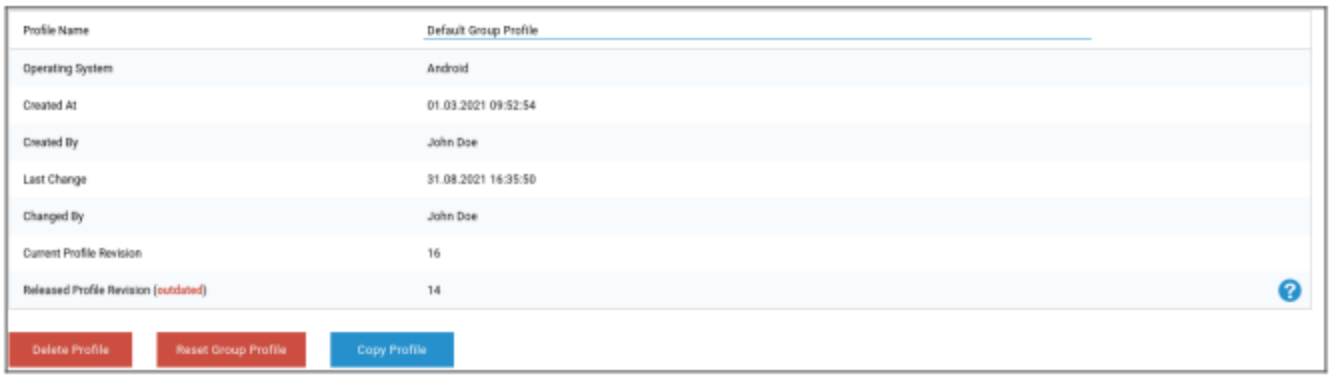
Čierna a biela listina založená na bráne	Čierna listina má tieto požiadavky: • Fungujúca univerzálna brána AppTec ("Všeobecné nastavenia" → "Univerzálna brána") • Fungujúca konfigurácia VPN so zadaným serverom DNS ("Všeobecné nastavenia" → "Univerzálna brána" → "Nastavenia VPN") • Konfigurácia čiernej listiny ("Všeobecné nastavenia" → "Univerzálna brána" → "Čierna listina domén") • Platné pripojenie VPN v profile ("Správa pripojení" → "VPN")

Konfigurácia systému Android

Všeobecné

Prehľad profilu skupiny (len na úrovni skupiny)

Po otvorení profilu skupiny sa zobrazí rýchly prehľad profilu.



Názov profilu	Názov profilu (tu sa dá zmeniť)
Operačný systém	Operačný systém, pre ktorý je profil určený
Vytvorené v	Čas vytvorenia
Vytvoril	Tvorca profilu
Posledná zmena	Čas poslednej zmeny profilu
Zmenené podľa	Účet, ktorý vykonal posledné zmeny
Aktuálna revízia profilu	Revízia uloženého stavu profilu
Vydaná revízia profilu	Priradená revízia profilu ("Priradiť teraz"). Ak sa za textom na štítku zobrazí " (zastaraný)", znamená to, že ste profil uložili, ale ešte ste ho nepriradili, takže zariadenia budú stále dostávať staršiu verziu.

Prehľad zariadení (len na úrovni zariadenia)

Ak sa nachádzate na zariadení, zobrazí sa prehľadné zhrnutie vybraného zariadenia, ktoré obsahuje nasledujúce informácie:

Názov zariadenia	Názov zariadenia
Posledná známa lokalita	Posledné známe súradnice GPS
Telefónne číslo	Telefónne číslo
Priradené povinné aplikácie	Počet pridelených povinných aplikácií
Verzia operačného systému	Verzia operačného systému zariadenia
Operačný systém	Operačný systém (Android / iOS / Windows Phone)
Sériové číslo	Sériové číslo zariadenia
Vlastníctvo zariadenia	Firemné alebo súkromné zariadenie
Typ zariadenia	Telefón alebo tablet
Zakorenené	Stav, ktorý uvádza, či bolo zariadenie rootnuté
V súlade s	V súlade s usmerneniami
IP adresa	IP adresa
Naposledy videné	Bod v čase, kedy sa zariadenie naposledy pripojilo k AppTecu
Posledný impulz	Bod v čase, keď server odoslal push do zariadenia
Priradenie používateľa	Rozbaľovacie okno na priradenie zariadenia inému používateľovi

Revízia konfigurácie (len na úrovni zariadenia)

Tu získate prehľad o tom, ktorý skupinový profil je priradený k zariadeniu.

Ak kliknete na profil skupiny, získate priamy prístup k profilu a môžete vykonať nastavenia.

Pomocou symbolu môžete vrátiť priradené aplikácie do nastavení skupinového profilu.

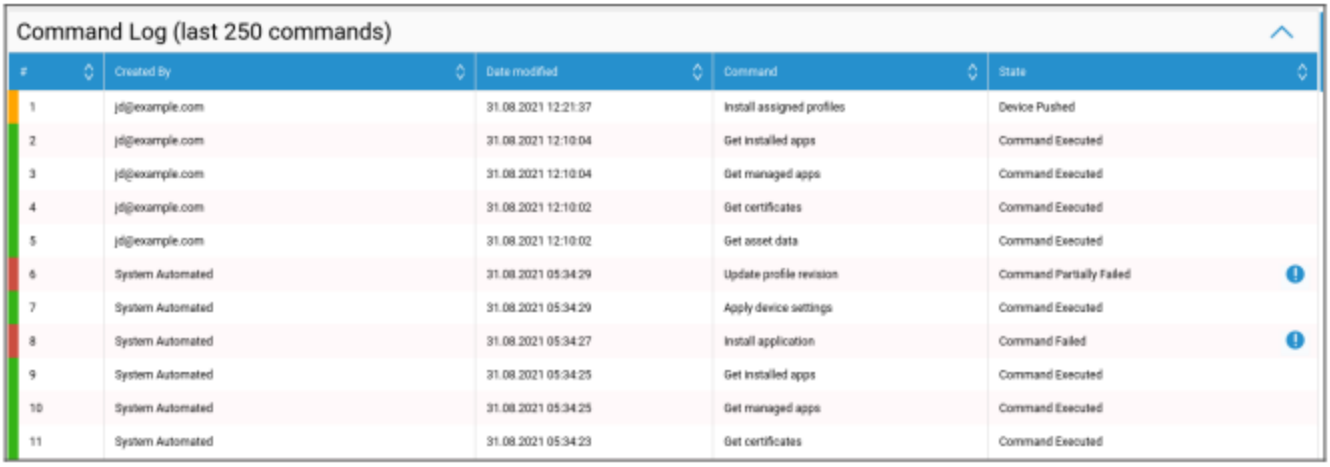
Pomocou symbolu môžete obnoviť profil zariadenia tak, aby nemal žiadne nastavenia.

"K dispozícii je novšia revízia" znamená, že profil skupiny bol zmenený a uložený, ale nie je priradený. Profil skupiny sa musí priradiť pomocou "Priradiť teraz" na úrovni skupiny, aby sa zmeny uplatnili na zariadeniach.

Protokol zariadenia (len na úrovni zariadenia)

Denník príkazov

Tu môžete vidieť, ktoré príkazy boli pre zariadenie vydané a aký je ich stav.



Príkazy vytvorené pomocou "System Automated" sú automaticky vytvorené systémom.

Možné stavy príkazov

Stlačené zariadenie	Do služby push (napr. APNS) bola odoslaná požiadavka na pripojenie, aby sa zariadenie pripojilo späť k serveru EMM.
Vytvorený príkaz	Príkaz bol vytvorený v systéme.
Odoslaný príkaz	Príkaz sa odoslal do zariadenia po jeho pripojení k serveru.
Vykonaný príkaz	Príkaz bol úspešne vykonaný.
Príkaz zlyhal	Príkaz zlyhal. *
Príkaz čiastočne zlyhal	V závislosti od operačného systému zariadenia môžu byť niektoré príkazy zoskupené. V tejto časti tejto skupiny príkazov zlyhali niektoré časti. *
Príkaz vykonaný, prípadne neúspešný	Príkaz bol vykonaný, ale možno nebol.
Príkaz Repushed	Príkaz bol opätovne odoslaný používateľom.
Vyradené	Príkaz bol zamietnutý. Napríklad preto, že bol nahradený iným príkazom alebo zariadenie bolo znovu zaregistrované a staré príkazy boli odstránené.

*Ak je za správou výkričník, môžete získať ďalšie informácie, ak kurzorom prejdete na ikonu.

Nastavenia zariadenia

Konfigurácia klienta

Tu môžete vykonať nasledujúce konfigurácie zariadenia so systémom Android:

Upozornenie po vypnutí správy zariadení	Založená varovná správa po vypnutí správy zariadení
Čas mimo súladu	Časový limit, po ktorom sa vykoná "Enforcement Action after compliance", ak zariadenie nie je v súlade. Min. 1 minúta Max. 24 hodín
Opatrenia na presadzovanie práva po uplynutí lehoty na dosiahnutie súladu	Opatrenia, ktoré sa majú prijať, akonáhle sa zariadenie stane nevyhovujúcim. • nerobiť nič = žiadna akcia • Uzamknúť zariadenie = uzamknúť zariadenie • Vymazať zariadenie = zariadenie sa obnoví na výrobné nastavenia
Frekvencia zberu údajov	Frekvencia zberu informácií o zariadení/GPS
Frekvencia srdcového tepu zariadenia	Interval, v ktorom má zariadenie kontaktovať server AppTec360 Min. 1 minúta Max. 24 hodín
Povolenie aktualizácií polohy	Ak je aktivované, zariadenie posiela aktualizácie polohy na server AppTec360
Čas aktualizácie polohy	Určuje, v akých časových intervaloch zariadenie odosiela aktualizácie polohy do aplikácie AppTec.
Používanie služby Google Location Accuracy na aktualizáciu polohy	Ak je aktivovaná, bude sa na aktualizácie polohy používať služba Google Location Accuracy (predtým známa ako sieťová poloha) (ak bola deaktivovaná v časti "Obmedzenia", toto nastavenie nebude mať žiadny vplyv).
Používanie polohy GPS na aktualizáciu polohy	Ak je aktivovaná, GPS sa bude používať na aktualizáciu polohy
Povolenie falošných lokalít	Umožňuje falšovanie informácií o polohe prostredníctvom aplikácií tretích strán

Akcia strateného spojenia	Umožňuje nastaviť určitú akciu, ktorá sa vykoná po určitom počte zlyhaných úderov srdca.
Režim presadzovania zásad	Definuje, ako agresívne bude klient AppTec360 žiadať používateľa o vykonanie určitých akcií, ktoré vyžadujú vstup používateľa. Interval (predvolené nastavenie) = pýtať sa v intervaloch, takže používateľ to môže na chvíľu odložiť do pozadia. Žiadne upozornenie = žiadne vyskakovacie okno pre požadovanú interakciu. Musíte manuálne otvoriť klienta AppTec360, aby ste skontrolovali, či je potrebná akcia. Stále upozornenie = Používateľ môže vykonať len požadovanú akciu. Klient AppTec360 sa vynúti v popredí, ak sa mu používateľ pokúsi vyhnúť
Zámok verzie AppTec360	Umožňuje definovať verziu klienta AppTec360, ktorá je maximálnou verziou, na ktorú sa klient aktualizuje.

Tapety

Tu môžete definovať vlastnú tapetu.

"Zadanie farby" umožňuje definovať farbu v hexadecimálnom formáte (napr. #000000). Povolené sú len hodnoty v hexadecimálnom tvare.

"Nastaviť obrázok ako tapetu" umožňuje nahrať obrázok. Upozorňujeme, že rôzne zariadenia s rôznymi spúšťačmi a verziami operačného systému fungujú odlišne. Neexistuje všeobecný návod na veľkosť a pomer, pretože to závisí od zariadenia.

Pre formát súboru použite JPG (alebo JPEG) alebo PNG.

Správa aktív (len na úrovni zariadenia)

Správa aktív

Informácie o zariadení

Model	**Označenie modelu zariadenia**
Operačný systém	OS
Verzia operačného systému	Verzia operačného systému
Podpora AE	Podpora pre Android Enterprise (kontajner a plne spravovaný systém)
Sériové číslo	Sériové číslo
Názov zariadenia	Názov zariadenia
Stav batérie	Stav batérie
Voľná / celková pamäť	Voľná / celková pamäť
Samsung KNOX	Úroveň rozhrania API Samsung KNOX
K dispozícii je karta SD	K dispozícii je karta SD
Emulovaná karta SD	Emulovaná karta SD
Vymeniteľná karta SD	Vymeniteľná karta SD
SD Voľná / celková pamäť	SD Voľná / Celková pamäť karty SD

Wi-Fi

IP adresa	IP adresa zariadenia
WiFi MAC	Adresa MAC WiFi

Cellular

Stav	Stav (nainštalovaná karta SIM)
Telefónne číslo	Telefónne číslo
Roaming (hlas / dáta)	Roaming pre hlas / dáta
Stav roamingu	Aktuálny stav roamingu
IP adresa	IP adresa
Prevádzkovateľ/prepravca	Prevádzkovateľ/prepravca
Mobilná technológia	Mobilná technológia
IMEI	Číslo IMEI
ICCID	Ide o identifikátor karty SIM, často aj karty Smartcard alebo karty s integrovaným obvodom (ICC).
IMSI	Medzinárodná identita mobilného účastníka (IMSI) poskytuje v mobilných sieťach GSM a UMTS jednoznačnú identifikáciu používateľov siete. IMSI pozostáva z maximálne 15 číslic a konfiguruje sa takto: • Kód mobilnej krajiny (MCC), 3 číslice • Kód mobilnej siete (MNC), 2 alebo 3 číslice • Identifikačné číslo mobilného účastníka (MSIN), 1-10 číslic
Súčasné MCC/MNC	Pozri "SIM MCC/MNC".
SIM MCC/MNC	Kód mobilnej krajiny je zavedený identifikátor krajiny, ktorý stanovila ITU podľa normy E.212. Funguje v spojení s kódom mobilnej siete (MNC) na identifikáciu mobilnej siete. Znamená kód krajiny/mobilnej siete karty SIM. Ak sa pohybujete v inej mobilnej sieti, potom sa logicky budú "Aktuálne MCC/MNC" a "SIM MCC/MNC" líšiť.

Bluetooth

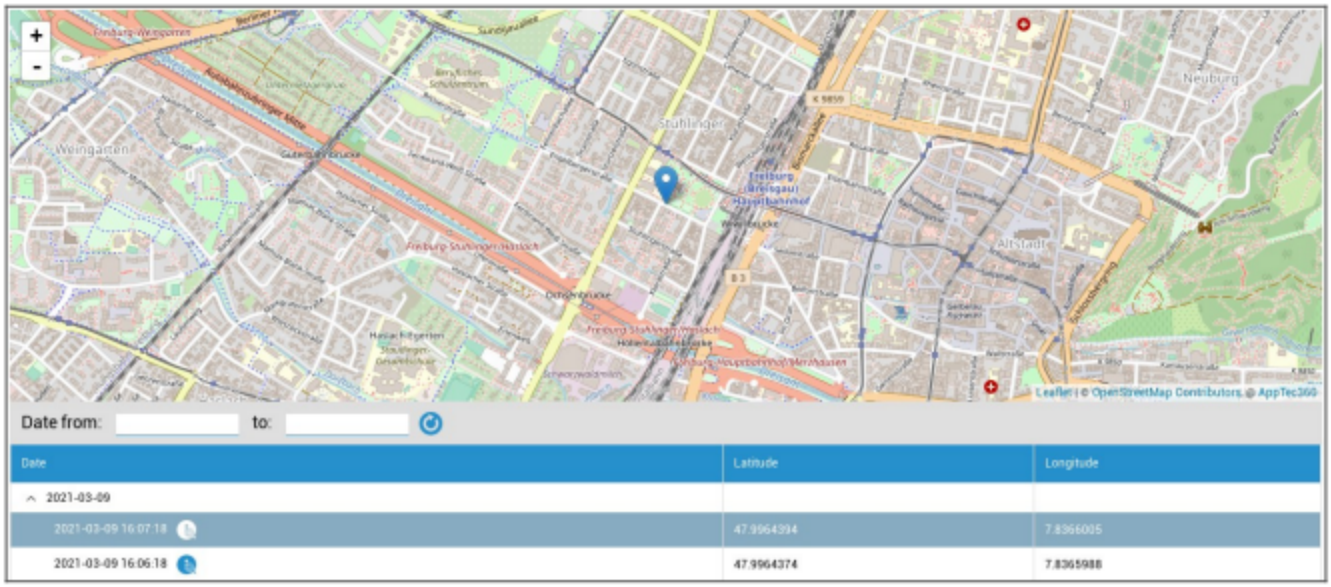
Bluetooth MAC	Adresa MAC Bluetooth

Riadenie bezpečnosti

Ochrana proti krádeži (len na úrovni zariadenia)

Informácie GPS (len na úrovni zariadenia)

Tu môžete určiť aktuálne/posledné umiestnenie zariadenia. Lokalizácia môže byť chránená jedným alebo dokonca dvoma heslami - pozri: Všeobecné nastavenia - Súkromie - Prístup k GPS



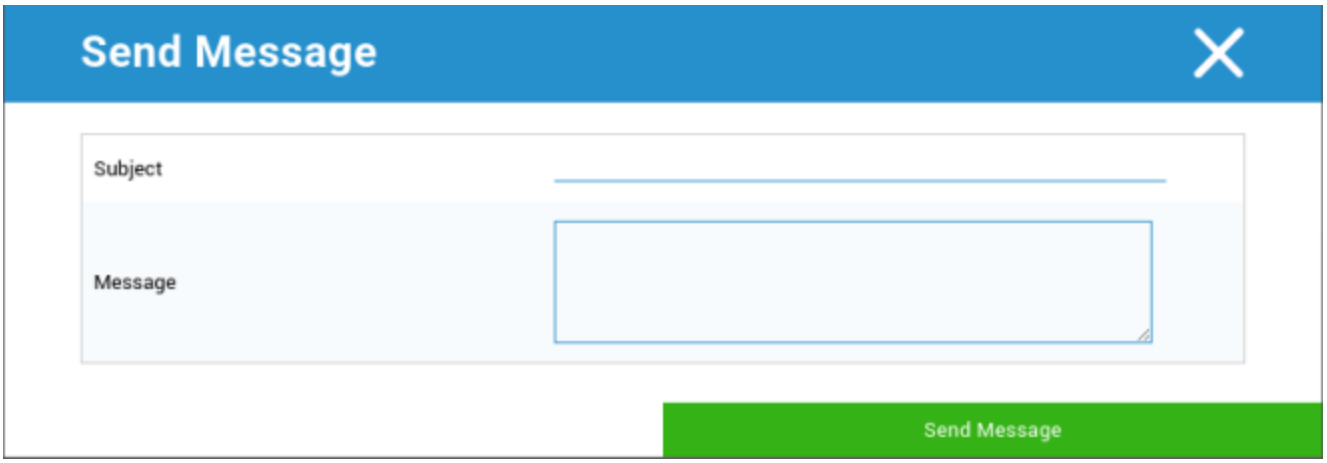
Vyčistiť a uzamknúť (len na úrovni zariadenia)

V časti "Vyčistiť a uzamknúť" môžete vykonať nasledujúce tri akcie:

Úplné utretie	Zariadenie sa obnoví do továrenského nastavenia (vymažú sa firemné aj osobné údaje).
Podnik Wipe	Zo zariadenia koncového používateľa sa odstránia len firemné údaje (všetky aplikácie, údaje atď., ktoré poskytla spoločnosť AppTec360)
Uzamknutie obrazovky	Ak je aktivovaný zámok obrazovky, stačí zariadenie odomknúť pomocou hesla zariadenia/PIN kódu.

Správa (len na úrovni zariadenia)

Môžete vyplniť predmet a správu a odoslať ju koncovému používateľskému zariadeniu. Táto správa sa zobrazí v aplikácii AppTec360 Client.



Konfigurácia zabezpečenia

Prístupový kód

V časti "Prístupový kód" môžete povoliť heslo zariadenia, pričom máte k dispozícii tieto možnosti nastavenia

Minimálna dĺžka hesla	stanovuje minimálny počet symbolov, ktoré musí heslo obsahovať
Kvalita hesla	Sila hesla Nešpecifikované = nešpecifikované Každé heslo je v poriadku = každé heslo je prijateľné aspoň číselné znaky = musí obsahovať aspoň číselné znaky aspoň komplex znakov = musí obsahovať aspoň špeciálne znaky aspoň alfanumerické znaky = musí obsahovať aspoň alfanumerické znaky aspoň abecedné znaky = musí obsahovať aspoň abecedné znaky
Maximálny čas blokovania nečinnosti	Maximálny časový limit obrazovky. Týmto sa konfiguruje iba maximálna hodnota, ktorú môže vybrať používateľ
Minimálny počet malých písmen v hesle	Minimálny počet malých písmen v hesle
Minimálny počet veľkých písmen v hesle	Minimálny počet veľkých písmen v hesle
Minimálny počet nepísmenových znakov požadovaných v hesle	Minimálny počet nepísmenových znakov požadovaných v hesle
Minimálne číselné znaky požadované v hesle	Minimálne číselné znaky požadované v hesle
Minimálne požadované symboly v hesle	Minimálne požadované symboly v hesle
Časový limit vypršania platnosti hesla	stanovuje, po uplynutí ktorého časového intervalu heslo vyprší a musí sa vydať nové heslo
Obmedzenie histórie hesiel	Počet predtým použitých hesiel, ktoré nie sú povolené
Maximálny počet neúspešných pokusov o zadanie hesla	stanovuje, ako často môže byť heslo zadané nesprávne, kým sa vykoná úplné vymazanie zariadenia

Šifrovanie

V tomto bode môžete šifrovať internú pamäť zariadenia, ako aj pamäť karty SD.

Vyžadovať šifrovanie úložiska	Ak je toto nastavenie aktivované, pamäť zariadenia bude šifrovaná, pokiaľ zariadenie túto funkciu podporuje. Po prvom zašifrovaní pamäte zariadenia ju už nie je možné odšifrovať. Podobne sa aj politika hesla automaticky prepne na 6 alfanumerických symbolov.
Vyžadovať šifrovanie karty SD	Toto nastavenie sa vzťahuje len na zariadenia Samsung! Ak je toto nastavenie aktivované, externá karta SD môže byť zašifrovaná a na zariadení koncového používateľa ju možno odšifrovať len manuálne. Podobne sa aj politika hesla automaticky prepne na 6 alfanumerických symbolov.

AntiVirus

Povolením AntiVirus sa do zariadení nainštaluje Ikarus. Upozorňujeme, že si to vyžaduje samostatnú licenciu, ktorú môžete zadať vo Všeobecných nastaveniach → Správa aplikácií → Aplikácie tretích strán.

Automatické skenovanie	Definuje, či Ikarus skenuje automaticky a ako často toto skenovanie vykonáva. Ak povolíte možnosť "Úplné automatické skenovanie", vykoná sa úplné skenovanie. V opačnom prípade sa vykoná rýchle skenovanie
Automatické aktualizácie	Povolenie automatickej aktualizácie vírusovej databázy a nastavenie frekvencie aktualizácie.
Ochrana aplikácií	Okrem bežného skenovania, ktoré skenuje iba súbory, umožňuje aj skenovanie aplikácií.
Ochrana karty SD	Povolí ochranu karty SD. Bez tohto nastavenia je skenovanie obmedzené na lokálne úložisko.
Aktualizácia iba Wi-Fi	Obmedzenia aktualizácie na Wi-Fi

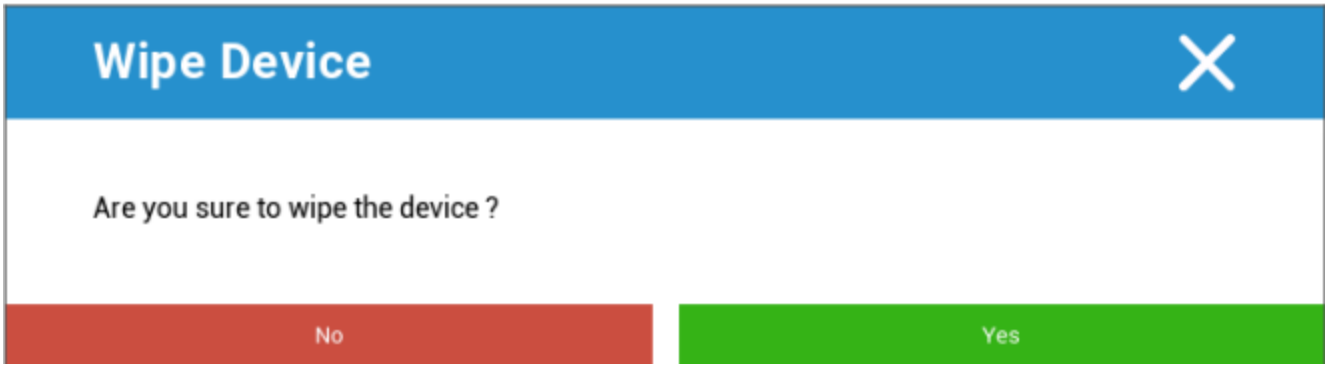
Koniec životnosti (len na úrovni zariadenia)

Vyčistiť (len na úrovni zariadenia)

V časti "Vymazať" môžete obnoviť výrobné nastavenia zariadenia. Tu sa odstránia firemné, ako aj súkromné údaje v zariadení koncového používateľa.

Po kliknutí na "Symbol mínus" by sa mala zobraziť nasledujúca správa

Vymazať aj kartu SD?	Vymaže sa aj pamäť karty SD



Pomocou možnosti "Áno" môžete vykonať vymazanie.

V časti "Wipe Report" sa môžu zobraziť tieto položky

Zotreté	História toho, kto vykonal utretie
Dátum	Dátum
Stav	Stav (napr. či bolo vymazanie vykonané úspešne)

Nastavenia obmedzenia

Obmedzenia

Tu je možné obmedziť a zablokovať rôzne veci.

Povolenie kamery	Povolenie používania kamery
Vynútiť automatickú synchronizáciu	Vzťahuje sa na rozhranie "Synchronizácia" Zapnuté = synchronizácia je trvalo aktivovaná Vypnuté = synchronizácia je trvalo deaktivovaná Výber používateľa = výber používateľa
Vynútiť Bluetooth	Zapnuté = Bluetooth je trvalo aktivované Vypnuté = Bluetooth je trvalo deaktivované Výber používateľa = výber používateľa
Force GPS	Zapnuté = GPS je trvalo aktivované Vypnuté = GPS je trvalo deaktivované Výber používateľa = výber používateľa
Vynútenie presnosti polohy Google	Zapnuté = trvalá lokalizácia na internete Vypnuté = trvalá deaktivácia lokalizácie internetu Výber používateľa = výber používateľa

Pre zariadenia Samsung s rozhraním KNOX 1.0 alebo vyšším sú k dispozícii nasledujúce možnosti nastavení.

Povolenie karty SD	Povolenie karty SD
Povolenie zápisu na kartu SD	Povolenie "zápisu" na kartu SD
Povolenie snímania obrazovky	Povolenie snímania obrazovky
Povoliť schránku	Povoliť schránku
Zálohovanie nastavení a údajov aplikácie v službe Google Cloud	Vypnuté = deaktivácia zálohovania Google Zapnuté = aktivácia zálohovania Google Výber používateľa = výber používateľa
Povolenie ladenia USB	Povolenie ladenia USB (používa sa napríklad na vytváranie denníkov zariadení (ADB))
Povoliť hlásenie o zrážke Google	Povolenie odosielania hlásení o havárii Google z aplikácií
Povolenie obnovenia továrenského nastavenia	Umožňuje používateľovi obnoviť výrobné nastavenia zariadenia
Povolenie aktualizácie OTA	Povolenie aktualizácií "Over-The-Air"
Povolenie ukladania do hostiteľského počítača USB	Ak je aktivovaná, je možné pripojiť pamäť USB vo forme HD alebo čítačky kariet SD.
Povolenie prehrávača médií USB (MTP,PTP)	Povolenie prehrávača médií USB (MTP,PTP)
Povoliť mikrofón	Zapnuté = povolenie mikrofónu pre aplikácie tretích strán Vypnuté = blokovanie mikrofónu pre aplikácie tretích strán Voľba používateľa = používatelia si môžu vybrať, či má aplikácia tretej strany prístup k mikrofónu.
Povolenie NFC (Near Field Communication)	Povoliť NFC
Povolenie neznámych zdrojov (APK Sideloading)	Ak je povolené vedľajšie načítanie aplikácií (súborov APK), je povolené. Po vypnutí tohto nastavenia ho musí používateľ povoliť ručne, keď opätovne povolíte inštaláciu súborov APK z neznámych zdrojov.
Povolenie vytvárania používateľov	Umožňuje vytváranie viacerých používateľov

Vlastník zariadenia AE

(Zariadenie musí byť v režime vlastníka zariadenia Android Enterprise) Odporúča sa vytvoriť zariadenia ako zariadenie "Android Enterprise" a nie ako zariadenie "Android".

Zabezpečenie	
Zakázať zdieľanie umiestnenia	Určuje, či je používateľovi zakázané zapnúť zdieľanie polohy.
Zakázať bezpečné spustenie systému	Určuje, či používateľ nesmie reštartovať zariadenie do núdzového režimu.
Zakázať resetovanie siete	Určuje, či je používateľovi zakázané resetovať sieťové nastavenia z Nastavení.
Zakázať obnovenie továrenských nastavení	Určuje, či je používateľovi zakázané resetovať zariadenie.
Povolenie ADB	Umožňuje pripojenie k počítaču prostredníctvom ADB
Zakázanie funkcie Keyguard	Vypnutie funkcie Keyguard
Informácie o uzamknutej obrazovke vlastníka zariadenia	Nastavenie informácií o vlastníkovi zariadenia, ktoré sa majú zobrazovať na uzamknutej obrazovke.
Presadzovanie súladu	Režim Výzva používateľovi - používateľ bude vyzvaný na vykonanie potrebných činností. Kontajner s uzamknutým režimom - skryje všetky aplikácie, kým nie sú splnené všetky požiadavky

Správa aplikácií	
Povolenie prepojenia aplikácií medzi profilmi	Umožňuje aplikáciám v nadradenom profile spracúvať webové odkazy zo spravovaného profilu.
Zakázať ovládanie aplikácií	Určuje, či je používateľovi zakázané upravovať aplikácie v Nastaveniach alebo spúšťacích programoch.
Zakázať inštaláciu aplikácií	Určuje, či je používateľovi zakázané inštalovať aplikácie.
Zakázať odinštalovanie aplikácií	Určuje, či je používateľovi zakázané odinštalovať aplikácie.
Zásady oprávnení počas behu	Určuje, ako sa budú spracovávať nové žiadosti o povolenie od aplikácií.
Povolenie neznámych zdrojov	Ak je táto funkcia povolená, používatelia môžu aplikácie načítavať zboku inštaláciou súboru .apk.

Pripojenie	
Zakázať konfiguráciu mobilnej siete	Určuje, či je používateľovi zakázané konfigurovať mobilné siete.
Zakázať konfiguráciu tetheringu	Určuje, či je používateľovi zakázané konfigurovať Tethering a prenosné hotspoty.
Zakázať konfiguráciu VPN	Určuje, či je používateľovi zakázané konfigurovať sieť VPN.
Zakázať konfiguráciu Wifi	Určuje, či je používateľovi zakázané meniť prístupové body WiFi.
Zakázanie odchádzajúceho lúča NFC	Určuje, či používateľ nesmie používať NFC na prenos údajov z aplikácií.
Konfigurácia uzamknutia WiFi	Toto nastavenie určuje, či majú byť konfigurácie WiFi vytvorené aplikáciou Vlastník zariadenia uzamknuté (t. j. či ich môže upravovať alebo odstraňovať iba aplikácia Vlastník zariadenia, nie však ani aplikácia Nastavenia).
Povolenie dátového roamingu	Aktivácia dátového roamingu

Bluetooth	
Zakázať pripojenie Bluetooth	Určuje, či je v zariadení zakázaný bluetooth. Vyžaduje systém Android 8.0
Zakázanie zdieľania cez Bluetooth	Určuje, či je v zariadení zakázané odchádzajúce zdieľanie cez bluetooth. Vyžaduje systém Android 8.0
Zakázať konfiguráciu Bluetooth	Určuje, či je používateľovi zakázané konfigurovať bluetooth.

Správa účtov	
Zakázať pridávanie spravovaného profilu	Určuje, či je používateľovi zakázané pridávať spravované profily. Vyžaduje Android 8.0
Zakázať pridávanie používateľov	Určuje, či je používateľovi zakázané pridávať nových používateľov.
Zakázať Odstrániť spravovaný profil	Určuje, či spravované profily tohto používateľa môžu byť odstránené inak ako jeho vlastníkom profilu. Vyžaduje Android 8.0
Zakázať úpravu účtu	Určuje, či je používateľovi zakázané pridávať a odstraňovať účty, pokiaľ ich program Authenticator nepridá programovo.

Telefonovanie	
Zakázať odchádzajúce hovory	Určuje, že používateľ nemá povolené uskutočňovať odchádzajúce telefónne hovory.
Zakázať SMS	Určuje, že používateľ nemá povolené odosielať alebo prijímať SMS správy.

Systém	
Zakázať vytváranie okien	Určuje, že okrem okien aplikácie sa nemajú vytvárať žiadne iné okná.
Zakázať nastaviť ikonu používateľa	Určuje, či používateľ nesmie zmeniť svoju ikonu.
Zakázať nastavenie tapety	Obmedzenie používateľa na zakázanie nastavenia tapety.
Zakázanie stavového riadka	Zakázanie stavového riadka blokuje oznámenia, rýchle nastavenia a ďalšie prekrytia obrazovky, ktoré umožňujú únik z jednorazového zariadenia.
Povolenie automatického času	Automaticky nastaví čas.
Povolenie automatického časového pásma	Automaticky nastaví časové pásmo.
Zostať zapnutý, keď je pripojený k sieti	Zariadenie zostane aktívne, kým je pripojené k zdroju napájania.

Úložisko	
Zakázať zakázanie overovania aplikácií	Určuje, či je používateľovi zakázané vypnúť overovanie aplikácie.

Zakázať pripojenie fyzických médií	Určuje, či je používateľovi zakázané pripájať fyzické externé médiá.
Povolenie služby zálohovania	Služba zálohovania spravuje všetky mechanizmy zálohovania a obnovy v zariadení. Nastavenie tejto hodnoty na false zabráni zálohovaniu alebo obnove údajov. Služba zálohovania je v predvolenom nastavení vypnutá. Vyžaduje systém Android 8.0
Povolenie veľkokapacitného úložiska USB	Povolí používanie veľkokapacitného úložiska USB.

Klávesnica	
Zakázať automatické vypĺňanie	Určuje, či používateľ nesmie používať služby automatického vypĺňania. Vyžaduje Android 8.0
Zakázať kopírovanie a vkladanie medzi profilmi	Určuje, či to, čo sa skopíruje do schránky tohto profilu, možno vložiť do súvisiacich profilov.

Zvuk	
Zakázať úpravu objemu	Určuje, či je používateľovi zakázané upravovať hlavnú hlasitosť.
Zakázať vypnutie mikrofónu	Určuje, či je používateľovi zakázané nastavovať hlasitosť mikrofónu.
Zariadenie na stlmenie zvuku	Zariadenie na stlmenie zvuku.

Zásady aktualizácie systému	
Ovládanie aktualizácií operačného systému	Ak zapnete túto možnosť, nastavíte správanie aktualizácie na automatické, okenné alebo odložené.

Kontajner BYOD

Android Enterprise

Android Enterprise

Povolenie systému Android Enterprise	Povolenie systému Android Enterprise (AE). AE je podporovaná od verzie Android 5.1 a vyššej.
Presadzovanie súladu	Režim Výzva používateľovi - používateľ bude vyzvaný na vykonanie potrebných činností. Kontajner s uzamknutým režimom - skryje všetky aplikácie, kým nie sú splnené všetky požiadavky
Zásady oprávnení počas behu	Výzva používateľovi na zadanie nových požiadaviek na povolenie Vždy udeľte nové žiadosti o nové povolenie Vždy zamietnuť nové žiadosti o povolenie Varovanie: Niektoré aplikácie majú problémy s rozpoznaním oprávnení, ak sú nastavené automaticky. Ak vždy udeľujete oprávnenia a stretávate sa s problémami s aplikáciami, ktoré tvrdia, že oprávnenia chýbajú, nastavte túto možnosť na "vyzvať používateľa" a znovu nainštalujte aplikáciu.
Povolenie odchádzajúcej schránky	Umožňuje kopírovanie a vkladanie zvnútra kontajnera do vonkajšej časti
Povolenie rozlíšenia ID volajúceho	Zobrazenie názvu prichádzajúceho hovoru na základe kontaktov v kontajneri
Povolenie rozlíšenia vyhľadávania kontaktov	Umožňuje vyhľadávať mená v kontajneri kontaktov pri uskutočňovaní hovorov
Povolenie zdieľania kontaktov cez Bluetooth	Umožňuje prístup ku kontaktu kontajnera v aute
Zakázanie odchádzajúceho lúča NFC	Zakázanie funkcie NFC pre kontajner
Povolenie neznámych zdrojov	Ak je táto funkcia povolená, používatelia môžu aplikácie načítavať zboku inštaláciou súboru .apk.

Povolenie ladenia USB	Ak je táto možnosť povolená, používatelia môžu zapnúť ladenie USB.
Zakázať úpravu účtu	Zakázanie vytvárania, odstraňovania a modifikácie účtov v kontajneri Majte na pamäti, že niektoré aplikácie potrebujú vytvoriť alebo upraviť kontá, aby fungovali podľa očakávania.

Výmena Gmail

Umožňuje konfigurovať službu Gmail v kontajneri. Upozorňujeme, že zapnutím tejto konfigurácie sa aplikácia automaticky nenainštaluje. Túto aplikáciu musíte ešte pridať ako povinnú aplikáciu.

E-mailová adresa	E-mailová adresa
Názov hostiteľa servera	Názov hostiteľa servera
Prihlasovacie meno	Prihlasovacie meno
Podpis	Podpis
Počet predchádzajúcich dní na synchronizáciu	Počet predchádzajúcich dní na synchronizáciu.
Identifikátor zariadenia	Identifikátor EAS. Ak to vaše prostredie nevyžaduje, nechajte túto položku prázdnu.
Používanie Secure Sockets Layer (SSL)	Povolí používanie protokolu SSL. Zakázanie tejto funkcie môže znížiť bezpečnosť
Prijať všetky certifikáty	Akceptuje všetky certifikáty. Zapnutie tejto funkcie môže znížiť bezpečnosť
Povolenie nespravovaných účtov	Umožňuje používateľovi pridať ďalšie účty
Certifikát klienta	Nahrajte klientsky certifikát, ak to váš server Exchange vyžaduje

Aplikácie systému AE

Tu môžete povoliť systémové aplikácie pre kontajner Android Enterprise. Majte na pamäti, že zadaná aplikácia musí byť v úložisku systému, inak sa nič nestane.

Prístupový kód kontajnera

Len pre systém Android 7.0 alebo vyšší

Umožňuje nastaviť špecifické požiadavky na heslo pre kontajner.

Minimálna dĺžka hesla	stanovuje minimálny počet symbolov, ktoré musí heslo obsahovať
Kvalita hesla	Sila hesla Nešpecifikované = nešpecifikované Každé heslo je v poriadku = každé heslo je prijateľné aspoň číselné znaky = musí obsahovať aspoň číselné znaky aspoň komplex znakov = musí obsahovať aspoň špeciálne znaky aspoň alfanumerické znaky = musí obsahovať aspoň alfanumerické znaky aspoň abecedné znaky = musí obsahovať aspoň abecedné znaky
Maximálny čas blokovania nečinnosti	Maximálny čas do uzamknutia kontajnera. Toto nastavuje iba maximálnu hodnotu, ktorú môže vybrať používateľ
Minimálny počet malých písmen v hesle	Minimálny počet malých písmen v hesle
Minimálny počet veľkých písmen v hesle	Minimálny počet veľkých písmen v hesle
Minimálny počet nepísmenových znakov požadovaných v hesle	Minimálny počet nepísmenových znakov požadovaných v hesle
Minimálne číselné znaky požadované v hesle	Minimálne číselné znaky požadované v hesle
Minimálne požadované symboly v hesle	Minimálne požadované symboly v hesle
Časový limit vypršania platnosti hesla	stanovuje, po uplynutí ktorého časového intervalu heslo vyprší a musí sa vydať nové heslo
Obmedzenie histórie hesiel	Počet predtým použitých hesiel, ktoré nie sú povolené
Maximálny počet neúspešných pokusov o zadanie hesla	Určuje, ako často môže byť heslo zadané nesprávne, než sa kontajner vymaže.

Samsung KNOX

Aktivácia

Tu môžete povoliť kontajner Samsung KNOX. Upozorňujeme, že táto funkcia už nie je podporovaná spoločnosťou Samsung v systéme Android 10 alebo novšom. Používanie kontajnera Android

Enterprise Container v systéme Android 10 alebo vyššom

Prístupový kód Knox

Stanovenie usmernení týkajúcich sa nastavení hesla zariadenia

Minimálna dĺžka hesla	stanovuje, koľko symbolov musí heslo obsahovať
Kvalita hesla	Sila hesla Každé heslo je v poriadku = Každé heslo je v poriadku Najmenej číselných znakov = musí byť prítomných najmenej číselných znakov Aspoň komplex znakov = musí byť prítomný minimálny počet špeciálnych znakov Najmenej alfanumerických znakov = musí obsahovať minimálne alfanumerické znaky Aspoň abecedné znaky = musí byť prítomných minimálne abecedných znakov
Minimálny počet požadovaných komplexných znakov	Musia byť prítomné minimálne zložené znaky
Maximálny čas nečinnosti	Maximálny časový limit nečinnosti používateľa pred zablokovaním klávesnice
Povolenie overovania odtlačkom prsta	Povolenie overovania odtlačkov prstov
Povolenie overovania pomocou dúhovky	Povolenie overovania pomocou rozpoznávania dúhovky
Maximálny vek hesla	určuje, po akom čase heslo vyprší a musí byť vydané nové heslo.
História uložených hesiel	Počet bývalých hesiel, ktoré nie sú povolené
Maximálny počet neúspešných pokusov o zadanie hesla	stanovuje, ako často môže byť heslo zadané nesprávne, než dôjde k úplnému vymazaniu zariadenia.

Knox Security

Obmedzenie špecifických funkcií zariadenia

Povolenie kamery	Povolenie používania fotoaparátu
Povolenie obchodu s aplikáciami Samsung KNOX	Povolenie používania obchodu s aplikáciami Samsung KNOX

Povolenie služieb Google Play	Povolenie služieb Google Play
Povoliť prehliadač	Povolenie používania pôvodného prehliadača
Povolenie snímok obrazovky	Umožniť vytváranie snímok obrazovky
Povoliť import kontaktov	Ak je aktivovaná, je povolený prístup ku kontaktom zariadenia z kontajnera KNOX
Povoliť export kontaktov	Ak je aktivovaná, je povolený prístup ku kontaktom KNOX zo zariadenia
Povoliť import kalendára	Ak je aktivovaná, je povolený prístup ku kalendáru zariadenia z kontajnera KNOX
Povolenie exportu kalendára	Ak je aktivovaná, je povolený prístup do kalendára KNOX zo zariadenia
Povolenie klávesnice bez zabezpečenia	Povolenie používania nezabezpečenej klávesnice
Povolenie importu súborov	Povolenie importu súborov do kontajnera KNOX
Povolenie exportu súborov	Povolenie exportu súborov z kontajnera KNOX

Výmenník Knox Exchange

Tu môžete nakonfigurovať profil Exchange pre kontajner KNOX

E-mailová adresa	Poskytnutá e-mailová adresa používateľa Všimnite si "zástupné symboly", ktoré môžete použiť na prácu s povereniami a nevykonávate zmeny ručne na každom zariadení. Kliknutím na **Zobraziť zástupné symboly** si ich môžete zobraziť
Názov hostiteľa servera	Adresa servera vašich serverov Exchange
Prihlasovacie meno	Prihlasovacie meno pre príslušné zariadenie koncového používateľa, tu si prosím všimnite aj "zástupné znaky".
Doména	Adresa domény
Heslo (len na úrovni zariadenia)	Voliteľne môže byť jednotlivému zariadeniu poskytnuté heslo, ak zostane prázdne, používateľ bude vyzvaný, aby zadal svoje heslo Exchange.
Počet predchádzajúcich dní na synchronizáciu	Počet dní, ktoré určujú, kedy sa e-maily synchronizujú späť
Podpis	Môže byť pripojený podpis
Predvolený účet	stanovuje, že toto e-mailové konto je štandardné konto
Používanie Secure Sockets Layer (SSL)	Použitie pripojenia SSL
Používanie protokolu TLS (Transport Layer Security)	Použitie pripojenia TLS
Prijať všetky certifikáty	Všetky certifikáty sú akceptované. Túto možnosť vyberte, ak váš server Exchange používa certifikát s vlastným podpisom.

Knox eMail

E-mailová adresa	Poskytnutá e-mailová adresa používateľa Všimnite si "zástupné symboly", ktoré môžete použiť na prácu s povereniami a nevykonávate zmeny ručne na každom zariadení. Kliknutím na **Zobraziť zástupné symboly** si ich môžete zobraziť
Protokol prichádzajúceho servera	Protokol prichádzajúceho servera IMAP alebo POP
Adresa prichádzajúceho servera	Adresa prichádzajúceho servera
Port prichádzajúceho servera	Port prichádzajúceho servera
Prihlasovacie meno/meno používateľa prichádzajúceho servera	Prihlasovacie meno/meno používateľa prichádzajúceho servera
Heslo prichádzajúceho servera	Heslo prichádzajúceho servera
Prichádzajúci server používa protokol SSL	Prichádzajúci server používa protokol SSL
Prichádzajúci server používa TLS	Prichádzajúci server používa TLS
Prichádzajúci server akceptuje všetky certifikáty	Prichádzajúci server akceptuje všetky typy certifikátov
Protokol odchádzajúceho servera	Protokol odchádzajúceho servera SMTP
Port odchádzajúceho servera	Port odchádzajúceho servera
Odchádzajúci server používa ďalšie poverenia	Ďalšie poverenia pre odchádzajúci server. Ak je táto možnosť nastavená na "off", použijú sa nastavenia prichádzajúceho servera
Prihlasovacie meno/meno používateľa odchádzajúceho servera	Prihlasovacie meno/meno používateľa odchádzajúceho servera
Heslo odchádzajúceho servera	Heslo odchádzajúceho servera
Odchádzajúci server používa protokol SSL	Odchádzajúci server používa protokol SSL
Odchádzajúci server používa TLS	Odchádzajúci server používa TLS
Odchádzajúci server akceptuje všetky certifikáty	Odchádzajúci server akceptuje všetky typy certifikátov

Podpis	Tu je možné pripojiť podpis
Upozorniť používateľa na prijatie novej elektronickej pošty	Upozorniť používateľa na prijatie novej elektronickej pošty

Aplikácie Knox

Tu vytvorte aplikácie, ktoré chcete distribuovať do zariadení koncových používateľov. Tie budú potom k dispozícii v kontajneri KNOX. Ak chcete pridať aplikáciu, postupujte ako v ponuke Povinné aplikácie

Názov aplikácie	Názov aplikácie
Povinné od	Bod v čase, kedy bola aplikácia pridaná
Zdroj	Zdroj aplikácie (Obchod Play | In-House)

Kliknutím na symbol môžete príslušnú aplikáciu opäť odstrániť.

Správa pripojenia

Wifi

Pre toto nastavenie vykonajte predbežnú konfiguráciu koncových používateľských zariadení pre prístup k interným prístupovým bodom

Identifikátor súboru služieb (SSID)	SSID pre sieť, ktorá sa má pripojiť
Skrytá sieť	Aktivácia v prípade, že prístupový bod nevysiela identifikátor SSID
Typ zabezpečenia	Stanovenie typu zabezpečenia prístupového bodu

Typ zabezpečenia

WEP

Heslo	Heslo pre AP

WPA/WPA2

Heslo	Heslo pre AP

802.1x EAP

Metóda EAP	

PWD	Identita	Identita
	Heslo	Heslo

PEAP	Fáza 2 autentifikačného protokolu	žiadne	Žiadny dodatočný protokol
		MSCHAPV2	Protokol MSCHAPV2
		GTC	Protokol GTC
	Certifikát CA	Certifikát CA	
	Identita	Identita	
	Anonymná identita	Anonymná identita	
	Heslo	Heslo	

Metóda EAP	

TTLS	Fáza 2 autentifikačného protokolu	žiadne	Žiadny dodatočný protokol
		PAP	Protokol PAP
		MSCHAP	Protokol MSCHAP
		MSCHAPV2	Protokol MSCHAPV2
		GTC	Protokol GTC
	Certifikát CA	Certifikát CA	
	Identita	Identita	
	Anonymná identita	Anonymná identita	
	Heslo	Heslo	

TLS	Certifikát CA	Certifikát CA
	Identita	Identita
	Heslo	Heslo

VPN

Typ pripojenia	**Vytvorenie typu pripojenia VPN**

Ak ako typ VPN vyberiete možnosť "Per-App VPN", zmení sa zoznam dostupných klientov VPN. Funkcia Per-App VPN obmedzuje sieť VPN na určité aplikácie a automaticky spúšťa pripojenie VPN, ak je spustená určitá aplikácia.

Klient VPN AppTec360	Používa klienta AppTec360 VPN v kombinácii s univerzálnou bránou
Názov pripojenia	Názov pripojenia VPN
Konfigurácia brány	Vyberte konfiguráciu VPN univerzálnej brány
Vždy zapnutá sieť VPN	Vynúti VPN, aby bola vždy aktívna, takže celá prevádzka prechádza cez VPN.
Povolenie funkcie Native Lockdown	Zablokuje všetky siete, keď zariadenie nie je pripojené k sieti VPN. Používajte to opatrne, pretože to môže spôsobiť úplnú stratu spojenia, ak nie je správne nakonfigurované. Len pre Android Enterprise na systéme Android 7 alebo vyššom
Povolenie uzamknutia AppTec360	Zablokuje používanie všetkých aplikácií, kým sa nespustí pripojenie VPN

Cisco AnyConnect	
Názov pripojenia	Názov pripojenia VPN
Server	Adresa servera
Režim certifikátu	Disabled = deaktivovaný Automatic = automatický

L2TP (iba KNOX)	K dispozícii len v zariadeniach Samsung
Názov pripojenia	Názov pripojenia
Server	Adresa servera
Povolenie funkcie L2TP Secret	
Vyhľadávanie domén DNS	Vyhľadávanie domén DNS

Typ pripojenia	**Vytvorenie typu pripojenia VPN**

PPTP (len pre systém KNOX)	K dispozícii len v zariadeniach Samsung
Názov pripojenia	Názov pripojenia VPN
Server	Adresa servera
Povolenie šifrovania	Povolenie šifrovania
Vyhľadávanie domén DNS	Vyhľadávanie domén DNS

L2TP / IPSec PSK (iba KNOX)	K dispozícii len v zariadeniach Samsung
Názov pripojenia	Názov pripojenia VPN
Server	Adresa servera
Predsdieľaný kľúč IPSec	Predbežne zdieľaný kľúč na overovanie
Povolenie funkcie L2TP Secret	
Tajomstvo L2TP	
Vyhľadávanie domén DNS	Vyhľadávanie domén DNS

IPSec XAuth PSK (iba KNOX)	K dispozícii len v zariadeniach Samsung
Názov pripojenia	Názov pripojenia VPN
Server	Adresa servera
Identifikátor IPSec	Meno používateľa pre pripojenie
Predsdieľaný kľúč IPSec	Heslo pre pripojenie
Vyhľadávanie domén DNS	Vyhľadávanie domén DNS

OpenVPN	
Názov pripojenia	Názov pripojenia

Profil OpenVPN	Tu sa skopíruje obsah súboru .ovpn
Aplikácia OpenVPN	Na používanie siete OpenVPN existujú dve rôzne aplikácie Odporúčame aplikáciu "OpenVPN pre Android". Alternatívne však môžete použiť aplikáciu "OpenVPN Connect".

Obmedzenia

Tu môžete nastaviť obmedzenia týkajúce sa správy pripojenia.

Povolenie dátového roamingu	Povolenie mobilných dát počas roamingu
Vynútenie dátového roamingu	Ak je aktivovaný, roaming pre mobilné dáta je trvalo aktivovaný (neodporúča sa!) Toto nastavenie prepíše nastavenie "Povoliť dátový roaming"!
Nasledujúce nastavenia sú k dispozícii len v systéme Samsung KNOX 2.0 alebo vyššom	
Povoľte len tiesňové volania	Povoľte len tiesňové volania
Povolenie Wi-Fi	Povolenie Wi-Fi
Minimálna úroveň zabezpečenia siete WiFi	Minimálna úroveň zabezpečenia siete WiFi Otvorené = všetky typy WiFi sú povolené
Zakázať používateľovi pridávať siete WiFi	Používateľ nemôže sám pridať sieť WiFi Toto nastavenie je možné len vtedy, ak bol profil WiFi definovaný v časti "Správa pripojenia".
Povolenie SMS a MMS	Všetky = všetka prevádzka SMS a MMS je povolená Len prichádzajúce SMS = povolené sú len prichádzajúce SMS správy Len odchádzajúce SMS = povolené sú len odchádzajúce SMS správy Žiadne = nie je povolená žiadna prevádzka SMS / MMS
Povolenie synchronizácie počas roamingu	Povolenie synchronizácie počas roamingu Zapnuté = aktivované Vypnuté = deaktivované Voľba používateľa = voľba používateľa
Povolenie hlasového roamingu	Povolenie hlasového roamingu Zapnuté = aktivované Vypnuté = deaktivované Voľba používateľa = voľba používateľa
Použitie systémového servera http Proxy	Použitie proxy servera HTTP, ktorý je k dispozícii v nastaveniach systému, závisí od pripojenej siete (WiFi alebo APN).

APN

Nasledujúce nastavenia sú k dispozícii len v systéme Samsung SAFE 2.0 alebo vyššom!

Zobrazovaný názov APN	Zobrazovaný názov APN	
Názov prístupového bodu	Názov APN	
Protokol odchádzajúceho servera	Nie je nastavené	
	Žiadne	
	PAP	Protokol PAP
	CHAP	Protokol CHAP
	PAP alebo CHAP	Protokol PAP alebo CHAP
MCC - kód mobilnej krajiny	Tu sa zadáva MCC, ak sa má použiť MCC vloženej karty SIM, nechajte toto pole prázdne.	
MNC - Kód mobilnej siete	Tu sa zadáva MNC, ak sa má použiť MCC vloženej karty SIM, nechajte toto pole prázdne.	
Adresa servera	Adresa servera	
Číslo portu servera	Číslo portu servera	
Adresa servera proxy	Adresa servera proxy	
Adresa servera MMS	Adresa servera MMS, pre štandardné ponechajte prázdne	
Číslo portu MMS	Číslo portu MMS	
Adresa proxy servera MMS	Adresa proxy servera MMS	
Meno používateľa	Meno používateľa	
Heslo	Heslo	
Typ prístupového bodu	Povolené typy sú: "default", "mms", "supl" Ak toto pole zostane prázdne, použije sa "default,supl,mms".	
Uprednostňované APN	Uprednostňuje sa APN	

Bluetooth

Tu je možné vykonať rôzne nastavenia Bluetooth.

Nasledujúce nastavenia sú k dispozícii len v systéme Samsung KNOX 1.0 alebo vyššom!

Povolenie zisťovania zariadenia cez Bluetooth	Povolenie zisťovania zariadenia prostredníctvom Bluetooth
Povolenie párovania cez Bluetooth	Povolenie párovania cez Bluetooth
Povolenie zariadení s náhlavnou súpravou Bluetooth	Povolenie zariadení s náhlavnou súpravou Bluetooth
Povolenie zariadení Bluetooth Hands-free	Povolenie zariadení Bluetooth Hands-free
Povolenie zariadení Bluetooth A2DP	Povolenie streamovania zvuku cez Bluetooth A2DP medzi zariadeniami
Povolenie odchádzajúcich hovorov	Povolenie odchádzajúcich hovorov cezBT
Povolenie prenosu údajov cez Bluetooth	Povolenie prenosu údajov cez Bluetooth
Povolenie tetheringu Bluetooth	Umožňuje používať zariadenie ako modem (internetové pripojenie Bluetooth)
Povolenie pripojenia k počítaču cez Bluetooth	Povolenie pripojenia k počítaču cez Bluetooth

Správa PIM

Výmena

K dispozícii len pre Samsung KNOX 1.0 alebo vyššiu verziu!

E-mailová adresa	Poskytnutá e-mailová adresa používateľa Všimnite si "zástupné symboly", ktoré môžete použiť na prácu s povereniami a nevykonávate zmeny ručne na každom zariadení. Kliknutím na **Zobraziť zástupné symboly** si ich môžete zobraziť
Názov hostiteľa servera	Adresa servera vašich serverov Exchange
Prihlasovacie meno	Prihlasovacie meno pre príslušné zariadenie koncového používateľa, všimnite si tiež "Placeholders here".
Doména	Adresa domény
Heslo (len na úrovni zariadenia)	Voliteľne možno jednotlivému zariadeniu poskytnúť heslo, ak zostane prázdne, používateľ bude vyzvaný, aby zadal svoje heslo Exchange.
Počet predchádzajúcich dní na synchronizáciu	Počet dní, ktoré určujú, kedy sa e-maily synchronizujú späť
Podpis	Môžete pripojiť podpis (Tip: Niektoré zariadenia vyžadujú formátovanie podpisu v HTML).
Predvolený účet	stanovuje, že toto poštové konto je štandardné konto
Používanie Secure Sockets Layer (SSL)	Použitie pripojenia SSL
Používanie protokolu TLS (Transport Layer Security)	Použitie pripojenia TLS
Prijať všetky certifikáty	Všetky certifikáty sú akceptované. Túto možnosť vyberte, ak váš server Exchange používa certifikát s vlastným podpisom.

E-mail

Tu môžete rozdeliť účty IMAP a POP na príslušné zariadenia koncových používateľov.

Nasledujúce nastavenia sú k dispozícii len v systéme Samsung KNOX 1.0 alebo vyššom!		
E-mailová adresa	Poskytnutá e-mailová adresa používateľa Všimnite si "zástupné symboly", ktoré môžete použiť na prácu s povereniami a nevykonávate zmeny ručne na každom zariadení. Kliknutím na **Zobraziť zástupné symboly** si ich môžete zobraziť	
Protokol prichádzajúceho servera	Protokol prichádzajúceho servera	IMAP oder POP
Adresa prichádzajúceho servera	Adresa prichádzajúceho servera	
Port prichádzajúceho servera	Port prichádzajúceho servera	
Prihlasovacie meno/meno používateľa prichádzajúceho servera	Prihlasovacie meno/meno používateľa prichádzajúceho servera	
Heslo prichádzajúceho servera (iba na úrovni zariadenia)	Heslo prichádzajúceho servera (iba na úrovni zariadenia)	
Prichádzajúci server používa protokol SSL	Prichádzajúci server používa protokol SSL	
Prichádzajúci server používa TLS	Prichádzajúci server používa TLS	
Prichádzajúci server akceptuje všetky certifikáty	Prichádzajúci server akceptuje všetky typy certifikátov	
Protokol odchádzajúceho servera	Protokol odchádzajúceho servera	SMTP
Port odchádzajúceho servera	Port odchádzajúceho servera	
Odchádzajúci server používa ďalšie poverenia	Ďalšie poverenia pre odchádzajúci server. Ak je táto možnosť nastavená na "off", použijú sa nastavenia prichádzajúceho servera	
Prihlasovacie meno/meno používateľa odchádzajúceho servera	Prihlasovacie meno/meno používateľa odchádzajúceho servera	
Heslo odchádzajúceho servera (iba na úrovni zariadenia)	Heslo odchádzajúceho servera	
Odchádzajúci server používa protokol SSL	Odchádzajúci server používa protokol SSL	
Odchádzajúci server používa TLS	Odchádzajúci server používa TLS	

Odchádzajúci server akceptuje všetky certifikáty	Odchádzajúci server akceptuje všetky typy certifikátov
Podpis	Tu môžete pripojiť podpis (Tip: niektoré zariadenia vyžadujú formátovanie podpisu v HTML).
Upozorniť používateľa na prijatie novej elektronickej pošty	Upozorní používateľa na prijatie nového e-mailu

AE Gmail Exchange

Informácie: Táto konfigurácia sa použije pre aplikáciu Gmail. Preto musíte schváliť a nainštalovať aplikáciu Gmail.

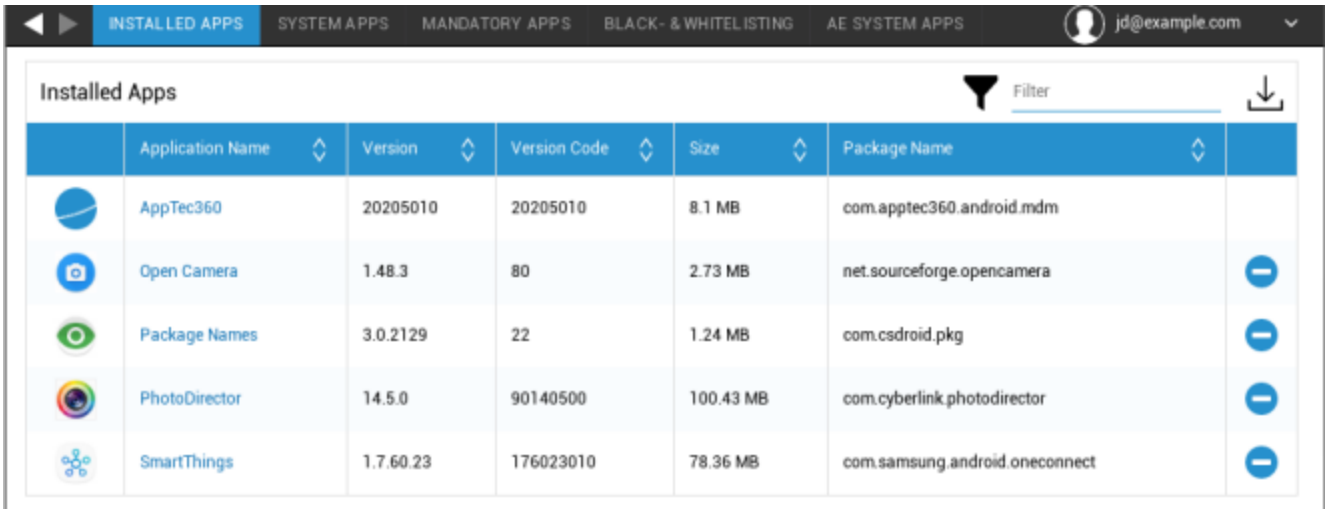
E-mailová adresa	Poskytnutá e-mailová adresa používateľa Všimnite si "zástupné symboly", ktoré môžete použiť na prácu s povereniami a nevykonávate zmeny ručne na každom zariadení. Kliknutím na Zobraziť zástupné symboly si ich môžete zobraziť
Názov hostiteľa servera	Adresa servera vašich serverov Exchange
Prihlasovacie meno	Prihlasovacie meno pre príslušné zariadenie koncového používateľa, všimnite si tiež "Placeholders here".
Podpis	Môžete pripojiť podpis (Tip: Niektoré zariadenia vyžadujú formátovanie podpisu v HTML).
Počet predchádzajúcich dní na synchronizáciu	Počet dní, ktoré určujú, kedy sa e-maily synchronizujú späť
Identifikátor zariadenia	Identifikátor EAS. Ak to vaše prostredie nevyžaduje, nechajte túto položku prázdnu.
Používanie Secure Sockets Layer (SSL)	Použitie pripojenia SSL
Prijať všetky certifikáty	Všetky certifikáty sú akceptované. Túto možnosť vyberte, ak váš server Exchange používa certifikát s vlastným podpisom.
Povolenie nespravovaných účtov	Umožňuje používateľovi pridať ďalšie účty
Certifikát klienta	Nahrajte klientsky certifikát, ak to váš server Exchange vyžaduje

Správa aplikácií

Správca podnikových aplikácií

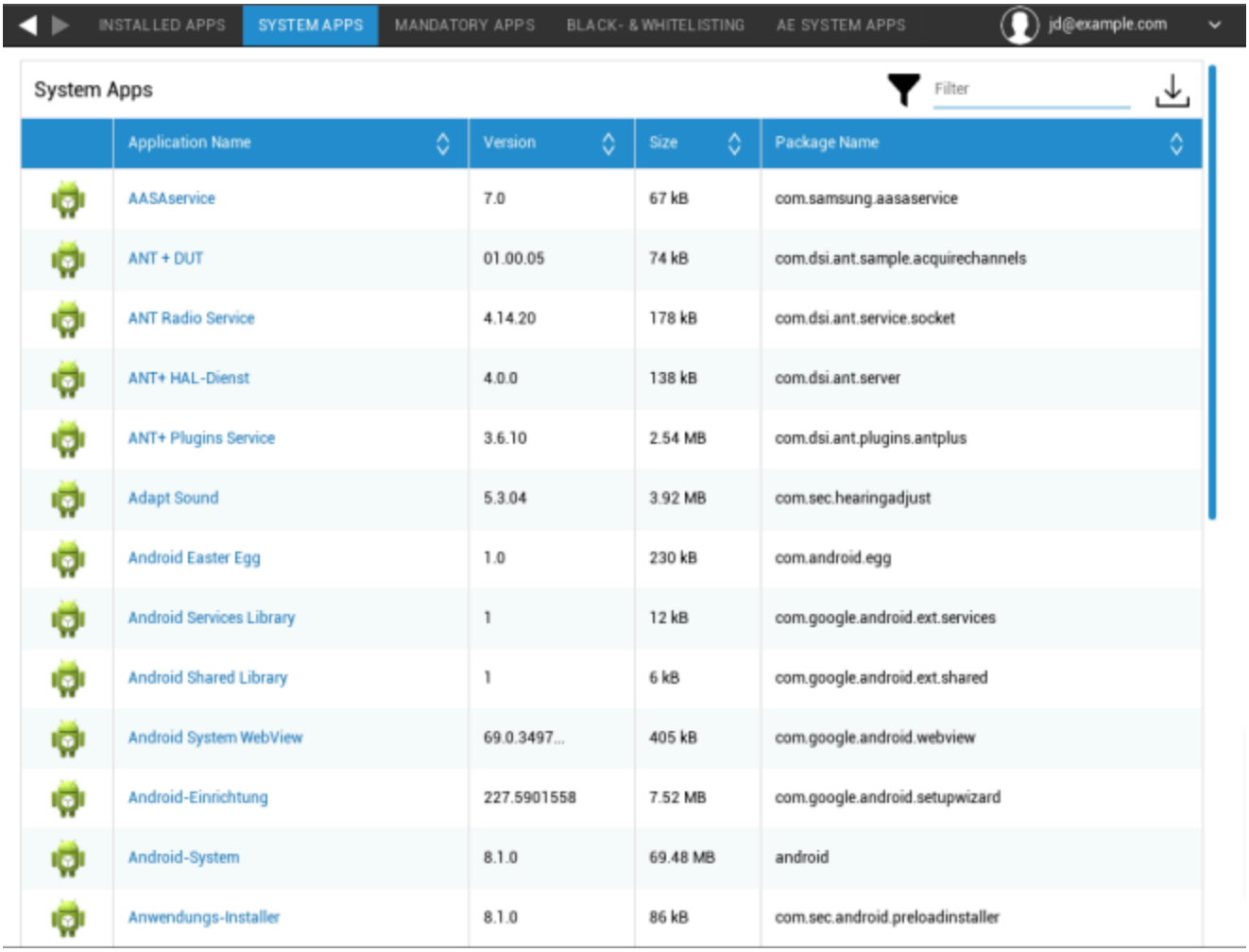
Nainštalované aplikácie (len na úrovni zariadenia)

Tu sa zobrazia všetky aplikácie, ktoré sú aktuálne nainštalované v zariadení koncového používateľa.


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

Systémové aplikácie (len na úrovni zariadenia)

V časti "Systémové aplikácie" sa zobrazí zoznam všetkých predinštalovaných systémových aplikácií s ich názvom a verziou.



Povinné aplikácie

V časti Povinné aplikácie môžete definovať, ktoré aplikácie musia byť v zariadení nainštalované. V závislosti od konfigurácie a zariadenia sa aplikácia nainštaluje automaticky alebo bude používateľ vyzvaný, aby ju nainštaloval.

Upozorňujeme, že na jednoduchú správu aplikácií sa odporúča používať Android Enterprise.

Scenáre sú uvedené nižšie:

Bežné aplikácie v Obchode Play

Inštalácie aplikácií v službe Playstore vždy vyžadujú interakciu používateľa. Okrem toho musí byť v zariadení nakonfigurované konto Google.

Inštalácia aplikácií InHouse

V zariadeniach Samsung sa tieto aplikácie nainštalujú potichu. Jedinou výnimkou je kontajner, pri ktorom musí používateľ potvrdiť inštaláciu.

V každom inom prípade musí používateľ potvrdiť inštaláciu aplikácie.

Aplikácie pre Android Enterprise Play Store

Tieto aplikácie sa vždy nainštalujú potichu, bez interakcie používateľa.

Ak chcete pridať povinnú aplikáciu, kliknite na "+" a vyberte požadovanú aplikáciu zo zoznamu. Upozorňujeme, že nie je možné inštalovať aplikácie z karty "Obchod Google Play", ak je zariadenie nakonfigurované so systémom Android Enterprise ako plne spravované alebo ako kontajner.

Ak používate systém Android Enterprise, vyberte aplikácie zo sekcie "Obchod AE Play". Ak chcete, aby tu boli aplikácie dostupné, potvrďte ich v obchode Google Enterprise Play tak, že prejdete do časti Všeobecné nastavenia → AE Play Store → Play Store Apps.

Pri odstránení povinnej aplikácie sa táto aplikácia odinštaluje aj zo zariadenia.

V zozname povinných aplikácií môžete kliknúť na názov aplikácie a prejsť na kartu "konfigurácia" a nakonfigurovať aplikáciu. To si vyžaduje použitie systému Android Enterprise a aplikácia to musí podporovať. Dostupné možnosti preto závisia od vybranej aplikácie.

Aplikácie systému AE

Tu môžete povoliť systémové aplikácie pre zariadenia Android Enterprise. Majte na pamäti, že zadaná aplikácia musí byť v úložisku systému, inak sa nič nestane. 296

Obmedzenia a nastavenia

Čierna a biela listina

Tu môžete definovať čiernu alebo bielu listinu. Všetky aplikácie na čiernej listine budú blokované. Všetky aplikácie, ktoré nie sú na bielom zozname, budú blokované. Prázdny čierny zoznam neblokuje nič, zatiaľ čo prázdny biely zoznam blokuje všetko*

**Všetky povinné aplikácie a aplikácie z podnikového obchodu s aplikáciami budú automaticky zaradené na biely zoznam. Nemusíte ich pridávať ručne*

Po kliknutí na "+" môžete buď vyhľadať aplikáciu, ktorú chcete pridať na čiernu alebo bielu listinu, alebo ručne zadať názov balíka.

Obmedzenia aplikácie Sys

V časti "Obmedzenia aplikácií systému" môžete okrem iného podľa potreby blokovať predinštalované aplikácie a služby.

Zakázať prehliadač	Zakázanie štandardného prehliadača
Zakázať kalendár	Zakázanie natívneho kalendára
Zakázať kalkulačku	Zakázať kalkulačku
Zakázanie prehliadača Chrome	Zakázanie prehliadača Chrome
Zakázať hodiny	Vypnutie hodín
Zakázať kontakty	Zakázať kontakty
Zakázanie služby Dialer	Zakázanie natívneho dialera
Zakázanie elektronickej pošty	Zakázať e-mail
Zakázať výmenu	Zakázanie účtov Exchange
Zakázanie služby Facebook	Zakázanie aplikácie Facebook
Zakázať galériu	Zakázanie natívnej aplikácie galérie
Zakázanie služby Gmail	Zakázanie služby Gmail
Zakázanie služby Google Books	Zakázanie služby Google Books
Zakázanie služby Google Play Kiosk	Zakázanie služby Google Play Kiosk
Zakázanie služby Mapy Google	Zakázanie služby Mapy Google
Zakázanie služby Google Music	Zakázanie služby Google Music
Zakázanie služby Google Movies	Zakázanie služby Google Movies
Zakázanie obchodu Google Play	Zakázanie obchodu Google Play (verejný obchod App Store)
Zakázanie služby Google Plus	Zakázanie služby Google Plus
Zakázanie vyhľadávania Google	Zakázanie vyhľadávania Google
Zakázanie služby Google Talk / Google Hangouts	Zakázanie služby Google Talk / Google Hangouts
Zakázanie prehrávača hudby	Zakázanie natívneho prehrávača hudby
Zakázať nastavenia	Zakázanie nastavení zariadenia
Zakázanie súpravy Sim Toolkit	Zakázanie služieb Sim Toolkit
Zakázať SMS / MMS	Zakázať SMS / MMS
Zakázanie služby Street View	Zakázanie služieb Street View
Zakázať službu Youtube	Zakázať službu Youtube

Aplikácie Samsung

V časti "Samsung Apps" môžete definovať ďalšie nastavenia a/alebo obmedzenia pre zariadenia Samsung.

Zakázanie služby AllShare Play / Samsung Link	Zakázanie služby AllShare Play / Samsung Link
Zakázanie služby ChatON	Zakázanie služby ChatON
Zakázanie herného centra	Zakázanie herného centra
Zakázanie skupinovej hry	Zakázanie skupinovej hry
Zakázať pomoc	Zakázanie služby Samsung Help
Zakázanie funkcie KNOX	Zakázanie kontajnera Samsung KNOX
Zakázať Memo	Zakázanie hlasových poznámok
Zakázať moje súbory	Zakázať moje súbory
Zakázanie optickej čítačky	Zakázanie optickej čítačky
Zakázanie služby Polaris Office	Zakázanie služby Polaris Office
Zakázanie rozbočovača Readers Hub / Samsung Books	Zakázanie rozbočovača Readers Hub / Samsung Books
Zakázanie funkcie S Memo	Zakázanie aplikácie Samsung Memo
Zakázanie prekladača S	Zakázanie aplikácie Samsung Translator
Zakázanie funkcie S Voice	Zakázanie hlasového asistenta S
Zakázanie aplikácií Samsung	Zakázanie obchodu Samsung App Store
Zakázanie rozbočovača Samsung Hub	Zakázanie obchodov Samsung Entertainment Stores
Zakázanie prehrávača videa	Zakázanie prehrávača videa
Zakázanie hlasového záznamníka	Zakázanie hlasového záznamníka
Zakázanie služby WatchON	Zakázať funkciu WatchON (simuluje diaľkové ovládanie)

Aplikácie Huawei

V časti "Huawei Apps" môžete definovať ďalšie nastavenia a/alebo obmedzenia zariadenia Huawei.

Zakázanie služby DLNA	Zakázanie služby DLNA
Zakázanie inštalátora aplikácií	Zakázanie inštalátora aplikácií
Zakázanie správcu súborov	Zakázanie správcu súborov
Zakázanie Správcu zálohovania	Zakázanie Správcu zálohovania
Zakázanie aktualizátora systému	Zakázanie aktualizátora systému
Zakázať skrinku s nástrojmi	Zakázať skrinku s nástrojmi
Zakázať počasie	Zakázať počasie
Zakázanie rádia FM	Zakázanie rádia FM

Nastavenia správy aplikácií

Tu môžete definovať správanie aktualizácie aplikácií InHouse Apps.

Frekvencia kontroly aktualizácií definuje, ako často aplikácia AppTec360 vyhľadáva aktualizácie pre aplikácie InHouse. Po zistení novej verzie sa táto stiahne a nainštaluje.

Prahová hodnota Wi-Fi definuje, či sa má sťahovanie obmedziť na pripojenie Wi-Fi, ak je aplikácia väčšia ako nakonfigurovaná prahová hodnota. Ak je menšia alebo prahovú hodnotu nedefinujete, aplikácia sa bude sťahovať v sieti Wi-Fi aj v mobilnej sieti.

Obchod s podnikovými aplikáciami

Upozorňujeme, že aplikácie pridané sem (Enterprise App Store) NEZABEZPEČIA ich automatickú inštaláciu do zariadenia (zariadení). Používateľ musí otvoriť Enterprise App Store v zariadení a nainštalovať aplikáciu manuálne.

Ak chcete do zariadenia automaticky nainštalovať aplikácie, prejdite do časti "Správa aplikácií" → "Správca podnikových aplikácií" → "Povinné aplikácie" a pridajte tam požadované aplikácie.

V tomto bode môžete používateľom distribuovať voliteľné aplikácie.

Obchod Playstore

Kliknutím na "+" pridáte aplikáciu do obchodu Play. Ak používate systém Android Enterprise, prejdite na "App Management Enterprise Play Store". Upozorňujeme tiež, že na inštaláciu tu definovaných aplikácií musí byť na → zariadení nakonfigurované konto Google.

Vnútorná stránka

V bode "In-House" môžete nahrať a distribuovať interne vyvinuté aplikácie.

Kliknutím na "+" pridáte aplikáciu InHouse do podnikového obchodu s aplikáciami, ktorú si potom môže používateľ nainštalovať. V tomto dialógu môžete tiež nahrať novú aplikáciu InHouse.

Obchod Play pre podniky

Upozorňujeme, že pridanie aplikácií sem (do obchodu Play) NEZABEZPEČÍ ich automatickú inštaláciu do zariadenia (zariadení). Používateľ musí otvoriť Obchod Play v zariadení a nainštalovať aplikáciu manuálne.

Ak chcete do zariadenia automaticky nainštalovať aplikácie, prejdite do časti "Správa aplikácií" → "Správca podnikových aplikácií" → "Povinné aplikácie" a pridajte tam požadované aplikácie.

V tomto bode môžete používateľom distribuovať voliteľné aplikácie.

Tu môžete pridať aplikácie do obchodu Android Enterprise Playstore. Upozorňujeme, že Aplikácie musíte schváliť v časti Všeobecné nastavenia → Obchod AE Play → Obchod Play Apps. Tieto Aplikácie budú pridané do bežného obchodu Google Play.

Tiež si uvedomte, že najskôr musíte definovať Rozloženie s aplikáciami v časti Všeobecné nastavenia → Správa aplikácií → Obchod AE Play → Rozloženie obchodu.

Pred úspešným pridaním aplikácií do obchodu musia byť aplikácie v Rozložení.

Režim kiosku a spúšťač

Režim kiosku

Režim Kiosk umožňuje vopred definovať aplikáciu alebo adresu URL. Potom bude možné spustiť/navštíviť výlučne túto aplikáciu alebo adresu URL.

Podobne je možné deaktivovať rôzne hardvérové tlačidlá v režime Kiosk Mode.

Automatický štart	Automatické spustenie režimu Kiosk, hneď ako profil dorazí do zariadenia koncového používateľa.
Plánovaný režim kiosku?	Môžete si naplánovať čas pre režim kiosku, ktorý sa potom začne a skončí automaticky vo vami nastavenom čase.
Čas začiatku	Čas začiatku
Čas v minútach	Čas v minútach, po ktorom by sa mal režim Kiosk opäť ukončiť

Typ aplikácie

Jedna aplikácia	Ak chcete spustiť aplikáciu v režime kiosku, vyberte možnosť Balík" v časti "Typ aplikácie".
Aplikácia kiosku	Kliknite sem, ak chcete vybrať aplikáciu, ktorá sa má spustiť v režime kiosku. Nájdete tu obvyklý prehľad správy aplikácií Môžete si vybrať medzi "Google Play Store", "Android In-House Apps" a "Packagename".

Typ aplikácie

ADRESA URL	Ak chcete v režime kiosku spustiť adresu URL, vyberte položku "URL" v časti "Typ aplikácie". Potom definujte požadovanú adresu URL
Vymazanie prehliadača po nečinnosti	Tu môžete definovať časový interval v minútach, po ktorom sa má režim kiosku znovu spustiť.
Vymazanie webovej vyrovnávacej pamäte a súborov cookie	Ak túto funkciu aktivujete, po reštarte režimu Kiosk sa vymaže webová vyrovnávacia pamäť (súbory cookie a obrázky v medzipamäti).
Politika rovnakého pôvodu	Ak je táto funkcia aktívna, používateľ môže surfovať iba na podstránkach definovanej adresy URL Napríklad ste definovali nasledujúcu adresu URL:www.mypage.com Potom môže používateľ surfovať na: www.mypage.com/subpage
Adresy URL na bielej listine	Tu môžete udržiavať bielu listinu, všetky tieto adresy URL sú povolené Maximálne 1 adresa URL na riadok Adresa URL musí začínať http:/ alebo https://
Adresy URL na čiernej listine	Tu môžete udržiavať čiernu listinu, všetky tieto adresy URL nie sú povolené. Maximálne 1 adresa URL na riadok Adresa URL musí začínať http:/ alebo https://
Orientácia obrazovky	Toto nastavenie sa týka úprav obrazovky Automatic = automatický Portrét = vertikálny formát Krajina = režim na šírku

Viacnásobná aplikácia	Ak vyberiete režim "Multi App" Kiosk Mode, bude sa vyžadovať používanie spúšťacieho programu AppTec360.
Aplikácie	Použitie: Ako aplikáciu pre kiosk vyberte aplikáciu z obchodu Playstore alebo vlastnú aplikáciu. Je možné zadať aj názov balíka. Vybraná aplikácia Kiosk Application musí byť nainštalovaná v zariadení. Nezabudnite nastaviť Kiosk Application ako povinnú. Skratka na domovskej obrazovke: Ak je nastavená na "Zapnuté", vytvorí sa skratka na domovskej obrazovke. Ak je nastavená na "Off" (Vyp.), aplikácia sa bude stále zobrazovať v zozname aplikácií.

Povolené heslo pre ukončenie	Ak túto funkciu aktivujete, používateľ môže ukončiť režim kiosku pomocou vami vopred definovaného hesla.
Heslo pre ukončenie	Toto je heslo, ktoré ste preddefinovali.
Automatické zbalenie stavového riadku	Ak je táto možnosť povolená, stavový riadok sa automaticky podfarbí. S touto možnosťou môžu používatelia vidieť informácie na stavovom riadku, ale nemajú prístup k jeho funkciám
Zakázanie stavového riadka	Stavový riadok obsahuje Upozornenia, Skratky a Informácie. K dispozícii len pre zariadenia Samsung s funkciou KNOX 1.0 alebo vyššou.
Zakázanie tlačidiel hlasitosti	Zakázanie tlačidiel hlasitosti (k dispozícii len v zariadeniach Samsung so systémom KNOX 1.0 alebo vyšším)
Zakázanie vypínača zapnutia/vypnutia	Zakázanie prepínača zapnutia/vypnutia (dostupné len v zariadeniach Samsung s funkciou KNOX 1.0 alebo vyššou)
Zakázanie tlačidla Domov	Zakázanie tlačidla Domov. Ak je táto funkcia aktivovaná, režim Kiosk je možné ukončiť len v konzole AppTec360. (k dispozícii len v zariadeniach Samsung s funkciou KNOX 1.0 alebo vyššou)
Zakázanie navigačného panela	Pomocou tejto funkcie môžete vypnúť navigačný panel (Späť / Menu) Ak bola táto funkcia aktivovaná, režim Kiosk je možné ukončiť len v konzole AppTec360. (k dispozícii len v zariadeniach Samsung s funkciou KNOX 1.0 alebo vyššou)

Nastavenia aktualizácie aplikácie	
Povolenie aktualizácií aplikácií	Používatelia budú vyzvaní na vykonanie aktualizácie aplikácie aj vtedy, keď je aktívny režim Kiosk. Na zariadeniach so Samsung KNOX sa budú aplikácie aktualizovať potichu.
Okno aktualizácie	Nastavenie intervalu, v ktorom budú používatelia vyzvaní na inštaláciu aktualizácií aplikácií.

TeamViewer	
Povolenie bezobslužného prístupu	Ak je táto možnosť povolená, správcovia môžu zariadenie ovládať na diaľku bez interakcie používateľa. V zariadení musí byť nainštalovaná aplikácia TeamViewer Host.

Spúšťač AppTec360

Povolenie AppTec360 Launcher	Na: AppTec360 Launcher. Používateľ ho musí jednorazovo nastaviť ako predvolený spúšťač. Poznámka: Ak je povolený režim kiosku a režim kiosku je nastavený na "Multi App", bude sa vyžadovať používanie spúšťacieho programu AppTec360.
Veľké ikony	Na: Zobrazí väčšiu verziu ikon aplikácií v spúšťači
Skryť ikonu aplikácie AppTec360	Na: Úplne skryje aplikáciu AppTec360
Skryť ikonu obchodu AppTec360	Na: Úplne skryje AppTec360 Enterprise AppStore

Nastavenia aplikácie AppTec360

Povolenie aplikácie AppTec360 Settings	Aplikácia AppTec360 Settings poskytuje kontrolu nad pripojeniami WiFi a Bluetooth
Povolenie nastavení v aplikácii Multi App Režim kiosku	Ak je táto možnosť povolená, používatelia môžu pristupovať k aplikácii AppTec360 Settings, keď je aktívny režim Multi App Kiosk Mode.

Diaľkové ovládanie

Splashtop

Zobrazuje aktuálny stav nastavenia Splashtop. Tu sa zobrazia kroky, ktoré je potrebné vykonať na vzdialený prístup k zariadeniu prostredníctvom Splashtop. Tu musíte tiež zadať svoj kód nasadenia, ktorý môžete získať na webovej lokalite Splashtop. Deploy kód je potrebný na pripojenie k zariadeniu.

Teamviewer

Zobrazuje aktuálny stav nastavenia aplikácie Teamviewer. Tu sa zobrazia kroky, ktoré je potrebné vykonať na vzdialený prístup k zariadeniu prostredníctvom programu Teamviewer.

Správa obsahu

Obsahové okno

Tu môžete povoliť Contentbox pre toto zariadenie. Po aktivácii sa do zariadenia nainštaluje aplikácia Contentbox.

Zabezpečený prehliadač

Tu môžete povoliť Zabezpečený prehliadač pre toto zariadenie. Po aktivácii sa do zariadenia nainštaluje aplikácia Zabezpečený prehliadač. Tento prehliadač môžete nakonfigurovať tak, aby v zariadení ponúkal webový prehliadač, ktorý je obmedzený podľa vašich potrieb.

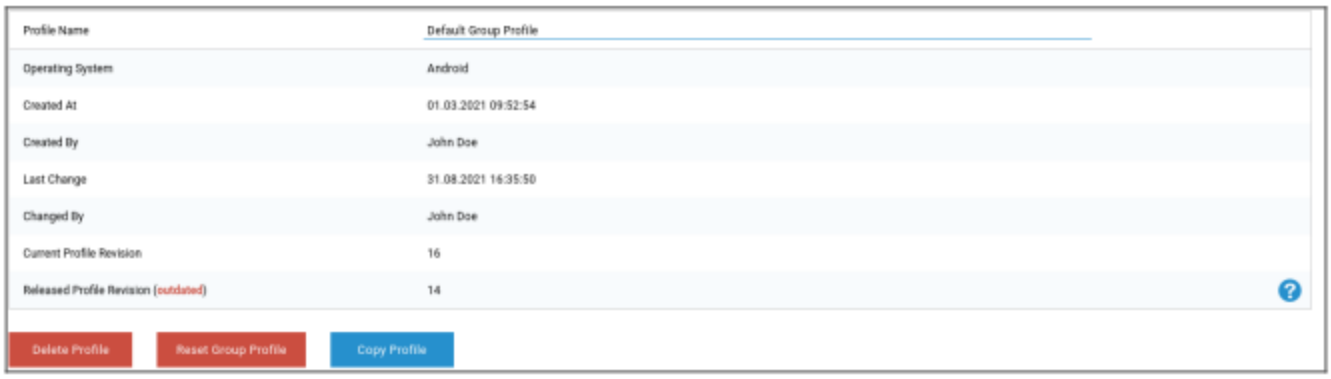
Vyžadovať heslo	Vyžadovať od používateľa nastavenie a používanie hesla na prístup do prehliadača.
Obmedzenie sťahovania / Otvoriť v	Blokuje sťahovanie z webových lokalít
Obmedzenie nahrávania	Obmedzí nahrávanie na určité adresy URL. Ak chcete úplne zablokovať odosielanie, nezadajte žiadnu adresu URL
Povoliť kopírovanie	Povoľte kopírovanie, vyrezávanie alebo zdieľanie textu vo vnútri webových stránok.
Povolenie snímania obrazovky	Umožniť zachytávanie snímok obrazovky.
Frekvencia čistenia údajov	Vyberte, s akou frekvenciou sa majú automaticky odstraňovať VŠETKY údaje používateľa (história, vyrovnávacia pamäť atď.).
Záložky spoločnosti	Záložky sa zobrazia v priečinku "Firemné záložky" v záložkách prehliadača. Používateľ ich nemôže upravovať.
Skryť adresný riadok	Skryje adresný riadok, aby používateľ nevidel navštívenú adresu URL
Biela listina v prehliadači (bez univerzálnej brány)	Povolí vytváranie bielych zoznamov URL na strane klienta. - Firemné záložky sú vždy zaradené do bielej listiny - Podporované len pre 100 URL - Pre neobmedzené zaradenie do čiernej a bielej listiny použite univerzálnu bránu
Čierna a biela listina založená na bráne	Čierna listina má tieto požiadavky: - Fungujúca univerzálna brána AppTec360 ("Všeobecné nastavenia" → "Univerzálna brána") - Fungujúca konfigurácia VPN s určeným serverom DNS ("Všeobecné nastavenia" → "Univerzálna brána" → "Nastavenia VPN") - Konfigurácia čiernej listiny ("Všeobecné nastavenia" → "Univerzálna brána" → "Čierna listina domén") - Platné pripojenie VPN v profile ("Správa pripojení" → "VPN")

Konfigurácia PC so systémom Windows 10

Všeobecné

Prehľad profilu skupiny (len na úrovni skupiny)

Po otvorení profilu skupiny sa zobrazí rýchly prehľad profilu.



Názov profilu	Názov profilu (tu sa dá zmeniť)
Operačný systém	Operačný systém, pre ktorý je profil určený
Vytvorené v	Čas vytvorenia
Vytvoril	Tvorca profilu
Posledná zmena	Čas poslednej zmeny profilu
Zmenené podľa	Účet, ktorý vykonal posledné zmeny
Aktuálna revízia profilu	Revízia uloženého stavu profilu
Vydaná revízia profilu	Priradená revízia profilu ("Priradiť teraz"). Ak sa za textom na štítku zobrazí " (zastaraný)", znamená to, že ste profil uložili, ale ešte ste ho nepriradili, takže zariadenia budú stále dostávať staršiu verziu.

Prehľad zariadení (len na úrovni zariadenia)

Súhrnný prehľad zariadenia, ktorý obsahuje:

Názov počítača	Názov počítača
Klient	Zariadenia typu Windows
Posledná známa lokalita	Zemepisná šírka a dĺžka poslednej známej polohy zariadenia
Priradené povinné aplikácie	Počet povinných aplikácií priradených k zariadeniu
PC UID	UID počítača
Vydanie pre operačný systém	Zobrazuje vaše vydanie systému Windows
Verzia operačného systému	Aktuálne nainštalovaná verzia systému Windows
Zostavenie operačného systému	Aktuálne zostavenie systému Windows
Operačný systém	Aktuálne nainštalovaný operačný systém
Sériové číslo	Sériové číslo zariadenia
Vlastníctvo zariadenia	Nakonfigurovaný typ vlastníctva
Typ zariadenia	Typ zariadenia
Zakorenené	Zobrazuje, či je zariadenie zakorenené
V súlade s	Zobrazuje, či je zariadenie kompatibilné
Naposledy videné	Dátum a čas vykonania zmien v profile
Priradenie používateľa	Zobrazuje používateľa alebo skupinu, ku ktorej je toto zariadenie aktuálne priradené. Zariadenie môžete presunúť výberom iného používateľa alebo skupiny z rozbaľovacieho zoznamu.

Nastavenia

Povoliť automatickú aktualizáciu	Povolenie alebo zakázanie automatických aktualizácií systému os.

Revízia konfigurácie (len na úrovni zariadenia)

Tu získate prehľad o tom, ktorý skupinový profil je priradený k zariadeniu.

Ak kliknete na profil skupiny, získate priamy prístup k profilu a môžete vykonať nastavenia.

Pomocou symbolu môžete vrátiť priradené aplikácie do nastavení skupinového profilu.

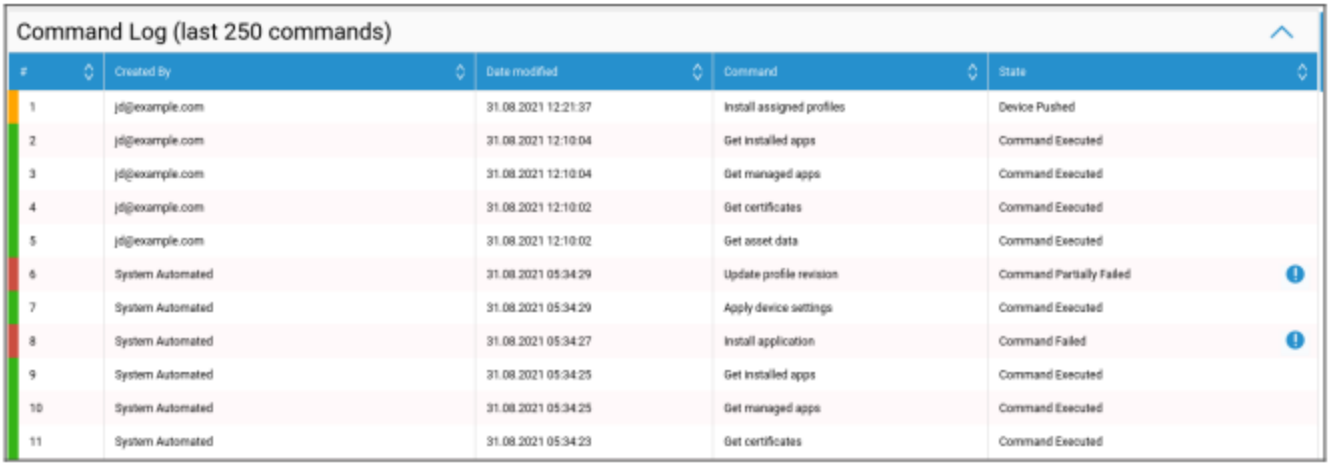
Pomocou symbolu môžete obnoviť profil zariadenia tak, aby nemal žiadne nastavenia.

"K dispozícii je novšia revízia" znamená, že profil skupiny bol zmenený a uložený, ale nie je priradený. Profil skupiny sa musí priradiť pomocou "Priradiť teraz" na úrovni skupiny, aby sa zmeny uplatnili na zariadeniach.

Protokol zariadenia (len na úrovni zariadenia)

Denník príkazov

Tu môžete vidieť, ktoré príkazy boli pre zariadenie vydané a aký je ich stav.



Príkazy vytvorené pomocou "System Automated" sú automaticky vytvorené systémom.

Možné stavy príkazov

Stlačené zariadenie	Do služby push (napr. APNS) bola odoslaná požiadavka na pripojenie, aby sa zariadenie pripojilo späť k serveru EMM.
Vytvorený príkaz	Príkaz bol vytvorený v systéme.
Odoslaný príkaz	Príkaz sa odoslal do zariadenia po jeho pripojení k serveru.
Vykonaný príkaz	Príkaz bol úspešne vykonaný.
Príkaz zlyhal	Príkaz zlyhal. *
Príkaz čiastočne zlyhal	V závislosti od operačného systému zariadenia môžu byť niektoré príkazy zoskupené. V tejto časti tejto skupiny príkazov zlyhali niektoré časti. *
Príkaz vykonaný, prípadne neúspešný	Príkaz bol vykonaný, ale možno nebol.
Príkaz Repushed	Príkaz bol opätovne odoslaný používateľom.
Vyradené	Príkaz bol zamietnutý. Napríklad preto, že bol nahradený iným príkazom alebo zariadenie bolo znovu zaregistrované a staré príkazy boli odstránené.

*Ak je za správou výkričník, môžete získať ďalšie informácie, ak kurzorom prejdete na ikonu.

Správa aktív (len na úrovni zariadenia)

Informácie o zariadení

Výrobca	Výrobca zariadenia
Model	Model zariadenia
Číslo modelu	Číslo modelu
Operačný systém	Operačný systém
Verzia operačného systému	Verzia operačného systému
Sériové číslo	Sériové číslo
ExchangeID	ExchangeID
Celková pamäť RAM	Celková pamäť RAM
Rozlíšenie displeja	Rozlíšenie displeja
Jazyk telefónu	Jazyk zariadenia
Verzia firmvéru	Verzia firmvéru
Verzia klienta DM	Verzia klienta pre správu zariadení
Verzia hardvéru	Verzia hardvéru zariadenia
Architektúra CPU	Architektúra CPU (typ procesora)

Cellular

Sieť operátora SIM	Sieť dopravcov
Telefónne číslo	Telefónne číslo
Stav roamingu	Stav roamingu
IMEI	IMEI
IMSI	IMSI
Firmvér modemu	Firmvér modemu

Informácie o synchronizácii

Okamžité pripojenie DM	Zariadenie by malo okamžite vytvoriť spojenie s aplikáciou AppTec
Počiatočný čas opakovania	Počiatočný čas opakovania pre toto prvé spojenie
Opakovanie pripojenia	Počet nových pokusov o pripojenie po odpojení od Správcu pripojenia alebo chybe na úrovni WinInet
Maximálny čas spánku	Maximálny čas spánku po chybe pri odosielaní balíka
Prvé opakovanie synchronizácie	Čas pre prvú fázu po zápise
Interval prvého opakovania	Čas pre prvú fázu po zápise
Druhé opakovanie synchronizácie	Čas na druhú fázu po zápise
Druhý interval opakovania	Čas na druhú fázu po zápise
Pravidelné opakovanie synchronizácie	Čas na ďalšie fázy po zápise
Pravidelný interval opakovania	Čas na ďalšie fázy po zápise

Riadenie bezpečnosti

Ochrana proti krádeži (len na úrovni zariadenia)

Informácie GPS (len na úrovni zariadenia)

Tu môžete určiť aktuálne/posledné umiestnenie zariadenia. Lokalizácia môže byť chránená jedným alebo dokonca dvoma heslami - pozri: "Všeobecné nastavenia" > "Súkromie" > "Prístup k GPS".

Nastavenia GPS

Povolenie sledovania GPS	Povoľte pravidelnú synchronizáciu informácií GPS.
Interval sledovania	Nastavenie intervalu synchronizácie informácií GPS.

Konfigurácia zabezpečenia

Prístupový kód

Minimálna dĺžka hesla	Minimálna dĺžka hesla	
Zloženie hesla	Určuje počet špecifických znakov, ktoré musí heslo obsahovať Tvoria ich veľké písmená, malé písmená, číslice a špeciálne symboly.	
Kvalita hesla	Tu môžete nastaviť kvalitu hesla	
	Alfanumerické	Len čísla a písmená
	Číselné	Iba čísla
	Číselné alebo alfanumerické	Čísla alebo čísla a písmená
Uzamknutie maximálneho času nečinnosti	Počet minút nečinnosti používateľa na zariadení, po ktorých sa zariadenie zablokuje. Používateľ musí po uplynutí tohto času zariadenie odomknúť zadaním hesla zariadenia.	
Vypršanie platnosti hesla	Nastavenie času, dokedy sa musí nastaviť nové heslo	
Obmedzenie histórie hesiel	Počet predtým použitých hesiel, ktoré nie sú povolené	
Maximálny počet neúspešných pokusov o zadanie hesla	Počet prípadov, keď je možné nesprávne zadať heslo, kým sa vykoná úplné vymazanie zariadenia	

Antivírusový program

Nastavenia antivírusového programu - Nastavenie konfigurácie skenovania	
Typ skenovania	Vyberie, či sa má vykonať rýchle alebo úplné skenovanie.
Nastavenie začiatku skenovania	Výber denného času, v ktorom program Windows Defender spustí skenovanie
Frekvencia skenovania	Výber dňa, v ktorom sa má spustiť kontrola programu Windows Defender
Frekvencia aktualizácie podpisov	Špecifikuje interval v hodinách, ktorý sa použije na kontrolu podpisov

Konfigurácia typu súborov na skenovanie	
Povolenie skenovania archívnych súborov	Povolenie alebo zakázanie skenovania archívov (napríklad .zip) pri prístupe.
Povolenie skenovania skriptov	Povolí alebo zakáže funkciu Skenovanie skriptov programu Windows Defender.
Povolenie skenovania e-mailov	Povolenie alebo zakázanie skenovania e-mailov.
Povolenie skenovania sieťových súborov	Povolenie alebo zakázanie skenovania sieťových súborov.
Povolenie úplného skenovania mapovaných sieťových jednotiek	Povoliť alebo zakázať skenovanie mapovaných sieťových jednotiek (povolené len pri zapnutom úplnom skenovaní).
Ovládanie obojsmerného skenovania	Riadi, ktoré súbory sa majú monitorovať.
Povolenie úplného skenovania vymeniteľných jednotiek	Povolenie alebo zakázanie úplného skenovania vymeniteľných jednotiek. Iniciuje sa len počas úplného skenovania.

Typ súborov, ktoré sa majú vylúčiť z kontroly	
Ignorovanie typov súborov pri skenovaní	Definujte sadu typov prípon súborov. Každá prípona súboru pre každé pole.
Ignorovanie ciest k adresárom	Definujte sadu ciest k adresárom, aby ste ich neskenovali. Jedna cesta pre každé pole. Príklady: "C:\Example", "C:\Windows" alebo "C:\Users".
Vylúčenie procesov z kontroly	Vylúčenie súborov, ktoré boli otvorené konkrétnymi procesmi, z antivírusového skenovania programu Microsoft Defender. . Jedna cesta pre každé pole. Príklady: "C:\myFile.exe", "C:\Windows\myProcess.exe", "C:\myScript.bat

Dodatočné nastavenia	
Povolenie monitorovania v reálnom čase	Povolenie alebo zakázanie funkcie monitorovania v reálnom čase programu Windows Defender
Umožniť monitorovanie správania	Povolenie alebo zakázanie funkcie monitorovania správania systému Windows
Povolenie ochrany v cloude	Povoliť alebo zakázať programu Windows Defender odosielať spoločnosti Microsoft informácie o všetkých nájdených problémoch. Spoločnosť Microsoft tieto informácie analyzuje, dozvie sa viac o probléme, ktorý ovplyvňuje zariadenie, a ponúkne vylepšené riešenia.
	Správanie pri odosielaní vzoriek
Povolenie ochrany IOAV programu Windows Defender	Povolenie alebo zakázanie ochrany Windows Defender IOAV
Povolenie prístupu k používateľskému rozhraniu Defenders "On Access protection"	
Priemerný faktor zaťaženia CPU	Predstavuje priemerný faktor zaťaženia procesora pri skenovaní programu Windows Defender (v percentách).

Spracovanie škodlivého softvéru	
Nízka závažnosť	Pre každú úroveň závažnosti môžete definovať, ako zariadenie spracuje škodlivý softvér. K dispozícii sú tieto možnosti: • Clean • Karanténa • Odstránenie stránky • Povoľte • Definované používateľom • Blok
Stredná závažnosť	
Vysoká závažnosť	
Závažnosť	
Dni na uchovanie vyčisteného malvéru	Časové obdobie v dňoch, počas ktorého budú súbory/položky v karanténe uložené v systéme. Predvolená hodnota je 0, ktorá ponecháva položky v karanténe a automaticky ich neodstraňuje. Maximálna hodnota je 90.

Bezpečnostné centrum

Centrum zabezpečenia systému Windows - Nastavenia zabezpečenia systému Windows	
Zakázanie používateľského rozhrania ochrany pred vírusmi a hrozbami	
Skryť používateľské rozhranie pre obnovu dát Ransomware	
Zakázanie používateľského rozhrania ochrany účtu	
Zakázanie brány firewall a používateľského rozhrania ochrany siete	
Zakázanie ovládania aplikácií a používateľského rozhrania prehliadača	
Zakázať zmeny ochrany pred zneužitím	Zakázať používateľovi vykonávať zmeny v nastaveniach ochrany proti zneužitiu
Zakázanie používateľského rozhrania zabezpečenia zariadenia	
Skrytie riešenia problémov s TPM	Skrytie nastavení riešenia problémov s čipom TPM
Zakázať tlačidlo Clear TPM	
Zakázanie používateľského rozhrania výkonu a stavu zariadenia	
Zakázanie možností rodiny používateľského rozhrania	

Prispôsobenie prípitkov	
Povolenie prispôsobených informácií o podpore	Povolenie zobrazenia prispôsobených kontaktných informácií podpory pre vašu spoločnosť v pravom dolnom rohu aplikácie centra zabezpečenia.
E-mailová adresa	Nastavenie e-mailovej adresy spoločnosti
Názov spoločnosti	Nastavenie názvu spoločnosti
Telefón spoločnosti	Nastavenie telefónu spoločnosti
Adresa URL nápovedy	Nastavenie adresy URL pomoci spoločnosti

Dodatočné nastavenia	
Zakázanie oznámení	Zakázanie zobrazovania oznámení Centra zabezpečenia systému Windows Defender.
Skrytie odporúčaní na aktualizáciu firmvéru TPM	Skryť odporúčanie aktualizovať firmvér TPM, keď sa zistí zraniteľný firmvér.
Zobrazenie názvu spoločnosti a možností kontaktu	Zobrazenie názvu vašej spoločnosti a možností kontaktu na vyletiacej karte kontaktu v Centre zabezpečenia systému Windows Defender.
Skryť Secure Boot	Skryť oblasť Security Boot.
Skryť ovládanie oblasti bezpečnostných oznámení	Skrytie ovládacieho prvku oblasti oznámení zabezpečenia systému Windows.

Konfigurácia brány firewall

Konfigurácia brány firewall - Globálne nastavenia	
Ignorovanie nastaveného overovania	Ignorovať celú sadu overovania, ak nepodporujú všetky sady overovania uvedené v sade.
Typ radenia paketov do frontu	Určuje, ako je povolené škálovanie softvéru na strane príjmu pre šifrovaný príjem aj pre čistú cestu pre scenár tunelovej brány IPsec.
Zakázať vykonávanie stavového filtrovania FTP	Ak je vypnutá, nevykoná stavové filtrovanie protokolu FTP (File Transfer Protocol), aby povolila sekundárne pripojenia.
Čas nečinnosti bezpečnostného združenia	V tomto poli sa konfiguruje čas nečinnosti združenia zabezpečenia v sekundách. Bezpečnostné asociácie sa odstránia po tom, čo sa počas tohto zadaného času nezobrazí sieťová prevádzka.
Kódovanie vopred zdieľaného kľúča	Nastavenie kódovania zdieľaného kľúča
Výnimky IPSec	Konfigurácia výnimiek internetového protokolu
Kontrola zoznamu zrušených certifikátov	

Profily brány firewall (doménový profil / súkromný profil / verejný profil)	
Povolenie brány firewall pre tento profil	
Zakázanie oznámení	Zakázanie zobrazovania upozornenia používateľovi, keď je aplikácii zablokované počúvanie na porte.
Blokovanie odpovedí unicast vysielania na multicast vysielanie	
Vykonávanie autorizovaných pravidiel brány firewall pre aplikácie	Ak nie je vynútená, autorizované pravidlá brány firewall aplikácie v miestnom úložisku sa ignorujú a nevynútia.
Vykonávanie globálnych pravidiel brány firewall pre porty	Ak nie je vynútená, globálne pravidlá brány firewall portov v miestnom úložisku sa ignorujú a nevynucujú. Nastavenie má význam len vtedy, ak je nastavené alebo vymenované v úložisku zásad skupiny alebo ak je vymenované z úložiska GroupPolicyRSoPStore
Vykonávanie pravidiel brány firewall	Ak nie je vynútená, pravidlá brány firewall z miestneho úložiska sa ignorujú a nevykonávajú.
Vykonávanie pravidiel zabezpečenia pripojenia	Ak sa nevykonáva, pravidlá zabezpečenia pripojenia z miestneho úložiska sa ignorujú a nevykonávajú.
Predvolená odchádzajúca akcia	Akcia, ktorú brána firewall predvolene vykonáva pri odchádzajúcich pripojeniach
Predvolená prichádzajúca akcia	Akcia, ktorú brána firewall predvolene vykonáva pri prichádzajúcich pripojeniach
Zakázanie režimu Stealth	Skrytý režim je mechanizmus v bráne Windows Firewall, ktorý pomáha zabrániť škodlivým používateľom zistiť informácie o sieťových počítačoch a službách, ktoré sú na nich spustené.
Zakázanie zabránenia odpovede na nevyžiadanú prevádzku	Ak je vypnuté, pravidlá skrytého režimu brány firewall nesmú brániť hostiteľskému počítaču reagovať na nevyžiadanú sieťovú prevádzku, ak je táto prevádzka zabezpečená pomocou protokolu IPsec.

Pravidlá brány firewall

Pravidlá brány firewall	
Názov	Názov pravidla
Popis	Opis pravidla
Akcia	Určite, či toto pravidlo bude blokovať alebo povoľovať prevádzku. Zohľadnite, že možnosť Blokovať by mohla blokovať aj prevádzku (v závislosti od zvyšku konfigurácie) medzi serverom MDM a zariadením.
Smer	
Povoliť prechádzanie hraníc (k dispozícii len vtedy, keď je **smer** nastavený na **prichádzajúcu prevádzku**)	Označuje, že špecifická prichádzajúca prevádzka je povolená na tunelovanie cez NAT a iné okrajové zariadenia pomocou technológie tunelovania Teredo.

Programy a služby	
Definujte aplikácie, všetky inak	Ak nie je povolená, bude brať do úvahy všetky aplikácie
Názov rodiny balíkov	Názov rodiny balíkov, na ktorú sa pravidlo bude vzťahovať.
Cesta k súboru aplikácie	Celá aplikácia, napríklad C:\Windows\System\Notepad.exe, na ktorú sa pravidlo bude vzťahovať
Plne kvalifikovaný binárny názov	Plne kvalifikovaný binárny názov, na ktorý sa pravidlo vzťahuje. FQBN je reťazec v nasledujúcom tvare: {Vydavateľ\Produkt\Filename,Version}
Názov služby	Zadajte názov služby (napr. "EventLog"). Zoznam názvov služieb môžete získať v prostredí Powershell spustením príkazu "Get-Service".

Protokoly a porty				
Protokol	Protokol používaný pravidlom.			
	Dostupné hodnoty: - Akékoľvek - Vlastné - HOPORT - ICMPv4 - IGMP - TCP - UDP - IPv6 - IPv6-Route - IPv6-Frag - GRE - ICMPv6 - IPv6-NoNxt - IPv6-Opts - VRRP - PGM - L2TP	Keď je nastavená na možnosť Vlastné	Vložte číslo protokolu v rozsahu 0 až 255	Číslo protokolu
		Pri nastavení na TCP alebo UDP	Zadajte miestne porty, inak sa použijú všetky	Miestne porty, ktoré bude pravidlo používať, povolené sú aj porty rozsahu
			Miestny prístav	Jeden port alebo rad portov. Napr. 100-120,200,300-320.
			Zadajte vzdialené porty, inak sa použijú všetky	Vzdialené porty, ktoré bude pravidlo používať, povolené sú aj porty rozsahu
			Vzdialený port	Jeden port alebo rad portov. Napr. 100-120,200,300-320.

Rozsah pôsobnosti	
Zadajte miestne IP, inak ľubovoľné IP	Sada lokálnych IP adries, môže to byť aj rozsah IP adries oddelených znakom -
Miestna IP adresa	Súbor jednotlivých IP adries alebo rozsah IP adries oddelených znakom -
Zadajte vzdialené IP adresy, inak akúkoľvek vzdialenú IP adresu	Zadajte sadu vzdialených IP adries, môže to byť aj rozsah IP adries oddelených znakom "-".
Vzdialená IP adresa	Zadanie jednotlivých IP adries alebo rozsahu IP adries
Žetóny	Tokeny, ktoré možno nastaviť spolu so vzdialenými adresami. Tokeny Intranet, RmtIntranet a Ply2Renders sú podporované v systéme Windows 10, verzia 1809 a novšia.

Rozšírené nastavenia

Určite profily, inak sa použijú všetky	Ak je vypnuté, použijú sa všetky profily
Doména	Profil domény
Súkromná stránka	Súkromný profil
Verejnosť	Verejný profil
Uveďte rozhrania, inak sa použijú všetky	Ak je vypnuté, použijú sa všetky rozhrania
Miestna sieť	Rozhranie lokálnej siete
Vzdialený prístup	Rozhranie vzdialeného prístupu
Bezdrôtové pripojenie	Bezdrôtové rozhranie

Miestni riaditelia	
Pridanie autorizovaných miestnych používateľov	Umožňuje pridať zoznam miestnych používateľov, ktorí budú používať toto pravidlo
Autorizovaní používatelia	Zoznam oprávnených miestnych používateľov pre toto pravidlo. Používateľ musí byť vo formáte SDDL (Security Description Definition Language), napr. PC_NAME\USERNAME. Toto pole sa nesmie vyplniť, ak je na používanie tohto pravidla nastavený názov služby

Nastavenia obmedzenia

Funkčnosť zariadenia

Povolenie karty SD	Povolenie používania karty SD
Povoliť fotoaparát	Povolenie používania fotoaparátu
Povolenie služby určovania polohy	Povolenie služby určovania polohy zariadenia
Povolenie bočného načítania aplikácií	Povolenie inštalácie aplikácií z neznámych zdrojov
Povolenie režimu pre vývojárov	Umožňuje režim pre vývojárov
Povolenie mobilného dátového roamingu	Povolenie mobilného dátového roamingu
Povolenie Cortany	Povolenie hlasovej asistentky Cortana
Povolenie vyhľadávania pomocou polohy	Povolenie vyhľadávania pomocou polohy
Povolenie pridania e-mailového konta iného ako Microsoft	Určite, či používateľ môže pridávať e-mailové kontá, ktoré nie sú MSA.
Povolenie pripojenia k účtu Microsoft	Určite, či chcete povoliť používanie konta MSA na overovanie a služby pripojenia, ktoré nesúvisia s e-mailom.
Povoliť synchronizáciu mojich nastavení	Umožňuje synchronizáciu nastavení v celom zariadení
Chránené doménové mená podnikov	Určuje názvy podnikových domén oddelené znakom ";".
Povolenie používateľovi zakázať obnovenie systému	Umožňuje používateľovi vypnúť funkciu Obnovenie systému. **VAROVANIE!** Táto funkcia by sa mala používať len na zariadeniach, ktoré vlastní alebo poskytuje podniková spoločnosť alebo organizácia, alebo na zariadení vo vlastníctve používateľa, ak používateľ povolí, aby zariadenie plne spravovala podniková spoločnosť. Ak toto nastavenie zásad zakážete, funkcia Obnovenie

	systému bude vypnutá a Sprievodca obnovením systému nebude prístupný. Možnosť nakonfigurovať Obnovenie systému alebo vytvoriť bod obnovenia prostredníctvom funkcie Ochrana systému je tiež vypnutá.
Povolenie zrušenia registrácie používateľa	Umožňuje používateľovi odstrániť firemnú časť zo zariadenia, a tým sa odpojiť od serverov AppTec360. Ak sa tak stane, zariadenie už nebude možné spravovať **VAROVANIE!** Táto funkcia by sa mala používať len na zariadeniach, ktoré vlastní alebo poskytuje podniková spoločnosť alebo organizácia, alebo na zariadení vo vlastníctve používateľa, ak používateľ povolí, aby zariadenie plne spravovala podniková spoločnosť. Ak toto nastavenie zásad zakážete, používatelia nebudú môcť odstrániť registrácie MDM. Určite, či používateľ môže vymazať účet pracoviska prostredníctvom ovládacieho panela pracoviska. Server MDM by vždy mohol účet vymazať na diaľku.

BitLocker

Konfigurácia nástroja BitLocker

Všeobecné nastavenia	
Vyžadovať šifrovanie zariadenia	V závislosti od vydania systému Windows a konfigurácie systému sa používateľom môže zobraziť výzva na zapnutie šifrovania zariadenia: - Potvrdenie, že šifrovanie od iného poskytovateľa nie je povolené. - Vypnutie funkcie BitLocker Drive Encryption a následné zapnutie funkcie BitLocker.
Metódy šifrovania	
Metóda šifrovania diskov operačného systému	
Metóda šifrovania pevných dátových jednotiek	
Metóda šifrovania vymeniteľných dátových diskov	
Zakázanie upozornenia na šifrovanie disku treťou stranou	Zakázanie výstražného hlásenia o službe šifrovania disku tretej strany, ktorá sa používa v zariadení. Od verzie 1803 systému Windows 10 je toto nastavenie podporované len pre zariadenia pripojené k službe Azure Active Directory.
Povolenie spúšťania šifrovania, keď je prihlásený používateľ, ktorý nie je správcom	Podporované len pre zariadenia pripojené k službe Azure Active Directory

Rozšírenia AppTec360		
Tiché šifrovanie		Ak sa vyberie možnosť "Vyžadovať šifrovanie zariadenia", služba AppTec360 Management Service spustí automatické tiché šifrovanie diskov zariadenia.
	Automatické generovanie poverení používateľa	Šifrovaný disk operačného systému bude chránený automaticky generovanými povereniami používateľa. Buď kód PIN čipu TPM, ak je čip TPM k dispozícii, alebo 6-miestne textové heslo. Vygenerované poverenia sa odošlú na e-mailovú adresu registrovanú pre dané zariadenie. Ak je táto možnosť vypnutá, jedinou možnou ochranou pre tiché šifrovanie je použitie TPM. V takom prípade sa v prípade zariadení bez čipu TPM tiché šifrovanie nepodarí.
	Šifrovanie pevných diskov	Všetky dostupné pevné dátové disky budú tiež zašifrované a chránené funkciou "Automatické odomknutie" pomocou kľúča uloženého na disku operačného systému.

Nastavenia jednotky OS

Vyžadovanie dodatočného overenia pri spustení		Toto nastavenie umožňuje nakonfigurovať, či nástroj BitLocker vyžaduje overenie pri každom spustení počítača. Toto nastavenie sa použije počas nastavenia nástroja BitLocker. Ak toto nastavenie povolíte, používatelia môžu v sprievodcovi nastavením nástroja BitLocker konfigurovať rozšírené možnosti spúšťania.
	Blokovanie nástroja BitLocker bez kompatibilného čipu TPM	
	Len TPM	
	TPM a PIN	
	TPM a kľúč	
	TPM, kľúč a PIN	Ak chcete vyžadovať používanie kódu PIN a USB flash disku (kľúča), používateľ musí nastaviť nástroj BitLocker pomocou nástroja príkazového riadka "manage-bde" namiesto sprievodcu nastavením nástroja BitLocker Drive Encryption.

Vyžadovať minimálnu dĺžku kódu PIN

	Minimálny počet znakov

Konfigurácia správy o obnovení pred spustením a adresy URL	Nakonfigurujte celú správu o obnovení alebo nahraďte existujúcu adresu URL, ktorá sa zobrazuje na obrazovke obnovenia pred zavedením kľúča, keď je jednotka OS uzamknutá. Poznámka: Nie všetky znaky a jazyky sú podporované v režime pred spustením systému. Dôrazne sa odporúča otestovať, či sa znaky, ktoré používate, zobrazujú na obrazovke obnovy pred spustením systému správne.
	Možnosť správy o obnovení pred spustením systému
	Vlastná správa o obnovení
	Vlastná adresa URL na obnovenie

Možnosti obnovy jednotky OS		Toto nastavenie umožňuje ovládať spôsob obnovy diskov operačného systému chránených nástrojom BitLocker v prípade, že nie sú k dispozícii požadované poverenia. Toto nastavenie sa použije počas nastavenia nástroja BitLocker. V predvolenom nastavení je povolený agent na obnovu údajov založený na certifikáte, možnosti obnovy môže určiť používateľ vrátane hesla na obnovu a kľúča na obnovu a informácie o obnove sa nezálohujú do služby AD DS.
	Agent na obnovu údajov založený na blokovom certifikáte	Určite, či sa agent na obnovu údajov môže používať s diskami operačného systému chránenými nástrojom BitLocker. Pred použitím agenta na obnovu údajov ho treba pridať z položky Zásady verejného kľúča v konzole na správu zásad skupiny alebo v editore miestnych zásad skupiny. Ďalšie informácie o pridávaní agentov na obnovu údajov nájdete v príručke BitLocker Drive Encryption Deployment Guide na stránke Microsoft TechNet.
	Nastavenia hesla pre obnovenie nástroja BitLocker	
	Nastavenia kľúča na obnovenie nástroja BitLocker	
	Uloženie informácií o obnovení nástroja BitLocker do služby Active Directory Domain Services	
	Konfigurácia úložiska na obnovenie nástroja AD DS BitLocker	Uloženie balíka kľúčov podporuje obnovu údajov z jednotky, ktorá bola fyzicky poškodená.
	Požiadavka na ukladanie údajov o obnove do služby AD DS	Zabráňte používateľom zapnúť nástroj BitLocker, pokiaľ počítač nie je pripojený k doméne a

Pevné nastavenia pohonu	
Možnosti obnovy pevných diskov	Toto nastavenie umožňuje ovládať spôsob obnovy pevných diskov chránených nástrojom BitLocker v prípade, že nie sú k dispozícii požadované poverenia. Toto nastavenie sa použije počas nastavenia nástroja BitLocker. V predvolenom nastavení je povolený agent na obnovu údajov založený na certifikáte, možnosti obnovy môže určiť používateľ vrátane hesla na obnovu a kľúča na obnovu a informácie o obnove sa nezálohujú do služby AD DS.
Agent na obnovu údajov založený na blokovom certifikáte	
Nastavenia hesla pre obnovenie nástroja BitLocker	
Nastavenia kľúča na obnovenie nástroja BitLocker	
Uloženie informácií o obnovení nástroja BitLocker do služby Active Directory Domain Services	
Konfigurácia úložiska na obnovenie nástroja AD DS BitLocker	Uloženie balíka kľúčov podporuje obnovu údajov z jednotky, ktorá bola fyzicky poškodená.
Požiadavka na ukladanie údajov o obnove do služby AD DS	Zabráňte používateľom zapnúť nástroj BitLocker, pokiaľ počítač nie je pripojený k doméne a pokiaľ sa nepodarí zálohovať informácie o obnovení nástroja BitLocker do služby AD DS. Poznámka: Heslo na obnovenie sa generuje automaticky.
Odmietnutie prístupu k nechráneným pevným diskom	

Nastavenia vymeniteľného disku	
Odmietnutie prístupu k zápisu na nechránené vymeniteľné jednotky	Odmietnutie prístupu k vymeniteľným dátovým jednotkám, ktoré nie sú chránené programom Bitlocker. Poznámka: Ak "Vymeniteľné disky: Odmietnuť prístup k zápisu" je v zásadách skupiny povolená, toto nastavenie zásad sa bude ignorovať.
Odmietnutie prístupu k zápisu do zariadení nakonfigurovaných v inej organizácii	Prístup na zápis budú mať len jednotky s identifikačnými poľami zhodnými s identifikačnými poľami počítača. Tieto polia sú definované nastavením zásad skupiny "Poskytnúť jedinečné identifikátory pre vašu organizáciu".

Stav nástroja BitLocker

Tu si môžete pozrieť aktuálny stav diskov zašifrovaných nástrojom BitLocker

C [OS Drive]
Stav šifrovania
Zašifrované (%)
Stav ochrany
Metóda šifrovania
Chrániče kľúčov
Heslo na obnovenie

Kliknutím na tlačidlo "Rotate recovery password" (Otočiť heslo obnovy) môžete otočiť heslo obnovy nástroja BitLocker.

Správa certifikátov

Zoznam certifikátov

Tu je zoznam certifikátov, ktoré sú nainštalované v zobrazenom zariadení.

Konfigurácia certifikátu

Tu môžete nakonfigurovať certifikáty a spôsob ich inštalácie do zariadenia.

Dôveryhodný certifikát	
Popis	Popis certifikátu
Rozsah pôsobnosti	Rozsah nasadenia certifikátu: Aktuálny používateľ vs. zariadenie
Úložisko certifikátov	"Nedôveryhodné certifikáty" sú k dispozícii len od systému Windows 10, verzia 1803
Súbor s certifikátom	Nahratie súboru PKCS#1

Certifikát totožnosti			
Popis	Popis certifikátu		
Rozsah pôsobnosti	Rozsah nasadenia certifikátu: Aktuálny používateľ vs. zariadenie		
Kľúčové umiestnenie	Poskytovateľ úložiska kľúčov, do ktorého sa má nainštalovať súkromný kľúč.		
		TPM. Zlyhá, ak nie je prítomný TPM	
	TPM. Ak nie je prítomný TPM, vráti sa k softvéru KSP		
	Poskytovateľ softvérového úložiska kľúčov		Označiť súkromný kľúč ako exportovateľný
	Windows Hello pre firmy	Názov kontajnera	Určuje názov kontajnera Windows Hello for Business (predtým známy ako Microsoft Passport for Work).
		Text výzvy PIN	Určuje vlastný text, ktorý sa má zobraziť na výzve na zadanie PIN kódu Windows Hello for Business počas registrácie certifikátu.
Potvrdenie	Odoslanie súboru PKCS#12		

SCEP

Popis	Popis servera SCEP		
Rozsah nasadenia	Rozsah nasadenia certifikátu: Aktuálne zariadenie vs. používateľ		
Adresy URL servera SCEP	Jeden alebo viac serverov, ktoré vydávajú certifikáty prostredníctvom protokolu SCEP		
Predmet	Reprezentácia názvu X.500. Napr. "C=US, O=Microsoft Corporation, CN=foo, 1.2.5.3=bar"		
Alternatívne názvy predmetov	Typ	E-mailová adresa	
		DNS	
		URI	
		Hlavné meno používateľa (UPN)	
Odtlačok prsta CA	Odtlačok SHA1 certifikátu certifikačnej autority. E.g. 31:8F:1E:78:5C:D5:12:9F:7E:3B:AD:F3:1C:C0:19:03:96:43:A9:E5		
Jednotky obdobia platnosti	Dni, mesiace alebo roky		
Obdobie platnosti			
Výzva	Používa sa ako vopred zdieľané tajomstvo pre automatickú registráciu		
Opakované pokusy	Počet pokusov, ktoré má zariadenie opakovať, ak server odošle odpoveď PENDING. Predvolená hodnota je 5. Maximálna hodnota je 30.		
Oneskorenie opakovania	Počet minút, ktoré sa majú počkať pred opakovaním pokusu. Predvolená hodnota je 5. Minimálna hodnota je 1.		
Veľkosť kľúča	Veľkosť kľúča v bitoch		
Algoritmus Hash	Rodina hašovacích algoritmov		
Kľúčové použitie	Rozšírenie použitia kľúča definuje účel (napr. šifrovanie, podpis) kľúča obsiahnutého v certifikáte. Je potrebné vybrať aspoň jedno z týchto nastavení: "Digital signature" (digitálny podpis) alebo "Key encipherment" (šifrovanie kľúča).		
Rozšírené používanie kľúčov	Špecifikuje rozšírené použitie kľúčov.Podlieha konfigurácii servera SCEP. Zadajte zoznam zodpovedajúcich OID, napr. 1.3.6.1.5.5.7.3.2 (Autentifikácia klienta)		

Kľúčové umiestnenie	Poskytovateľ úložiska kľúčov, do ktorého sa má nainštalovať súkromný kľúč.		
		TPM. Zlyhá, ak nie je prítomný TPM	
	TPM. Ak nie je prítomný TPM, vráti sa k softvéru KSP		
	Poskytovateľ softvérového úložiska kľúčov		
	Windows Hello pre firmy	Názov kontajnera	Určuje názov kontajnera Windows Hello for Business (predtým známy ako Microsoft Passport for Work).
		Text výzvy PIN	Určuje vlastný text, ktorý sa má zobraziť na výzve na zadanie PIN kódu Windows Hello for Business počas registrácie certifikátu.

Správa pripojenia

Wifi

Pri tomto nastavení vykonajte predbežnú konfiguráciu zariadení koncových používateľov pre prístup k interným prístupovým bodom

Identifikátor súboru služieb (SSID)	SSID siete, ku ktorej sa vytvorí pripojenie
Automatické pripojenie	Aktivácia automatického pripojenia k sieti
Skrytá sieť	Aktivácia v prípade, že prístupový bod nevysiela identifikátor SSID

Typ zabezpečenia

Stanovenie typu zabezpečenia AP

Otvorený systém WEP	
Heslo	Heslo pre AP

WPA PSK	
Heslo	Heslo pre AP

WPA EAP	
Typ overovania	Typ overovania, možné len s "PEAP-MSCAHPv2"
Rýchle opätovné pripojenie	Zariadenia môžu prepínať medzi prístupovými bodmi bez toho, aby sa museli znova overovať
Prístup pre hostí	Používateľ nemá účet, a preto by sa mal zaregistrovať ako hosť
Kontroly karantény	Klient musí vykonať kontrolu NAP (Network Access Protection) a zdieľať výsledky so systémom, ktorý potom rozhodne, či sa klient môže pripojiť.
Vyžadovať kryptografickú väzbu	Overovanie je možné len prostredníctvom Crypto Binding
Overenie servera	Klient skontroluje, či je certifikát servera platný. Ak áno, vytvorí sa spojenie
Výzva na predloženie certifikátov	Umožňuje používateľovi prijímať nedôveryhodné certifikáty
Názvy serverov	Ponúka možnosť zobraziť názov servera RADIUS, ktorý ponúka sieťové overovanie a autorizáciu.

WPA2-PSK	
Heslo	Heslo AP

WPA2 EAP	
Typ overovania	Typ overovania, možné len s "PEAP-MSCAHPv2"
Rýchle opätovné pripojenie	
Prístup pre hostí	
Kontroly karantény	Aktivuje ochranu prístupu k sieti NAP
Vyžadovať kryptografickú väzbu	Overovanie je možné len prostredníctvom Crypto Binding
Overenie servera	
Výzva na predloženie certifikátov	Výzva na zadanie overeného certifikátu servera, názvu alebo overenia koreňového certifikátu (CA)
Názvy serverov	Zoznam serverov, ktorým by mali zariadenia dôverovať
Žiadne	Žiadne zavedené zabezpečenie
Použitie servera proxy	Používanie servera proxy
Adresa servera	Adresa proxy servera
Port servera	Port servera proxy servera

Použitie servera proxy

Povolenie používania proxy servera.

Adresa servera	Adresa proxy servera používaná v tejto sieti.
Port servera	Port proxy servera používaný v tejto sieti.

Obmedzenia Wifi

Tu môžete definovať rôzne obmedzenia Wifi.

Povolenie Wi-Fi	Povolenie/zakázanie pripojenia Wi-Fi
Povolenie zdieľania internetu	Povolenie používania hotspotu
Povolenie automatického pripojenia k zmyslovým bodom WiFi	Povolenie automatického pripojenia k zmyslovým bodom WiFi
Povolenie manuálnej konfigurácie WiFi	Umožniť používateľovi pripojiť sa k sieťam WiFi, ktoré neboli definované spoločnosťou AppTec
Frekvencia skenovania siete WLAN	Nastaví interval WLAN-Scan. Vyššia hodnota zvyšuje schopnosť rozpoznať siete WIFI.

VPN

Tu vykonajte príslušné nastavenia, aby ste mohli nakonfigurovať pripojenia VPN

Názov pripojenia	Uvedený názov pripojenia		
Typ VPN	Pripojenie VPN pre jednotlivé aplikácie sa používa na zabezpečenie prevádzky určitých aplikácií.		
	VPN	Vždy zapnuté	Tým sa VPN automaticky pripojí pri prihlásení a zostane pripojená, kým sa používateľ manuálne neodpojí.
	Sieť VPN pre jednotlivé aplikácie	Aplikácie VPN	Definovanie aplikácií, ktoré používajú toto pripojenie VPN
		Uzamknutie na jednu aplikáciu	Uzamknutie na jednu aplikáciu spôsobí, že vybrané aplikácie budú mať pripojenie len prostredníctvom tohto pripojenia VPN. Táto funkcia závisí od brány Windows Defender Firewall.
	Profil WIP	Doména WIP pre toto pripojenie	ID podniku, ktoré je potrebné na prepojenie tohto profilu VPN so zásadou ochrany informácií systému Windows (WIP).

Typ pripojenia

AppTec360 VPN	
Pre "AppTec360 VPN" sa vyžaduje, aby bolo povolené načítavanie aplikácií na stranu. Povoľte "Povoliť sideloading aplikácií" v "Správa zabezpečenia" → "Nastavenia obmedzení" → "Funkcionalita zariadenia".	
Konfigurácia brány	Ak chcete nakonfigurovať pripojenie VPN s čiernou listinou, vyberte konfiguráciu VPN so zadaným serverom DNS. Konfiguráciu VPN môžete nastaviť v časti "Všeobecné nastavenia" → "Univerzálna brána" → "Nastavenia VPN".

IKEv2		
Servery	Zoznam serverov VPN	
Tunel zariadenia	Povolenie pripojenia pred prihlásením používateľa.	
Spôsob overovania	EAP	EAP XML
	Certifikáty stroja	
Šifrovací algoritmus		
Algoritmus kontroly integrity		
Diffie-Hellmanova skupina		
Algoritmus šifrovej transformácie		
Algoritmus transformácie overovania		
Skupina dokonalého utajenia (PFS)		

PPTP		
Servery	Zoznam serverov VPN	
Spôsob overovania	EAP	EAP XML

L2TP		
Servery	Zoznam serverov VPN	
Spôsob overovania	EAP	EAP XML
Šifrovací algoritmus		
Algoritmus kontroly integrity		
Diffie-Hellmanova skupina		
Algoritmus šifrovej transformácie		
Algoritmus transformácie overovania		
Skupina dokonalého utajenia (PFS)		

Automatické		
Servery	Zoznam serverov VPN	
Spôsob overovania	EAP	EAP XML

Všeobecné konfigurácie VPN

Zapamätanie si poverení pri každom prihlásení	
Registrácia adries IP pomocou interného systému DNS	
Pravidlá filtrovania sieťovej prevádzky	Obmedzenie pripojenia VPN na definovaný súbor pravidiel.
Vyhľadávací zoznam prípon DNS	Prípony DNS, ktoré sa pridajú do zoznamu vyhľadávania DNS na smerovanie krátkych názvov.
Pravidlá tabuľky zásad rozlíšenia názvov (NRPT)	Pravidlá NRPT (Name Resolution Policy table) definujú, ako DNS prekladá názvy pri pripojení k sieti VPN.
Detekcia dôveryhodnej siete	Zoznam prípon DNS na identifikáciu dôveryhodnej siete.
Delené tunelovanie	Rozdelené tunelovanie znamená, že prevádzka môže prechádzať cez ľubovoľné rozhranie, ktoré určí sieťový zásobník.
Rozdelenie tunelových trás	Zoznam trás, ktoré sa majú pridať do smerovacej tabuľky pre rozhranie VPN.
Nastavenie servera proxy	Konfiguruje proxy server používaný s touto sieťou
Adresa splnomocnenca	Adresa proxy servera ako plne kvalifikovaný názov hostiteľa alebo IP adresa.
Prístav	Port proxy servera.
Adresa URL automatickej konfigurácie proxy servera	URL na automatické načítanie nastavení proxy servera.

Obmedzenia VPN

Tu môžete definovať rôzne obmedzenia VPN.

Povolenie nastavení siete VPN	Toto usmernenie umožňuje/zakazuje používateľovi deaktivovať a meniť nastavenia siete VPN
Povolenie siete VPN cez mobilnú sieť	Povolí/zakáže zariadeniu vytvoriť pripojenie VPN, ak zariadenie používa mobilné dáta
Povolenie roamingu VPN cez mobilnú sieť	Povolenie/zakázanie zariadenia vytvoriť pripojenie VPN, ak je zariadenie v roamingu

Bluetooth

Tu môžete nastaviť, či má byť Bluetooth povolené/zakázané.

Povoliť Bluetooth	Aktivácia/deaktivácia funkcie Bluetooth

Správa PIM

Exchange Active Sync

Nastavenie konta ActiveSync v zariadení koncového používateľa

Názov účtu	Názov e-mailového konta
Názov hostiteľa servera	Adresa servera/FQDN
Názov domény	Doména servera
E-mailová adresa	E-mailová adresa
Meno používateľa	Meno používateľa
Heslo používateľa	Voliteľne tu už môžete k používateľovi pripojiť heslo
Používanie protokolu SSL	Použitie pripojenia SSL
Interval synchronizácie	Tu je možné stanoviť interval synchronizácie Manuálna synchronizácia = Používateľ musí prevziať svoje e-maily a vykonať manuálnu synchronizáciu.
Filter veku pošty	Čas, za ktorý sa majú e-maily synchronizovať Žiadny filter = neobmedzené
Úroveň protokolu	Stanovenie úrovní protokolovania pre prevádzku ActiveSync
Synchronizácia e-mailu	Aktivované = e-maily sú synchronizované
Synchronizácia kontaktov	Aktivované = kontakty sú synchronizované
Synchronizácia kalendára	Aktivované = kalendár je synchronizovaný
Úlohy synchronizácie	Aktivované = úlohy sú synchronizované

E-mail

Zriadenie účtov POP3/IMAP4 v zariadení koncového používateľa.

Popis účtu	Názov e-mailového konta
Názov odosielateľa	Zobrazené meno odosielateľa
Názov domény	Názov domény pre e-mailové konto
E-mailová adresa	E-mailová adresa používateľa
Meno používateľa	Meno používateľa
Heslo používateľa	Voliteľne tu už môžete k používateľovi pripojiť heslo
Alternatívne prihlasovacie údaje odchádzajúceho servera	Tu je možné definovať, či sú pre odchádzajúci server potrebné ďalšie poverenia
Názov odchádzajúcej domény	Názov odchádzajúcej domény
Meno používateľa odchádzajúceho servera	Meno používateľa odchádzajúceho servera
Heslo odchádzajúceho servera	Heslo odchádzajúceho servera
E-mailový protokol	POP3 alebo IMAP4, možno použiť ako protokol
Názov hostiteľa servera prichádzajúcej pošty	Názov hostiteľa servera prichádzajúcej pošty
Používanie protokolu SSL pre prichádzajúcu poštu	Používanie protokolu SSL pre prichádzajúce e-maily
Názov hostiteľa servera odchádzajúcej pošty	Názov hostiteľa servera odchádzajúcej pošty
Používanie protokolu SSL pre odchádzajúcu poštu	Používanie protokolu SSL pre odchádzajúce e-maily
Overovanie odchádzajúceho servera	Vyžaduje sa overenie odchádzajúceho servera
Interval synchronizácie	Tu je možné stanoviť interval synchronizácie Manuálna synchronizácia = Používateľ musí prevziať svoje e-maily a vykonať manuálnu synchronizáciu.
Filter veku pošty	Čas, za ktorý sa majú e-maily synchronizovať Žiadny filter = neobmedzené

Správa aplikácií

Správca podnikových aplikácií

Nainštalované aplikácie

Tu je zoznam aplikácií, ktoré sú v súčasnosti nainštalované v zobrazenom zariadení.

Povinné aplikácie

Tu môžete nakonfigurovať zoznam aplikácií, ktoré sú v zariadení povinné.

Tento zoznam sa skontroluje pri každom pripojení zariadenia k MDM a nainštalujú sa všetky aplikácie z tohto zoznamu, ktoré náhodou nie sú v zariadení nainštalované, bez ohľadu na to, či bola aplikácia odinštalovaná alebo nikdy predtým nebola nainštalovaná.

Môžete nahrať aplikácie Windows 10 In-House Apps a potom ich pridať do tohto zoznamu alebo môžete pridať konfigurácie Microsoft Office, ktoré je potrebné vopred nakonfigurovať v časti "Všeobecné nastavenia" > "Správa aplikácií" > "Microsoft Office".

Obmedzenia aplikácie Sys

Doručené aplikácie
Povolenie budíkov a hodín
Povoliť kalkulačku
Povoliť fotoaparát
Povolenie kontaktnej podpory
Povolenie Cortany
Povolenie Prieskumníka súborov
Umožniť začať
Povoľte Groove Music
Povoliť mapy
Povolenie zasielania správ
Povolenie prehliadača Microsoft Edge
Povoliť filmy a televíziu
Povoľte peniaze
Povoliť správy
Povolenie služby OneDrive
Povolenie aplikácie OneNote
Povolenie kalendára a pošty programu Outlook
Umožniť ľuďom
Povoliť telefón
Povoliť fotografie
Povoliť PowerPoint
Povoliť nastavenia
Povolenie služby Skype
Umožniť šport
Umožniť uložiť
Povolenie hlasového záznamníka
Povoliť peňaženku
Povoliť počasie

Povolenie rozbočovača spätnej väzby systému Windows
Povoliť Word
Povolenie služby Xbox

Nastavenie stránok
Povolenie účtov Pracovisko
Povoliť rozšírené informácie
Povolenie rohu aplikácií
Povoliť blokovanie a filtrovanie
Povolenie farebného profilu
Povolenie režimu jazdy
Povolenie e-mailu a účtov
Povoliť ekvalizér
Povoliť klávesnicu
Povolenie navigačného panela
Povolenie sieťového režimu Lietadlo
Povolenie zdieľania internetu v sieti
Povolenie sieťových služieb
Povolenie siete Wi-Fi
Povolenie systému PC Bluetooth
Povoliť hodnotenie zariadenia
Povoliť obnovenie aktualizácie
Povoliť zdieľanie
Povoliť spustenie
Povolený čas Jazyk
Povolený čas Región
Povolenie predvoleného uzamknutia obrazovky systému Windows
Povolenie pracovného alebo školského účtu

Čierna a biela listina

V časti "Black- & Whitelisting" si môžete vybrať medzi režimom "Whitelist" a režimom "Blacklist".

Biela listina	Do zariadenia koncového používateľa je možné nainštalovať iba aplikácie a služby, ktoré sú pridané do zoznamu. Ak sú už v zariadení koncového používateľa predinštalované, budú aktivované a nastavené tak, aby ich používateľ mohol spustiť.
	Všetky ostatné aplikácie, ktoré nie sú pridané do zoznamu, nie je možné nainštalovať do zariadenia koncového používateľa. Ak sú tieto aplikácie už predinštalované v zariadení koncového používateľa, budú deaktivované a nastavené tak, aby ich používateľ nemohol spustiť.
Čierna listina	Aplikácie a služby, ktoré sú pridané do zoznamu, nie je možné nainštalovať do zariadenia koncového používateľa. Ak sú už v zariadení koncového používateľa predinštalované, budú deaktivované a nastavené tak, aby ich používateľ nemohol spustiť.
	Všetky ostatné aplikácie, ktoré nie sú pridané do zoznamu, sa môžu nainštalovať do zariadenia koncového používateľa. Ak sú tieto aplikácie už predinštalované v zariadení koncového používateľa, budú aktivované a nastavené tak, aby ich používateľ mohol spustiť.

Prostredníctvom tlačidla , pridáte do zoznamu aktuálne používaných aplikácií alebo služieb ďalšie aplikácie alebo služby.

Prostredníctvom tlačidla , pridáte ďalšie aplikácie alebo služby do aktuálne neaktívneho zoznamu.

Môžete pridať aplikáciu z obchodu Windows App Store alebo priamo zadať identifikátor aplikácie a pridať ju do čiernej alebo bielej listiny.

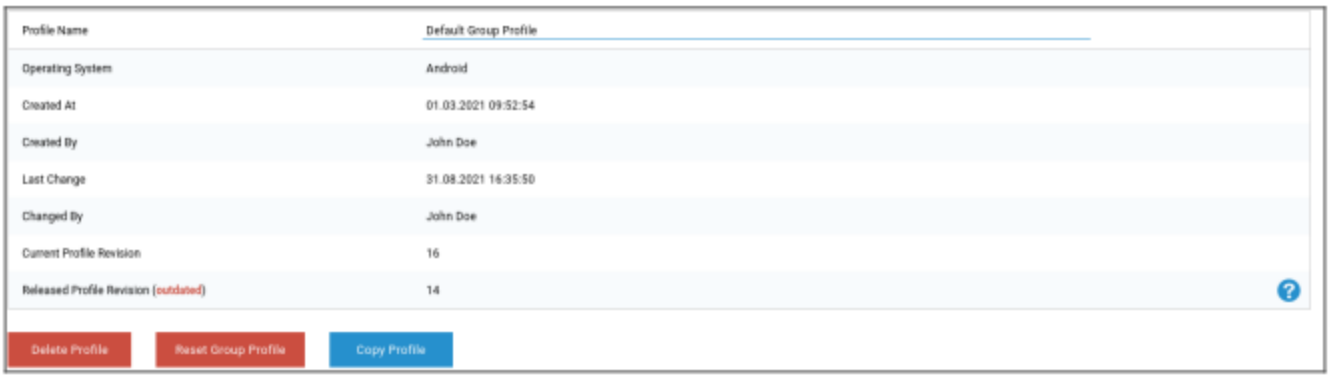
Konfigurácia systému MacOS

V závislosti od toho, či ste vybrali profil alebo zariadenie, sa zobrazenie a jeho čiastkové body líšia - venujte tomu zvýšenú pozornosť!

Všeobecné

Prehľad profilu skupiny (len na úrovni skupiny)

Po otvorení profilu skupiny sa zobrazí rýchly prehľad profilu.



Názov profilu	Názov profilu (tu sa dá zmeniť)
Operačný systém	Operačný systém, pre ktorý je profil určený
Vytvorené v	Čas vytvorenia
Vytvoril	Tvorca profilu
Posledná zmena	Čas poslednej zmeny profilu
Zmenené podľa	Účet, ktorý vykonal posledné zmeny
Aktuálna revízia profilu	Revízia uloženého stavu profilu
Vydaná revízia profilu	Priradená revízia profilu ("Priradiť teraz"). Ak sa za textom na štítku zobrazí " (zastaraný)", znamená to, že ste profil uložili, ale ešte ste ho nepriradili, takže zariadenia budú stále dostávať staršiu verziu.

Prehľad zariadení (len na úrovni zariadenia)

Súhrnný prehľad zariadenia.

Názov zariadenia	Názov zariadenia
Model	Model
Operačný systém	Operačný systém
Sériové číslo	Sériové číslo zariadenia
Vlastníctvo zariadenia	Nakonfigurovaný typ vlastníctva
Typ zariadenia	Typ zariadenia
V súlade s	Zobrazuje, či je zariadenie kompatibilné
IP adresa	Adresa IP, z ktorej sa zariadenie pripojilo k serveru
Naposledy videné	Čas posledného pripojenia zo zariadenia
Posledný impulz	Čas posledného tlačidla odoslaného do zariadenia
Zadanie	Tu môžete zariadenie presunúť k inému používateľovi alebo skupine

Revízia konfigurácie (len na úrovni zariadenia)

Tu získate prehľad o tom, ktorý skupinový profil je priradený k zariadeniu.

Ak kliknete na profil skupiny, získate priamy prístup k profilu a môžete vykonať nastavenia.

Pomocou symbolu môžete vrátiť priradené aplikácie do nastavení skupinového profilu.

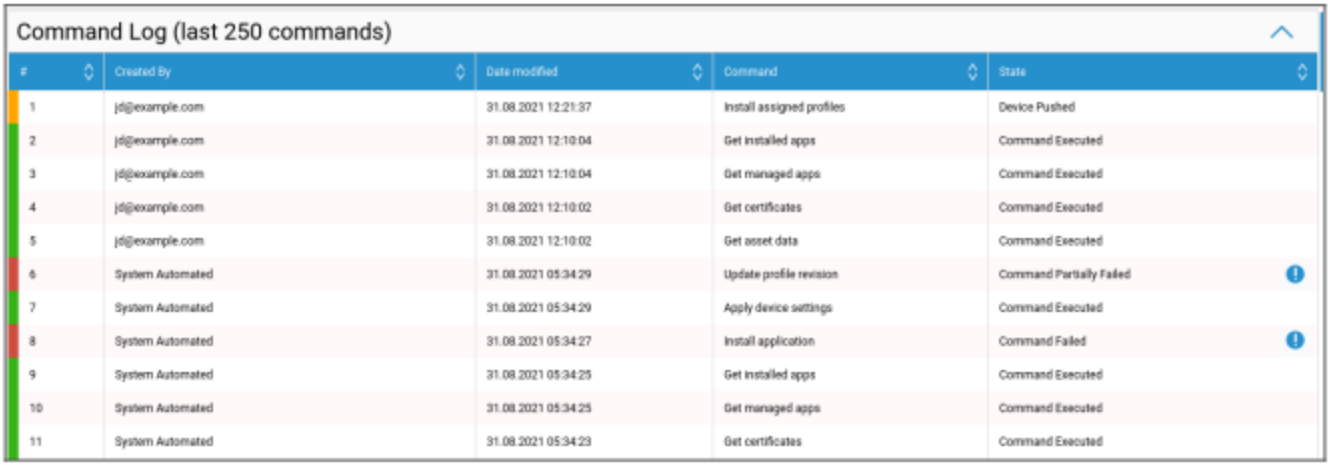
Pomocou symbolu môžete obnoviť profil zariadenia tak, aby nemal žiadne nastavenia.

"K dispozícii je novšia revízia" znamená, že profil skupiny bol zmenený a uložený, ale nie je priradený. Profil skupiny sa musí priradiť pomocou "Priradiť teraz" na úrovni skupiny, aby sa zmeny uplatnili na zariadeniach.

Protokol zariadenia (len na úrovni zariadenia)

Denník príkazov

Tu môžete vidieť, ktoré príkazy boli pre zariadenie vydané a aký je ich stav.



Príkazy vytvorené pomocou "System Automated" sú automaticky vytvorené systémom.

Možné stavy príkazov

Stlačené zariadenie	Do služby push (napr. APNS) bola odoslaná požiadavka na pripojenie, aby sa zariadenie pripojilo späť k serveru EMM.
Vytvorený príkaz	Príkaz bol vytvorený v systéme.
Odoslaný príkaz	Príkaz sa odoslal do zariadenia po jeho pripojení k serveru.
Vykonaný príkaz	Príkaz bol úspešne vykonaný.
Príkaz zlyhal	Príkaz zlyhal. *
Príkaz čiastočne zlyhal	V závislosti od operačného systému zariadenia môžu byť niektoré príkazy zoskupené. V tejto časti tejto skupiny príkazov zlyhali niektoré časti. *
Príkaz vykonaný, prípadne neúspešný	Príkaz bol vykonaný, ale možno nebol.
Príkaz Repushed	Príkaz bol opätovne odoslaný používateľom.
Vyradené	Príkaz bol zamietnutý. Napríklad preto, že bol nahradený iným príkazom alebo zariadenie bolo znovu zaregistrované a staré príkazy boli odstránené.

*Ak je za správou výkričník, môžete získať ďalšie informácie, ak kurzorom prejdete na ikonu.

Správa aktív (len na úrovni zariadenia)

Informácie o zariadení

Číslo modelu	Číslo modelu
Názov hostiteľa	Názov hostiteľa
Miestne meno hostiteľa	Miestne meno hostiteľa
Operačný systém	Operačný systém
Verzia operačného systému	Verzia operačného systému
UDID	UDID
Voľná / celková pamäť	Voľná / celková pamäť

WiFi

IP adresa	IP adresa
WiFi MAC	WiFi MAC

Cellular

Telefónne číslo	Telefónne číslo
Stav roamingu	Stav roamingu
Roaming (hlas / dáta)	Roaming (hlas / dáta)
IP adresa	IP adresa
Prevádzkovateľ/prepravca	Prevádzkovateľ/prepravca
Sieť operátora SIM	Sieť dopravcov
Verzia nosiča	Verzia nosiča
ICCID	ICCID
Súčasné MCC/MNC	Súčasné MCC/MNC
SIM MCC/MNC	SIM MCC/MNC

Bluetooth

Bluetooth MAC	Bluetooth MAC

Správa aktualizácií (len na úrovni zariadenia)

Aktualizácia informácií

Na tejto karte sa zobrazujú informácie o nastaveniach aktualizácie systému v zariadení.

Automatická kontrola povolená	Ak systém kontroluje aktualizáciu automaticky.
Povolená automatická aktualizácia aplikácií	Ak systém automaticky nainštaluje aktualizácie aplikácií.
Povolené automatické aktualizácie operačného systému	Ak systém nainštaluje aktualizácie OS automaticky.
Povolené automatické aktualizácie zabezpečenia	Ak systém automaticky nainštaluje aktualizácie zabezpečenia.
Aktualizácia aplikácie na pozadí - stiahnutie povolené	Ak bude systém sťahovať aktualizácie aplikácií na pozadí.
Adresa URL katalógu	Adresa URL katalógu aktualizácií softvéru, ktorý klient používa.
Je predvolený katalóg	Ak je "áno", Katalóg je predvolený katalóg.
Vykonávanie pravidelnej kontroly	Ak "áno", spustite nové skenovanie.
Dátum predchádzajúceho skenovania	Dátum poslednej kontroly aktualizácie softvéru.
Výsledok predchádzajúceho skenovania	Kód výsledku poslednej kontroly aktualizácie softvéru.

Riadenie bezpečnosti

Ochrana proti krádeži

Utrite a uzamknite

Úplné utretie	Odoslanie príkazu na obnovenie výrobných nastavení zariadenia
Podnik Wipe	Odstránenie MDM zo zariadenia a odstránenie všetkých údajov MDM (napr. účtov, aplikácií)
Uzamknutie obrazovky	Návrat zariadenia na uzamknutú obrazovku

Konfigurácia zabezpečenia

Prístupový kód

Povolená deaktivácia kódu	Určuje, či je používateľ nútený nastaviť kód PIN. Jednoduché nastavenie tejto hodnoty (a nie iných) núti používateľa zadať prístupový kód bez určenia dĺžky alebo kvality.
Povolenie jednoduchej hodnoty	Umožniť používateľovi používať rovnaké, stupňujúce sa a znižujúce sa číselné reťazce (napr. 1234, 1111)
Vyžadovať alfanumerickú hodnotu	Heslá musia obsahovať aspoň jedno písmeno
Minimálna dĺžka prístupového kódu	Minimálna dĺžka hesla
Minimálny počet zložených znakov	Minimálny počet alfanumerických symbolov v hesle
Maximálny vek prístupového kódu	Počet dní, po ktorých sa musí heslo zmeniť
Maximálny automatický zámok	Maximálny čas, po uplynutí ktorého sa zariadenie uzamkne
Maximálna doba odkladu na zablokovanie zariadenia	Čas, počas ktorého môže byť zariadenie uzamknuté bez výzvy na zadanie prístupového kódu pri odomknutí
Maximálny vek prístupového kódu (1-730 dní alebo žiadny)	Dni, po ktorých sa musí zmeniť prístupový kód
História prístupových kódov (1-50 prístupových kódov alebo žiadny)	Počet jedinečných prístupových kódov pred opakovaným použitím

Certifikát

PKCS#1	
Popis	Zadajte opis certifikátu
Potvrdenie	Nahratie súboru pkcs1

PKCS#12	
Popis	Zadajte opis certifikátu
Potvrdenie	Nahratie súboru pkcs12

Nastavenia obmedzenia

Funkčnosť zariadenia

Povoliť fotoaparát	Povolenie používania fotoaparátu
Povolenie služby Game Center	Ak je hodnota nepravdivá, služba Game Center je vypnutá a jej ikona je odstránená z domovskej obrazovky.
Umožniť hranie pre viacerých hráčov	Ak je hodnota false, zakazuje hranie hier pre viacerých hráčov.
Povolenie pridávania priateľov do služby Game Center	Ak je hodnota false, zakazuje pridávanie priateľov do služby Game Center.
Povolenie knižnice fotografií iCloud	Ak je nastavená na hodnotu false, zakáže iCloud Photo Library. Všetky fotografie, ktoré neboli úplne stiahnuté z iCloud Photo Library do zariadenia, sa odstránia z miestneho úložiska.
Povolenie identifikácie dotykom	Ak je false, zabráni odomknutiu zariadenia pomocou Touch ID.

iCloud

Blokovanie určitých funkcií počas párovania iCloud

Povolenie synchronizácie dokumentov	Povolenie synchronizácie dokumentov
Povolenie synchronizácie iCloud Keychain	Povolenie synchronizácie iCloud Keychain
Povolenie poznámok iCloud	Keď je false, zakáže služby iCloud Notes v systéme MacOS
Povolenie iCloud BTMM	Ak je hodnota false, zakáže službu iCloud v systéme MacOS Back to My Mac.
Povolenie iCloud FMM	Ak je hodnota false, zakáže službu iCloud v systéme MacOS Find My Mac.
Povolenie záložiek iCloud	Ak je hodnota false, zakáže synchronizáciu záložiek MacOS iCloud.
Povolenie služby iCloud Mail	Ak je hodnota false, zakáže služby iCloud v systéme MacOS Mail.

Povolenie kalendára iCloud	Ak je hodnota false, zakáže služby iCloud v systéme MacOS Cloud.
Povolenie pripomienok iCloud	Ak je hodnota false, zakáže služby iCloud Reminder.
Povolenie služby iCloud Addressbook	Ak je hodnota false, zakáže služby MacOS iCloud Address Book.

Manažment médií

Vysunutie pri odhlásení	Vysunutie všetkých vymeniteľných médií pri odhlásení
Povoliť sieť	Povolenie prístupu pre sieťové médiá
Povolenie interného disku	Povolenie prístupu pre interný disk.
Vyžadovať overenie	Vyžadovať overenie pre používanie tohto média
Len na čítanie	Používateľ môže z média čítať iba údaje
Povolenie externého disku	Povolenie prístupu pre externý disk.
Vyžadovať overenie	Vyžadovať overenie pre používanie tohto média
Len na čítanie	Používateľ môže z média čítať iba údaje
Povolenie používania obrazov diskov	Povolenie prístupu pre obrázky.
Vyžadovať overenie	Vyžadovať overenie pre používanie tohto média
Len na čítanie	Používateľ môže z média čítať iba údaje
Povolenie používania diskov DVD-RAM	Povolenie prístupu pre disk DVD-RAM.
Vyžadovať overenie	Vyžadovať overenie pre používanie tohto média
Len na čítanie	Používateľ môže z média čítať iba údaje
Povolenie používania diskov DVD	Povolenie prístupu k disku DVD.
Vyžadovať overenie	Vyžadovať overenie pre používanie tohto média
Povolenie používania diskov CD	Povolenie prístupu pre disk CD.
Vyžadovať overenie	Vyžadovať overenie pre používanie tohto média

Správa pripojenia

Wi-Fi

Tu môžete pridávať a konfigurovať pripojenia Wi-Fi

Identifikátor súboru služieb (SSID)	SSID siete, ku ktorej sa vytvorí pripojenie
Automatické pripojenie	Povolenie automatického pripojenia k sieti
Skrytá sieť	Povoliť v prípade, že prístupový bod nevysiela SSID
Nastavenie servera proxy	Konfigurácia proxy servera pre každý prístupový bod
Žiadne	Nepoužívajte proxy server
Manuálne	Zriadenie manuálneho zástupcu
Adresa URL servera proxy	Adresa pre prístup k nastaveniam proxy servera
Prístav	Nastavenie portu pre proxy server
Overovanie	Meno používateľa pre overovanie na serveri Proxy
Heslo	Heslo pre overovanie na serveri Proxy
Automatické	Automatické vytvorenie proxy servera
Adresa URL servera proxy	Adresa URL pre súbor s nastaveniami proxy servera
Typ zabezpečenia	Vytvorenie typu zabezpečenia pre prístupový bod
WEP	
Heslo	Heslo pre AP
WPA/WPA2	
Heslo	Heslo pre AP
WEP Enterprise - WPA / WPA2 Enterprise / Akýkoľvek podnik	Pozri tabuľku Chyba: Zdroj odkazu nebol nájdený nižšie
Žiadne	Nezaviesť žiadnu bezpečnosť
Zakázanie náhodného výberu adresy MAC	Zakáže náhodné nastavenie adresy MAC pre danú sieť Wi-Fi, kým je pridružená k sieti. Tým sa v Nastaveniach zobrazí aj upozornenie na

	ochranu súkromia, ktoré naznačuje, že sieť má zníženú ochranu súkromia.

Konfigurácia podnikovej siete Wi-Fi

Poznámka: K dispozícii len vtedy, keď je položka "Typ zabezpečenia" nastavená na typ Enterprise.

Protokoly	Protokol overovania podporovaný v cieľovej sieti
TLS	Povolenie / zakázanie používania
TTLS	Povolenie / zakázanie používania
Vnútorné overovanie	Autentifikačný protokol, ktorý by sa mal použiť: PAP, CHAP, MSCHAP, MSCHAPv2
LEAP	Povolenie / zakázanie používania
PEAP	Povolenie / zakázanie používania
EAP-FAST	Povolenie / zakázanie používania
EAP-SIM	Povolenie / zakázanie používania
Používanie PAC	Používanie systému PAC (Protected Access Control)
Ustanovenie PAC	Konfigurácia Provision PAC
Anonymné poskytovanie PAC	Anonymné poskytovanie PAC
Overovanie	
Používateľské meno	Používateľské meno na overovanie
Nepoužívajte Na pripojenie Heslo	Nepoužívajte heslo na pripojenie
Heslo	Heslo, ktoré sa má použiť
Certifikát totožnosti	Nahratie/výber certifikátu overenia
Vonkajšia identita	Identita, ktorá je viditeľná navonok
Trust	
Dôveryhodný certifikát 1	Nahratie prvého dôveryhodného certifikátu
Dôveryhodný certifikát 2	Nahratie druhého dôveryhodného certifikátu
Dôveryhodný certifikát 3	Nahratie tretieho dôveryhodného certifikátu
Dôveryhodný server Názvy certifikátov	Názvy očakávaných certifikátov servera (v zozname oddelenom čiarkou)

VPN

V závislosti od vybraného typu pripojenia sa môžu zobraziť rôzne polia.

Názov pripojenia	Názov profilu VPN
Typ VPN	
VPN	Všetka sieťová prevádzka zariadenia bude smerovaná cez pripojenie VPN.
Typ pripojenia	Vytvorenie typu pripojenia VPN
IPsec (cisco)	Protokol IPsec od spoločnosti cisco
L2TP	Protokol L2TP
Vlastné SSL	Pripojenie prostredníctvom vlastného protokolu SSL
IKEv2	Protokol IKEv2
Nastavenie servera proxy	Konfigurácia proxy servera pre pripojenie VPN
Žiadne	Zriadenie bez splnomocnenia
Manuálne	Ručné vytvorenie servera Proxy
Adresa URL servera proxy	Adresa pre prístup k nastaveniam proxy servera
Prístav	Nastavenie portu pre proxy server
Overovanie	Používateľské meno pre overovanie na serveri Proxy
Heslo	Heslo pre overovanie na serveri Proxy
Automatické	Automatické vytvorenie proxy servera
Adresa URL servera proxy	URL adresa pre prístup k nastaveniam proxy servera

Proxy server HTTP

Typ proxy servera	
Manuálne	Zriadenie proxy servera manuálne
Adresa URL servera proxy	Adresa pre prístup k nastaveniam proxy servera
Prístav	Zriadenie portu proxy servera
Overovanie	Používateľské meno pre overovanie na serveri Proxy
Heslo	Heslo pre overovanie na serveri Proxy
Automatické	Automatické vytvorenie proxy servera
Adresa URL proxy servera PAC	Adresa URL proxy servera PAC
Povolenie priameho pripojenia, ak je PAC nedostupný	Povolenie priameho pripojenia (bez VPN), ak je PAC nedostupný
Umožnenie obchádzania proxy servera na prístup k vlastným sieťam	Umožniť obídenie proxy servera na prístup k interným sieťam

AirPrint

IP adresa	IP adresa tlačiarne
Cesta k zdroju	Definitívna cesta k zariadeniu AirPrint

AirPlay

Názov zariadenia	Názov zariadenia
Heslo	Heslo párovania
Biela listina	Definovanie zoznamu zariadení, s ktorými sa zariadenie môže výlučne spárovať

Správa PIM

Exchange Active Sync

Názov účtu	Názov účtu.
E-mailová adresa	Adresa účtu (napr. max@company.com)
Názov hostiteľa servera	Interný názov hostiteľa
Prihlasovacie meno	"Doména" a "Prihlasovacie meno" musia byť prázdne, aby sa zariadenie spýtalo na používateľa.
Doména	"Doména" a "Prihlasovacie meno" musia byť prázdne, aby sa zariadenie spýtalo na používateľa. Ak je povolená konfigurácia brány ACL a pole Domain nie je prázdne, univerzálna brána AppTec360 overí zariadenie s nasledujúcim názvom "Domain\Login Name".
Heslo	Heslo pre účet (napr. secretUserPassword)
Minulé dni služby Mail to Sync	Počet posledných dní pošty, ktoré sa majú synchronizovať
Používanie protokolu SSL	Používanie protokolu SSL pre interného hostiteľa Exchange
Rozšírená možnosť	Zobraziť rozšírené možnosti
Port servera	Interný port
Cesta k serveru	Vnútorná cesta
Externý názov hostiteľa	Externý hostiteľ
Externý port	Externý port
Externá cesta	Externá cesta
Používanie protokolu SSL pre externé Exchange Host	Použitie protokolu SSL pre externého hostiteľa Exchange

E-mail

Nastavenie účtov POP3 / IMAP na zariadení koncového používateľa

Popis účtu	Názov des E-mailové kontá
Typ účtu	
IMAP	
Prefix cesty	Prefix cesty pre špeciálne priečinky
POP	
Zobrazované meno používateľa	Zobrazované meno používateľa
E-mailová adresa	E-mailová adresa používateľa

Prichádzajúca pošta	Nastavenia prichádzajúceho servera
Adresa poštového servera	Adresa poštového servera
Port poštového servera	Port poštového servera
Meno používateľa	Príslušné meno používateľa
Typ overovania	Typ overovania
Žiadne	Žiadny typ overovania
Heslo (len na úrovni zariadenia)	Výzva na zadanie hesla
MDM Challenge-Response	
NTLM	Overovanie NTLM
HTTP MD5 Digest	
Používanie protokolu SSL	V prípade potreby použite protokol SSL

Odchádzajúca pošta	Nastavenia odchádzajúceho servera
Adresa poštového servera	Adresa poštového servera
Port poštového servera	Port poštového servera
Meno používateľa	Príslušné meno používateľa
Typ overovania	
Žiadne	Žiadna metóda overovania
Heslo (len na úrovni zariadenia)	Výzva na zadanie hesla
MDM Challenge-Response	
NTLM	Overovanie NTLM
HTTP MD5 Digest	
Používanie protokolu SSL	V prípade potreby použite protokol SSL
Odchádzajúce heslo rovnaké ako prichádzajúce	Odchádzajúce heslo rovnaké ako prichádzajúce
Používajte len v pošte	Aktivácia, ak sa majú všetky odchádzajúce e-maily odosielať prostredníctvom aplikácie Mail-App

CalDav

Konfigurácia nastavenia a distribúcie účtu CalDav

Popis účtu	Zobrazovaný názov účtu
Názov hostiteľa	Názov hostiteľa a/alebo IP adresa
Prístav	Prístav účtu CalDav
Hlavná adresa URL	Hlavná adresa URL účtu
Používateľské meno	Príslušné používateľské meno CalDav
Heslo (len na úrovni zariadenia)	Príslušné heslo CalDav
Používanie protokolu SSL	V prípade potreby použite protokol SSL

CardDav

Konfigurácia nastavenia a distribúcie účtu CardDav

Popis účtu	Zobrazovaný názov účtu
Názov hostiteľa	Názov hostiteľa a/alebo IP adresa
Prístav	Port účtu CardDav
Hlavná adresa URL	Hlavná adresa URL účtu
Používateľské meno	Príslušné používateľské meno CardDav
Heslo (len na úrovni zariadenia)	Príslušné heslo CardDav
Používanie protokolu SSL	V prípade potreby použite protokol SSL

LDAP

V tejto oblasti nastavte pripojenie LDAP, aby ste umožnili dynamickú výmenu certifikátov medzi koncovým používateľským zariadením a adresárom Active Directory.

Upozorňujeme, že vybraný používateľ vyžaduje príslušné oprávnenie na čítanie.

Popis účtu	Popis účtu
Používateľské meno účtu	Používateľ pre prístup k LDAP
Heslo účtu	Heslo pre prístup k LDAP
Názov hostiteľa účtu	Názov hostiteľa/IP adresa servera LDAP
Používanie protokolu SSL	V prípade potreby použite protokol SSL

V druhej časti môžete definovať jednotlivé filtre na vyhľadávanie v registri LDAP.

Popis	Rozsah pôsobnosti	Vyhľadávacia základňa
Popis filtra	Úroveň vyhľadávania v registri LDAP	Definovanie jednotlivých filtrov

Prístrojový panel a podávanie správ

Nastavenia prístrojovej dosky

Tu si môžete pozrieť existujúce ovládacie panely, upraviť ich alebo vytvoriť nové. Každý panel má vlastnú sadu údajov na zobrazenie a konfiguráciu grafov.

Ovládanie nastavení prístrojovej dosky

Verejnosť	Nastaví panel Dashboard na verejný, aby ho mohli vidieť aj ostatní používatelia. Používatelia musia mať samozrejme možnosť prihlásiť sa a zobraziť Dashboardy. Ak nie je aktivovaná možnosť "Public" (Verejný), môže ho vidieť len jeho tvorca.
Predvolené nastavenie	Nastaví prístrojový panel ako predvolený, takže sa automaticky otvorí pri ďalšom prístupe k zobrazeniu prístrojového panelu.
	Zobrazenie prístrojovej dosky a jej grafov
	Odstránenie prístrojovej dosky
	Úprava názvu a nastavení prístrojovej dosky
	Vytvorenie kópie prístrojovej dosky
	Pridanie úplne nového prístrojového panela

Zobrazenie prístrojovej dosky

Zobrazia sa údaje a grafy vybraného panela a môžete ich aj zmeniť.

Ovládanie prístrojovej dosky

	Umožňuje definovať, ktoré údaje sa majú zobrazovať na informačnom paneli, množstvo údajov, ktoré sa majú zobrazovať, a veľkosť, v akej sa majú tieto údaje zobrazovať.
	Prenesie vás späť na prehľad prístrojového panela
	Obnovenie predvoleného nastavenia aktuálne otvoreného prístrojového panela
	Uloží všetky zmeny, ktoré ste vykonali na aktuálne otvorenom paneli (napr. ktoré údaje sa majú zobraziť).
	Zmena typu grafu na stĺpcový graf
	Zmena typu grafu na koláčový graf
	Zmeniť typ grafu na graf koblihy
	Zmena typu grafu na graf polárnej oblasti
	Zmena poradia triedenia

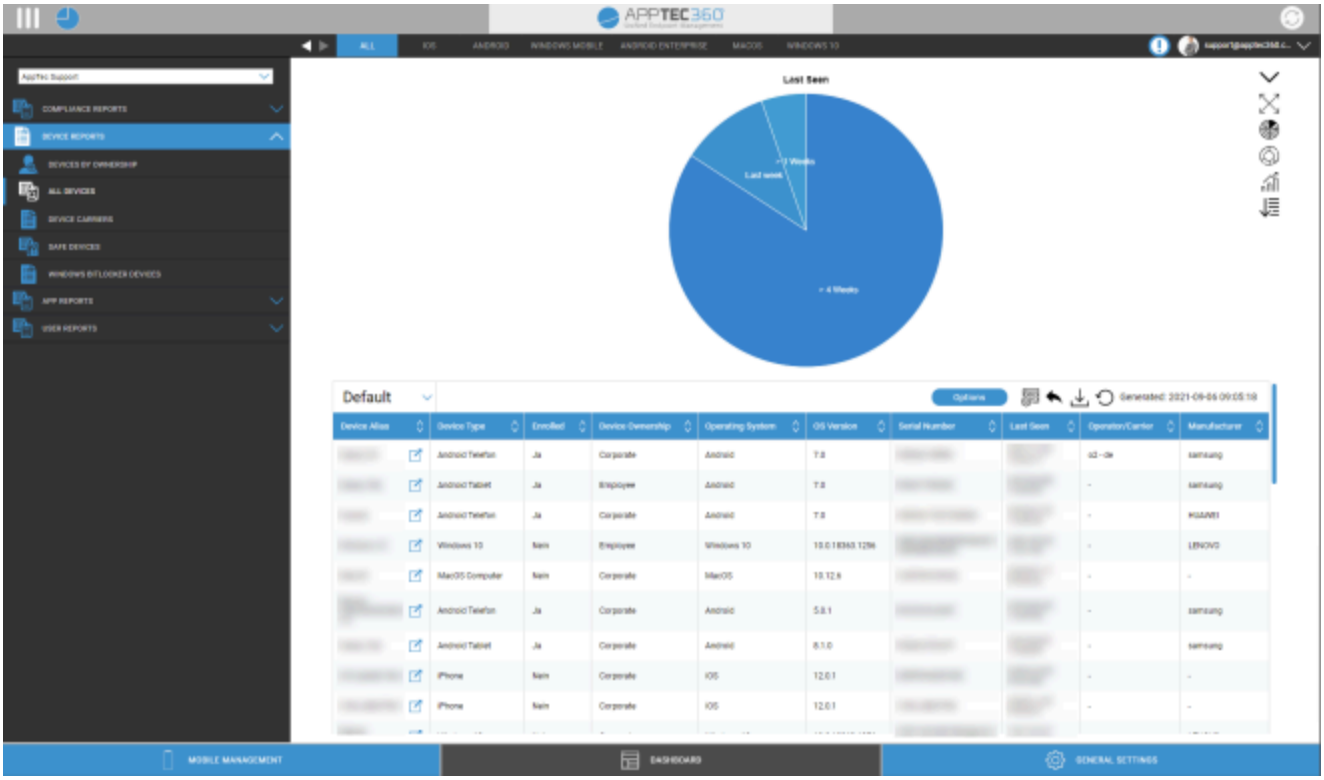
Rozšírené podávanie správ

"Rozšírené hlásenia" ponúkajú podrobné prehľady a grafy informácií o zariadení a používateľoch.

Existuje niekoľko predvolených zostáv, ale všetky sa dajú ručne zmeniť a pridať alebo odstrániť údaje, ktoré sa majú zobraziť.

Upozorňujeme, že údaje, ktoré sa zobrazujú, môžete meniť len manuálne. Vybraná kategória hlásenia definuje údaje, na ktorých sa zakladá. Napr. v prehľade Zariadenia všetky zariadenia iOS nikdy nebudete môcť zobraziť zariadenia so systémom Android

V ľavom hornom rohu môžete obmedziť údaje hlásenia na určitú skupinu (a všetky jej podskupiny). V predvolenom nastavení je táto skupina nastavená na váš koreňový uzol, takže sa zohľadňujú VŠETKY zariadenia a používatelia.



Rozšírená kontrola hlásení

V každom prehľade môžete použiť nasledujúce funkcie na ľubovoľnú zmenu správy:

	Skryť graf (ak je graf zobrazený)
	Zobraziť graf (ak je graf skrytý)
	Rozbaliť graf (Ak je graf zbalený)
	Zložiť graf (Ak je graf rozbalený)
	Zmena typu grafu na stĺpcový graf
	Zmena typu grafu na koláčový graf
	Zmeniť typ grafu na graf koblihy
	Zmena typu grafu na graf polárnej oblasti
	Zmena poradia triedenia
	Upravte nasledujúce časti zobrazeného prehľadu: • Pridanie/odstránenie stĺpcov • Určenie poradia zobrazenia stĺpcov • Zobraziť/skryť graf nad tabuľkou • Vyberte stĺpec, ktorý sa použije pre graf • Filtrovanie údajov v tabuľke
	Otvorenie správcu nastavení na ukladanie a načítanie rôznych správ
	Obnoví predvolené nastavenie aktuálne otvorenej správy
	Exportovať aktuálnu správu ako súbor .csv
	Regenerácia údajov a opätovné načítanie aktuálnej správy

Zoznam všetkých predvolených zostáv nájdete na ďalších stranách.

Správy o dodržiavaní predpisov

Zakorenené zariadenia

Prehľad zariadení, ktoré boli rootnuté/prelomené.

Predvolené stĺpce tejto správy:

Alias zariadenia
Vlastník zariadenia
E-mail
Operačný systém
Telefónne číslo
Naposledy videné
Výrobca

Roamingové zariadenia

Prehľad všetkých zariadení, ktoré sú v roamingu

Predvolené stĺpce tejto správy:

Alias zariadenia
Vlastník zariadenia
E-mail
Typ zariadenia
Operačný systém
Telefónne číslo
Naposledy videné

Zariadenia s povoleným roamingom

Prehľad všetkých zariadení, ktoré majú aktivovaný roaming, ale nemusia byť práve v roamingu.

Predvolené stĺpce tejto správy:

Alias zariadenia
Vlastník zariadenia
E-mail
Typ zariadenia
Operačný systém
Telefónne číslo
Naposledy videné

Zariadenia pod dohľadom

Prehľad všetkých zariadení, ktoré sú pod dohľadom v režime pod dohľadom (len iOS)

Predvolené stĺpce tejto správy:

Alias zariadenia
Vlastník zariadenia
E-mail
Typ zariadenia
Naposledy videné

Neaktívne zariadenia

Prehľad všetkých zariadení, ktoré sa za posledných 7 dní nepripojili k serveru

Predvolené stĺpce tejto správy:

Alias zariadenia
Vlastník zariadenia
E-mail
Typ zariadenia
Operačný systém
Naposledy videné

Správy o zariadení

Zariadenia podľa vlastníctva

Tu môžete vidieť, koľko zariadení bolo aktuálne nasadených ako podnikové (firemné zariadenia) a zamestnanecké (súkromné zariadenia).

Predvolené stĺpce tejto správy:

Alias zariadenia
Vlastník zariadenia
Typ zariadenia
Vlastníctvo zariadenia
Operačný systém

Všetky zariadenia

Tu si môžete pozrieť prehľad všetkých zariadení s najdôležitejšími informáciami.

Predvolené stĺpce tejto správy:

Alias zariadenia
Typ zariadenia
Zapísaný
Vlastníctvo zariadenia
Operačný systém
Verzia operačného systému
Sériové číslo
Naposledy videné
Prevádzkovateľ/prepravca
Výrobca

Nosiče zariadení

Tu si môžete pozrieť prehľad operátora (mobilného operátora).

Predvolené stĺpce tejto správy:

Alias zariadenia
Vlastník zariadenia
E-mail
Operačný systém
Verzia operačného systému
Prevádzkovateľ/prepravca

Zariadenia SAFE

Tu si môžete pozrieť prehľad zariadení, ktoré používajú verziu SAFE.

Keďže prehľad a/alebo SAFE je k dispozícii len pre zariadenia Samsung, pod týmto bodom sa nezobrazia obvyklé karty.

Predvolené stĺpce tejto správy:

Alias zariadenia
Vlastník zariadenia
E-mail
Typ zariadenia
Naposledy videné
Verzia SAFE

Zariadenia so systémom Windows BitLocker

Tu si môžete pozrieť prehľad zariadení so systémom Windows, ktoré používajú nástroj BitLocker.

Predvolené stĺpce tejto správy:

Alias zariadenia
Vlastník zariadenia
E-mail

Stav nástroja BitLocker

Správy o aplikáciách

Tu získate rôzne prehľady týkajúce sa aplikácií. Vo všetkých týchto prehľadoch môžete kliknutím na položku ďalej zistiť, ktoré verzie sú nainštalované v zariadeniach a ako často. V tomto zobrazení môžete opäť kliknúť na konkrétnu verziu, aby ste videli, v ktorých zariadeniach je táto konkrétna verzia nainštalovaná.

Poznámka: Môže trvať určitý čas, kým systém získa aktuálne informácie zo zariadenia. Okrem toho sa správy neaktualizujú každú minútu. Ak ste práve priradili novú aplikáciu alebo verziu, možno budete musieť byť trpezliví, aby ste videli aktuálny stav. Ručné opätovné načítanie správy prinúti správu zobraziť najaktuálnejšie dostupné údaje

Nainštalované aplikácie

Tu získate prehľad o všetkých nainštalovaných aplikáciách.

Predvolené stĺpce tejto správy:

Názov	Názov príslušnej aplikácie a/alebo služby
Identifikátor	Určité ID aplikácie/služby
Celkový počet	Ako často bola táto aplikácia/služba nainštalovaná na zariadeniach koncových používateľov

Najviac nainštalovaných aplikácií

Tu získate prehľad o aplikáciách, ktoré boli nainštalované najčastejšie.

Predvolené stĺpce tejto správy:

Názov	Názov príslušnej aplikácie a/alebo služby
Identifikátor	Určité ID aplikácie/služby
Celkový počet	Ako často bola táto aplikácia/služba nainštalovaná na zariadeniach koncových používateľov

Povinné aplikácie

Tu získate prehľad povinných (povinne vyžadovaných) aplikácií.

Predvolené stĺpce tejto správy:

Názov	Názov príslušnej aplikácie a/alebo služby
Identifikátor	Určité ID aplikácie/služby
Zdroj aplikácie	O ktorý AppStore ide: • Google PlayStore (Android) • iTunes AppStore (iOS)
OS	Operačný systém

Aplikácie na čiernej listine

Tu získate prehľad o všetkých definovaných aplikáciách na čiernej listine.

Predvolené stĺpce tejto správy:

Názov	Názov príslušnej aplikácie a/alebo služby
Identifikátor	Určité ID aplikácie/služby
Zdroj aplikácie	O ktorý AppStore ide: • Google PlayStore (Android) • iTunes AppStore (iOS)
OS	Operačný systém

Správy používateľov

Tarifa

Tu získate prehľad o telefónnych tarifách a kartách SIM svojich používateľov.

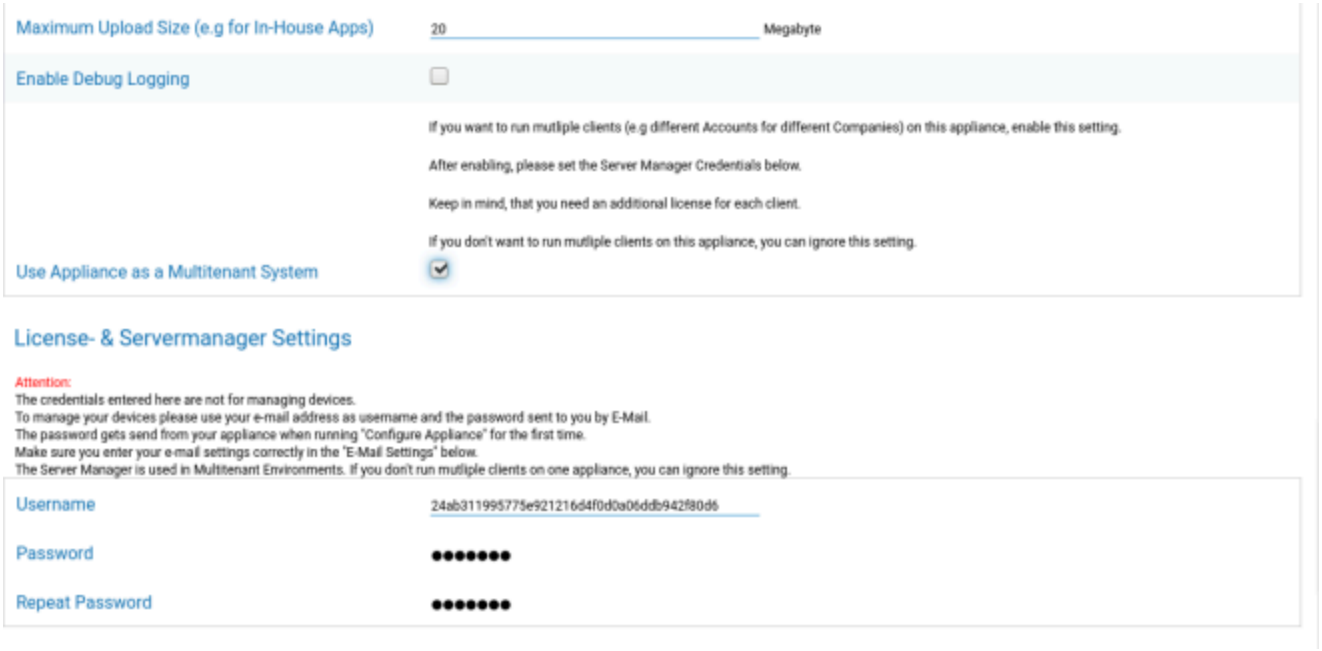
Predvolené stĺpce tejto správy:

E-mail
Názov
phoneNumber
nosič
tarifa
možnosť
cena
zmluvaZrušená
contractStart
duringTime
mobileAndData
dataVolume
multiSIM
typ
simCardSerial1
simCardSerial2
simCardSerial3
pin1
pin2
puk1
puk2
Poznámka

Správa viacerých nájomníkov

Systém AppTec360 EMM dokáže hostiť viacero samostatných nájomcov, z ktorých každý má vlastných používateľov a skupiny, oprávnenia a globálne nastavenia.

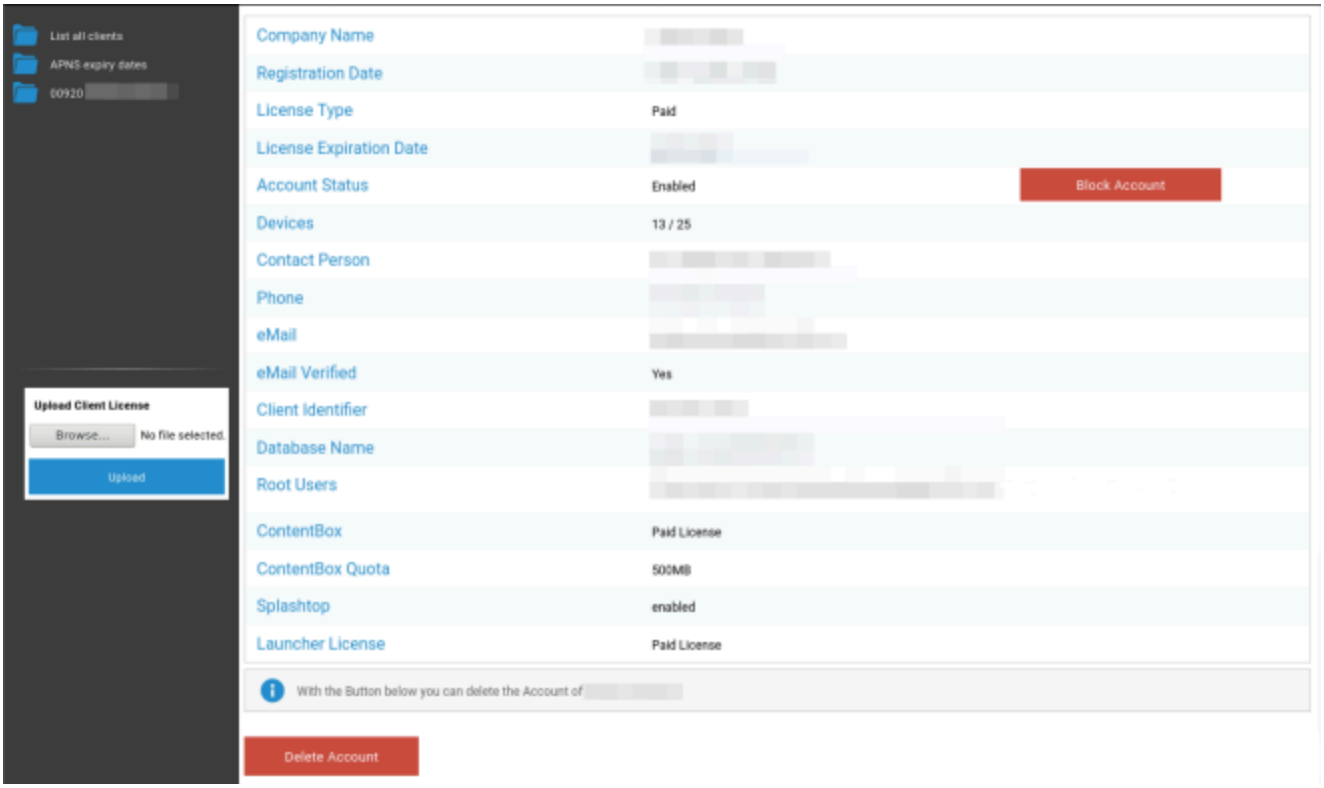
Ak chcete povoliť funkciu Multitenant, musíte ju povoliť v konfiguračnom rozhraní zariadenia v "treťom kroku - Nastavenia servera".



V novej ponuke nastavte používateľské meno a heslo pre správcu servera. Uložte nastavenia a spustite "Konfigurácia zariadenia" v "Piatom kroku - Licenčná zmluva", aby ste použili nastavenie.

Po dokončení konfigurácie sa môžete prihlásiť pomocou nastavených poverení cez bežné rozhranie správy mobilných zariadení.

Po prihlásení sa zobrazí nasledujúce zobrazenie.



Vľavo vidíte všetkých nájomcov (v tomto prípade len jedného s id 920) a vpravo informácie o tomto klientovi. Máte tiež možnosť zablokovať prístup k účtu, ako aj odstrániť klienta (POZOR: Tým sa odstránia všetky údaje týkajúce sa tohto klienta).

Vľavo môžete nahrať novú klientsku licenciu, ktorá môže byť buď aktualizáciou licencie pre existujúceho klienta, alebo novou licenciou, ktorá automaticky vytvorí nového klienta. Po vytvorení nového klienta sa na e-mailovú adresu, pre ktorú bola licencia vydaná, automaticky odošle e-mail obsahujúci prihlasovacie heslo.

Ak chcete získať novú alebo aktualizovanú klientsku licenciu (napr. ak potrebujete viac licencií pre zariadenia), obráťte sa na svojho obchodného zástupcu.

Ďalšie názory

Zoznam všetkých klientov

Zobrazí prehľad všetkých klientov v systéme.

ID klienta	ID klienta
Identifikátor	Identifikátor klienta
Databáza	Databáza
Názov spoločnosti	Názov spoločnosti
E-mail	Kontaktná osoba eMail
Overené	Či je e-mail kontaktnej osoby overený alebo nie
Krajina	Krajina
Zariadenia	Počet registrovaných zariadení
Dátum registrácie	Bod v čase pridelenia licencie
Posledné prihlásenie	Posledné prihlásenie do konta správcu
Licencia	Zobrazenie typu licencie (Free|Paid)
Licencia CB	Typ licencie ContentBox (Bezplatná|platená)
Stav	Aktuálny stav AppTec-Client
Vypršala platnosť	Zobrazí, ak licencia vypršala
iOS	Počet zariadení iOS
Android	Počet zariadení so systémom Android
Windows Mobile	Počet zariadení so systémom Windows Mobile
MacOS	Počet zariadení so systémom MacOS
Windows 10	Počet zariadení so systémom Windows 10
Android Enterprise	Počet podnikových zariadení so systémom Android
IOS BYOD (registrácia používateľov)	Počet zariadení IOS BYOD (registrácia používateľov)
IoT	Počet zariadení IoT

Dátumy skončenia platnosti APNS

Zobrazuje prehľad všetkých dátumov vypršania platnosti certifikátov APNS všetkých klientov.

ID klienta	ID klienta
Názov spoločnosti	Názov spoločnosti
Dátum skončenia platnosti	Dátum skončenia platnosti certifikátu Apple APNS
Informácie	Informácie o uplynutí platnosti

Kontakt

Ďalšie otázky? Jednoducho nás kontaktujte v sekcii:

Všeobecné technické otázky

support@apptec360.com

+41 61 511 3210

Otázky týkajúce sa inštalácie virtuálneho zariadenia

consulting@apptec360.com

+41 61 511 3214

Zrieknutie sa zodpovednosti