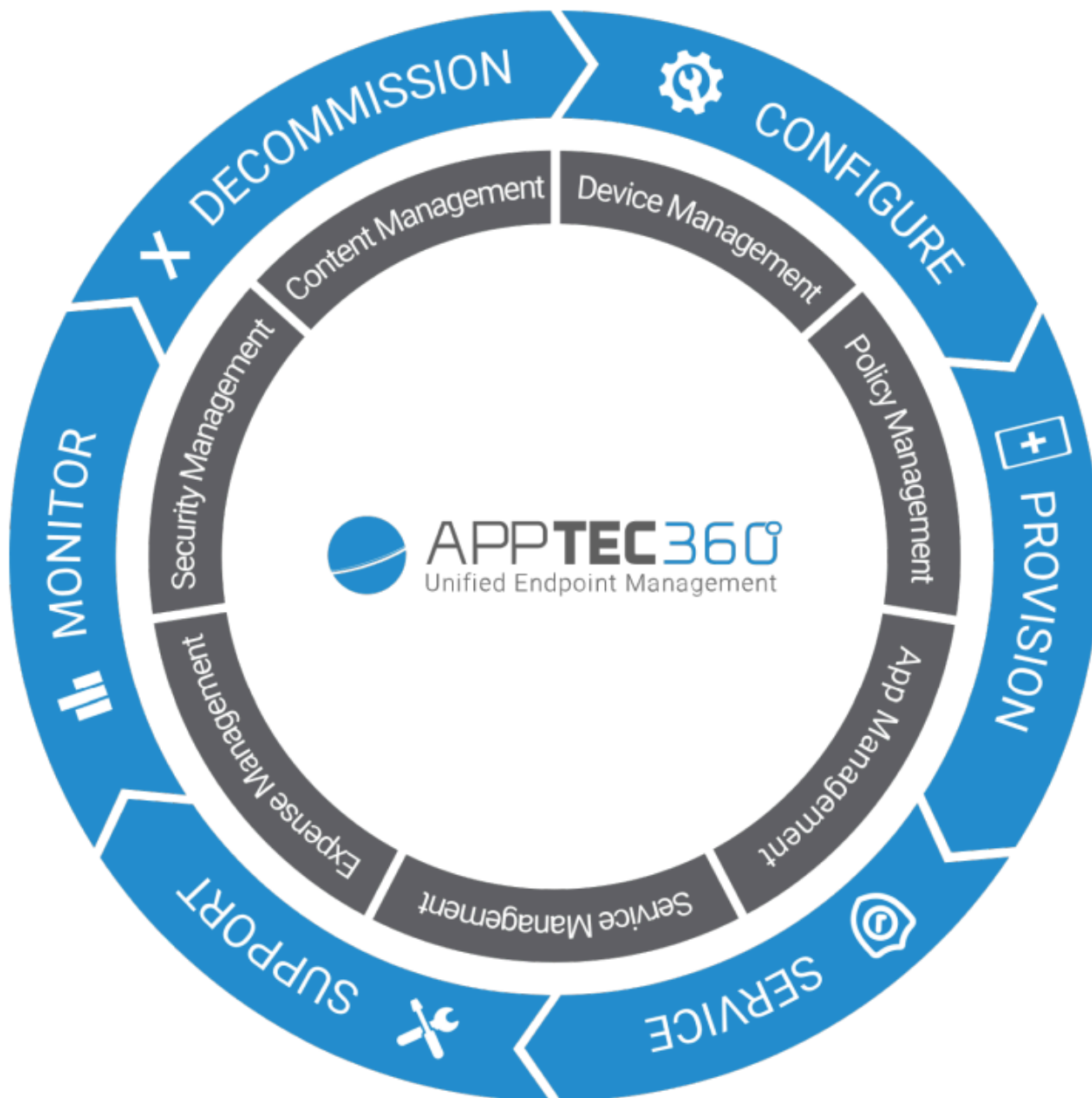


AppTec360 Enterprise Mobile Manager in ContentBox

Priročnik za upravljanje | Različica 5.0 (202110)



Kazalo vsebine

Splošni pregled

Uvod v AppTec360

Podprti operacijski sistemi naprav

Podprti imeniki LDAP

Razlaga “nadzorovanega načina” v napravah Apple

Na voljo v nadzorovanem načinu

Aktivacija nadzorovanega načina

Dodajanje naprave v DEP

Razlaga sistema Android Enterprise

Kaj je Android Enterprise?

Kakšne so zahteve za uporabo sistema Android Enterprise?.

Kateri načini so na voljo v sistemu Android Enterprise?

Kako lahko dodelim aplikacije napravam Android Enterprise?

Prenos lastnih aplikacij v trgovino Google Play

Zahteve in namestitvev

Zahteve

Sistemske zahteve

Licenčni ključ

Reševanje naslovov IP in DNS

SSL-certifikat

Strežnik SMTP

Pravila požarnega zidu

Varnostne posodobitve

Privzeta gesla navidezne naprave

Konfiguracija navidezne naprave

Priprava

Konfiguracija iz zunanjega gostitelja

Prvi korak – Licenca naprave

Drugi korak – certifikat SSL

Samodejno

- Po meri

- Tretji korak – Nastavitve strežnika

- Četrty korak – Nastavitev MySQL

- Peti korak – licenčna pogodba

- Odpravljanje težav

- Varnostna priporočila

Splošne nastavitve

Pregled računa

- Informacije o računu

- Pregled

- Poročilo o napaki

- Zahteva za funkcijo

Globalna konfiguracija

- Nastavitve elektronske pošte

- Predloge za elektronsko pošto

- Vpis SMS

Zasebnost

- Dostop do GPS

Dostop na podlagi vlog

- Upravljanje vlog

- Dodelitve vlog

- Dodelitev vloge

- Dostop do API

- Dostop do vmesnika AppTec360 REST API

- Splošna pravila

- Primer zahteve

- Poizvedbe

- Primer kode v Pythonu3

Konfiguracija Apple

- Certifikat APNS

- Korak 1

- Korak 2

- Korak 3

- Upravljeni dostop

- Vpis uporabnika

- Skupni iPad

- DEP

- Konfigurator in URL

- URL-ji za vpis v bazen

- Profil MDM – Apple Configurator

Konfiguracija sistema Android

- Konfiguracija sistema Android

- Samodejni vpis

- Android Enterprise

- Prva metoda: Android Enterprise Account (Google račun)

- Druga metoda: Račun G-Suite

- Zaščita pred ponastavitvijo tovarniških nastavitev

- AE Vpis

- Metoda 1: Vpis kode QR

- Metoda 2: Vpis NFC

- Metoda 3: Google račun

- KNOX Vpis

- Brez dotika

Konfiguracija sistema Windows

- Konfiguracija sistema Windows

Vsebinsko polje

- Konfiguracija

Konfiguracija LDAP

- Pregled protokola LDAP

Upravljanje aplikacij

- Notranja aplikacija DB

- Android

- iOS

- MacOS

- Windows 10

- Nastavitve aplikacije

- Nastavitve aplikacije iOS

- Nastavitve aplikacije Android

Aplikacije tretjih oseb

- Android
- iOS

VPP / KNOX Premium

- Licence VPP
- Žeton VPP
- Ključ KNOX Premium

Nastavitve trgovine App Store

- Regija in jezik

Trgovina AE Play

- Odobrene aplikacije
- Aplikacije v Trgovini Play
- Zasebne aplikacije
- Spletne aplikacije
- Postavitve trgovine

Paket aplikacij

Daljinski upravljalnik

TeamViewer

- Povezovalnik TeamViewer
- Namestitev programa TeamViewer QuickSupport
- Daljinsko upravljanje naprave
- Dostop brez nadzora

Splashtop

Upravljanje kartice Sim

- Množični uvoz CSV
- Prevoznik in tarifa

Upravljanje naročnin

- Upravljanje naročnin

Splošni revizijski dnevnik

- Revizijski dnevnik
- Nastavitve revizijskega dnevnika

Upravljanje certifikatov

Upravljanje mobilnih naprav

Zaslon za upravljanje mobilnih naprav

- Filter naprave
- Iskalno okno
- Opcije orodja
- Navigacijske puščice

Nastavitve računa v administraciji

- Informacije o uporabniku
- Nastavitve konzole
- Prijavni dnevnik

Korporativna uprava (korensko vozlišče) v mobilnem upravljanju

- Ustvarjanje podskupine
- Preimenovanje korenkega vozlišča
- Množični vpis
- Dodelitev mase
- Hitro upravljanje aplikacij
- Uvoz uporabnika CSV

Upravljanje skupin v mobilnem upravljanju

- Ustvarjanje podskupine
- Urejanje izbrane skupine
- Brisanje izbrane skupine
- Ustvarjanje uporabnika
 - Ustvari novega uporabnika upravitelja

Upravljanje uporabnikov v mobilnem upravljanju

- Dodajanje in vpisovanje naprave

Upravljanje profilov v mobilnem upravljanju

- Ustvarite profil
- Urejanje profila
- Kopiranje profila
- Brisanje profila
- Dedovanje profilov

Upravljanje naprav v mobilnem upravljanju

- IOS
 - Urejanje naprave
 - Izbriši geslo
 - Naprava za zaklepanje

- Naprava za izklop
- Ponovni zagon naprave
- Alarm in način izgube | Onemogoči način izgube
- Brisanje naprave
- Brisanje naprave
- Brisanje v podjetju | Odstranitev MDM
- Pošlji sporočilo
- Daljinski nadzor TeamViewer
- Pošlji zahtevo za vpis

Android

- Urejanje naprave
- Izbriši geslo
- Naprava za zaklepanje
- Brisanje naprave
- Brisanje naprave
- Odstranitev MDM
- Pošlji sporočilo
- Preoblikovanje v način COPE
- Pošlji zahtevo za vpis
- Migracija starejše naprave

Windows

- Urejanje naprave
- Brisanje naprave
- Brisanje v podjetju | Odstranitev MDM
- Daljinski nadzor TeamViewer
- Pošlji zahtevo za vpis

Upravljanje vsebine

- Datoteke skupin
- Raziskovalec datotek
- Revizijska sled
- Odpadki
- Zunanje shranjevanje

Revizijski dnevnik

Konfiguracija sistema iOS

Splošno

- Pregled profila skupine (samo na ravni skupine)
- Splošne informacije
- Nastavitve
- Revizija konfiguracije
- Dnevnik naprave (samo na ravni naprave)
 - Dnevnik ukazov
 - Možni statusi ukazov

Upravljanje sredstev (samo na ravni naprave)

- Upravljanje sredstev (samo na ravni naprave)
 - Informacije o napravi
 - Wi-Fi
 - Cellular
 - Bluetooth

Upravljanje varnosti

- Zaščita pred krajo (samo na ravni naprave)
 - Informacije GPS (samo na ravni naprave)
 - Brisanje in zaklepanje (samo na ravni naprave)
 - Sporočilo (samo na ravni naprave)
- Varnostna konfiguracija
 - Pristopna koda
 - Potrdilo (samo na ravni naprave)
 - Šifriranje
 - Enotna prijava
- Konec življenjske dobe (samo na ravni naprave)
 - Brisanje (samo na ravni naprave)
- Nastavitve omejitev
 - Funkcionalnost naprave
 - iCloud
 - Varnost in zasebnost

BYOD

- Vgrajena varnost sistema iOS (vsebnik)
 - Aktivacija
 - SecurePIM Geslo

- Varnost SecurePIM
- Brskalnik SecurePIM
- Izmenjava

Upravljanje povezav

- Wi-Fi
 - Nastavitev posredniškega strežnika
 - Vrsta varnosti

VPN

- Vrsta VPN
 - VPN
 - VPN za posamezno aplikacijo
- Nastavitev posredniškega strežnika

APN

- Cellular
- Proxy strežnik HTTP
- AirPrint
- AirPlay

Upravljanje PIM

- Exchange Active Sync
- Elektronska pošta
 - Dohodna pošta
 - Odhodna pošta
- CalDav
- Naročeni koledarji
- LDAP

Spletno upravljanje

- Spletni posnetki
- Filter spletnih vsebin

Upravljanje aplikacij

- Upravitelj aplikacij za podjetja
 - Nameščene aplikacije (samo na ravni naprave)
 - Obvezne aplikacije
 - Možnosti namestitve
 - Spletne aplikacije

Omejitve in nastavitve

- Aplikacije na črnem seznamu / belem seznamu
- Omejitve aplikacije SysApp
- App-VPN
- Nastavitve aplikacije

Trgovina z aplikacijami za podjetja

- Aplikacije iTunes
- Lastna spletna stran

Način kioska

Vrsta uporabe

- Paket
- URL

Nastavitve načina Kiosk

Android Enterprise – Popolnoma upravljana konfiguracija naprav

Splošno

- Pregled profila skupine (samo na ravni skupine)
- Pregled naprave (samo na ravni naprave)
- Revizija konfiguracije (samo na ravni naprave)
- Dnevnik naprave (samo na ravni naprave)

Dnevnik ukazov

Možni statusi ukazov

Nastavitve naprave

- Konfiguracija odjemalca
- Ozadje

Upravljanje sredstev (samo na ravni naprave)

Informacije o napravi

Wi-Fi

Cellular

Bluetooth

Upravljanje varnosti

Zaščita pred krajo (samo na ravni naprave)

Informacije GPS (samo na ravni naprave)

Brisanje in zaklepanje (samo na ravni naprave)

Sporočilo (samo na ravni naprave)

Varnostna konfiguracija

- Pristopna koda naprave
- AntiVirus

Konec življenjske dobe (samo na ravni naprave)

- Brisanje (samo na ravni naprave)

Nastavitve omejitev

- Omejitve

Upravljanje certifikatov

Upravljanje povezav

Wifi

- Vrsta varnosti
 - WEP
 - WPA/WPA2
 - 802.1x EAP

VPN

- Vrsta VPN
 - VPN
 - VPN za posamezno aplikacijo

Omejitve

Upravljanje PIM

Gmail Exchange

Upravljanje aplikacij

Upravitelj aplikacij za podjetja

- Nameščene aplikacije (samo na ravni naprave)
- Sistemske aplikacije (samo na ravni naprave)
- Obvezne aplikacije
- Črna in bela lista
- Aplikacije sistema AE

Omejitve in nastavitve

- Nastavitve upravljanja aplikacij

Trgovina z aplikacijami za podjetja

- Lastna spletna stran

Trgovina Play za podjetja

- Trgovina AE Play

Način Kiosk in zaganjalnik

- Način kioska
- AppTec360 zaganjalnik
- Nastavitve AppTec360

Daljinski upravljavnik

- Splashtop
- TeamViewer

Upravljanje vsebine

- Vsebinsko polje
- Varen brskalnik

Dodatni API

- Samsung KNOX
 - Omejitve
 - E-pošta
 - Izmenjava
 - APN
 - Bluetooth
 - Povezava

Android Enterprise – Popolnoma upravljana naprava z delovnim profilom (COPE)

Splošna razlaga COPE

Konfiguracija profilov za naprave COPE

Vrnitev na popolnoma upravljano napravo AE

Android Enterprise – Konfiguracija zabojnika

Splošno

- Pregled profila (samo na ravni profila)
- Pregled profila skupine (samo na ravni skupine)
- Pregled naprave (samo na ravni naprave)
- Revizija konfiguracije
- Dnevnik naprave (samo na ravni naprave)
 - Dnevnik ukazov
 - Možni statusi ukazov
- Nastavitve naprave
 - Konfiguracija odjemalca

- | Ozadje

| Upravljanje sredstev (samo na ravni naprave)

- | Informacije o napravi

- | Wi-Fi

- | Cellular

- | Bluetooth

| Upravljanje varnosti

- | Zaščita pred krajo (samo na ravni naprave)

- | Informacije GPS (samo na ravni naprave)

- | Brisanje in zaklepanje (samo na ravni naprave)

- | Sporočilo (samo na ravni naprave)

- | Varnostna konfiguracija

- | Pristopna koda naprave

- | Pristopna koda zabojnika

- | AntiVirus

- | Konec življenjske dobe (samo na ravni naprave)

- | Brisanje (samo na ravni naprave)

- | Nastavitve omejitev

- | Omejitve

- | Upravljanje certifikatov

| Upravljanje povezav

- | Wifi

- | Vrsta varnosti

- | WEP

- | WPA/WPA2

- | 802.1x EAP

- | VPN

- | Vrsta VPN

- | VPN

- | VPN za posamezno aplikacijo

- | Omejitve

| Upravljanje PIM

- | Gmail Exchange

| Upravljanje aplikacij

- | Upravitelj aplikacij za podjetja

- Nameščene aplikacije (samo na ravni naprave)
- Sistemske aplikacije (samo na ravni naprave)
- Obvezne aplikacije
- Aplikacije sistema AE

Omejitve in nastavitve

- Nastavitve upravljanja aplikacij

Trgovina z aplikacijami za podjetja

- Lastna spletna stran

Trgovina Play za podjetja

- Trgovina AE Play

Upravljanje vsebine

- Vsebinsko polje
- Varen brskalnik

Konfiguracija sistema Android

Splošno

- Pregled profila skupine (samo na ravni skupine)
 - Pregled naprave (samo na ravni naprave)
- Revizija konfiguracije (samo na ravni naprave)
- Dnevnik naprave (samo na ravni naprave)
 - Dnevnik ukazov
 - Možni statusi ukazov
- Nastavitve naprave
 - Konfiguracija odjemalca
 - Ozadje

Upravljanje sredstev (samo na ravni naprave)

- Upravljanje sredstev
 - Informacije o napravi
 - Wi-Fi
 - Cellular
 - Bluetooth

Upravljanje varnosti

- Zaščita pred krajo (samo na ravni naprave)
 - Informacije GPS (samo na ravni naprave)
 - Brisanje in zaklepanje (samo na ravni naprave)

- | Sporočilo (samo na ravni naprave)

- | **Varnostna konfiguracija**

- | Pristopna koda

- | Šifriranje

- | AntiVirus

- | **Konec življenjske dobe (samo na ravni naprave)**

- | Brisanje (samo na ravni naprave)

- | **Nastavitve omejitev**

- | Omejitve

- | Lastnik naprave AE

- | **Zabojnik BYOD**

- | **Android Enterprise**

- | Android Enterprise

- | Gmail Exchange

- | Aplikacije sistema AE

- | Pristopna koda zabojnika

- | **Samsung KNOX**

- | Aktivacija

- | Pristopna koda Knox

- | Knox Security

- | Knox Exchange

- | Elektronska pošta Knox

- | Aplikacije Knox

- | **Upravljanje povezav**

- | **Wifi**

- | Vrsta varnosti

- | WEP

- | WPA/WPA2

- | 802.1x EAP

- | **VPN**

- | Omejitve

- | APN

- | Bluetooth

- | **Upravljanje PIM**

- | Izmenjava

- Elektronska pošta
- AE Gmail Exchange

Upravljanje aplikacij

- Upravitelj aplikacij za podjetja
 - Nameščene aplikacije (samo na ravni naprave)
 - Sistemske aplikacije (samo na ravni naprave)
 - Obvezne aplikacije
 - Aplikacije sistema AE

- Omejitve in nastavitve

- Črna in bela lista
- Omejitve aplikacij sistema
 - Aplikacije Samsung
 - Aplikacije Huawei

- Nastavitve upravljanja aplikacij

- Trgovina z aplikacijami za podjetja

- Trgovina Playstore
- Lastna spletna stran

- Trgovina Play za podjetja

- Način Kiosk in zaganjalnik

- Način kioska
- AppTec360 zaganjalnik
- Nastavitve AppTec360

Daljinski upravljalnik

- Splashtop
- Teamviewer

Upravljanje vsebine

- Vsebinsko polje
- Varen brskalnik

Konfiguracija Računalnik z operacijskim sistemom Windows 10

Splošno

- Pregled profila skupine (samo na ravni skupine)
- Pregled naprave (samo na ravni naprave)
- Nastavitve
- Revizija konfiguracije (samo na ravni naprave)

Dnevnik naprave (samo na ravni naprave)

- Dnevnik ukazov

- Možni statusi ukazov

Upravljanje sredstev (samo na ravni naprave)

- Informacije o napravi

- Cellular

- Informacije o sinhronizaciji

Upravljanje varnosti

- Zaščita pred krajo (samo na ravni naprave)

- Informacije GPS (samo na ravni naprave)

- Nastavitve GPS

- Varnostna konfiguracija

- Pristopna koda

- Protivirusni program

- Varnostni center

- Konfiguracija požarnega zidu

- Pravila požarnega zidu

- Nastavitve omejitev

- Funkcionalnost naprave

- BitLocker

- Konfiguracija programa BitLocker

- Stanje programa BitLocker

- Upravljanje certifikatov

- Seznam certifikatov

- Konfiguracija potrdila

- SCEP

Upravljanje povezav

- Wifi

- Vrsta varnosti

- Uporaba strežnika proxy

- Omejitve brezžičnega interneta

- VPN

- Vrsta povezave

- Splošne konfiguracije VPN

- Omejitve VPN

- Bluetooth

Upravljanje PIM

- Exchange Active Sync

- Elektronska pošta

Upravljanje aplikacij

- Upravitelj aplikacij za podjetja

- Nameščene aplikacije

- Obvezne aplikacije

- Omejitve aplikacij sistema

- Črna in bela lista

Konfiguracija sistema MacOS

Splošno

- Pregled profila skupine (samo na ravni skupine)

- Pregled naprave (samo na ravni naprave)

- Revizija konfiguracije (samo na ravni naprave)

- Dnevnik naprave (samo na ravni naprave)

- Dnevnik ukazov

- Možni statusi ukazov

Upravljanje sredstev (samo na ravni naprave)

- Informacije o napravi

- WiFi

- Cellular

- Bluetooth

Upravljanje posodobitev (samo na ravni naprave)

- Posodobitev informacij

Upravljanje varnosti

- Boj proti kraji

- Brisanje in zaklepanje

- Varnostna konfiguracija

- Pristopna koda

- Potrdilo

- Nastavitve omejitev

- Funkcionalnost naprave

- iCloud

- Upravljanje medijev

Upravljanje povezav

Wi-Fi

Konfiguracija omrežja Wi-Fi v podjetju

VPN

Proxy strežnik HTTP

AirPrint

AirPlay

Upravljanje PIM

Exchange Active Sync

Elektronska pošta

CalDav

CardDav

LDAP

Nadzorna plošča in poročanje

Nastavitve armaturne plošče

Pogled na armaturno ploščo

Razširjeno poročanje

Poročila o skladnosti

Ukoreninjene naprave

Naprave za gostovanje

Naprave z omogočenim gostovanjem

Nadzorovane naprave

Neaktivne naprave

Poročila o napravah

Naprave po lastništvu

Vse naprave

Nosilci naprav

Naprave SAFE

Naprave Windows BitLocker

Poročila o aplikacijah

Nameščene aplikacije

Najbolj nameščene aplikacije

Obvezne aplikacije

Aplikacije na črnem seznamu

Poročila uporabnikov

| Tarifa

| Upravljanje več najemnikov

| **Dodatni pogledi**

| Navedite vse stranke

| Datumi izteka veljavnosti APNS

| Pišite na

| **Za splošna tehnična vprašanja**

| **Za vprašanja v zvezi z namestitvijo navidezne naprave**

| Izjava o omejitvi odgovornosti

Splošni pregled

Uvod v AppTec360

AppTecova rešitev Enterprise-Mobile-Management-Solution ponuja možnost upravljanja in konfiguriranja vseh mobilnih naprav z intuitivno konzolo za upravljanje. V tem scenariju lahko strežnik EMM deluje v vašem lastnem okolju ali pa uporabite našo rešitev v oblaku.

Tudi glede osrednje namestitve poslovnih aplikacij v pametne telefone ste prišli na pravo mesto. S programom Enterprise Mobile Manager lahko v nekaj sekundah razporedite poslovne aplikacije in dokumente v naprave ali pa z belim/črnim seznamom blokirate nezaželene aplikacije.

Uporaba zasebnih naprav v podjetjih predstavlja nov izziv za varovanje pametnih telefonov in tabličnih računalnikov. Ker zaposleni vse pogosteje uporabljajo svoje pametne telefone, morajo skrbniki IT zaščititi veliko število različnih vrst naprav. Pomagali vam bomo zaščititi vse naprave in občutljive podatke, ki so shranjeni v njih, ter jih upravljali z intuitivno konzolo.

Podprti operacijski sistemi naprav

AppTec360 ponuja podporo za naprave iOS, Android in Windows. Upoštevajte, da se zmogljivosti funkcij omenjenih platform lahko razlikujejo od operacijskega sistema do operacijskega sistema.

- Apple iOS 11.0 ali novejši*
- Apple macOS 10.11 ali novejši
- Google Android 4.4 ali novejši** v različici v oblaku
- Google Android 4.1 ali novejši** v različici OnPrem
- MS Windows 10 ali novejši*** (namizni računalnik, prenosni računalnik in tablični računalnik)

**Upoštevajte, da naprav z operacijskim sistemom iOS 10 ali starejšim ni mogoče vpisati zaradi drastičnih sprememb, ki jih je Apple uvedel v postopku vpisa.*

***Ureditve je mogoče povezati in konfigurirati, tudi če uporabljajo različico, ki je proizvajalec ne podpira več. Upoštevajte, da lahko nekatere funkcije zahtevajo določeno različico sistema Android. V primerih podpore sledimo uradni podpori proizvajalca. V primeru težav ali napak, ki jih povzroča zastarela različica, ki je proizvajalec ne podpira več, si pridržujemo pravico do omejene podpore.*

****Domača različica sistema Windows ni podprta zaradi omejitev operacijskega sistema. Priporočamo uporabo različice operacijskega sistema, ki jo proizvajalec še vedno podpira. Ne le zaradi združljivosti, temveč tudi zaradi varnosti. Zato priporočamo iOS 12 ali novejši in Android 9 ali novejši.*

Podprti imeniki LDAP

- Microsoftov imenik Active Directory
- Odprite LDAP

Najnovejše informacije o "podprtih operacijskih sistemih naprav" in "podprtih imenikih LDAP" so na voljo tukaj:

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

Razlaga “nadzorovanega načina” v napravah Apple

Nadzorni način je razširjen vmesnik za naprave iOS.

V ustrezno konfigurirani napravi se lahko uporabijo dodatne omejitve, ki se nanašajo na funkcionalnost naprave končnega uporabnika. Ti so prav tako navedeni v priročniku za upravo in so označeni s transparentom.

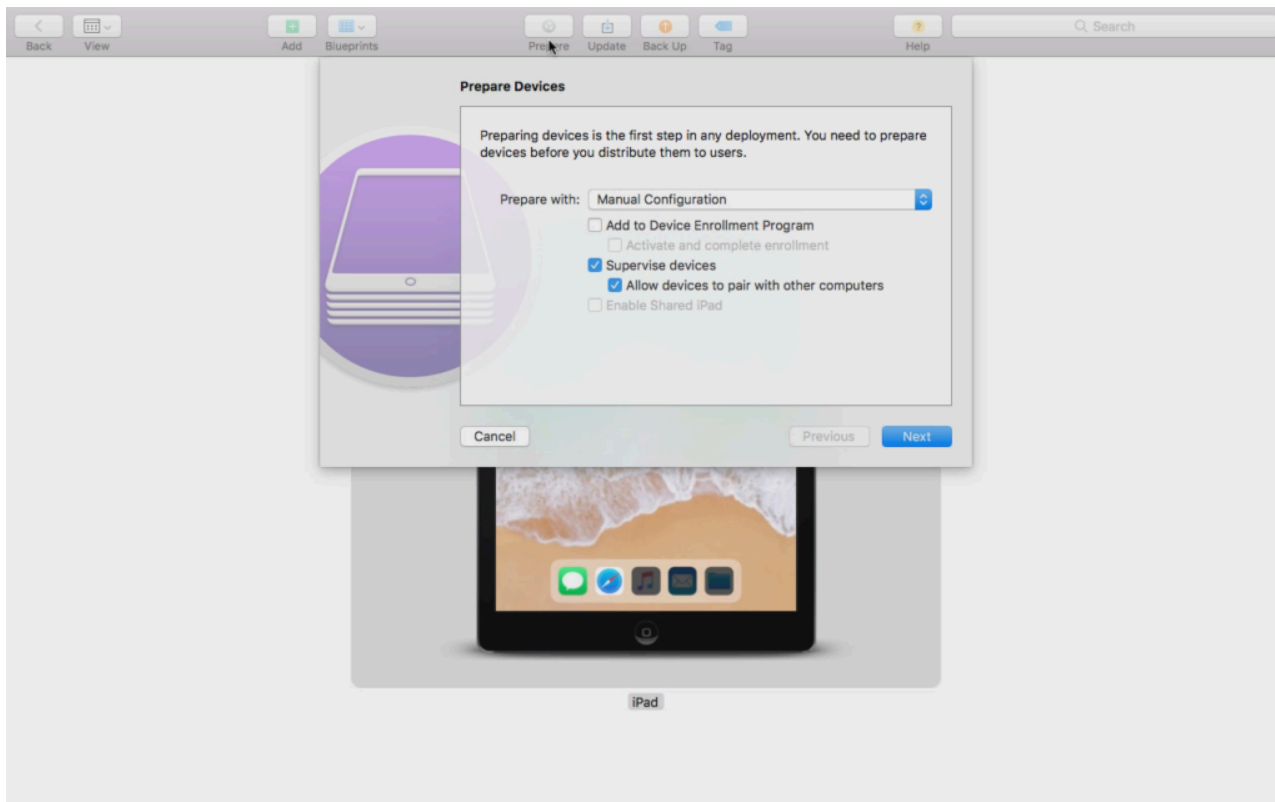
Na voljo v nadzorovanem načinu

"Nadzorni način" lahko aktivirate s programom "Apple Configurator". Apple Configurator lahko kot orodje za konfiguracijo (prek vmesnika USB) nastavi privzete nastavitve v novih napravah iOS.

Orodje lahko poleg konfiguracijskih profilov namesti tudi aplikacije. Je brezplačna, vendar zahteva računalnik Mac.

Aktivacija nadzorovanega načina

1. Odprite Apple Configurator



2. Kliknite na napravo in izberite "Pripravi".

3. Izberite "Ročna konfiguracija" in "Nadzor naprav".

4. Kliknite "Naprej".

5. (neobvezno) Zdaj lahko dodate strežnik MDM, v katerega bo naprava vpisana. Povezavo za to najdete v razdelku "Splošne nastavitve - Konfiguracija iOS - Konfigurator in URL". Izberite svojo organizacijo ali ustvarite novo.

6. Izberite svojo organizacijo ali ustvarite novo.

7. Izberite korake, ki jih želite preskočiti pri začetni namestitvi, in kliknite "Naprej" (POZOR: nadaljevanje bo izbrisalo napravo!)

Vaša naprava bo zdaj preklopljena v nadzorovani način. To lahko traja nekaj minut. Po tem se bo naprava znova zagnala.

Zdaj je vaša naprava pod nadzorom!

Dodajanje naprave v DEP

Naprave lahko v program DEP (Device Enrollment Programm) dodajate tudi prek programa Apple Configurator, če so vaše naprave v operacijskem sistemu iOS 11 ali novejšem.

Več informacij o DEP: <https://www.apple.com/business/dep/>

Izvedite enake korake, kot bi nadzorovali napravo, in dodatno preverite možnost "Add to Device Enrollment Programm" (Dodaj v program za vpisovanje naprav). Če se še nikoli niste prijavili v program DEP s programom Apple Configurator, boste morali navesti podatke za prijavo v DEP.

Po končanem postopku lahko napravo najdete v strežniku DEP "Devices Added by Apple Configurator 2". Zdaj lahko uporabite ta strežnik in ga povežete s konzolo za upravljanje ali pa napravo prenesete v že obstoječi strežnik.

Napravo ste uspešno dodali v DEP!

Razlaga sistema Android Enterprise

Kaj je Android Enterprise?

Android Enterprise omogoča boljši nadzor nad delovnimi napravami, ki jih upravljate z MDM. Tako lahko skrbniki v celoti nadzorujejo svoje androidne naprave ali pa ločijo podatke podjetja od zasebnih podatkov na napravah v zaboju. Poleg tega Android Enterprise omogoča lažje vpisovanje naprav in enostavno distribucijo aplikacij.

Kakšne so zahteve za uporabo sistema Android Enterprise?

Aplikacijo Android Enterprise lahko brezplačno uporablja vsakdo. Za omogočanje vseh funkcij sistema Android Enterprise morate le povezati račun Google z MDM. Več o tem najdete v razdelku [Android Enterprise](#).

Android Enterprise lahko uporabljate v napravah z operacijskim sistemom Android 5.1 ali novejšim, z izjemo izboljšanega delovnega profila (glej spodaj). Priporočamo vsaj Android 7 ali novejši za lažji vpis ali Android 11 za uporabo vseh razpoložljivih funkcij.

Kateri načini so na voljo v sistemu Android Enterprise?

Pri uporabi sistema Android Enterprise lahko uporabite tri različne načine.

AE Popolnoma upravljana naprava (upravljanje dela): Naprava, s katero se upravlja v celoti in se uporablja samo za delo. To omogoča skrbniku popoln nadzor nad napravo. To ne omogoča zasebne uporabe naprave. Za vpis naprav v ta način je treba naprave ponastaviti in vpisati s kodo QR (glejte [Vpis AE](#)) ali vpisati prek vpisa Knox ali Zero Touch.

AE BYOD Container: Uporabniki lahko do podatkov podjetja dostopajo s svojim zasebnim telefonom v ločenem zaboju. V tem načinu zasebne aplikacije ne morejo videti podatkov in aplikacij podjetja in obratno. Za vpis naprav v ta način je treba prenesti aplikacijo AppTec in prebrati kodo QR. V konzoli ustvarite napravo in kot vrsto naprave izberite "AE Container (BYOD & Enhanced Work Profile)". Kliknite na kodo QR na novo ustvarjeni napravi, da dobite kodo QR in nastavite prvo stikalo na "Legacy & BYOD".

AE Enhanced Work Profile: (zahteva Android 11 ali novejši) Medtem ko zgoraj omenjeni BYOD Container prinaša podatke podjetja v zasebno napravo, Enhanced Work Profile naredi enako, vendar za napravo v lasti podjetja. Ustvari enak vsebnik, vendar skrbniku omogoča nekoliko več nadzora nad napravo, tako da uporabnik ne more preprosto odstraniti MDM iz naprave. V konzoli ustvarite napravo in kot vrsto naprave izberite "AE Container (BYOD & Enhanced Work Profile)". Kliknite na kodo QR na novo ustvarjeni napravi, da dobite kodo QR in nastavite prvo stikalo na "Enhanced Work Profile". To

kodo QR lahko optično preberete po ponastavitvi naprave in šestkratnem tapkanju po zaslonu, kot je pojasnjeno v načinu 1 v razdelku [AE Enrolment \(Vpis v AE\)](#).

Kako lahko dodelim aplikacije napravam Android Enterprise?

Najprej morate odobriti aplikacije, ki jih želite uporabljati, v Splošne nastavitve → Upravljanje aplikacij → AE Play Store → Play Store Apps. Ko aplikacijo odobrite, jo lahko uvrstite na seznam obveznih aplikacij → svojega profila tako, da kliknete na "+" in izberete aplikacijo v zavihku "AE Play Store". Tako se bo aplikacija samodejno prenesla in namestila. Googlov račun v napravi ni potreben in uporabniku tega ni treba potrditi ali dovoliti.

Prenos lastnih aplikacij v trgovino Google Play

Notranje aplikacije lahko naložite v trgovino Google Play. Tako lahko izkoristite različne prednosti, kot je mehanizem za posodabljanje v trgovini Play.

Za to potrebujete Googlov razvijalski račun. Prijavite se v konzolo Google Play (<https://play.google.com/apps/publish>).

Kliknite "Ustvari aplikacijo". Izberite privzeti jezik in naslov aplikacije.

Create application

Default language *

English (United Kingdom) – en-GB ▼

Title *

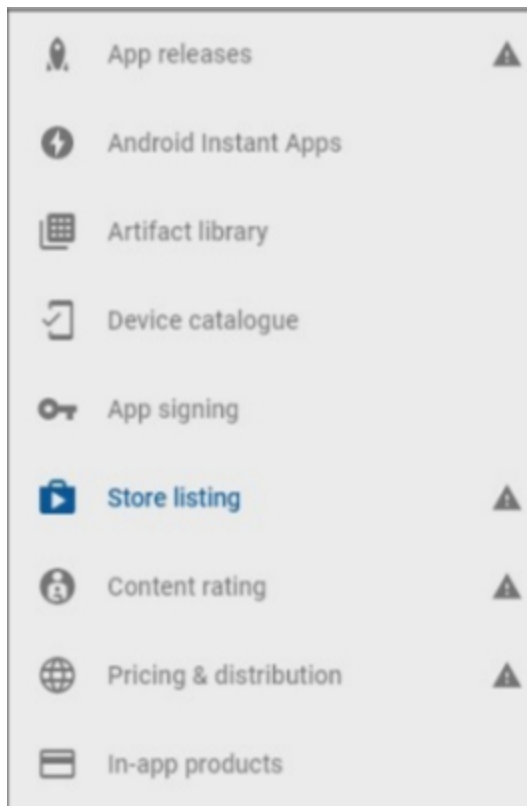
AppTec Demo App

15/50

CANCEL

CREATE

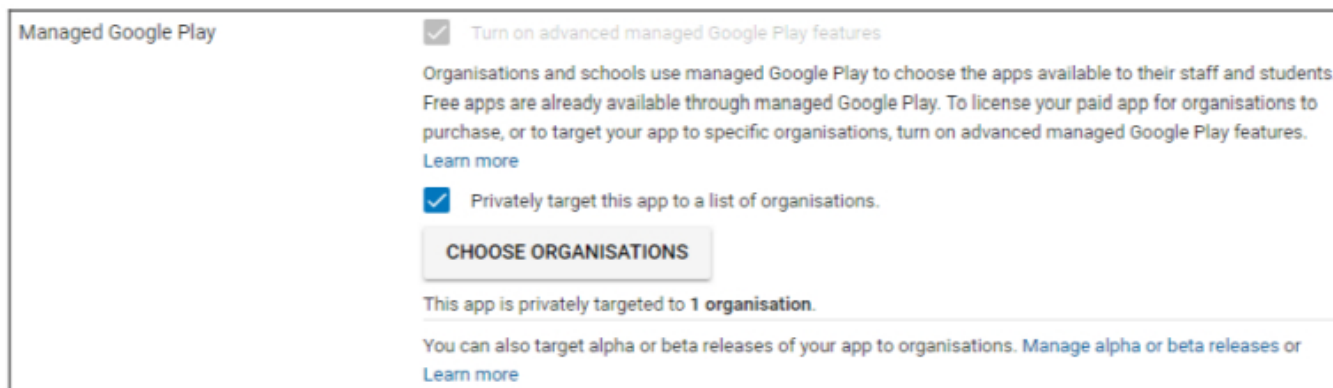
Na naslednji strani boste morali vnesti različne podrobnosti o svoji aplikaciji.



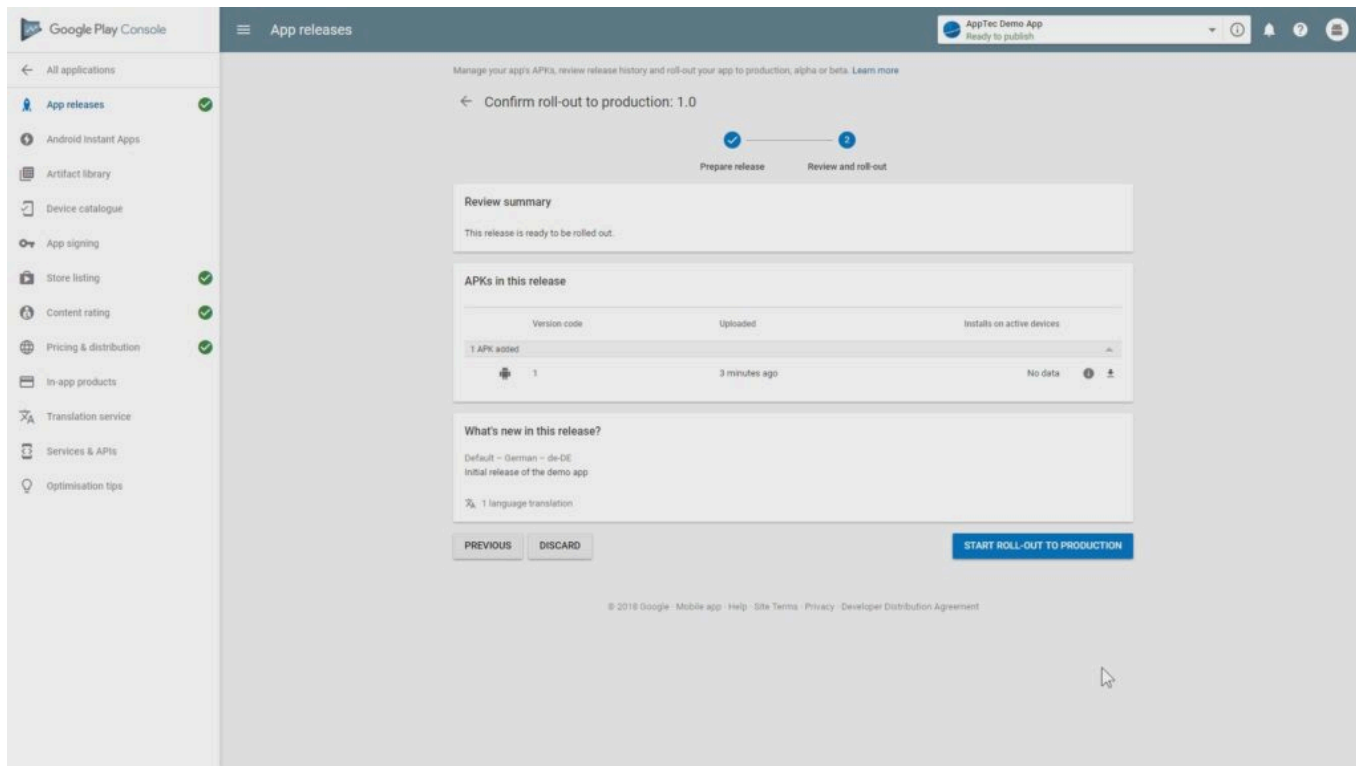
Ko vnesete vse podatke, se na levi strani prikažejo različni simboli namigov.

Z miško se pomaknite nanje, da vidite, kateri koraki so ostali, in jih izvajajte v poljubnem vrstnem redu.

Opomba: Prepričajte se, da sta v razdelku "Obvladovanje Google Play" v razdelku "Določanje cen in distribucija" označeni dve potrditveni polji. V nasprotnem primeru bo aplikacija javna in bo do nje lahko dostopal vsakdo. Prav tako se prepričajte, da ste izbrali državo za distribucijo.



Ko ste opravili vse korake, se lahko odpravite na "Izdaje aplikacij". Kliknite "Review" in "Start Roll-Out to Production", da dokončate osnutek in objavite aplikacijo.



Do trenutka, ko bo aplikacija na voljo v trgovini Play Store, bo minilo nekaj časa. Po končanem postopku lahko aplikacijo poiščete v trgovini Play for Work in jo odobrite. Nato lahko aplikacijo preprosto dodelite napravam z uporabo konzole EMM, tako kot to počnete z drugimi aplikacijami.

Zahteve in namestitvev

Zahteve

Sistemske zahteve

Virtualna naprava je na voljo v odprtem virtualizacijskem formatu (VMWare, VirtualBox, Citrix Xen Server) in kot stisnjena datoteka .vhdx (Hyper-V)*.

*Pomnilo: Pri uporabi Hyper-V je treba računalnik ustvariti z Generacijo 1.

Ciljna velikost navideznega diska je 20 GB, računalnik pa potrebuje 4 GB pomnilnika RAM.

Naprava temelji na sistemu Debian 9 64bit

Uvoženi stroj nadgradite na najnovejšo združljivost (npr. v VMWare) in se prepričajte, da je vrsta operacijskega sistema stroja pravilno nastavljena v hipervizorju.

Licenčni ključ

Za uspešno aktivacijo in namestitev strežnika potrebujete veljavno licenčno datoteko. Pridobite jo lahko neposredno pri AppTec360 in/ali pri svojem prodajalcu.

Reševanje naslovov IP in DNS

Naprava AppTec360 mora biti dosegljiva z napravo, ki uporablja ime gostitelja, za katerega je izdana licenca.

Če želite vpisati naprave Windows 10, morate nastaviti tudi dodatno poddomeno v obliki "enterpriseenrollment.", ki kaže na napravo.

SSL-certifikat

Ker morajo biti vse povezave v naprave in iz njih zaščitene z uporabo protokola SSL, potrebujete veljavno potrdilo za ime gostitelja, ki ga je izdal organ za potrjevanje, ki mu naprava zaupa. Zasebni ključ za potrdilo je treba naložiti brez zaščite z geslom. V večini primerov je potrebno vmesno potrdilo za overitelja, da naprave prepoznajo potrdilo strežnika.

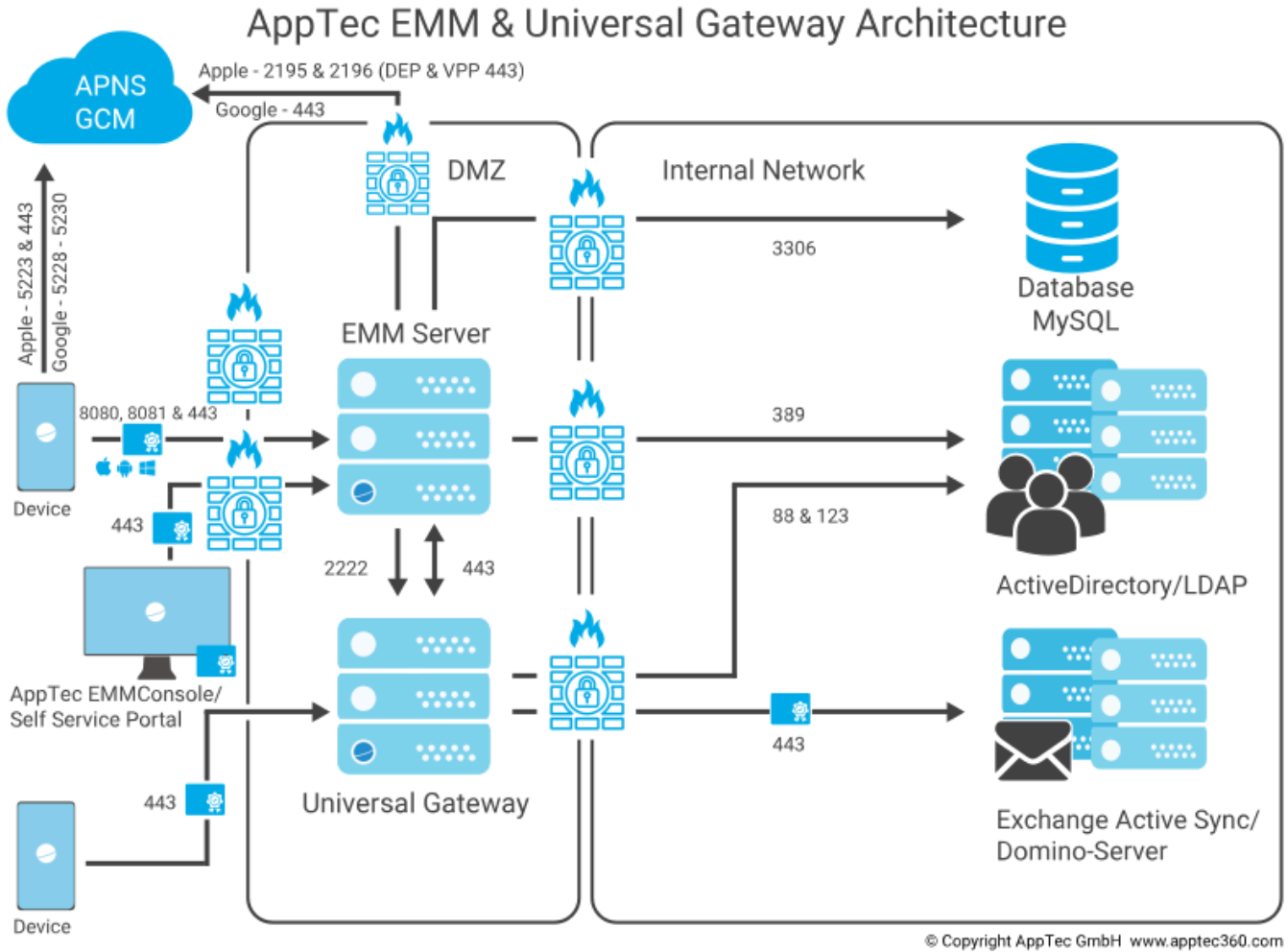
Naprave z operacijskim sistemom Windows 10 bodo za poddomeno enterpriseenrollment potrebovale posebno potrdilo.

Od različice naprave 202104 lahko uporabljate tudi potrdila Let's Encrypt, ki se ustvarijo samodejno (opisano v drugem koraku - potrdilo SSL).

Strežnik SMTP

Potreben je e-poštni strežnik in/ali e-poštni posrednik, da lahko AppTec360 EMM pošilja e-pošto (npr. za registracijo naprave in potrditev računa).

Pravila požarnega zidu



Ta diagram prikazuje, katera povezava je potrebna glede na to, katere storitve želite uporabljati.

Podrobnejši opis je v tabeli na naslednji strani.

Kakršno koli (zunanje/oprema)	→	AppTec360 Appliance / emmconsole.com
Pristanišča	443	Upravljanje, trgovina z aplikacijami za podjetja in komunikacija s sistemom Windows Phone
	8080	Komunikacija s sistemom Android in iOS
	80	Prva nastavitve programa Let's Encrypt. Kasneje uporablja 443.
Vse (naprave)	→	Katera koli (zunanja)
Pristanišča	5223, 443	Storitev Apple Push Service, mora biti dosegljiva brez posredniškega strežnika, 443 kot nadomestna storitev, glejte https://support.apple.com/en-us/HT203609 .
	5228-5230	Storitev Android Push Service (FCM) mora biti dosegljiva brez posredniškega strežnika
AppTec360 Appliance	→	Nadzornik domene
Pristanišča	389, (LDAPS 636)	Sinhronizacija uporabnikov s protokolom LDAP
AppTec360 Appliance	→	Vse
Pristanišče	443	Uporablja se za storitev Android Push Service (GCM) Iskanje v trgovini AppStore / Play Store
AppTec360 Appliance	→	emmconsole.com
Pristanišča	443	AppTec360 Appliance posodobitve, APNS certifikat generacije
AppTec360 Appliance	→	Omrežje Apple (17.0.0.0/8)
Pristanišča	2195, 2196	Storitev Apple Push Service in storitev za povratne informacije
	443	DEP IN VPP

Varnostne posodobitve

Operacijski sistem Debian je treba redno posodabljan, da bo vseboval najnovejše varnostne popravke. Vendar se prepričajte, da ne nadgrajujete na novejšo glavno različico Debiana ročno. Ko bo AppTec360 EMM združljiv z novejšo različico, bomo dodali način za nadgradnjo v posodobitvi naprave.

Privzeta gesla navidezne naprave

Prijava Uporabnik (Korenska prijava je onemogočena. Uporabite "sudo" za upravna opravila)

apptec

Geslo za prijavo

apptec

Korenski uporabnik MySQL

koren

Korensko geslo MySQL

apptec

Privzet uporabnik MySQL

AppTec

Privzeto uporabniško geslo MySQL

AppTec

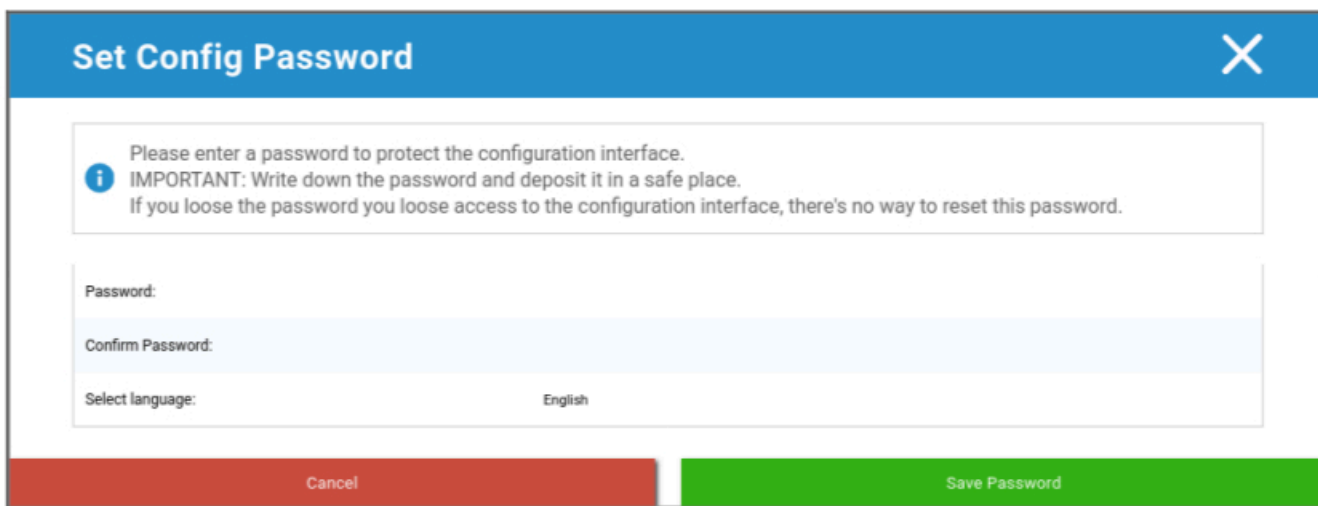
Konfiguracija navidezne naprave

Pomembno: Preden začnete s konfiguracijo virtualne naprave, mora biti ločljivost zaslona nastavljena na vsaj 1280 x 800 slikovnih pik.

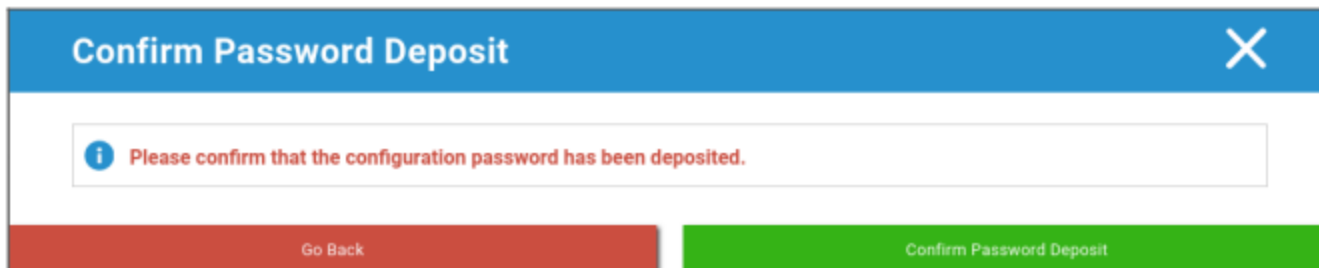
Po tem, ko ste se vklopili v napravo, se mora Firefox samodejno zagnati in prikazati konfiguracijski vmesnik.

Priprava

Najprej je treba zagotoviti geslo za konfiguracijski vmesnik. To geslo se uporablja za šifriranje vseh informacij in datotek, vnesenih v konfiguracijski vmesnik. Tu lahko nastavite tudi jezik, v katerem naj bo vmesnik prikazan (lahko ga spremenite pozneje).

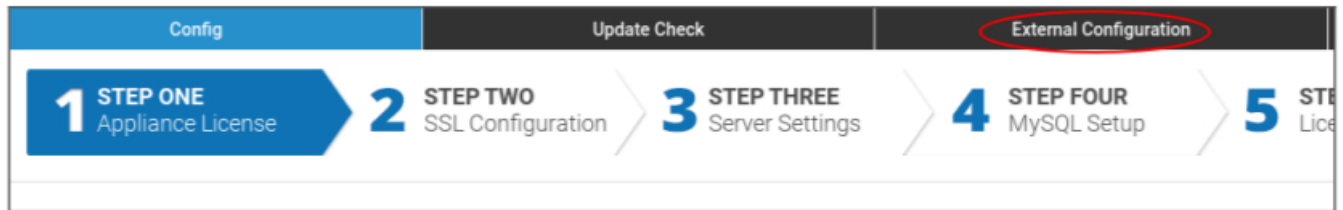


Geslo lahko ponastavi le podpora AppTec360, zato ga shranite na varno in potrdite prihajajoče pojavno okno.



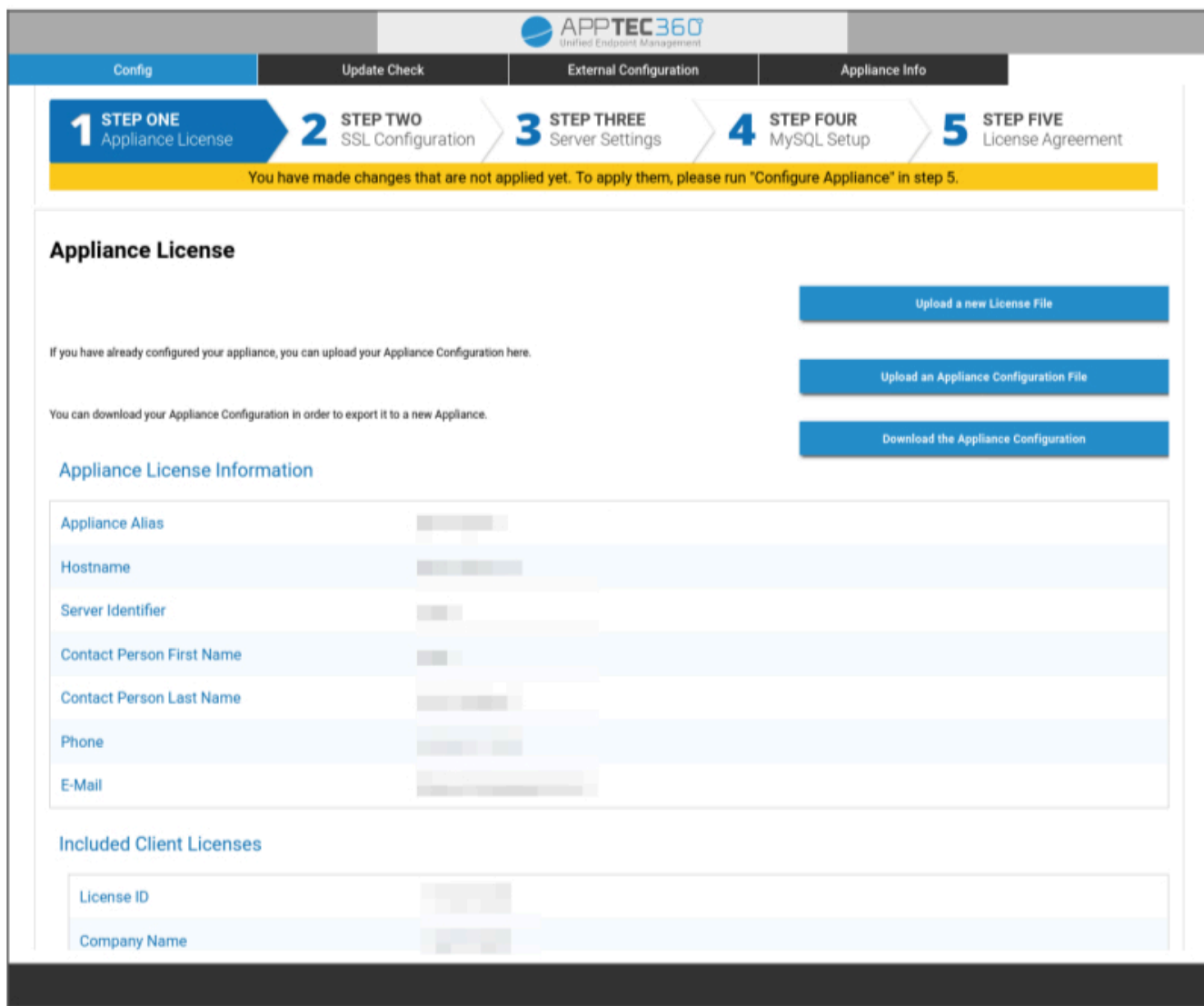
Konfiguracija iz zunanjega gostitelja

Če želite olajšati postopek nastavitve, lahko stran za nastavitve omogočite na oddaljenem naslovu. V ta namen sledite korakom v razdelku "Konfiguracija iz zunanjega gostitelja".



Prvi korak – Licenca naprave

1. Naložite licenčno datoteko, ki ste jo prejeli od družbe AppTec.
2. Če je bila datoteka z licenco uspešno naložena, lahko vidite informacije o licenci naprave, kot na spodnji sliki zaslona.



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.

Appliance License

Upload a new License File

If you have already configured your appliance, you can upload your Appliance Configuration here.

Upload an Appliance Configuration File

You can download your Appliance Configuration in order to export it to a new Appliance.

Download the Appliance Configuration

Appliance License Information

Appliance Alias	
Hostname	
Server Identifier	
Contact Person First Name	
Contact Person Last Name	
Phone	
E-Mail	

Included Client Licenses

License ID	
Company Name	

Drugi korak – certifikat SSL

Uporabite lahko samodejno nastavitev potrdil z Let's Encrypt ali pa potrdila zagotovite sami (za več informacij glejte SSL-Certifikat).

Samodejno

Potrdilo se samodejno ustvari s [storitvijo Let's Encrypt](#).

AppTec360 EMM za preverjanje domene uporablja [izziv HTTP-01](#), kar pomeni, da morajo biti vrata HTTP za prvo zahtevo potrdila odprta iz interneta. Nadaljnji zahtevki za podaljšanje se lahko potrdijo prek HTTPS.

Preklopite radijske gumbе na "Automatic (Let's Encrypt)" in pritisnite "SAVE VALUES". Certifikat bo samodejno zahtevan pri uporabi konfiguracije v petem koraku - Licenčna pogodba. Certifikat se bo po potrebi samodejno obnovil in prejeli boste e-poštno sporočilo, če bo certifikat kmalu potekel (kar pomeni, da obnovev morda ni bila uspešna).

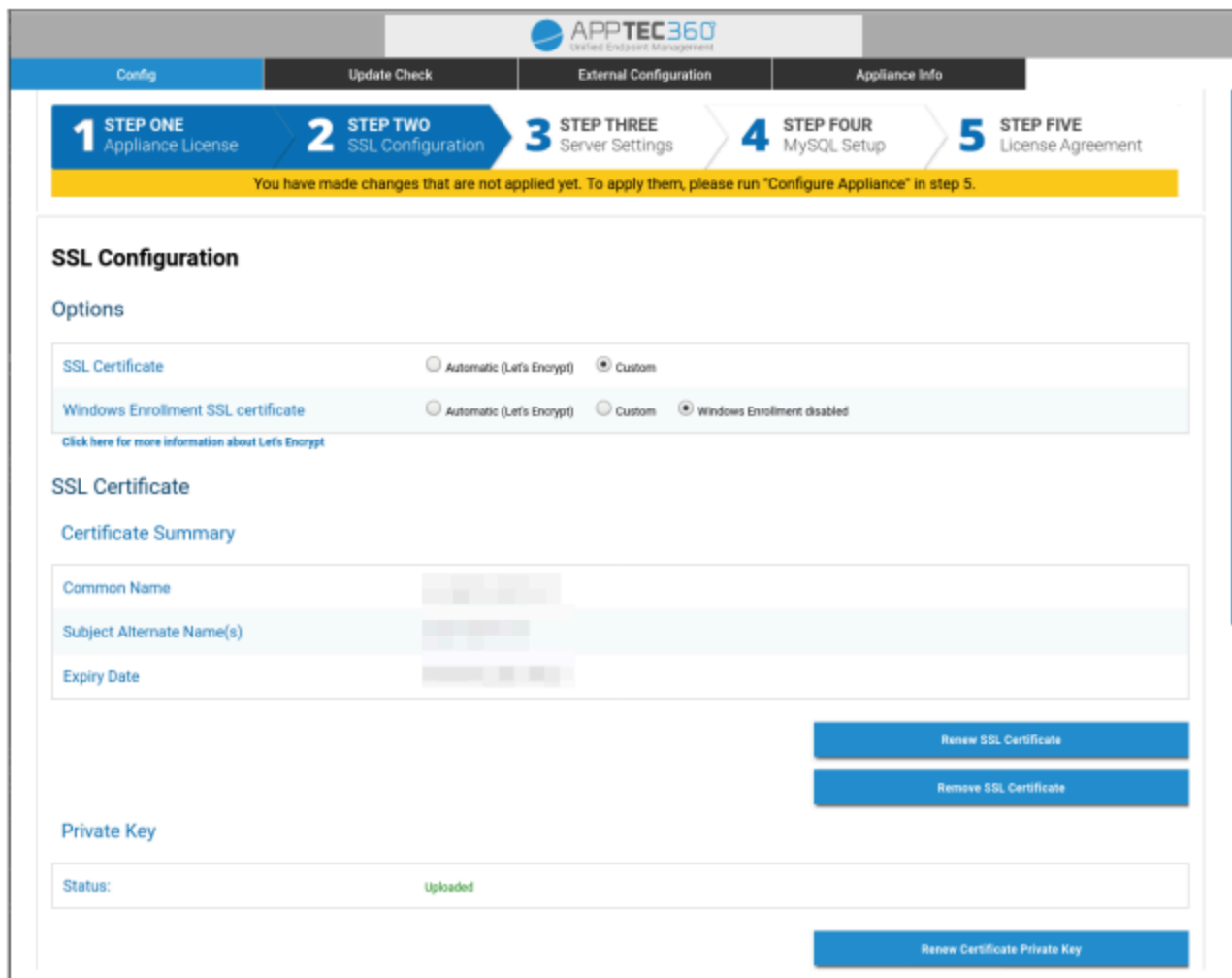
Po meri

1. Naložite SSL-certifikat za svoje licencirano gostiteljsko ime. Ime gostitelja si lahko ogledate v prvem koraku - Licenca naprave.

2. Prenesite tudi zasebni ključ za potrdilo in po potrebi vmesno potrdilo.

Pomembno: Ključ ne sme biti zaščiten z geslom. Če je, pred prenosom odstranite geslo.

Namig: Če želite uporabljati tudi naprave s sistemom Windows 10, morate omogočiti možnost "Windows Enrollment SSL certificate" ter naložiti certifikat, zasebni ključ in vmesni certifikat za poddomeno (opisano v razdelku Prenos IP-naslova in resolucije DNS) na dnu strani.



The screenshot displays the AppTec360 configuration interface. At the top, there is a navigation bar with tabs for "Config", "Update Check", "External Configuration", and "Appliance Info". Below this is a progress indicator showing five steps: 1. STEP ONE Appliance License, 2. STEP TWO SSL Configuration (highlighted), 3. STEP THREE Server Settings, 4. STEP FOUR MySQL Setup, and 5. STEP FIVE License Agreement. A yellow banner below the progress indicator states: "You have made changes that are not applied yet. To apply them, please run 'Configure Appliance' in step 5."

The main content area is titled "SSL Configuration" and includes an "Options" section with the following settings:

- SSL Certificate: Automatic (Let's Encrypt) Custom
- Windows Enrollment SSL certificate: Automatic (Let's Encrypt) Custom Windows Enrollment disabled

A link below the options reads: "Click here for more information about Let's Encrypt".

The "SSL Certificate" section includes a "Certificate Summary" table:

Field	Value
Common Name	[Redacted]
Subject Alternate Name(s)	[Redacted]
Expiry Date	[Redacted]

Below the summary are two buttons: "Renew SSL Certificate" and "Remove SSL Certificate".

The "Private Key" section shows a "Status:" field with the value "Uploaded" in green. Below this is a "Renew Certificate Private Key" button.

Tretji korak – Nastavitve strežnika

1. Vnesite globalni e-poštni naslov za podporo. Ta naslov bo uporabljen v e-poštnih sporočilih uporabnikom, da bodo vedeli, na koga se obrniti v primeru kakršnih koli težav v zvezi z njihovo napravo.
2. Navedite nastavitve e-pošte, ki jih bo sistem uporabljal za pošiljanje e-poštnih sporočil. Nastavitve se bodo uporabljale za pošiljanje e-pošte uporabniku in tudi za pošiljanje poročil o napakah in zahtevkov za funkcije na naslov "support@apptec360.com". Ko shranite nastavitve e-pošte, jih morate preveriti tako, da kliknete na "Test E-Mail Configuration" in sledite navodilom.

E-Mail Settings

Please enter valid SMTP credentials!
All E-Mails generated by AppTec EMM Console will be sent using this account.
After entering and saving the email server settings, please verify them by using the "Test E-Mail Configuration" Button below.

Email Address	<input type="text"/>
From Name	<input type="text"/>
SMTP Auth Method	login
Username	<input type="text"/>
Password	<input type="password"/>
Hostname	<input type="text"/>
Port (leave empty for default)	<input type="text"/>
Encryption	none

[Test E-Mail Configuration](#)

Četrty korak – Nastavitev MySQL

1. Če želite uporabiti notranjo zbirko podatkov, lahko ta korak preskočite. V nasprotnem primeru lahko vnesete podatke za povezavo z zunanjim strežnikom podatkovne zbirke.

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.

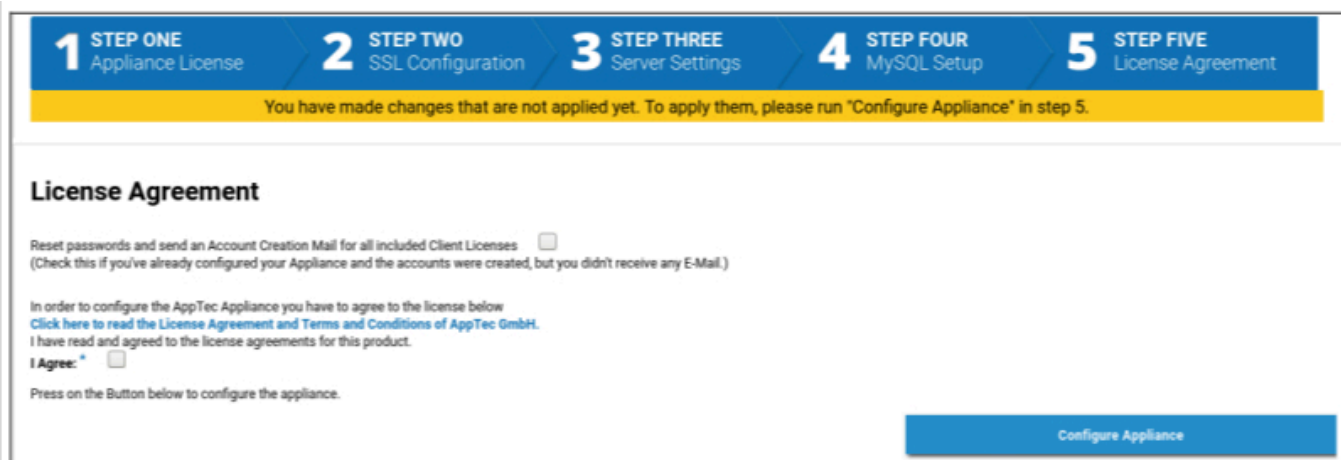
If you change the settings after the initial configuration, you have to reconfigure your appliance by clicking on "Configure now" in step 5.

IP Address or Hostname	<input type="text" value="127.0.0.1"/>	(Default: 127.0.0.1)
Username	<input type="text" value="AppTec"/>	(Default: AppTec)
Password	<input type="password" value="••••••"/>	(Default: AppTec)
Port	<input type="text" value="3306"/>	(Default: 3306)

Peti korak – licenčna pogodba

1. Preberite licenčno pogodbo.
2. Označite "I Agree" (Strinjam se) in pritisnite gumb "Configure Appliance" (Konfiguriraj napravo), da uporabite nastavitve.

Namig: Vsakič, ko spremenite nastavitve v petih korakih, boste morali zagnati "Configure Appliance", da se nastavitve uporabijo.



The screenshot shows a configuration wizard with five steps: 1. Appliance License, 2. SSL Configuration, 3. Server Settings, 4. MySQL Setup, and 5. License Agreement. A yellow banner indicates that changes made in previous steps are not yet applied and that the user should run "Configure Appliance" in step 5. The "License Agreement" section includes a checkbox for "Reset passwords and send an Account Creation Mail for all included Client Licenses" and a checkbox for "I Agree". A blue "Configure Appliance" button is located at the bottom right.

Čestitamo!

Končali ste konfiguracijo navidezne naprave.

Na naslov, ki ste ga navedli za licenco (viden v razdelku "Vključene licence za odjemalce" v prvem koraku - Licenca za napravo), je bilo poslano e-poštno sporočilo z geslom.

Zdaj se lahko v konzolo prijavite s tem geslom in e-poštnim naslovom, na katerega ste ga prejeli.

Če se želite prijaviti v konzolo, v naslovno vrstico brskalnika vnesite ime gostitelja konzole.

Ime gostitelja naprave najdete v prvem koraku - Licenca naprave.

Odpravljanje težav

1. Pri konfiguriranju naprave v petem koraku - Licenčna pogodba - niste prejeli e-poštnega sporočila:

Prepričajte se, da so nastavitve e-pošte v tretjem koraku - Nastavitve strežnika pravilne. Za ponovno pošiljanje gesla preverite "Reset passwords and send an Account Creation Mail for all included Client Licenses" v petem koraku - Licenčna pogodba, preden ponovno zaženete "Configure Appliance".

2. Med konfiguracijo v petem koraku - Licenčna pogodba - ste prejeli napako v zvezi z Let's Encrypt:

Prepričajte se, da je naprava dosegljiva z imenom domene na vratih 80. Program Let's encrypt tudi zapiše dnevnik v "/var/log/letsencrypt", kar lahko pomaga pri nadaljnjem odpravljanju težav.

Varnostna priporočila

Za zaščito naprave AppTec360 je priporočljivo izvesti naslednje korake.

To ni celoten sklop navodil, temveč le priporočilo za osnovno konfiguracijo.

- Sprememba gesla za uporabnika AppTec360
- Spremenite geslo za uporabnika MySQL "root" in "AppTec" ter ustrezno posodobite četrti korak - Nastavitve MySQL
- Spreminjanje privzetih vrat strežnika SSH
- V konzoli blokirajte vrata 80 in onemogočite dohodni promet HTTP, uporabljajte samo HTTPS. Po nastavitvi je mogoča tudi zunanja konfiguracija prek HTTPS.
- Na dnu tretjega koraka - Nastavitve strežnika - omejite dostop do vmesnika za upravljanje samo določenim IPS.
- Konfiguracija požarnega zidu

Splošne nastavitve

Pregled računa

Informacije o računu

Pregled

Tu si lahko ogledate pregled svojega računa AppTec360.

Ime podjetja	Ime vašega podjetja
Datum ustanovitve	Datum odprtja računa
Vrsta licence	Plačana = plačana licenca Brezplačna = neplačana licenca Opomba: Računi v napravi OnPremise bodo iz tehničnih razlogov vedno prikazani kot plačani.
Identifikator stranke	Identifikator vašega računa (to NI vaša številka stranke)
Datum izteka veljavnosti licence	Datum izteka veljavnosti licence AppTec360
Licenca ContentBox	Brezplačno = brezplačna licenca za 25 naprav Plačano = plačana licenca za x naprav
Zaganjalnik	Pokaže, ali lahko uporabite zaganjalnik po meri za Android
Naprave	Število trenutno uporabljenih licenc / vseh licenc
Kontaktna oseba	Zagotovljena kontaktna oseba
Telefon	Zagotovljena telefonska številka
e-pošta*	Zagotovljeni e-poštni naslov
Korenski uporabnik	Korenski uporabniki, ki se lahko prijavijo
Različica programske opreme	Trenutna različica programske opreme

**Pomnilnik: Tukaj je prikazan e-poštni naslov, ki ste ga vnesli pri registraciji računa. Na podlagi tega bo uporabnik ustvarjen v drevesu uporabnikov/ naprav in ga je mogoče spreminjati. Pri urejanju tega uporabnika se bo spremenil e-poštni naslov, ki ga morate uporabiti za prijavo, ne pa tudi podatki v pregledu računa. .*

Poročilo o napaki

Poročilo o hrošču lahko pošljete neposredno podpori za podporo, če želite prijaviti težave ali hrošče, vključuje pa informacije in dnevnike o vašem računu in nastavitvah.

Zadeva	Predmet poročila o hrošču. Če želite to dodati obstoječi vtičnici za podporo, vključite številko vtičnice.
Pričakovano vedenje	Podrobno opišite, kaj ste storili in kaj ste pričakovali, da se bo zgodilo.
Dejansko vedenje	Natančno opišite, kaj se je zgodilo. Natančno navedite sporočila o napakah. Pomaga tudi, če v priponko dodate posnetke zaslona.
Kdaj se je težava pojavila?	Navedite natančen čas, ko ste dobili določeno sporočilo o napaki/problem. V najboljšem primeru vključite tudi sekunde, npr. 18:55:27
Ali je mogoče težavo ponoviti? Če da, kako (podrobno)?	Podrobno opišite, kako lahko ponovite težavo.
Ali je ta funkcija prej delovala, kot ste pričakovali? Če da, do kdaj?	Če ne veste, pustite prazno.
Ali so bile pred pojavom te težave v sistemu izvedene kakšne posebne spremembe? Če da, katere spremembe (podrobno)?	Vedno omenite, kaj ste nazadnje spremenili ali storili pred pojavom težave, tudi če menite, da je to nepomembno.
Če je primerno: Kateri modeli naprav in različice operacijskega sistema so prizadeti?	Vedno natančno navedite različico operacijskega sistema (npr. iOS 14.7.1 ali Android 11)
Če je primerno: Kateri je javni naslov IP in/ali serijska številka naprave?	Navedite vsaj eno, tudi če so prizadete vse naprave.
Vključite dnevniške datoteke	Označite to, če želite poslati dnevniško datoteko s poročilom o napaki. To je priporočljivo storiti.
Prenesite trenutno stanje VPP od družbe Apple in ga vključite v poročilo o napaki	Vključuje informacije o dodelitvah licenc VPP. Aktivirajte jo le, če vas za to zaprosi podpora ali če se vaša težava nanaša na VPP.
Priponka	Priložite vse datoteke, ki bi lahko bile koristne (npr. posnetke zaslona s sporočilom o napaki).

Zahteva za funkcijo

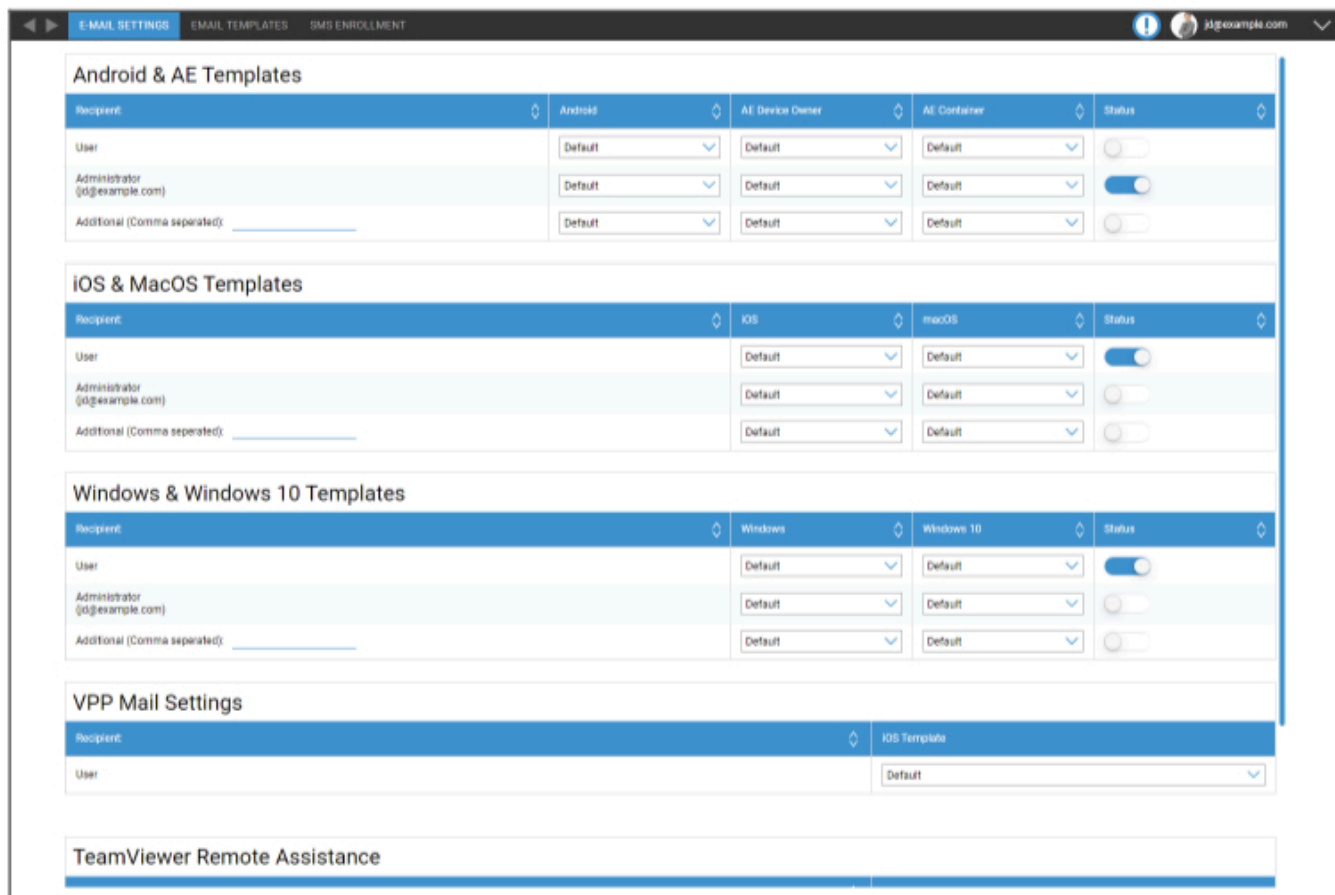
Zahtevo za funkcijo lahko pošljete neposredno podpori. Ta lahko vsebuje zahtevo za določeno funkcijo ali izboljšavo za

Povzetek	Kratek povzetek vaše težave
Opis	Podroben opis težave, ki naj bo čim bolj natančen.
Priponka	Priložite datoteke poročilu o hrošču

Globalna konfiguracija

Nastavitve elektronske pošte

Tu lahko določite, kdo bo prejel pošto, ko bo ustvarjena zahteva za vpis, in katera besedilna predloga bo uporabljena za to pošto.



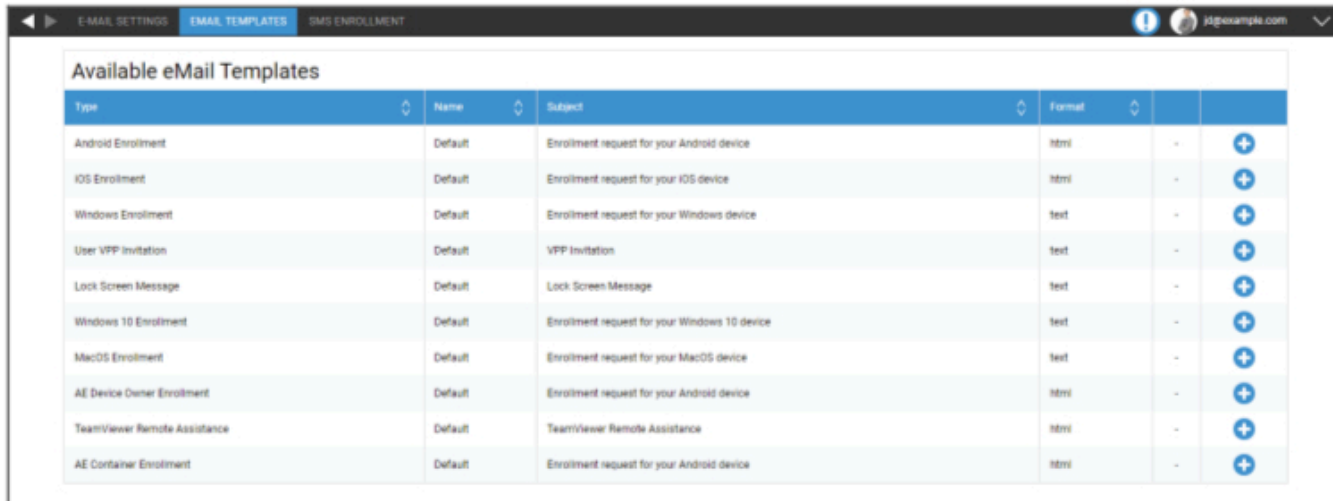
The screenshot displays the 'E-MAIL SETTINGS' configuration page. It is organized into several sections:

- Android & AE Templates:** A table with columns for Recipient, Android, AE Device Owner, AE Container, and Status. It includes rows for 'User', 'Administrator (jd@example.com)', and 'Additional (Comma separated):'.
- iOS & MacOS Templates:** A table with columns for Recipient, iOS, macOS, and Status. It includes rows for 'User', 'Administrator (jd@example.com)', and 'Additional (Comma separated):'.
- Windows & Windows 10 Templates:** A table with columns for Recipient, Windows, Windows 10, and Status. It includes rows for 'User', 'Administrator (jd@example.com)', and 'Additional (Comma separated):'.
- VPP Mail Settings:** A section with a 'Recipient' dropdown set to 'iOS Template' and a 'User' dropdown set to 'Default'.
- TeamViewer Remote Assistance:** A section at the bottom of the page.

Predloge za elektronsko pošto

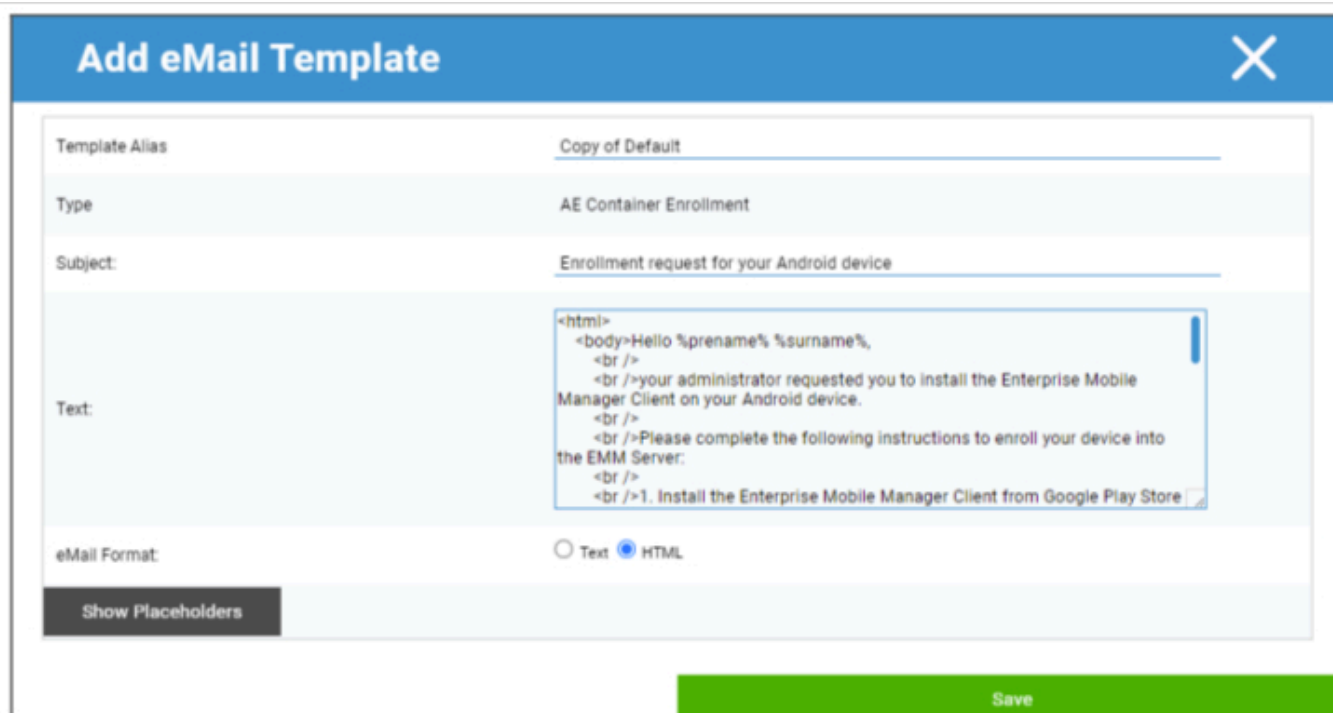
Tu lahko ustvarite in urejate predloge za različne scenarije. Te so lahko v običajni besedilni obliki ali v obliki HTML. Pri HTML lahko bolje nadzorujete oblikovanje besedila.

Privzete predloge ni mogoče urejati ali izbrisati.



Type	Name	Subject	Format		
Android Enrollment	Default	Enrollment request for your Android device	html	-	+
iOS Enrollment	Default	Enrollment request for your iOS device	html	-	+
Windows Enrollment	Default	Enrollment request for your Windows device	text	-	+
User VPP Invitation	Default	VPP Invitation	text	-	+
Lock Screen Message	Default	Lock Screen Message	text	-	+
Windows 10 Enrollment	Default	Enrollment request for your Windows 10 device	text	-	+
MacOS Enrollment	Default	Enrollment request for your MacOS device	text	-	+
AE Device Owner Enrollment	Default	Enrollment request for your Android device	html	-	+
TeamViewer Remote Assistance	Default	TeamViewer Remote Assistance	html	-	+
AE Container Enrollment	Default	Enrollment request for your Android device	html	-	+

Namestna imena lahko uporabite tudi kot spremenljivko, ki bo samodejno nadomeščena. Med urejanjem kliknite na "Prikaži nadomestne znake", da si ogledate razpoložljive nadomestne znake. Različne kategorije imajo različna Namestna imena.



Add eMail Template

Template Alias: Copy of Default

Type: AE Container Enrollment

Subject: Enrollment request for your Android device

Text:


```
<html>
<body>Hello %prename% %surname%,
<br />
<br />your administrator requested you to install the Enterprise Mobile
Manager Client on your Android device.
<br />
<br />Please complete the following instructions to enroll your device into
the EMM Server:
<br />
<br />1. Install the Enterprise Mobile Manager Client from Google Play Store
```

eMail Format: Text HTML

Show Placeholders

Save

Vpis SMS

Tu lahko vnesete/aktivirate postopek prijave SMS.

(privzeto: deaktivirano)

Prikazalo se bo tudi, koliko kreditov SMS je še na voljo.

Kredite SMS je treba kupiti ločeno.

Zasebnost

Dostop do GPS

Tukaj lahko pogled GPS za vsako napravo zaščitite z 1 ali 2 gesli (načelo štirih oči). Ob vsakem poskusu dostopa do lokacije naprave boste morali vnesti geslo(a).

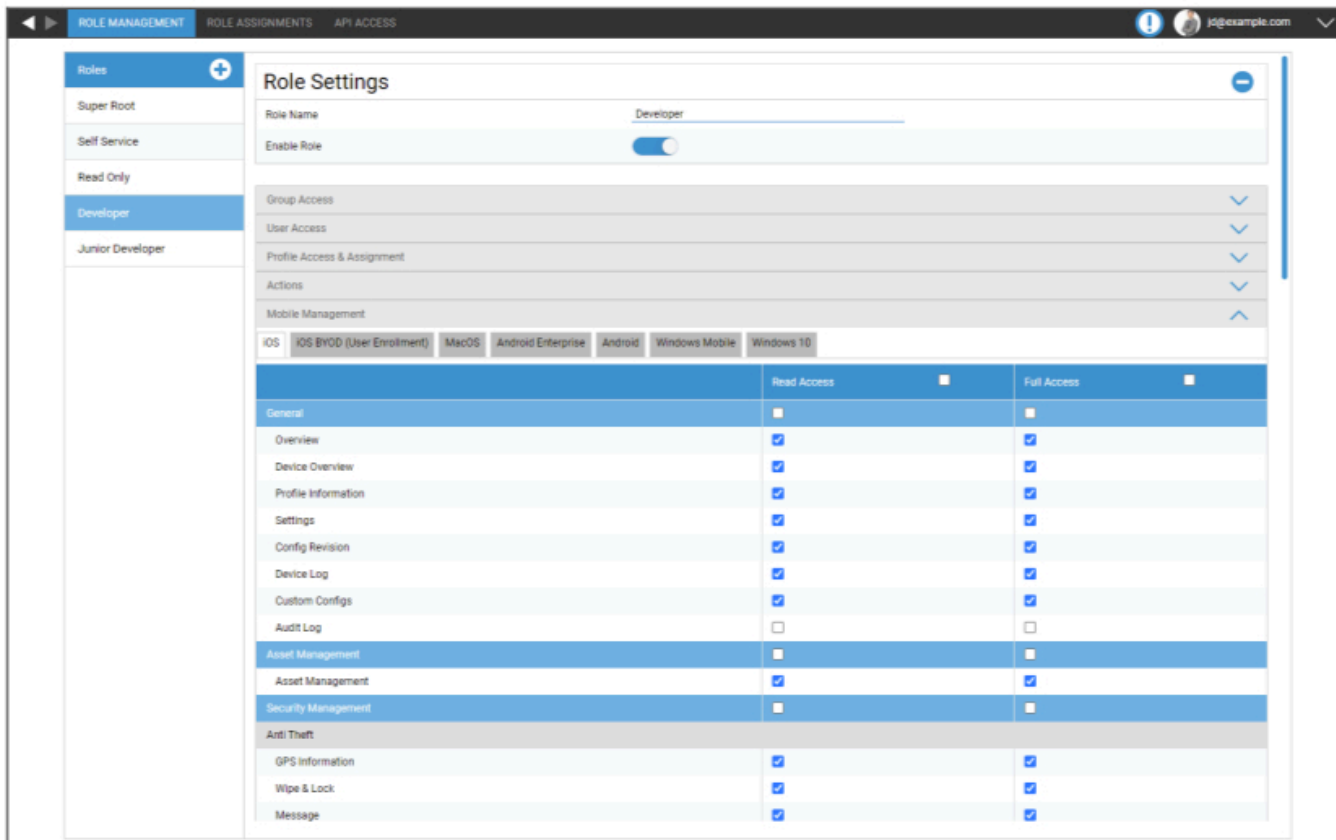
Omejitev dostopa do nastavitev GPS	Izklopljeno = funkcija je izklopljena in za lokalizacijo ni potrebno geslo.
	Vklopljeno = funkcija je vklopljena in za lokalizacijo je potrebno geslo.
Metoda zaščite	Uporabi eno geslo = uporabi eno geslo za lokalizacijo
	Uporaba dveh gesel = uporaba dveh gesel za lokalizacijo
Vnesite geslo (1)	Vnesite izbrano geslo
Ponovitev gesla (1)	Ponovno vnesite izbrano geslo
neobvezno: Vnesite geslo 2	Vnesite drugo izbrano geslo
neobvezno: Ponovite geslo 2	Ponovno vnesite drugo izbrano geslo

Opomba: Ko nastavite geslo(a), ga morate vnesti še enkrat, preden je popolnoma omogočeno.

Dostop na podlagi vlog

Upravljanje vlog

Vloge določajo, kaj lahko uporabnik vidi in počne, ko se prijavi v konzolo za upravljanje. Tako lahko ustvarite uporabnike, ki se lahko prijavijo, vendar imajo omejene funkcije.



OS	Read Access	Full Access
General	<input type="checkbox"/>	<input type="checkbox"/>
Overview	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Device Overview	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Profile Information	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Settings	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Config Revision	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Device Log	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Custom Configs	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Audit Log	<input type="checkbox"/>	<input type="checkbox"/>
Asset Management	<input type="checkbox"/>	<input type="checkbox"/>
Asset Management	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Security Management	<input type="checkbox"/>	<input type="checkbox"/>
Anti Theft	<input type="checkbox"/>	<input type="checkbox"/>
GPS Information	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Wipe & Lock	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Message	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

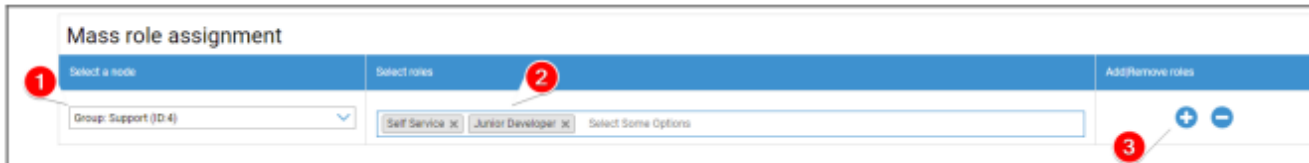
Vloga Super Root je privzeta vloga, ki lahko vedno vidi in spreminja vse. Ni je mogoče spremeniti ali izbrisati. Vloga za samopostrežbo lahko vidi le svoje uporabnike in naprave. Samopostrežno vlogo in vlogo po meri lahko združite, da npr. omogočite uporabnikom, da se prijavijo in vpišejo naprave sami in samo za svojega uporabnika.

Vloge po meri lahko ročno omogočite ali onemogočite. Nove vloge so privzeto onemogočene. Uporabniki z onemogočeno vlogo delajo, kot da je nimajo. To vam omogoča, da določeni vlogi npr. začasno omejite njena dejanja.

Vsa dovoljenja so razdeljena na "Dostop za branje" in "Polni dostop". Če vlogi omogočite dostop za branje, lahko vidi določen del konzole. Polni dostop omogoča vlogi, da vidi in spreminja določen del konzole.

Dodelitve vlog

Tu dobite pregled vseh uporabnikov, ki imajo vlogo, in vidite, katero vlogo imajo. Vlogo lahko dodelite tudi uporabnikom ali celotnim skupinam:

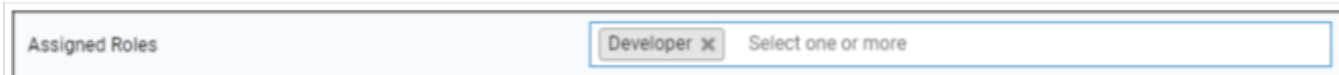


1. Izberite, za katero skupino ali uporabnika želite dodati ali odstraniti vloge. Izberete lahko posameznega uporabnika ali skupino. Če izberete skupino, bo vaša sprememba vplivala na vse uporabnike v tej skupini in na vse uporabnike podskupin znotraj izbrane skupine.
2. Izberite vlogo, ki jo želite dodati ali odstraniti. Izberete lahko eno ali več vlog.
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. Za dokončanje postopka shranite. Uporabniki, ki prej niso imeli vloge in so imeli onemogočeno možnost "Lahko se prijavim", bodo samodejno prejeli e-pošto s povezavo za nastavitev gesla.

Pod dodelitvijo masovne vloge je prikazan pregled dodeljenih vlog. Tam lahko tudi ročno spremenite vloge za določene uporabnike.

Dodelitev vloge

Če želite uporabniku dodeliti vlogo, morate iti v Upravljanje mobilnih naprav, kjer najdete drevo skupin, uporabnikov in naprav. Uredite uporabnika in mu dodelite vlogo. Druga možnost je, da zgoraj navedeno metodo uporabite tudi za posamezne uporabnike.



Dostop do API

Dostop do vmesnika AppTec360 REST API

API AppTec360 REST zahteva avtentikacijski žeton (ključ API) in zasebni ključ, ki ju je treba ustvariti v upravljalni konzoli.

V ta namen se prijavite v aplikacijo AppTec360 EMM in pojdite na

Splošne nastavitve → Dostop na podlagi vlog → Dostop do API in dodajte nov ključ.

Izbrati morate uporabnika, katerega dovoljenja bodo veljala za ključ API.

Zasebni ključ lahko prenesete samo enkrat. Ko se prenos začne, se ključ izbriše, gumb "Prenos" pa izgine.

Če izgubite zasebni ključ, morate ustvariti nov ključ API.

Splošna pravila

- API REST je na voljo pod osnovnim naslovom URL:

/public/external/api

- Vsi zahtevki morajo biti poslani prek protokola POST.
- API REST podpira samo zahteve prek protokola HTTPS.
- Zahteve morajo vsebovati naslednje glave:

Ime glave	Vrednost glave	Opis
Vrsta vsebine	application/json	popravljeno
avtentikacija	123...xyz	Ključ API z zavihka "Dostop do API".
podpis	podpis v kodi Base64	Podpis koristnega bremena, ustvarjenega z zasebni ključ z zavihka "Dostop do API".

- Telo zahteve mora biti kodiran objekt json, ki mora vsebovati naslednje vrednosti:

Polje	Polje Primer Vrednost	Opis
api	v2/device/listdevices	Ime API
čas	1529662725	Časovni žig Unix (UTC) odjemalskega računalnika. Največja dovoljena časovna razlika med odjemalcem in strežnikom je 30 minut.

- Ob uspehu API vrne zahtevane podatke (glejte poizvedbe spodaj) in kodo stanja HTTP 200.
- Če pride do napake, bo koda stanja HTTP med 4xx in 5xx, odvisno od napake, objekt odgovora pa bo vseboval polje s ključem "errors", ki vsebuje seznam človeku razumljivih sporočil o napakah.
- Če za napravo ni ustreznih podatkov, se vrne prazno polje.
- Če Id naprave ne obstaja, bodo vrnjeni podatki nič.

Primer zahteve

POST /public/external/api HTTP/1.1

Host: myapptecemm.com

Accept: /

Content-Type: application/jsonauth: 1234567890abcdefghijklmnopqrstuvwxyz

signature: a/bnOV466a0SiyVfsbpspZ+NxiTpmeF18NkfnOlq+OrEZDu9+VW7ESKziPXvw
 kTM5B9j/t1WGN1mRcIKe80m8fDKPj+lr3BqoMJe7wGXift+uy6iS7Chpdz2iZA4KPxxU9Z
 GU2cdQ/SQceX57pi+ch7ApxBeVX2+IJapTwA6CfB0mJFaf4MPcg/
 7LZWkzKxKF7LNzNJHiy/vSpZcqjbXjpC4HWrX6j2uZG5eSP8kYcTR
 9VQfGtKX9pcyaNAwguR7zOOwMu/8L0oKq21/19rkabE4ZgUjtKS2+
 +q+rh6mrP1g4BCZ7Xq/wvgZkaP
 b0CStBdMRvj46i3enxCXcLQQ==

Content-Length: 74

{"api": "v2/device/listposition", "time": 1529665112, "params": {"ids": [10]}}

Poizvedbe

Seznam vseh naprav

Funkcionalnost:

API URI: v2/device/listdevices

Obvezni parametri: ni

Izbirni parametri: ni

Primer telesa zahtevka

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

Primer telesa odgovora

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

Pridobi seznam položajev (GPS)

Funkcionalnost:

API URI: v2/device/listposition

Obvezni parametri: "ids" - polje identifikatorjev naprav

Neobvezni parametri: ni

Primer telesa zahtevka

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

Primer telesa odgovora

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

Pridobite zemljevid sredstev

Funkcionalnost:

Vrne seznam vseh shranjenih možnih sredstev, ki jih je treba zahtevati z uporabo funkcije Get any asset data.

Za zahtevo podatkov lahko uporabite človeku berljivo obliko ali oznako sredstva.

API URI: v2/device/getassetmap

Obvezni parametri: ni

Izbirni parametri: ni

Primer telesa zahtevka

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

Primer telesa odgovora

Ta odgovor je bil skrajšan zaradi lažje berljivosti.

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

Pridobite vse podatke o sredstvih

Funkcionalnost:

API URI: v2/device/getassetdata

Obvezni parametri:

"Neobvezni parametri:

"assetkeys" - ključni podatkov o sredstvih, ki jih je treba vrniti. Če ni navedeno, bodo vrnjeni vsi razpoložljivi podatki o sredstvih

. Seznam ključev sredstev lahko dobite z uporabo Get asset map (Pridobi zemljevid sredstev).

Primer telesa zahtevka

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

Primer telesa odgovora

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

Primer kode v Pythonu3

```
! /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-XXXXXXXXXXXXX.pem"
apptecAPIAuthToken = "7eXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX20"
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)
```

Konfiguracija Apple

Certifikat APNS

Tu lahko naložite potrdilo APNS. To je potrebno za upravljanje naprav iOS in MacOS.

Opomba: Potrdilo APNS velja le eno leto. Pred iztekom veljavnosti ga je treba obnoviti. Postopek obnovitve je enak postopku ustvarjanja (glejte spodaj) in traja le nekaj kratkih minut.

Če ga pozabite pravočasno obnoviti, ne morete spreminjati že vpisanih naprav. **in morate vse naprave ponovno vpisati.**



Korak 1

- Najprej vnesite svoj Apple ID, ki ga želite uporabiti za ustvarjanje potrdila APNS.

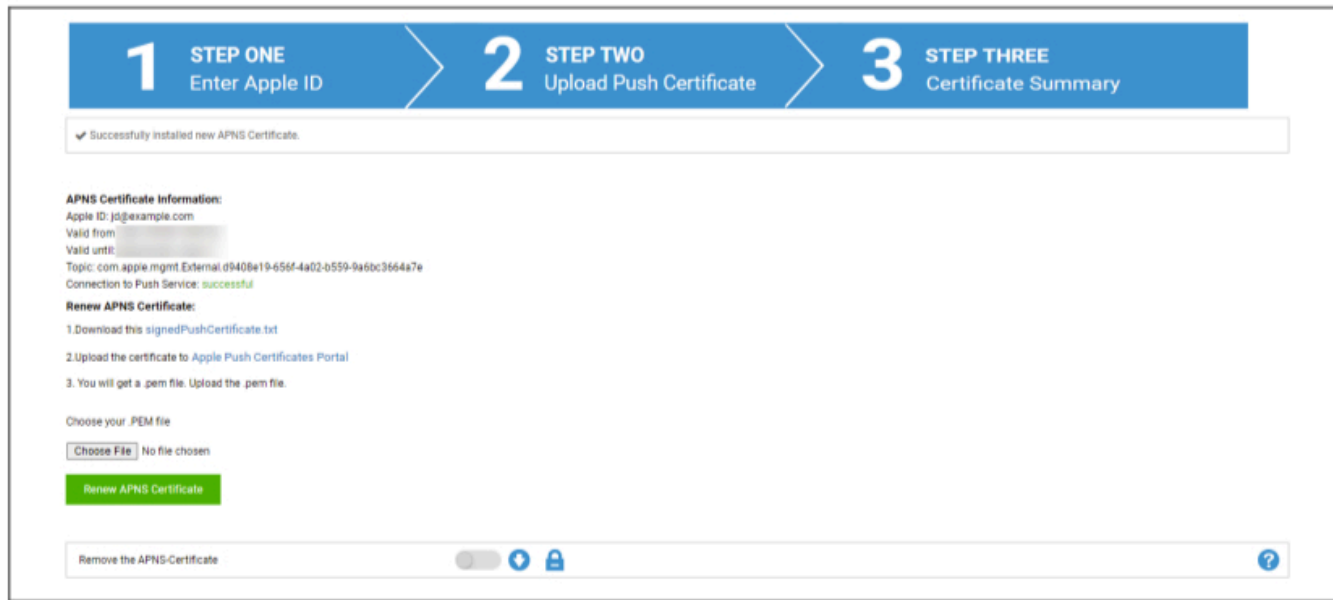
Opomba: Ta Apple ID se uporablja samo za ustvarjanje potrdila APNS. Ta Apple ID nima nobene zveze z napravami in naprave ne bodo vedele za ta Apple ID. Poleg tega potrebujete dostop do tega Apple ID tudi za obnovitev potrdila APNS. Zato je priporočljivo uporabiti neko splošno Apple ID in dokumentirati podatke za prijavo. Pred iztekom veljavnosti potrdila APNS se na uporabljeni poštni naslov Apple ID pošlje opomnik.

- Za nadaljevanje kliknite "Naslednji korak".
- (neobvezno) Če ste pomotoma izbrisali predhodno izbrisano potrdilo APNS, ga lahko tudi obnovite.



Korak 2

- Prenesite datoteko signedPushCertificate.txt
- Pojdite na [spletno stran https://identity.apple.com/pushcert/](https://identity.apple.com/pushcert/) in se prijavite z Apple ID iz koraka 1.
- Kliknite na "Ustvari potrdilo".
- (neobvezno) vnesite opombo. To je lahko koristno, če upravljate več najemnikov, da jih lažje prepoznate.
- Kliknite "Izberi datoteko" in izberite prej preneseni datotečni niz signedPushCertificate.txt
- Kliknite "Naloži".
- Zdaj boste videli potrditev, da ste ustvarili potrdilo APNS.
- Kliknite "Download" in ga shranite.
- Vrnite se v konzolo za upravljanje.
- Kliknite "Izberi datoteko" in izberite potrdilo APNS, ki ga želite naložiti.
- Kliknite na "Naloži".



Korak 3

Zdaj ste uspešno nastavili potrdilo APNS in lahko upravljate naprave iOS in MacOS.

V koraku 3 boste videli pregled trenutno uporabljenega certifikata APNS.

Prav tako imate možnost, da obnovite potrdilo APNS, tako da sledite korakom, prikazanim na zaslону. Ne pozabite ga obnoviti, preden poteče.

Pri obnovi potrdila APNS ne pozabite, da se morate prijaviti z Apple ID, prikazanim v koraku 3, in obnoviti že uporabljeno potrdilo ter NE ustvariti novega. "Tema" potrdila APNS bo prikazana v koraku 3 in ob kliku na "i" na portalu Apple Push Certificate Portal. To je edinstven ID, ki identificira potrdilo. To vam bo pomagalo pri prepoznavanju pravega in obnovitvi pravega.

Ko se prikaže "Napaka: To pomeni, da ste obnovili drugo potrdilo ali ustvarili novo.

Če želite naložiti novo potrdilo, npr. če ne morete več dostopati do predhodno uporabljenega Apple ID, morate najprej izbrisati trenutno naloženo potrdilo.

Kakor koli že, brisanje potrdila APNS pomeni, da ne morete več spreminjati trenutno vpisanih naprav, dokler jih ponovno ne vpišete. Zato se prepričajte, da ste na to pripravljeni, in certifikat odstranite le, če ni druge možnosti.

Upravljeni dostop

Tu lahko omogočite prijavo uporabnika za naprave iOS in skupni iPad za naprave iOS.

Vpis uporabnika

"Vpis uporabnika" omogoča poseben način za naprave BYOD.

Za vsakega uporabnika je treba v poslovnem portalu Apple ustvariti upravljeni Apple-ID.

Med postopkom vpisa bodo uporabniki morali navesti svoje poverilnice Apple-ID.

"Vpis uporabnika" zagotavlja največjo varnost za uporabnika, saj omogoča, da MDM konfigurira le omejen nabor nastavitev in omejitev.

Upravljana domena:

Domena, ki se uporablja za preslikavo uporabnikovega e-poštnega naslova na njegov upravljeni Apple-ID (mora biti v obliki: "@appleid.company.com").Npr. john.doe@example.com bo preslikan na john.doe@appleid.company.com.

V programu Apple Business Manager preverite upravljanjo domeno

Skupni iPad

iPad v skupni rabi je naprava DEP, konfigurirana s posebnim profilom DEP.

Tako se lahko več uporabnikov v napravo prijavi z upravljanim Apple-ID.

Upravljeni Apple-ID je treba ustvariti v Apple Business Portalu ali Apple School Managerju.

Uporabniki, ki se prijavijo v skupni iPad, morajo navesti svoje upravljanje poverilnice Apple-ID.

Upravljana domena:

Domena, ki se uporablja za preslikavo uporabnikovega e-poštnega naslova na njegov upravljeni Apple-ID (mora biti v obliki: "@appleid.company.com").Npr. john.doe@example.com bo preslikan na john.doe@appleid.company.com.

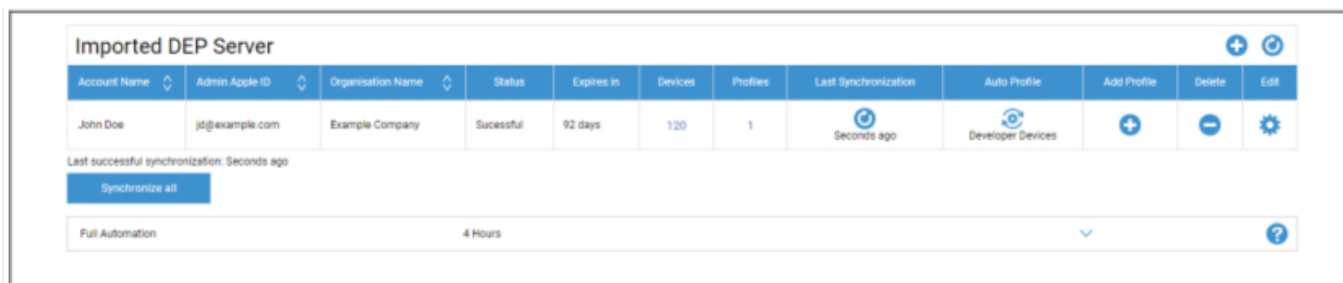
V programu Apple Business Manager preverite upravljanjo domeno

DEP

Program DEP (Device Enrollment Program) vam omogoča enostavno vpisovanje naprav v MDM. Če uporabljate DEP, bodo naprave ob nastavitvi naprave samodejno povezane z MDM. Prav tako lahko preskočite skoraj vse korake nastavitve, ki so v sistemu iOS običajno obvezni.

Ne pozabite, da morate naprave kupiti pri prodajalcu, ki podpira DEP. Za več informacij se obrnite na prodajalca ali Apple.

Več informacij o DEP: <https://www.apple.com/business/dep/>



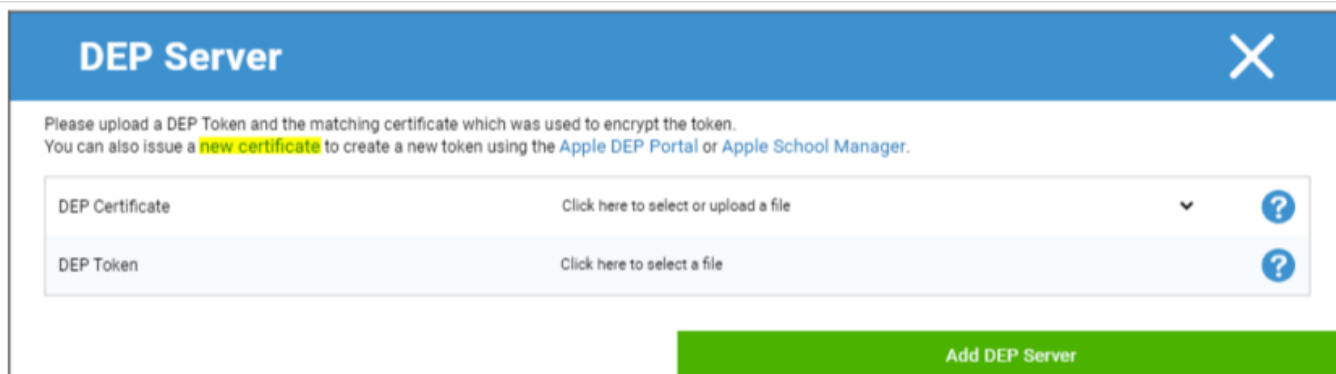
Account Name	Admin Apple ID	Organisation Name	Status	Expires in	Devices	Profiles	Last Synchronization	Auto Profile	Add Profile	Delete	Edit
John Doe	jd@example.com	Example Company	Successful	92 days	120	1	Seconds ago	Developer Devices	+	-	⚙️

Last successful synchronization: Seconds ago

Synchronize all

Full Automation: 4 Hours

Če želite dodati žeton DEP, kliknite na "+". V pojavnem oknu kliknite na "novo potrdilo" v besedilu (na spodnji sliki označeno z rumeno). To bo ustvarilo in preneslo potrdilo DEP. Nato pojdite v Apple Business Manager(<https://business.apple.com/>) ali Apple School Manager(<https://school.apple.com/>).



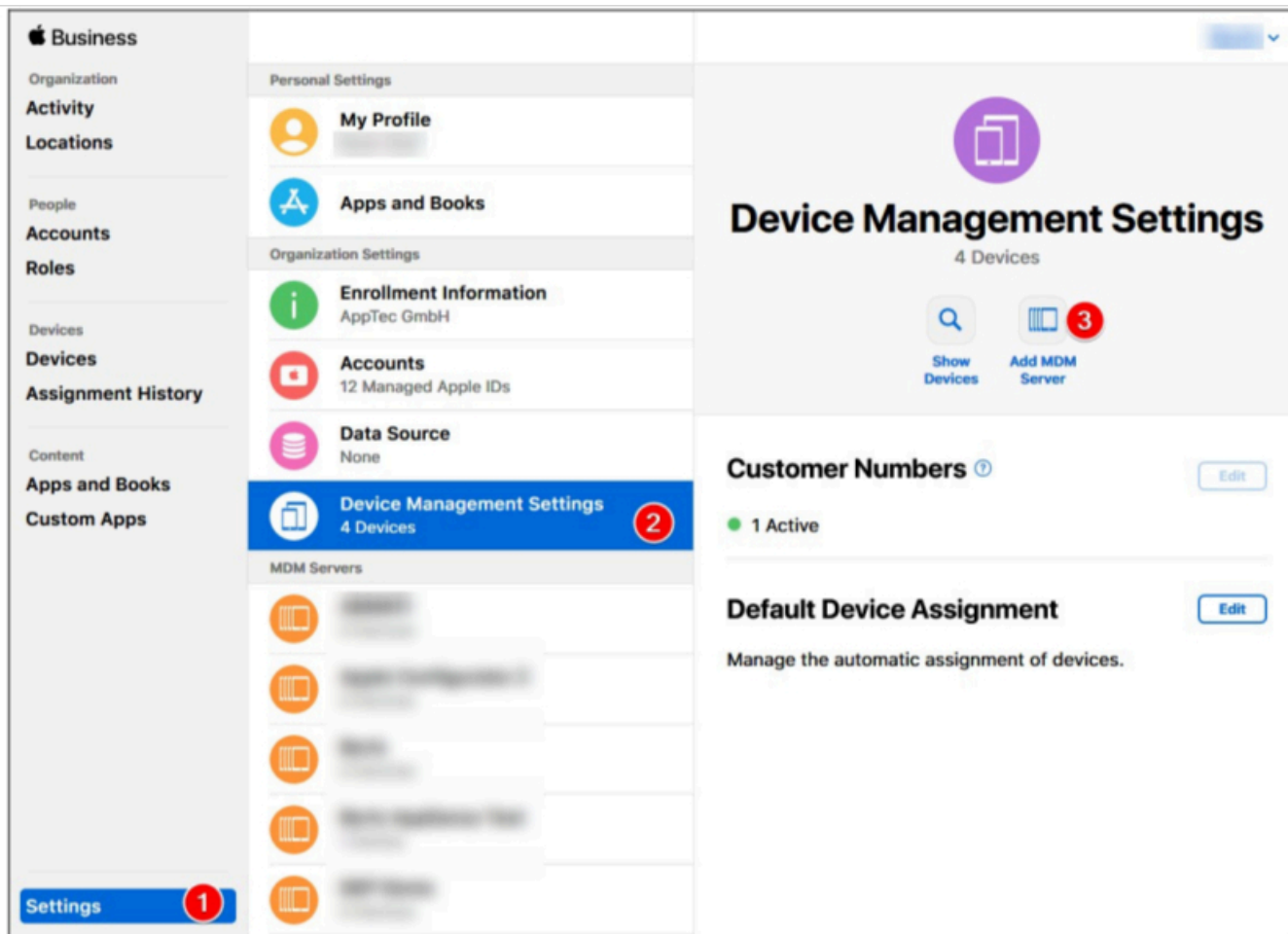
DEP Server

Please upload a DEP Token and the matching certificate which was used to encrypt the token.
You can also issue a **new certificate** to create a new token using the [Apple DEP Portal](#) or [Apple School Manager](#).

DEP Certificate Click here to select or upload a file

DEP Token Click here to select a file

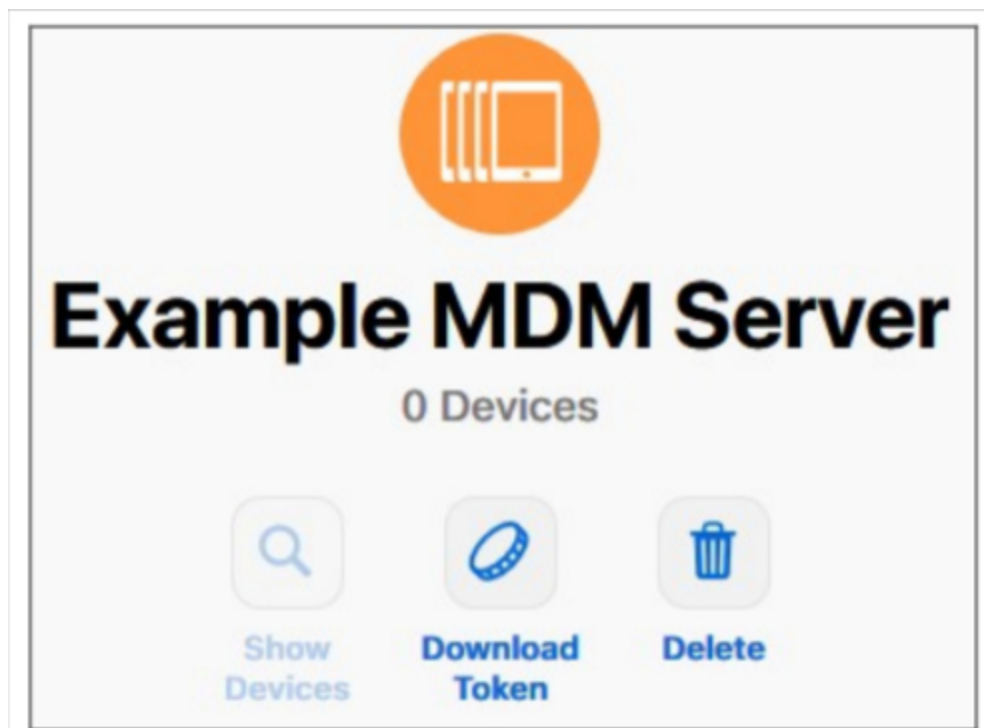
Add DEP Server



V programu Apple Business Manager sledite korakom, kot je prikazano na zgornji sliki. Nastavitve → Nastavitve upravljanja naprav → Dodaj strežnik MDM.

Strežniku dajte poljubno ime in prenesite predhodno preneseno potrdilo DEP v nastavitvah strežnika MDM → Upload Public Key in kliknite "Save".

Na voljo bo možnost "Prenesi žeton". Kliknite jo in jo shranite. Žeton velja le eno leto. Toda s ponovnim klikom na "Download Token" boste dobili nov žeton, zato je podaljšanje žetona zelo enostavno.



Zdaj se lahko vrnete v MDM, kamor ste prenesli potrdilo DEP. Če zavihka niste zaprli, mora biti pojavno okno za dodajanje strežnika DEP še vedno odprto in potrdilo DEP mora biti že izbrano. Zdaj lahko v polje "DEP Token" naložite svoj žeton in kliknete na DEP Server.

V stolpcu "**Naprave**" je prikazano število naprav, ki so dodeljene temu strežniku DEP. Naprave, dodane temu strežniku DEP, bodo samodejno ustvarjene v bazenu DEP v Upravljanju mobilnih naprav.

S klikom na to številko si lahko ogledate vse naprave DEP in njihovo stanje.

Opomba: Glede na potek dela ali konfiguracijo v Business Managerju se lahko zgodi, da boste morali te naprave ročno dodeliti strežniku DEP. V Apple Business Managerju lahko za nove naprave nastavite tudi privzeti strežnik DEP.

V stolpcu "**Profili**" je prikazano število profilov DEP, ki jih imate. S klikom na to številko si lahko ogledate podrobnosti o svojih profilih DEP in tukaj lahko izbrišete stare/neuporabljene profile. Trenutno jih ni mogoče spreminjati. Če jih želite spremeniti, morate ustvariti nove.

V stolpcu "**Zadnja sinhronizacija**" lahko ročno sinhronizirate strežnik DEP (npr. če ste v DEP pravkar dodali novo napravo) in si ogledate datum zadnje uspešne sinhronizacije.

V stolpcu "**Samodejni profil**" lahko nastavite profil DEP kot samodejno privzeto nastavitv. Ta profil bo samodejno dodeljen novim napravam. Če ne nastavite samodejnega profila, morate profil vsakič ročno dodeliti novim napravam.

V stolpcu "**Dodaj profil**" lahko dodate nov profil DEP. Naprava ga bo prejela na začetku nastavitve naprave. Profil DEP določa, kako se naprava nastavi in kateri koraki nastavitve bodo preskočeni.

Opomba: ko je naprava vpisana, lahko te nastavitve spremenite le tako, da izvedete tovarniško ponastavitev in vpišete napravo z novim profilom. To še posebej velja za možnosti "**Odstranljivo**" in "**Dovoli združevanje**". V primeru "**Allow pairing**" je priporočljivo to vklopiti, saj je to mogoče onemogočiti prek omejitev MDM, vendar tega ni mogoče ponovno omogočiti, če je to onemogočeno v profilu DEP.

V stolpcu "**Uredi**" lahko naložite nov žeton, npr. ob podaljšanju žetona.

Konfigurator in URL

URL-ji za vpis v bazen

Tu lahko ustvarite URL za vpis in kodo QR za vpis, ki velja za določen znesek vpisa in do določenega datuma. To vam omogoča vpis več naprav z eno samo povezavo ali kodo QR.

Naprave, vpisane s tem naslovom URL ali kodo QR, bodo v bazenu v Upravljanju mobilnih naprav, nato pa jih boste morali ročno dodeliti skupini ali uporabniku.

Opomba: to velja samo za ročni vpis. Če naprave vpisujete prek programa Apple Configurator, tega naslova URL ne uporabljajte.

Profil MDM – Apple Configurator

Tu lahko dobite URL, ki ga potrebujete pri vpisovanju naprav prek programa Apple Configurator. Pri pripravi naprav s programom Apple Configurator lahko v istem postopku naprave dodate v MDM. Apple Configurator za to potrebuje ta URL.

Naprave, dodane prek programa Apple Configurator, bodo v bazenu v Upravljanju mobilnih naprav, nato pa jih boste morali ročno dodeliti skupini ali uporabniku.

Tu boste našli tudi datoteko .mobileconfig, ki jo lahko uporabite za vpis naprav prek programa Apple Configurator. Vsekakor je priporočljivo uporabiti naslov URL.

Konfiguracija sistema Android

Konfiguracija sistema Android

Odstranitev zaščite	<p>Če je ta funkcija aktivirana, uporabnik ne more deaktivirati skrbnika naprave, ne da bi vnesel geslo, ki ga je določil skrbnik MDM. Geslo je nastavljeno med vpisom, zato je treba naprave za posodobitev gesla ponovno vpisati.</p> <p>Za odstranitev upraviteljev naprave obstajata dve možnosti:</p> <ol style="list-style-type: none"> 1. Ročno v napravi <ul style="list-style-type: none"> ○ Odprite aplikacijo EMM v napravi ○ Preklopite na zavihek Stanje ○ Tapnite "Odstranitev zaščite". ○ Vnesite geslo Za pridobitev pravilnega gesla lahko uporabite revizijo iz "Zgodovine gesel" v konzoli. ○ Pomaknite se navzdol in tapnite novo dodano točko "Tap to uninstall AppTec360 MDM App" (za izvedbo te naloge imate na voljo 20 sekund). ○ Potrdite dialog "Odstranitev aplikacije AppTec360 MDM App" z "ok". S tem bo naprava odjavljena iz konzole. ○ Če želite aplikacijo odstraniti iz naprave, potrdite dialog "AppTec360 MDM bo odstranjen" z "UNINSTALL". 2. samodejni (konzola) <ul style="list-style-type: none"> ○ Izberite napravo v konzoli ○ Kliknite na modro ikono zobnika in izberite "Enterprise Wipe". <p>Opomba: Na voljo samo z operacijskim sistemom Android 4.x in nižjimi različicami ali v napravah z vmesnikom KNOX API (naprave Samsung).</p>
Geslo za odstranitev (revizija x)	<p>Vzpostavljeno geslo, s katerim lahko uporabnik odstrani skrbnika naprave. Revizija x = števec, kolikokrat je bilo geslo že spremenjeno Pomembno je, katero geslo potrebuje uporabnik, saj je mogoče, da naprava ni</p>

	komunicirala s strežnikom AppTec360 in zato najnovejše geslo še ni bilo poslano.
Zgodovina gesel	Ko kliknete na modri gumb ("Prikaži zgodovino"), si lahko ogledate predhodno določena gesla.
Razširjena zaščita pred odstranitvijo	Ta možnost zagotavlja zaščito pred napravami, ki niso varne. Dokler je ta nastavitev aktivirana, skrbnika naprave ni mogoče preprosto deaktivirati.
Uporabnika pozovete, naj odstrani blokirane aplikacije?	Če je mogoče, blokirane aplikacije ne bodo samo blokirane, temveč tudi samodejno odstranjene. Če samodejna odstranitev ni mogoča, bo uporabnik pozvan k odstranitvi blokiranih aplikacij.
Blokiranje aplikacij inteligentnega sistema	Če je omogočena bela lista, odjemalec Android MDM blokira vse uporabniško nameščene aplikacije. Omogočite to nastavitev, če želite v načinu bele liste blokirati vse sistemske aplikacije, ki jih je mogoče zagnati.

Samodejni vpis

Tu lahko omogočite funkcijo samodejnega vpisa, da se naprave samodejno vpišejo, ko se v napravi odpre odjemalec AppTec360 MDM.

Pomembno: Ta metoda vpisa je zastarela in ne deluje več v operacijskem sistemu Android 10 ali novejšem. Če uporabljate sistem Android 7 ali novejši, morate naprave tako ali tako vpisati kot popolnoma upravljane naprave Android Enterprise. Če želite uporabiti vsebnik Android Enterprise BYOD in uporabljate sistem Android 10 ali novejši, morate napravo vpisati ročno prek poverilnic, kode QR ali sporočila SMS. Vsekakor se seznam za samodejno vpisovanje še vedno uporablja za avtomatizacijo postopka vpisovanja, npr. za vpisovanje AE, vpisovanje Knox itd.

Seznam samodejnega vpisa se še vedno uporablja za avtomatizacijo postopka vpisa, npr. za vpis AE, vpis Knox itd.

S klikom na "Serial Manager" ali "IMEI Manager" lahko dodate serijske številke oziroma IMEI svojih naprav. Za vaše naprave ni treba narediti obeh, dovolj je le ena.

Serial Auto Enrollment Manager ✕

Save Auto Enrollment List
Export as CSV
Import CSV
Show Group IDs
Add Serial

Filter table

Serial	Action	eMail / Group ID or Group Name	Dev. Type	Dev. Alias	Dev. Ownership	Delete?
UkY4SzMwWTJXVko	Auto Discover ▼	jd@apptec360.com	AE Container ▼	Galaxy S9+	Corporate ▼	<input type="checkbox"/>

If you select "Auto Discover" an eMail address is required. If you select "Assign to Group" the Group ID or the exact Group name is required"

You can easily add new entries by adding them at the end of a exported CSV. Import the CSV afterwards and save the new list.
 Example: ae78gf237,2,email@address.com,tablet,Tablet of User,employee

Ukrep določa, ali bodo naprave vpisane v bazen, uporabnika ali skupino.

Prav tako lahko izvozite in uvozite datoteko .csv ter filtrirate vnose po ključnih besedah.

Android Enterprise

Tu lahko nastavite Android Enterprise. To je potrebno za uporabo vseh funkcij Android Enterprise.

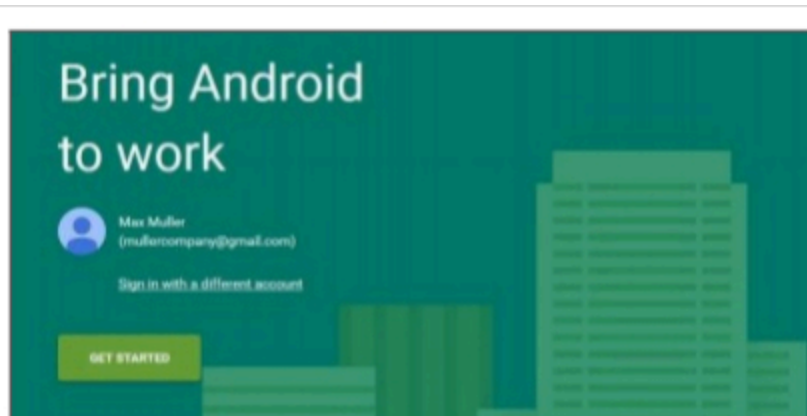
Prva metoda: Android Enterprise Account (Google račun)

Najprej pritisnite "Prepare Setup" (Pripravi nastavitve), po kratkem trenutku pa se mora prikazati gumb "Start Setup" (Začni nastavitve).

Tako boste prišli na Googlovo stran za nastavitve sistema Android Enterprise.

Če še niste prijavljeni, se prijavite z Googlovim računom, ki ga želite uporabljati, in pritisnite "Začni".

Zdaj lahko vnesete ime svojega podjetja. Ko to storite, označite potrditveno polje in pritisnite "Potrdi".



Organisation name
Max Muller Company

Enterprise mobility management (EMM) provider
AppTec Enterprise Mobile Manager

I have read and agree to the [Android for Work agreement](#).

V zadnjem koraku lahko dokončate registracijo in se vrnete v konzolo. Če je vse delovalo, mora biti videti takole:



Zdaj lahko začnete konfigurirati kontejner Android Enterprise Container.

Druga metoda: Račun G-Suite

Pritisnite "Use G-Suite" in se prijavite v svoj skrbniški račun Google. Tam pojdite na "Varnost" -> "Prikaži več" -> "Upravljanje ponudnika EMM za Android" in ustvarite žeton. Opomba: Če v svojem računu G-Suite ne vidite nastavitev podjetja za Android, morate iti v "Get more apps and services" in dodati upravljanje naprav za Android. Zdaj vnesite žeton in svojo primarno domeno v našo konzolo ter kliknite "Shrani spremembe". Ko končate, kliknite na "Use Android Enterprise Account".

Zdaj se prikaže gumb "Ustvari storitveni račun". Kliknite nanj. Ta postopek lahko traja nekaj trenutkov.

Če je vse delovalo, mora biti videti takole:



Zdaj lahko začnete konfigurirati kontejner Android Enterprise Container.

Zaščita pred ponastavitvijo tovarniških nastavitev

Z zaščito za ponastavitev tovarniških nastavitev lahko napravo povežete z izbranim računom Google, ki tudi prekrije vse obstoječe povezave z računom Google. Če želite uporabljati funkcijo Zaščita pred ponastavitvijo tovarniškega delovanja, jo morate najprej nastaviti tukaj in jo nato aktivirati v svojih profilih.

Če želite nastaviti zaščito pred ponastavitvijo tovarniških podatkov, kliknite "FRP Setup" in sledite navodilom na zaslonu.

OPOMBA: Pozorno preberite in izvedite naslednje korake. Priporočamo, da to storite v novem oknu brskalnika inkognito, da se izognete samodejni prijavi v napačen Google Račun. Če vnesete napačno ID ali izgubite dostop do uporabljenega računa Google, se lahko popolnoma zaklenete iz naprave!

AE Vpis

Tu lahko aktivirate Android Enterprise Enrollment. Z uporabo te metode bodo vaše naprave vpisane v način lastnika naprave Android Enterprise. V tem načinu boste imeli popoln nadzor nad napravo.

Omogoči vpis AE	Aktivira AE Enrolment Caution: Če onemogočite AE Enrollment, obstoječe kode QR in že konfigurirane naprave za programiranje NFC ne bodo več delovale. Če AE Enrollment ponovno omogočite, boste morali ponovno poslati konfiguracije za potiskanje NFC / ustvariti nove kode QR.
Omogočanje samodejnega odkrivanja	Ko se naprava prijavi prek funkcije "AE Enrollment", jo bo sistem poskušal dodeliti uporabniku na podlagi informacij, nastavljenih v beli listi serijskih števil / IMEI ("General Settings" > "Android Configuration" > "Auto Enrollment").
Blokiranje neznanih naprav	Samo naprave, ki so bile uvrščene na belo listo Serial / IMEI Whitelist ("Splošne nastavitve" > "Konfiguracija sistema Android" > "Samodejno vpisovanje"), se lahko vpisujejo.

Opomba za metodo 1 in 2: "Dobrodošel zaslon" se nanaša na prvi zaslon, ki se prikaže po tovarniški ponastavitvi. Ta se lahko razlikuje glede na različico Androida in/ali model naprave, ki jo uporabljate.

Metoda 1: Vpis kode QR

(zahteva operacijski sistem Android 7.0 ali novejši) Če uporabljate operacijski sistem Android 7 ali novejši, priporočamo, da vedno uporabite to metodo.

1. Tovarniška ponastavitev naprave
2. Kodo QR za vpis ustvarite na enega od naslednjih dveh načinov:
 - V razdelku "Splošne nastavitve -> Konfiguracija Androida -> AE Enrollment" kliknite na "Generate QR Code". Izberite, ali želite preskočiti šifriranje shrambe in/ali odstraniti vse sistemske aplikacije.
 - (alternativno) Izberite obstoječo napravo. V "Pregled naprave" kliknite na prikazano kodo QR. Izberite, ali želite preskočiti šifriranje shrambe in/ali odstraniti vse sistemske aplikacije.
3. Zdaj šestkrat tapnite na pozdravnem zaslonu naprave. S tem se bo začel način vpisa QR.
4. Zdaj se povežite z brezžičnim omrežjem in počakajte, da se bralnik kod QR namesti.
5. Zdaj preberite kodo QR
6. To je to. Vaša naprava je zdaj vpisana v način naprave Android Enterprise.

- a. Če ste v splošnih nastavitvah uporabili kodo QR, lahko svojo napravo najdete v razdelku "Pool -> AE Device Owner Devices". (Namig: Možno je, da boste morali ponovno naložiti spletno mesto, da boste videli naprave). Če ste potrdili možnost "Omogoči samodejno odkrivanje", jo boste našli znotraj uporabnika za samodejno odkrivanje.
- Če ste uporabili kodo QR obstoječega profila naprave, bo naprava vpisana v ta profil.

Metoda 2: Vpis NFC

(zahteva NFC in Android 6.0 ali novejši)

Priprava: Vnesite podatke o WiFi v "Splošne nastavitve -> Konfiguracija Androida -> Prijava AE -> Podatki za zagotavljanje NFC". Sedaj uporabite "NFC Device" za iskanje naprave, ki bo postala programator. Ta naprava bo uporabljena za pošiljanje podatkov o vpisu drugim napravam prek NFC.

1. Ponastavitev naprave na tovarniško nastavitev
2. Odprite aplikacijo za seznanjanje NFC iz programa AppTec360 na programatorju.
3. Izberite, ali želite preskočiti šifriranje shrambe in/ali odstraniti vse sistemske aplikacije.
4. Obe napravi držite drugo za drugo
5. Zdaj bi moral Android Enterprise Enrolment močno
6. V konzoli zdaj najdete svojo napravo.
 - a. Če v bazenu niste konfigurirali samodejnega odkrivanja
 - b. V uporabniku, ki ste ga konfigurirali za samodejno odkrivanje
 - c. Namig: Morda boste morali znova naložiti spletno mesto, da boste videli naprave.

Metoda 3: Google račun

(zahteva operacijski sistem Android 5.1 ali novejši)

(Opomba: Če uporabljate to metodo, naprava ne bo samodejno vpisana. Namesto tega jo morate vpisati ročno ali pa postopek avtomatizirati z uporabo samodejnega vpisa.)

1. Ponastavitev naprave na tovarniško nastavitev
2. Opravite korake za nastavitev, dokler se ne morete prijaviti z računom Google.
3. Kot uporabniško ime/naslov vnesite "afw#apptec".
4. Tapnite "Naprej".
5. Vaša naprava je zdaj naprava Android Enterprise

KNOX Vpis

Tu lahko aktivirate vpis KNOX in najdete informacije, ki jih potrebujete za ustvarjanje vpisnega profila KNOX na portalu za uvajanje KNOX. Za konfiguracijo in uporabo potrebujete račun na portalu KNOX Deployment Portal.

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

Omogočite vpis KNOX	Aktivira vpis KNOX. Pozor: Če onemogočite vpis KNOX, obstoječi profili MDM ne bodo več delovali. Če ponovno omogočite KNOX Enrollment, boste morali posodobiti polje "Podatki JSON po meri" v profilu MDM.
Omogočanje samodejnega odkrivanja	Ko se naprava prijavi prek funkcije "KNOX Enrollment", jo bo sistem poskušal dodeliti uporabniku na podlagi podatkov, nastavljenih v beli listi serijskih števil / IMEI ("Splošne nastavitve" > "Konfiguracija sistema Android" > "Samodejno vpisovanje").

1. Prijavite se v portal Samsung KNOX Mobile Enrolment Portal
<https://eukme.samsungknox.com/itadmin>.
2. Pojdite na "Profili MDM".
3. Kliknite na "Dodaj".
4. Izberite "Server URI not required for my MDM" in kliknite "Next".
5. Ustvarite profil z informacijami, ki so prikazane v konzoli za upravljanje.

Ta profil za vpis KNOX lahko Samsung neposredno namesti v napravo, če naprave pridobite neposredno od Samsunga.

Lahko pa prenesete aplikacijo KNOX Deployment App, se prijavite s svojim računom KNOX Deployment Account in profil za vpis KNOX prek NFC pošljete drugim napravam.

Če ima naprava nameščen profil za vpis KNOX, bo prenesla našo aplikacijo in vpisala napravo, če ima delujočo internetno povezavo.

Vpis naprav prek funkcije KNOX Enrollment lahko najdete v razdelku "Pool -> KNOX Enrollment" ali v uporabniku, ki ste ga določili v funkciji Auto Discover.

Brez dotika

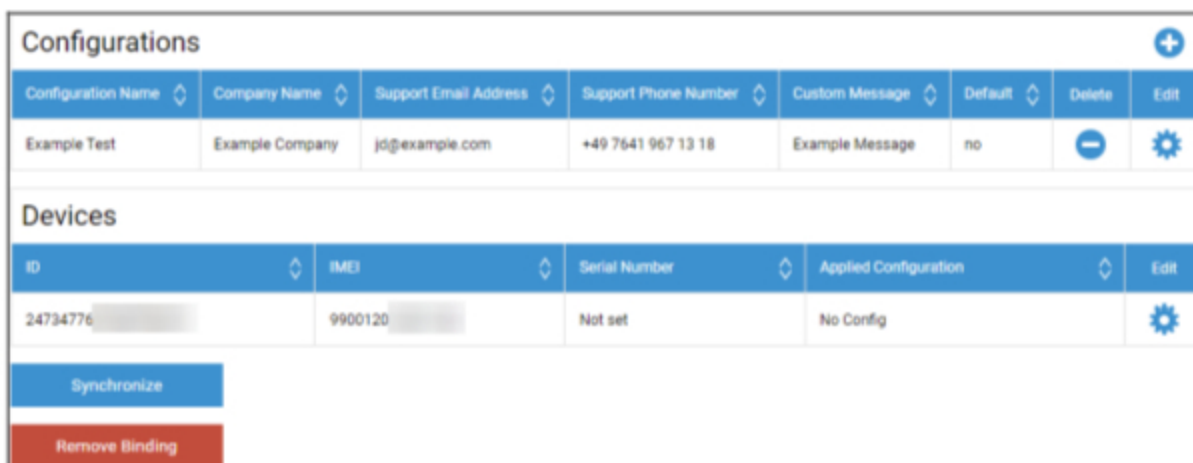
S funkcijo Zero-Touch lahko preprosto registrirate svoje naprave, ne da bi se jih morali dotakniti ali kar koli konfigurirati v sami napravi. Samo vklopiti jo morate, nadaljevati z običajno konfiguracijo in naprava bo popolnoma samodejno prejela vse informacije o tem, kako nastaviti in se povezati z MDM.

Če želite uporabljati funkcijo Zero-Touch, morate naprave kupiti pri prodajalcu, ki podpira funkcijo Zero-Touch. Isti preprodajalec za vas ustvari tudi račun na portalu Zero-Touch. Za več informacij o postopku ali v primeru težav pri dostopu do portala Zero-Touch se obrnite na preprodajalca.

Kliknite "Start Setup", da začnete z nastavitvijo. Preusmerjeni boste na prijavno stran, kjer morate izbrati svoj Google račun, ki ima dostop do portala Zero-Touch.

OPOMBA: Izberete lahko katerikoli račun. Zato v tem koraku izberite pravi račun. Če ne vidite svojih naprav/konfiguracij, ste najverjetneje uporabili napačen račun.

Po končani prijavi bo videti takole:



Configurations								
Configuration Name	Company Name	Support Email Address	Support Phone Number	Custom Message	Default	Delete	Edit	
Example Test	Example Company	jd@example.com	+49 7541 967 13 18	Example Message	no	–	⚙️	

Devices				
ID	IMEI	Serial Number	Applied Configuration	Edit
24734776	9900120	Not set	No Config	⚙️

Synchronize

Remove Binding

Če želite dodati konfiguracijo, kliknite na "+" in izpolnite polja, kot so prikazana na zaslonu. Če konfiguracijo omogočite kot privzeto konfiguracijo, bo samodejno dodeljena novim napravam. Ustvarjanje ali nastavljanje privzete konfiguracije je ne dodeli že obstoječim napravam.

Če naprava nima dodeljene konfiguracije, se nastavi kot običajna naprava in se ne poveže z MDM. Zato se prepričajte, da je napravam dodeljena konfiguracija.

Ko ste povezali račun, so naprave vidne in jim je dodeljena konfiguracija, lahko začnete nastavljanje naprave.

Naprave lahko dodate na seznam samodejnega vpisa, tako da bodo samodejno vpisane v določeno skupino ali uporabnika. Če na seznamu za samodejno vpisovanje niste ničesar konfigurirali, bodo naprave vpisane v skupino.

Konfiguracija sistema Windows

Konfiguracija sistema Windows

Tu lahko omogočite naslednje konfiguracije v računalniku z operacijskim sistemom Windows 10:

Takojšnja DM povezava	
Začetni čas ponovitve	Vzpostavi prvi poskus povezave z napravo, ta vrednost se eksponentno povečuje.
Ponovitve povezave	Označuje, koliko poskusov vzpostavitve povezave naj odjemalec DM izvede med napako pri vzpostavitvi povezave.
Najdaljši čas spanja	Označuje najdaljši čas mirovanja po napaki v povezavi
Prvi ponovni poskusi sinhronizacije	Intervali, v katerih mora naprava komunicirati s strežnikom po prvi povezavi
Interval prvega ponovnega poskusa	Se nanaša na "Prvi ponovni poskusi sinhronizacije". Tu so časi navedeni v minutah. Na primer, pod "First Sync Retries" (Prvi ponovni poskusi sinhronizacije) je navedena vrednost "2", pod "First Retry Interval" (Interval prvih ponovnih poskusov) pa vrednost "4 Minutes" (4 minute), tako da naprava po prvi povezavi komunicira dvakrat na vsake 4 minute.
Drugi ponovni poskusi sinhronizacije	Intervali, v katerih mora naprava komunicirati s strežnikom, potem ko je končala "Prve ponovitve sinhronizacije".
Drugi interval ponovitve	Enako načelo kot pri "First Retry Interval" - le da tukaj velja za "Second Sync Retries".
Redni ponovni poskusi sinhronizacije	Intervali, kako pogosto naj naprava v prihodnosti komunicira s strežnikom. Privzeto: "Neskončno" Priporočamo, da te vrednosti ne spreminjate, ker če vnesete "10", bo naprava 10x komunicirala s strežnikom in nato prenehala. Zato je komunikacija s strežnikom AppTec360 prekinjena!
Redni interval ponavljanja	Enako načelo kot pri "Intervalu prvega/drugega ponovnega poskusa" - le da se tu uporabljajo nastavitve za prihodnost.

Redni interval ponavljanja	Enako načelo kot pri "Intervalu prvega/drugega ponovnega poskusa" - le da se tu uporabljajo nastavitve za prihodnost.
----------------------------	---

Vsebinsko polje

Konfiguracija

Tu lahko konfigurirate vsebinsko polje. V ContentBox lahko namestite datoteke za skupine, do katerih lahko dostopate z aplikacijo ContentBox v napravi.

Omogočanje vsebinskega polja	Omogočite vsebinsko polje. Če tega ne uporabljate ContentBoxa, lahko prihranite vire v računalnikih OnPremise.
Uporaba zunanje namestitve ContentBox	ContentBox lahko upravljate tudi z lastnim Nextcloudom.
URL	Celoten URL entitete Nextcloud
Korenski uporabnik	Korenski uporabnik računa Nextcloud
Korensko geslo	Korensko geslo računa Nextcloud
Privzeta dovoljenja skupinskih map	Privzeta dovoljenja skupinskih map, ki jih je mogoče individualno spreminjati po skupinah (v Upravljanju mobilnih naprav).
Skupinska mapa v skupni rabi s podskupinami	Če je aktivna, lahko vsaka podskupina prebere vse mape glavne skupine, lahko pa jo tudi individualno konfigurirate za vsako skupino (upravljanje mobilnih naprav).
Dovoljenja za podskupine	Dovoljenja za podskupine lahko konfigurirate za vsako skupino posebej (upravljanje mobilnih naprav).
Omogočanje souporabe	Uporabniku omogoča deljenje vsebine prek povezav, ki jih je mogoče konfigurirati za vsako skupino posebej.
Največja velikost prenesene datoteke v MB	Največja velikost datoteke Standardno: 512 MB Največja konfiguracija: 2048
Pooblastila WebDAV	
URL WebDAV	Vsebinsko polje lahko odprete tudi z WebDAV. V nobenem primeru ne brišite naslednjih map: /apptecgroups /apptecgroups/AppTecGroup-X
Korenski uporabnik	Ime korenskega uporabnika
Geslo	Geslo korenskih uporabnikov

Sinhronizacija z okencem ContentBox se izvede samodejno. Lahko pa izvedete ročno sinhronizacijo s funkcijo "Sinhroniziraj ContentBox".

Poleg tega lahko tukaj aktivirate/deaktivirate ContentBox v vsaki posamezni napravi.

To je pomembno le, če niste dodatno licencirali programa ContentBox, potem imate še vedno dostop do 25 naprav, s katerimi lahko preizkusite program ContentBox - tukaj lahko to aktivirate za ustrezne naprave.

Konfiguracija LDAP

Pregled protokola LDAP

Tu lahko vzpostavite povezavo z imenikom Active Directory prek protokola LDAP in množično uvozite uporabnike in skupine. Sinhronizacijo je treba izvesti ročno. Nastavite lahko več povezav LDAP z različnimi sistemi ali z različnimi konfiguracijami/filtri.

Ime strežnika	Prikazno ime strežnika
Tip	Trenutno so podprti samo aktivni imeniki, ki podpirajo LDAP.
Domena LDAP	Primarna domena LDAP (npr. example.com)
Gostitelj LDAP	Potrebno samo, če gostitelj LDAP ni dosegljiv v dani domeni LDAP.
Pristanišče	Pustite prazno za uporabo standardnih vrat (389 ali 636 za SSL)
Uporabniško ime	Npr. CN=John,OU=Users,DC=EXAMPLE,DC=COM Opomba: Večina sistemov zahteva uporabniško ime v tej obliki in ne sprejme "John" kot uporabniško ime.
Geslo	
Potrditev gesla	
Varnost povezave	Opomba: če uporabljate protokol SSL ali TLS, se preveri potrdilo aktivnega imenika. Če je to samopodpisano, morate korenski CA dodati v skladišče zaupanja naprave OnPremise. Če ste v oblaku, mora imenik Active Directory zagotoviti zaupanja vredno potrdilo, sicer bo povezava delovala le brez šifriranja
Samodejna sinhronizacija.	Omogoča samodejno sinhronizacijo imenika LDAP v časovnem intervalu, določenem v splošnih nastavitvah LDAP.
Osnovni DN	Če ne želite sinhronizirati celotnega imenika, lahko tukaj določite OU.Npr. OU=AndroidUsers,OU=Users,DC=EXAMPLE,DC=COM
Član	Vsi uvoženi uporabniki bodo dodani v izbrano skupino.
Samo aktivirani uporabniki?	Če je omogočeno, se bo upošteval atribut userAccountControl, uporabniki brez tega atributa ne bodo uvoženi.
Filter LDAP	S filtrom LDAP lahko filtrirate, kateri uporabniki se uvozijo.
Filter Regex	Za filtriranje uporabnikov, ki se uvozijo, lahko uporabite filter Regex
Testna povezava	Preizkuša povezavo ob shranjevanju konfiguracije
Ponastavitev strukture imenikov ob sinhronizaciji?	Če je to res, se vsi vnosi LDAP premaknejo nazaj na prvotno lokacijo v drevesu LDAP. Priporočljivo, da je omogočeno.

Ponovni uvoz izbrisanih uporabnikov in skupin?	Če je ta možnost omogočena, se izbrisani uporabniki in skupine ponovno ustvarijo. Priporočljivo je, da se omogoči.
Sinhronizacija izbrisov?	Če je ta možnost omogočena, se skupine in uporabniki izbrišejo, ko so izbrisani v strežniku LDAP. Izbrišejo se tudi naprave izbrisanih uporabnikov.

Pod seznamom konfiguracij LDAP lahko določite obdobje, v katerem se sistem samodejno sinhronizira. Za samodejno sinhronizacijo se uporabljajo samo Konfiguracije LDAP, pri katerih je aktivirana ustrezna možnost.

Upravljanje aplikacij

Notranja aplikacija DB

Android

Tu lahko naložite aplikacije za Android, ki jih je razvilo vaše podjetje, in jih pozneje razdelite v programu Mobile Management v profile naprav ali skupin.

Zavedajte se, da svetujemo, da na ta način distribuirate samo aplikacije, ki niso na voljo v trgovini Google Play.

S klikom na "+" naložite APK aplikacije, ki jo želite naložiti. Trenutno je podprta samo oblika APK.

Omejitev prenosa v napravah OnPremise lahko povečate v 3. koraku konfiguracije naprave. Če želite povečati omejitev nalaganja v oblaku, se za več informacij obrnite na podporo.

Zavedajte se, da so paketi APK običajno nekoliko manjši od svoje vsebine. Možno je, da nalaganje zaradi tega ne uspe, saj se APK med postopkom razpakira. Na primer, možno je, da 95 MB velik APK ni uspešen pri omejitvi prenosa 100 MB. V tem primeru povečajte omejitev prenosa, kot je navedeno zgoraj.

Svetujemo vam tudi, da APK najprej ročno prenesete v eno testno napravo (npr. prek USB) in ga poskusite ročno namestiti z aplikacijo Datoteke v napravi. Če to iz kakršnegakoli razloga ne bo delovalo, bo neuspešna tudi namestitev prek MDM.

Cilj posodobitve

S funkcijo "Cilj posodobitve" lahko izberete različico aplikacije, ki naj bo nameščena, ali različico, na katero naj bo aplikacija posodobljena, če ste za aplikacijo aktivirali možnost "Posodobi".

Če niste izbrali cilja posodobitve, bo uporabljena najvišja različica.

Upoštevajte, da Android ne more znižati vrednosti aplikacij. Prav tako se zavedajte, da "koda različice" določa, ali je različica višja, nižja ali enaka. Zato se prepričajte, da ste pri izdelavi posodobitve pravilno povečali to različico v svoji aplikaciji.

iOS

Tu lahko naložite aplikacije za iOS, ki ste jih razvili, in jih pozneje razdelite v programu Mobile Management v profilu naprave ali skupine.

S klikom na "+" naložite IPA aplikacije, ki jo želite naložiti. Za zdaj je podprta samo oblika IPA.

Omejitev prenosa v napravah OnPremise lahko povečate v 3. koraku konfiguracije naprave. Če želite povečati omejitev nalaganja v oblaku, se za več informacij obrnite na podporo.

Cilj posodobitve

S funkcijo "Cilj posodobitve" lahko izberete različico aplikacije, ki naj bo nameščena, ali različico, na katero naj bo aplikacija posodobljena, če ste za aplikacijo aktivirali možnost "Posodobi".

Če niste izbrali cilja posodobitve, bo uporabljena najvišja različica.

MacOS

Tu lahko naložite aplikacije za MacOS, ki ste jih razvili, in jih pozneje razdelite v programu Mobile Management v profilu naprave ali skupine.

S klikom na "+" naložite PKG aplikacije, ki jo želite naložiti. Za zdaj je podprta samo oblika PKG.

Omejitev prenosa v napravah OnPremise lahko povečate v 3. koraku konfiguracije naprave. Če želite povečati omejitev nalaganja v oblaku, se za več informacij obrnite na podporo.

Cilj posodobitve

S funkcijo "Update Target" lahko izberete, katera različica aplikacije naj bo nameščena ali na katero različico naj bo posodobljena, če ste za aplikacijo aktivirali funkcijo "Keep up to date".

Če niste izbrali cilja posodobitve, bo uporabljena najvišja različica.

Windows 10

Tu lahko prenesete aplikacije Windows 10 in jih pozneje razdelite v mobilnem upravljanju v profilu naprave ali skupine.

S klikom na "+" naložite APPX, APPXBUNDLE ali MSI aplikacije, ki jo želite naložiti. Za zdaj je podprta samo oblika APPX, APPXBUNDLE ali MSI.

Za aplikacijo lahko naložite in določite tudi odvisnosti, ki se samodejno razdelijo in namestijo pred namestitvijo zelene aplikacije.

Omejitev prenosa v napravah OnPremise lahko povečate v 3. koraku konfiguracije naprave. Če želite povečati omejitev nalaganja v oblaku, se za več informacij obrnite na podporo.

Cilj posodobitve

S funkcijo "Update Target" lahko izberete, katera različica aplikacije naj bo nameščena ali na katero različico naj bo posodobljena, če ste za aplikacijo aktivirali funkcijo "Keep up to date".

Če niste izbrali cilja posodobitve, bo uporabljena najvišja različica.

Paket Win32 (.exe)

Datoteke .exe/namestitvene programe lahko razpošiljate tudi v svoje naprave.

Ime paketa	Ime, ki bo prikazano v MDM
Opis	Opis, prikazan v MDM
Datoteka paketa	Dovoljene so samo datoteke .zip. Datoteke, ki jih želite namestiti, vstavite v to datoteko zip.
Kontekst uvajanja	Sistem: Ukaz za namestitev se zažene s sistemskimi privilegiji, ki so višji od privilegija "Uporabnik". Prav tako pri uporabi "System" proces nima uporabniškega vmesnika, zato bo neslišen in uporabniški profil, npr. okoljske spremenljivke, kot je %AppDat%, ni dostopen. Uporabnik: Ukaz za namestitev ima dostop do uporabniškega profila in lahko po potrebi prikaže uporabniški vmesnik. Opomba: Nekateri procesi lahko delujejo samo v enem kontekstu. Npr. če se programska oprema namesti v datoteko AppData, bo delovala samo ob izbiri možnosti "Uporabnik".
Ukaz za namestitev	Ukaz, uporabljen za namestitev programa. Na primer namestitveni ukaz za datoteko zip, ki v svojem korenu vsebuje "setup.exe", ki podpira parameter "/s" za tiho namestitev, bi bil namestitveni ukaz "setup.exe /s". Zavedajte se, da imajo lahko različni programi različne parametre.
Ukaz za odstranitev	Ukaz, ki ga zaženete za odstranitev programske opreme prek MDM. Običajno kaže na program za odstranjevanje. Na primer "C:\Program Files\ExampleSoftware\uninstall.exe".
Zahteve	
Opomba: Za namestitev programske opreme morajo biti izpolnjene vse določene zahteve. V nasprotnem primeru ne bo nameščena. Nekatera polja so lahko obvezna. Če za zahtevo ni nastavljena nobena vrednost, se zahteva ne upošteva.	
Arhitektura operacijskega sistema	Arhitektura operacijskega sistema
Min različica operacijskega sistema	Min različica operacijskega sistema
Najmanjši prosti prostor na disku (MB)	Najmanjši prosti prostor na disku (MB)
Najmanjši fizični pomnilnik	Najmanjši fizični pomnilnik (MB)

(MB)	
Najmanjše število logičnih procesorjev	Najmanjše število logičnih procesorjev
Min. hitrost procesorja (MHz)	Min. hitrost procesorja (MHz)
Dodatne zahteve	Če želite, lahko tu tudi ročno določite pravila ali naložite skripto za izvajanje dodatnih preverjanj zahtev.
Pravila odkrivanja	
Metoda odkrivanja	Tu lahko določite, kako zaznati, ali je aplikacija nameščena v napravi. Ukazi za namestitve se izvedejo le, če ta pravila zaznajo, da aplikacija NI nameščena. Ukazi za odstranitev se izvedejo le, če ta pravila zaznajo, da aplikacija ni nameščena. Ročno opredelite pravila: V tem primeru lahko ročno določite eno ali več pravil, s katerimi na primer preverite prisotnost določene datoteke, mape, ključa MSI ali ključa registra. Če so vsa navedena pravila za zaznavanje resnična, se aplikacija šteje za prisotno. Uporabi skripto: Naložite lastno skripto z lastnimi preverjanji. Če skripta vrne "\$TRUE", se aplikacija šteje za prisotno.
Pravila odkrivanja	

Nastavitve aplikacije

Nastavitve aplikacije iOS

Tu lahko določite privzete nastavitve za dodajanje aplikacije v obvezno trgovino z aplikacijami ali trgovino z aplikacijami za podjetja.

Opomba: S tem nastavite le tisto, kar je privzeto izbrano pri dodajanju aplikacij. To NE spremeni obstoječih nastavitev za aplikacije, ki so že dodane v obveznih aplikacijah ali trgovini z aplikacijami za podjetja.

Spremljajte dogajanje	Samodejno posodablja aplikacijo. Upoštevajte, da lahko posodobitev aplikacije traja tudi do 7 dni po izdaji posodobitve.
Prehitevanje, kadar ni upravljano	Če je aplikacija že nameščena kot neurejena (s strani uporabnika), jo bo prevzel in upravljajal MDM.
Odstranitev aplikacije ob odstranitvi profila MDM	Aplikacijo odstrani, ko je MDM odstranjen.
Preprečevanje varnostnega kopiranja podatkov aplikacije	Preprečuje varnostno kopiranje podatkov aplikacije.

Nastavitve aplikacije Android

Tu lahko določite privzete nastavitve za dodajanje aplikacije v obvezno trgovino z aplikacijami ali trgovino z aplikacijami za podjetja.

Opomba: S tem nastavite le tisto, kar je privzeto izbrano pri dodajanju. To NE spremeni nastavitvev za aplikacije, ki so že dodane v obveznih aplikacijah ali trgovini z aplikacijami za podjetja.

Spremljajte dogajanje	Samodejno posodablja aplikacijo. Na voljo samo za aplikacije InHouse Apps.
Nadzorovana posodobitev odjemalca AppTec360 EMM	Če je omogočeno, lahko skrbniki določijo cilj posodobitve za odjemalca AppTec360 EMM. Seznam vseh razpoložljivih različic odjemalca AppTec360 EMM Client bo prikazan v razdelku "Splošne nastavitve" → "Upravljanje aplikacij" → "Notranja baza aplikacij" → "Android".

Aplikacije tretjih oseb

Android

Tukaj lahko nastavite aktivacijsko kodo za Ikarus.

Nastavite to na "Uporabi aktivacijsko kodo" in tukaj vnesite aktivacijsko kodo.

Opomba: Ko vnesete kodo in jo shranite, še ni dodana profilu, ki se pošlje v napravo. Da se koda doda profilu, morate v profilu izvesti kakršno koli spremembo. Npr. spremenite katero koli stikalo v profilu iz izklopljeno → vklopljeno → izklopljeno - Shrani → Pripisi zdaj.

iOS

Tu lahko vnesete svojo licenco SecurePIM. Po vnosu licence pritisnite "Save Changes" in lahko uporabljate možnosti SecurePIM.

VPP / KNOX Premium

Applov program za množični nakup (VPP) vam omogoča enostavno distribucijo plačljivih in brezplačnih aplikacij v naprave. To je zelo priporočljivo, saj v napravah ne potrebujete Apple ID, uporabnikom ni treba potrditi namestitve (pod nadzorom), uporabnikom ne bo treba vnesti gesla Apple ID in lahko preprosto distribuirate plačljive Aplikacije, ne da bi jih ponovno kupovali v vsaki napravi.

Če želite uporabljati program VPP, se morate registrirati v programu Apple Business Manager.

Licence VPP

Tu lahko dobite pregled nad aplikacijami VPP, koliko licenc je uporabljenih in koliko jih je na voljo.

S klikom na kolo boste videli, katerim napravam je dodeljena licenca in kakšno je stanje te dodelitve.

S klikom na osveži predpomnilnik VPP, ki primerja licence, dodeljene v MDM, z licencami, dodeljenimi na Applovi strani. To lahko v nekaterih primerih odpravi težave z licencami.

Žeton VPP

Tu lahko naložite žeton VPP, ki ga najdete v programu Apple Business Manager v Nastavitve → Aplikacije in knjige. Naložite lahko več žetonov VPP.

Žeton lahko podaljšate tako, da v programu Apple Business Manager preprosto prenesete novega, kliknete na kolesce "Uredi" in naložite novega.

Način VPP določa, kako se obravnava dodelitev licence. Glede na scenarij morate uporabiti različne načine:

"Na podlagi naprave" je treba uporabiti pri vpisovanju naprav prek kode QR, povezave, programa Apple Configurator ali DEP.

"Na podlagi uporabnika" je potrebno, če so naprave vpisane z vpisom uporabnika ali kot skupni iPad.

Če omogočite funkcijo "Avtomatsko upravljanje licenc", bodo uporabnikom, ki so premeščeni iz ene skupine v drugo, samodejno dodeljene licence Apple VPP na podlagi profila skupine, v katero so premeščeni.

Obstoječe licence Apple VPP iz skupine, iz katere so se preselili, ne bodo preklicane.

Novim uporabnikom, dodanim v skupino, bodo samodejno dodeljene licence Apple VPP na podlagi ustreznega profila skupine.

Ključ KNOX Premium

Tu lahko vnesete svoj ključ KNOX Premium Key za uporabo vsebnika Samsung KNOX.

Upoštevajte, da od sistema Android 10 to ni več podprto. Namesto tega uporabite zabojnik Android Enterprise Container.

Nastavitve trgovine App Store

Regija in jezik

Tukaj lahko nastavite privzeti jezik in regijo za iskanje aplikacij v upravljanju aplikacij.

Upoštevajte, da nastavev za iTunes določa tudi, kako sistem pridobiva informacije o določenih aplikacijah. Če na seznamih naletite na aplikacije, ki so prikazane na čuden način (npr. manjkajoča ikona), ste morda nastavili območje, kjer določena aplikacija ni na voljo.

Trgovina AE Play

Tu so na voljo vse možnosti za Trgovino Play za naprave Android za podjetja za odobritev aplikacij, nalaganje lastnih aplikacij v Trgovino Play ali ustvarjanje lastnih spletnih aplikacij.

Odobrene aplikacije

Tu lahko dobite pregled nad vsemi aplikacijami, ki ste jih odobrili.

Aplikacije v Trgovini Play

To bo naložilo okvir iFrame, ki prikazuje Trgovino Play. Poiščite zeleno aplikacijo, kliknite nanjo in jo potrdite. Med odobritvijo aplikacije lahko določite tudi, da se odobritev prekliče, če se spremenijo zahtevana dovoljenja. Priporočamo, da pri odobritvi aplikacij te nastavitve pustite privzete.

Ko je aplikacija odobrena, jo lahko dodate v svoje profile.

Gumb "Odobritev" se bo po odobritvi spremenil v gumb "Preklic odobritve", tako da lahko aplikacije vedno odstranite, če jih ne potrebujete več.

Zasebne aplikacije

Tu lahko v trgovino Google Play Store naložite svojo aplikacijo kot zasebno aplikacijo. Tako lahko aplikacijo distribuirate prek Googlovih storitev in jo prek njih posodabljate. Prednost tega je tudi ta, da lahko svoje aplikacije namestite brez potrditve uporabnika, ki je običajno potrebna.

Spletne aplikacije

Tu lahko ustvarite spletne aplikacije, ki so povezave do določenih spletnih strani, ki jih lahko dodelite kot aplikacije.

Temu lahko dodate tudi ikono po meri in podrobneje določite, kako natančno se prikaže.




Postavitev trgovine

Postavitev trgovine določa, kako so aplikacije prikazane v Trgovini Play oziroma ali so sploh prikazane.

Če želite prikazati aplikacije v Trgovini Play, ki jih mora uporabnik ročno namestiti, jih je treba dodati tukaj v postavitev. **IN**, v profilu v Trgovino Play podjetja. Če aplikacijo dodate samo v eno od teh možnosti, ne bo prikazana.

Paket aplikacij

S paketi aplikacij lahko določite skupine aplikacij, ki jih lahko z enim klikom dodelite profilom naprave ali skupine.

App Bundles +					
	Alias	Number of apps	Delete	Edit	Deploy
	Example Bundle	4			

S klikom na "+" ustvarite nov paket aplikacij. Ko ustvarite paket aplikacij, lahko kliknete na "Uredi" in v paket dodate aplikacije iz različnih virov.

Paket je mogoče dodati profilom tako kot vse druge aplikacije. Pri dodajanju aplikacij boste imeli dodaten zavihek z imenom "App Bundles", kjer boste imeli svoje pakete.

Če v paketu aplikacij naredite kakršno koli spremembo, se prikaže gumb v stolpcu "Deploy". S tem boste lahko te spremembe prenesli v vse profile, ki vsebujejo ta paket. Zato imejte v mislih, da morate to narediti ročno, ko dodate ali odstranite aplikacije v paketu.

Daljinski upravljalnik

TeamViewer

Povezovalnik TeamViewer

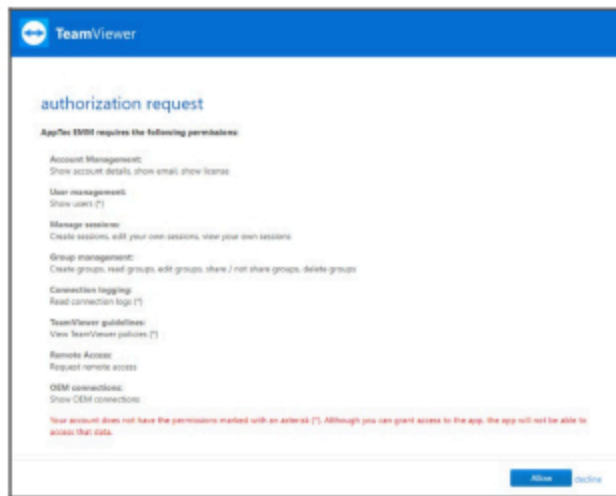
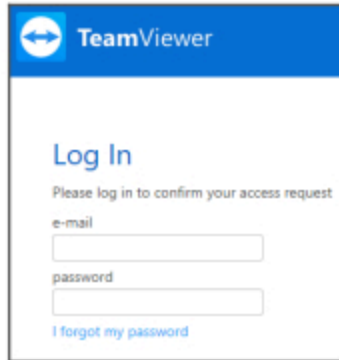
Opomba: V brezplačnem preizkusu naše različice v oblaku ne morete povezati svojega računa TeamViewer. Namesto tega se samodejno poveže brezplačni demo račun.

Pojdite v Splošne nastavitve -> Daljinski nadzor -> TeamViewer. Tu lahko povežete račun TeamViewer s konzolo ali si ogledate informacije o trenutno povezanem računu. Prav tako si lahko ogledate vse trenutno aktivne seje, če se odpravite na "Aktivne seje".

Če želite povezati račun, kliknite "Začni nastavitve".

To vas bo preusmerilo na novo stran, kjer se morate prijaviti s svojim računom TeamViewer.

Po prijavi morate AppTec360 MDM pooblastiti za uporabo tega računa. Ko to potrdite, morate počakati nekaj sekund in račun je povezan.



Namestitev programa TeamViewer QuickSupport

Dodajte aplikacijo "TeamViewer QuickSupport" med obvezne aplikacije profila naprave ali profila skupine in kliknite "Assign Now". Počakajte, da se aplikacija namesti v napravo.

Če poskušate dostopati do naprave, v kateri aplikacija ni nameščena, bo glede na konfiguracijo naprave nameščena ali pa bo od vas zahtevana njena namestitev.

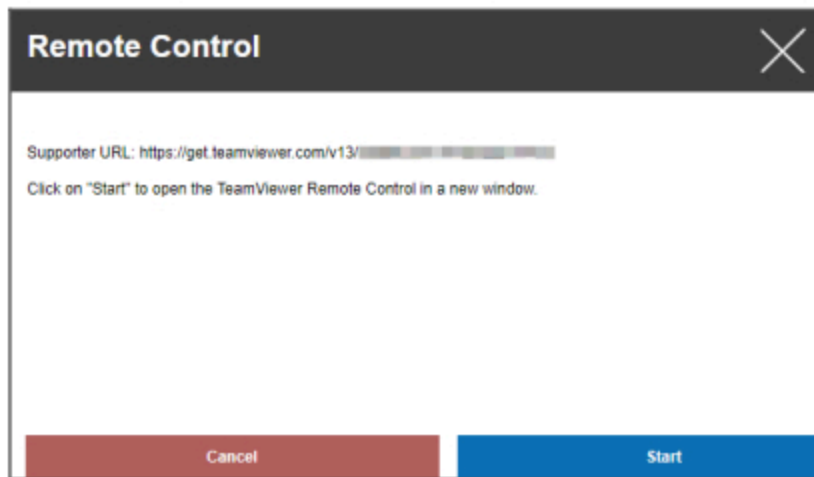
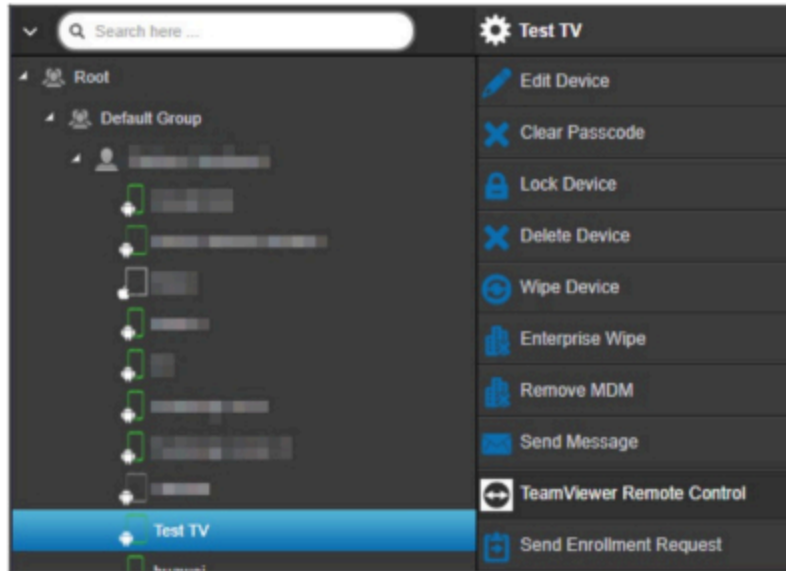
Daljinsko upravljanje naprave

Če želite napravo upravljati na daljavo, izberite napravo, kliknite na kolesce in izberite "TeamViewer Remote Control".

Če je seja že aktivna, lahko uporabite staro sejo ali ustvarite novo.

Potrdite, da želite ustvariti novo sejo TeamViewer.

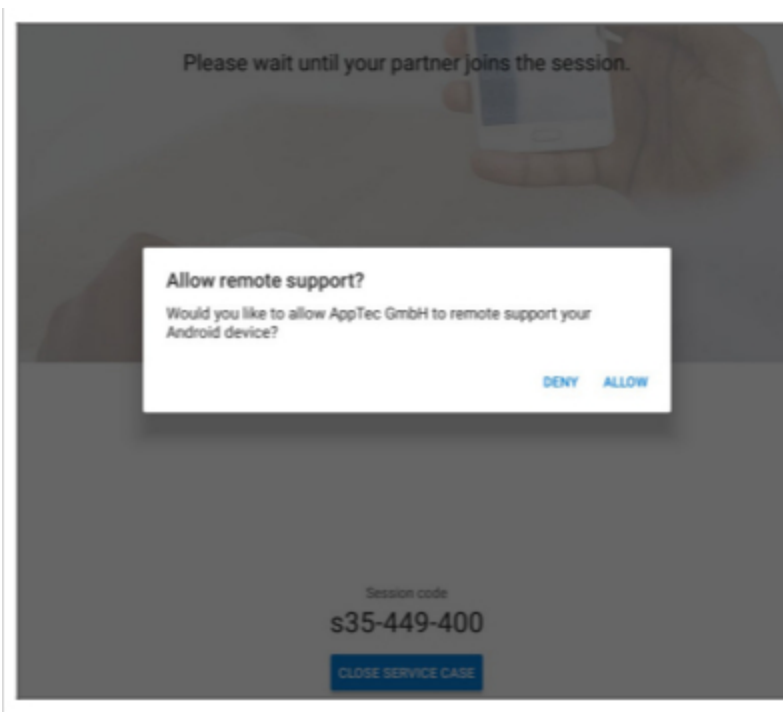
Po nekaj sekundah se bo prikazala povezava za vašo sejo TeamViewer. S klikom na "Začni" lahko to povezavo odprete v novem oknu.



Ta povezava bo odprla nameščen program TeamViewer in vas povežala z napravo.



Zdaj morate potrditi povezavo v sami napravi, da jo lahko daljinsko upravljate.

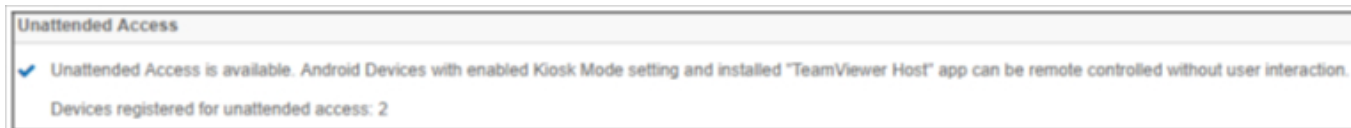


Če uporabljate iOS, boste v odjemalcu AppTec360 MDM prejeli sporočilo. S to povezavo se bo naprava pridružila oddaljeni seji. Odvisno od nastavitve obveščanja v napravi je mogoče, da obvestila ne boste prejeli in boste morali odjemalca AppTec360 MDM Client odpreti ročno.

Na nekaterih napravah s sistemom Android (npr. Samsung) je treba namestiti dodatno aplikacijo kot dodatek. Aplikacija TeamViewer v napravi vas bo o tem obvestila, če je to v vaši napravi potrebno.

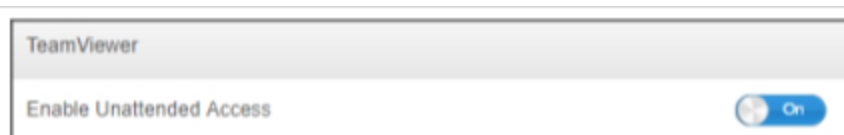
Dostop brez nadzora

Opomba: Nenadzorovan dostop je mogoč samo v napravah s sistemom Android.



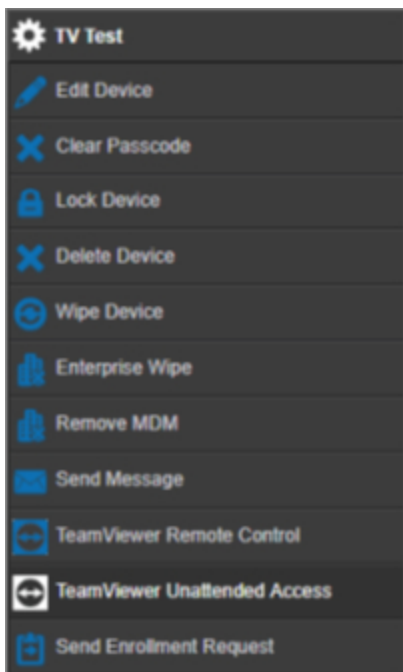
Z napravami se lahko povežete, ne da bi sprejeli povezavo v napravi, samo če vaš račun TeamViewer uporablja licenco "Tensor" ali "Corporate".

To lahko preverite po povezavi računa v razdelku "Splošne nastavitve".



Če želite uporabljati nenadzorovan dostop, morate namestiti aplikacijo "TeamViewer Host" in v svojem profilu v razdelku "Kiosk Mode & Launcher" aktivirati možnost "Enable Unattended Access".

Upoštevajte, da je to mogoče le, če uporabljate način Kiosk Mode.



Zdaj lahko izberete nenadzorovan dostop, če izberete svojo napravo in kliknete na kolesce. Tako se boste povezali z napravo, ne da bi bila potrebna potrditev na sami napravi. Upoštevajte, da lahko traja nekaj trenutkov, dokler ne dobite povezave za dostop do naprave.

Splashtop

Če omogočite možnost Splashtop, se v profilih prikažejo možnosti konfiguracije Splashtop.

Če želite uporabljati aplikacijo Splashtop, morate v svojem profilu kot obvezno aplikacijo nastaviti Streamer Splashtop (com.splashtop.streamer.csrs). Nato lahko omogočite konfiguracijo Splashtop v svojem profilu v razdelku "Daljinski nadzor". Če to omogočite, se konfigurira aplikacija Splashtop Streamer. Če uporabljate aplikacijo Splashtop Streamer, vendar ne v kombinaciji z MDM, morate to pustiti izklopljeno.

V svojem profilu v razdelku "Daljinski upravljalnik" morate nastaviti tudi kodo za namestitev. Pojdite na <https://my.splashtop.com> in se prijavite v svoj račun Splashtop. Kliknite "Dodaj računalnik" in s strani, ki se prikaže, kopirajte 12-mestno kodo za razporeditev.

Brez kode Deploy Code daljinski nadzor NI mogoč.

Ko to storite, lahko z desno tipko miške kliknete napravo in zaženete oddaljeno sejo s klikom na "Splashtop Remote Control".

Upravljanje kartice Sim

Množični uvoz CSV

Prikaže se pregled dodeljenih kartic Sim in vse informacije o njih. To vam pomaga, da imate vse informacije, ne le o svojih napravah, temveč tudi o karticah Sim v enem sistemu.

OPOMBA: To je ročno upravljanje/dokumentacija. Teh podatkov ni mogoče samodejno pridobiti iz naprav zaradi mehanizmov zasebnosti/varnosti operacijskih sistemov.

Ta seznam lahko tudi uvozite kot CSV.

Prevoznik in tarifa

Tariff Information			+	📄
Carrier	↕	Tariff	↕	
carrier		tariff		- ⚙️

Optional add-ons			+	
Carrier	↕	Option	↕	
carrier		addon		- ⚙️

Če želite dodati kartico Sim, najprej kliknite gumb za dodajanje enega ali več operaterjev.

Nato kliknite na "+" v razdelku "Tarifne informacije", če želite dodati tarifo prevozniku.

Po želji lahko spodaj dodate neobvezne dodatke, če imate nekaj takega.

Pripravljeno je vse, kar potrebujete za dodajanje dejanske kartice Sim. Kartice Sim so trenutno dodeljene uporabniku. Zato pojdite v Upravljanje mobilnih naprav, izberite Uporabnika in pojdite na "Pregled kartic Sim".

Tukaj so prikazane kartice Sim teh uporabnikov. Če obstaja, jo lahko uredite ali odstranite. Uporabniki imajo lahko več kartic Sim.

SIM Card Info +	
− ⚙	
Phone Number	+49 7641 967 13 18
Carrier	carrier
Tariff	tariff
Options	addon
Tariff Price	9,99€
Contract cancelled	No
Contract Start	2170-12-31 (extended 2170-12-31)
Contract End	2171-07-01
During Time	6
Mobile & Data	Mobile & Data
Data Volume (MB)	25000
Multi SIM	No
SIM Card Serial 1	123456789
PIN 1	***** 👁
PIN 2	***** 👁
PUK 1	***** 👁
PUK 2	***** 👁
Note	Example Note

Če želite dodati kartico SIM, kliknite na "+" in dodajte vse potrebne informacije. Te kartice Sim bodo navedene tudi na seznamu vseh vaših kartic Sim v razdelku Splošne nastavitve → Upravljanje kartic Sim.

Upravljanje naročnin

Upravljanje naročnin

Tu lahko dokumentirate tekoče naročnine, njihove podrobnosti in shranite različne datoteke, npr. podpisano pogodbo, obvestilo o prekinitvi itd. Nastavite lahko tudi opomnike, ki vas po pošti opomnijo pred iztekom naročnine in jo morda samodejno podaljšajo.

Subscription Management									
Vendor	Product	Number of licenses	Start of contract	End of contract	Duration	Billing Interval	Automatic Renewal	Renewal Period	Subscription contract
AppTec360	Unified Endpoint Management Package	100	2038-01-19	2038-01-19	24 Months	12 Months	Yes	12 Months	

First < 1 > Last Page 1/1

Če želite dodati naročnino, kliknite na "+" na vrhu. Dodate lahko poljubno število naročnin.

Če želite naložiti datoteke, ki se nanašajo na to naročnino, kliknite na "+" v različnih poljih. Tehnično lahko naložite katero koli vrsto datoteke, vendar se zavedajte, da vseh vrst datotek ni mogoče predogledati v brskalniku.

Splošni revizijski dnevnik

Revizijski dnevnik

Tu je na voljo splošni revizijski dnevnik, ki prikazuje vse opravljene spremembe. Medtem ko revizijski dnevnik v uporabniku ali skupini prikazuje le spremembe, ki se nanašajo na tega uporabnika ali skupino, ta dnevnik prikazuje VSE spremembe, opravljene kjer koli v konzoli.

Log Information					Items per page: 20
Action taken / Setting changed	Value	User	Date	Path / Type	
Edit Device profile		John Doe		Device: Device of John Doe	
Edit Device profile		John Doe		Device: Device of John Doe	
Edit Console Settings		John Doe		User: John Doe	
Console Language	English	John Doe		Console Settings	

Vidite lahko, kaj, kdo, kdaj in kje je spremenil. V nekaterih primerih lahko vnos razširite in si ogledate dodatne podrobnosti.

Kliknite na uporabnika ali na vnos v razdelku "Pot / Vrsta", da pridete na mesto, kjer je bila sprememba izvedena.

Start Time: X

End Time: X

Type of Element: v

Name of element: → X

Name of setting: → X

V zgornjem desnem kotu lahko določite tudi filter, ki vam lahko pomaga pri iskanju določenih sprememb v okolju, v katerem se dogajajo številne spremembe.

Nastavitve revizijskega dnevnika

"Obdobje hranjenja revizijskega dnevnika" določa, kako dolgo naj se revizijski dnevniki hranijo pred izbrisom.

Upravljanje certifikatov

Tu boste imeli pregled nad vsemi prenesenimi in uporabljenimi potrdili v konzoli. To je le pregled. Dejanska konfiguracija npr. certifikatov Wi-Fi se še vedno izvaja v profilu na ustreznem mestu.

Tu lahko tudi odstranite ali posodobite potrdila, kar se bo samodejno odrazilo v prizadetih profilih. Kliknite na informacijo v razdelku "Uporabljeno v profilu", da vidite, kje natančno je še vedno dodeljeno katero potrdilo.

CA Certificates										
ID	Subject	Issuer	Valid Until	Filename	Upload Date	Used in Profile				
13	APSP:c133784-343...	Apple Application...		MDM_AppTec GmbH...		CCQQ02S6GGK6 → Co...				
130		RapidSSL TLS DV R...								

Identity Certificates										
ID	Subject	Issuer	Valid Until	Password	Filename	Upload Date	Used in Profile			
26				Valid	test.p12		iPad → Security M...			
28	DEP	DEP		Valid	DEP_Credential.p12					
34	DEP	DEP		Valid	DEP_Credential.p12					
36	jd@apptec360.com	jd@apptec360.com		Valid	jd@apptec360.com.p12		CCQQ02S6GGK6 → PI...			
							CCQQ02S6GGK6 → PI...			
							CCQQ02S6GGK6 → PI...			
							CCQQ02S6GGK6 → Co...			
79	client1	Apptec CA	2026-05-08	Valid	openVPN.p12					
114	jd@apptec360.com	jd@apptec360.com	2029-12-09	Valid	smime_jd.p12		ipod → PIM Manage...			
							ipod → PIM Manage...			

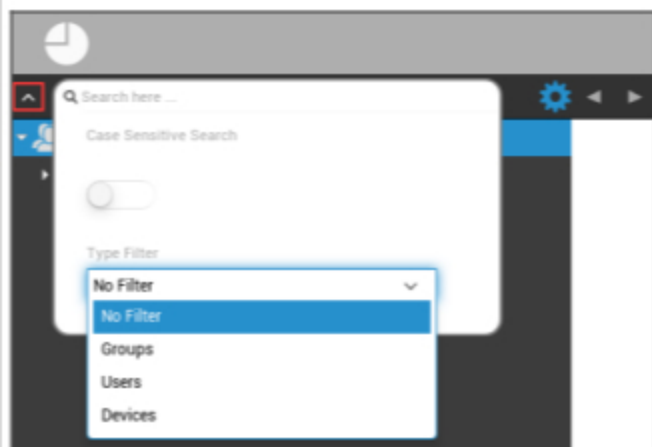
Other Certificates						
ID	Filename	Upload Date	Used in Profile			
24	caocert.pem		CCQQ02S6GGK6 → BYOD → SecurePIM Container → Security			

Gateway Certificates						
ID	Type	Filename	Date	Used in Setting		
163	Gateway Certificate					
165	Gateway Certificate					
166	Gateway Certificate			Universal Gateway → Gateway Settings		

Upravljanje mobilnih naprav

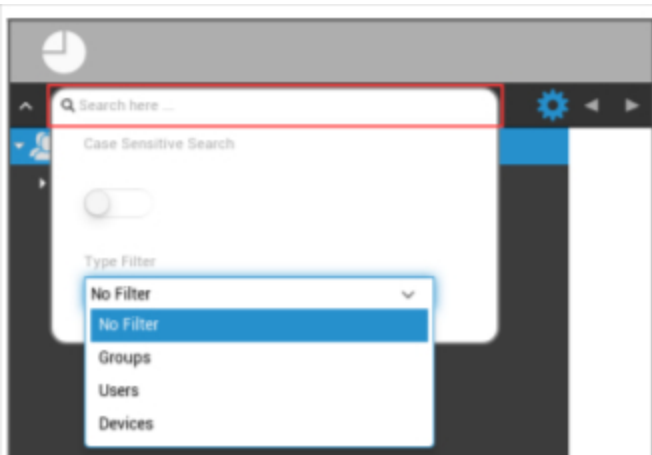
Zaslon za upravljanje mobilnih naprav

Filter naprave



S klikom v zgornjem levem kotu zaslona lahko najdete različne filtre za prikaz naprav.

Iskalno okno



Okno za iskanje omogoča iskanje vseh naprav in/ali uporabnikov z določeno ključno besedo.

Opcije orodja



Po kliku na ustrezen simbol se prikaže seznam možnosti, ki so vam na voljo.

Ti se spreminjajo z vsakim trenutnim oknom in so pojasnjeni v ustreznih poglavjih.

Navigation arrows



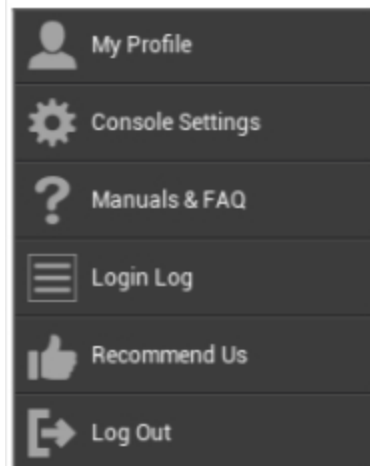
S klikom na puščico v levo boste preusmerjeni na prejšnjo stran.

Nato boste s klikom na desno puščico preusmerjeni na stran, ki ste jo pravkar zapustili.

Nastavitve računa v administraciji



S klikom na e-poštni naslov, kot je prikazano zgoraj, se prikaže naslednji meni:



Moj profil	Urejanje podrobnosti o računu upravitelja
Nastavitve konzole	Konfiguracija nastavitvev konzole za račun Admins
Priročniki in pogosta vprašanja	Oglejte si stran "Priročniki in pogosta vprašanja" v razdelku "Splošne nastavitve".
Prijavni dnevnik	Dostopite do "Prijavnega dnevnika"
Priporočite nas	Oglejte si stran "Priporočite nas" v razdelku "Splošne nastavitve".
Odjava	Odjava iz konzole MDM

Informacije o uporabniku

Tu lahko urejate podatke o računu trenutno prijavljenega upravitelja.

Uporabniško ime	Uporabniško ime in/ali e-poštni naslov računa
Ime	Ime in priimek upraviteljev
Priimek	Priimek upraviteljev
Prijavno ime	Prijavno ime administratorjev
E-poštni naslov	E-poštni naslov upraviteljev
Alternativni e-naslov	Nadomestni e-poštni naslov skrbnikov
Slika	Profilna slika
Telefonska številka	Telefonska številka upraviteljev
Mobilna številka	Mobilna številka upraviteljev
Podaljšek telefona	Podaljšek telefona
Lokacija	Lokacija
Položaj	Položaj v podjetju
Uporabniška skupina	Izberite, kateri skupini uporabnikov želite dodeliti račun upravitelja.
Komentar:	Vnesite komentar
Vnesite novo geslo	Vnesite geslo za spremembo gesla
Ponovite novo geslo	Ponovite novo geslo za potrditev

Upoštevajte, da je lahko dostop za upravljanje v hierarhični strukturi podan tudi kot lokalni uporabniški račun. Brez vzpostavitve dodatnega skrbnika tega ne smete izbrisati!

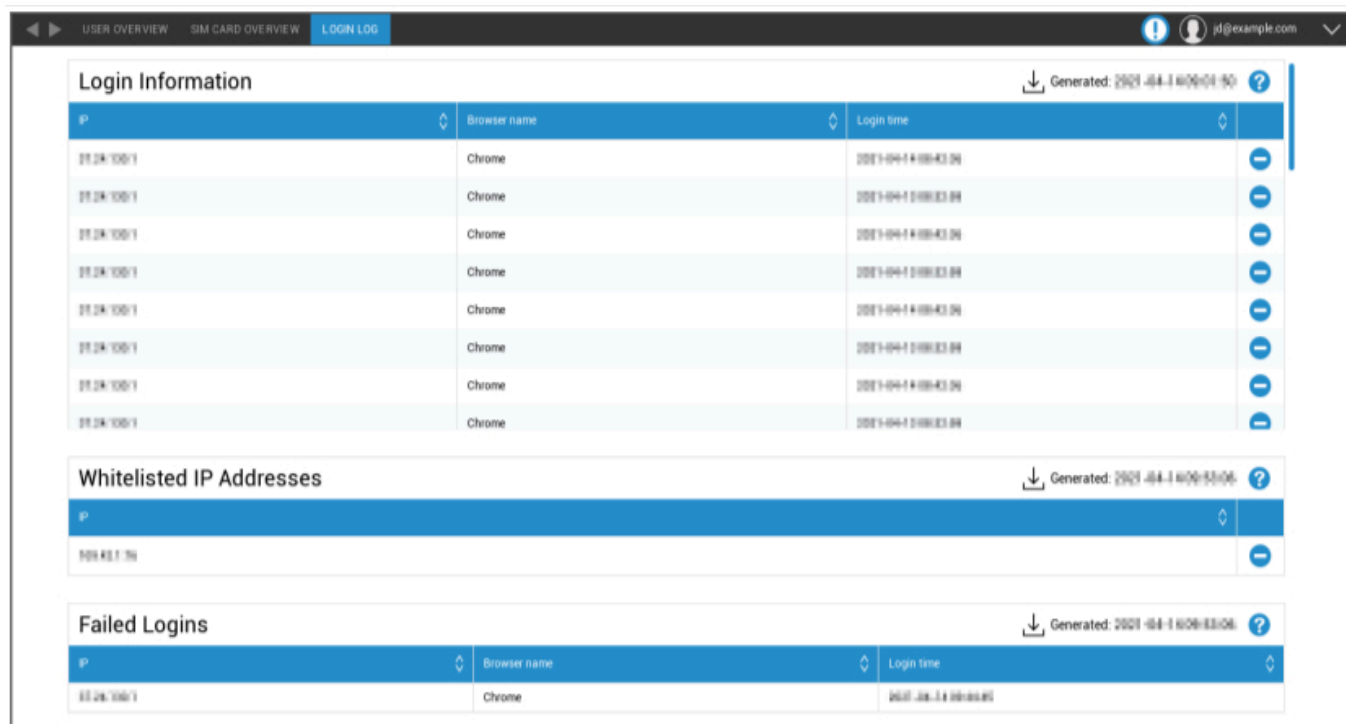
Nastavitve konzole

Tu lahko za račun Admins konfigurirate naslednje nastavitve konzole:

Možnosti prikaza uporabnika imenika	Določite, kako naj bodo uporabniki označeni v drevesu.
Možnosti prikaza imeniške naprave	Določite, kako naj bodo naprave označene v drevesu.
Časovna omejitev seje	Če uporabnik v določenem času ne stori ničesar, bo odjavljen. Privzeta vrednost je 60 minut. Ko spremenite to nastavitvev, se odjavite in ponovno prijavite.
Časovni pas	Izberite časovni pas, ki se uporablja
Časovni format	Izberite, kako naj se prikažejo časovni žigi
Jezik konzole	Izberite jezik, v katerem bo prikazana konzola. Na voljo sta angleščina in nemščina.
Glavna barva	Nastavite lahko barvo, ki bo uporabljena kot osnova za barvno shemo konzole. Uporabite lahko izbirnik barv ali vnesete barvo v zapisu HTML HEX. Oblikovalniki RGB, kot sta "roza" in "rumena", prav tako delujejo.
Ukaz za shranjevanje	Kombinacija tipk za sprožitev shranjevanja brez pritiska gumba "Shrani".
Uporabite dvofaktorsko preverjanje pristnosti	Omogočite uporabo dvostopenjskega preverjanja pristnosti pri prijavi. Ob prijavi boste prejeli e-poštno sporočilo s kodo, ki jo boste morali vnesti za prijavo.
Časovna omejitev dvofaktorske avtentikacije	Nastavite časovno obdobje, v katerem vas po že uspešni avtentikaciji ne bo treba pozvati k dvostopenjski avtentikaciji.
Pošlji kodo za preverjanje prek	Koda za preverjanje bo poslana na izbrane možnosti. Sporočilo o napravi bo prikazano v aplikaciji AppTec360 MDM App na vseh napravah Android in iOS, ki so v vaši lasti.
Pošlji prijavno sporočilo po prijavi	Če je to omogočeno, bo za vsako prijavo z naslova ip, ki ni uvrščen na beli seznam, poslano e-poštno sporočilo. E-poštno sporočilo vsebuje informacije o prijavi (npr. IP, brskalnik).

Prijavni dnevnik

Tu si lahko ogledate informacije o prijavih trenutno prijavljenega skrbniškega računa.



<p>Podatki za prijavo</p>	<p>Seznam, ki vsebuje prijave trenutno prijavljenega skrbniškega računa, ki jih je zabeležila konzola. Ta seznam prikazuje vse vaše uspešne prijave v zadnjih 30 dneh.</p>
<p>Naslovi IP na beli listi</p>	<p>To je seznam vseh vaših naslovov IP, ki so uvrščeni na beli seznam. Če se prijavite z IP-ja, ki je naveden na tem seznamu, se sporočilo o prijavi ne bo prikazalo. Na ta seznam lahko dodate naslov IP tako, da kliknete na gumb poleg vnosa na zgornjem seznamu "Prijavni podatki". Naslov IP lahko s tega seznama odstranite tako, da kliknete na gumb poleg vnosa na tem seznamu ali na zgornjem seznamu "Prijavni podatki".</p>
<p>Neuspešne prijave</p>	<p>To je seznam vseh neuspešnih poskusov prijave v zadnjih 30 dneh. Če v 20 minutah vsaj trikrat niste vnesli pravilnega gesla, se na tem seznamu prikaže vnos. O neuspešnih poskusih prijave boste obveščeni tudi po e-pošti.</p>

Korporativna uprava (korensko vozlišče) v mobilnem upravljanju



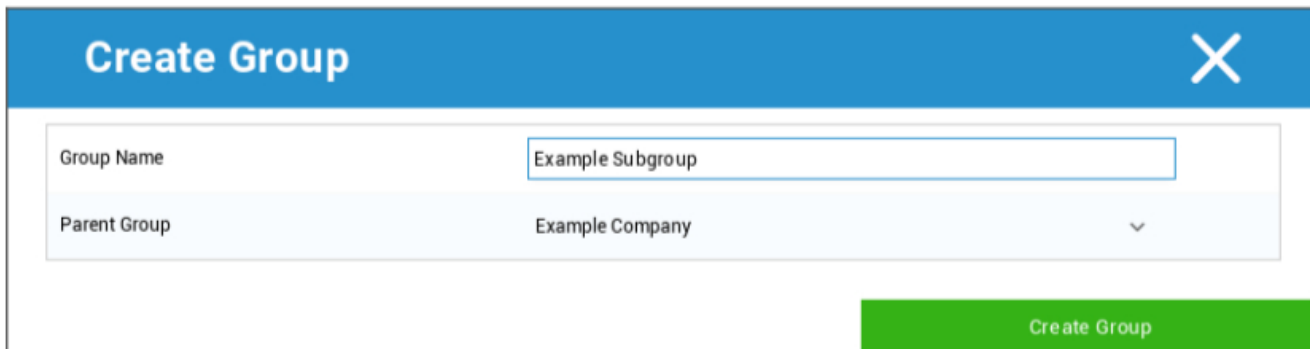
Ko pridete do korenkega vozlišča (prva skupina), lahko za svoje podjetje izvedete različne nastavitve v zvezi z upravljanjem mobilnih naprav.

Ustvarjanje podskupine	Ustvari podskupino
Preimenovanje korenkega vozlišča	Preimenovanje korenkega vozlišča (npr. ime vašega podjetja)
Množični vpis	Vpis več naprav/uporabnikov hkrati
Dodelitev mase	Dodelitev profila za posamezne skupine z enim samim pogledom
Hitro upravljanje aplikacij	Pošiljanje zahtevkov za (ne)namestitev aplikacije ustreznim skupinam naprav
Uvoz uporabnika CSV	Uvoz uporabnikov iz CSV v ustrezno skupino

Ustvarjanje podskupine

S funkcijo "Ustvari podskupino" lahko ustvarite dodatno podskupino.

Določite lahko, v katero skupino naj bo podskupina dodeljena.



(Privzeto je ustvarjena nova skupina, ki je dodeljena kot podskupina v korenem vozlišču)

Preimenovanje korenkega vozlišča

Default Title
✕

Root Node Name	AppTec360
----------------	-----------

Update Name

Tu lahko preimenujete svoje korenko ime. Običajno se v tem primeru uporablja ime podjetja.

Množični vpis

Z množičnim vpisom lahko vpišete več naprav in uporabnikov.

Mass Enrollment
✕

Enroll?	Name	eMail	Alternative eMail	Phone Number	eMail	alt. eMail	SMS	OS	Type	Emp.	Corp.
<input type="checkbox"/>	Default Group				<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	iOS	Phone	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	John Doe	jd@example.com			<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Android Enterprise	AE Work Managed Device	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Example Subgroup				<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	iOS	Phone	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Test User	test@example.co			<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	iOS	Phone	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Start Mass Enrollment
Export as CSV
Import CSV

On average it takes 10 seconds for creating and enrolling one device
 You can easily create users and devices by adding them at the end of a exported CSV. Import the CSV afterwards and start the Mass Enrollment.
 The following line will add a new user:
 Philipp Reiss; philipp.reis@apptec360.com; pr@apptec360.com; +41 61 511 3210;
 The following line will add a new device:
 New Device; mail-for-enrollment@apptec360.com;+41 61 511 3210;1;0;0;0;0;-1
 Your account is limited to 25 devices. You can add 21 devices.

Neposredno lahko izberete, na kakšen način naj uporabnik prejme prijavo (e-pošta; alternativna e-pošta; SMS).

Glede na to, katero napravo bo uporabnik prejel (iOS, Android, Windows Phone), lahko to neposredno označite tukaj.

Tukaj lahko nastavite tudi razlikovanje med pametnim telefonom in tabličnim računalnikom, ki ga morate pravilno izbrati s kljukico.

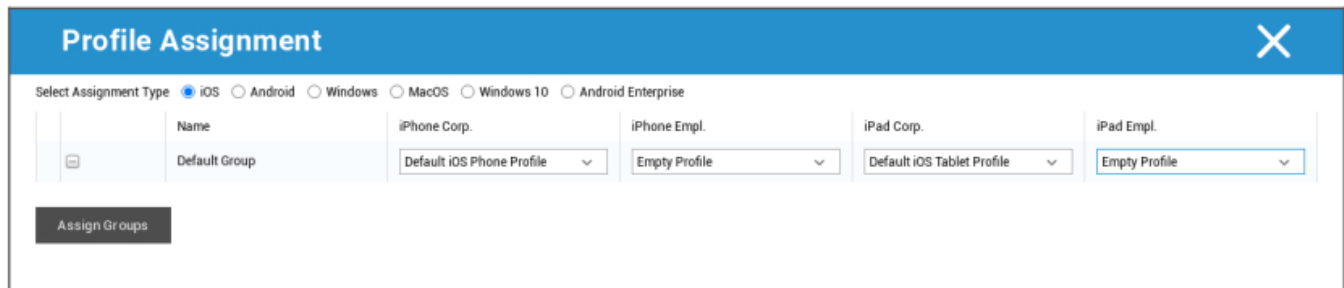
V zadnjem koraku lahko ugotovite, ali je zadevna naprava službena ali zasebna (BYOD).

S funkcijo "Izvozi kot CSV" lahko informacije izvozite kot podatkovno datoteko CSV. Datoteko s podatki CSV lahko uvozite tudi z "Uvozi CSV", datoteka pa mora biti videti kot v spodnjem primeru:

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

Dodelitev mase

V razdelku Množična dodelitev lahko profil dodelite vsem skupinam, ki so razdeljene na iOS - Android - Windows - MacOS - Windows 10 - Android Enterprise.



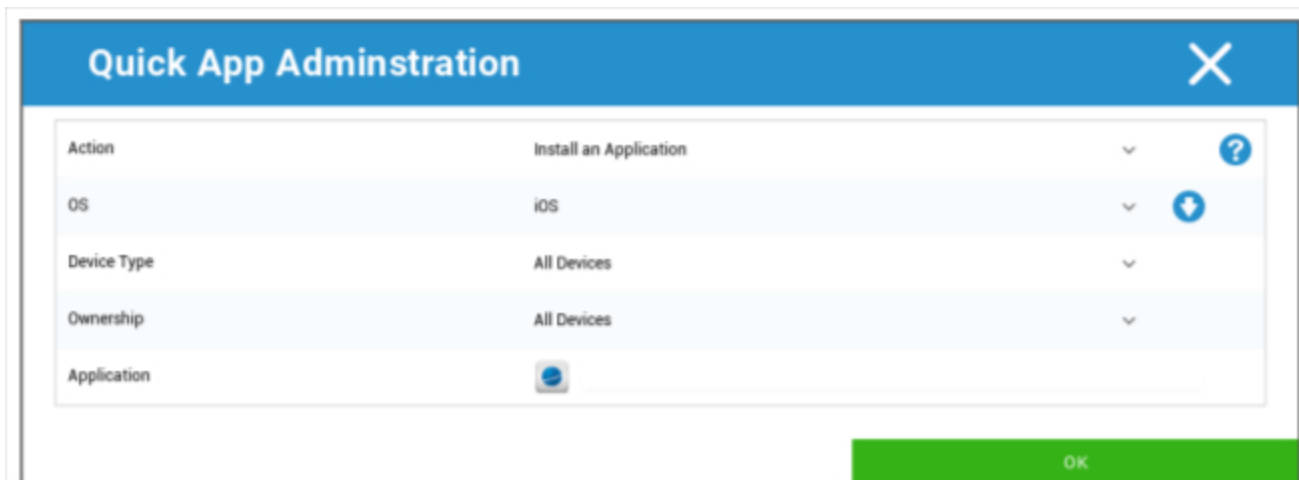
The screenshot shows a dialog box titled "Profile Assignment" with a close button (X) in the top right corner. Below the title bar, there is a "Select Assignment Type" section with radio buttons for iOS (selected), Android, Windows, MacOS, Windows 10, and Android Enterprise. Below this, there are four columns for different device types: iPhone Corp., iPhone Empl., iPad Corp., and iPad Empl. Each column has a "Name" field and a "Default Group" dropdown menu. The "Name" fields contain "iPhone Corp.", "iPhone Empl.", "iPad Corp.", and "iPad Empl." respectively. The "Default Group" dropdowns are set to "Default iOS Phone Profile", "Empty Profile", "Default iOS Tablet Profile", and "Empty Profile". At the bottom left, there is a dark button labeled "Assign Groups".

Windows - MacOS - Windows 10 - Android Enterprise


Hitro upravljanje aplikacij

V razdelku Hitro upravljanje aplikacij lahko operacijskemu sistemu po lastni izbiri pošljete zahteve za namestitev ali odstranitev določene aplikacije.

Določite lahko tudi, ali naj se zahteva pošlje vsem vrstam naprav izbranega operacijskega sistema ali samo določeni vrsti naprave.



The screenshot shows a dialog box titled "Quick App Administration" with a close button (X) in the top right corner. Below the title bar, there is a table with the following rows:

Action	Install an Application	▼	?
OS	iOS	▼	↓
Device Type	All Device Type	▼	
Ownership	All Devices	▼	
Application			

At the bottom right, there is a green button labeled "OK".

Uvoz uporabnika CSV

Uvozite uporabnike iz CSV v ustrezno skupino.

S funkcijo "Prenesi predlogo CSV" lahko izvozite datoteko s predlogo CSV, ki jo lahko izpolnite (ali pa jo uporabite kot referenco).

Možnosti "Prikaži identitete vlog" in "Prikaži identitete skupin" lahko uporabite tudi kot referenco za ustvarjanje lastne datoteke CSV.

Datoteko CSV lahko naložite v MDM s funkcijo "Naloži CSV".

V zadnjem koraku lahko začnete uvoz s klikom na "Start Import".

CSV Import ✕

Name	Surname	Login Name	eMail Address	Alternative eMail	Phone Number	Mobile Number	Phone Extension	Location	Position	Usergroup	Roles	Comment	Password
Philipp	Reis	p.reis	p.reis@apptec360.com	preis@phone.com	+41 1234 56789	+41 7777 12345	1834	Basel (Switzerland)	Developer	Default Group	Self Service	Good Developer	1604400129

If you leave the field "Usergroup" empty users will be assigned to the group "Default Group", but you can also enter a specific group id.
The following fields are mandatory: Name, Surname, eMail Address
An eMail address of a new user mustn't be used by another user.
Libre Office Calc is the recommended Software for editing the CSV Template

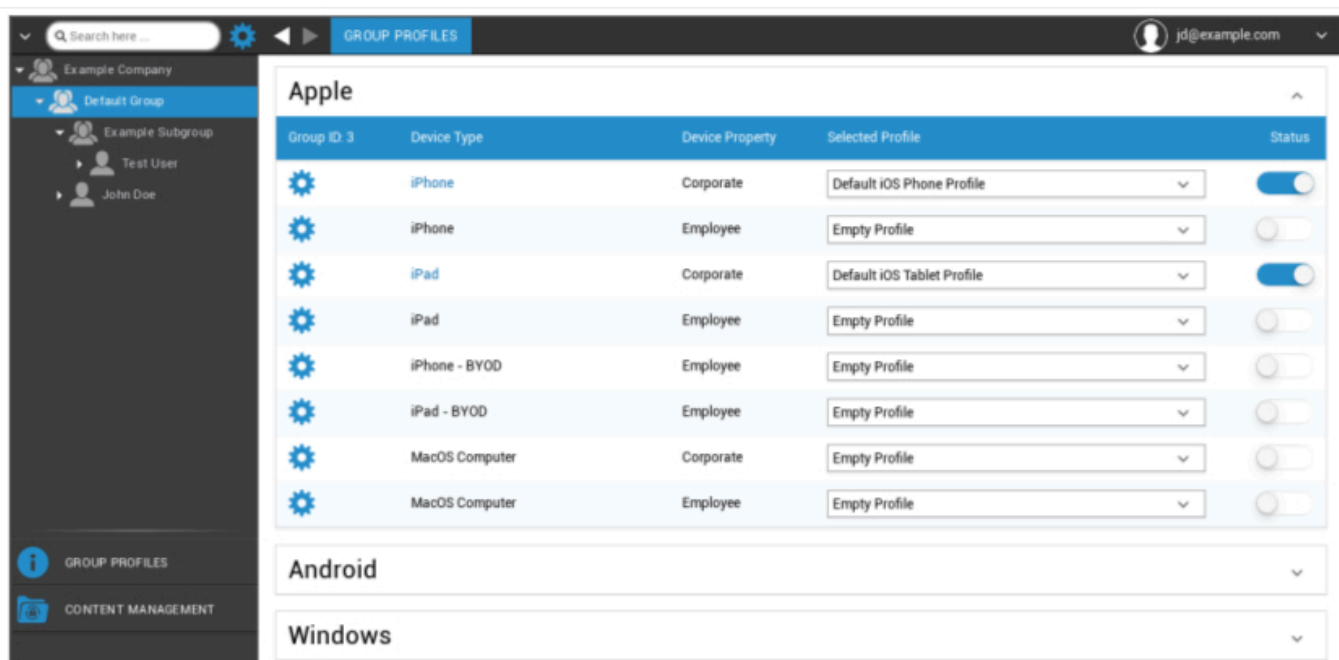
Upravljanje skupin v mobilnem upravljanju

Z enim klikom na pregled se prikažejo različni konfiguracijski profili za posamezne platforme.

En profil vsebuje vse možnosti nastavitvev, ki jih je mogoče z AppTec360 vnaprej določiti v napravi končnega uporabnika. Na vsaki platformi lahko ustvarite profile za naprave podjetja (Corporate) ali naprave, ki jih lahko prinesete sami (Bring-Your-Own-Device) (Employee).

Za razlikovanje konfiguracij za skupine naprav, na primer glede na lokacijo ali funkcijo, je priporočljivo ustvariti več podskupin.

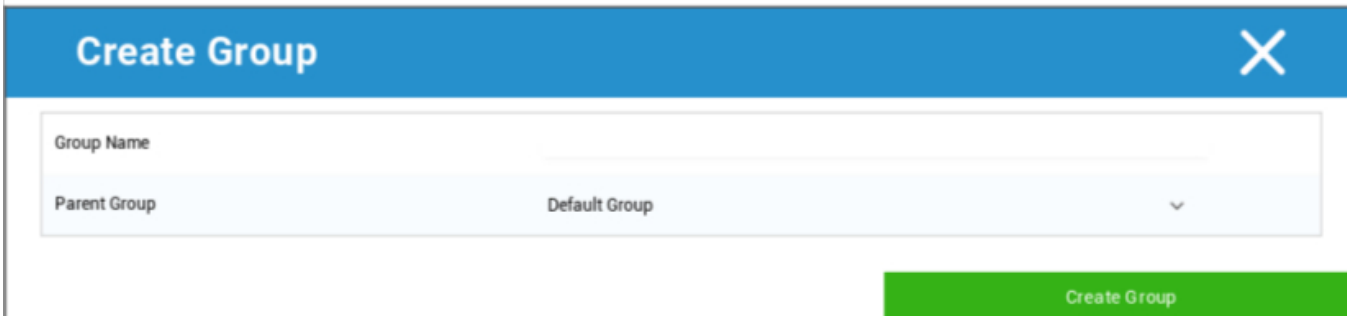
Upoštevajte Upravljanje profilov v Upravljanju mobilnih naprav



V meniju opreme lahko nastavite različne nastavitve za posamezno (pod)skupino.

Ustvarjanje podskupine	Ustvarite podskupino za ustrezno (pod)skupino
Urejanje izbrane skupine	Urejanje izbrane skupine
Brisanje izbrane skupine	Brisanje izbrane skupine
Množični vpis	Za izbrani profil lahko hkrati vpišete več naprav/uporabnikov.
Dodelitev mase	dodelitev profilov skupini, ki je trenutno izbrana.
Ustvarjanje podskupine	Ustvarite podskupino za ustrezno (pod)skupino
Ustvarjanje uporabnika	Ustvarite uporabnika za ustrezno (pod)skupino

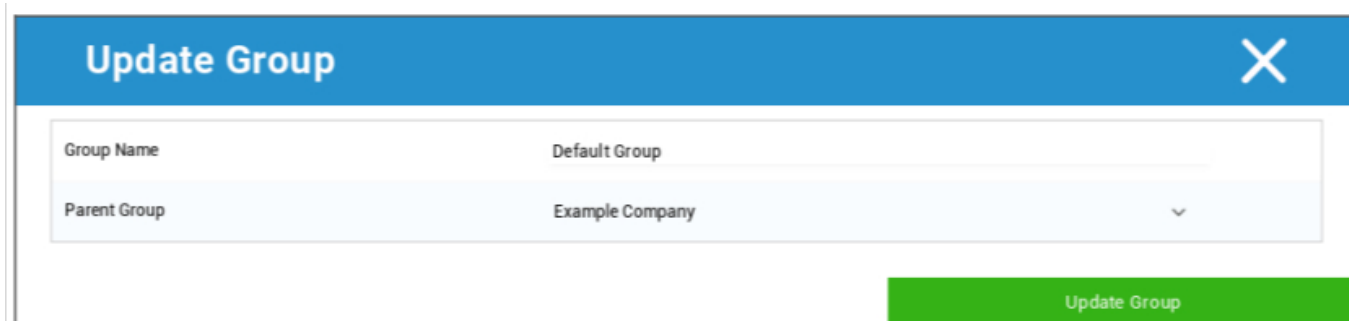
Ustvarjanje podskupine



S funkcijo "Ustvari podskupino" lahko ustvarite dodatno podskupino.

Določite lahko, v katero skupino bo podskupina dodeljena (privzeto je podskupina dodeljena skupini, ki je trenutno izbrana).

Urejanje izbrane skupine



Tu lahko uredite profil - tu so na voljo naslednje nastavitve:

- Ime skupine lahko spremenite
- Skupino staršev lahko spremenite

Brisanje izbrane skupine

V razdelku "izbriši izbrano skupino" so navedeni vsi uporabniki in naprave, ki so v zadevni skupini. Tu jih lahko izbrišete.

Za enega uporabnika lahko izvedete naslednje ukaze za brisanje:

Izbriši uporabnika	Uporabnik je izbrisan
Premakni uporabnika v skupino:	Uporabnika lahko premaknete v drugo skupino (naslednji stolpec, npr. "Administratorji").

Za eno napravo lahko izvedete naslednje ukaze za brisanje:

Brisanje in brisanje	Brisanje in brisanje naprave
Izbriši iz sistema	Odstranitev naprave samo iz aplikacije AppTec

[Referenca: Množični vpis](#)

[Referenca: Pripisovanje mase](#)

Ustvarjanje uporabnika

S funkcijo "Ustvari uporabnika" lahko dodate novega uporabnika.

Ustvari novega uporabnika upravitelja

Uporabnika lahko nastavite kot uporabnika Admin-User. S tem mu boste dali dovoljenja za prijavo v konzolo in spreminjanje uporabnikov/skupin/naprav.

Ustvarite običajnega uporabnika ali uporabite obstoječega uporabnika. Izberite uporabnika, ki mu želite podeliti skrbniška dovoljenja, kliknite na kolesce in izberite "Uredi uporabnika":



Aktivirajte stikalo za "Can Login" (Lahko se prijavi), dodelite uporabniku vlogo "Super-Root" in nastavite geslo.

User Information
✕

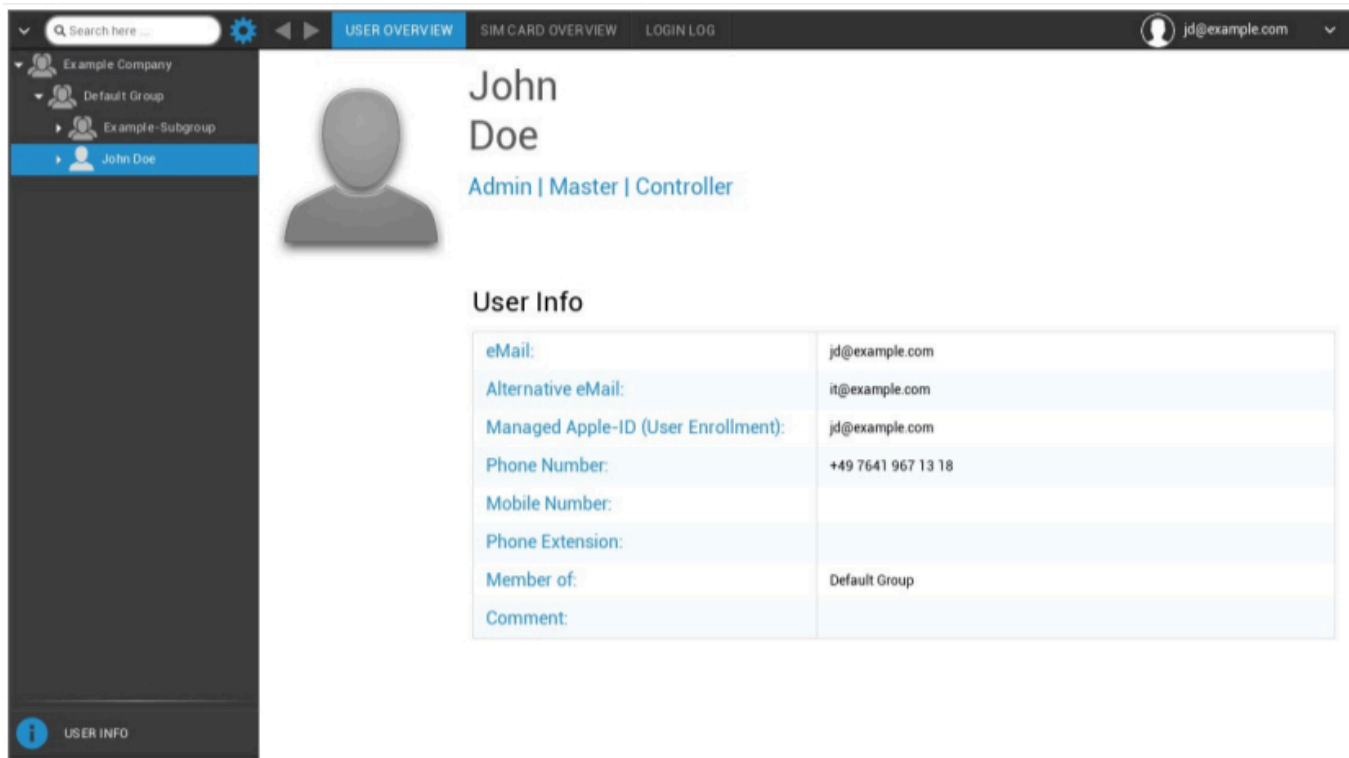
Username	jd@example.com	
First Name	John	
Last Name	Doe	
Login Name		?
eMail Address	jd@example.com	?
Alternative eMail Address		
Map Apple-ID automatically	<input checked="" type="checkbox"/>	?
Picture	Click here to select a file	?
Phone Number		
Mobile Number		
Phone Extension		
Location		
Position		
Can Login	<input checked="" type="checkbox"/>	?
Usergroup	Default Group	▼
Assigned Roles	Super Root ✕	
Comment		↵
New Password	*****	?
Confirm new password	*****	?

Save

To shranite in uporabnik se lahko zdaj prijavi z uporabniškim imenom in geslom.

Upravljanje uporabnikov v mobilnem upravljanju

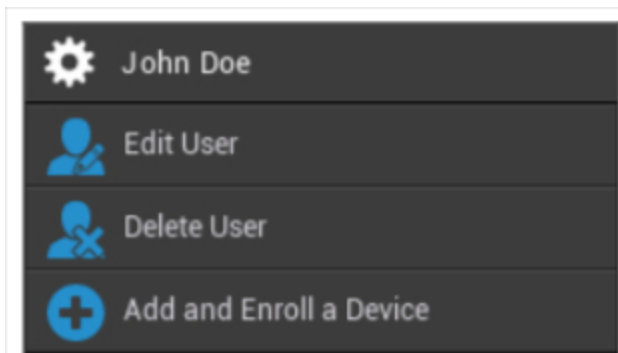
Ko izberete določenega uporabnika, se prikaže naslednji pregled:



User Info	
eMail:	jd@example.com
Alternative eMail:	it@example.com
Managed Apple-ID (User Enrollment):	jd@example.com
Phone Number:	+49 7641 967 13 18
Mobile Number:	
Phone Extension:	
Member of:	Default Group
Comment:	

Prikazan bo pregled vseh podatkov, ki ste jih vnesli v razdelku "Ustvari uporabnika".

Z zobnikom, ki je nameščen na vrhu, lahko izvedete naslednje konfiguracije:



Uporabniško ime	Uporabniško ime izbranega uporabnika
Uredi uporabnika	Urejanje informacij o uporabniku
Izbriši uporabnika	Izbriši uporabnika <ul style="list-style-type: none"> Izbriši iz sistema = naprava bo odstranjena iz sistema AppTec

	<ul style="list-style-type: none">• Brisanje in brisanje = naprava bo obnovljena na tovarniške nastavitve in odstranjena iz aplikacije AppTec.
Dodajanje in vpis naprave	Vpis naprave za izbranega uporabnika

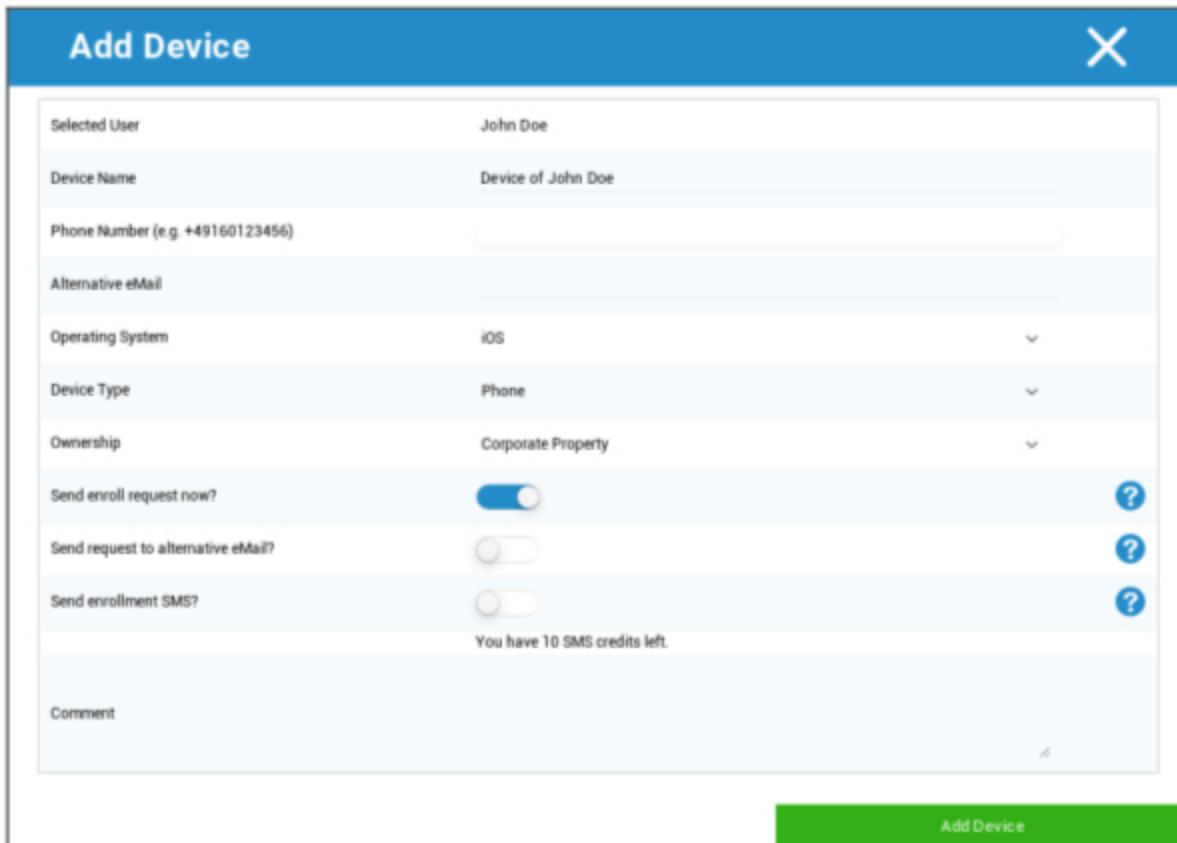
Upoštevajte, da je lahko dostop za upravljanje v hierarhični strukturi podan tudi kot lokalni uporabniški račun. Brez vzpostavitve dodatnega skrbnika tega ne smete izbrisati!

Dodajanje in vpisovanje naprave

Tu lahko izberete napravo za izbrano uporabo.

Naprave lahko v skupino vpišete tudi neposredno. To storite tako, da kliknete na skupino, kliknete na kolesce in izberete "Dodaj in vpiši napravo".

Prikaže se naslednji pregled:



The screenshot shows a web form titled "Add Device" with a blue header and a close button (X) in the top right corner. The form contains the following fields and options:

Selected User	John Doe
Device Name	Device of John Doe
Phone Number (e.g. +49160123456)	<input type="text"/>
Alternative eMail	<input type="text"/>
Operating System	iOS <input type="button" value="v"/>
Device Type	Phone <input type="button" value="v"/>
Ownership	Corporate Property <input type="button" value="v"/>
Send enroll request now?	<input checked="" type="checkbox"/> <input data-bbox="1323 1003 1356 1045" type="button" value="?"/>
Send request to alternative eMail?	<input type="checkbox"/> <input data-bbox="1323 1056 1356 1098" type="button" value="?"/>
Send enrollment SMS?	<input type="checkbox"/> <input data-bbox="1323 1108 1356 1150" type="button" value="?"/>
You have 10 SMS credits left.	
Comment	<input type="text"/>

At the bottom right of the form is a green button labeled "Add Device".

Glede na vrsto naprave, ki jo želite vpisati, morate izvesti naslednje konfiguracije:

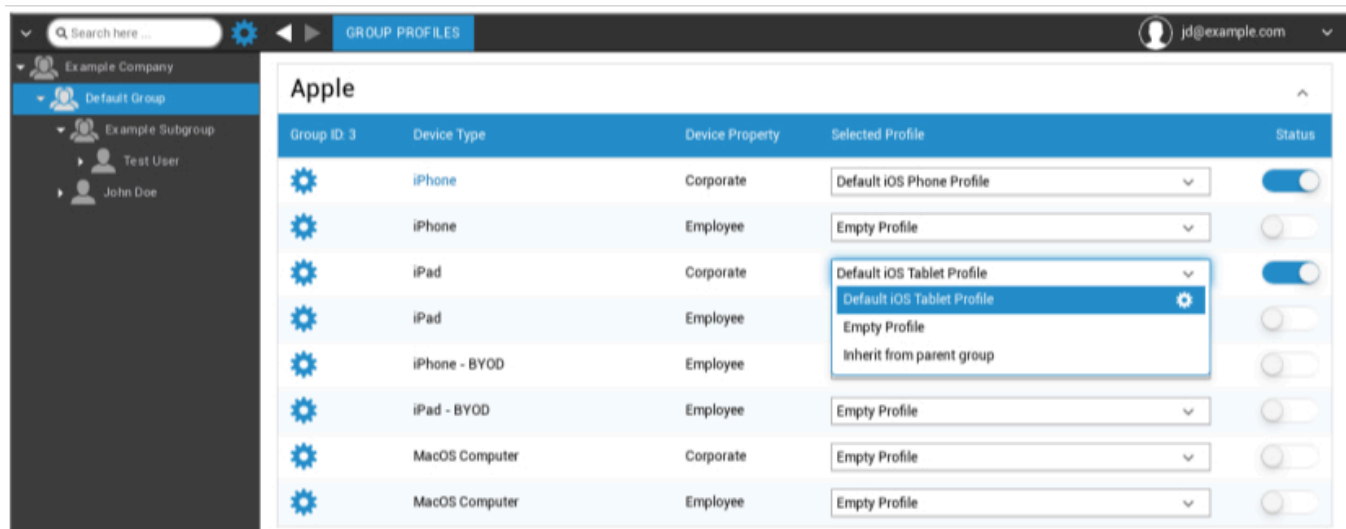
Izbrani uporabnik	Izbrani uporabnik (samodejno se izpolni)
Ime naprave	Vnese se samodejno (naprava za "ime uporabnika") - lahko pa ga spremenite.
Telefonska številka	Telefonska številka se izpolni samodejno (če jo je uporabnik navedel) - tukaj jo lahko dodate ali spremenite.
Alternativna elektronska pošta	nadomestni e-poštni naslov, ki se izpolni samodejno (če ga je uporabnik navedel) - tukaj pa ga lahko dodate ali spremenite.
Lastnik naprave	Lastnina podjetja = naprava podjetja Lastnina zaposlenega = naprava BYOD
Izberite operacijski sistem	Tu lahko izbirate med naslednjimi operacijskimi sistemi: <ul style="list-style-type: none"> • iOS • iOS BYOD (prijava uporabnikov) • MacOS • Android Enterprise • Android • Windows Mobile • Windows 10
Pošljite zahtevo za vpis?	e-poštno sporočilo se takoj pošlje na glavni e-poštni naslov, uporabnik pa je pozvan, da poveže svojo napravo.
Pošljite zahtevek na alternativni e-naslov?	Pošljite e-poštno sporočilo dodatno ali izključno (v primeru, da je bila možnost "Pošlji zahtevo za vpis?" deaktivirana) na nadomestni e-poštni naslov (e-poštno sporočilo se razlikuje od "običajnega" e-poštnega sporočila z zahtevo za vpis).
Pošljite SMS za vpis?	Pošljite zahtevo za vpis prek sporočila SMS (vnesti je treba "telefonsko številko").

Po pošiljanju zahtevka za vpis se naprava takoj prikaže (označena z rdečo barvo).

Ko je naprava uspešno povezana, bo kmalu zatem označena z zeleno barvo in tako pripravljena za sprejemanje omejitev, aplikacij itd.

Upravljanje profilov v mobilnem upravljanju

Po kliku na skupino se prikaže pregled vseh platform naprav, ki jih je treba konfigurirati, in dodeljenih profilov.



	Izvedite konfiguracijo za izbrani profil
Vrsta naprave	Vrsta naprave in/ali model
Lastnost naprave	lastnik naprave (podjetje = lastnina podjetja, zaposleni = zasebna naprava zaposlenega)
Izbrani profil	Izbrani profil (zobnik odpre pogovorno okno za konfiguracijo profila)
Status	Vklop/izklop (profil je aktiviran/deaktiviran)

Ko izberete prestavo, so na voljo naslednje možnosti:

Ustvarite profil

Za vsak vnos in/ali platformo lahko ustvarite in konfigurirate nov profil. Po kliku na to podtočko bo profil ustvarjen takoj in takoj lahko začnete s konfiguracijo za iOS, Android in Windows Phone.

Urejanje profila

Po kliku na "Uredi profil" se prikaže prikaz konfiguracije za zadevni profil, kjer lahko nastavite konfiguracije.

Kopiranje profila

S funkcijo "Kopiraj profil" lahko kopirate nastavitve/konfiguracije iz že obstoječega profila in jih dodate v nov profil.

Copy Group Profile
✕

Source Profile Name	Default iOS Phone Profile
New Profile Name	Copy of Default iOS Phone Profile
Profile Type	iPhone ▼

Copy

Ime profila vira	Ime profila, ki se kopira
Novo ime profila	Ime novega profila
Vrsta profila	Vrsta profila (telefon/tablica)

Ko kliknete na "Kopiraj", bo profil ustvarjen in ga lahko dodelite skupini.

Brisanje profila

Tu lahko profil trajno izbrišete. Upoštevajte, da med postopkom brisanja in naslednjim postopkom "Assign Now" za profil konfiguracija izgine na ustreznih napravah prizadete skupine in je ni mogoče obnoviti!

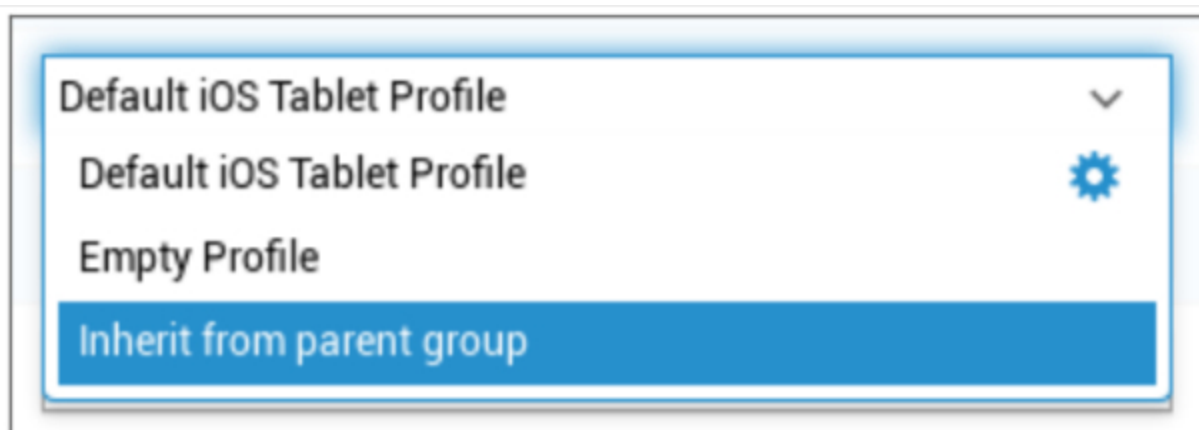
Delete Group Profile ✕

Profile to Delete: Default iOS Tablet Profile

Cancel Delete

Dedovanje profilov

Med izbiro profilov je na voljo možnost "Podeduj od nadrejene skupine".



Ko je profil aktiviran, se za izbrano napravo (in ustrezno vrsto naprave) uporabi profil nadrejene skupine. Upoštevajte tudi, da lahko spremembe tega profila vplivajo na številne skupine.

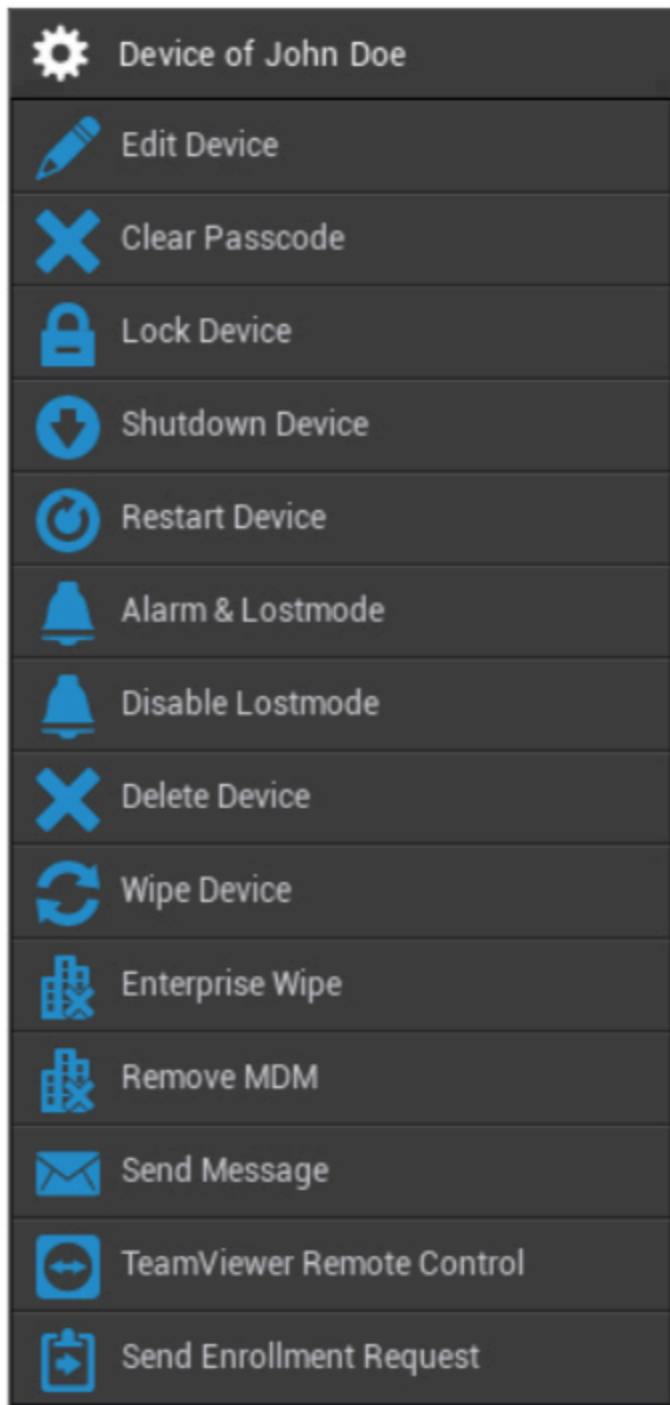
Ta konfiguracija je ob ustvarjanju nove podskupine nastavljena kot privzeta vrednost.

Na voljo je tudi konfiguracija "Empty Profile", ki ustreza praznemu profilu, kar pomeni, da se na koncu v napravi končnega uporabnika ne bodo izvedle nobene nove konfiguracije.

Upravljanje naprav v mobilnem upravljanju

Ko izberete napravo, lahko s pomočjo "orodja" opravite različna opravila. Te se razlikujejo glede na platformo operacijskega sistema (iOS, Android Enterprise, Android, Windows Mobile, Windows 10).

IOS



Urejanje naprave	Urejanje naprave
Izbriši geslo	Izbriše se geslo naprave
Naprava za zaklepanje	Zaklepanje naprave (zaklepanje zaslona)
Naprava za izklop	Naprava za izklop

Ponovni zagon naprave	Ponovni zagon naprave
Alarm & Lostmode	Začetek Alarm & Lostmode
Onemogočite Lostmode	Onemogočite Lostmode
Brisanje naprave	Odstranitev naprave iz sistema AppTec
Brisanje naprave	Obnovitev tovarniških nastavitev naprave
Izbris podjetja	Informacije, aplikacije in profili, ki jih zagotavlja AppTec360, so izbrisani (naprava je ločena od MDM).
Odstranitev MDM	
Pošlji sporočilo	Pošiljanje potisnih obvestil v napravo Sporočilo bo prikazano v aplikaciji AppTec360 (zavihek Sporočilo).
Daljinski nadzor TeamViewer	Začetek seje daljinskega nadzora z uporabo programa TeamViewer
Pošlji zahtevo za vpis	Pošlji (ponavljajočo se) zahtevo za vpis

Urejanje naprave

Update Device
✕

Selected User	John Doe
Device Name	Device of John Doe
Phone Number (e.g. +49160123456)	<input type="text"/>
Operating System	iOS ▼
Device Type	Phone ▼
Ownership	Corporate Property ▼
Comment	<input style="width: 100%;" type="text"/>

Save

Tu lahko posodobite različne informacije o napravi.

Izbriši geslo

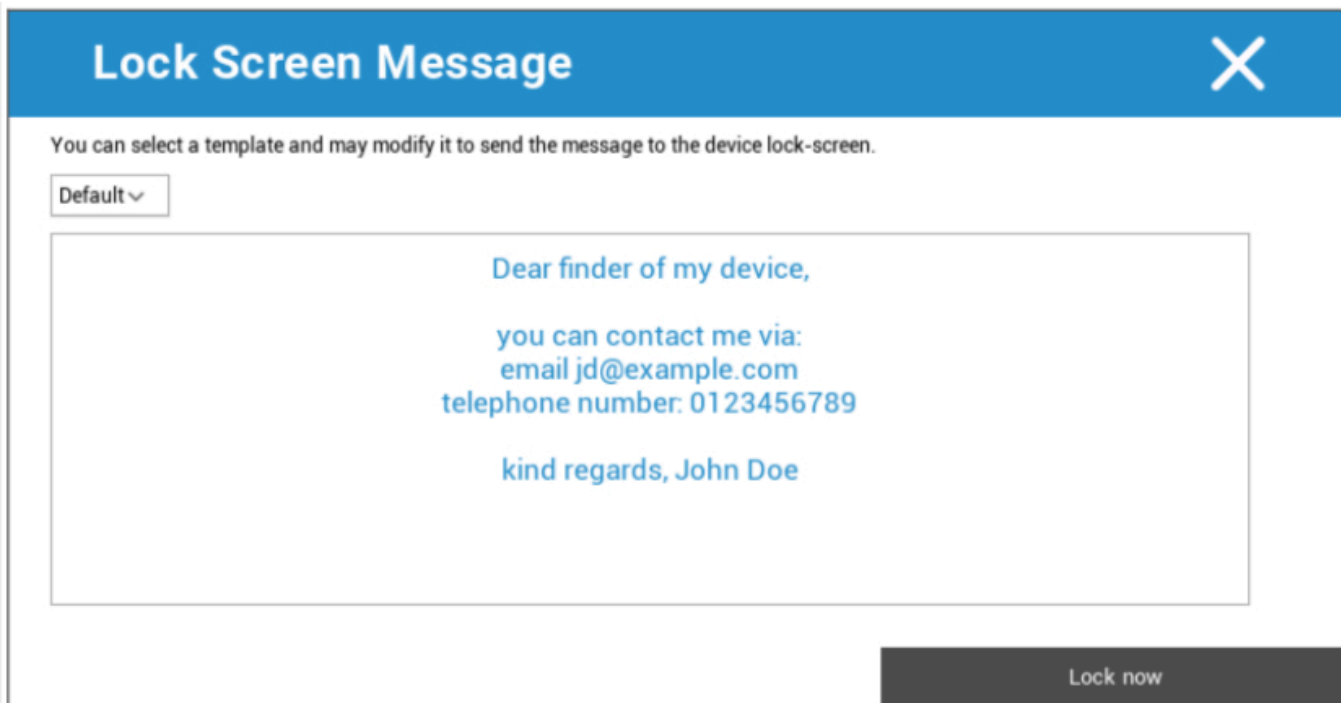
Clear Passcode?
✕

Are you sure to remove the passcode from the device?

No
Yes

V razdelku "Clear Passcode" lahko na daljavo odstranite geslo iz naprave. Nato bo uporabnik pozvan, da izda novo geslo (odvisno od smernic za geslo).

Naprava za zaklepanje



Lock Screen Message X

You can select a template and may modify it to send the message to the device lock-screen.

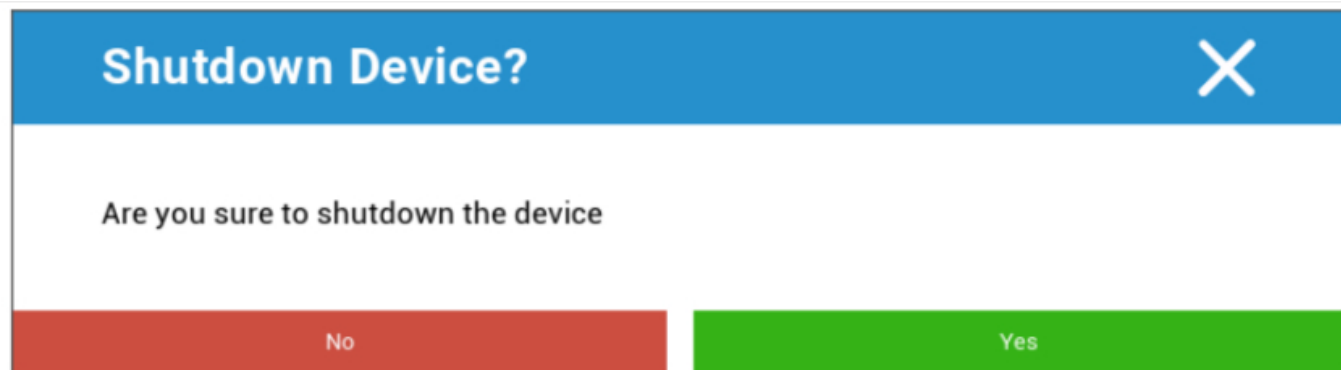
Default ▾

Dear finder of my device,
you can contact me via:
email jd@example.com
telephone number: 0123456789
kind regards, John Doe

Lock now

V tem primeru se končni uporabniški napravi pošlje ukaz za zaklepanje (zaklenjeni zaslon).

Naprava za izklop



Shutdown Device? X

Are you sure to shutdown the device

No Yes

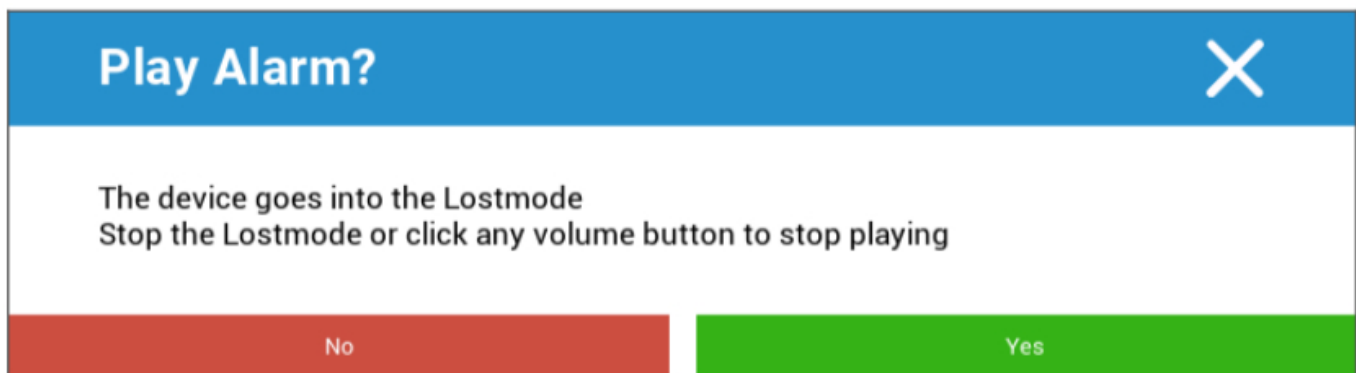
V tem primeru se končni uporabniški napravi pošlje ukaz za izklop.

Ponovni zagon naprave

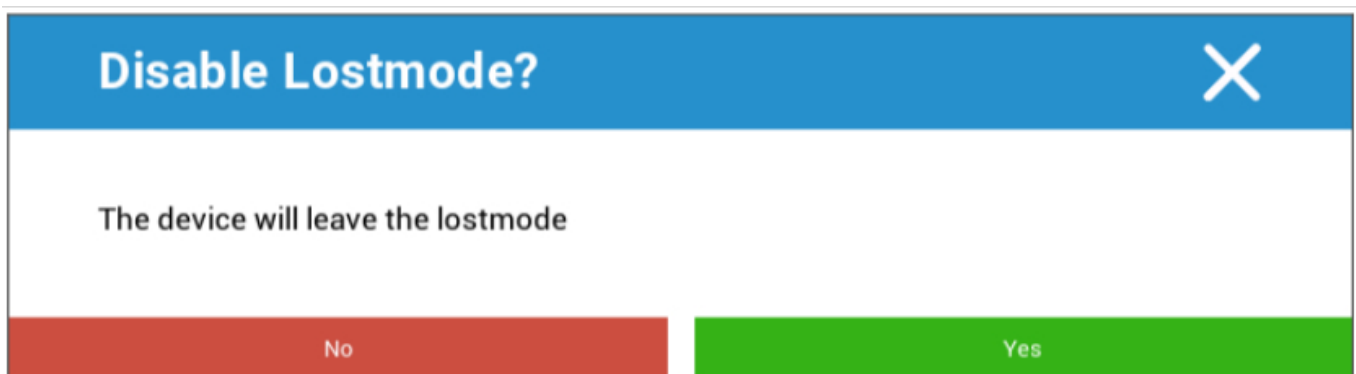


V tem primeru se končni uporabniški napravi pošlje ukaz za ponovni zagon.

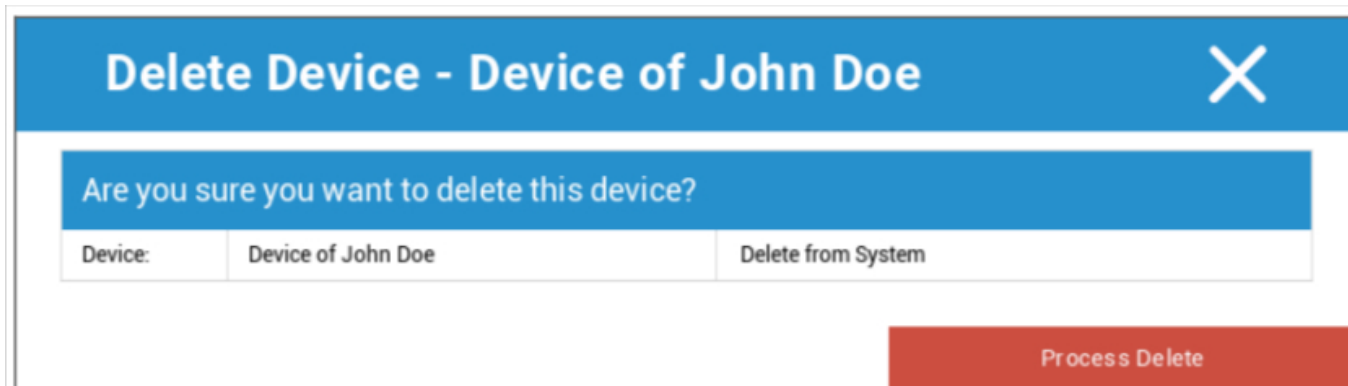
Alarm in način izgube | Onemogoči način izgube



Tukaj lahko napravo nastavite v način Lostmode, v katerem naprava stalno predvaja zvok alarma. Izgubljeni način lahko ustavite s pritiskom na kateri koli gumb za glasnost naprave ali na daljavo s klikom na "Disable Lostmode" (Onemogoči izgubljeni način):

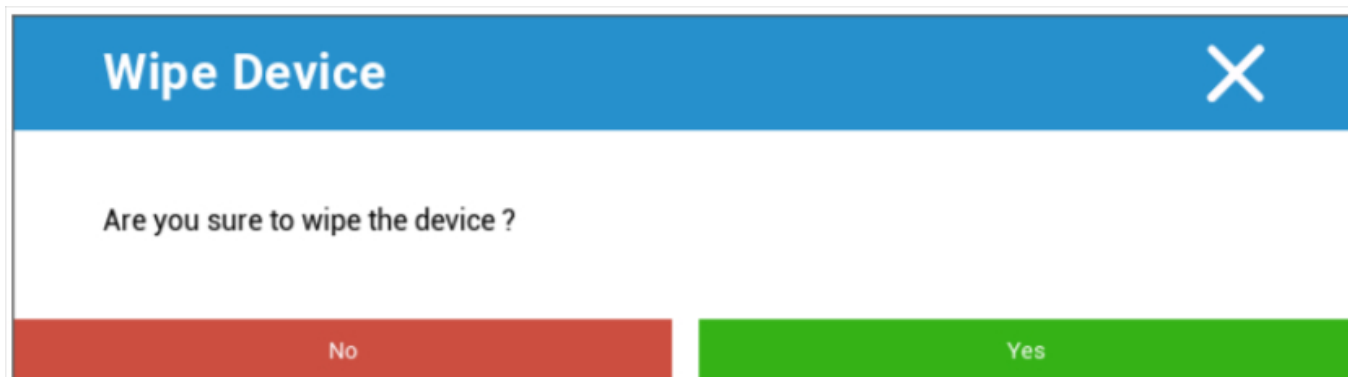


Brisanje naprave



Tu lahko izvedete ukaz za brisanje. Še enkrat se lahko odločite, ali naj se naprava odstrani samo iz AppTec360 ("Delete from System") ali pa naj se naprava odstrani iz AppTec360 in obnovi na tovarniško nastavitve ("Wipe & Delete").

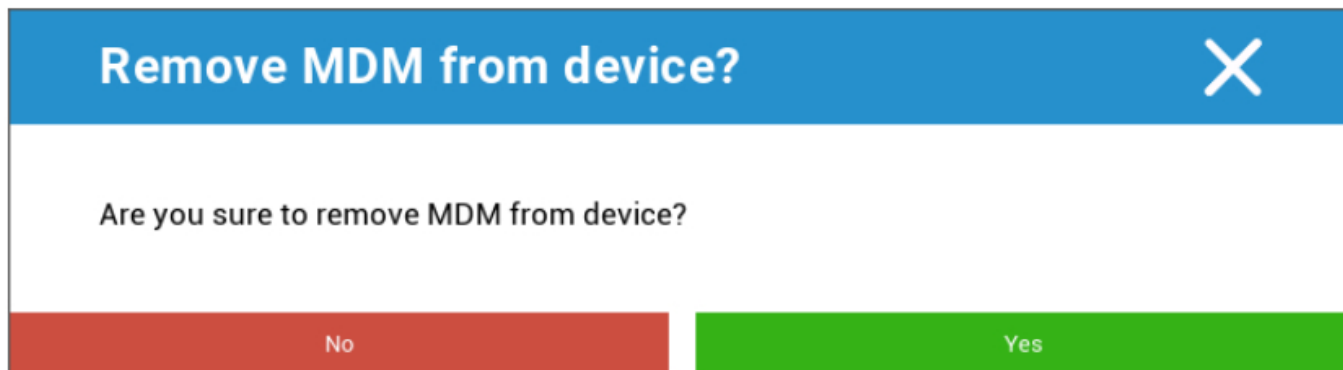
Brisanje naprave



V razdelku "Brisanje naprave" lahko izvedete popolno brisanje naprave. Naprava bo obnovljena na tovarniške nastavitve.

Brisanje v podjetju | Odstranitev MDM

Izbrišejo se samo informacije, aplikacije in profili, ki jih zagotovi AppTec360. Tako podatki podjetja ne bodo več na voljo v napravi končnega uporabnika. Na zasebno področje to ne vpliva in še naprej ostaja na napravi končnega uporabnika.



S funkcijo "Remove MDM" lahko odstranite profil MDM na napravi končnega uporabnika in vse druge elemente, ki jih zagotavlja AppTec.

Ta ukaz izvede enako dejanje kot ukaz "Enterprise Wipe".

Pošlji sporočilo

Send Message [X]

Subject: Attention! Please contact your IT administrator!

Message: Dear Mr. Doe,
Please contact your IT administrator immediately.

Send Message

Tu lahko pošljete potisno obvestilo v ustrezno napravo.

Daljinski nadzor TeamViewer

Remote Control [X]

Create a new TeamViewer session?

No Yes

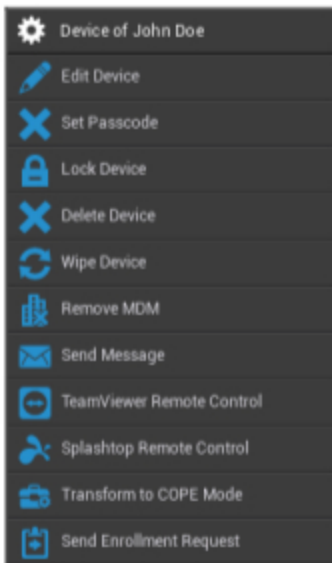
Tu lahko zaženete sejo oddaljenega nadzora Teamviewer.

Pošlji zahtevo za vpis

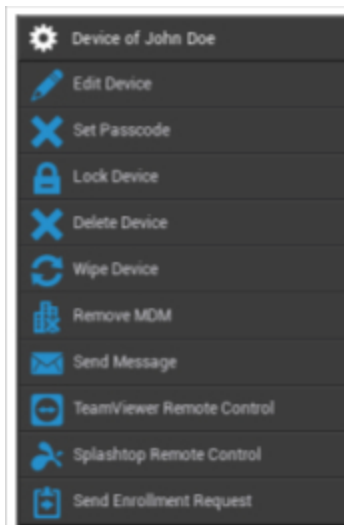
S funkcijo "Pošlji zahtevo za vpis" lahko zadevnemu uporabniku (ponovno) pošljete zahtevo za vpis.

Android

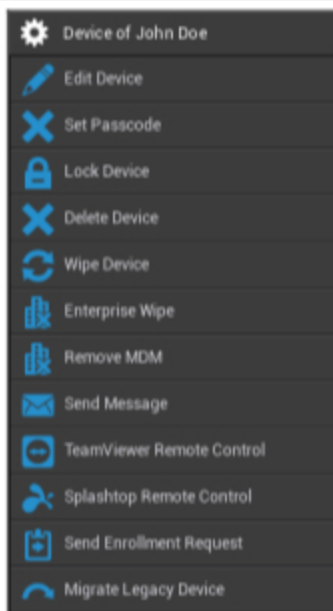
AE Popolnoma upravljana naprava (upravljanje dela)



Delovni profil AE (zabojnik)



Telefon s sistemom Android | Tablični računalnik



Urejanje naprave	Urejanje informacij o napravi
Nastavitev gesla	Nastavitev gesla naprave
Naprava za zaklepanje	Zaklepanje naprave (zaklepanje zaslona)
Brisanje naprave	Brisanje naprave iz aplikacije AppTec
Brisanje naprave	Obnovitev tovarniških nastavitev naprave
Izbris podjetja	Informacije, aplikacije in profili, ki jih zagotavlja AppTec360, so izbrisani (naprava bo ločena od MDM).
Odstranitev MDM	
Pošlji sporočilo	Pošiljanje potisnih obvestil v napravo Sporočilo bo prikazano v aplikaciji AppTec360 (zavihek Sporočilo).
Daljinski nadzor TeamViewer	Začetek seje daljinskega nadzora za to napravo z uporabo programa TeamViewer
Daljinski upravljalnik Splashtop	Začetek seje daljinskega upravljanja za to napravo s programom Splashtop
Preoblikovanje v način COPE (samo v napravi AE s popolnim upravljanjem (upravljanje dela))	Ustvarjanje delovnega profila v tej popolnoma upravljani (delovno upravljani) napravi AE
Pošlji zahtevo za vpis	Pošlji (ponavljajočo se) zahtevo za vpis
Migracija starejše naprave (samo v telefonu ali tabličnem računalniku s sistemom Android, če je	Migracija profila telefona ali tabličnega računalnika s sistemom Android v profil

vpisan z uporabo načina zagotavljanja lastnika
naprave)

popolnoma upravljane naprave AE
(upravljanje dela)

Urejanje naprave

Tu lahko posodobite različne informacije o napravi.

Update Device
✕

Selected User	John Doe
Device Name	Device of John Doe
Phone Number (e.g. +49160123456)	<input type="text"/>
Operating System	Android Enterprise ▼
Device Type	AE Fully Managed Device (Work Managed) ▼
Ownership	Corporate Property ▼
Comment	<input type="text"/>

Save

Izbrani uporabnik	Uporabnik naprave
Ime naprave	Ime naprave
Telefonska številka	Telefonska številka naprave
Operacijski sistem	Android Enterprise Android
Vrsta naprave	Android Enterprise: <ul style="list-style-type: none"> AE Popolnoma upravljana naprava (upravljanje dela) Način delovnega profila AE (samo zabožnik) AE Popolnoma upravljana naprava z delovnim profilom (COPE) Android: <ul style="list-style-type: none"> Telefon Tablični računalnik
Lastništvo	Corporate = lastnina podjetja

	Zaposleni = lastnost zaposlenega
Komentar:	Dodatni opisi za napravo

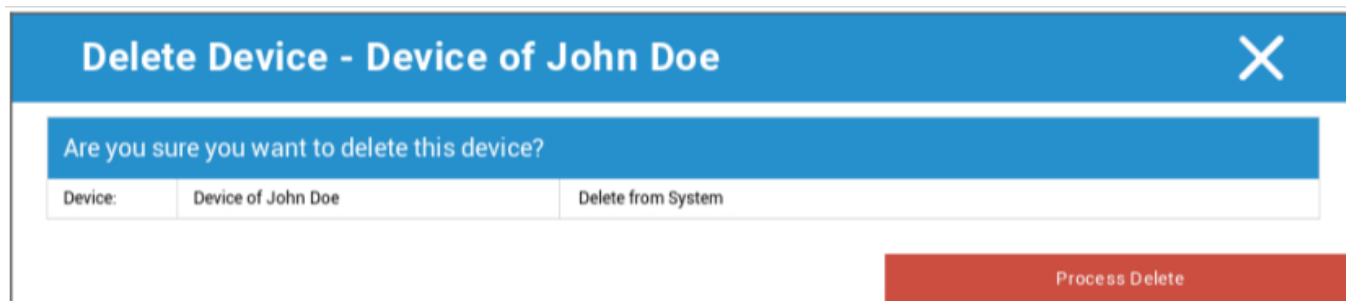
Izbriši geslo

Tukaj lahko odstranite geslo naprave v izbrani napravi. V sistemu Android je geslo privzeto nastavljeno na "123456" - uporabnik ga lahko in mora pozneje spremeniti.

Naprava za zaklepanje

Tu se napravi pošlje ukaz za zaklepanje naprave (zaklepanje zaslona).

Brisanje naprave



Tu lahko izvedete ukaz za brisanje. Še enkrat se lahko odločite, ali naj se naprava odstrani samo iz aplikacije AppTec360 ("Delete from System") ali pa naj se naprava odstrani iz aplikacije AppTec360 in dodatno obnovi na tovarniške nastavitve ("Wipe & Delete").

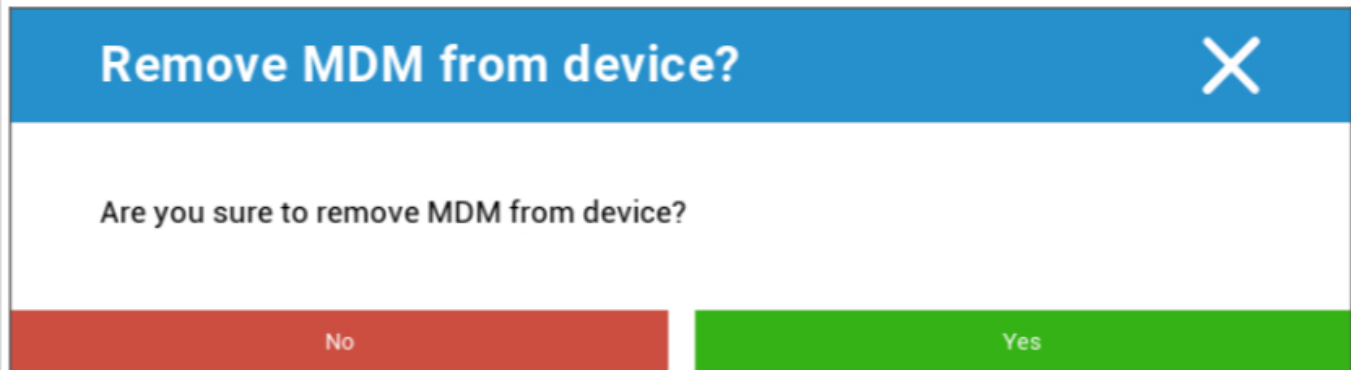
Brisanje naprave

V razdelku "Brisanje naprave" lahko izvedete popolno brisanje naprave. Naprava bo nato obnovljena na tovarniške nastavitve.



Če je v napravi kartica SD, lahko izbrišete tudi kartico SD. To lahko storite tako, da nastavite "Wipe SD Card too?" na "Vklopljeno".

Odstranitev MDM



Remove MDM from device? ✕

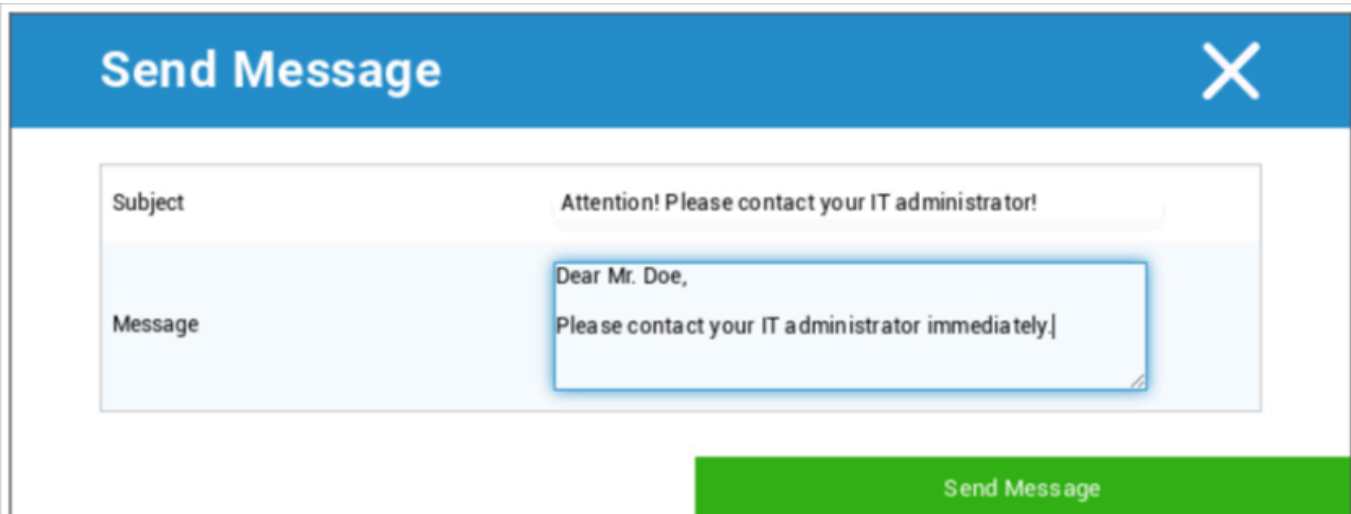
Are you sure to remove MDM from device?

No Yes

To je priporočena metoda za vzpostavitev ločitve od MDM.

Izbrišejo se samo informacije, aplikacije in profili, ki jih zagotovi AppTec360, kar pomeni, da vsi podatki podjetja ne bodo več na voljo v napravi končnega uporabnika. Na zasebno sfero pa to ne vpliva in še naprej ostaja v napravi končnega uporabnika.

Pošlji sporočilo



Send Message ✕

Subject Attention! Please contact your IT administrator!

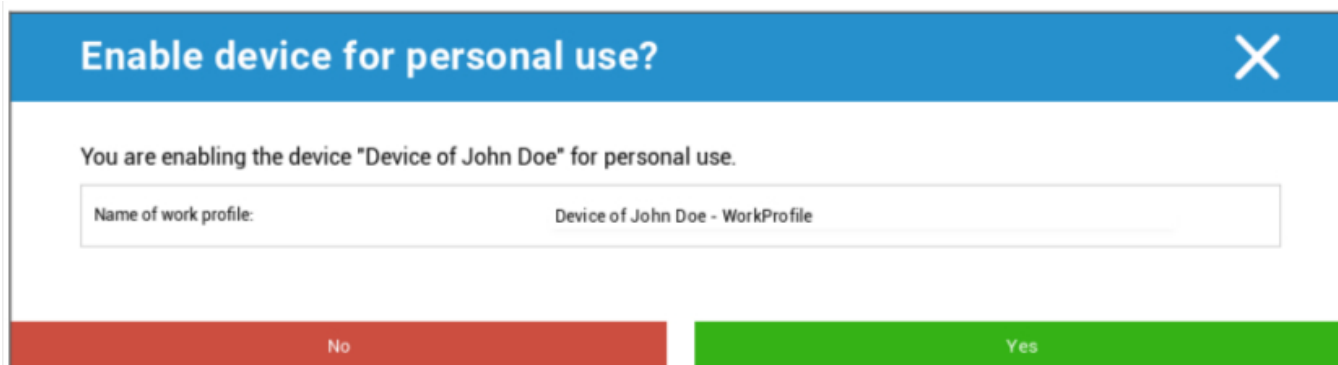
Message Dear Mr. Doe,
Please contact your IT administrator immediately!

Send Message

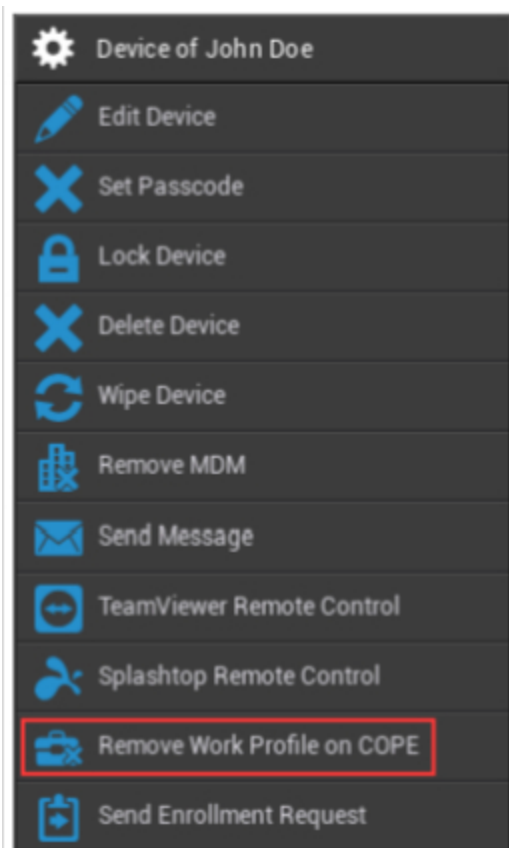
Tu lahko pošljete potisno obvestilo v ustrezno napravo končnega uporabnika.

Preoblikovanje v način COPE

Ustvarjanje delovnega profila v tej popolnoma upravljani (delovno upravljani) napravi AE



Po preoblikovanju naprave v način COPE lahko delovni profil odstranite tako, da kliknete možnost **Odstrani delovni profil v COPE**:



Remove Work Profile ✕

Do you really want to remove the work profile from this device

Cancel Delete

Pošlji zahtevo za vpis







S funkcijo "Pošlji zahtevo za vpis" lahko zadevnemu uporabniku (ponovno) pošljete zahtevo za vpis.

Upoštevajte, da je veljavna samo najnovejša prijava - zahtevk.

Migracija starejše naprave

Migracija profila telefona ali tabličnega računalnika s sistemom Android v profil popolnoma upravljane naprave AE (upravljanje dela)

Windows

 Device of John Doe	Ime naprave	Ime izbrane naprave
 Edit Device	Urejanje naprave	Urejanje naprave
 Delete Device	Brisanje naprave	Odstranitev naprave iz sistema AppTec
 Enterprise Wipe	Izbris podjetja	Informacije, aplikacije in profil, ki jih zagotovi AppTec360, so izbrisani
 Remove MDM	Odstranitev MDM	
 TeamViewer Remote Control	Daljinski nadzor TeamViewer	Daljinski nadzor naprave s programom TeamViewer
 Send Enrollment Request	Pošlji zahtevo za vpis	Pošlji zahtevo za vpis (ponovno)

Urejanje naprave

Update Device
✕

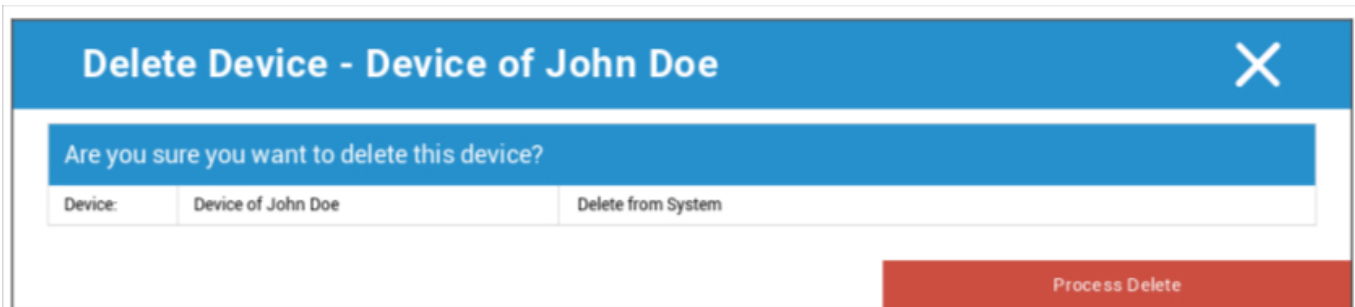
Selected User	John Doe
Device Name	Device of John Doe
Phone Number (e.g. +49160123456)	
Operating System	Windows 10 ▼
Device Type	Computer ▼
Ownership	Corporate Property ▼
Comment	<div style="border: 1px solid #ccc; height: 20px; width: 100%;"></div>

Save

Tu lahko posodobite različne informacije o napravi.

Brisanje naprave

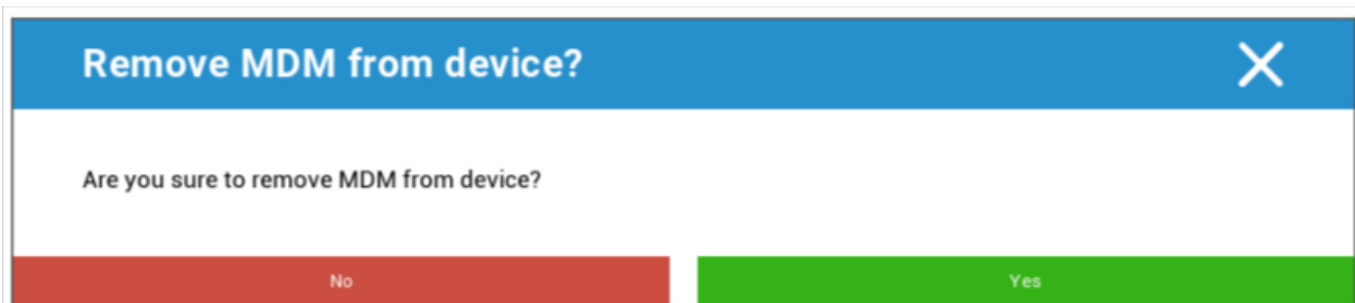
Tu lahko izvedete ukaz za brisanje, ki samo odstrani napravo iz aplikacije AppTec360.



Device:	Delete from System
Device of John Doe	Delete from System

Process Delete

Brisanje v podjetju | Odstranitev MDM



No Yes

Izbrišejo se samo informacije, aplikacije in profili, ki jih zagotovi AppTec360. Tako podatki podjetja ne bodo več na voljo v napravi končnega uporabnika. Na zasebno področje to ne vpliva in še naprej ostaja na napravi končnega uporabnika.

Daljinski nadzor TeamViewer



No Yes

Tu lahko zaženete sejo oddaljenega nadzora TeamViewer za to napravo.

Pošlji zahtevo za vpis

S funkcijo "Pošlji zahtevo za vpis" lahko zadevnemu uporabniku (ponovno) pošljete zahtevo za vpis.

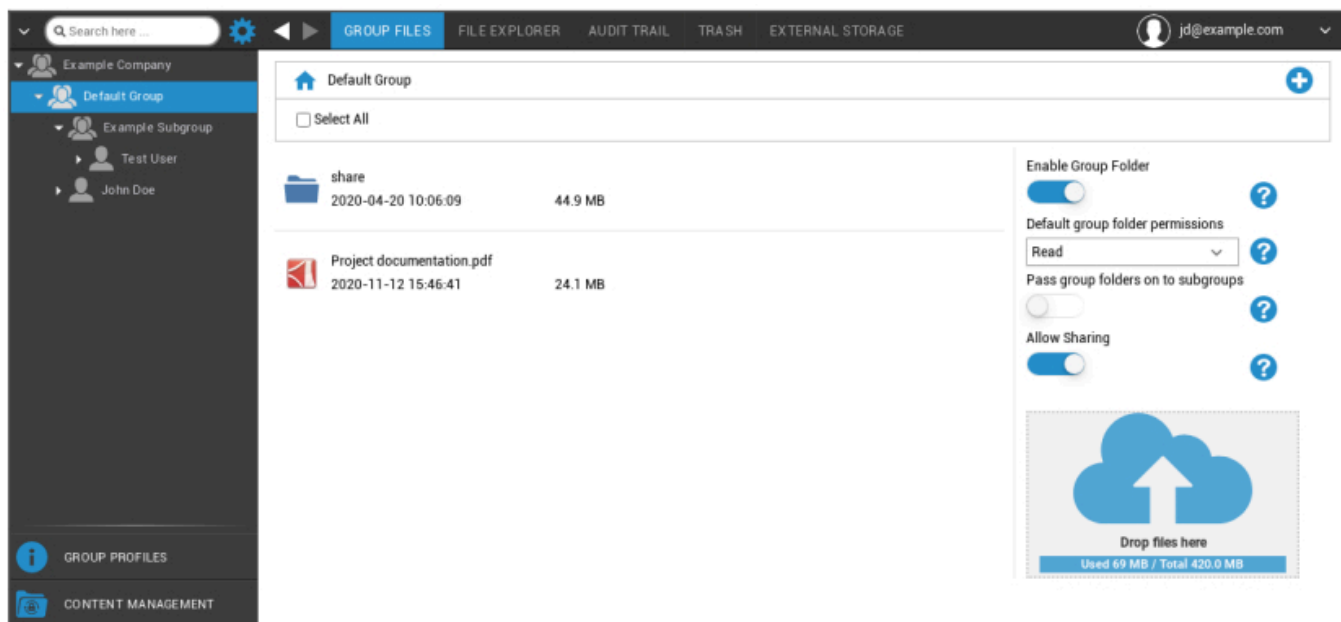
Upravljanje vsebine

Ko ste v skupini, lahko upravljate aplikacijo AppTec's ContentBox z "Upravljanje vsebine".

Z aplikacijo Content Box lahko dokumente in druge podatke podjetja varno razpošiljate v naprave končnih uporabnikov.

Datoteke skupin

"Datoteke skupine" predstavljajo temeljni del ContentBox. Tu lahko določite nastavitve, naložite dokumente, ustvarite nove mape itd.



S simbolom v zgornjem desnem kotu lahko ustvarite nove mape, ki jih z "Dodaj mapo" določite v ustrezno skupino.

S simbolom v zgornjem desnem kotu lahko prek možnosti "Dodaj mapo" ustvarite novo mapo, ki jo je treba dodeliti ustrezni skupini.

Mapo lahko poimenujete poljubno.



Prek možnosti "Naloži datoteke" lahko naložite podatke. Tu se bo odprl raziskovalec Standard-Explorer. Seveda lahko ti dve akciji izvedete v vsaki (pod)mapi.

S simbolom v zgornjem levem kotu se lahko vrnete v glavni meni.

Izberete lahko več map in datotek ter jih prenesete z gumbom "Download" ali pa jih izbrišete s klikom na gumb "Delete".

Izberete lahko tudi vse datoteke in mape z ukazoma "Prenesi" in "Izbriši".

Ko se z miško premaknete nad mapo ali datoteko, se prikaže naslednji pregled:



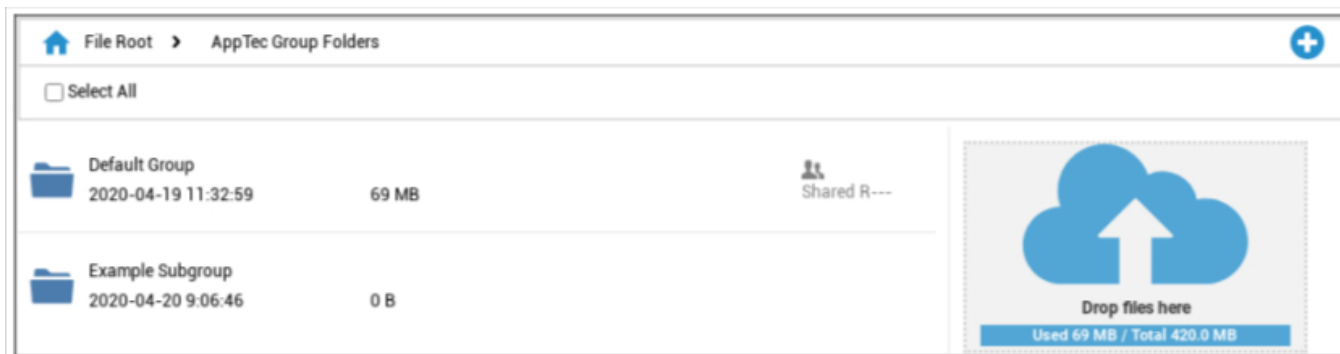
- S funkcijo "Preimenuj" lahko preimenujete mapo/datoteko.
- Z možnostjo "Prenos" lahko prenesete mapo/datoteko.
- Z "Delete" lahko izbrišete mapo/datoteko.

Omogočite mapo skupine	Če je aktivirano, imajo vsi člani skupine dostop do ustrezne mape.
Privzeta dovoljenja skupinskih map	Dovoljenja uporabnikov v izbrani skupini: Branje = dovoljenje samo za branje Posodobitev = dovoljenje za posodobitev Ustvari = dovoljenje za ustvarjanje Izbriši = dovoljenje za brisanje
Posredovanje skupinskih map podskupinam	Če je aktivirano, imajo lahko ustrezne podskupine dostop do nadrejenih podatkovnih datotek.
Dovoljenja za podskupine	Dovoljenja uporabnikov v izbrani podskupini: Branje = dovoljenje samo za branje Posodobitev = dovoljenje za posodobitev Ustvari = dovoljenje za ustvarjanje Izbriši = dovoljenje za brisanje
Omogočanje souporabe	Če je aktivirano, lahko uporabnik deli datoteke prek povezave.



Za nalaganje datotek lahko uporabite to polje tako, da v to okno povlečete datoteko z metodo povleci in spusti. To polje lahko tudi kliknete, da izberete in naložite datoteko s pomočjo brskalnika Internet Explorer.

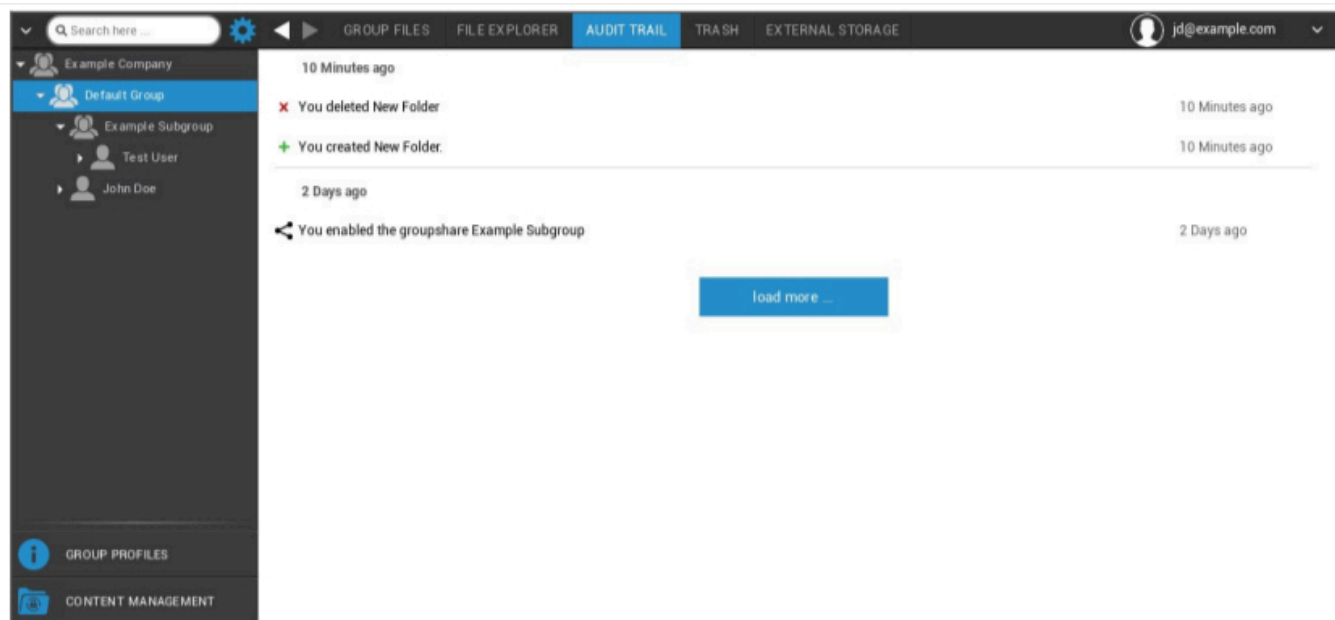
Raziskovalec datotek



Z Raziskovalcem datotek lahko upravljate vse mape in datoteke - ne glede na skupino, v kateri so shranjene.

Našli boste tudi nastavitve in gumbе, ki ste jih spoznali v poglavju "Skupinske datoteke".

Revizijska sled

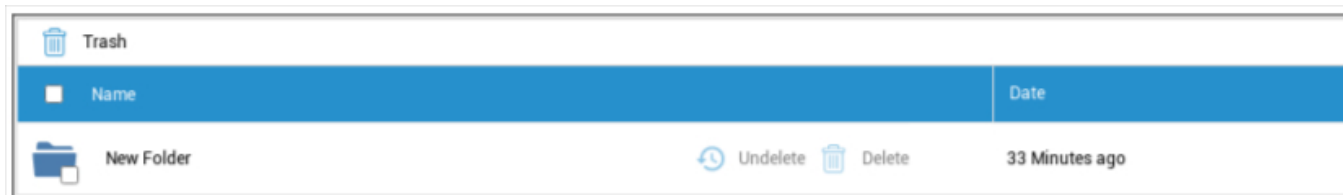


V razdelku "Revizijska sled" lahko iz zgodovine preverite, kateri uporabnik je kaj ustvaril, izbrisal ali delil. Tako lahko kadar koli ugotovite, kaj je bilo storjeno s podatki podjetja.

Odpadki

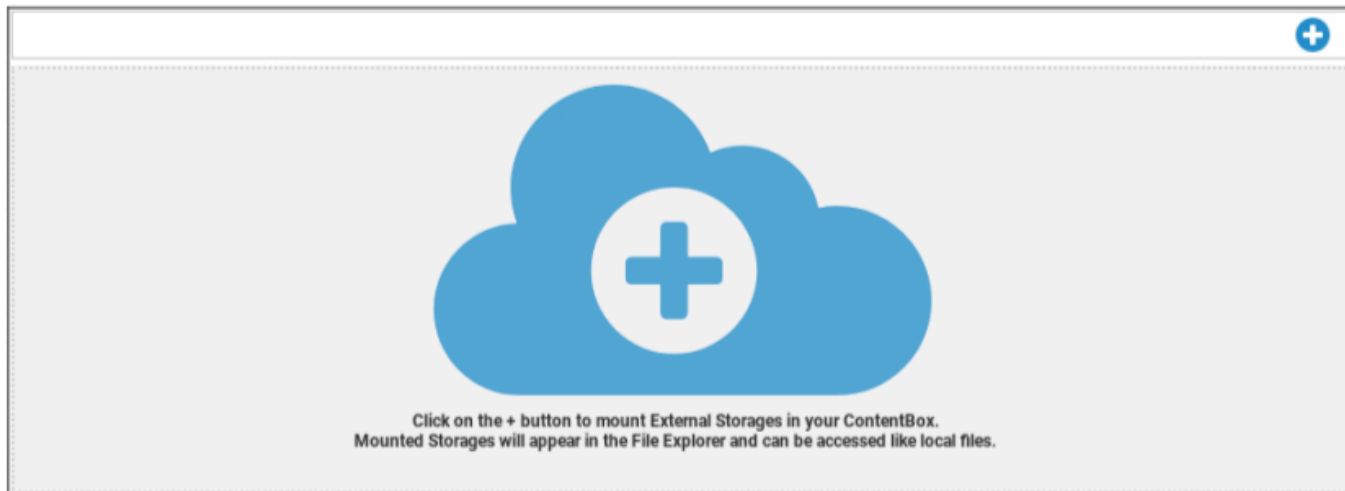
Če ste (po nesreči) kaj izbrisali, si lahko mape in datoteke ogledate v razdelku "Koš" in jih po želji obnovite.

- S funkcijo "Odstrani" lahko obnovite podatke/pomnilnik.
- Z ukazom "Izbriši" lahko trajno izbrišete podatke oz. mapo - ukaz za brisanje morate še enkrat potrditi.



Upoštevajte, da zmogljivost shranjevanja, ki se uporablja v košu, zmanjšuje razpoložljivi skupni prostor - to je zahteva storitve ownCloud.

Zunanje shranjevanje



Pod naslovom "Zunanji pomnilnik" lahko povežete zunanji pomnilnik.

S simbolom lahko dodate (dodatno) shrambo.

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

Amazon S3	
Prikazno ime	Prikaži ime
Ključ za dostop	Ključ za dostop
Skrivnostni ključ	Varnostni ključ
Vedro	Določena identiteta podmape, ki vam je bila dodeljena
Ime gostitelja (neobvezno)	Ime gostitelja (neobvezno)
Pristanišče (neobvezno)	Pristanišče (neobvezno)
Regija	Regija (neobvezno)
Omogočite SSL	Omogočite SSL
Omogoči slog poti	Izbrisati naslov poti, ki vam je bil dodeljen

FTP	
Prikazno ime	Prikaži ime
Gostitelj	Naslov gostitelja
Uporabniško ime	Uporabniško ime
Geslo	Geslo
Korenina	Glavni meni
Varno ftps://	

SFTP	
Prikazno ime	Prikaži ime
Gostitelj	Naslov gostitelja
Uporabniško ime	Uporabniško ime
Geslo	Geslo
Korenina	Glavni meni

ownCloud	
Prikazno ime	Prikaži ime
URL	URL lastnega oblaka
Uporabniško ime	Uporabniško ime
Geslo	Geslo
Oddaljena podmapa	Standardna mapa
Varna stran https://	

WebDAV	
Prikazno ime	Prikaži ime
URL	URL WebDAV
Uporabniško ime	Uporabniško ime
Geslo	Geslo
Korenina	Glavni meni
Varna stran https://	
Skupna raba sistema Windows	Podpora za Windows Share bo kmalu na voljo
SharePoint	Podpora za Microsoft SharePoint bo kmalu na voljo

Revizijski dnevnik

Tu najdete dnevnik, v katerem so zapisane informacije o dejanjih, ki se izvajajo v konzoli MDM.

Z ikono filtra lahko uporabite filtre za prikazani seznam.

V spustnem meniju **Elementi na stran**: lahko izberete število elementov, ki bodo prikazani na eni strani seznama.

Sprejeti ukrepi / spremenjene nastavitve	Ukrep, ki je bil izveden / nastavev, ki je bila spremenjena
Vrednost	Vrednost izvedenega ukrepa / spremenjene nastavitve
Uporabnik	Ime uporabnika, ki je izvedel dejanje / spremenil nastavev
Datum	Časovni žig, ko je bilo to dejanje izvedeno / ta nastavev spremenjena.
Pot / tip	Pot do kraja, kjer je bilo to dejanje izvedeno / ta nastavev je bila spremenjena

Konfiguracija sistema iOS

Splošno

Glede na to, ali ste trenutno izbrali skupino ali napravo, se prikaz in njegove podtočke razlikujejo - na to bodite pozorni!

Pregled profila skupine (samo na ravni skupine)

Ko odprete profil skupine, dobite hiter pregled profila.

Profile Name	Default Group Profile
Operating System	Android
Created At	01.03.2021 09:52:54
Created By	John Doe
Last Change	31.08.2021 16:35:50
Changed By	John Doe
Current Profile Revision	16
Released Profile Revision (outdated)	14

Delete Profile
Reset Group Profile
Copy Profile

Ime profila	Ime profila (tukaj ga lahko spremenite)
Operacijski sistem	Operacijski sistem, za katerega je profil namenjen
Ustvarjeno na	Čas nastanka
Ustvaril je	Ustvarjalec profila
Zadnja sprememba	Čas zadnje spremembe profila
Spremenjeno s	Račun, ki je opravil zadnje spremembe
Trenutna revizija profila	Revizija stanja shranjenega profila
Objavljena revizija profila	Dodeljena revizija profila ("Assigned profile revision"). Če je za besedilom na etiketi "(zastarela)", to pomeni, da ste profil shranili, vendar ga še niste dodelili, zato bodo naprave še vedno dobile starejšo različico.

Splošne informacije

Če ste neposredno v napravi, se prikaže kratek pregled izbrane naprave.

Ime naprave	Ime naprave
Telefonska številka	Telefonska številka naprave
Model	Številka modela
Operacijski sistem	OS
Serijska številka	Serijska številka naprave
Lastništvo naprave	Naprava za podjetja ali zasebna naprava Korporativni = naprava podjetja Zaposleni = zasebna naprava
Vrsta naprave	Vrsta naprave (tablični računalnik ali telefon)
Jailbrejk	Če je v napravi program Jailbreak
Pod nadzorom	Označuje, ali gre za nadzorovano napravo.
V skladu s predpisi	Če so bile kršene smernice
Nazadnje videno	Stanje, kdaj je naprava nazadnje komunicirala s strežnikom AppTec360

Nastavitve

Te nastavitve vsebujejo ime naprave in vnaprej določeno ozadje.

Ime naprave z imenom sistema	Ime, ki bo izdano v konzoli AppTec360 (v levi hierarhični strukturi), bo enako kot na zadevni napravi končnega uporabnika (vidno v nastavitvah naprave).
Uporaba ozadja po meri (samo nadzorovane naprave)	Tu lahko vnaprej določite ozadje, ki naj se prikaže na napravi končnega uporabnika (npr. za oblikovanje blagovne znamke podjetja za napravo). Je na voljo samo v nadzorovanem načinu!
Samodejne posodobitve operacijskega sistema	Posodobitve operacijskega sistema, če so na voljo. Samo za naprave DEP v nadzorovanem načinu.
Pisave po meri	Tu lahko dodate pisave po meri.
Ime	Po želji. Uporabniku vidno ime pisave. To polje se po namestitvi nadomesti z dejanskim imenom pisave.
Pisava	Naložite datoteko s pisavo (.otf ali .ttf).

Revizija konfiguracije

Tu boste dobili pregled nad tem, kateri profil skupine je določen za napravo.

Revision Overview			
	Installed Profile	Assigned Profile	Last Generated Profile
Device Profile	Device Profile: Revision 5	Device Profile: Revision 5	Device Profile: Revision 5
Group Profile	Default Group Profile: Revision 13	Default Group Profile: Revision 13 (Newer Revision available)	Default Group Profile: Revision 13

Če kliknete na profil skupine, boste neposredno dostopali do profila in opravili nastavitve.

S simbolom lahko dodeljene aplikacije vrnete v nastavitve skupinskega profila.



S tem simbolom lahko ponastavite profil naprave, tako da nima nobenih nastavitvev.

"Na voljo je novejša revizija" pomeni, da je bil profil skupine spremenjen in shranjen, vendar ni dodeljen. Profil skupine je treba dodeliti s funkcijo "Assign now" na ravni skupine, da se spremembe uporabijo v napravah.

Dnevnik naprave (samo na ravni naprave)

Dnevnik ukazov

Tu si lahko ogledate, kateri ukazi so bili izdani za napravo in kakšen je njihov status.

Command Log (last 250 commands)					
#	Created By	Date modified	Command	State	
1	jd@example.com	31.08.2021 12:21:37	Install assigned profiles	Device Pushed	
2	jd@example.com	31.08.2021 12:10:04	Get installed apps	Command Executed	
3	jd@example.com	31.08.2021 12:10:04	Get managed apps	Command Executed	
4	jd@example.com	31.08.2021 12:10:02	Get certificates	Command Executed	
5	jd@example.com	31.08.2021 12:10:02	Get asset data	Command Executed	
6	System Automated	31.08.2021 05:34:29	Update profile revision	Command Partially Failed 	
7	System Automated	31.08.2021 05:34:29	Apply device settings	Command Executed	
8	System Automated	31.08.2021 05:34:27	Install application	Command Failed 	
9	System Automated	31.08.2021 05:34:25	Get installed apps	Command Executed	
10	System Automated	31.08.2021 05:34:25	Get managed apps	Command Executed	
11	System Automated	31.08.2021 05:34:23	Get certificates	Command Executed	

Ukazi, ustvarjeni s "Sistemska avtomatizirano", se samodejno ustvarijo v sistemu.

Možni statusi ukazov

Potisnjena naprava	Storitvi za potiskanje (npr. APNS) je bila poslana potisna zahteva, da se naprava poveže nazaj s strežnikom EMM.
Ustvarjen ukaz	Ukaz je bil ustvarjen v sistemu.
Poslan ukaz	Ukaz je bil napravi poslan, ko se je povezala s strežnikom.
Izveden ukaz	Ukaz je bil uspešno izveden.
Ukaz ni uspel	Ukaz ni uspel. *
Ukaz delno ni uspel	Odvisno od operacijskega sistema naprave so lahko nekateri ukazi združeni. Pri tem nekateri deli te skupine ukazov niso bili uspešni. *
Ukaz se je izvršil, vendar je bil neuspešen	Ukaz je bil izveden, vendar morda ni bil.
Ukaz se ponovno premakne	Ukaz je ponovno poslal uporabnik.
Zavrženi	Ukaz je bil zavržen. Na primer zato, ker ga je nadomestil drug ukaz ali ker je bila naprava ponovno vpisana in so bili stari ukazi odstranjeni.

Če je za sporočilom izklicnik, lahko več informacij dobite tako, da s kazalcem podrsate nad ikono.

Upravljanje sredstev (samo na ravni naprave)

Upravljanje sredstev (samo na ravni naprave)

Informacije o napravi

Model	Številka modela naprave
Operacijski sistem	OS
Različica operacijskega sistema	Različica operacijskega sistema
Serijska številka	Serijska številka
UDID	UDID naprave
Ime naprave	Ime naprave
Pod nadzorom	Prikaže, ali je naprava nadzorovana
Stanje baterije	Stanje baterije

Wi-Fi

Naslov IP	Naslov IP naprave
WiFi MAC	Naslov WiFi MAC

Cellular

Status	Stanje (kartica SIM je prisotna)
Telefonska številka	Telefonska številka
Status gostovanja	Trenutni status gostovanja
Gostovanje (glasovno/po podatkih)	Status gostovanja za govorne/poštne storitve
Naslov IP	Naslov IP
IMEI	Številka IMEI
Operater/prevoznik	Ponudnik mobilnih storitev
Omrežje operaterja SIM	Nosilno omrežje SIM
Različica nosilca	Različica nosilca
Vdelana programska oprema modema	Vdelana programska oprema modema
Trenutni MCC/MNC	Glejte "SIM MCC/MNC".
SIM MCC/MNC	Koda mobilne države je identifikacija države, ki jo je določila ITU v skladu s standardom E.212 in se v povezavi s kodo mobilnega omrežja (MNC) uporablja za identifikacijo mobilnega omrežja (=koda države). Ko preidete v drugo mobilno omrežje, sta "trenutni MCC/MNC" in "SIM MCC/MNC" različna.

Bluetooth

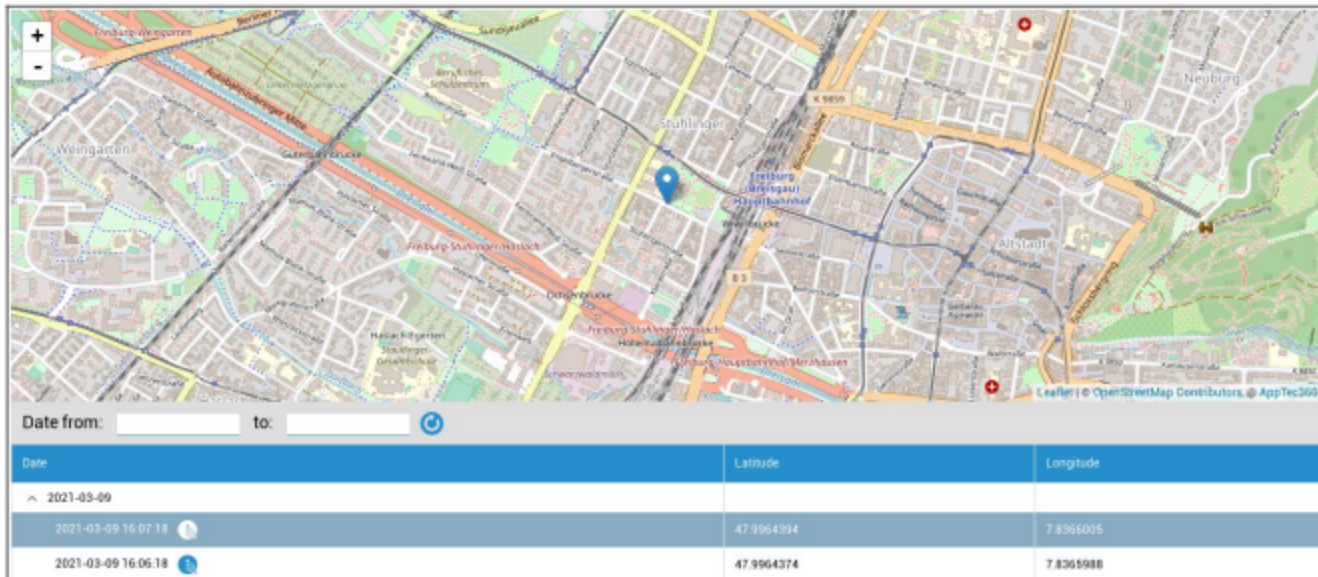
Bluetooth MAC	Naslov MAC Bluetooth
---------------	----------------------

Upravljanje varnosti

Zaščita pred krajo (samo na ravni naprave)

Informacije GPS (samo na ravni naprave)

Tu lahko ocenite trenutno/ zadnjo lokacijo naprave. Lokalizacijo lahko zaščitite z enim ali celo dvema gesloma - glejte: Splošne nastavitve - Zasebnost - Dostop do GPS





Date from: to:

Date	Latitude	Longitude
2021-03-09		
2021-03-09 16:07:18	47.9964394	7.8365005
2021-03-09 16:06:18	47.9964374	7.8365988

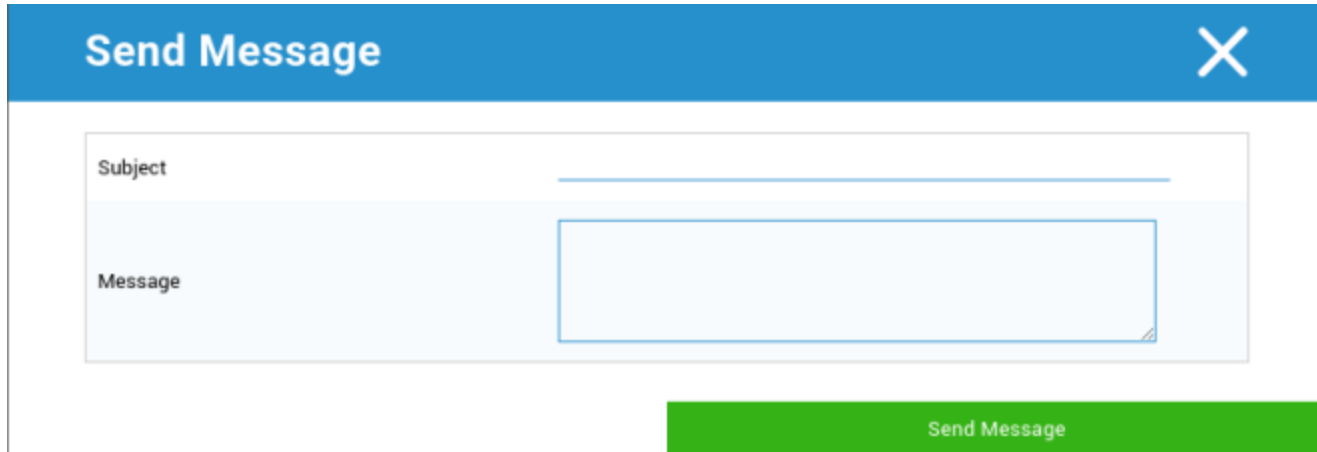
Brisanje in zaklepanje (samo na ravni naprave)

V razdelku "Brisanje in zaklepanje" lahko izvedete naslednja tri dejanja:

Celotno brisanje	Naprava je obnovljena na tovarniške nastavitve (izbrisani so tako poslovni kot osebni podatki).
Izbris podjetja	Iz naprave končnega uporabnika se odstranijo samo podatki podjetja (vse aplikacije, podatki itd., ki jih je zagotovil AppTec).
Zaklepanje zaslona	Zaklepanje zaslona je aktivirano, napravo je treba odkleniti z geslom naprave/PIN.
Forenzična zapora (samo nadzorovane naprave)	Če je ta funkcija aktivirana s simbolom  , se naprava zaklene s prikazom sporočila, ki ga ni mogoče zapreti. Zaposleni tudi ne more odkleniti naprave. Napravo lahko odklene samo skrbnik v konzoli s simbolom za odklepanje  .
Dovoli aktivacijsko zaporo (samo nadzorovane naprave)	Če je ta funkcija aktivirana , se naprava zaklene, takoj ko je v nastavitvah iCloud aktivirana funkcija "Poišči moj iPhone".

Sporočilo (samo na ravni naprave)

V naslednjem oknu lahko izpolnite predmet in sporočilo ter ga pošljete v napravo končnega uporabnika:



The screenshot shows a dialog box titled "Send Message" with a blue header and a white body. The dialog has a close button (X) in the top right corner. Inside the dialog, there are two input fields: "Subject" and "Message". The "Subject" field is a single-line text input, and the "Message" field is a multi-line text area. A green "Send Message" button is located at the bottom right of the dialog.

Varnostna konfiguracija

Pristopna koda


Tu določite nastavitve za geslo naprave.


Dovoljena deaktivacija kode	Ko je ta nastavev aktivirana, ni poziva za vnos gesla. Ko je geslo vzpostavljeno, ga ni mogoče deaktivirati.
Dovolite preprosto vrednost	Uporabniku omogočite uporabo enakih, naraščajočih in zmanjšanih nizov števil (npr. 1234, 1111).
Zahtevajte črkovno-številčno vrednost	Gesla morajo vsebovati vsaj eno črko.
Najmanjša dolžina gesla	Minimalna dolžina gesla
Najmanjše število zapletenih znakov	Najmanjše število alfanumeričnih simbolov v geslu
Najvišja starost gesla	Število dni, po katerih je treba geslo spremeniti
Največja samodejna zapora	Najdaljši čas, po katerem se naprava zaklene
Najdaljše obdobje odloga za zaklepanje naprave	Čas, po katerem naprava preide v zaklenjeno stanje pripravljenosti
Največje število neuspešnih poskusov	določa, kolikokrat je mogoče napačno vnesti geslo, preden se izvede popolno brisanje naprave.
Največja starost gesla (1-730 dni)	Najvišja starost gesla
Zgodovina geselskih kod (1-50 geselskih kod)	Po tem številu je dovoljena uporaba starega gesla.

S klikom na smetnjak se odpre Dialog za ponastavitev gesla, s katerim lahko izbrišete pozabljeno geslo naprave.

Potrdilo (samo na ravni naprave)

Prikaže potrdila, ki so na voljo v napravi

Navigation: Passcode | **Certificate** | Encryption | Single Sign On |  support@milanconsult.de

Installed Certificates			
Common Name	Is Identity	valid to	Show
33A1A2D1-CB30-E2D3-C1D2-6D7FC50E7352	YES	30.04.2017 - 13.25	

Šifriranje

Zahtevajte šifriranje shranjevanja	Aktivacija funkcije šifriranja nameščene naprave
------------------------------------	--

Enotna prijava

Pod točko "Enotna prijava" lahko konfigurirate preverjanje pristnosti Kerberos.

Tu določite poverilnice za dostop in ustrezne naslove URL/aplikacije, ki lahko uporabljajo žetone Kerberos.

Na voljo v nadzorovanem načinu	
Ime računa	Ime računa
Glavno ime	Edinstvena identiteta, ki ji je mogoče razdeliti vstopnice Kerberos
Področje	vaš Kerberos Realm, ki se bo uporabljal (npr. vaša domena)

S simbolom lahko določite dodatne naslove URL.

Vzorec URL, ki se uporablja za omejevanje tega računa	URL-ji, ki jih je treba določiti in na katere je mogoče razdeliti vstopnice Kerberos
---	--

S simbolom lahko vzpostavite dodatne aplikacije.

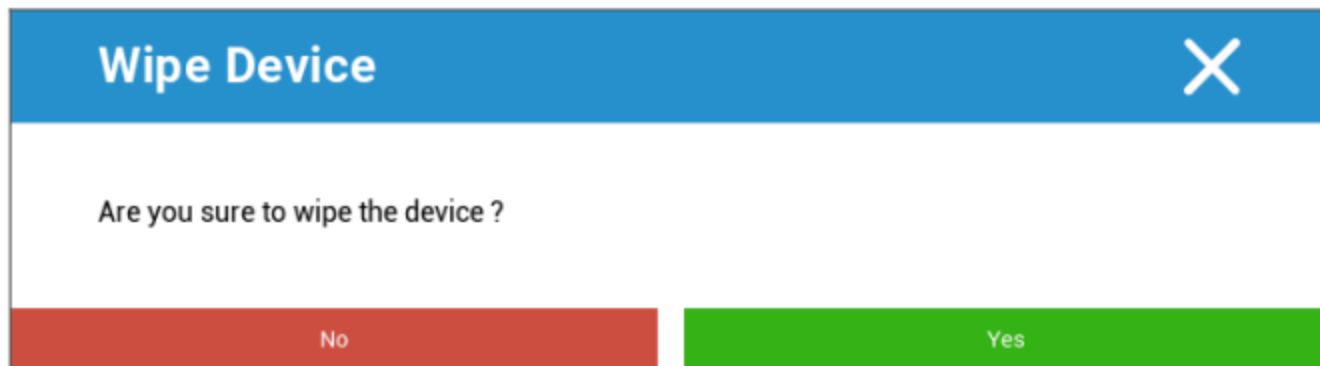
Aplikacije za omejitev tega računa	Določi se Aplikacije, ki jim je mogoče razdeliti vstopnice Kerberos
------------------------------------	---

Konec življenjske dobe (samo na ravni naprave)

Brisanje (samo na ravni naprave)

V razdelku "Brisanje" lahko obnovite tovarniške nastavitve naprave. Pri tem bodo v napravi končnega uporabnika izbrisani poslovni in zasebni podatki.

S klikom na simbol Minus se prikaže naslednje sporočilo



Z "Da" lahko izvedete brisanje.

V razdelku "Poročilo o brisanju" lahko prikažete naslednje elemente

Izbrisano z	Zgodovina izvajalca brisanja
Datum	Datum
Status	Status (npr. če je bilo brisanje uspešno izvedeno)

Nastavitve omejitev

Funkcionalnost naprave

Tu lahko blokirate posamezne funkcije naprave končnega uporabnika.

Omogočanje nameščanja aplikacij	Omogočanje nameščanja aplikacij
Dovolite kamero	Dovolite uporabo fotoaparata
Dovolite FaceTime	Dovolite FaceTime
Omogočite zajem zaslona	Omogočite zajem zaslona
Omogočanje samodejne sinhronizacije med gostovanjem	Omogočanje samodejne sinhronizacije med gostovanjem
Dovolite Siri	Dovolite Siri
Omogočanje glasovnega klicanja	Omogočanje glasovnega klicanja
Omogočanje nakupa v aplikaciji	Omogočanje nakupa v aplikaciji
Zahtevanje gesla trgovine iTunes Store za vse nakupe	Zahtevanje gesla trgovine iTunes Store za vse nakupe
Omogočite igranje iger za več igralcev	Omogočite igranje iger za več igralcev
Omogočanje dodajanja prijateljev v storitvi Game Center	Omogočanje dodajanja prijateljev v storitvi Game Center
Omogočanje odprtja iz upravljanega v neupravljanega	Omogočanje odpiranja vsebine v upravljanih aplikacijah v neupravljanih aplikacijah
Omogočanje odprtja iz upravljanega v upravljano	Omogočanje odpiranja vsebine iz neusmerjenih aplikacij v upravljanih aplikacijah
Omogočanje pogleda danes v zaklenjenem zaslonu	Ko je ta nastavek aktivna, se v središču za obvestila na zaklenjenem zaslonu prikaže pogled "Danes".
Dovolite nadzorno središče v zaklenjenem zaslonu	Omogočanje nadzornega središča na zaklenjenem zaslonu
Dovolite TouchID	Dovolite TouchID
Omogočanje posodobitev PKI v zraku	Omogočanje posodobitev PKI v zraku

Omogočanje knjižice, ko je zaklenjena	Omogočanje passbook, ko je naprava zaklenjena
Omejitev sledenja oglasov	Ta funkcija deaktivira sledenje oglasom (npr. oglaševalci ne morejo uporabljati sledenja oglasom za distribucijo prilagojenih oglasov).
Omogočanje posredovanja	Omogočanje posredovanja
Dovolite internetne rezultate v središču pozornosti	dovolite internetne rezultate v žarometu (npr. Bing ali Wikipedija).
Zahteva za geslo pri prvem seznanjanju AirPlay	Zahteva za geslo pri prvem seznanjanju AirPlay
Zaščita zapestja ure Force Watch	Če je aktivirana, je ura Apple Watch prisiljena uporabljati "zaščito zapestja" (prepoznavanje zapestja).
Omogočanje fototeke iCloud	Omogoča uporabo Fototeke iCloud. Če ni dovoljeno, bodo vse slike, ki niso bile v celoti prenesene iz oblaka iCloud, izbrisane v lokalni shrambi.
Na voljo v nadzorovanem načinu	
Dovolite spreminjanje računa	Omogočite spreminjanje "pošte, stikov, koledarja"
Omogočanje storitve AirDrop	Omogočanje storitve AirDrop
Dovolite aplikacijo Cellular Modification	Ta nastavitev blokira nastavitve za aplikacije, ki jim je dovoljena uporaba mobilnih podatkov. To nastavitev lahko na primer ročno nastavite v napravi končnega uporabnika in nato to omejitev aktivirate.
Dovolite Siri, da poizveduje po vsebini iz spleta, ki jo ustvarijo uporabniki	Spletno iskanje na nekaterih spletnih mestih je blokirano, npr. na Wikipediji, saj lahko vsakdo spreminja, kar želi.
Omogočanje Sirijevega preklinjanja	Preklinjanje, ki je namenjeno Siri, je cenzurirano.
Dovolite trgovino iBook Store	Dovolite trgovino iBook Store
Dovolite iBook Store Erotika	Dovolite iBook Store Erotika
Omogočanje spreminjanja nastavitve poišči moje prijatelje	Omogočanje spreminjanja nastavitve poišči moje prijatelje
Omogočite storitev Game Center	Omogočite storitev Game Center
Omogočanje združevanja gostiteljev	Usklajevanje nadzornih računalnikov

Omogočanje namestitve konfiguracijskih profilov	Omogočanje namestitve konfiguracijskih profilov
Dovolite Odstrani aplikacijo	Odstranitev nadzornih aplikacij
Dovolite iMessage	Dovolite iMessage
Omogočite brisanje vseh vsebin in nastavitev	Omogočanje brisanja vseh vsebin in nastavitev
Omogočanje konfiguriranja omejitev	Omogočanje konfiguriranja omejitev
Dovolite podcast	Dovolite podcast
Omogoči iskanje definicij	Omogoči iskanje definicije
Omogočanje napovedne tipkovnice	Omogočanje napovedne tipkovnice
Omogoči samodejno popravljanje	Omogočite samodejno popravljanje
Omogočanje namestitve aplikacij uporabniškega vmesnika	Če je deaktivirano, ni mogoče namestiti aplikacij iz javne trgovine AppStore (ikona ne bo več prikazana). Vendar pa lahko aplikacije še vedno namestite prek iTunes in Konfiguratorja.
Omogočanje bližnjic na tipkovnici	Omogočite bližnjice na tipkovnici, če je naprava povezana s fizično tipkovnico.
Omogočanje seznanjanja z uro Apple Watch	Prepoveduje seznanjanje med napravo in uro Apple Watch, obstoječe povezave bodo prekinjene.
Omogočanje spreminjanja gesla	Če ni dovoljeno, ni mogoče dodati, spremeniti ali odstraniti gesla naprave.
Dovolite spreminjanje imena naprave	Navodilo za določanje, ali je mogoče spremeniti ime naprave
Omogočite spreminjanje ozadja	Smernica za določanje, ali je mogoče spremeniti ozadje
Omogočanje samodejnega prenosa aplikacij	Če je deaktivirana, se kupljena aplikacija ne bo samodejno namestila v druge naprave. Ne velja za posodobitve za obstoječe aplikacije.
Dovolite novice	Dovolite novice v napravi iOS
Omogočanje zaupanja aplikacijam v podjetjih	Če je nastavljena na false, preprečuje zaupanje aplikacijam za podjetja.

iCloud

Blokiranje nekaterih funkcij med seznanjanjem z iCloudom

Dovolite varnostno kopiranje	Dovolite varnostno kopiranje
Omogočite sinhronizacijo dokumentov	Omogočite sinhronizacijo dokumentov
Dovolite tok fotografij	Dovolite tok fotografij
Omogočanje skupnega toka fotografij	Omogočanje skupnega toka fotografij
Omogočanje sinhronizacije ključev v oblaku	Omogočanje sinhronizacije ključev v oblaku
Upravljanim aplikacijam dovolite shranjevanje podatkov	Upravljanim aplikacijam dovolite shranjevanje podatkov
Omogočanje sinhronizacije opomb in poudarkov za poslovne knjige	Omogočanje sinhronizacije opomb in poudarkov za poslovne knjige
Omogočanje varnostnega kopiranja poslovnih knjig	Omogočanje varnostnega kopiranja poslovnih knjig

Varnost in zasebnost

Blokiranje teh funkcij, povezanih z diagnostičnimi podatki

Omogočanje pošiljanja diagnostičnih podatkov družbi Apple	Omogočanje pošiljanja diagnostičnih podatkov družbi Apple
Dovolite uporabniku, da sprejme nezaupanja vredna potrdila TLS	Dovolite uporabniku, da sprejme nezaupanja vredna potrdila TLS
Prisilite k šifriranim varnostnim kopijam	Prisilite k šifriranim varnostnim kopijam

BYOD

Vgrajena varnost sistema iOS (vsebnik)

iOS je vedno omogočal razlikovanje med upravljanimi (poslovnimi) in neupravljanimi (zasebnimi). Vse, kar prihaja iz sistema MDM, se obravnava kot upravljano. Če na primer namestite aplikacijo prek sistema MDM ali konfigurirate račun Exchange, bo sistem iOS to obravnaval kot upravljano.

Vse ostalo, kar se ročno konfigurira/namešča v napravo, se bo obravnavalo kot neupravljano. Na primer, če uporabnik sam namesti aplikacijo WhatsApp ali če doda račun Exchange. Vendar to ločevanje nikoli ni vplivalo na stike. Od različice iOS 11.3 (in višje) pa je bilo to dodano tudi za stike.

Ker je to osnovna funkcionalnost operacijskega sistema, vam ni treba ničesar nameščati ali nastavljati posebne posode.

Aktivirajte vgrajeno funkcijo za ločevanje zasebnih in poslovnih aplikacij/informacij/datotek. Ta nastavev bo onemogočila tudi nekatere druge funkcije, ki bi sicer lahko po pomoti izklopile dele tega ločevanja.

Aktivacija

Aktivirajte rešitve zabožnikov, ki jih podpira AppTec360

Omogočanje vsebnika Google Divide	Omogočanje vsebnika Google Divide
Omogočanje vsebnika SecurePIM	Omogočanje vsebnika SecurePIM

Če ste aktivirali SecurePIM Container, boste pod "Activation" našli tudi naslednjo točko. Poleg tega se bodo takoj odprli še štirje zavihki, ki so opisani v nadaljevanju.

E-poštni naslov za podporo	e-poštni naslov za podporo, kamor se lahko uporabnik obrne s težavami
----------------------------	---

SecurePIM Geslo

V razdelku "SecurePIM Password" lahko določite smernice za varnostno moč gesla.

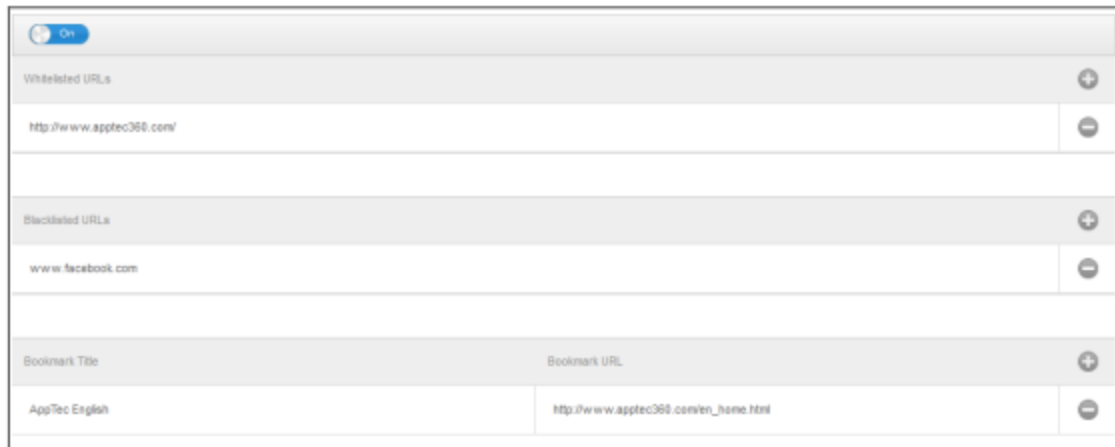
Časovna omejitev seje	Tu lahko določite, po koliko minutah je treba ponovno vnesti novo geslo, ko SecurePIM deluje v ozadju.
Dolžina gesla	Dolžina gesla za dostop do vsebnika SecurePIM
Znaki velike začetnice	Najmanjši obseg velikih črk
Znaki malih črk	Najmanjši obseg malih črk
Posebni znaki	Najmanjši število posebnih znakov
Številke	Najmanjši številčni podatki
Uporaba brisanja	Kolikokrat je mogoče napačno vnesti geslo, preden se vsebina SecurePIM izbriše. (Aplikacija pa še vedno ostane v napravi končnega uporabnika.)

Varnost SecurePIM

V razdelku "SecurePIM Security" lahko določite različne varnostne nastavitve.

Odkrivanje naprav z odloženim dostopom	Če je ta nastavitev aktivirana, bo dostop do vsebnika SecurePIM blokiran, takoj ko bo naprava zaznana kot zlomljena.
Varna besedilna polja	Vsebina polj za oddajo bo šifrirana, operacijski sistem (iOS) ne bo prejel nobenih informacij. Opomba: Dokler je ta nastavitev aktivna, samodejni popravek ni več na voljo.
Izvoz podatkov o stikih v napravo	Če je ta nastavitev aktivirana, lahko uporabnik izvozi stike Exchange v svojo lokalno napravo. Opomba: Izvozita se samo ime in telefonska številka.
Prikaži lokacijo dogodka	Če je ta nastavitev aktivirana, se v vrstici z obvestili prikaže lokacija prihajajočih dogodkov.
Prikaži naslov dogodka	Če je ta nastavitev aktivirana, se v vrstici z obvestili prikaže lokacija naslova prihajajočega dogodka.

Brskalnik SecurePIM



Tu lahko nastavite brskalnik SecurePIM.

S simbolom lahko določite nov naslov URL.

S simbolom lahko znova odstranite določen URL.

"URL-ji z bele liste" so URL-ji, ki jih je mogoče naložiti.

"URL-ji s črnega seznama" so URL-ji, ki jih ni mogoče naložiti in so zato blokirani.

Upoštevajte, da imajo vnosi na beli seznam večjo prednost kot vnosi na črni seznam. V razdelku "Bookmark Title" (Naslov zaznamka) lahko določite naslov. V razdelku "Bookmark URL" lahko naslov URL povežete z naslovom zaznamka - tako lahko posameznim uporabnikom razdelite individualizirane zaznamke.

Izmenjava

V razdelku "Exchange" lahko konfigurirate račun Exchange.

e-poštni naslov storitve ActiveSync	e-poštni naslov Exchange (upoštevajte "Namestna imena").
ActiveSync Exchange Prijava	Uporabniška imena izmenjave (upoštevajte "Namestna imena")
ActiveSync Strežnik Exchange	Naslov strežnika Exchange (FQDN)
ActiveSync Domena Exchange	Naslov domene Exchange
Potrdilo uporabnika	Potrdilo uporabnika
Preverjanje pristnosti na podlagi potrdila	Uporabnik se avtentificira s potrdilom
Omogočanje šifriranja S/MIME	Uporabniku omogoča, da šifrira svojo pošto.
Omogočanje podpisovanja S/MIME	Uporabniku omogoča, da podpiše svojo pošto.
Preverjanje CRL	Če je aktivno, se zasebno potrdilo primerja s seznamom CRL (Certificate Revocation List).

Upravljanje povezav

Wi-Fi

Identifikator nabora storitev (SSID)	SSID omrežja, ki ga želite povezati
Samodejno pridruževanje	Aktivacija samodejnega pridruževanja ob pridružitvi omrežju
Skrito omrežje	Aktiviraj, če AP ne oddaja SSID.

Nastavitev posredniškega strežnika

Konfiguracija posredniškega strežnika za vsako dostopno točko

Ni	Vzpostavitev brez pooblaščenca
Priročnik	Vzpostavitev ročnega pooblaščenca
URL strežnika proxy	Naslov za dostop do nastavitve posredniškega strežnika
Pristanišče	Določite vrata za posrednika
Preverjanje pristnosti	Uporabniško ime za preverjanje pristnosti v posredniškem strežniku
Geslo	Geslo za preverjanje pristnosti v posredniškem strežniku
Samodejno	Samodejna vzpostavitev pooblaščenca
URL strežnika proxy	URL za dostop do nastavitve posredniškega strežnika

Vrsta varnosti

Vzpostavitev varnostne vrste za AP

WEP	
Geslo	Geslo za AP

WPA/WPA2	
Geslo	Geslo za AP

WEP Enterprise - WPA / WPA2 Enterprise - Any Enterprise		
Protokoli		
TLS	Aktivacija/deaktivacija	
TTLS	Aktivacija/deaktivacija	
LEAP	Aktivacija/deaktivacija	
PEAP	Aktivacija/deaktivacija	
EAP-FAST	Aktivacija/deaktivacija	
EAP-SIM	Aktivacija/deaktivacija	
Uporaba PAC		Uporaba sistema PAC (Protected Access Control)
Določba PAC	Konfiguracija sistema Provision PAC	
Anonimno zagotavljanje PAC	Anonimno zagotavljanje PAC	
Notranje preverjanje pristnosti	Protokol za preverjanje pristnosti, ki ga je treba uporabiti: PAP, CHAP, MSCHAP, MSCHAPv2	
Uporabniško ime	Uporabniško ime za preverjanje pristnosti	
Ne uporabljajte gesla na povezavo	Ne uporabljajte gesla na povezavo	
Potrdilo o identiteti	Prenos/izbira potrdila za preverjanje pristnosti	
Zunanja identiteta	Identiteta, ki je vidna navzven	
Zaupanje		
Zaupanja vredno potrdilo 1	Prenesite prvo zaupanja vredno potrdilo	
Zaupanja vredno potrdilo 2	Naložite drugo zaupanja vredno potrdilo	
Zaupanja vredno potrdilo 3	Prenos tretjega zaupanja vrednega potrdila	
Imena potrdil zaupanja vrednih strežnikov	Imena pričakovanih strežniških potrdil (na seznamu, ločenem z vejico)	

Ni	Ne vzpostavi varnosti
----	-----------------------

VPN

Ime povezave	Ime profila VPN
--------------	-----------------

Vrsta VPN

VPN

Ves omrežni promet naprave bo usmerjen prek povezave VPN.

Vrsta povezave	Vzpostavitev vrste povezave VPN
IPsec (cisco)	Protokol IPsec podjetja cisco
PPTP	Protokol PPTP
L2TP	Protokol L2TP
Cisco AnyConnect	Protokol AnyConnect
Juniper SSL	Protokol Juniper SSL
F5 SSL	Protokol SSL družbe F5
SonicWall mConnect	SonicWall mobile Connect
Aruba VIA	Protokol Aruba VIA
SSL po meri	Povezava prek SSL po meri
OpenVPN	Protokol OpenVPN

VPN za posamezno aplikacijo

Ob odprtju določene aplikacije se vzpostavi povezava VPN.

Samodejni zagon povezave VPN za posamezno aplikacijo	Samodejni zagon povezave VPN za posamezno aplikacijo
Vrsta povezave	Vzpostavitev vrste povezave VPN
Cisco AnyConnect	Protokol AnyConnect
Juniper SSL	Protokol Juniper SSL
F5 SSL	Protokol SSL družbe F5
SonicWall mConnect	SonicWall mobile Connect
Aruba VIA	Protokol Aruba VIA
SSL po meri	Povezava prek SSL po meri
OpenVPN	Protokol OpenVPN

Nastavitev posredniškega strežnika

Konfiguracija posredniškega strežnika za povezavo VPN

Ni	Vzpostavitev brez pooblaščenca
Priročnik	Ročna vzpostavitev posredniškega strežnika
URL strežnika proxy	Naslov za dostop do nastavitv posredniškega strežnika
Pristanišče	Določite vrata za posrednika
Preverjanje pristnosti	Uporabniško ime za preverjanje pristnosti v posredniškem strežniku
Geslo	Geslo za preverjanje pristnosti v posredniškem strežniku
Samodejno	Samodejna vzpostavitev pooblaščenca
URL strežnika proxy	URL za dostop do nastavitv posredniškega strežnika

Prikaži nadomestna mesta	Prikaže vse razpoložljive uporabniške spremenljivke, ki jih AppTec360 lahko uporablja.
--------------------------	--

APN

Ime dostopne točke	Ime dostopne točke
Uporabniško ime dostopne točke	Uporabniško ime dostopne točke
Geslo dostopne točke	Geslo dostopne točke
Strežnik proxy	Naslov strežnika proxy
Pristanišče	Ustrezna vrata posredniškega strežnika

Cellular

Omogočanje podatkovnega gostovanja	Omogočanje podatkovnega gostovanja
Omogočanje glasovnega gostovanja	Omogočanje glasovnega gostovanja
Omogočanje vroče točke	Omogočanje vroče točke

Proxy strežnik HTTP

Vrsta pooblaščenca	
Priročnik	Ročno vzpostavite proxy strežnik
URL strežnika proxy	Naslov za dostop do nastavitve posredniškega strežnika
Pristanišče	Vzpostavitev pristanišča posredniškega strežnika
Preverjanje pristnosti	Uporabniško ime za preverjanje pristnosti v posredniškem strežniku
Geslo	Geslo za preverjanje pristnosti v posredniškem strežniku
Samodejno	Samodejna vzpostavitev pooblaščenca
URL naslov proxy PAC	URL naslov proxy PAC
Omogoči neposredno povezavo, če je PAC nedosegljiv	Omogočite neposredno povezavo (brez VPN), če PAC ni dosegljiv
Omogočanje izogibanja posredniškemu strežniku za dostop do omrežij v ujetništvu	Omogočanje izogibanja posredniškemu strežniku za dostop do notranjih omrežij v ujetništvu

AirPrint

Naslov IP	Naslov IP tiskalnika
Pot virov	Določena pot do naprave AirPrint

AirPlay

Ime naprave	Ime naprave
Geslo	Geslo za seznanjanje
Bela lista	Opredelitev seznama naprav, s katerimi se lahko naprava izključno poveže

Upravljanje PIM

Exchange Active Sync

Ime računa	Ime e-poštnega računa
Gostitelj Exchange ActiveSync	Naslov/FQDN strežnika
Dovolite premik	Omogočite premikanje e-poštnih sporočil
Uporabljajte samo v pošti	Interakcije se lahko pojavijo samo v domači aplikaciji Mail App.
Uporaba protokola SSL	Uporaba šifriranja SSL
Domena	Domena strežnika
Uporabnik	Uporabniško ime
E-poštni naslov	e-poštni naslov (samo na ravni naprave).
Geslo (samo na ravni naprave)	Uporabniško geslo
Potrdilo o identiteti	Izberite ustrezno potrdilo za preverjanje pristnosti v strežniku
Pretekli dnevi programa Mail to Sync	Število dni, do katerih je treba e-pošto sinhronizirati nazaj. Brez omejitev = neomejeno
Omogočite S/MIME	Omogočanje šifriranja S/MIME
Podpisno potrdilo	Naložite ustrezno potrdilo za podpisovanje
Potrdilo o šifriranju	Prenesite ustrezno šifrirno potrdilo

Elektronska pošta

Nastavitev računov POP3 / IMAP v napravi končnega uporabnika

Opis računa	Ime des E-poštni računi		
Vrsta računa	IMAP	Predpona poti	Predpona poti za posebne mape
	POP		
Prikazno ime uporabnika	Prikazno ime uporabnika		
Elektronski naslov	Elektronski naslov uporabnika		
Dovolite premik	Omogočite premikanje e-poštnih sporočil		
Omogočite S/MIME	Omogočanje šifriranja S/MIME		
Podpisno potrdilo	Naložite ustrezno potrdilo za podpisovanje		
Potrdilo o šifriranju	Prenesite ustrezno šifrirno potrdilo		

Dohodna pošta

Nastavitve dohodnega strežnika

Naslov poštnega strežnika	Naslov poštnega strežnika
Vrata poštnega strežnika	Vrata poštnega strežnika
Uporabniško ime	Ustrezno uporabniško ime
Vrsta preverjanja pristnosti	Vrsta preverjanja pristnosti
Ni	Ne Vrsta preverjanja pristnosti
Geslo (samo na ravni naprave)	Poziv za geslo
MDM izziv-odgovor	
NTLM	Preverjanje pristnosti NTLM
HTTP MD5 Digest	
Uporaba protokola SSL	Po potrebi uporabite SSL

Odhodna pošta

Nastavitve odhodnega strežnika

Naslov poštnega strežnika	Naslov poštnega strežnika
Vrata poštnega strežnika	Vrata poštnega strežnika
Uporabniško ime	Ustrezno uporabniško ime
Vrsta preverjanja pristnosti	
Ni	Ni metode avtentikacije
Geslo (samo na ravni naprave)	Poziv za geslo
MDM izziv-odgovor	
NTLM	Preverjanje pristnosti NTLM
HTTP MD5 Digest	
Uporaba protokola SSL	Po potrebi uporabite SSL
Odhodno geslo enako kot vhodno	Odhodno geslo enako kot vhodno
Uporabljajte samo v pošti	Aktivirajte, če naj se vsa odhodna e-poštna sporočila pošiljajo prek aplikacije Mail-App.

CalDav

Konfiguracija vzpostavitve in distribucije računa CalDav

Opis računa	Prikazno ime računa
Ime gostitelja	Ime gostitelja in/ali naslov IP
Pristanišče	Pristanišče računa CalDav
Glavni naslov URL	Glavni naslov URL računa
Uporabniško ime	Ustrezno uporabniško ime CalDav
Geslo (samo na ravni naprave)	Ustrezno geslo CalDav
Uporaba protokola SSL	Po potrebi uporabite SSL

Naročeni koledarji

Nastavitev in distribucija naročenih koledarjev

Opis	Prikazno ime računa
URL	URL baze podatkov koledarja
Uporabniško ime	Uporabniško ime naročnine na koledar
Geslo (samo na ravni naprave)	Geslo naročnine na koledar
Uporaba protokola SSL	Po potrebi uporabite SSL

LDAP

Na tem področju nastavite povezavo LDAP, da omogočite dinamično izmenjavo potrdil med napravo končnega uporabnika in imenikom Active Directory.

Upoštevajte, da izbrani uporabnik potrebuje ustrezno dovoljenje za branje.

Opis računa	Opis računa
Uporabniško ime računa	Uporabnik za dostop do protokola LDAP
Geslo računa	Geslo za dostop do protokola LDAP
Ime gostitelja računa	Gostiteljsko ime/IP naslov strežnika LDAP
Uporaba protokola SSL	Po potrebi uporabite SSL

V drugem delu lahko določite posamezne filtre za iskanje v registru LDAP.

Opis	Področje uporabe	Osnova za iskanje
Opis filtra	Raven iskanja v registru LDAP	Oprelitev posameznega filtra

Spletno upravljanje

Spletni posnetki

Na tem mestu določite zaznamke s povezavami do spletnih strani, intranetnih portalov itd., ki bodo vidni kot aplikacija v napravi končnega uporabnika.

Oznaka	Ime povezave v napravi končnega uporabnika
URL	Povezava do ustreznega spletnega mesta
Odstranljiva stran	Če je aktivirano, lahko uporabnik odstrani spletni posnetek
Ikona	V tem pogovornem oknu naložite logotip za povezavo: Velikost 180x180, format png
Predhodno sestavljena ikona	Če je aktivirano, se na ikoni ne prikažejo dodatni učinki (senca, odsev).
Celoten zaslon	Pri odpiranju spletnih posnetkov se brskalnik odpre v celozaslonskem načinu

Filter spletnih vsebin

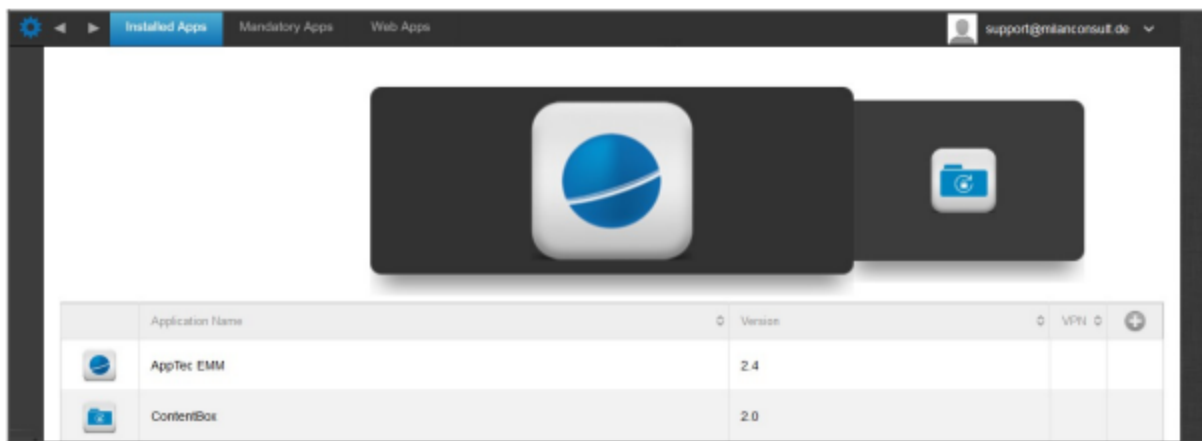
Filter spletnih vsebin omogoča omejitve dostopa do določenih spletnih strani.

Dovoljene spletne strani	
Omejite vsebino za odrasle	Spletni filter se samodejno uporabi za vsebino za odrasle
Dovoljeni naslovi URL	S simbolom + dodajte dovoljene strani
URL-ji na črnem seznamu	S simbolom + dodajte blokirane strani
Samo določene spletne strani	Prikaže se lahko samo določena vsebina, ki jo lahko dodate s simbolom +.

Upravljanje aplikacij

Upravitelj aplikacij za podjetja

Nameščene aplikacije (samo na ravni naprave)



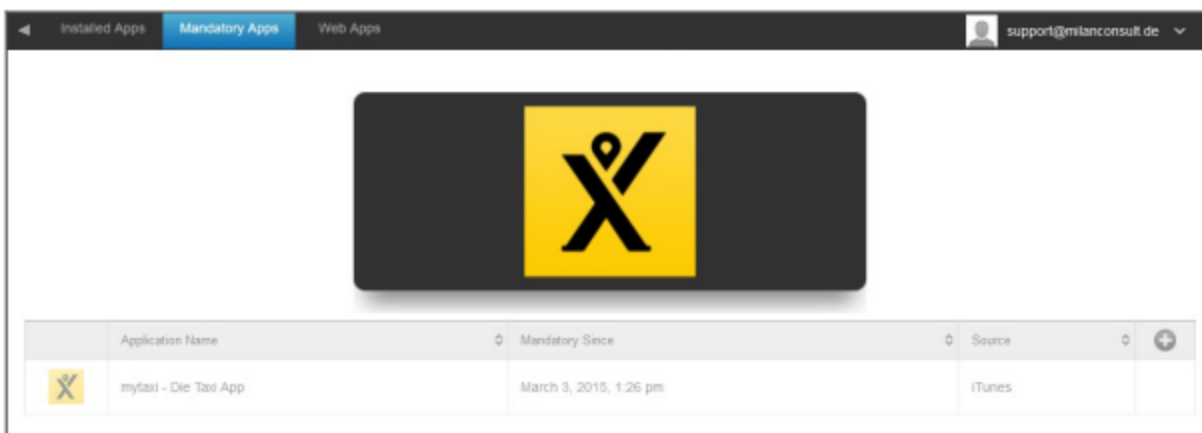
Tu si lahko ogledate aplikacije, ki so trenutno nameščene v napravi.

Obvezne aplikacije

V razdelku Obvezne aplikacije lahko določite potrebne aplikacije.

Uporabnik bo nenehno opominjan, da mora namestiti to aplikacijo.

V oknu , je mogoče opredeliti obvezno aplikacijo.



To je lahko aplikacija Apple App Store, lahko pa tudi notranja aplikacija.

Če gre za nadzorovano napravo, se aplikacija namesti samodejno.

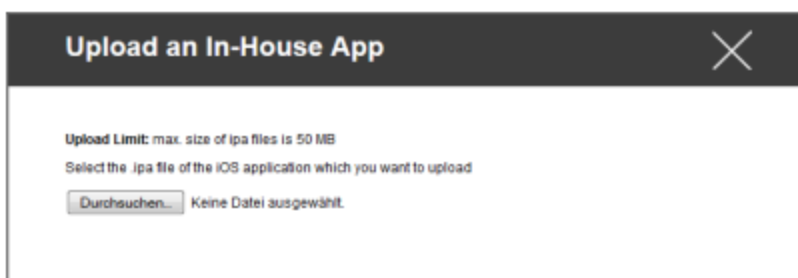
V napravo lahko prenesete aplikacijo iz javne trgovine Apple AppStore in interno razvito aplikacijo.

Lahko pa izberete kategorijo "Lastne aplikacije za iOS" in izberete lastno aplikacijo, ki ste jo naložili v Splošne nastavitve.

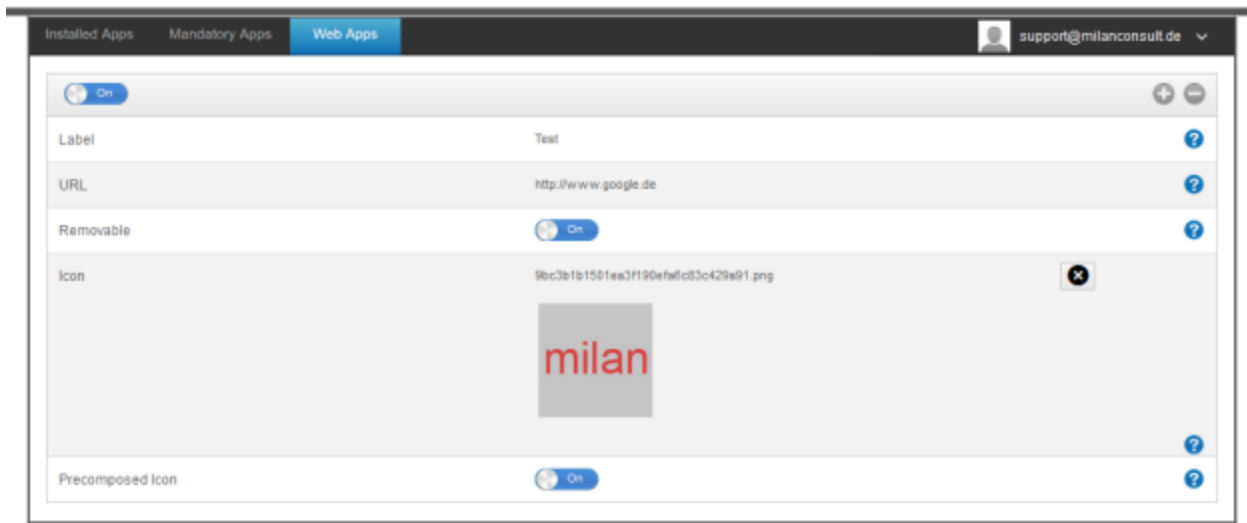
Možnosti namestitve

Posodabljanje (podprto samo za VPP na napravo)	Enkrat na teden bo določeno, ali je za aplikacijo na voljo posodobitev. Če je odgovor pritrdilen, bo posodobitev nameščena. Za domače aplikacije se bo za postopek posodabljanja uporabil cilj posodabljanja, ki ste ga konfigurirali v splošnih nastavitvah.
Prehitevanje, kadar ni upravljano	Če je aplikacija že nameščena, bo MDM prevzel aplikacijo in jo upravljati.
Odstranitev aplikacije ob odstranitvi profila MDM	V primeru odstranitve naprave za upravljanje bo aplikacija odstranjena.
Preprečevanje varnostnega kopiranja podatkov aplikacije	Varnostna kopija podatkov, specifičnih za aplikacijo, ne bo ustvarjena.
Nastavitve aplikacije	V razdelku "Nastavitve aplikacije" lahko aplikaciji dodelite določene vrednosti v ospredje (če aplikacija to podpira, po potrebi vprašajte razvijalca aplikacije).

Datoteko ipa lahko tudi neposredno izberete in naložite prek možnosti "Naloži domačo aplikacijo".



Spletne aplikacije



Pod točko "Spletne aplikacije" lahko, podobno kot pri "Spletnih klipih", internetne strani ali intranetne portale kot aplikacijo prenesete v napravo končnega uporabnika na področju upravljanja spleta. Privzeto bodo spletne aplikacije prikazane v celozaslonskem načinu, ki ga lahko konfigurirate v razdelku Spletni posnetki.

Oznaka	Ime povezave v napravi končnega uporabnika
URL	Povezava na zadevno spletno mesto
Odstranljiv	Če je aktivirano, lahko uporabnik odstrani spletno sličico
Ikona	V tem pogovornem oknu naložite logotip za povezavo: Velikost 180x180, format png
Predhodno sestavljena ikona	Če je aktivirano, na ikoni ne bodo prikazani dodatni učinki (senca, odsev).

Omejitve in nastavitve

Aplikacije na črnem seznamu / belem seznamu

Tu lahko nastavite aplikacije, ki so blokirane (ali dovoljene) glede na vaše nastavitve v "Splošnih nastavitvah". S klikom na se prikaže iskanje znanih aplikacij. Tam lahko poiščete aplikacije, ki jih želite dodati.

Upošteвайте, da je za to funkcijo potrebna nadzorovana naprava.

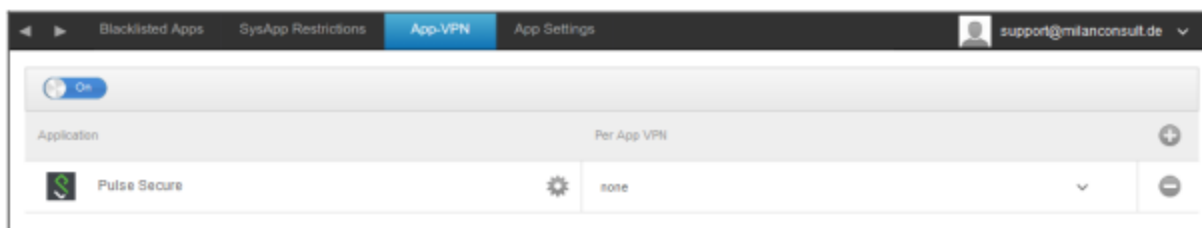
Omejitve aplikacije SysApp

blokiranje določenih aplikacij ali funkcij naprave

Dovolite uporabo storitve YouTube	Dovolite uporabo storitve YouTube
Omogočanje uporabe trgovine iTunes Store	Omogočanje uporabe trgovine iTunes Store
Dovolite uporabo brskalnika Safari	Dovolite uporabo brskalnika Safari
Omogočanje samodejnega izpolnjevanja	Omogoča samodejno izpolnjevanje
Opozorilo o goljufijah s strani sile	Izključi opozorilo o goljufiji
Omogočite jezik JavaScript	Omogoča uporabo JavaScript
Blokiranje pojavnih oken	Blokira vse vrste lutk-ups
Dovolite piškotke	Izberite, kdaj bo Safari sprejemal piškotke

App-VPN

S simbolom lahko določite aplikacije, ki bodo ob zagonu samodejno zagnale izbrano povezavo VPN.



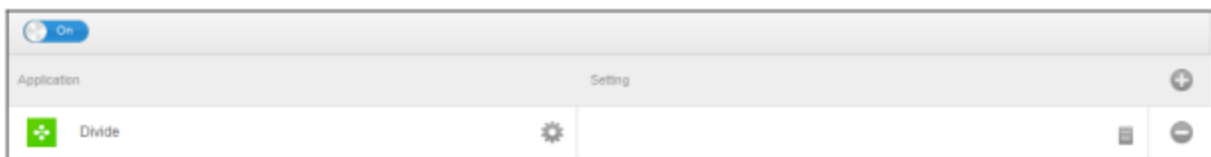
Nastavitve aplikacije


V razdelku "Nastavitve aplikacije" lahko aplikaciji dodelite določene vrednosti v ospredje (če aplikacija to podpira, po potrebi vprašajte razvijalca aplikacije).

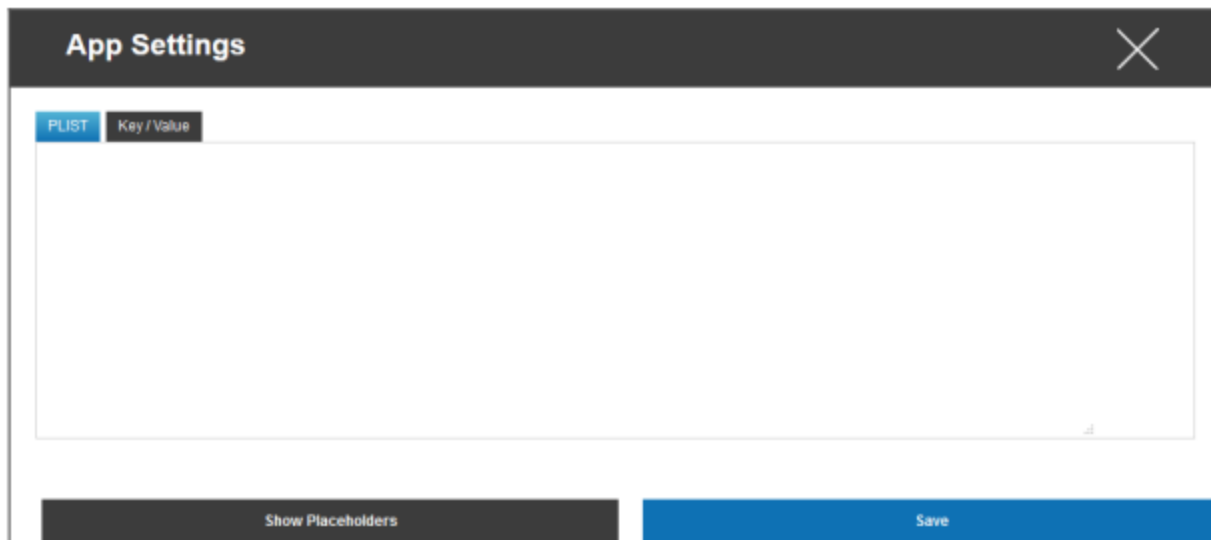
S simbolom dodate (dodatno) aplikacijo. Spet boste našli znano predstavitev AppTec360 za uvoz aplikacij.

Tu poiščite aplikacijo, ki jo želite konfigurirati, in jo izberite. Nastavitve bodo veljale samo za upravljane aplikacije.

Če je bil uvoz uspešen, se prikaže naslednji prikaz:

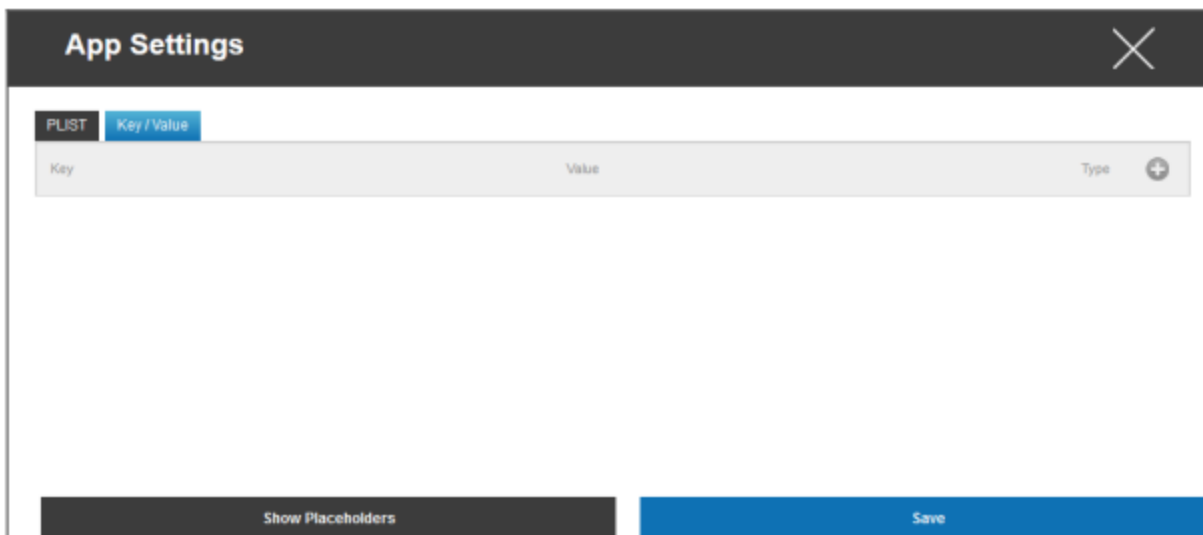


Zdaj lahko s klikom na  , izvedete različne konfiguracije. Nato se vam bo prikazal naslednji pregled:

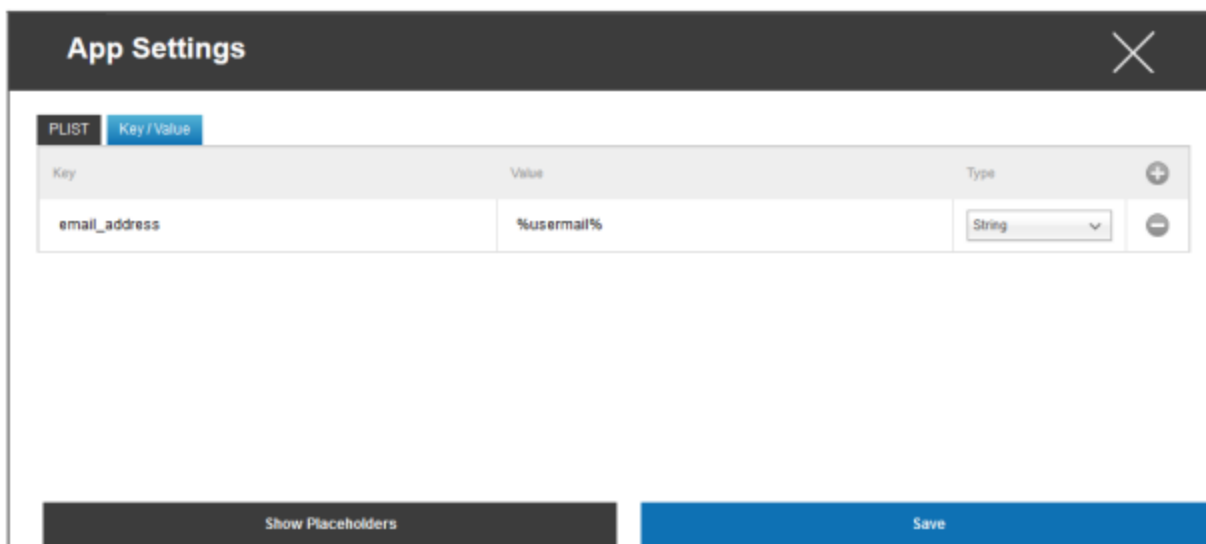


Če že imate PLIST (izvorno besedilo konfiguracije), ga lahko dodate tukaj in vse skupaj shranite s "Shrani".

V razdelku "Ključ / vrednost" lahko aplikaciji priložite določene konfiguracije.



Tu lahko s simbolom določite nov ključ in njegovo vrednost.



Seveda so vam na voljo vsi namestni elementi programa AppTec.

Razlaga "Type":

Niz	Besedilo
Boolean	Resnično/neresnično
Številka	Številka

S simbolom lahko aplikacijo znova odstranite.

Trgovina z aplikacijami za podjetja

Aplikacije iTunes

V tej točki lahko za uporabnika razdelite izbirne aplikacije.

Če je tukaj aplikacija, se samodejno namesti v napravo končnega uporabnika trgovine AppTec360.

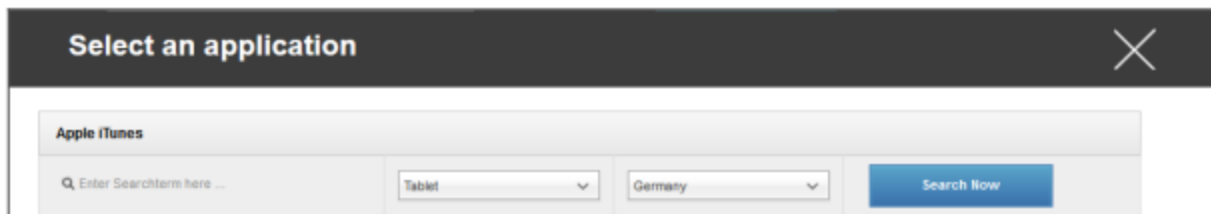
To so samo povezave do uradne trgovine Apple App Store. Zato mora biti vsaka naprava končnega uporabnika opremljena z Apple ID.

Na tej točki priporočamo, da ima vsak uporabnik svoj Apple ID.

S simbolom lahko dodate dodatne aplikacije.

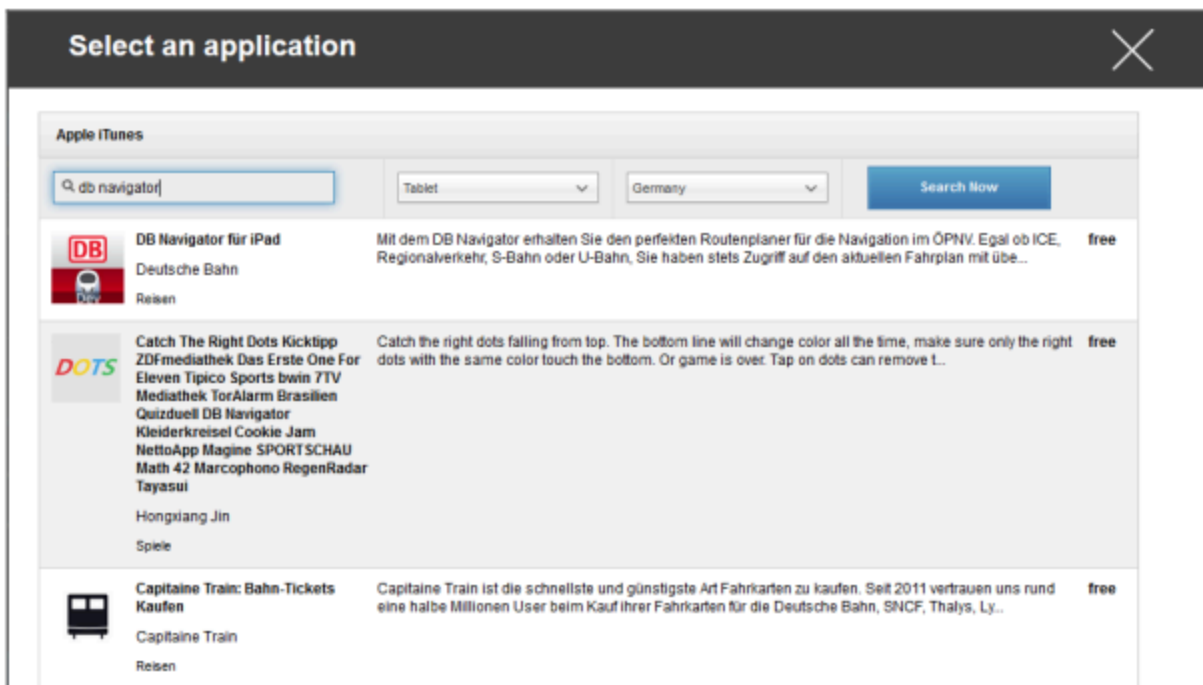


Nato se odpre okno z naslednjim pregledom.



Upoštevajte, da bodo prikazane samo brezplačne aplikacije, plačljive aplikacije bodo prikazane samo prek omrežja VPN.

Pod "Enter Search Term here ..." lahko poiščete aplikacijo, ki je v trgovini Apple App Store.



Ko kliknete ikono ali ime aplikacije, boste znova pozvani k izvedbi dodatnih konfiguracij.



Spremljajte dogajanje	Enkrat na teden bo določeno, ali je za aplikacijo na voljo posodobitev. Če je odgovor pritrdilen, bo posodobitev nameščena.
Odstranitev aplikacije ob odstranitvi profila MDM	V primeru odstranitve naprave za upravljanje bo aplikacija odstranjena.
Preprečevanje varnostnega kopiranja podatkov aplikacije	Varnostna kopija podatkov, značilnih za aplikacijo, ne bo ustvarjena.
App-VPN	Izberite povezavo VPN, ki se zažene ob odprtju aplikacije.

Po kliku na "Namesti" bo aplikacija dodana v trgovino Enterprise App Store, nato pa jo bo mogoče namestiti v napravo končnega uporabnika prek trgovine AppTec360 AppStore.

Če je bil uvoz v trgovino App-Store uspešen, boste prejeli naslednji pregled:

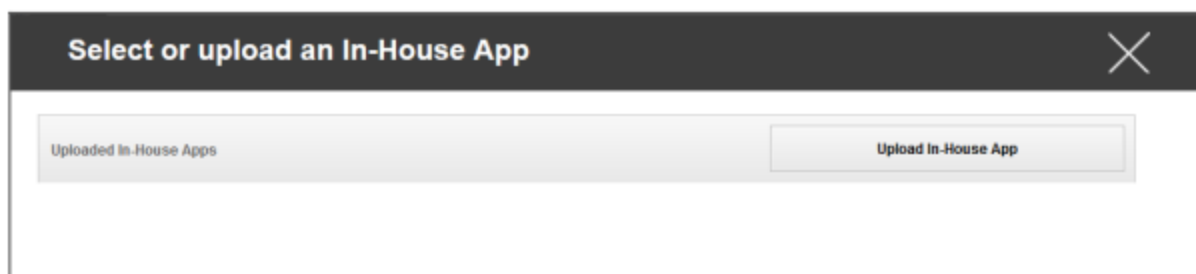


Lastna spletna stran

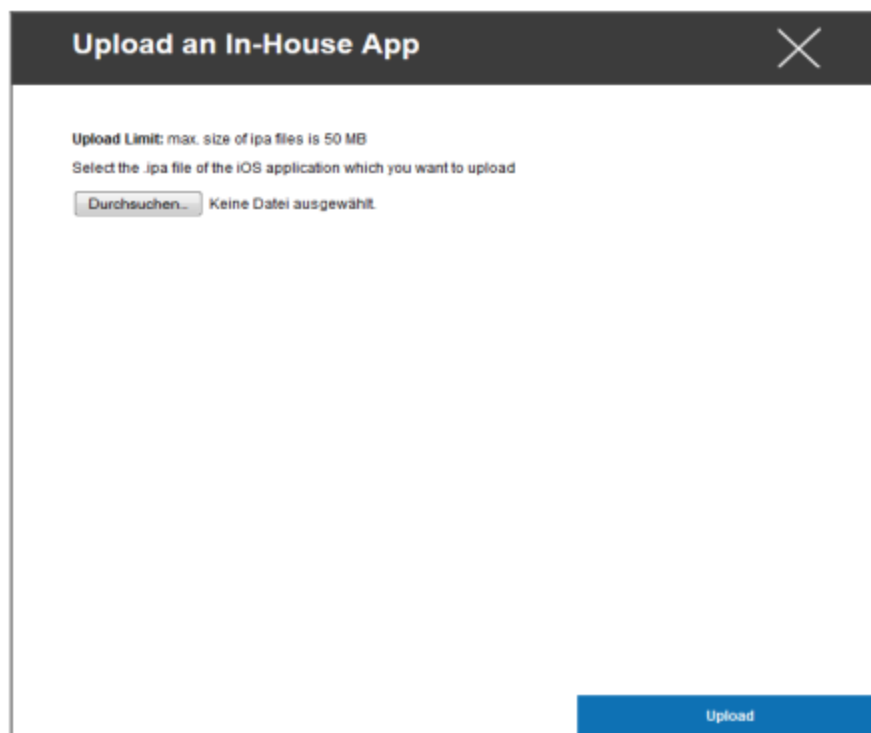
Pod točko "Lastno" lahko naložite interno razvite aplikacije in jih distribuirate.

S tem simbolom lahko distribuirate dodatne domače aplikacije.

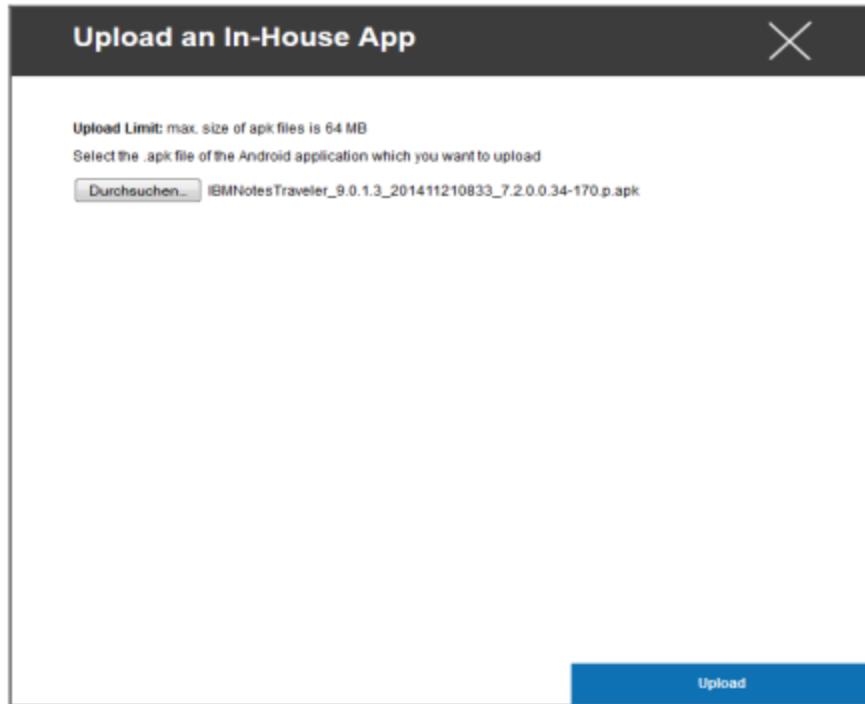
Če še nikoli niste distribuirali aplikacije In-House, boste prejeli naslednji pregled:



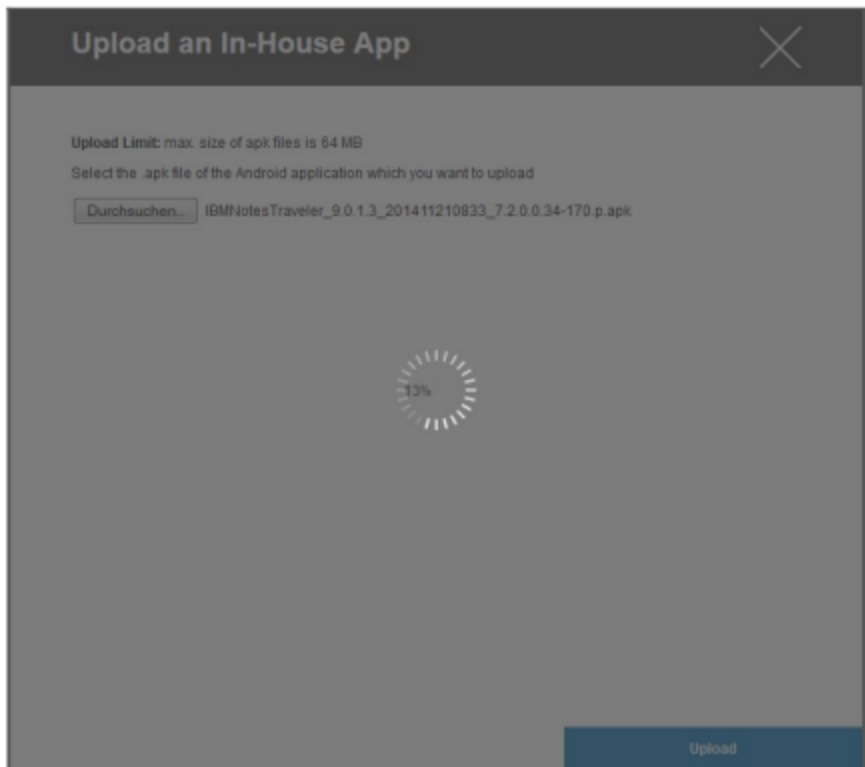
Za to kliknite "Upload In-House App", nato pa se vam bo prikazal naslednji pregled:



Zdaj z gumbom "Išči..." izberite datoteko .ipa in nato kliknite "Naloži".



Vaša aplikacija bo zdaj naložena. V sredini kroga je prikazan odstotek, koliko vaše aplikacije je bilo že naložene.



Če je bilo nalaganje domače aplikacije uspešno izvedeno, boste novo naloženo aplikacijo videli v katalogu aplikacij.

Uporabnik ima zdaj možnost videti in namestiti to aplikacijo v trgovini AppTec360 Store v napravi končnega uporabnika v kategoriji "In-House".

Ker to ne vključuje javne aplikacije Apple AppStore, uporabnik ne potrebuje shranjenega Apple ID v napravi končnega uporabnika.

Način kioska

Način Kiosk iOS je na voljo samo v nadzorovanem načinu

V načinu Kiosk lahko vnaprej določite aplikacijo ali URL, tako da bo mogoče zagnati/obiskati izključno to aplikacijo/URL.

Poleg tega lahko v načinu Kiosk deaktivirate različne strojne gumbе.

Vrsta uporabe

Paket

Če želite aplikacijo zagnati v načinu Kiosk, v razdelku "Vrsta aplikacije" izberite "Paket".

Uporaba kioska	Kliknite tukaj, da izberete aplikacijo, ki naj se zažene v načinu Kiosk. Na voljo je trenutni pregled upravljanja aplikacij Izbirate lahko med "Aplikacijami Apple iTunes" in "Lastnimi aplikacijami iOS".
----------------	--

URL

Če želite v načinu Kiosk zagnati URL, v razdelku "Vrsta aplikacije" izberite "URL".

URL	Zdaj določite želeni naslov URL
Politika enakega izvora	Če je ta funkcija aktivna, lahko uporabnik brska le po podstraneh vnaprej določenega naslova URL. Če ste na primer določili naslednji naslov URL: www.mypage.com, potem lahko uporabnik brska po www.mypage.com/subpage
URL-ji na belem seznamu	Tu lahko vzdržujete beli seznam, vsi ti URL-ji so dovoljeni. Največ 1 URL na vrstico URL se mora začeti s http:/ ali https://.
URL-ji na črnem seznamu	Tu lahko vzdržujete črni seznam, na katerem so vsi ti naslovi URL prepovedani. Največ 1 URL na vrstico URL se mora začeti s http:/ ali https://.
Počisti brskalnik po neaktivnosti	Po neaktivnosti se predpomnilnik brskalnika izprazni.
Izhodno geslo Omogočeno	Če aktivirate to funkcijo, ima uporabnik možnost, da način Kiosk zaključi z geslom, ki ste ga vnaprej določili.
Izhodno geslo	To je geslo, ki ste ga vnaprej določili.

Nastavitve načina Kiosk

Načrtovani način kioska	Glede na dnevni čas lahko nastavite način Kiosk, tako da se način samodejno začne in konča ob vnaprej določenem času.
Čas začetka	Čas začetka
Čas v minutah	Čas v minutah, po katerem se način Kiosk ponovno zaključí
Onemogoči dotik	Če je aktiviran, je zaslon na dotik deaktiviran
Onemogočite vrtenje naprave	Če je aktivirano, je samodejno prilagajanje zaslona deaktivirano.
Onemogočite stikalo za zvonjenje	Če je aktivirano, se stikalo za zvonjenje deaktivira. Od takrat je obnašanje odvisno od predhodno nastavljene funkcije
Onemogočanje gumbov za glasnost	Če je aktivirana, so gumbi za glasnost deaktivirani.
Onemogočanje gumba za budnost v spanju	Če je aktivirano, bo stikalo za vklop/izklop deaktivirano.
Onemogočanje samodejnega zaklepanja	Če je aktivirano, se naprava ne preklopi v stanje pripravljenosti.
Omogočanje funkcije prenosa govora	Če je aktiviran, se aktivira pomočnik za govorjenje z glasom.
Omogočanje povečave	Če je aktivirano, se aktivira povečava.
Omogočanje obrnjenih barv	Če je aktiviran, se aktivira način obrnjenega prikaza.
Omogočanje pomožnega dotika	Če je aktiviran, se aktivira funkcija AssistiveTouch.
Omogoči izbiro govora	Če je aktiviran, se aktivira izbira govora.
Omogočanje mono zvoka	Če je aktiviran, se aktivira monofonski zvok.
VoiceOver	Če je aktivirano, lahko uporabnik omogoči funkcijo VoiceOver
Povečanje	Če je aktivirano, lahko uporabnik omogoči funkcijo Zoom
Invertiranje barv	Če je aktivirano, lahko uporabnik omogoči obrnjene barve.
Pomožni dotik	Če je aktivirano, lahko uporabnik omogoči pomoč pri dotiku

Android Enterprise – Popolnoma upravljana konfiguracija naprav

Glede na to, ali ste trenutno izbrali profil skupine ali napravo, se pregled in njegove podtočke razlikujejo - to natančno upoštevajte!

Splošno

Pregled profila skupine (samo na ravni skupine)

Ko odprete profil skupine, dobite hiter pregled profila.

Profile Name	Default Group Profile
Operating System	Android
Created At	01.03.2021 09:52:54
Created By	John Doe
Last Change	31.08.2021 16:35:50
Changed By	John Doe
Current Profile Revision	16
Released Profile Revision (outdated)	14

Delete Profile
Reset Group Profile
Copy Profile

Ime profila	Ime profila (tukaj ga lahko spremenite)
Operacijski sistem	Operacijski sistem, za katerega je profil namenjen
Ustvarjeno na	Čas nastanka
Ustvaril je	Ustvarjalec profila
Zadnja sprememba	Čas zadnje spremembe profila
Spremenjeno s	Račun, ki je opravil zadnje spremembe
Trenutna revizija profila	Revizija stanja shranjenega profila
Objavljena revizija profila	Dodeljena revizija profila ("Assigned profile revision"). Če je za besedilom na etiketi "(zastarela)", to pomeni, da ste profil shranili, vendar ga še niste dodelili, zato bodo naprave še vedno dobile starejšo različico.

Pregled naprave (samo na ravni naprave)

Če ste v napravi, boste prejeli pregledni povzetek izbrane naprave, ki vsebuje naslednje informacije:

Ime naprave	Ime naprave
Lokacija	Koordinate lokacije
Telefonska številka	Telefonska številka
Dodeljene obvezne aplikacije	Število dodeljenih obveznih aplikacij
Različica operacijskega sistema	različica operacijskega sistema naprave
Operacijski sistem	Operacijski sistem (Android Enterprise)
Serijska številka	Serijska številka naprave
Lastništvo naprave	Poslovna ali zasebna naprava
Vrsta naprave	Upravljana naprava AE Work
Ukoreninjen	Stanje, ki označuje, ali je bila naprava zakoreninjena.
V skladu s predpisi	Skladnost s smernicami
Naslov IP	Naslov IP naprave
Nazadnje videno	Točka v času, ko je bila naprava nazadnje povezana z AppTecom
Zadnji potisk	Točka v času, ko je bil napravi poslan zadnji potisk.
Način lastnika naprave AE	Da
Dodelitev uporabnika	Uporabnik ali skupina, ki ji je ta naprava dodeljena.

Revizija konfiguracije (samo na ravni naprave)

Tu dobite pregled, kateri profil skupine je dodeljen napravi.

Revision Overview			
	Installed Profile	Assigned Profile	Last Generated Profile
Device Profile	Device Profile: Revision 5	Device Profile: Revision 5	Device Profile: Revision 5
Group Profile	Default Group Profile: Revision 13	Default Group Profile: Revision 13 (Newer Revision available)	Default Group Profile: Revision 13

Če kliknete profil skupine, boste dobili neposreden dostop do tega profila in lahko opravite nastavitve.

S tem simbolom lahko razdeljene aplikacije vrnete v nastavitve skupinskega profila.

S tem simbolom lahko vse uporabljene aplikacije vrnete v nastavitve skupinskega profila.

"Na voljo je novejša revizija" pomeni, da je bil profil skupine spremenjen in shranjen, vendar ni dodeljen. Profil skupine je treba dodeliti s funkcijo "Assign now" na ravni skupine, da se spremembe uporabijo v napravah.

Dnevnik naprave (samo na ravni naprave)

Dnevnik ukazov

Tu si lahko ogledate, kateri ukazi so bili izdani za napravo in kakšen je njihov status.

Command Log (last 250 commands)					
#	Created By	Date modified	Command	State	
1	jd@example.com	31.08.2021 12:21:37	Install assigned profiles	Device Pushed	
2	jd@example.com	31.08.2021 12:10:04	Get installed apps	Command Executed	
3	jd@example.com	31.08.2021 12:10:04	Get managed apps	Command Executed	
4	jd@example.com	31.08.2021 12:10:02	Get certificates	Command Executed	
5	jd@example.com	31.08.2021 12:10:02	Get asset data	Command Executed	
6	System Automated	31.08.2021 05:34:29	Update profile revision	Command Partially Failed !	
7	System Automated	31.08.2021 05:34:29	Apply device settings	Command Executed	
8	System Automated	31.08.2021 05:34:27	Install application	Command Failed !	
9	System Automated	31.08.2021 05:34:25	Get installed apps	Command Executed	
10	System Automated	31.08.2021 05:34:25	Get managed apps	Command Executed	
11	System Automated	31.08.2021 05:34:23	Get certificates	Command Executed	

Ukazi, ustvarjeni s "Sistemsko avtomatizirano", se samodejno ustvarijo v sistemu.

Možni statusi ukazov

Potisnjena naprava	Storitvi za potiskanje (npr. APNS) je bila poslana potisna zahteva, da se naprava poveže nazaj s strežnikom EMM.
Ustvarjen ukaz	Ukaz je bil ustvarjen v sistemu.
Poslan ukaz	Ukaz je bil napravi poslan, ko se je povezala s strežnikom.
Izveden ukaz	Ukaz je bil uspešno izveden.
Ukaz ni uspel	Ukaz ni uspel. *
Ukaz delno ni uspel	Odvisno od operacijskega sistema naprave so lahko nekateri ukazi združeni. Pri tem nekateri deli te skupine ukazov niso bili uspešni. *
Ukaz se je izvršil, vendar je bil neuspešen	Ukaz je bil izveden, vendar morda ni bil.
Ukaz se ponovno premakne	Ukaz je ponovno poslal uporabnik.
Zavrženi	Ukaz je bil zavrnjen. Na primer zato, ker ga je nadomestil drug ukaz ali ker je bila naprava ponovno vpisana in so bili stari ukazi odstranjeni.

Če je za sporočilom izklicnik, lahko več informacij dobite tako, da s kazalcem podrsate nad ikono.

Nastavitve naprave

Konfiguracija odjemalca

Tu lahko v napravi s sistemom Android izvedete naslednje konfiguracije:

Čas neskladnosti	Omejitev časovnega limita odziva uporabnika, po katerem se uporabi ukrep izvrševanja.
Izvršilni ukrepi po izteku roka za izpolnjevanje zahtev	Izvršilni ukrepi, kadar uporabnik ne izvede dejanj, ki vodijo do statusa naprave, ki je skladna s predpisi
Pogostost zbiranja podatkov	Pogostost zbiranja podatkov o napravi/GPS
Frekvenca srčnega utripa naprave	Interval, v katerem mora naprava stopiti v stik s strežnikom AppTec360 Min. 1 minuta Največ. 24 ur
Omogočanje posodobitev lokacije	Če je aktivirano, naprava pošlje posodobitve lokacije v strežnik AppTec360.
Čas posodobitve lokacije	Določa, v katerih časovnih intervalih naprava AppTec360 pošilja posodobitve lokacije.
Uporaba Googlove natančnosti lokacije za posodobitev lokacije	Če je aktivirana, se za posodobitve lokacije uporablja omrežna lokacija (če je bila ta možnost deaktivirana v razdelku "Omejitve", ta nastavitev ne bo vplivala na nič).
Uporaba lokacije GPS za posodobitev lokacije	Če je aktivirano, se za posodobitve lokacije uporablja GPS.
Dovolite navidezne (lažne) lokacije	Omogoča ponarejanje podatkov o lokaciji prek aplikacij tretjih oseb.
Ukrep za izgubljeno povezavo	Če je omogočeno, lahko določite ukrep za primer, ko naprava v intervalu srčnega utripa ne vzpostavi povezave s strežnikom MDM. Na primer, če ima naprava čas srčnega utripa 5 minut, se s strežnikom poveže ob 10:35. Nato naprava zapusti območje Wi-Fi. Naslednji srčni utrip ob 10:40 bo neuspešen, zato se bo izvedlo določeno dejanje.
Akcija	Ukrep, ki ga je treba sprejeti takoj, ko naprava postane neskladna. <ul style="list-style-type: none"> Zaklepanje naprave = naprava za zaklepanje

	<ul style="list-style-type: none"> • Brisanje naprave = naprava bo obnovljena na tovarniške nastavitve • Brisanje naprave in kartice SD = naprava bo obnovljena na tovarniške nastavitve, pomnilnik kartice SD pa bo izbrisan.
Prag	Določite lahko prag števila neuspešnih srčnih utripov, ki so potrebni za sprožitev določenega ukrepa.

Način uveljavljanja politik	Privzeto:	Uporabniki bodo občasno pozvani, naj izvedejo preostale ukrepe.
	Leno izvrševanje politik:	Uporabniki ne bodo nikoli pozvani k izvedbi neizvedenih dejanj. V odjemalcu AppTec360 bodo prikazana vsa odprta dejanja.
	Agresivno uveljavljanje politik:	Uporabniki bodo neprekinjeno pozvani k izvedbi preostalih dejanj.
Zaklepanje različice AppTec360	Če je omogočeno, lahko določite kodo različice odjemalca AppTec360 MDM. Odjemalec AppTec360 bo posodobljen samo na določeno različico. Novejše različice ne bodo upoštevane. Posodobitev na nižjo različico NI mogoča.	
Koda različice	Koda različice odjemalca AppTec360 MDM, ki jo je treba zakleniti.	
Onemogočite obvestilo AppTec360	Če je onemogočen, odjemalec AppTec360 ne bo prikazal obvestila v obvestilni vrstici. Uporabniki lahko odjemalca AppTec360 zaprejo prek upravitelja opravil. Če je odjemalec AppTec360 zaprt, več funkcij, vključno z načinom Kiosk Mode in črno/belo listo aplikacij, ne bo delovalo pravilno. Samsungove naprave ponujajo mehanizem za zaščito odjemalca AppTec360. Obvestilo je privzeto onemogočeno na napravah Samsung, ki podpirajo vmesnike API KNOX. Obvestilo ne sme biti onemogočeno v napravah z operacijskim sistemom Android 8.0 ali novejšim.	

Ozadje

Nastavitev ozadja po meri	Omogočanje/izklop ozadja po meri
Ozadje	Nastavitev načina ozadja za uporabo barvne kode ali slike
Določite barvo	določite barvo ozadja kot šestnajstiško vrednost, npr. #000000 za črno ali #ffffff za belo.
Nastavite sliko kot ozadje	Naložite slikovno datoteko, ki jo želite uporabiti kot ozadje

Upravljanje sredstev (samo na ravni naprave)

Informacije o napravi

Model	Oznaka modela naprave
Operacijski sistem	OS
Različica operacijskega sistema	Različica operacijskega sistema
Serijska številka	Serijska številka
Ime naprave	Ime naprave
Stanje baterije	Stanje baterije
Prosti / skupni pomnilnik	Prosti / skupni pomnilnik
Samsung Safe	Vmesnik Samsung SAFE, potreben za različne možnosti nastavitvev
Na voljo je kartica SD	Na voljo je kartica SD
Emulirana kartica SD	Emulirana kartica SD
Kartica SD Odstranljiva	Odstranljiva kartica SD
SD Prosti / skupni pomnilnik	SD Prosti / skupni pomnilnik kartice SD

Wi-Fi

Naslov IP	Naslov IP naprave
WiFi MAC	Naslov WiFi MAC

Cellular

Status	Stanje (nameščena kartica SIM)
Telefonska številka	Telefonska številka
Gostovanje (glasovno/podatkovno)	Gostovanje za prenos govora/podatkov
Status gostovanja	Trenutni status gostovanja
Naslov IP	Naslov IP
Operater/prevoznik	Operater/prevoznik
Celična tehnologija	Celična tehnologija
IMEI	Številka IMEI
ICCID	To je identifikacijska oznaka za kartico SIM, pogosto tudi pametno kartico ali kartico z integriranim vezjem (ICC).
IMSI	<p>Mednarodna identiteta mobilnega naročnika (IMSI) v mobilnih omrežjih GSM in UMTS zagotavlja natančno identifikacijo uporabnikov omrežja. IMSI je sestavljen iz največ 15 števil in je konfiguriran na naslednji način:</p> <ul style="list-style-type: none"> • <u>Koda mobilne države</u> (MCC), 3 števke • <u>Koda mobilnega omrežja</u> (MNC), 2 ali 3 števke • Identifikacijska številka mobilnega naročnika (MSIN), 1-10 števil
Trenutni MCC/MNC	Glejte "SIM MCC/MNC".
SIM MCC/MNC	<p>Koda mobilne države je uveljavljena identifikacijska oznaka države, ki jo je določila ITU v skladu s standardom E.212. Uporablja se skupaj s kodo mobilnega omrežja (MNC) za identifikacijo mobilnega omrežja. Pomeni kodo države/mobilnega omrežja kartice SIM.</p> <p>Če gostujete v drugem mobilnem omrežju, bosta logično "trenutni MCC/MNC" in "SIM MCC/MNC" različna.</p>

Bluetooth

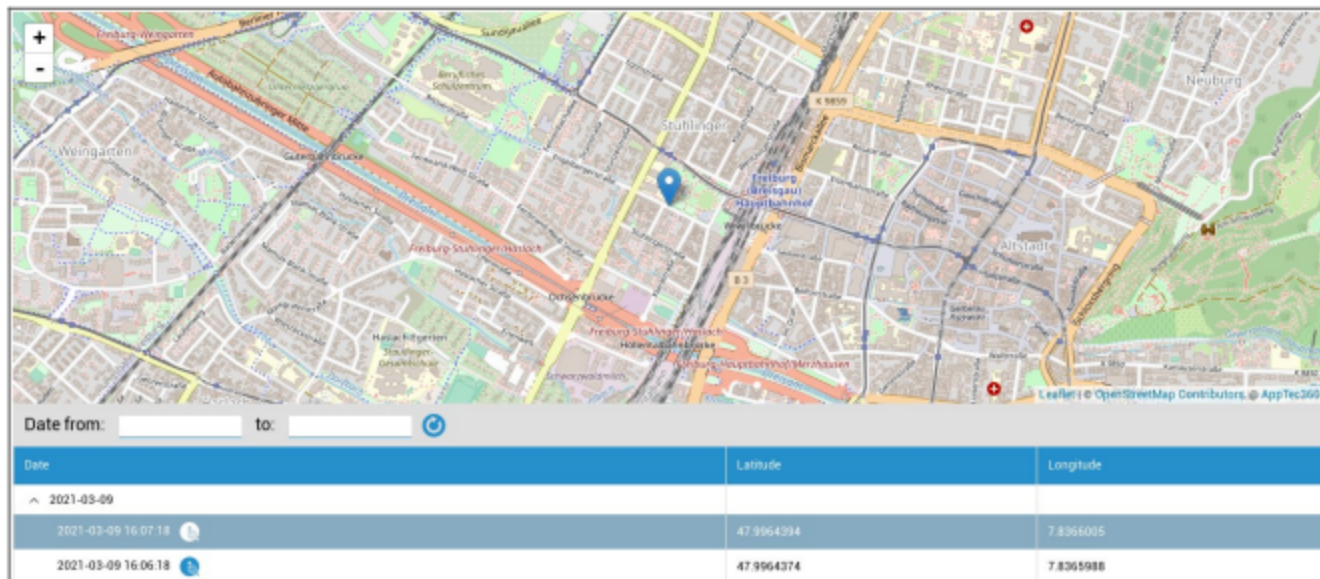
Bluetooth MAC	Naslov MAC Bluetooth
---------------	----------------------

Upravljanje varnosti

Zaščita pred krajo (samo na ravni naprave)

Informacije GPS (samo na ravni naprave)

Tu lahko določite trenutno/ zadnjo lokacijo naprave. Lokalizacijo lahko zaščitite z enim ali celo dvema gesloma - glejte: Splošne nastavitve - Zasebnost - Dostop do GPS



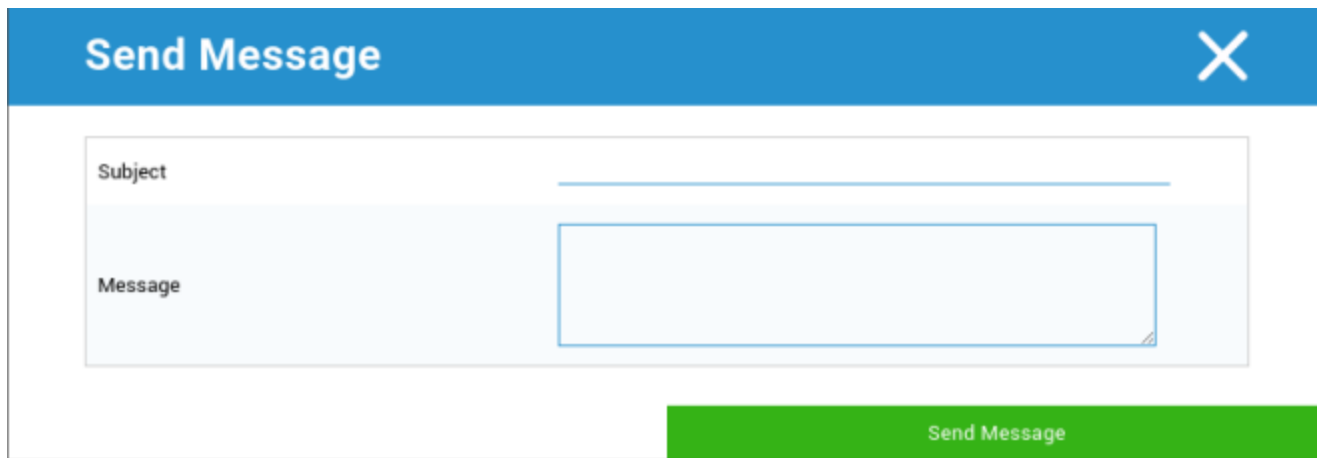
Brisanje in zaklepanje (samo na ravni naprave)

V razdelku "Brisanje in zaklepanje" lahko izvedete naslednja tri dejanja:

Celotno brisanje	Naprava je obnovljena na tovarniške nastavitve (izbrisani so tako poslovni kot osebni podatki).
Izbris podjetja	Iz naprave končnega uporabnika se odstranijo samo podatki podjetja (vse aplikacije, podatki itd., ki jih je zagotovil AppTec360)
Zaklepanje zaslona	Zaklepanje zaslona je aktivirano, napravo je treba odkleniti z geslom naprave/PIN.

Sporočilo (samo na ravni naprave)

Tu lahko izpolnite predmet in sporočilo ter ga pošljete v napravo končnega uporabnika.



The image shows a 'Send Message' dialog box. It has a blue header with the text 'Send Message' and a close button (X) in the top right corner. Below the header, there are two input fields: 'Subject' and 'Message'. The 'Subject' field is a single-line text input, and the 'Message' field is a multi-line text area. At the bottom right of the dialog, there is a green button labeled 'Send Message'.

Varnostna konfiguracija

Pristopna koda naprave

V razdelku "Geslo" lahko pooblastite geslo naprave, na voljo so naslednje možnosti nastavitvev

Najmanjša dolžina gesla	določa najmanjše število simbolov, ki jih mora imeti geslo.	
Kakovost gesla	Neopredeljeno	Ta pravilnik nima zahtev glede gesla.
	Biometrični šibki	Ta politika omogoča uporabo biometrične tehnologije prepoznavanja z nizko stopnjo varnosti. To pomeni tehnologije, ki lahko prepoznajo identiteto posameznika do približno trimestne številke PIN (napačna zaznava je manj kot 1 proti 1 000).
	Nekaj	Ta politika zahteva nastavitvev določenega gesla ali vzorca, vendar ne uveljavlja nobenih posebnih pravil.
	Abecedno	Uporabnik mora vnesti geslo, ki vsebuje vsaj abecedne znake (ali druge simbole).
	Alfanumerični	Uporabnik mora vnesti geslo, ki vsebuje vsaj dva številčna in abecedna (ali druga simbola) znaka.
	Kompleksni	Uporabnik mora vnesti geslo, ki privzeto vsebuje vsaj eno črko, številčno številko in poseben simbol. S to kakovostjo gesla lahko omejite gesla, da vsebujejo različne sklope znakov, na primer vsaj eno veliko črko itd.
Najmanjša dolžina gesla	Nastavite zahtevano število znakov za geslo. Tako lahko na primer zahtevate, da imajo gesla PIN ali gesla vsaj šest znakov.	
Najmanjše število števil v geslu	Najmanjše število števil v geslu	
Najmanjše število malih črk v geslu	Najmanjše število malih črk v geslu	
Najmanjše število velikih tiskanih črk v geslu	Najmanjše število velikih tiskanih črk v geslu	
Najmanjši zahtevani črkovni znaki v geslu	Najmanjši zahtevani črkovni znaki v geslu	

Najmanjši zahtevani simboli v geslu	Najmanjši zahtevani simboli v geslu
-------------------------------------	-------------------------------------

Zaklepanje največjega časa neaktivnosti	Največja neaktivnost uporabnika do časovne blokade
Časovna omejitev izteka gesla	vzpostavi, po tem časovnem intervalu geslo preneha veljati in je treba izdati novo geslo.
Omejitev zgodovine gesel	Število predhodno uporabljenih gesel, ki niso dovoljena
Največ neuspešnih poskusov gesla	določa, kolikokrat je mogoče napačno vnesti geslo, preden se izvede popolno brisanje naprave.
Omogočanje biometričnega preverjanja pristnosti	Omogoča preverjanje pristnosti s prstnim odtisom ali skeniranjem šarenice. Samo za Samsung KNOX 2.1 in višje.

AntiVirus

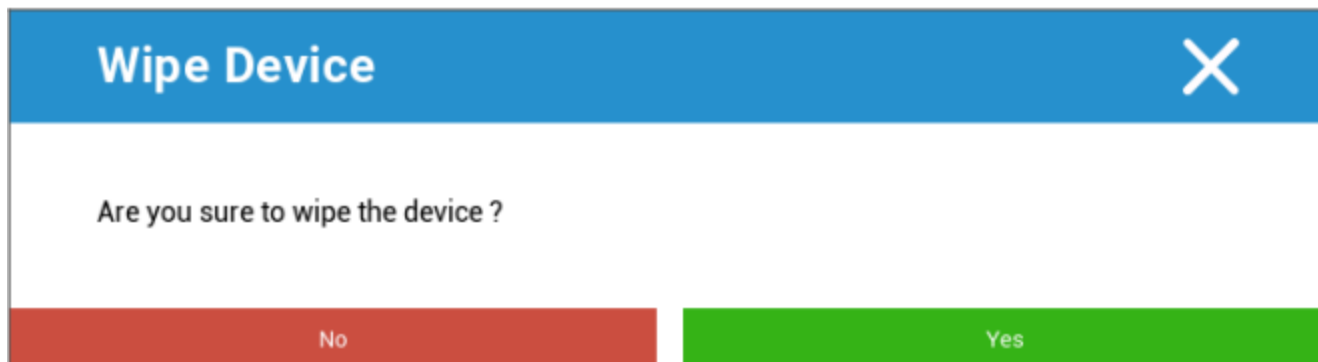
Samodejno skeniranje	Omogočite periodično samodejno pregledovanje
Interval skeniranja	Interval za pregled (hiter/celoten)
Popolno samodejno skeniranje	Omogočite popolnoma samodejno skeniranje
Samodejne posodobitve	Omogočanje samodejnih posodobitev
Interval preverjanja posodobitev	Kako pogosto je treba posodabljeni aplikaciji in njeno zbirko podatkov (virusi / poškodovana koda).
Zaščita aplikacij	Omogočanje samodejnega skeniranja aplikacij
Zaščita kartice SD	Omogočite samodejno skeniranje kartice SD
Posodobitev samo za Wi-Fi	Če je ta možnost omogočena, se posodobitve uporabijo le, ko je naprava uspešno povezana z omrežjem Wi-Fi.

Konec življenjske dobe (samo na ravni naprave)

Brisanje (samo na ravni naprave)

V razdelku "Brisanje" lahko obnovite tovarniške nastavitve naprave. Pri tem bodo v napravi končnega uporabnika izbrisani tako poslovni kot zasebni podatki.

S klikom na simbol Minus prejmete naslednje sporočilo:



Z "Da" lahko izvedete brisanje.

V razdelku "Poročilo o brisanju" lahko prikažete naslednje elemente

Izbrisano z	Zgodovina izvajalca brisanja
Datum	Datum
Status	Status (npr. če je bilo brisanje uspešno izvedeno)

Nastavitve omejitev

Omejitve

Tu lahko omejite in blokirate različne stvari.

Omogoči kamero	Dovolite uporabo fotoaparata	
Izvršite samodejno sinhronizacijo	Na spletni strani	Sinhronizacija je trajno aktivirana
	Izklopljeno	Sinhronizacija je trajno deaktivirana
	Izbira uporabnika	Izbere uporabnik
Sila Bluetooth	Na spletni strani	Bluetooth je trajno aktiviran
	Izklopljeno	Bluetooth je trajno deaktiviran
	Izbira uporabnika	Izbere uporabnik
Sila GPS	Na spletni strani	GPS je trajno aktiviran
	Izklopljeno	GPS je trajno deaktiviran
	Izbira uporabnika	Izbere uporabnik
Lokacija omrežja sil	Na spletni strani	Trajno internetno lociranje
	Izklopljeno	Trajna deaktivacija internetnega lociranja
	Izbira uporabnika	Izbere uporabnik

Varnost		
Prepovedati skupno rabo Lokacija	Določa, ali je uporabniku prepovedano vklopiti skupno rabo lokacije.	
Prepoved varnega zagona	Določa, ali uporabnik ne sme ponovno zagnati naprave v varni zagonski način.	
Prepoved ponastavitve omrežja	Določa, ali je uporabniku onemogočeno ponastavljanje omrežnih nastavitev iz Nastavitev.	
Prepoved ponastavitve tovarniških nastavitev	Določa, ali je uporabniku prepovedana ponastavitev naprave.	
Omogočanje ADB	Omogoča povezavo z računalnikom prek ADB	
Onemogočanje varovala ključev	Onemogoči varovanje ključev	
Lastnik naprave Informacije o zaklenjenem zaslonu	Nastavitev informacij o lastniku naprave, ki se prikažejo na zaklenjenem zaslonu.	
Izvrševanje skladnosti	Način poziv Uporabnik	Uporabnik bo pozvan, da izvede potrebna dejanja.
	Zabojnik za zaklepanje načina	Skrijte vse aplikacije, dokler niso izpolnjene vse zahteve.

Upravljanje aplikacij	
Omogočanje povezovanja aplikacij med profili	Aplikacijam v nadrejenem profilu omogoča, da obdelujejo spletne povezave iz upravljanega profila.
Prepovedati nadzor aplikacij	Določa, ali je uporabniku prepovedano spreminjanje aplikacij v nastavitvah ali zaganjalnikih.
Prepoved namestitve aplikacije	Določa, ali je uporabniku onemogočeno nameščanje aplikacij.
Onemogočanje odstranitve aplikacij	Določa, ali je uporabniku onemogočeno odstranjevanje aplikacij.
Pravilnik o dovoljenjih za izvajanje	Določa, kako bodo obravnavane nove zahteve za dovoljenja iz aplikacij.
Dovolite neznane vire	Če je ta možnost omogočena, lahko uporabniki z namestitvijo datoteke .apk prenesejo aplikacije na drugo stran.

Povezljivost	
Prepoved konfiguracije mobilnega omrežja	Določa, ali je uporabniku prepovedano konfiguriranje mobilnih omrežij.
Konfiguracija prepovedi privezovanja	Določa, ali je uporabniku prepovedano konfigurirati Tethering in prenosne dostopne točke.
Prepovedati konfiguracijo VPN	Določa, ali je uporabniku onemogočeno konfiguriranje omrežja VPN.
Prepovedati konfiguracijo Wifi	Določa, ali je uporabniku onemogočeno spreminjanje dostopnih točk WiFi.
Prepovedati odhodni žarek NFC	Določa, ali uporabnik ne sme uporabljati NFC za prenos podatkov iz aplikacij.
Zaklepanje konfiguracije WiFi	Ta nastavitev določa, ali naj bodo konfiguracije WiFi, ki jih ustvari aplikacija lastnika naprave, zaklenjene (to pomeni, da jih lahko ureja ali odstrani samo aplikacija lastnika naprave, ne pa tudi aplikacija Nastavitve).
Omogočanje podatkovnega gostovanja	Aktivacija podatkovnega gostovanja

Bluetooth	
Prepovedati Bluetooth	Določa, ali je bluetooth v napravi prepovedan. Zahteva operacijski sistem Android 8.0
Prepoved souporabe Bluetooth	Določa, ali je v napravi onemogočena odhodna souporaba bluetooth. Zahteva operacijski sistem Android 8.0
Prepovedati konfiguracijo Bluetooth	Določa, ali je uporabniku prepovedano konfigurirati bluetooth.

Upravljanje računa	
Prepoved dodajanja upravljanega profila	Določa, ali je uporabniku prepovedano dodajanje upravljanih profilov. Zahteva Android 8.0
Prepoved dodajanja uporabnikov	Določa, ali je uporabniku prepovedano dodajanje novih uporabnikov.
Prepoved Odstranitev upravljanega profila	Določa, ali je mogoče upravljane profile tega uporabnika odstraniti, razen če jih odstrani lastnik profila. Zahteva Android 8.0
Prepoved spreminjanja računa	Določa, ali je uporabniku prepovedano dodajanje in odstranjevanje računov, razen če jih programsko doda Authenticator.

Telefonija	
Prepoved odhodnih klicev	Določa, da uporabniku ni dovoljeno opravljati odhodnih telefonskih klicev.
Prepovedati sporočila SMS	Določa, da uporabnik ne sme pošiljati ali prejemati sporočil SMS.

Sistem	
Prepoved ustvarjanja oken	Določa, da se okna poleg oken aplikacije ne smejo ustvariti.
Prepovedati nastavitve ikone uporabnika	Določa, ali uporabnik ne sme spreminjati svoje ikone.
Prepoved nastavitve ozadja	Omejitev uporabnika, ki onemogoča nastavitve ozadja.
Onemogočite vrstico stanja	Onemogočanje vrstice stanja blokira obvestila, hitre nastavitve in druge prekrivne zaslone, ki omogočajo pobeg iz naprave za enkratno uporabo.
Omogoči samodejni čas	Samodejno nastavi čas.
Omogočanje samodejnega časovnega pasu	Samodejno nastavi časovno območje.
Ostanite vklopljeni, ko ste priključeni v električno omrežje	Naprava ostane aktivna, ko je priključena na vir napajanja.

Shranjevanje	
Onemogočanje onemogočanja preverjanja aplikacij	Določa, ali je uporabniku prepovedano onemogočiti preverjanje aplikacij.
Prepoved priklopa fizičnega medija	Določa, ali je uporabniku onemogočeno nameščanje fizičnih zunanjih medijev.
Omogočite storitev varnostnega kopiranja	Storitev varnostnega kopiranja upravlja vse mehanizme varnostnega kopiranja in obnovitve v napravi. Če to nastavite na false, preprečite varnostno kopiranje ali obnovitev podatkov. Storitev varnostnega kopiranja je privzeto izklopljena. Zahteva operacijski sistem Android 8.0
Omogočite masovni pomnilnik USB	Omogoča uporabo masovnega pomnilnika USB.

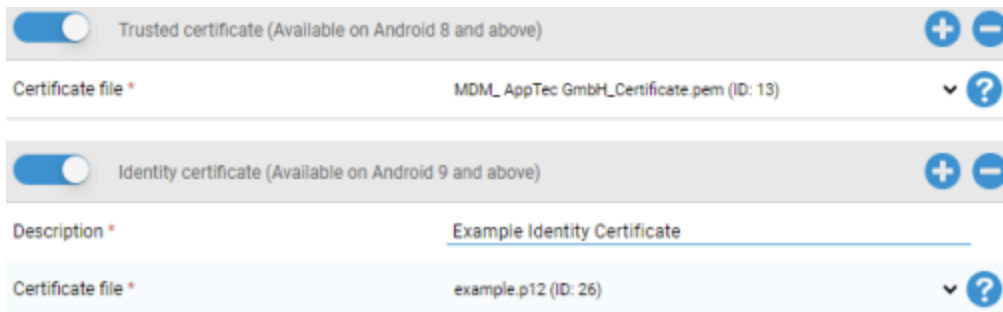
Tipkovnica	
Prepovedati samodejno izpolnjevanje	Določa, ali uporabnik ne sme uporabljati storitev samodejnega izpolnjevanja. Zahteva Android 8.0
Prepoved kopiranja in lepljenja med profili	Določa, ali je mogoče kopirano v odložišče tega profila prilepiti v povezane profile.

Zvok	
Prepoved prilagoditve obsega	Določa, ali je uporabniku prepovedano prilagajanje glavne glasnosti.
Prepoved izklopa mikrofona	Določa, ali je uporabniku onemogočeno prilagajanje glasnosti mikrofona.
Naprava za utišanje zvoka	Naprava za utišanje zvoka.

Upravljanje certifikatov

Tu lahko napravam razdelite zaupanja vredna potrdila in potrdila o identiteti.

Za distribucijo zaupanja vrednih potrdil je potreben operacijski sistem Android 8 ali novejši, za distribucijo identitetnih potrdil pa operacijski sistem Android 9 ali novejši.



The screenshot displays two sections for certificate management. The first section, titled "Trusted certificate (Available on Android 8 and above)", has a toggle switch turned on. Below it, the "Certificate file" field is set to "MDM_AppTec GmbH_Certificate.pem (ID: 13)". The second section, titled "Identity certificate (Available on Android 9 and above)", also has a toggle switch turned on. Below it, the "Description" field is set to "Example Identity Certificate" and the "Certificate file" field is set to "example.p12 (ID: 26)". Both sections include plus and minus icons for adding or removing certificates, and a question mark icon for help.

Z znakom "+" lahko dodate več potrdil.

Zaupanja vredna potrdila morajo biti v formatu PEM.

Potrdila o istovetnosti morajo biti v formatu PKCS12.

Upravljanje povezav

Wifi

Za to nastavitve izvedite predhodno konfiguracijo naprav končnega uporabnika za dostop do notranjih točk dostopa

Identifikator nabora storitev (SSID)	SSID za omrežje, ki ga želite povezati
Skrito omrežje	Aktiviraj, če AP ne oddaja SSID.

Vrsta varnosti

Določite varnostno vrsto AP

WEP

Geslo	Geslo za AP
-------	-------------

WPA/WPA2

Geslo	Geslo za AP
-------	-------------

802.1x EAP

Metoda EAP

PWD	Identiteta	Identiteta
	Geslo	Geslo

PEAP	Protokol preverjanja pristnosti v fazi 2	ni	Brez dodatnega protokola
		MSCHAPV2	Protokol MSCHAPV2
		GTC	Protokol GTC
	Potrdilo CA	Potrdilo CA	
	Identiteta	Identiteta	
	Anonimna identiteta	Anonimna identiteta	
	Geslo	Geslo	

TTLS	Protokol preverjanja pristnosti v fazi 2	ni	Brez dodatnega protokola
		PAP	Protokol PAP
		MSCHAP	Protokol MSCHAP
		MSCHAPV2	Protokol MSCHAPV2
		GTC	Protokol GTC
	Potrdilo CA	Potrdilo CA	
	Identiteta	Identiteta	
Anonimna identiteta	Anonimna identiteta		
Geslo	Geslo		

TLS	Potrdilo CA	Potrdilo CA
	Identiteta	Identiteta
	Geslo	Geslo

VPN

Ime povezave	Ime povezave VPN
--------------	------------------

Vrsta VPN

VPN

Odjemalec VPN

Odjemalec AppTec360 VPN	
Konfiguracija vrat	Izberite konfiguracijo VPN na prehodu (glejte Splošne nastavitve > Univerzalni prehod > Nastavitve VPN).
Vedno vklopljen VPN	Omogočanje funkcije Native Lockdown
Omogočite zaklepanje aplikacije AppTec360	Omogočite zaklepanje aplikacije AppTec360

Vgrajeno (na voljo samo v napravah Samsung)			
Vrsta povezave	PPTP	Strežnik	Strežnik
		Omogočanje šifriranja PPTP	Omogočanje šifriranja PPTP
	L2TP / IPsec PSK	Strežnik	Strežnik
		Predhodni zaupni ključ IPsec	Predhodni zaupni ključ IPsec
		Omogočite L2TP Secret	Omogočite L2TP Secret
		Skrivnost L2TP	Skrivnost L2TP
	IPsec XAuth PSK	Strežnik	Strežnik
		Identifikator IPsec	Identifikator IPsec
		Predhodni zaupni ključ IPsec	Predhodni zaupni ključ IPsec
	DNS Iskanje domen	DNS Iskanje domen	
Strokovne nastavitve	Strežniki DNS	Strežniki DNS	
	Usmeritve za posredovanje	Usmeritve za posredovanje	

Odprto omrežje VPN		
Strežnik	Strežnik	
Profil OpenVPN	Profil OpenVPN	
Aplikacija OpenVPN	OpenVPN za Android (priporočljivo)	
	Povezava OpenVPN	
Strokovne nastavitve	Strežniki DNS	Strežniki DNS
	Usmeritve za posredovanje	Usmeritve za posredovanje

Samsung / Strong Swan			
Vrsta povezave	PPTP	Strežnik	Strežnik
		Uporabniško ime	Uporabniško ime
		Geslo	Geslo
		Omogočanje šifriranja PPTP	Omogočanje šifriranja PPTP
	L2TP / IPsec PSK	Strežnik	Strežnik
		Predhodni zaupni ključ IPsec	Predhodni zaupni ključ IPsec
		Uporabniško ime	Uporabniško ime
		Geslo	Geslo
		Omogočite L2TP Secret	Skrivnost L2TP
	IPsec XAuth PSK	Strežnik	Strežnik
		Identifikator IPsec	Identifikator IPsec
		Predhodni zaupni ključ IPsec	Predhodni zaupni ključ IPsec
		Uporabniško ime	Uporabniško ime
		Geslo	Geslo
	Strokovne nastavitve	Strežniki DNS	Strežniki DNS
Usmeritve za posredovanje		Usmeritve za posredovanje	

Cisco Any Connect		
Strežnik	Strežnik	
Način potrdila	Onemogočeno	Onemogočeno
	Samodejno	Samodejno
Strokovne nastavitve	Strežniki DNS	Strežniki DNS
	Usmeritve za posredovanje	Usmeritve za posredovanje

VPN za posamezno aplikacijo

Odjemalec VPN

Odjemalec AppTec360 VPN		
Konfiguracija vrat	Izberite konfiguracijo VPN na prehodu (glejte Splošne nastavitve > Univerzalni prehod > Nastavitve VPN).	
Aplikacije VPN	Aplikacije VPN	
Vedno vklopljen VPN	Omogočanje funkcije Native Lockdown	Vedno vklopljen VPN
Omogočite zaklepanje aplikacije AppTec360	Omogočite zaklepanje aplikacije AppTec360	

Samsung / Strong Swan			
Vrsta povezave	PPTP	Strežnik	Strežnik
		Aplikacije VPN	Aplikacije VPN
		Uporabniško ime	Uporabniško ime
		Geslo	Geslo
		Omogočanje šifriranja PPTP	Omogočanje šifriranja PPTP
	L2TP / IPsec PSK	Strežnik	Strežnik
		Aplikacije VPN	Aplikacije VPN
		Predhodni zaupni ključ IPsec	Predhodni zaupni ključ IPsec
		Uporabniško ime	Uporabniško ime
		Geslo	Geslo
		Omogočite L2TP Secret	Skrivnost L2TP
	IPsec XAuth PSK	Strežnik	Strežnik
		Aplikacije VPN	Aplikacije VPN
		Identifikator IPsec	Identifikator IPsec
		Predhodni zaupni ključ IPsec	Predhodni zaupni ključ IPsec
		Uporabniško ime	Uporabniško ime
		Geslo	Geslo
Strokovne nastavitve	Strežniki DNS	Strežniki DNS	
	Usmeritve za posredovanje	Usmeritve za posredovanje	

Omejitve

Tu lahko nastavite omejitve v zvezi z upravljanjem povezave.

Omogočanje podatkovnega gostovanja	Omogočanje mobilnih podatkov med gostovanjem
Prisiliti podatkovno gostovanje	Če je aktivirano, je gostovanje za mobilne podatke trajno aktivirano (ni priporočljivo!) Ta nastavev prepíše nastavev "Dovoli podatkovno gostovanje"!
Naslednje nastavitve so na voljo samo v sistemu SAFE 2.x ali novejšem	
Dovolite samo klice v sili	Dovolite samo klice v sili
Omogočanje omrežja WiFi	Omogočanje omrežja WiFi
Najnižja stopnja varnosti omrežja WiFi	Najnižja stopnja varnosti omrežja WiFi Odprto = dovoljene so vse vrste brezžičnega interneta.
Prepoved dodajanja omrežij WiFi uporabniku	Uporabnik ne sme sam dodati omrežja WiFi. Ta nastavev je mogoča le, če je bil profil WiFi opredeljen v razdelku "Upravljanje povezav".
Dovolite sporočila SMS in MMS	Vse = dovoljen je ves promet SMS in MMS Samo dohodna sporočila SMS = dovoljena so samo dohodna sporočila SMS Samo odhodna sporočila SMS = dovoljena so samo odhodna sporočila SMS Ni = promet SMS/ MMS ni dovoljen.
Dovolite sinhronizacijo med gostovanjem	Dovolite sinhronizacijo med gostovanjem Vklopljeno = aktivirano Izklopljeno = deaktivirano Izbira uporabnika = izbira uporabnika
Omogočanje glasovnega gostovanja	Omogočanje glasovnega gostovanja Vklopljeno = aktivirano Izklopljeno = deaktivirano Izbira uporabnika = izbira uporabnika
Uporaba sistemskega strežnika http Proxy Server	Uporaba posredniškega strežnika HTTP, ki je na voljo v nastavitvah sistema, je odvisna od povezanega omrežja (WiFi ali APN).

Upravljanje PIM

Gmail Exchange

Informacije: Ta konfiguracija bo uporabljena za aplikacijo Gmail. Zato morate odobriti in namestiti aplikacijo Gmail.

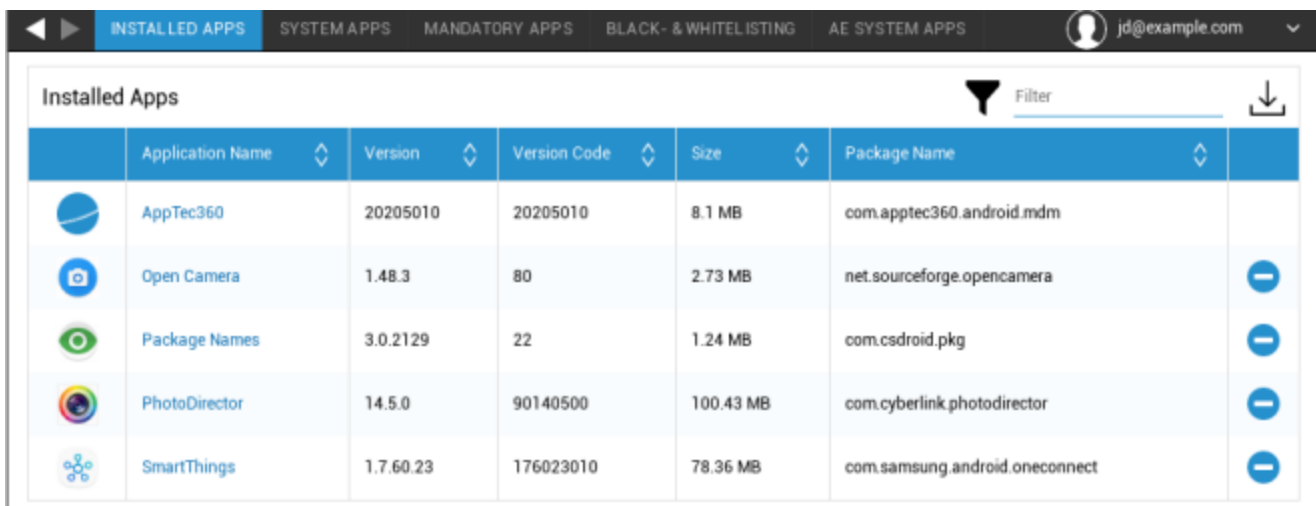
E-poštni naslov	e-poštni naslov uporabnika Upoštevajte "Namestnike", ki jih lahko uporabite za delo s poverilnicami in ne izvajate sprememb ročno v vsaki napravi. S klikom jih lahko prikažete sami
Gostiteljsko ime strežnika	Strežniški naslov strežnikov Exchange
Prijavno ime	Prijavno ime za zadevno napravo končnega uporabnika, upoštevajte tudi "Namestna imena tukaj".
Podpis	Priložite lahko podpis (namig: nekatere naprave zahtevajo oblikovanje HTML za podpis).
Število prejšnjih dni za sinhronizacijo	Število dni, ki določajo, kdaj se e-poštna sporočila sinhronizirajo nazaj
Identifikator naprave	Ein String der die EAS DeviceID enthält. Dies ist Teil des EAS Protokolls und wird in einigen Umgebungen benötigt
Uporabite Secure Sockets Layer (SSL)	Uporaba povezave SSL
Sprejmite vsa potrdila	Sprejemajo se vsa potrdila. Izberite to možnost, če vaš strežnik Exchange uporablja samopodpisano potrdilo.

Upravljanje aplikacij










Upravitelj aplikacij za podjetja

Nameščene aplikacije (samo na ravni naprave)

Tu so prikazane vse aplikacije, ki so trenutno nameščene v napravi končnega uporabnika.

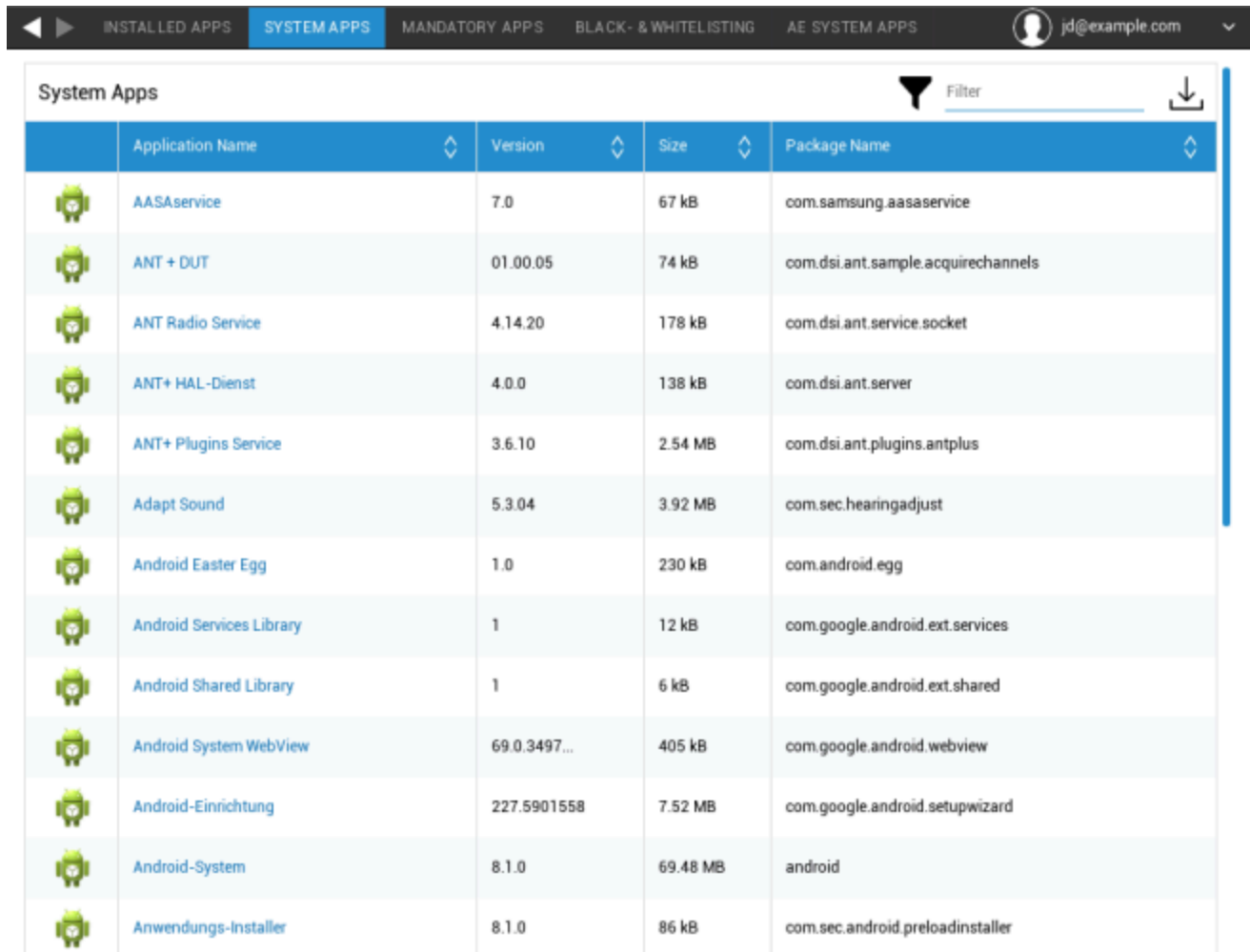















The screenshot shows the 'Installed Apps' section of the AppTec360 management console. At the top, there are navigation tabs: 'INSTALLED APPS' (selected), 'SYSTEM APPS', 'MANDATORY APPS', 'BLACK- & WHITELISTING', and 'AE SYSTEM APPS'. A user profile icon for 'jd@example.com' is visible in the top right. Below the tabs, there is a table of installed applications with columns for Application Name, Version, Version Code, Size, and Package Name. Each row also includes a small icon and a minus sign in the right margin. A search filter and a download icon are located at the top right of the table area.

	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	

Sistemske aplikacije (samo na ravni naprave)

V razdelku "Sistemske aplikacije" so navedene vse aplikacije in storitve, ki jih je proizvajalec naprave že namestil v napravo končnega uporabnika.



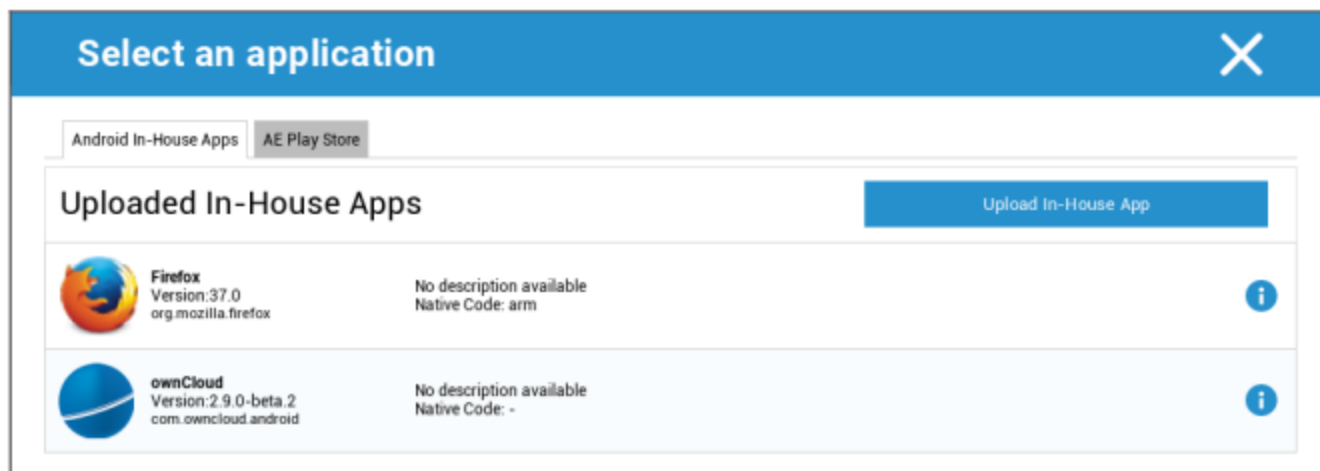
	Application Name	Version	Size	Package Name
	AASAservice	7.0	67 kB	com.samsung.aasaservice
	ANT + DUT	01.00.05	74 kB	com.dsi.ant.sample.acquirechannels
	ANT Radio Service	4.14.20	178 kB	com.dsi.ant.service.socket
	ANT+ HAL-Dienst	4.0.0	138 kB	com.dsi.ant.server
	ANT+ Plugins Service	3.6.10	2.54 MB	com.dsi.ant.plugins.antplus
	Adapt Sound	5.3.04	3.92 MB	com.sec.hearingadjust
	Android Easter Egg	1.0	230 kB	com.android.egg
	Android Services Library	1	12 kB	com.google.android.ext.services
	Android Shared Library	1	6 kB	com.google.android.ext.shared
	Android System WebView	69.0.3497...	405 kB	com.google.android.webview
	Android-Einrichtung	227.5901558	7.52 MB	com.google.android.setupwizard
	Android-System	8.1.0	69.48 MB	android
	Anwendungs-Installer	8.1.0	86 kB	com.sec.android.preloadinstaller

Obvezne aplikacije

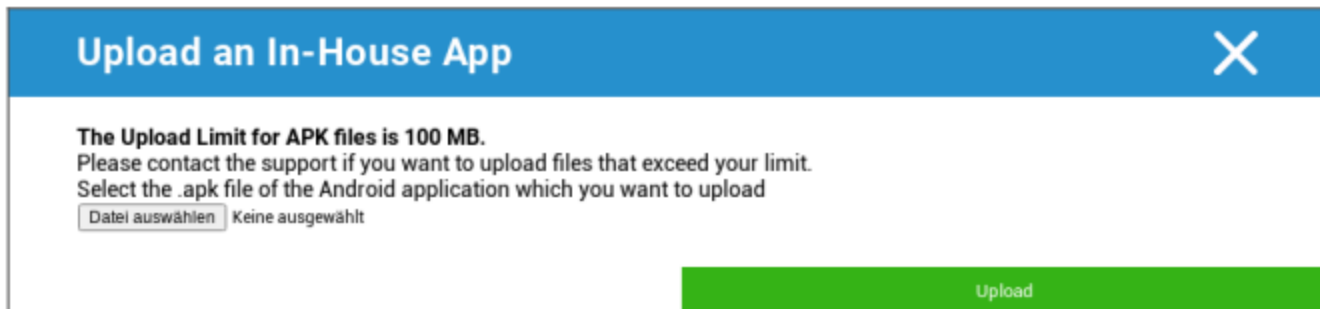
V razdelku Obvezne aplikacije lahko določite obvezne zahtevane aplikacije. Uporabnik bo nenehno pozvan k namestitvi te določene aplikacije.

Prek , je mogoče opredeliti predpisano zahtevano aplikacijo.

To je lahko domača aplikacija iz seznama "Androidove domače aplikacije", ki ste jo naložili v splošnih nastavitvah.

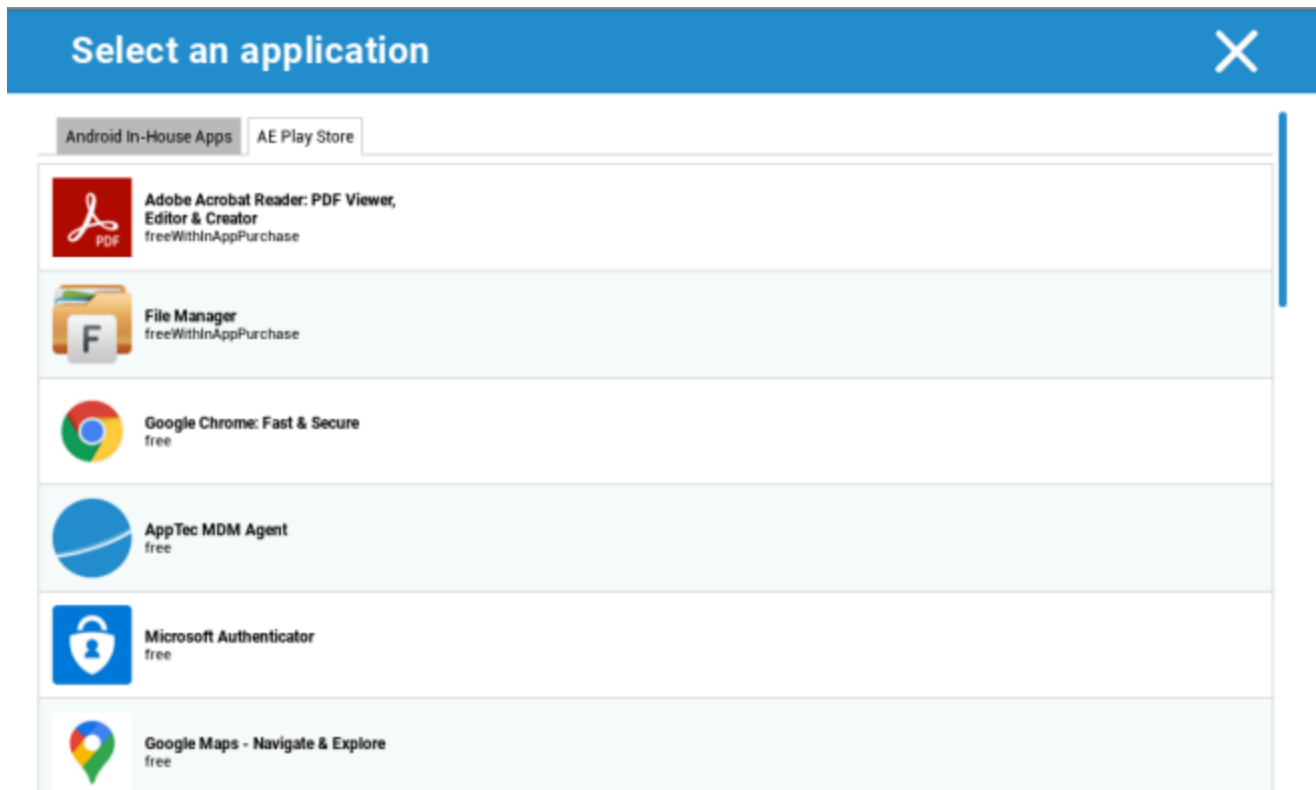


Datoteko apk lahko izberete in naložite tudi neposredno z "Naložite domačo aplikacijo".



Če nameščate aplikacijo v hiši, lahko aktivirate možnost "Posodobljanje". Če je ta možnost aktivirana in ste v DB domače aplikacije določili novejšo različico, bo aplikacija posodobljena v napravi.

Lahko pa je aplikacija "AE Play Store" iz trgovine Google Work Play Store.



V tem zavihku bodo prikazane samo odobrene aplikacije "AE Play Store Apps".

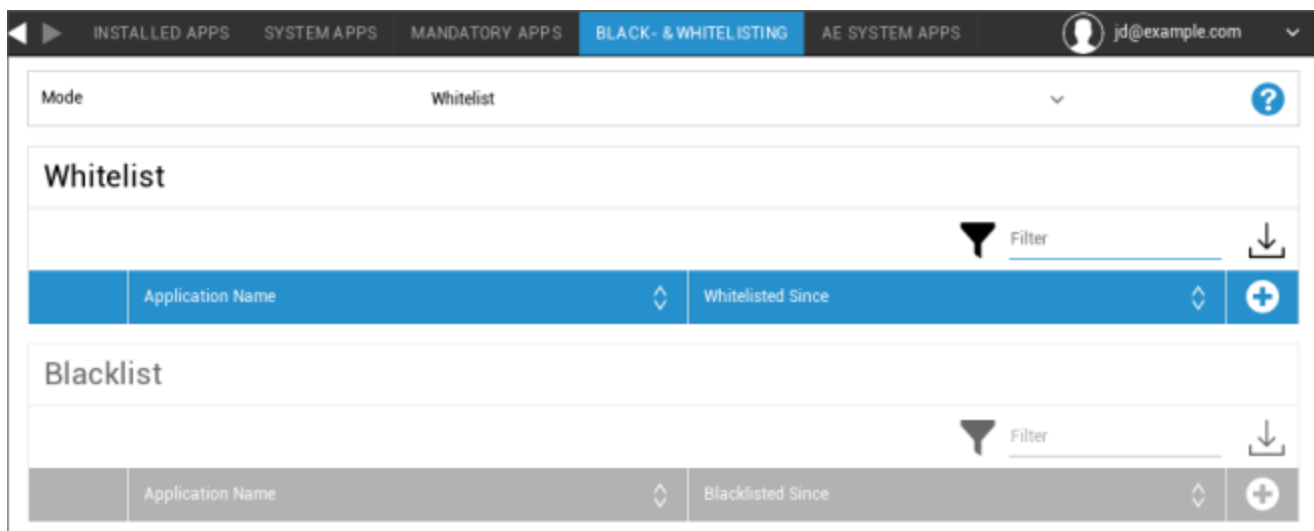
Če želite odobriti aplikacijo "AE Play Store App", pojdite v "Splošne nastavitve" > "Upravljanje aplikacij" > "AE Play

Trgovina" in dodajte aplikacijo z gumbom, ki vas bo preusmeril na zavihek "Aplikacije v trgovini Play" (ali pa lahko neposredno odprete zavihek "Aplikacije v trgovini Play").

V zavihku "Aplikacije v trgovini Play" lahko iščete aplikacije. Ko kliknete aplikacijo, se odpre stran z aplikacijo, kjer lahko aplikacijo odobrite s klikom na "Approve".

Črna in bela lista

V razdelku "Črna in bela lista" lahko izbirate med načinom "Bela lista" in načinom "Črna lista".



Bela lista	V napravo končnega uporabnika je mogoče namestiti samo aplikacije in storitve, ki so dodane na seznam. Če so te že predhodno nameščene v napravi končnega uporabnika, bodo aktivirane in nastavljene tako, da jih bo uporabnik lahko zagnal.
	Vseh drugih aplikacij, ki niso dodane na seznam, ni mogoče namestiti v napravo končnega uporabnika. Če so te aplikacije že predhodno nameščene v napravi končnega uporabnika, bodo deaktivirane in nastavljene tako, da jih uporabnik ne bo mogel zagnati.
Črni seznam	Aplikacij in storitev, ki so dodane na seznam, ni mogoče namestiti v napravo končnega uporabnika. Če so te že predhodno nameščene v napravi končnega uporabnika, bodo deaktivirane in nastavljene tako, da jih uporabnik ne bo mogel zagnati.
	Vse druge aplikacije, ki niso dodane na seznam, je mogoče namestiti v napravo končnega uporabnika. Če so te že predhodno nameščene v napravi končnega uporabnika, bodo aktivirane in nastavljene tako, da jih bo uporabnik lahko zagnal.

Prek gumba , dodate dodatne aplikacije ali storitve na trenutno uporabljeni seznam.

Prek gumba , dodate dodatne aplikacije ali storitve na trenutno neaktivni seznam.

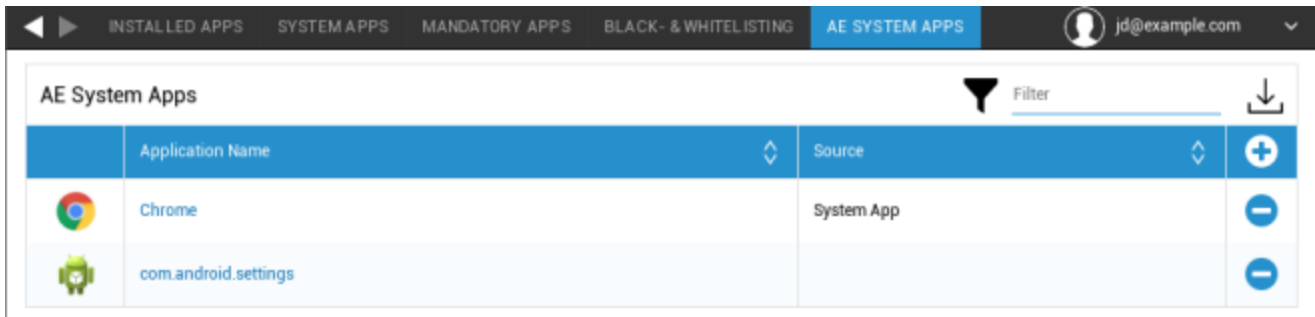
Določite lahko "Packagename":

Select an application ✕

Package Name

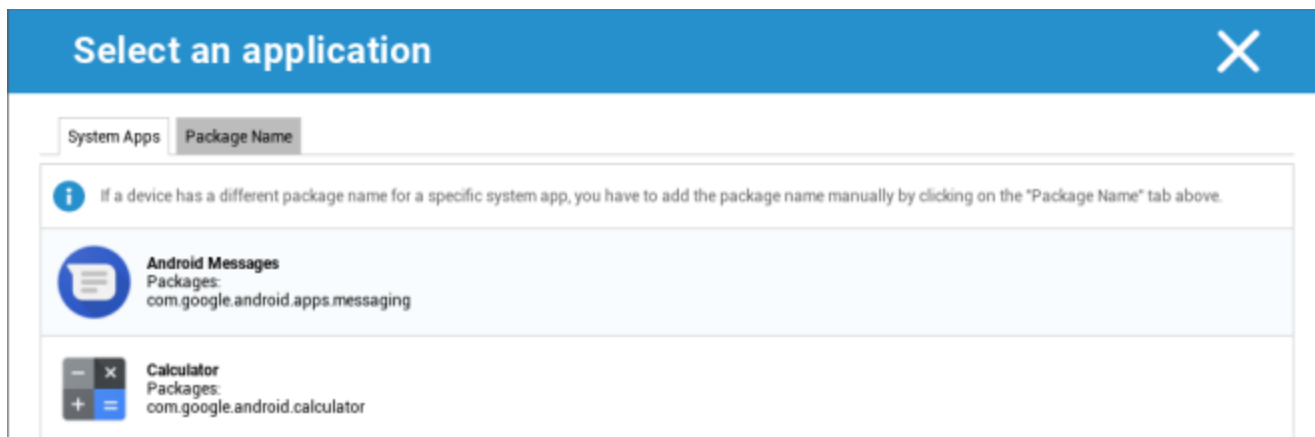
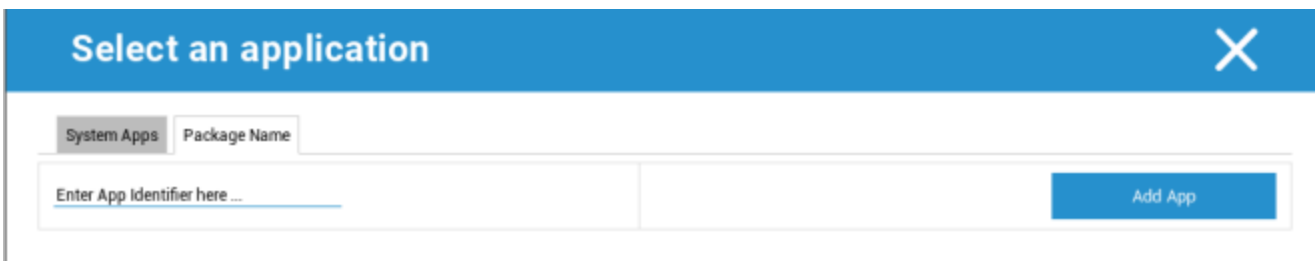
Aplikacije sistema AE

Tu lahko določite seznam, ki vsebuje določene sistemske aplikacije, ki jih je treba aktivirati v napravah.



Application Name	Source	
Chrome	System App	+ -
com.android.settings		-

Če kliknete gumb, lahko izberete s seznama možnih sistemskih aplikacij, ki ga zagotovi Google, ali neposredno vnesete ime paketa sistemske aplikacije, ki jo je treba aktivirati.

Ne pozabite, da so sistemske aplikacije na seznamu, ki ga je pripravil Google, le aplikacije, ki so lahko sistemske, vendar ni nujno, da so sistemske aplikacije v vaših napravah.

Vendar ta seznam zadeva le aplikacije, ki so že vnaprej nameščene.

Dodajanje aplikacij, ki niso vnaprej nameščene v napravah, ne bo vplivalo na naprave, ne glede na to, ali je aplikacija s seznama, ki ga zagotovi Google, ali pa je ime paketa aplikacije vneseno neposredno.

Omejitve in nastavitve

Nastavitve upravljanja aplikacij

Tu lahko nastavite obnašanje naprave glede posodobitev aplikacij.

Pogostost preverjanja posodobitev	Določite, v katerem intervalu bo odjemalec AppTec360 iskal posodobitve aplikacije. Privzeta vrednost je 24 ur.
Prag Wi-Fi	Aplikacije, ki so večje od določene velikosti, bodo prenesene prek omrežja Wi-Fi. Če je izbrana možnost "Samo Wi-Fi", bodo vse aplikacije prenesene prek omrežja Wi-Fi.

Trgovina z aplikacijami za podjetja

Lastna spletna stran

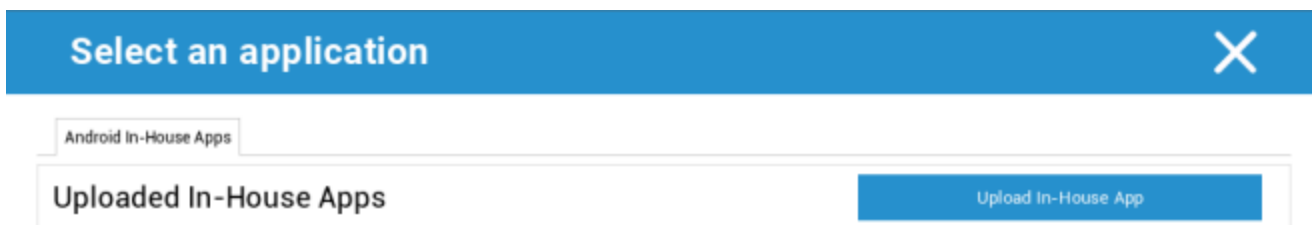
Pod točko "Lastno" lahko naložite in distribuirate interno razvite aplikacije.

S tem simbolom lahko distribuirate dodatne domače aplikacije.

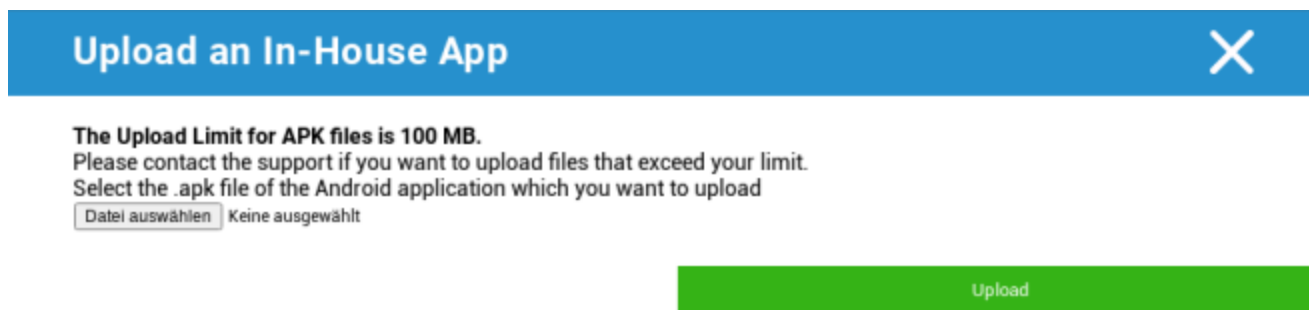
Če nameščate aplikacijo v podjetju, lahko aktivirate možnost "Posodobi". Če je to aktivirano in ste v DB domače aplikacije določili novejšo različico, bo aplikacija v napravi posodobljena.



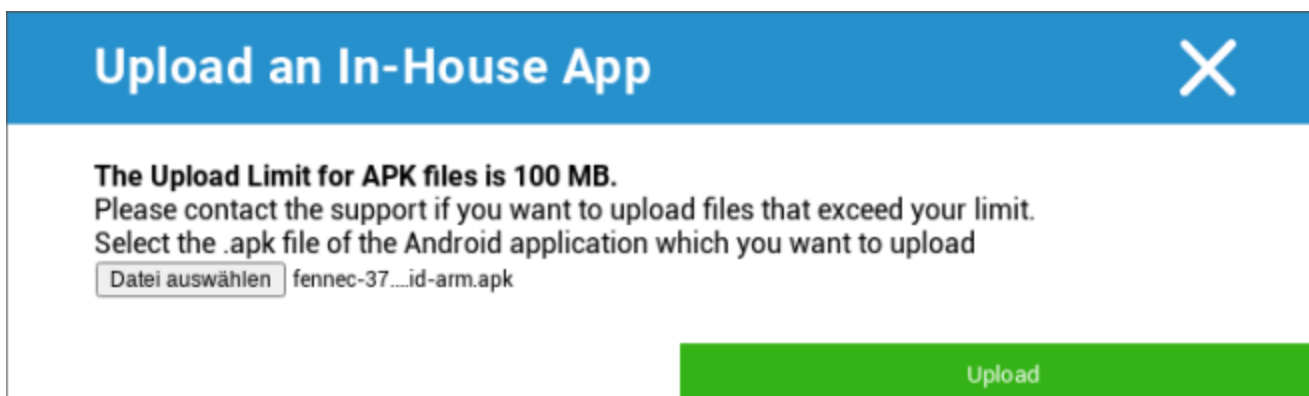
Če niste razdelili aplikacij znotraj podjetja, boste prejeli naslednji pregled:



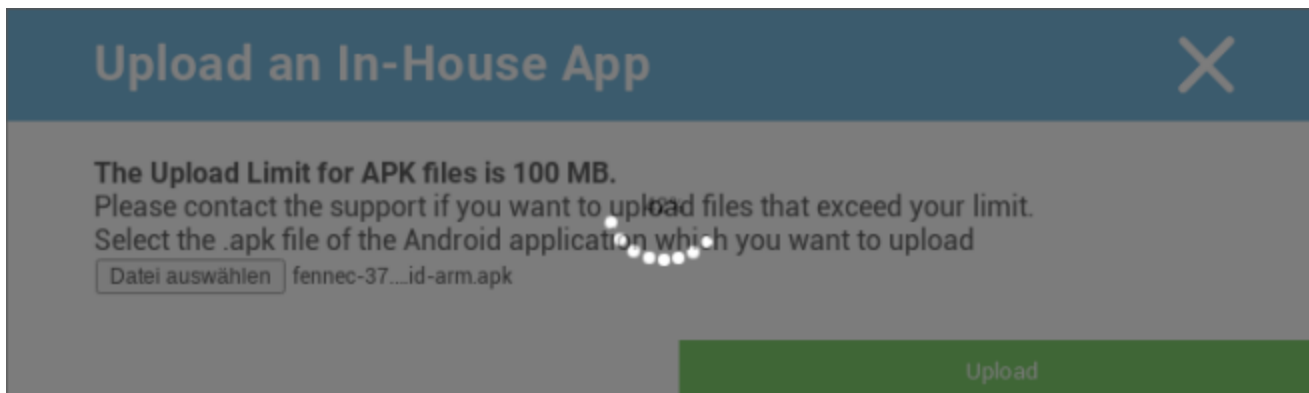
V ta namen kliknite "Upload In-House App", nato pa se vam bo prikazal naslednji pregled:



Zdaj z "Išči..." izberite datoteko .apk in nato kliknite na "Naloži".



Vaša aplikacija bo zdaj naložena, v sredini kroga pa bo prikazan kazalnik odstotka, ki prikazuje, kolikšen del vaše aplikacije je bil že naložen.



Če je bilo nalaganje vaše domače aplikacije uspešno, lahko naloženo aplikacijo najdete na spletnem mestu v katalogu aplikacij.

Uporabnik ima zdaj možnost videti in namestiti to aplikacijo v trgovini AppTec360 Store v napravi končnega uporabnika v kategoriji "In-House".



In-House						Filter	↓
	Application Name	Version	Native Code	Size	Package Name	+	
	Firefox	37.0	arm	28.67 MB	org.mozilla.firefox	-	

Ker to ne vključuje aplikacije Google PlayStore, uporabnik ne potrebuje shranjenega Googlovega ID v svoji napravi končnega uporabnika.

Trgovina Play za podjetja

Trgovina AE Play

Tu lahko dodate aplikacije v trgovino Android Enterprise Playstore. Upoštevajte, da morate pred dodajanjem aplikacij odobriti Apps z računom upravitelja AE, preden jih lahko dodate.

Za odobritev aplikacije glejte navodila v razdelku Obvezne aplikacije.

Način Kiosk in zaganjalnik

Način kioska

V načinu Kiosk lahko vnaprej določite aplikacijo ali naslov URL. Nato bo mogoče izključno zagnati/obiskati to aplikacijo ali URL.

Prav tako lahko različne strojne gumbе deaktivirate v načinu Kiosk Mode.

Samodejni zagon	Samodejno zažene način Kiosk, takoj ko profil doseže napravo končnega uporabnika.
Načrtovani način kioska?	Načrtujete lahko čas za način Kiosk, ki se bo nato samodejno začel in končal ob času, ki ga določite vi.
Čas začetka	Čas začetka
Čas v minutah	Čas v minutah, po katerem se mora način Kiosk ponovno končati

Vrsta uporabe

Posamezna aplikacija	Če želite aplikacijo zagnati v načinu Kiosk, v razdelku "Vrsta aplikacije" izberite možnost Paket.
Uporaba kioska	Kliknite tukaj, da izberete aplikacijo, ki naj se zažene v načinu Kiosk. Našli boste običajen pregled upravljanja aplikacij. Izbirate lahko med "Google Play Store", "Android In-House Apps" in "Packagename".

Vrsta uporabe

URL	Če želite v načinu Kiosk zagnati URL, v razdelku "Vrsta aplikacije" izberite "URL". Nato določite želeni naslov URL
Izbriši brskalnik po neaktivnosti	Tu lahko določite časovni interval v minutah, po katerem naj se način Kiosk ponovno zažene.
Izbriši spletni predpomnilnik in piškotke	Če aktivirate to funkcijo, se po ponovnem zagonu načina Kiosk izbriše spletni predpomnilnik (piškotki in slike v predpomnilniku).
Politika enakega izvora	Če je ta funkcija aktivna, lahko uporabnik brska le po podstraneh določenega naslova URL. Na primer, določili ste naslednji URL: www.mypage.com Potem lahko uporabnik brska po: www.mypage.com/subpage
URL-ji na belem seznamu	Tu lahko vzdržujete beli seznam, na katerem so dovoljeni vsi ti naslovi URL. Največ 1 URL na vrstico URL se mora začeti s http:/ ali https://.
URL-ji na črnem seznamu	Tu lahko vzdržujete črni seznam, vsi ti naslovi URL niso dovoljeni. Največ 1 URL na vrstico URL se mora začeti s http:/ ali https://.
Usmeritev zaslona	Ta nastavitvev se nanaša na prilagoditve zaslona Samodejno = samodejno Portret = navpični format Pokrajina = krajinski način

Več aplikacij	Če izberete način "Multi App" Kiosk Mode, se bo uveljavila uporaba zaganjalnika AppTec360.
Aplikacije	Uporaba: Kot aplikacijo za kiosk izberite aplikacijo iz trgovine Playstore ali lastno aplikacijo. Možno je vnesti tudi ime paketa. Izbrana aplikacija Kiosk Application mora biti nameščena v napravi. Ne pozabite nastaviti, da je aplikacija Kiosk Application obvezna. Bližnjica na domačem zaslonu: Če je nastavljeno na "Vklopljeno", se ustvari bližnjica na domačem zaslonu. Če je nastavljena na "Izklopljeno", se bo aplikacija še vedno prikazovala na seznamu aplikacij.

Izhodno geslo Omogočeno	Če aktivirate to funkcijo, lahko uporabnik z geslom, ki ste ga vnaprej določili, zaključí način Kiosk.
Izhodno geslo	To je geslo, ki ste ga vnaprej določili.
Samodejno zvišanje vrstice stanja	Če je omogočeno, se vrstica stanja samodejno obkroži. S to možnostjo lahko uporabniki vidijo informacije v vrstici stanja, vendar ne morejo dostopati do njenih funkcij.
Onemogočite vrstico stanja	Vrstica stanja vsebuje obvestila, bližnjice in informacije. Na voljo samo za naprave Samsung s programom SAFE 4.0 ali novejšim.
Onemogočanje tipk za glasnost	Onemogočite tipke za glasnost (na voljo samo v Samsungovih napravah s programom SAFE 3.0 ali novejšim)
Onemogočite stikalo za vklop/izklop	Onemogočite stikalo za vklop/izklop (na voljo samo v Samsungovih napravah s programom SAFE 3.0 ali novejšim)
Onemogočanje gumba Domov	Onemogočite gumb Domov. Če je ta funkcija aktivirana, lahko način Kiosk prekinete samo v konzoli AppTec360. (na voljo samo v Samsungovih napravah s programom SAFE 3.0 ali novejšim)
Onemogočite navigacijsko vrstico	S tem lahko onemogočite navigacijsko vrstico (Nazaj / Meni). Če je ta funkcija aktivirana, lahko način Kiosk prekinete samo v konzoli AppTec360. (na voljo samo v Samsungovih napravah s programom SAFE 3.0 ali novejšim)

AppTec360 zaganjalnik

Omogočite zaganjalnik AppTec360	Na: Vklopi zaganjalnik AppTec360. Uporabnik ga mora enkrat nastaviti kot privzeti zaganjalnik. Opomba: Če je omogočen način Kiosk in je način Kiosk nastavljen na "Multi App", se bo uporabil zaganjalnik AppTec360.
Velike ikone	Na: Prikaže večjo različico ikon aplikacij v zaganjalniku
Skrivanje ikone aplikacije AppTec360	Na: Aplikacijo AppTec360 popolnoma skrije
Skrivanje ikone trgovine AppTec360	Na: AppTec360 Enterprise AppStore se popolnoma skrije.

Nastavitve AppTec360

Omogočite aplikacijo AppTec360 Settings	Aplikacija AppTec360 Settings omogoča nadzor nad povezavami WiFi in Bluetooth
Omogočanje nastavitve v več aplikacijah Način kioska	Če je omogočeno, lahko uporabniki dostopajo do aplikacije AppTec360 Settings, ko je aktiven način Multi App Kiosk Mode.

Daljinski upravljalnik

Splashtop

Za začetek seje daljinskega upravljanja za vašo napravo je treba v napravo namestiti aplikacijo "Splashtop Streamer" tako, da jo dodate v **Upravljanje aplikacij** → **Upravitelj aplikacij za podjetja** → **Obvezne aplikacije**.

Nato konfigurirajte naslednje nastavitve za Splashtop:

Omogočite storitev Splashtop	Če je to omogočeno, AppTec360 konfigurira aplikacijo Splashtop tako, da omogoča oddaljeni nadzor
Namestitev kode	Pojdite na https://my.splashtop.com in se prijavite v svoj račun Splashtop. Kliknite "Dodaj računalnik" in s strani, ki se odpre, kopirajte 12-mestno kodo za namestitev.
Nastavitev Vrata za namestitev po meri?	Namestitev prehoda
Namestitev domene / gostitelja vrat	Namestitev prehoda
Preverjanje potrdila	Preverjanje potrdila

Nato lahko uporabite možnost Splashtop Remote Control v kontekstnem meniju (zobnik poleg iskalne vrstice, ko je naprava izbrana, ali desni klik na napravo v drevesu) za začetek seje daljinskega upravljanja.

TeamViewer

Če želite začeti sejo daljinskega upravljanja za svojo napravo, morate v napravo namestiti aplikacijo "TeamViewer QuickSupport" tako, da jo dodate v **Upravljanje aplikacij** → **Upravitelj aplikacij za podjetja** → **Obvezne aplikacije**.

Nato lahko z možnostjo **TeamViewer Remote Control** v kontekstnem meniju (zobnik poleg iskalne vrstice, ko je naprava izbrana, ali desni klik na napravo v drevesu) zaženete sejo daljinskega upravljanja.

Upravljanje vsebine

Vsebinsko polje

Tu lahko aktivirate vsebinsko polje.

Takoј ko preklopite možnost "Omogoči ContentBox" na "Vklopljeno", se v napravo končnega uporabnika samodejno namesti ločena aplikacija ContentBox

Varen brskalnik

Tukaj lahko konfigurirate nastavitve za varni brskalnik AppTec360.

Takoj ko preklopite razdelek v "Varnem brskalniku" na "Vklopljeno", se v napravo končnega uporabnika samodejno namesti ločena aplikacija za brskalnik

Zahtevati geslo	Od uporabnika zahtevajte, da nastavi in uporablja geslo za dostop do brskalnika.
Najmanjša zahtevana dolžina gesla	Nastavitev zahtevanega števila znakov za geslo
Zahtevana kakovost gesla	Nastavite zahtevano kakovost gesla
Omejitev prenosov / Odprite v	
Omejitev nalaganja	
Prenos bele liste	Seznam naslovov URL, za katere bo nalaganje vedno dovoljeno.
Dovoli kopiranje	Omogočite kopiranje, rezanje ali deljenje besedila na spletnih straneh.
Omogočite zajem zaslona	Omogočite zajemanje posnetkov zaslona.
Pogostost čiščenja podatkov	Izberite, s kakšno pogostostjo naj se samodejno odstranijo VSI uporabniški podatki (zgodovina, predpomnilnik itd.).
Zaznamki podjetja	Zaznamki bodo prikazani v mapi "Company bookmarks" (zaznamki podjetja) v zaznamkih brskalnikov. Uporabnik jih ne more urejati.
Skrij naslovno vrstico	
Bela lista v brskalniku (brez univerzalnega prehoda)	Omogoča beli seznam URL-jev na strani odjemalca. <ul style="list-style-type: none"> • Zaznamki podjetja so vedno uvrščeni na beli seznam • Podprto samo za 100 naslovov URL • Uporabite univerzalni prehod za neomejeno črno in belo listo
URL-ji na belem seznamu	Seznam dovoljenih naslovov URL.
Črni in beli seznam na podlagi prehodov	Za uvrstitev na črni seznam veljajo naslednje zahteve: <ul style="list-style-type: none"> • Delujoča univerzalna vrata AppTec360 ("Splošne nastavitve" → "Univerzalna vrata")

- Delujoča konfiguracija VPN z določenim strežnikom DNS ("Splošne nastavitve" → "Univerzalni prehod" → "Nastavitve VPN")
- Konfiguracija črne liste ("Splošne nastavitve" → "Universal Gateway" → "Domain Blacklist")
- Veljavna povezava VPN v profilu ("Upravljanje povezav" → "VPN")

Dodatni API

Samsung KNOX

Omejitve

Dovolite kartico SD	
Dovolite zapis na kartico SD	
Omogočite zajem zaslona	
Omogočite uporabo odložišča	
Varnostno kopiranje nastavitvev in podatkov aplikacije v Google Cloud	
Obnovitev nastavitvev iz Googlovega oblaka pri ponovni namestitvi aplikacije	
Omogočanje razhroščevanja USB	
Dovolite poročilo o trku Google	
Dovolite ponastavitev tovarniške nastavitve	
Omogočanje nadgradnje OTA	
Omogočanje shranjevanja v gostitelja USB	Če je ta možnost omogočena, lahko uporabnik poveže katerikoli pogon pisala (prenosni pomnilnik USB), zunanji trdi disk ali bralnik kartic Secure Digital (SD), ki se v napravi namesti kot pomnilniški pogon.
Dovolite predvajalnik medijev USB (MTP, PTP)	
Dovolite mikrofona	Onemogočanje mikrofona za aplikacije tretjih oseb
Omogočite NFC (Near Field Communication)	
Dovolite neznane vire (Sideloading APK)	Če je omogočeno, je stransko nalaganje aplikacij (datotek APK) dovoljeno. Ko je ta nastavev onemogočena, jo mora uporabnik omogočiti ročno, ko ponovno dovolite namestitev datotek APK iz neznanih

	virov.
Omogočanje ustvarjanja uporabnikov	Če je omogočeno, lahko uporabnik v napravi ustvari več računov, npr. račune za goste.

E-pošta

E-poštni naslov	
Protokol dohodnega strežnika	
Naslov dohodnega strežnika	
Vhodna vrata strežnika	
Prijavno/uporabniško ime dohodnega strežnika	
Geslo dohodnega strežnika	
Dohodni strežnik uporablja SSL	
Dohodni strežnik uporablja TLS	
Dohodni strežnik sprejme vsa potrdila	
Protokol odhodnega strežnika	
Naslov odhodnega strežnika	
Odhodna vrata strežnika	
Odhodni strežnik uporablja dodatne poverilnice	Če je to onemogočeno, sistem uporablja dohodne poverilnice tudi za odhodni strežnik.
Prijava/uporabniško ime odhodnega strežnika	
Geslo za odhodni strežnik	
Odhodni strežnik uporablja SSL	
Odhodni strežnik uporablja TLS	
Odhodni strežnik sprejme vsa potrdila	
Nastavite podpis	
Podpis	Opomba: Pri nekaterih napravah je treba podpis navesti v obliki HTML.
Obveščanje uporabnika o prejemu nove e-pošte	

Izmenjava

E-poštni naslov	
Gostiteljsko ime strežnika	Ime gostitelja strežnika Exchange
Prijavno ime	Uporabniško ime, ki se uporablja za prijavo v strežnik Exchange
Domena	Če je omogočena konfiguracija vrat ACL in polje Domain ni prazno, bo AppTec360 Universal Gateway avtenticiral napravo z naslednjim imenom "Domain\Login Name"
Geslo	
Število prejšnjih dni za sinhronizacijo	
Pogostost sinhronizacije elektronske pošte	
Sinhronizacija med gostovanjem	
Nastavite podpis	
Podpis	Opomba: Pri nekaterih napravah je treba podpis navesti v obliki HTML.
Privzeti račun	
Uporabite Secure Sockets Layer (SSL)	
Uporaba protokola TLS (Transport Layer Security)	
Sprejmite vsa potrdila	

APN

Prikazno ime APN	
Ime dostopne točke	Ime APN
Protokol odhodnega strežnika	
MCC - koda mobilne države	Pustite prazno, če želite uporabiti mmc nameščene kartice SIM
MNC - koda mobilnega omrežja	Pustite prazno, če želite uporabiti mnc nameščene kartice SIM
Naslov strežnika	
Številka vrat strežnika	
Naslov strežnika proxy	
Naslov strežnika MMS	Pustite prazno za privzeto
Številka vrat MMS	Pustite prazno za privzeto
Naslov posredniškega strežnika MMS	Pustite prazno za privzeto
Uporabniško ime	
Geslo	
Vrsta dostopne točke	Sprejete vrste so "default", "mms", "supl".
	Če je posredovan nič ali prazen, se privzeto uporabi "default,supl,mms".
	Pustite prazno kot privzeto.
Prednostna APN	

Bluetooth

Omogočanje odkrivanja naprave prek povezave Bluetooth	
Omogočanje seznanjanja prek povezave Bluetooth	
Dovolite naprave s slušalkami Bluetooth	
Omogočanje naprav za prostoročno telefoniranje Bluetooth	
Dovolite naprave Bluetooth A2DP	A2DP, Advanced Audio Distribution Profile, omogoča pretakanje zvoka med napravami.
Dovolite odhodne klice	
Omogočanje prenosa podatkov prek povezave Bluetooth	
Omogočanje povezovanja prek povezave Bluetooth	
Omogočanje povezave z računalnikom prek povezave Bluetooth	

Povezava

Dovolite samo klice v sili Dovolite Wi-Fi	
Najnižja stopnja varnosti omrežja Wi-Fi	
Prepoved dodajanja omrežij Wi-Fi uporabniku	To omejitev lahko aktivirate le, če je v Upravljanju povezav opredeljen vsaj en aktiven profil Wi-Fi.
Dovolite sporočila SMS in MMS	
Dovolite sinhronizacijo med gostovanjem	
Omogočanje glasovnega gostovanja	

Android Enterprise – Popolnoma upravljana naprava z delovnim profilom (COPE)

Splošna razlaga COPE

COPE je kratica za **Corporate Owned Personally Enabled**(osebno omogočeno v lasti podjetja).

Način COPE omogoča, da se naprava Android vpiše kot **naprava Android Enterprise - popolnoma upravljana naprava** z integriranim profilom **Android Enterprise - Container**.

To je lahko naprava Android, ki je že vpisana kot **naprava Android Enterprise - Popolnoma upravljana naprava** in na kateri je dodatno nastavljeno **ohišje Android Enterprise - Container**, ali novo vpisana naprava Android, ki je neposredno vpisana kot **naprava Android Enterprise - Popolnoma upravljana naprava** skupaj z **ohišjem Android Enterprise - Container** na njej.

Način COPE je na voljo samo za naprave z operacijskim sistemom Android 8, 9 in 10.

Konfiguracija profilov za naprave COPE

Ker za sam način COPE ni profila konfiguracije, je konfiguracija **Android Enterprise - popolnoma upravljana naprava** in **Android Enterprise - zabojnik** ločena na dva profila znotraj profila COPE. Med profiloma je mogoče preklapljati za konfiguracijo posameznega profila s klikom na ustrezen gumb na levi strani konzole:



Oba profila lahko konfigurirate, kot je opisano za vsak profil posebej:

Android Enterprise - Popolnoma upravljana naprava

Android Enterprise - Kontejner

Vrnitev na popolnoma upravljano napravo AE

Profil **Android Enterprise - Container** lahko odstranite, kot je opisano v poglavju **Upravljanje mobilnih naprav**.

Z odstranitvijo profila Container bo profil COPE spremenjen v profil **Android Enterprise - popolnoma upravljana naprava**.

Android Enterprise – Konfiguracija zabojnika

Glede na to, ali ste trenutno izbrali profil skupine ali napravo, se pregled in njegove podtočke razlikujejo - to natančno upoštevajte!

Splošno

Pregled profila (samo na ravni profila)

Če se nahajate v profilu, boste prejeli kratek pregled profila glede imena, operacijskega sistema, datuma ustvarjanja, avtorja itd.

Ime profila	Ime profila - tukaj ga lahko neposredno preimenujete
Operacijski sistem	Veljavni operacijski sistem za profil
Ustvarjeno na	Datum ustvarjanja
Ustvaril je	Ustvaril ga je
Zadnja sprememba	Datum zadnje spremembe
Spremenjeno s	Uporabnik, ki je opravil zadnje spremembe tega profila.
Trenutna revizija profila	Kolikokrat je bil profil že posodobljen
Objavljena revizija profila	Kolikokrat je bil profil že posodobljen in so mu bile dodeljene naprave.

Brisanje profila	Brisanje profila
Ponastavitev profila skupine	Ponastavitev profila skupine
Kopiranje profila	Kopiranje profila

Pregled profila skupine (samo na ravni skupine)

Ko odprete profil skupine, dobite hiter pregled profila.

Profile Name	Default Group Profile
Operating System	Android
Created At	01.03.2021 09:52:54
Created By	John Doe
Last Change	31.08.2021 16:35:50
Changed By	John Doe
Current Profile Revision	16
Released Profile Revision (outdated)	14

Delete Profile
Reset Group Profile
Copy Profile

Ime profila	Ime profila (tukaj ga lahko spremenite)
Operacijski sistem	Operacijski sistem, za katerega je profil namenjen
Ustvarjeno na	Čas nastanka
Ustvaril je	Ustvarjalec profila
Zadnja sprememba	Čas zadnje spremembe profila
Spremenjeno s	Račun, ki je opravil zadnje spremembe
Trenutna revizija profila	Revizija stanja shranjenega profila
Objavljena revizija profila	Dodeljena revizija profila ("Assigned profile revision"). Če je za besedilom na etiketi "(zastarela)", to pomeni, da ste profil shranili, vendar ga še niste dodelili, zato bodo naprave še vedno dobile starejšo različico.

Pregled naprave (samo na ravni naprave)

Če ste v napravi, boste prejeli pregledni povzetek izbrane naprave, ki vsebuje naslednje informacije:

Ime naprave	Ime naprave
Lokacija	Koordinate lokacije
Telefonska številka	Telefonska številka
Dodeljene obvezne aplikacije	Število dodeljenih obveznih aplikacij
Različica operacijskega sistema	različica operacijskega sistema naprave
Operacijski sistem	Operacijski sistem (Android Enterprise)
Serijska številka	Serijska številka naprave
Lastništvo naprave	Poslovna ali zasebna naprava
Vrsta naprave	Upravljana naprava AE Work
Ukoreninjen	Stanje, ki označuje, ali je bila naprava zakoreninjena.
V skladu s predpisi	Skladnost s smernicami
Naslov IP	Naslov IP naprave
Nazadnje videno	Točka v času, ko je bila naprava nazadnje povezana z AppTecom
Zadnji potisk	Točka v času, ko je bil napravi poslan zadnji potisk.
Dodelitev uporabnika	Uporabnik ali skupina, ki ji je ta naprava dodeljena.

Revizija konfiguracije

Tu dobite pregled, kateri profil skupine je dodeljen napravi.



	Installed Profile	Assigned Profile	Last Generated Profile
Device Profile	Device Profile: Revision 5	Device Profile: Revision 5	Device Profile: Revision 5
Group Profile	Default Group Profile: Revision 13	Default Group Profile: Revision 13 (Newer Revision available)	Default Group Profile: Revision 13

Če kliknete profil skupine, boste dobili neposreden dostop do tega profila in lahko opravite nastavitve.

S tem simbolom lahko razdeljene aplikacije vrnete v nastavitve skupinskega profila.

S tem simbolom lahko vse uporabljene aplikacije vrnete v nastavitve skupinskega profila.

"Na voljo je novejša revizija" pomeni, da je bil profil skupine spremenjen in shranjen, vendar ni dodeljen. Profil skupine je treba dodeliti s funkcijo "Assign now" na ravni skupine, da se spremembe uporabijo v napravah.

| Dnevnik naprave (samo na ravni naprave)

Tu boste prejeli različne dnevnik naprave. Po potrebi lahko tu neposredno ugotovite vzrok napake.

Dnevnik ukazov

Tu si lahko ogledate, kateri ukazi so bili izdani za napravo in kakšen je njihov status.

Command Log (last 250 commands)					
#	Created By	Date modified	Command	State	
1	jd@example.com	31.08.2021 12:21:37	Install assigned profiles	Device Pushed	
2	jd@example.com	31.08.2021 12:10:04	Get installed apps	Command Executed	
3	jd@example.com	31.08.2021 12:10:04	Get managed apps	Command Executed	
4	jd@example.com	31.08.2021 12:10:02	Get certificates	Command Executed	
5	jd@example.com	31.08.2021 12:10:02	Get asset data	Command Executed	
6	System Automated	31.08.2021 05:34:29	Update profile revision	Command Partially Failed !	
7	System Automated	31.08.2021 05:34:29	Apply device settings	Command Executed	
8	System Automated	31.08.2021 05:34:27	Install application	Command Failed !	
9	System Automated	31.08.2021 05:34:25	Get installed apps	Command Executed	
10	System Automated	31.08.2021 05:34:25	Get managed apps	Command Executed	
11	System Automated	31.08.2021 05:34:23	Get certificates	Command Executed	

Možni statusi ukazov

Potisnjena naprava	Storitvi za potiskanje (npr. APNS) je bila poslana potisna zahteva, da se naprava poveže nazaj s strežnikom EMM.
Ustvarjen ukaz	Ukaz je bil ustvarjen v sistemu.
Poslan ukaz	Ukaz je bil napravi poslan, ko se je povezala s strežnikom.
Izveden ukaz	Ukaz je bil uspešno izveden.
Ukaz ni uspel	Ukaz ni uspel. *
Ukaz delno ni uspel	Odvisno od operacijskega sistema naprave so lahko nekateri ukazi združeni. Pri tem nekateri deli te skupine ukazov niso bili uspešni. *
Ukaz se je izvršil, vendar je bil neuspešen	Ukaz je bil izveden, vendar morda ni bil.
Ukaz se ponovno premakne	Ukaz je ponovno poslal uporabnik.
Zavrženi	Ukaz je bil zavržen. Na primer zato, ker ga je nadomestil drug ukaz ali ker je bila naprava ponovno vpisana in so bili stari ukazi odstranjeni.

*Če je za sporočilom izklicnik, lahko več informacij dobite tako, da s kazalcem podrsate nad ikono.

Nastavitve naprave

Konfiguracija odjemalca

Tu lahko v napravi s sistemom Android izvedete naslednje konfiguracije:

Čas neskladnosti	Omejitev časovnega limita odziva uporabnika, po katerem se uporabi ukrep izvrševanja.
Izvršilni ukrepi po izteku roka za izpolnjevanje zahtev	Izvršilni ukrepi, kadar uporabnik ne izvaja dejanj, ki vodijo do statusa naprave, ki je skladna s predpisi
Pogostost zbiranja podatkov	Pogostost zbiranja podatkov o napravi/GPS
Frekvenca srčnega utripa naprave	Interval, v katerem mora naprava stopiti v stik s strežnikom AppTec Min. 1 minuta Največ. 24 ur
Omogočanje posodobitev lokacije	Če je aktivirano, naprava pošlje posodobitve lokacije v strežnik AppTec Server.
Čas posodobitve lokacije	Določa, v kakšnih časovnih intervalih naprava pošilja posodobitve lokacije AppTecu.
Uporaba Googleve natančnosti lokacije za posodobitev lokacije	Če je aktivirana, se za posodobitve lokacije uporablja omrežna lokacija (če je bila ta možnost deaktivirana v razdelku "Omejitve", ta nastavitev ne bo vplivala na nič).
Uporaba lokacije GPS za posodobitev lokacije	Če je aktivirano, se za posodobitve lokacije uporablja GPS.
Dovolite navidezne (lažne) lokacije	Omogoča ponarejanje podatkov o lokaciji prek aplikacij tretjih oseb.
Ukrep za izgubljeno povezavo	Če je omogočeno, lahko določite ukrep za primer, ko naprava v intervalu srčnega utripa ne vzpostavi povezave s strežnikom MDM. Na primer, če ima naprava čas srčnega utripa 5 minut, se s strežnikom poveže ob 10:35. Nato naprava zapusti območje Wi-Fi. Naslednji srčni utrip ob 10:40 bo neuspešen, zato se bo izvedlo določeno dejanje.
Akcija	Ukrep, ki ga je treba sprejeti takoj, ko naprava postane neskladna. <ul style="list-style-type: none"> • <input type="checkbox"/> Lock Naprava = naprava za zaklepanje • Brisanje naprave = naprava bo obnovljena na tovarniške nastavitve

	<ul style="list-style-type: none"> Brisanje naprave in kartice SD = naprava bo obnovljena na tovarniške nastavitve, pomnilnik kartice SD pa bo izbrisan.
Prag	Določite lahko prag neuspešnih srčnih utripov, ki so potrebni za sprožitev določenega dejanja.

Način uveljavljanja politik	Privzeto:	Uporabniki bodo občasno pozvani, naj izvedejo preostale ukrepe.
	Leno izvrševanje politik:	Uporabniki ne bodo nikoli pozvani k izvedbi neizvedenih dejanj. V odjemalcu AppTec bodo prikazana vsa odprta dejanja.
	Agresivno uveljavljanje politik:	Uporabniki bodo neprekinjeno pozvani k izvedbi preostalih dejanj.
Zaklepanje različice AppTec	Če je omogočeno, lahko določite kodo različice za aplikacijo AppTec. Odjemalec AppTec bo posodobljen samo na določeno različico. Novejše različice ne bodo upoštevane. Posodobitev na nižjo različico NI mogoča.	
Koda različice	Koda različice aplikacije AppTec, na katero se zaklene.	
Onemogočite obvestilo AppTec	<p>Če je onemogočen, odjemalec AppTec ne bo prikazal obvestila v obvestilni vrstici. Tako lahko uporabniki odjemalca AppTec zaprejo prek upravitelja opravil. Če je odjemalec AppTec zaprt, več funkcij, vključno z načinom Kiosk Mode in črno/belo listo aplikacij, ne bo delovalo pravilno.</p> <p>Samsungove naprave ponujajo mehanizem za zaščito odjemalca AppTec. Obvestilo je privzeto onemogočeno v napravah Samsung, ki podpirajo vmesnike KNOX API.</p> <p>Obvestilo ne sme biti onemogočeno v napravah z operacijskim sistemom Android 8.0 ali novejšim.</p>	

Ozadje

Nastavitev ozadja po meri	Omogočanje/izklop ozadja po meri
Ozadje	Nastavitev načina ozadja za uporabo barvne kode ali slike
Določite barvo	barvo ozadja določite kot šestnajstiško vrednost, npr. #000000 za črno ali #ffffff za belo.
Nastavite sliko kot ozadje	Naložite slikovno datoteko, ki jo želite uporabiti kot ozadje

Upravljanje sredstev (samo na ravni naprave)

Informacije o napravi

Model	Oznaka modela naprave
Operacijski sistem	OS
Različica operacijskega sistema	Različica operacijskega sistema
Serijska številka	Serijska številka
Ime naprave	Ime naprave
Stanje baterije	Stanje baterije
Prosti / skupni pomnilnik	Prosti / skupni pomnilnik
Samsung Safe	Vmesnik Samsung SAFE, potreben za različne možnosti nastavitvev
Na voljo je kartica SD	Na voljo je kartica SD
Emulirana kartica SD	Emulirana kartica SD
Kartica SD Odstranljiva	Odstranljiva kartica SD
SD Prosti / skupni pomnilnik	SD Prosti / skupni pomnilnik kartice SD

Wi-Fi

Naslov IP	Naslov IP naprave
WiFi MAC	Naslov WiFi MAC

Cellular

Status	Stanje (nameščena kartica SIM)
Telefonska številka	Telefonska številka
Gostovanje (glasovno/podatkovno)	Gostovanje za prenos govora/podatkov
Status gostovanja	Trenutni status gostovanja
Naslov IP	Naslov IP
Operater/prevoznik	Operater/prevoznik
Celična tehnologija	Celična tehnologija
IMEI	Številka IMEI
ICCID	To je identifikacijska oznaka za kartico SIM, pogosto tudi pametno kartico ali kartico z integriranim vezjem (ICC).
IMSI	<p>Mednarodna identiteta mobilnega naročnika (IMSI) v mobilnih omrežjih GSM in UMTS zagotavlja natančno identifikacijo uporabnikov omrežja. IMSI je sestavljen iz največ 15 števil in je konfiguriran na naslednji način:</p> <ul style="list-style-type: none"> • <u>Koda mobilne države</u> (MCC), 3 števke • <u>Koda mobilnega omrežja</u> (MNC), 2 ali 3 števke • Identifikacijska številka mobilnega naročnika (MSIN), 1-10 števil
Trenutni MCC/MNC	Glejte "SIM MCC/MNC".
SIM MCC/MNC	<p>Koda mobilne države je uveljavljena identifikacijska oznaka države, ki jo je določila ITU v skladu s standardom E.212. Uporablja se skupaj s kodo mobilnega omrežja (MNC) za identifikacijo mobilnega omrežja. Pomeni kodo države/mobilnega omrežja kartice SIM.</p> <p>Če gostujete v drugem mobilnem omrežju, bosta logično "trenutni MCC/MNC" in "SIM MCC/MNC" različna.</p>

Bluetooth

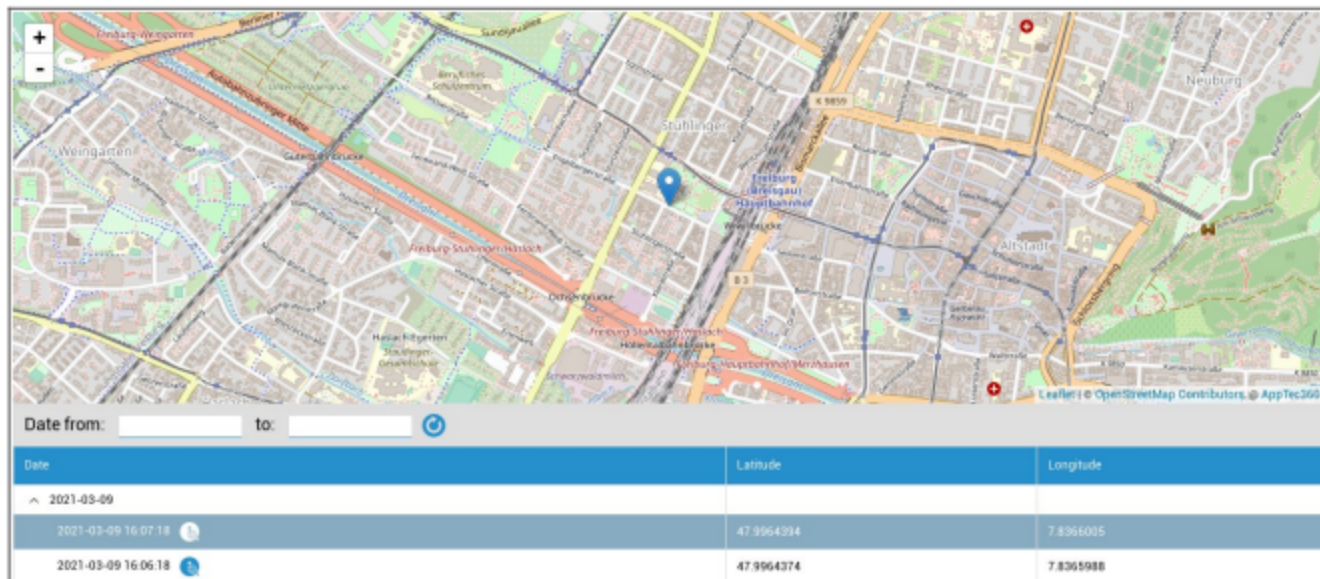
Bluetooth MAC	Naslov MAC Bluetooth
---------------	----------------------

Upravljanje varnosti

Zaščita pred krajo (samo na ravni naprave)

Informacije GPS (samo na ravni naprave)

Tu lahko določite trenutno/ zadnjo lokacijo naprave. Lokalizacijo lahko zaščitite z enim ali celo dvema gesloma - glejte: Splošne nastavitve - Zasebnost - Dostop do GPS



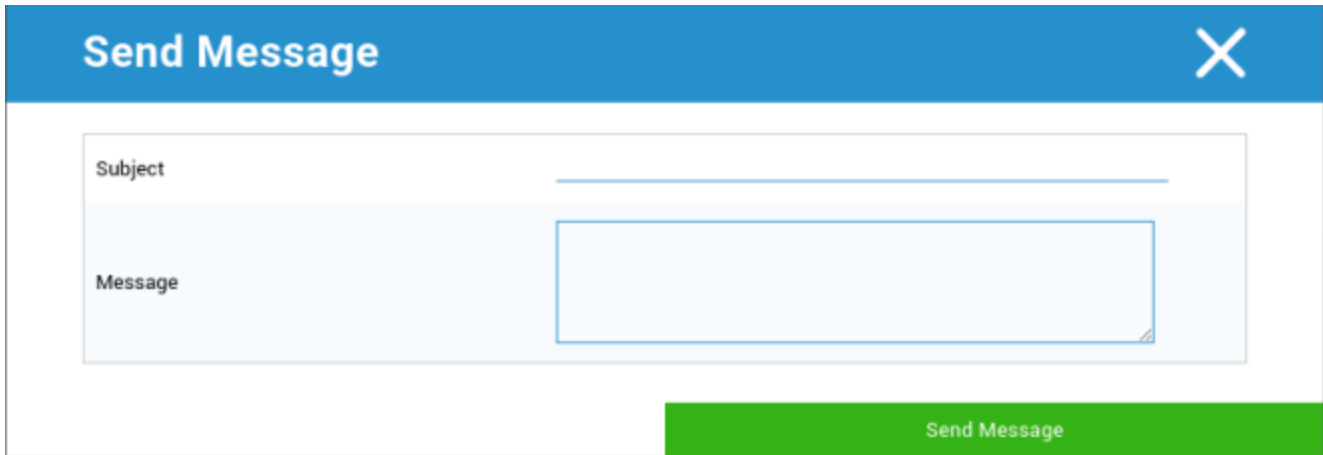
Brisanje in zaklepanje (samo na ravni naprave)

V razdelku "Brisanje in zaklepanje" lahko izvedete naslednja tri dejanja:

Celotno brisanje	V napravi se obnovijo tovarniške nastavitve (izbrišejo se podatki podjetja in osebni podatki). Deluje samo za izboljšani delovni profil
Izbris podjetja	Iz naprave končnega uporabnika se odstranijo samo podatki podjetja (vse aplikacije, podatki itd., ki jih je zagotovil AppTec).
Zaklepanje zaslona	Zaklepanje zaslona je aktivirano, napravo je treba odkleniti z geslom naprave/PIN.

Sporočilo (samo na ravni naprave)

Tu lahko izpolnite predmet in sporočilo ter ga pošljete napravi končnega uporabnika.



The image shows a 'Send Message' dialog box. It has a blue header with the text 'Send Message' and a close button (X) in the top right corner. Below the header, there is a form with two main sections: 'Subject' and 'Message'. The 'Subject' section has a text input field. The 'Message' section has a larger text area for the message content. At the bottom right of the dialog, there is a green button labeled 'Send Message'.

Varnostna konfiguracija

Pristopna koda naprave

V razdelku "Geslo" lahko pooblastite geslo naprave, na voljo so naslednje možnosti nastavitvev

Najmanjša dolžina gesla	določa najmanjše število simbolov, ki jih mora imeti geslo.	
Kakovost gesla	Neopredeljeno	Ta pravilnik nima zahtev glede gesla.
	Biometrični šibki	Ta politika omogoča uporabo biometrične tehnologije prepoznavanja z nizko stopnjo varnosti. To pomeni tehnologije, ki lahko prepoznajo identiteto posameznika do približno trimestne številke PIN (napačna zaznava je manj kot 1 proti 1 000).
	Nekaj	Ta politika zahteva nastavitvev določenega gesla ali vzorca, vendar ne uveljavlja nobenih posebnih pravil.
	Abecedno	Uporabnik mora vnesti geslo, ki vsebuje vsaj abecedne znake (ali druge simbole).
	Alfanumerični	Uporabnik mora vnesti geslo, ki vsebuje vsaj dva številčna in abecedna (ali druga simbola) znaka.
	Kompleksni	Uporabnik mora vnesti geslo, ki privzeto vsebuje vsaj eno črko, številčno številko in poseben simbol. S to kakovostjo gesla lahko omejite gesla, da vsebujejo različne sklope znakov, na primer vsaj eno veliko črko itd.
Najmanjša dolžina gesla	Nastavite zahtevano število znakov za geslo. Tako lahko na primer zahtevate, da imajo gesla PIN ali gesla vsaj šest znakov.	
Najmanjše število števil v geslu	Najmanjše število števil v geslu	
Najmanjše število malih črk v geslu	Najmanjše število malih črk v geslu	
Najmanjše število velikih tiskanih črk v geslu	Najmanjše število velikih tiskanih črk v geslu	
Najmanjši zahtevani črkovni znaki v geslu	Najmanjši zahtevani črkovni znaki v geslu	

Najmanjši zahtevani simboli v geslu	Najmanjši zahtevani simboli v geslu
-------------------------------------	-------------------------------------

Zaklepanje največjega časa neaktivnosti	Največja neaktivnost uporabnika do časovne blokade
Časovna omejitev izteka gesla	vzpostavi, po tem časovnem intervalu geslo preneha veljati in je treba izdati novo geslo.
Omejitev zgodovine gesel	Število predhodno uporabljenih gesel, ki niso dovoljena
Največ neuspešnih poskusov gesla	določa, kolikokrat je mogoče napačno vnesti geslo, preden se izvede popolno brisanje naprave.
Omogočanje biometričnega preverjanja pristnosti	Omogoča preverjanje pristnosti s prstnim odtisom ali skeniranjem šarenice. Samo za Samsung KNOX 2.1 in višje.

Pristopna koda zabojnika

V razdelku "Geslo" lahko pooblastite geslo za vsebnik, na voljo pa so tudi naslednje možnosti nastavitvev:

Najmanjša dolžina gesla	določa najmanjše število simbolov, ki jih mora imeti geslo.	
Kakovost gesla	Neopredeljeno	Ta pravilnik nima zahtev glede gesla.
	Biometrični šibki	Ta politika omogoča uporabo biometrične tehnologije prepoznavanja z nizko stopnjo varnosti. To pomeni tehnologije, ki lahko prepoznajo identiteto posameznika do približno trimestne številke PIN (napačna zaznava je manj kot 1 proti 1 000).
	Nekaj	Ta politika zahteva nastavitvev določenega gesla ali vzorca, vendar ne uveljavlja nobenih posebnih pravil.
	Abecedno	Uporabnik mora vnesti geslo, ki vsebuje vsaj abecedne znake (ali druge simbole).
	Alfanumerični	Uporabnik mora vnesti geslo, ki vsebuje vsaj dva številčna in abecedna (ali druga simbola) znaka.
	Kompleksni	Uporabnik mora vnesti geslo, ki privzeto vsebuje vsaj eno črko, številčno številko in poseben simbol. S to kakovostjo gesla lahko omejite gesla, da vsebujejo različne sklope znakov, na primer vsaj eno veliko črko itd.
Najmanjša dolžina gesla	Nastavite zahtevano število znakov za geslo. Tako lahko na primer zahtevate, da imajo gesla PIN ali gesla vsaj šest znakov.	
Najmanjše število števil v geslu	Najmanjše število števil v geslu	
Najmanjše število malih črk v geslu	Najmanjše število malih črk v geslu	
Najmanjše število velikih tiskanih črk v geslu	Najmanjše število velikih tiskanih črk v geslu	
Najmanjši zahtevani črkovni znaki v geslu	Najmanjši zahtevani črkovni znaki v geslu	
Najmanjši zahtevani simboli	Najmanjši zahtevani simboli v geslu	

v geslu	
---------	--

Zaklepanje največjega časa neaktivnosti	Največja neaktivnost uporabnika do časovne blokade
Časovna omejitev izteka gesla	vzpostavi, po tem časovnem intervalu geslo preneha veljati in je treba izdati novo geslo.
Omejitev zgodovine gesel	Število predhodno uporabljenih gesel, ki niso dovoljena
Največ neuspešnih poskusov gesla	določa, kolikokrat je mogoče napačno vnesti geslo, preden se izvede popolno brisanje naprave.

AntiVirus

Samodejno skeniranje	Omogočite periodično samodejno pregledovanje
Interval skeniranja	Interval za pregled (hiter/celoten)
Popolno samodejno skeniranje	Omogočite popolnoma samodejno skeniranje
Samodejne posodobitve	Omogočanje samodejnih posodobitev
Interval preverjanja posodobitev	Kako pogosto je treba posodabljeni aplikaciji in njeno zbirko podatkov (virusi / poškodovana koda).
Zaščita aplikacij	Omogočanje samodejnega skeniranja aplikacij
Zaščita kartice SD	Omogočite samodejno skeniranje kartice SD
Posodobitev samo za Wi-Fi	Če je ta možnost omogočena, se posodobitve uporabijo le, ko je naprava uspešno povezana z omrežjem Wi-Fi.

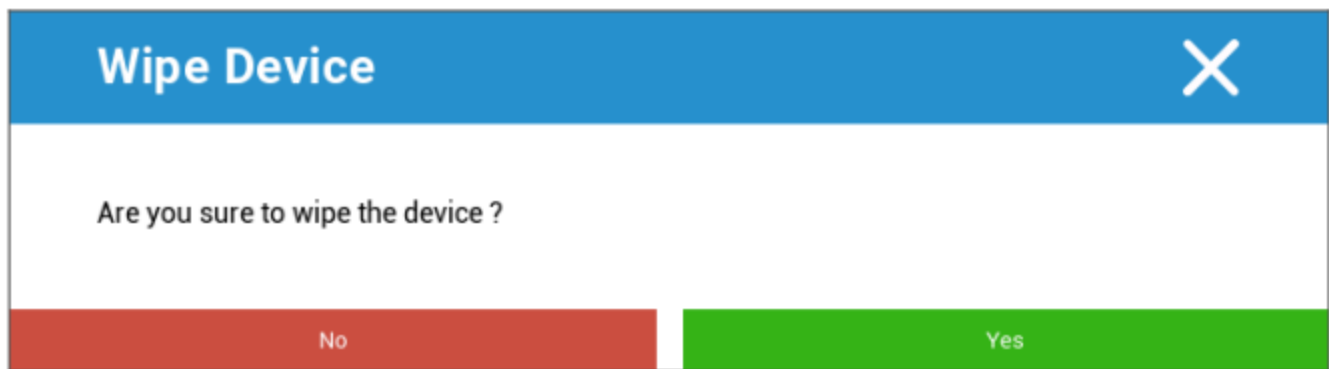
Konec življenjske dobe (samo na ravni naprave)

Brisanje (samo na ravni naprave)

V razdelku "Brisanje" lahko obnovite tovarniške nastavitve naprave (samo v razširjenem delovnem profilu).

Pri tem bodo v napravi končnega uporabnika izbrisani tako poslovni kot zasebni podatki.

S klikom na simbol Minus prejmete naslednje sporočilo:



Z "Da" lahko izvedete brisanje.

V razdelku "Poročilo o brisanju" lahko prikažete naslednje elemente

Izbrisano z	Zgodovina izvajalca brisanja
Datum	Datum
Status	Status (npr. če je bilo brisanje uspešno izvedeno)

Nastavitve omejitev

Omejitve

Tu lahko omejite in blokirate različne stvari.

Izvrševanje skladnosti	Način Poziv uporabniku - uporabnik bo pozvan, da izvede potrebna dejanja. Kontejner za zaklepanje načina - skrijte vse aplikacije, dokler niso izpolnjene vse zahteve
Pravilnik o dovoljenjih za izvajanje	Poziv uporabniku za nove zahteve za dovoljenja Vedno odobri nove zahtevke za nova dovoljenja Vedno zavrnite nove zahteve za dovoljenje Opozorilo: Nekatere aplikacije imajo težave s prepoznavanjem dovoljenj, če so ta nastavljena samodejno. Če vedno podeljujete dovoljenja in imate težave z aplikacijami, ki trdijo, da dovoljenja manjkajo, to nastavite na "pozvati uporabnika" in ponovno namestite aplikacijo.
Dovolite odhodno odložišče	Omogoča kopiranje in lepljenje iz notranjosti vsebnika na zunanjo stran
Omogočanje razreševanja ID klicatelja	Prikaže ime dohodnega klica na podlagi stikov v vsebniku
Omogočanje rešitve iskanja stikov	Omogoča iskanje imen v vsebniku za stike med klicanjem.
Omogočanje souporabe stikov Bluetooth	Omogoča dostop do stika z zabojsnikom v avtomobilu
Prepovedati odhodni žarek NFC	Onemogoči NFC za zabojsnik
Dovolite neznane vire	Če je ta možnost omogočena, lahko uporabniki z namestitvijo datoteke .apk prenesejo aplikacije na drugo stran.
Omogočanje razhroščevanja USB	Če je omogočeno, lahko uporabniki omogočijo razhroščevanje USB.
Prepoved spreminjanja računa	Prepoved ustvarjanja, brisanja in spreminjanja računov v vsebniku Upoštevajte, da morajo nekatere aplikacije ustvariti ali spremeniti račune, da delujejo, kot je bilo pričakovano.

Omejitve delovnega profila. Na voljo samo v napravah z operacijskim sistemom Android 11 ali novejšim, z izboljšanim delovnim profilom

Prepoved fotoaparata	Določa, ali je kamera v delovnem profilu prepovedana.
Prepovedati Bluetooth	Določa, ali je bluetooth v delovnem profilu prepovedan.
Omogočanje zaščite za ponastavitev tovarniških nastavitvev	Aktivirajte to možnost, da prekrijete zaščito za ponastavitev tovarniške nastavitve sistema Android z Googlovim računom, ki ste ga določili v "Splošne nastavitve" → "Konfiguracija sistema Android" → "Android Enterprise" → "Zaščita za ponastavitev tovarniške nastavitve" Če je to omogočeno in ponastavite napravo, boste morali za ponovno nastavitve naprave zagotoviti konfigurirani Googlov račun.
Posodobitev nadzornega operacijskega sistema	Omogočite to možnost, če želite nastaviti obnašanje posodobitve na samodejno, okensko ali odloženo.
Politika posodabljanja	Samodejno: namestite samodejno, takoj ko je posodobitev na voljo. Okensko: Namestite samodejno v dnevnom oknu vzdrževanja. To omogoča tudi nastavitve posodobitve aplikacij Play v oknu. To je zelo priporočljivo za naprave kiosk, saj lahko le tako aplikacijam, ki so trajno pripete v ospredje, aplikacija Play zagotovi posodobitev. Odloži: Odložite samodejno namestitev za največ 30 dni.

Omejitve osebnega profila. Na voljo samo v napravah z operacijskim sistemom Android 11 in novejših z izboljšanim delovnim profilom.

Prepoved fotoaparata	Določa, ali je fotoaparata v osebnem profilu prepovedan.
Prepovedati Bluetooth	Določa, ali je bluetooth v osebnem profilu prepovedan.
Dovolite neznane vire	Če je to omogočeno, lahko uporabniki delovnih profilov z namestitvijo datoteke .apk na stranski način naložijo aplikacije.

Upravljanje certifikatov

Tu lahko napravam razdelite zaupanja vredna potrdila in potrdila o identiteti. Za distribucijo zaupanja vrednih potrdil je potreben operacijski sistem Android 8 ali novejši, za distribucijo identitetnih potrdil pa operacijski sistem Android 9 ali novejši.

<input checked="" type="checkbox"/> Trusted certificate (Available on Android 8 and above) + -	
Certificate file *	MDM_AppTec GmbH_Certificate.pem (ID: 13) ▼ ?
<input checked="" type="checkbox"/> Identity certificate (Available on Android 9 and above) + -	
Description *	<u>Example Identity Certificate</u>
Certificate file *	example.p12 (ID: 26) ▼ ?

Z znakom "+" lahko dodate več potrdil.

Zaupanja vredna potrdila morajo biti v formatu PEM.

Potrdila o identiteti morajo biti v formatu PKCS12.

Upravljanje povezav

Wifi

Za to nastavitve izvedite predhodno konfiguracijo naprav končnega uporabnika za dostop do notranjih točk dostopa

.

Identifikator nabora storitev (SSID)	SSID za omrežje, ki ga želite povezati
Skrito omrežje	Aktiviraj, če AP ne oddaja SSID.

Vrsta varnosti

Določite varnostno vrsto AP

WEP

Geslo	Geslo za AP
-------	-------------

WPA/WPA2

Geslo	Geslo za AP
-------	-------------

802.1x EAP

Metoda EAP

PWD	Identiteta	Identiteta
	Geslo	Geslo

PEAP	Protokol preverjanja pristnosti v fazi 2	ni	Brez dodatnega protokola
		MSCHAPV2	Protokol MSCHAPV2
		GTC	Protokol GTC
	Potrdilo CA	Potrdilo CA	
	Identiteta	Identiteta	
	Anonimna identiteta	Anonimna identiteta	
	Geslo	Geslo	

TTLS	Protokol preverjanja pristnosti v fazi 2	ni	Brez dodatnega protokola
		PAP	Protokol PAP
		MSCHAP	Protokol MSCHAP
		MSCHAPV2	Protokol MSCHAPV2
		GTC	Protokol GTC
	Potrdilo CA	Potrdilo CA	
	Identiteta	Identiteta	
Anonimna identiteta	Anonimna identiteta		
Geslo	Geslo		

TLS	Potrdilo CA	Potrdilo CA
	Identiteta	Identiteta
	Geslo	Geslo

VPN

Ime povezave	Ime povezave VPN
--------------	------------------

Vrsta VPN

VPN

Odjemalec VPN

Odjemalec VPN AppTec	
Konfiguracija vrat	Izberite konfiguracijo VPN na prehodu (glejte Splošne nastavitve > Univerzalni prehod > Nastavitve VPN).
Vedno vklopljen VPN	Omogočanje funkcije Native Lockdown
Omogočanje zaklepanja AppTec	Omogočanje zaklepanja AppTec

Vgrajeno (na voljo samo v napravah Samsung)			
Vrsta povezave	PPTP	Strežnik	Strežnik
		Omogočanje šifriranja PPTP	Omogočanje šifriranja PPTP
	L2TP / IPsec PSK	Strežnik	Strežnik
		Predhodni zaupni ključ IPsec	Predhodni zaupni ključ IPsec
		Omogočite L2TP Secret	Omogočite L2TP Secret
		Skrivnost L2TP	Skrivnost L2TP
	IPsec XAuth PSK	Strežnik	Strežnik
		Identifikator IPsec	Identifikator IPsec
		Predhodni zaupni ključ IPsec	Predhodni zaupni ključ IPsec
	DNS Iskanje domen	DNS Iskanje domen	
Strokovne nastavitve	Strežniki DNS	Strežniki DNS	
	Usmeritve za posredovanje	Usmeritve za posredovanje	

Odprto omrežje VPN		
Strežnik	Strežnik	
Profil OpenVPN	Profil OpenVPN	
Aplikacija OpenVPN	OpenVPN za Android (priporočljivo)	
	Povezava OpenVPN	
Strokovne nastavitve	Strežniki DNS	Strežniki DNS
	Usmeritve za posredovanje	Usmeritve za posredovanje

Samsung / Strong Swan			
Vrsta povezave	PPTP	Strežnik	Strežnik
		Uporabniško ime	Uporabniško ime
		Geslo	Geslo
		Omogočanje šifriranja PPTP	Omogočanje šifriranja PPTP
	L2TP / IPsec PSK	Strežnik	Strežnik
		Predhodni zaupni ključ IPsec	Predhodni zaupni ključ IPsec
		Uporabniško ime	Uporabniško ime
		Geslo	Geslo
		Omogočite L2TP Secret	Skrivnost L2TP
	IPsec XAuth PSK	Strežnik	Strežnik
		Identifikator IPsec	Identifikator IPsec
		Predhodni zaupni ključ IPsec	Predhodni zaupni ključ IPsec
		Uporabniško ime	Uporabniško ime
		Geslo	Geslo
	Strokovne nastavitve	Strežniki DNS	Strežniki DNS
Usmeritve za posredovanje		Usmeritve za posredovanje	

Cisco Any Connect		
Strežnik	Strežnik	
Način potrdila	Onemogočeno	Onemogočeno
	Samodejno	Samodejno
Strokovne nastavitve	Strežniki DNS	Strežniki DNS
	Usmeritve za posredovanje	Usmeritve za posredovanje

VPN za posamezno aplikacijo

Odjemalec VPN

Odjemalec VPN AppTec		
Konfiguracija vrat	Izberite konfiguracijo VPN na prehodu (glejte Splošne nastavitve > Univerzalni prehod > Nastavitve VPN).	
Aplikacije VPN	Aplikacije VPN	
Vedno vklopljen VPN	Omogočanje funkcije Native Lockdown	Vedno vklopljen VPN
Omogočanje zaklepanja AppTec	Omogočanje zaklepanja AppTec	

Samsung / Strong Swan			
Vrsta povezave	PPTP	Strežnik	Strežnik
		Aplikacije VPN	Aplikacije VPN
		Uporabniško ime	Uporabniško ime
		Geslo	Geslo
		Omogočanje šifriranja PPTP	Omogočanje šifriranja PPTP
	L2TP / IPsec PSK	Strežnik	Strežnik
		Aplikacije VPN	Aplikacije VPN
		Predhodni zaupni ključ IPsec	Predhodni zaupni ključ IPsec
		Uporabniško ime	Uporabniško ime
		Geslo	Geslo
		Omogočite L2TP Secret	Skrivnost L2TP
	IPsec XAuth PSK	Strežnik	Strežnik
		Aplikacije VPN	Aplikacije VPN
		Identifikator IPsec	Identifikator IPsec
		Predhodni zaupni ključ IPsec	Predhodni zaupni ključ IPsec
		Uporabniško ime	Uporabniško ime
		Geslo	Geslo
Strokovne nastavitve	Strežniki DNS	Strežniki DNS	
	Usmeritve za posredovanje	Usmeritve za posredovanje	

Omejitve

Tu lahko nastavite omejitve v zvezi z upravljanjem povezave.

Omogočanje podatkovnega gostovanja	Omogočanje mobilnih podatkov med gostovanjem
Prisiliti podatkovno gostovanje	Če je aktivirano, je gostovanje za mobilne podatke trajno aktivirano (ni priporočljivo!) Ta nastavev prepiše nastavev "Dovoli podatkovno gostovanje"!
Uporaba sistemkega strežnika http Proxy Server	Uporaba posredniškega strežnika HTTP, ki je na voljo v nastavitvah sistema, je odvisna od povezanega omrežja (WiFi ali APN).

Upravljanje PIM

Gmail Exchange

Informacije: Ta konfiguracija bo uporabljena za aplikacijo Gmail. Zato morate odobriti in namestiti aplikacijo Gmail.

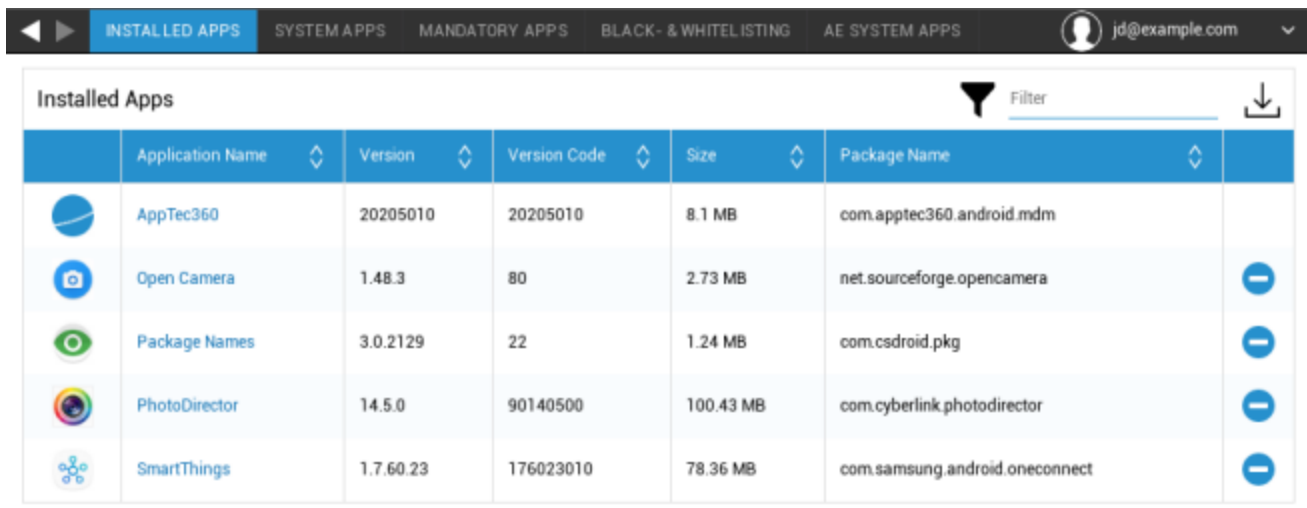
E-poštni naslov	e-poštni naslov uporabnika Upoštevajte "Namestnike", ki jih lahko uporabite za delo s poverilnicami in ne izvajate sprememb ročno v vsaki napravi. S klikom jih lahko prikažete sami
Gostiteljsko ime strežnika	Strežniški naslov strežnikov Exchange
Prijavno ime	Prijavno ime za zadevno napravo končnega uporabnika, upoštevajte tudi "Namestna imena tukaj".
Podpis	Priložite lahko podpis (namig: nekatere naprave zahtevajo oblikovanje HTML za podpis).
Število prejšnjih dni za sinhronizacijo	Število dni, ki določajo, kdaj se e-poštna sporočila sinhronizirajo nazaj
Identifikator naprave	Ein String der die EAS DeviceID enthält. Dies ist Teil des EAS Protokols und wird in einigen Umgebungen benötigt
Uporabite Secure Sockets Layer (SSL)	Uporaba povezave SSL
Sprejmite vsa potrdila	Sprejemajo se vsa potrdila. Izberite to možnost, če vaš strežnik Exchange uporablja samopodpisano potrdilo.
Dovoli neupravljane račune	Uporabnikom omogočite dodajanje ali odstranjevanje kateregakoli računa Exchange, razen računa, določenega v tej upravljani konfiguraciji. Če je ta nastavev omogočena, uporabnikom ne morete preprečiti dodajanja drugih računov Exchange v Gmail. Prav tako ne morete nadzorovati izmenjave podatkov med drugimi aplikacijami in računi Exchange, ki jih dodajo uporabniki. Ta nastavev naj bo omogočena le, če morajo vaši uporabniki v Gmailu vzdrževati več kot en delovni račun Exchange.
Potrdilo stranke	Potrdilo stranke. Zahteva se samo, če poštni strežnik pričakuje njegovo prisotnost.










Upravljanje aplikacij

Upravitelj aplikacij za podjetja

Nameščene aplikacije (samo na ravni naprave)

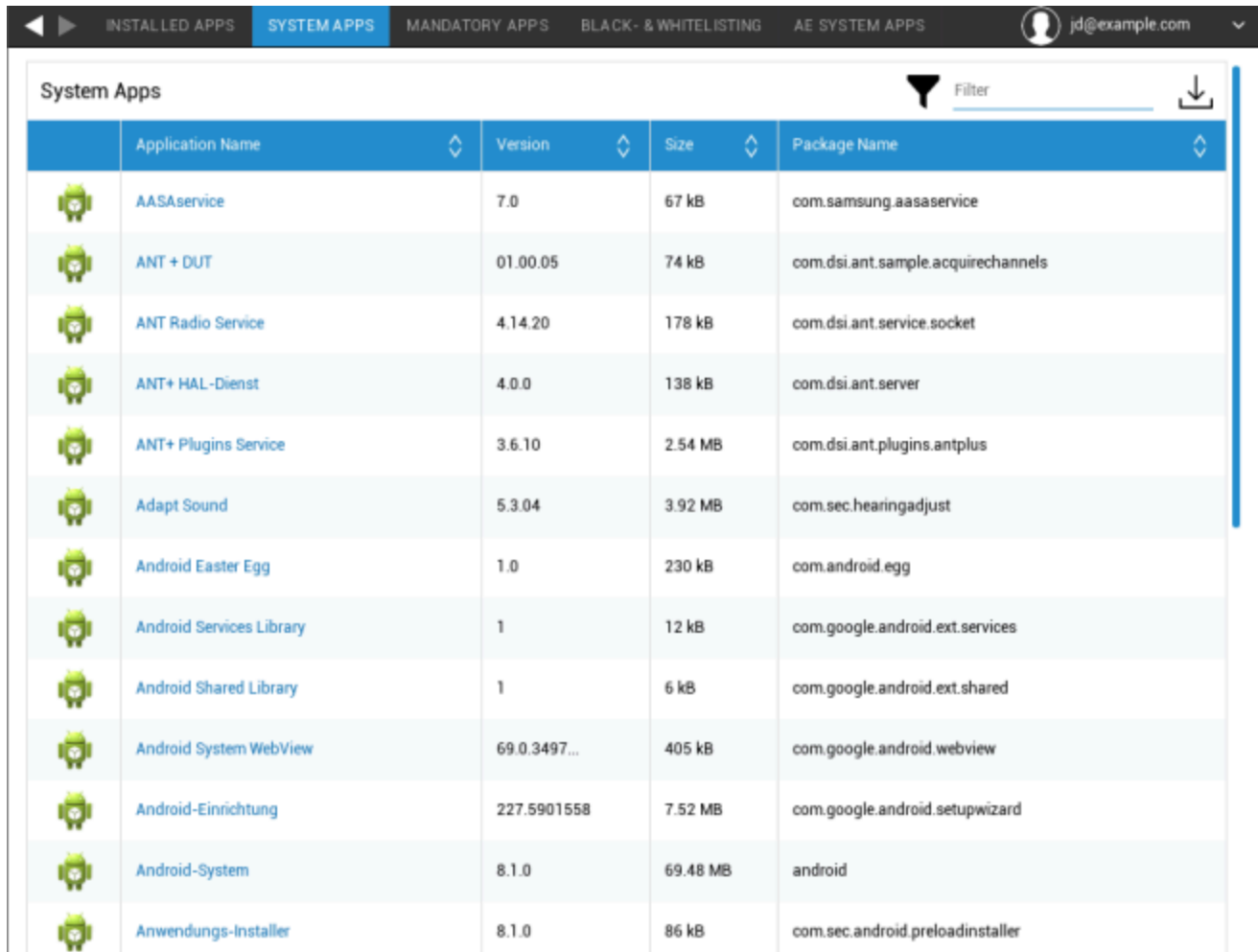
Tu so prikazane vse aplikacije, ki so trenutno nameščene v vsebniku.
















	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	

Sistemske aplikacije (samo na ravni naprave)

V razdelku "Sistemske aplikacije" so navedene vse aplikacije in storitve, ki jih je proizvajalec naprave že namestil v napravo končnega uporabnika.



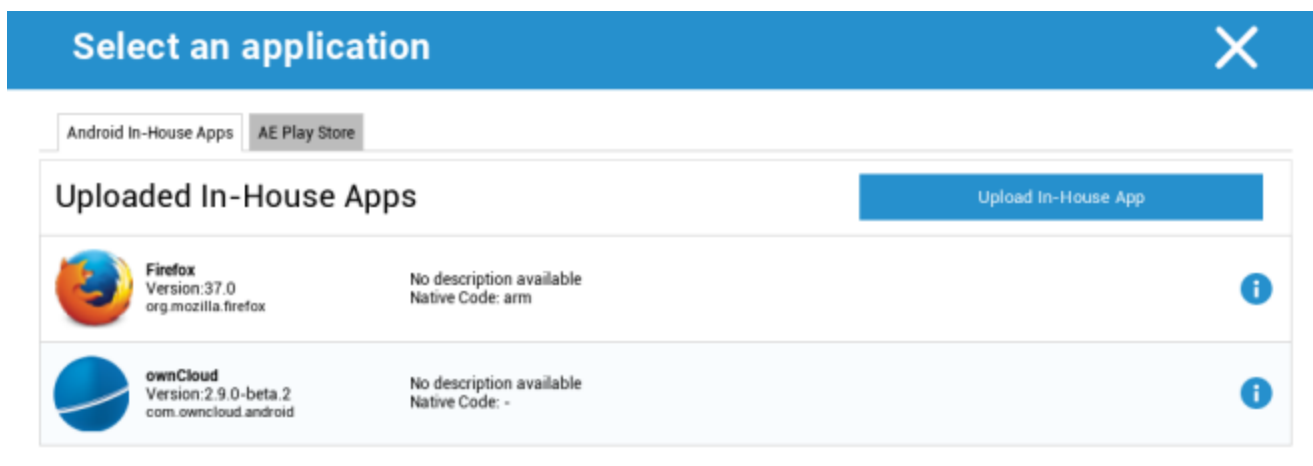
	Application Name	Version	Size	Package Name
	AASAservice	7.0	67 kB	com.samsung.aasaservice
	ANT + DUT	01.00.05	74 kB	com.dsi.ant.sample.acquirechannels
	ANT Radio Service	4.14.20	178 kB	com.dsi.ant.service.socket
	ANT+ HAL-Dienst	4.0.0	138 kB	com.dsi.ant.server
	ANT+ Plugins Service	3.6.10	2.54 MB	com.dsi.ant.plugins.antplus
	Adapt Sound	5.3.04	3.92 MB	com.sec.hearingadjust
	Android Easter Egg	1.0	230 kB	com.android.egg
	Android Services Library	1	12 kB	com.google.android.ext.services
	Android Shared Library	1	6 kB	com.google.android.ext.shared
	Android System WebView	69.0.3497...	405 kB	com.google.android.webview
	Android-Einrichtung	227.5901558	7.52 MB	com.google.android.setupwizard
	Android-System	8.1.0	69.48 MB	android
	Anwendungs-Installer	8.1.0	86 kB	com.sec.android.preloadinstaller

Obvezne aplikacije

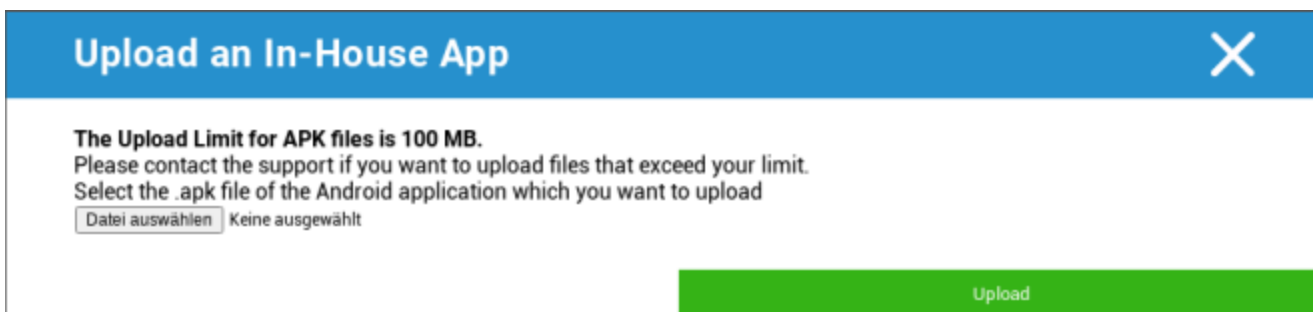
V razdelku Obvezne aplikacije lahko določite obvezne zahtevane aplikacije. Uporabnik bo nenehno pozvan k namestitvi te določene aplikacije, če gre za aplikacijo v hiši. Aplikacije iz trgovine Play Store se bodo namestile samodejno.

Prek , je mogoče opredeliti predpisano zahtevano aplikacijo.

To je lahko domača aplikacija iz seznama "Androidove domače aplikacije", ki ste jo naložili v splošnih nastavitvah.

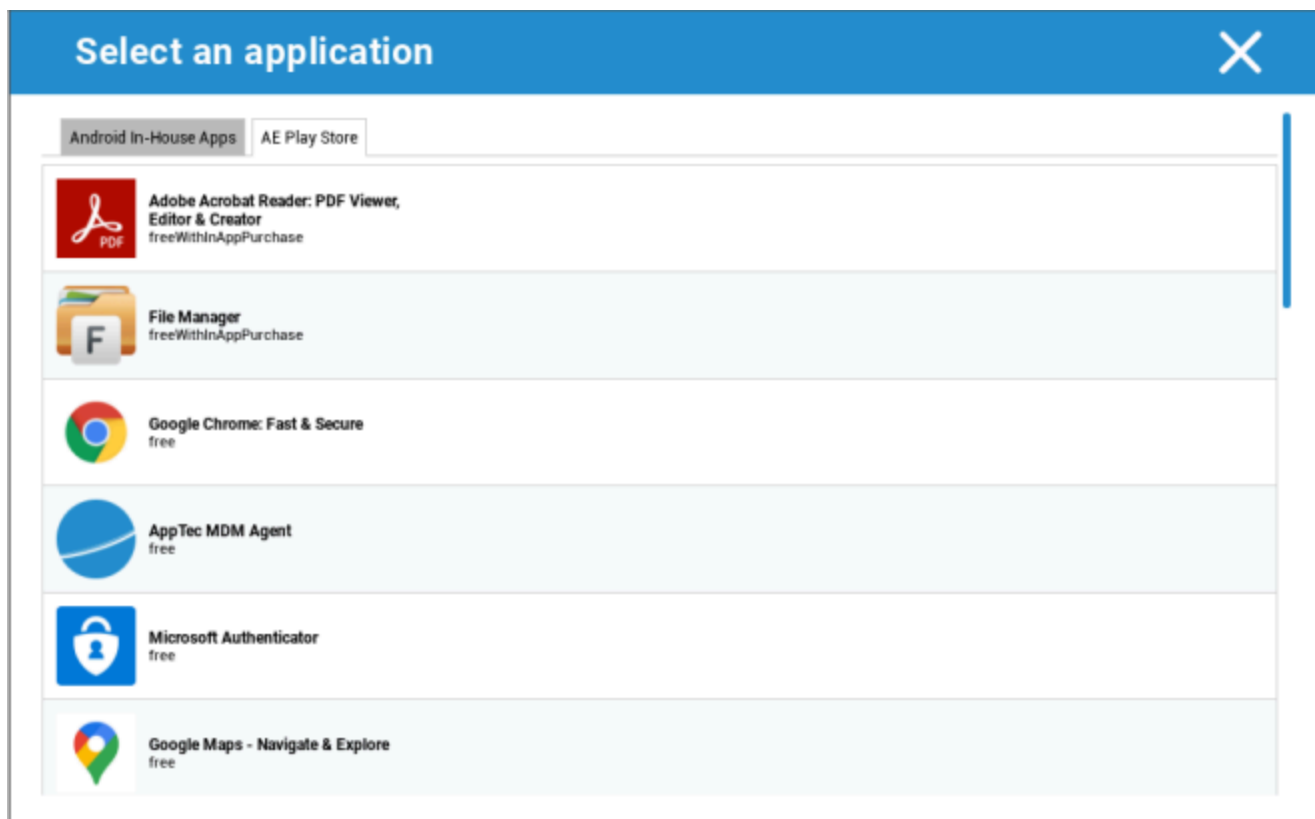


Datoteko apk lahko izberete in naložite tudi neposredno z "Naložite domačo aplikacijo".



Če nameščate aplikacijo v hiši, lahko aktivirate možnost "Posodabljanje". Če je ta možnost aktivirana in ste v DB domače aplikacije določili novejšo različico, bo aplikacija posodobljena v napravi.

Lahko pa je aplikacija "AE Play Store" iz trgovine Google Work Play Store.



V tem zavihku bodo prikazane samo odobrene aplikacije "AE Play Store Apps".

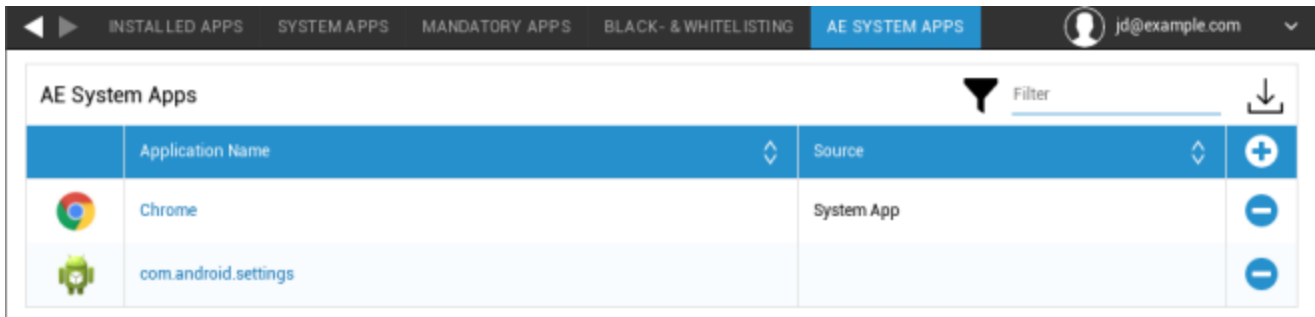
Če želite odobriti aplikacijo "AE Play Store App", pojdite v "Splošne nastavitve" > "Upravljanje aplikacij" > "AE Play

Trgovina" in dodajte aplikacijo z gumbom, ki vas bo preusmeril na zavihek "Aplikacije v trgovini Play" (ali pa lahko neposredno odprete zavihek "Aplikacije v trgovini Play").

V zavihku "Aplikacije v trgovini Play" lahko iščete aplikacije. Ko kliknete na aplikacijo, se odpre stran z aplikacijo, kjer lahko aplikacijo odobrite s klikom na "Approve".

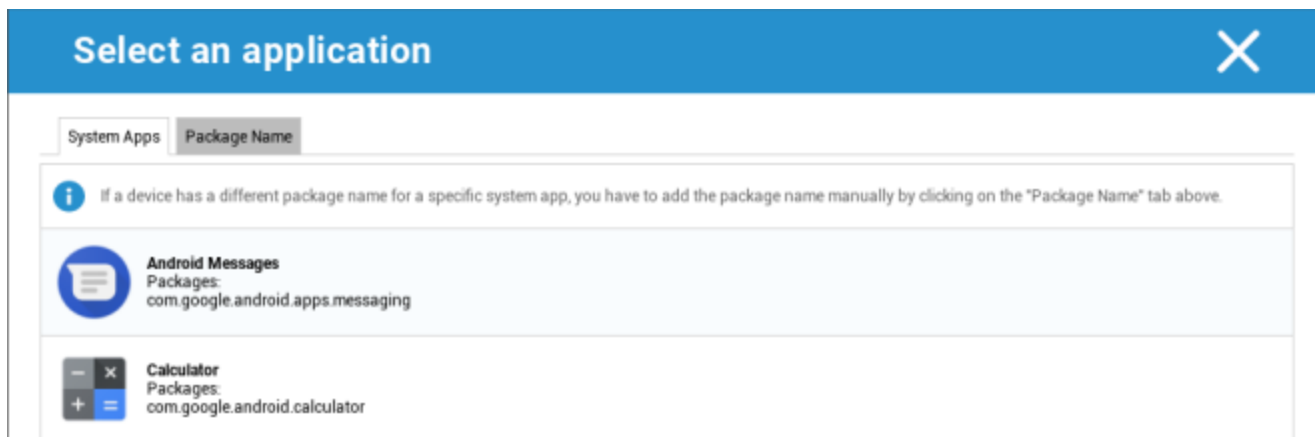
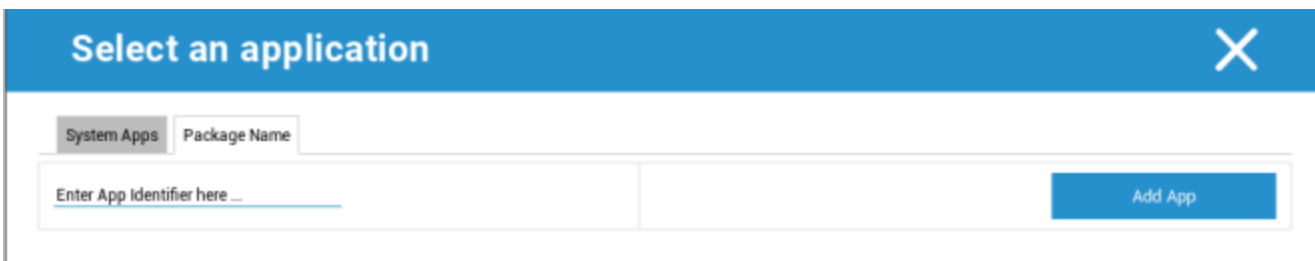
Aplikacije sistema AE

Tu lahko določite seznam, ki vsebuje določene sistemske aplikacije, ki jih je treba aktivirati v napravah.



Application Name	Source	
Chrome	System App	+ -
com.android.settings		-

Če kliknete gumb, lahko izberete s seznama možnih sistemskih aplikacij, ki ga zagotovi Google, ali neposredno vnesete ime paketa sistemske aplikacije, ki jo je treba aktivirati.

Ne pozabite, da so sistemske aplikacije na seznamu, ki ga je pripravil Google, le aplikacije, ki so lahko sistemske, vendar ni nujno, da so sistemske aplikacije v vaših napravah.

Vendar ta seznam zadeva le aplikacije, ki so že vnaprej nameščene.

Dodajanje aplikacij, ki niso vnaprej nameščene v napravah, ne bo vplivalo na naprave, ne glede na to, ali je aplikacija s seznama, ki ga zagotovi Google, ali pa je ime paketa aplikacije vneseno neposredno.

Omejitve in nastavitve

Nastavitve upravljanja aplikacij

Tu lahko nastavite obnašanje naprave glede posodobitev aplikacij.

Pogostost preverjanja posodobitev	Določite, v katerem intervalu bo odjemalec AppTec iskal posodobitve aplikacije. Privzeta vrednost je 24 ur.
Prag Wi-Fi	Aplikacije, ki so večje od določene velikosti, bodo prenesene prek omrežja Wi-Fi. Če je izbrana možnost "Samo Wi-Fi", bodo vse aplikacije prenesene prek omrežja Wi-Fi.

Trgovina z aplikacijami za podjetja

Lastna spletna stran

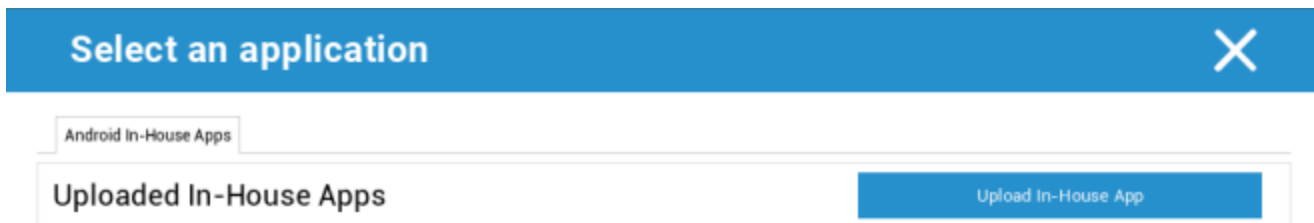
Pod točko "Lastno" lahko naložite in distribuirate interno razvite aplikacije.

S tem simbolom lahko distribuirate dodatne domače aplikacije.

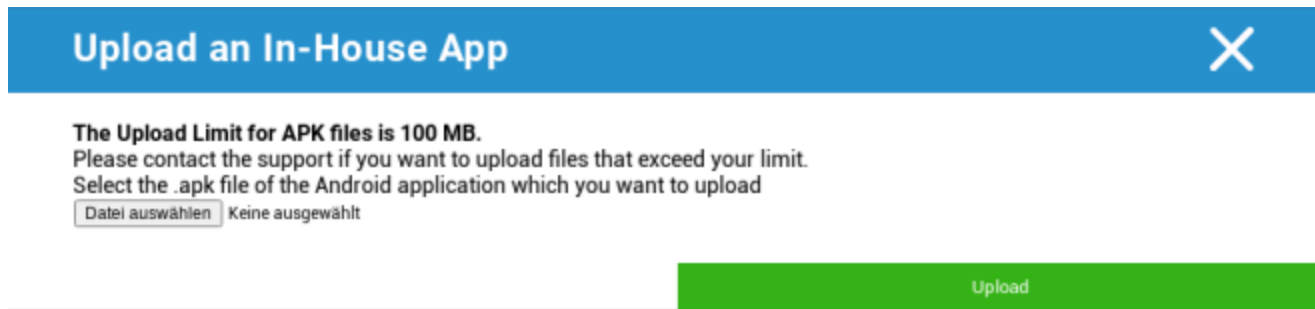
Če nameščate aplikacijo v hiši, lahko aktivirate možnost "Posodabljanje". Če je ta možnost aktivirana in ste v DB domače aplikacije določili novejšo različico, bo aplikacija posodobljena v napravi.



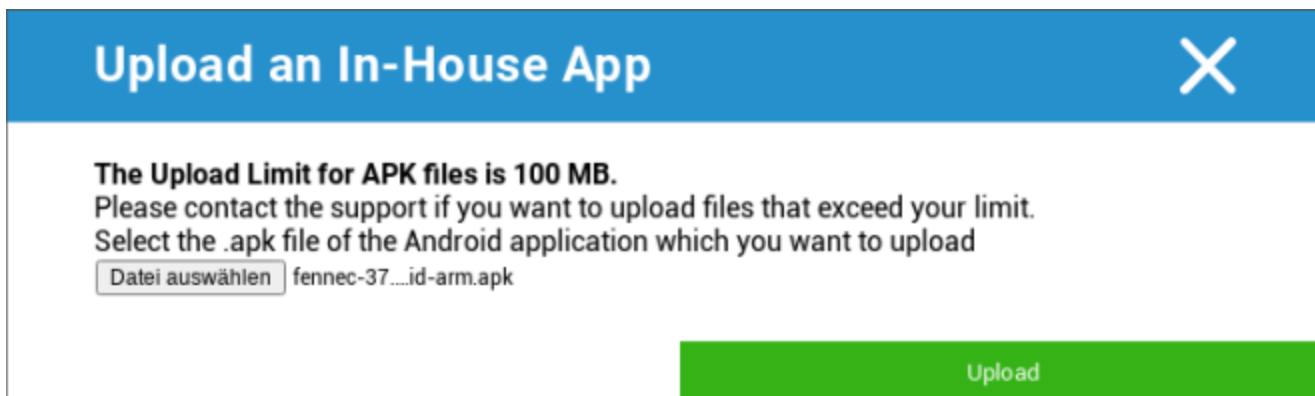
Če niste razdelili aplikacij znotraj podjetja, boste prejeli naslednji pregled:



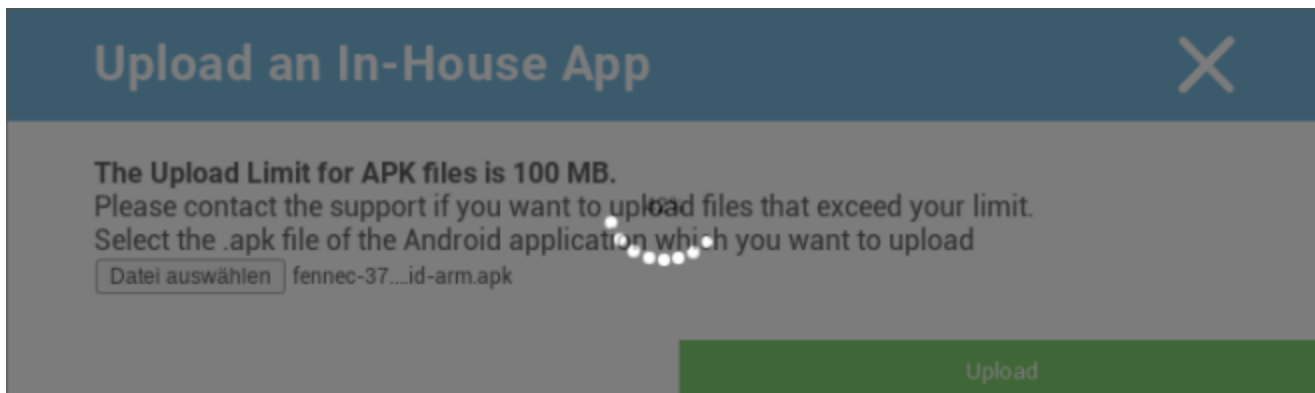
V ta namen kliknite "Upload In-House App", nato pa se vam bo prikazal naslednji pregled:



Zdaj z "Išči..." izberite datoteko .apk in nato kliknite na "Naloži".



Vaša aplikacija bo zdaj naložena, v sredini kroga pa bo prikazan kazalnik odstotka, ki kaže, kolikšen del aplikacije je bil že naložen.



Če je bilo nalaganje vaše domače aplikacije uspešno, lahko naloženo aplikacijo najdete v katalogu aplikacij.

Uporabnik ima zdaj možnost videti in namestiti to aplikacijo v trgovini AppTec Store v napravi končnega uporabnika v kategoriji "In-House".



In-House						Filter	↓
Application Name	Version	Native Code	Size	Package Name		+	
 Firefox	37.0	arm	28.67 MB	org.mozilla.firefox		-	

Ker to ne vključuje aplikacije Google PlayStore, uporabnik ne potrebuje shranjenega Googlovega ID v svoji napravi končnega uporabnika.

Trgovina Play za podjetja

Trgovina AE Play

Tu lahko dodate aplikacije v trgovino Android Enterprise Playstore. Upoštevajte, da morate aplikacije odobriti z računom skrbnika AE, preden jih lahko dodate.

Za odobritev aplikacije glejte navodila v razdelku Obvezne aplikacije.

Upravljanje vsebine

Vsebinsko polje

Tu lahko aktivirate vsebinsko polje.

Takoj ko preklopite "Omogoči ContentBox" na "Vklopljeno", se v napravo končnega uporabnika samodejno namesti ločena aplikacija ContentBox.

Varen brskalnik

Tu lahko konfigurirate nastavitve za AppTec Secure Browser.

Takoj ko preklopite razdelek v "Varnem brskalniku" na "Vklopljeno", se v napravo končnega uporabnika samodejno namesti ločena aplikacija za brskalnik.

Zahtevati geslo	Od uporabnika zahtevajte, da nastavi in uporablja geslo za dostop do brskalnika.
Najmanjša zahtevana dolžina gesla	Nastavitev zahtevanega števila znakov za geslo
Zahtevana kakovost gesla	Nastavite zahtevano kakovost gesla
Omejitev prenosov / Odprite v	
Omejitev nalaganja	
Prenos bele liste	Seznam naslovov URL, za katere bo nalaganje vedno dovoljeno.
Dovoli kopiranje	Omogočite kopiranje, rezanje ali deljenje besedila na spletnih straneh.
Omogočite zajem zaslona	Omogočite zajemanje posnetkov zaslona.
Pogostost čiščenja podatkov	Izberite, s kakšno pogostostjo naj se samodejno odstranijo VSI uporabniški podatki (zgodovina, predpomnilnik itd.).
Zaznamki podjetja	Zaznamki bodo prikazani v mapi "Company bookmarks" (zaznamki podjetja) v zaznamkih brskalnikov. Uporabnik jih ne more urejati.
Skrij naslovno vrstico	
Bela lista v brskalniku (brez univerzalnega prehoda)	Omogoča beli seznam URL-jev na strani odjemalca. <ul style="list-style-type: none"> • Zaznamki podjetja so vedno uvrščeni na beli seznam • Podprto samo za 100 naslovov URL • Uporabite univerzalni prehod za neomejeno črno in belo listo
URL-ji na belem seznamu	Seznam dovoljenih naslovov URL.
Črni in beli seznam na podlagi prehodov	Za uvrstitev na črni seznam veljajo naslednje zahteve: <ul style="list-style-type: none"> • Delujoč AppTec Universal Gateway ("Splošne nastavitve" → "Universal Gateway")

- Delujoča konfiguracija VPN z določenim strežnikom DNS ("Splošne nastavitve" → "Univerzalni prehod" → "Nastavitve VPN")
- Konfiguracija črne liste ("Splošne nastavitve" → "Universal Gateway" → "Domain Blacklist")
- Veljavna povezava VPN v profilu ("Upravljanje povezav" → "VPN")

Konfiguracija sistema Android

Splošno

Pregled profila skupine (samo na ravni skupine)

Ko odprete profil skupine, dobite hiter pregled profila.

Profile Name	Default Group Profile
Operating System	Android
Created At	01.03.2021 09:52:54
Created By	John Doe
Last Change	31.08.2021 16:35:50
Changed By	John Doe
Current Profile Revision	16
Released Profile Revision (outdated)	14

Delete Profile
Reset Group Profile
Copy Profile

Ime profila	Ime profila (tukaj ga lahko spremenite)
Operacijski sistem	Operacijski sistem, za katerega je profil namenjen
Ustvarjeno na	Čas nastanka
Ustvaril je	Ustvarjalec profila
Zadnja sprememba	Čas zadnje spremembe profila
Spremenjeno s	Račun, ki je opravil zadnje spremembe
Trenutna revizija profila	Revizija stanja shranjenega profila
Objavljena revizija profila	Dodeljena revizija profila ("Assigned profile revision"). Če je za besedilom na etiketi "(zastarela)", to pomeni, da ste profil shranili, vendar ga še niste dodelili, zato bodo naprave še vedno dobile starejšo različico.

Pregled naprave (samo na ravni naprave)

Če ste v napravi, boste prejeli pregledni povzetek izbrane naprave, ki vsebuje naslednje informacije:

Ime naprave	Ime naprave
Zadnja znana lokacija	Zadnje znane koordinate GPS
Telefonska številka	Telefonska številka
Dodeljene obvezne aplikacije	Število dodeljenih obveznih aplikacij
Različica operacijskega sistema	različica operacijskega sistema naprave
Operacijski sistem	Operacijski sistem (Android / iOS / Windows Phone)
Serijska številka	Serijska številka naprave
Lastništvo naprave	Poslovna ali zasebna naprava
Vrsta naprave	Telefon ali tablični računalnik
Ukoreninjen	Stanje, ki označuje, ali je bila naprava zakoreninjena.
V skladu s predpisi	Skladnost s smernicami
Naslov IP	Naslov IP
Nazadnje videno	Točka v času, ko je bila naprava nazadnje povezana z AppTecom
Zadnji potisk	Točka v času, ko je strežnik napravi poslal potisno sporočilo.
Dodelitev uporabnika	Spustno okno za dodelitev naprave drugemu uporabniku

Revizija konfiguracije (samo na ravni naprave)

Tu boste dobili pregled nad tem, kateri profil skupine je dodeljen napravi.

Revision Overview			
	Installed Profile	Assigned Profile	Last Generated Profile
Device Profile	Device Profile: Revision 5	Device Profile: Revision 5	Device Profile: Revision 5
Group Profile	Default Group Profile: Revision 13	Default Group Profile: Revision 13 (Newer Revision available)	Default Group Profile: Revision 13

Če kliknete na profil skupine, boste neposredno dostopali do profila in opravili nastavitve.

S simbolom lahko dodeljene aplikacije vrnete v nastavitve skupinskega profila.



S tem simbolom lahko ponastavite profil naprave, tako da nima nobenih nastavitvev.

"Na voljo je novejša revizija" pomeni, da je bil profil skupine spremenjen in shranjen, vendar ni dodeljen. Profil skupine je treba dodeliti s funkcijo "Assign now" na ravni skupine, da se spremembe uporabijo v napravah.

Dnevnik naprave (samo na ravni naprave)

Dnevnik ukazov

Tu si lahko ogledate, kateri ukazi so bili izdani za napravo in kakšen je njihov status.

Command Log (last 250 commands)					
#	Created By	Date modified	Command	State	
1	jd@example.com	31.08.2021 12:21:37	Install assigned profiles	Device Pushed	
2	jd@example.com	31.08.2021 12:10:04	Get installed apps	Command Executed	
3	jd@example.com	31.08.2021 12:10:04	Get managed apps	Command Executed	
4	jd@example.com	31.08.2021 12:10:02	Get certificates	Command Executed	
5	jd@example.com	31.08.2021 12:10:02	Get asset data	Command Executed	
6	System Automated	31.08.2021 05:34:29	Update profile revision	Command Partially Failed 	
7	System Automated	31.08.2021 05:34:29	Apply device settings	Command Executed	
8	System Automated	31.08.2021 05:34:27	Install application	Command Failed 	
9	System Automated	31.08.2021 05:34:25	Get installed apps	Command Executed	
10	System Automated	31.08.2021 05:34:25	Get managed apps	Command Executed	
11	System Automated	31.08.2021 05:34:23	Get certificates	Command Executed	

Ukazi, ustvarjeni s "Sistemska avtomatizirano", se samodejno ustvarijo v sistemu.

Možni statusi ukazov

Potisnjena naprava	Storitvi za potiskanje (npr. APNS) je bila poslana potisna zahteva, da se naprava poveže nazaj s strežnikom EMM.
Ustvarjen ukaz	Ukaz je bil ustvarjen v sistemu.
Poslan ukaz	Ukaz je bil napravi poslan, ko se je povezala s strežnikom.
Izveden ukaz	Ukaz je bil uspešno izveden.
Ukaz ni uspel	Ukaz ni uspel. *
Ukaz delno ni uspel	Odvisno od operacijskega sistema naprave so lahko nekateri ukazi združeni. Pri tem nekateri deli te skupine ukazov niso bili uspešni. *
Ukaz se je izvršil, vendar je bil neuspešen	Ukaz je bil izveden, vendar morda ni bil.
Ukaz se ponovno premakne	Ukaz je ponovno poslal uporabnik.
Zavrženi	Ukaz je bil zavržen. Na primer zato, ker ga je nadomestil drug ukaz ali ker je bila naprava ponovno vpisana in so bili stari ukazi odstranjeni.

*Če je za sporočilom izklicnik, lahko več informacij dobite tako, da s kazalcem podrsate nad ikono.

Nastavitve naprave

Konfiguracija odjemalca

Tu lahko v napravi s sistemom Android izvedete naslednje konfiguracije:

Opozorilno sporočilo po onemogočitvi upravljanja naprav	Vzpostavljeno opozorilno sporočilo po onemogočanju upravljanja naprav
Čas neskladnosti	Časovni rok, po katerem se izvede "ukrep izvrševanja po skladnosti", če naprava ni skladna. Min. 1 minuta Največ. 24 ur
Izvršilni ukrepi po izteku roka za izpolnjevanje zahtev	Ukrep, ki ga je treba sprejeti takoj, ko naprava postane neskladna. <ul style="list-style-type: none"> • ne stori ničesar = brez ukrepanja • Zaklepanje naprave = naprava za zaklepanje • Brisanje naprave = naprava bo obnovljena na tovarniške nastavitve
Pogostost zbiranja podatkov	Pogostost zbiranja podatkov o napravi/GPS
Frekvenca srčnega utripa naprave	Interval, v katerem mora naprava stopiti v stik s strežnikom AppTec360 Min. 1 minuta Največ. 24 ur
Omogočanje posodobitev lokacije	Če je aktivirano, naprava pošlje posodobitve lokacije v strežnik AppTec360.
Čas posodobitve lokacije	Določa, v kakšnih časovnih intervalih naprava pošilja posodobitve lokacije AppTecu.
Uporaba Google natančnosti lokacije za posodobitev lokacije	Če je aktivirana, se bo za posodobitve lokacije uporabljala Google Location Accuracy (prej znana kot omrežna lokacija) (če je bila deaktivirana v razdelku "Omejitve", ta nastavev ne bo vplivala na nič).
Uporaba lokacije GPS za posodobitev lokacije	Če je aktivirano, se za posodobitve lokacije uporablja GPS.
Dovolite navidezne (lažne) lokacije	Omogoča ponarejanje podatkov o lokaciji prek aplikacij tretjih oseb.

Ukrep za izgubljeno povezavo	Omogoča nastavitve določenega dejanja, ki se izvede po določenem številu neuspešnih srčnih utripov.
Način uveljavljanja politik	Določa, kako agresivno odjemalec AppTec360 od uporabnika zahteva, da izvede določena dejanja, ki zahtevajo vnos uporabnika. Interval (privzeto) = sprašuje v intervalih, tako da lahko uporabnik to za nekaj časa pusti v ozadju. Brez opozorila = ni pojavnega okna za zahtevano interakcijo. Odjemalca AppTec360 morate odpreti ročno, da preverite, ali je potrebno ukrepanje. Stalno opozorilo = Uporabnik lahko izvede le zahtevano dejanje. Odjemalec AppTec360 se bo vsilil v ospredje, če se mu bo uporabnik poskušal izogniti
Zaklepanje različice AppTec360	Omogoča opredelitev različice odjemalca AppTec360, ki je največja različica, na katero se odjemalec posodobi.

Ozadje

Tu lahko določite ozadje po meri.

"Določite barvo" vam omogoča, da določite barvo v šestnajstiškem formatu (npr. #000000). Dovoljene so samo šestnajstiške vrednosti.

"Nastavi sliko kot ozadje" vam omogoča, da naložite sliko. Upoštevajte, da različne naprave z različnimi zaganjalniki in različicami operacijskega sistema delujejo različno. Splošnih navodil za velikost in razmerje ni, saj je to odvisno od naprave.

Za format datoteke uporabite JPG (ali JPEG) ali PNG.

Upravljanje sredstev (samo na ravni naprave)

Upravljanje sredstev

Informacije o napravi

Model	Oznaka modela naprave
Operacijski sistem	OS
Različica operacijskega sistema	Različica operacijskega sistema
Podpora AE	Podpora za Android Enterprise (vsebnik in popolnoma upravljan)
Serijska številka	Serijska številka
Ime naprave	Ime naprave
Stanje baterije	Stanje baterije
Prosti / skupni pomnilnik	Prosti / skupni pomnilnik
Samsung KNOX	Samsung KNOX Raven API
Na voljo je kartica SD	Na voljo je kartica SD
Emulirana kartica SD	Emulirana kartica SD
Kartica SD Odstranljiva	Odstranljiva kartica SD
SD Prosti / skupni pomnilnik	SD Prosti / skupni pomnilnik kartice SD

Wi-Fi

Naslov IP	Naslov IP naprave
WiFi MAC	Naslov WiFi MAC

Cellular

Status	Stanje (nameščena kartica SIM)
Telefonska številka	Telefonska številka
Gostovanje (glasovno/podatkovno)	Gostovanje za prenos govora/podatkov
Status gostovanja	Trenutni status gostovanja
Naslov IP	Naslov IP
Operater/prevoznik	Operater/prevoznik
Celična tehnologija	Celična tehnologija
IMEI	Številka IMEI
ICCID	To je identifikacijska oznaka za kartico SIM, pogosto tudi pametno kartico ali kartico z integriranim vezjem (ICC).
IMSI	<p>Mednarodna identiteta mobilnega naročnika (IMSI) v mobilnih omrežjih GSM in UMTS zagotavlja natančno identifikacijo uporabnikov omrežja. IMSI je sestavljen iz največ 15 števil in je konfiguriran na naslednji način:</p> <ul style="list-style-type: none"> • <u>Koda mobilne države (MCC)</u>, 3 števke • <u>Koda mobilnega omrežja (MNC)</u>, 2 ali 3 števke • Identifikacijska številka mobilnega naročnika (MSIN), 1-10 števil
Trenutni MCC/MNC	Glejte "SIM MCC/MNC".
SIM MCC/MNC	<p>Koda mobilne države je uveljavljena identifikacijska oznaka države, ki jo je določila ITU v skladu s standardom E.212. Uporablja se skupaj s kodo mobilnega omrežja (MNC) za identifikacijo mobilnega omrežja. Pomeni kodo države/mobilnega omrežja kartice SIM. Če gostujete v drugem mobilnem omrežju, bosta logično "trenutni MCC/MNC" in "SIM MCC/MNC" različna.</p>

Bluetooth

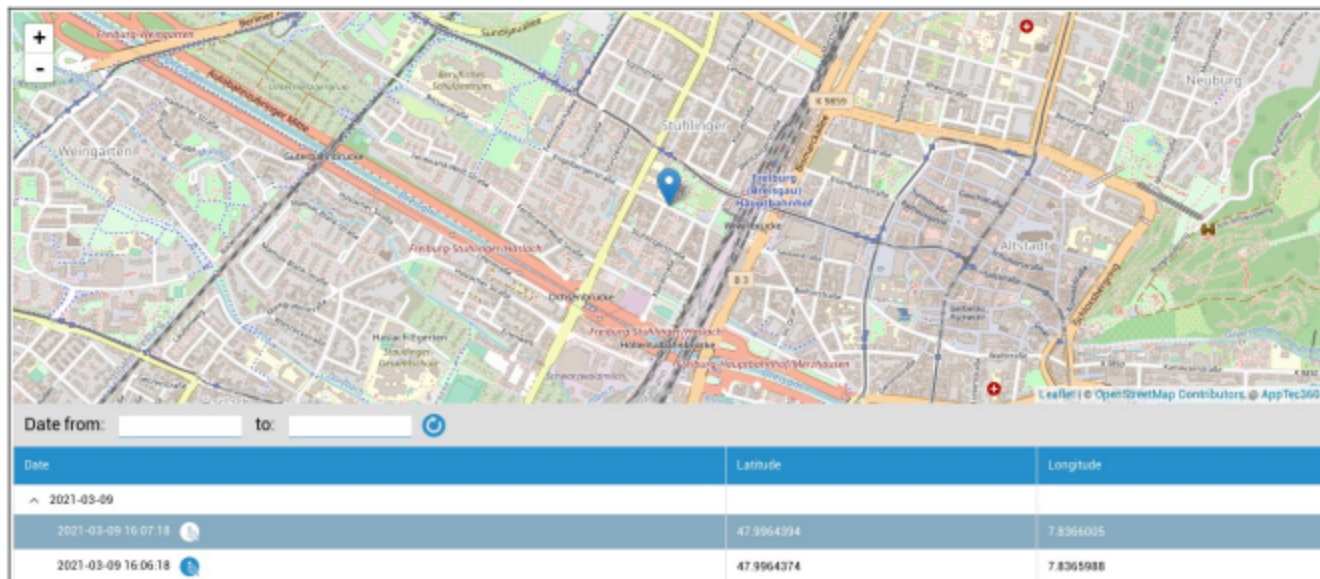
Bluetooth MAC	Naslov MAC Bluetooth
---------------	----------------------

Upravljanje varnosti

Zaščita pred krajo (samo na ravni naprave)

Informacije GPS (samo na ravni naprave)

Tu lahko določite trenutno/ zadnjo lokacijo naprave. Lokalizacijo lahko zaščitite z enim ali celo dvema gesloma - glejte: Splošne nastavitve - Zasebnost - Dostop do GPS



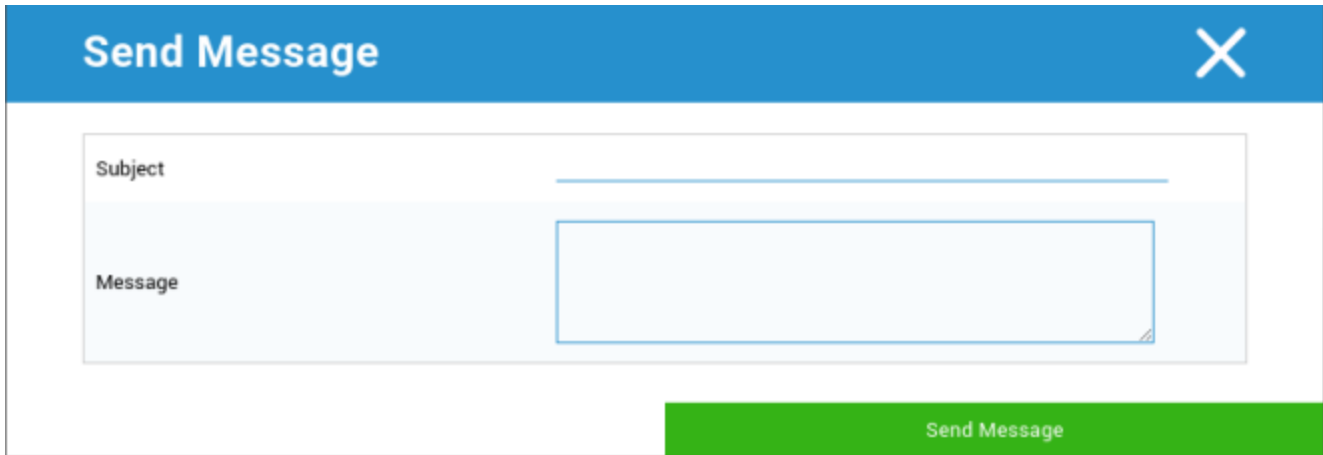
Brisanje in zaklepanje (samo na ravni naprave)

V razdelku "Brisanje in zaklepanje" lahko izvedete naslednja tri dejanja:

Celotno brisanje	Naprava je obnovljena na tovarniške nastavitve (izbrisani so tako poslovni kot osebni podatki).
Izbris podjetja	Iz naprave končnega uporabnika se odstranijo samo podatki podjetja (vse aplikacije, podatki itd., ki jih je zagotovil AppTec360)
Zaklepanje zaslona	Zaklepanje zaslona je aktivirano, napravo je treba odkleniti z geslom naprave/PIN.

Sporočilo (samo na ravni naprave)

Vnesete lahko predmet in sporočilo ter ga pošljete v napravo končnega uporabnika. To sporočilo bo prikazano v odjemalcu AppTec360.



The screenshot shows a 'Send Message' dialog box. It features a blue header bar with the text 'Send Message' on the left and a white 'X' icon on the right. The main content area is white and contains two input fields: a 'Subject' field with a single-line text input and a 'Message' field with a multi-line text area. At the bottom right of the dialog, there is a prominent green button with the text 'Send Message'.

Varnostna konfiguracija

Pristopna koda

V razdelku "Geslo" lahko pooblastite geslo naprave, na voljo so naslednje možnosti nastavitvev

Najmanjša dolžina gesla	določa najmanjše število simbolov, ki jih mora imeti geslo.
Kakovost gesla	Moč gesla Neopredeljeno = ni opredeljeno Vsako geslo je v redu = vsako geslo je sprejemljivo vsaj številčni znaki = vsebovati mora vsaj številčne znake vsaj kompleksni znaki = vsebovati mora vsaj posebne znake vsaj alfanumerični znaki = vsebovati mora vsaj alfanumerične znake vsaj abecedni znaki = vsebovati mora vsaj abecedne znake
Zaklepanje največjega časa neaktivnosti	Najdaljši čas trajanja zaslona. S tem se konfigurira samo največja vrednost, ki jo lahko izbere uporabnik.
Najmanjše število malih črk v geslu	Najmanjše število malih črk v geslu
Najmanjše število velikih tiskanih črk v geslu	Najmanjše število velikih tiskanih črk v geslu
Najmanjši zahtevani črkovni znaki v geslu	Najmanjši zahtevani črkovni znaki v geslu
Najmanjše število števil v geslu	Najmanjše število števil v geslu
Najmanjši zahtevani simboli v geslu	Najmanjši zahtevani simboli v geslu
Časovna omejitev izteka gesla	vzpostavi, po tem časovnem intervalu geslo preneha veljati in je treba izdati novo geslo.
Omejitev zgodovine gesel	Število predhodno uporabljenih gesel, ki niso dovoljena
Največ neuspešnih poskusov gesla	določa, kolikokrat je mogoče napačno vnesti geslo, preden se izvede popolno brisanje naprave.

Šifriranje

Na tej točki lahko šifirate notranji pomnilnik naprave in pomnilnik kartice SD.

Zahtevajte šifriranje shranjevanja	Če je ta nastavev aktivirana, bo pomnilnik naprave šifriran, če naprava podpira to funkcijo. Ko je pomnilnik naprave prvič šifriran, ga ni več mogoče dešifrirati. Prav tako se politika gesla samodejno preklopi na 6 alfanumeričnih simbolov.
Zahtevajte šifriranje kartice SD	Ta nastavev velja samo za naprave Samsung! Če je ta nastavev aktivirana, je mogoče zunanjo kartico SD šifrirati in jo je mogoče ročno odšifrirati samo v napravi končnega uporabnika. Prav tako se politika gesla samodejno preklopi na 6 alfanumeričnih simbolov.

AntiVirus

Če omogočite AntiVirus, bo v naprave nameščen program Ikarus. Upoštevajte, da je za to potrebna ločena licenca, ki jo lahko vnesete v Splošne nastavitve → Upravljanje aplikacij → Aplikacije tretjih oseb.

Samodejno skeniranje	Določa, ali Ikarus samodejno pregleduje in kako pogosto izvaja to pregledovanje. Če omogočite možnost "Popolno samodejno pregledovanje", bo opravljeno popolno pregledovanje. V nasprotnem primeru se izvede hitro pregledovanje.
Samodejne posodobitve	Omogoča samodejno posodabljanje podatkovne zbirke virusov in določa pogostost posodabljanja.
Zaščita aplikacij	Omogoča skeniranje aplikacij poleg običajnega skeniranja, ki skenira samo datoteke.
Zaščita kartice SD	Omogoča zaščito kartice SD. Brez tega je pregledovanje omejeno na lokalni pomnilnik.
Posodobitev samo za Wi-Fi	Omejitve posodabljanja na omrežje Wi-Fi

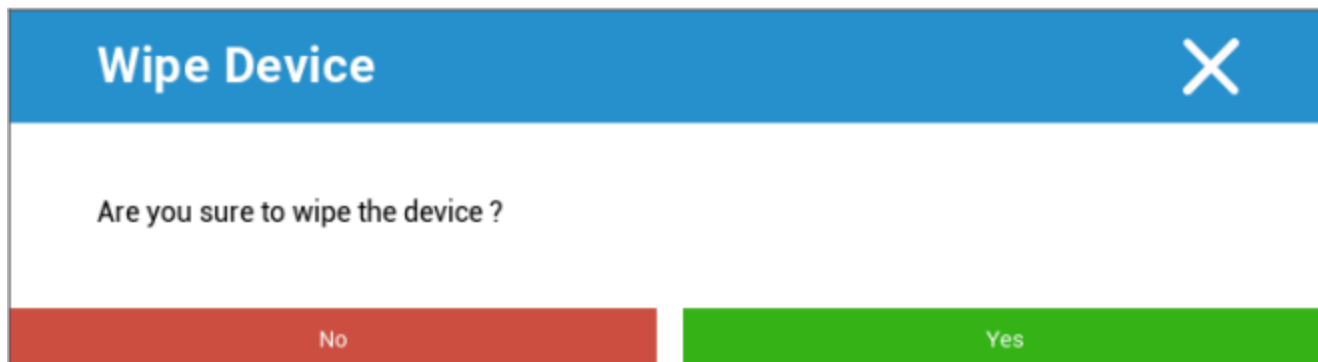
Konec življenjske dobe (samo na ravni naprave)

Brisanje (samo na ravni naprave)

V razdelku "Brisanje" lahko obnovite tovarniške nastavitve naprave. Pri tem bodo v napravi končnega uporabnika izbrisani poslovni in zasebni podatki.

S klikom na simbol Minus se prikaže naslednje sporočilo

Izbrišite tudi kartico SD?	Izbrisan bo tudi pomnilnik kartice SD.
----------------------------	--



Z "Da" lahko izvedete brisanje.

V razdelku "Poročilo o brisanju" lahko prikažete naslednje elemente

Izbrisano z	Zgodovina izvajalca brisanja
Datum	Datum
Status	Status (npr. če je bilo brisanje uspešno izvedeno)

Nastavitve omejitev

Omejitve

Tu lahko omejite in blokirate različne stvari.

Omogoči kamero	Dovolite uporabo fotoaparata
Izvršite samodejno sinhronizacijo	Nanaša se na vmesnik "Sinhronizacija". Vključeno = sinhronizacija je trajno aktivirana Izključeno = sinhronizacija je trajno deaktivirana Izbira uporabnika = izbere ga uporabnik
Sila Bluetooth	Vključeno = Bluetooth je trajno aktiviran Izključeno = Bluetooth je trajno deaktiviran Izbira uporabnika = izbere ga uporabnik
Sila GPS	Vključeno = GPS je stalno aktiviran Izključeno = GPS je trajno deaktiviran Izbira uporabnika = izbere ga uporabnik
Izvršite Google Location Accuracy (Natančnost lokacije Google)	Vključeno = stalno internetno lociranje Izključeno = trajna deaktivacija internetnega lociranja Izbira uporabnika = izbere ga uporabnik

Za naprave Samsung z vmesnikom KNOX 1.0 ali novejšim so na voljo naslednje možnosti nastavitvev.

Dovolite kartico SD	Dovolite kartico SD
Dovolite zapis na kartico SD	Dovolite "pisanje" na kartico SD
Omogočite zajem zaslona	Omogočite zajem zaslona
Omogočite uporabo odložišča	Omogočite uporabo odložišča
Varnostno kopiranje nastavitvev in podatkov aplikacije v Google Cloud	Izklopljeno = deaktiviranje varnostnega kopiranja Google Vključeno = aktiviranje varnostnega kopiranja Google Izbira uporabnika = izbere ga uporabnik
Omogočanje razhroščevanja USB	Omogoči razhroščevanje USB (uporablja se na primer za ustvarjanje dnevnikov naprav (ADB)).
Dovolite poročilo o trku Google	Omogočanje pošiljanja poročila o nesreči Google iz aplikacij
Dovolite ponastavitvev tovarniške nastavitve	Uporabniku omogoča, da obnovi tovarniške nastavitve naprave.
Omogočanje nadgradnje OTA	Omogočanje posodobitev "over-the-Air"
Omogočanje shranjevanja v gostitelja USB	Če je aktiviran, lahko priključite pomnilnik USB v obliki trdega diska ali bralnika kartic SD.
Dovolite predvajalnik medijev USB (MTP, PTP)	Dovolite predvajalnik medijev USB (MTP, PTP)
Dovolite mikrofona	Vključeno = dovolite mikrofona za aplikacije tretjih oseb Izklopljeno = blokiranje mikrofona za aplikacije tretjih oseb Izbira uporabnika = uporabniki lahko izberejo, če ima aplikacija tretje osebe dostop do mikrofona.
Omogočite NFC (Near Field Communication)	Dovolite NFC
Dovolite neznane vire (Sideloadng APK)	Če je omogočeno, je stransko nalaganje aplikacij (datotek APK) dovoljeno. Ko je ta nastavev onemogočena, jo mora uporabnik omogočiti ročno, ko ponovno dovolite namestitev datotek APK iz neznanih virov.
Omogočanje ustvarjanja uporabnikov	Omogoča ustvarjanje več uporabnikov

Lastnik naprave AE

(Naprava mora biti v načinu lastnika naprave Android Enterprise) Priporočljivo je, da naprave ustvarite kot napravo "Android Enterprise" in ne kot napravo "Android".

Varnost	
Prepovedati skupno rabo Lokacija	Določa, ali je uporabniku prepovedano vklopiti skupno rabo lokacije.
Prepoved varnega zagona	Določa, ali uporabnik ne sme ponovno zagnati naprave v varni zagonski način.
Prepoved ponastavitve omrežja	Določa, ali je uporabniku onemogočeno ponastavljanje omrežnih nastavitev iz Nastavitev.
Prepoved ponastavitve tovarniških nastavitev	Določa, ali je uporabniku prepovedana ponastavitev naprave.
Omogočanje ADB	Omogoča povezavo z računalnikom prek ADB
Onemogočanje varovala ključev	Onemogoči varovanje ključev
Lastnik naprave Informacije o zaklenjenem zaslonu	Nastavitev informacij o lastniku naprave, ki se prikažejo na zaklenjenem zaslonu.
Izvrševanje skladnosti	Način Poziv uporabniku - uporabnik bo pozvan, da izvede potrebna dejanja. Kontejner za zaklepanje načina - skrijte vse aplikacije, dokler niso izpolnjene vse zahteve

Upravljanje aplikacij	
Omogočanje povezovanja aplikacij med profili	Aplikacijam v nadrejenem profilu omogoča, da obdelujejo spletne povezave iz upravljanega profila.
Prepovedati nadzor aplikacij	Določa, ali je uporabniku prepovedano spreminjanje aplikacij v nastavitvah ali zaganjalnikih.
Prepoved namestitve aplikacije	Določa, ali je uporabniku onemogočeno nameščanje aplikacij.
Onemogočanje odstranitve aplikacij	Določa, ali je uporabniku onemogočeno odstranjevanje aplikacij.
Pravilnik o dovoljenjih za izvajanje	Določa, kako bodo obravnavane nove zahteve za dovoljenja iz aplikacij.
Dovolite neznane vire	Če je ta možnost omogočena, lahko uporabniki z namestitvijo datoteke .apk prenesejo aplikacije na drugo stran.

Povezljivost	
Prepoved konfiguracije mobilnega omrežja	Določa, ali je uporabniku prepovedano konfiguriranje mobilnih omrežij.
Konfiguracija prepovedi privezovanja	Določa, ali je uporabniku prepovedano konfigurirati Tethering in prenosne dostopne točke.
Prepovedati konfiguracijo VPN	Določa, ali je uporabniku onemogočeno konfiguriranje omrežja VPN.
Prepovedati konfiguracijo Wifi	Določa, ali je uporabniku onemogočeno spreminjanje dostopnih točk WiFi.
Prepovedati odhodni žarek NFC	Določa, ali uporabnik ne sme uporabljati NFC za prenos podatkov iz aplikacij.
Zaklepanje konfiguracije WiFi	Ta nastavitev določa, ali naj bodo konfiguracije WiFi, ki jih ustvari aplikacija lastnika naprave, zaklenjene (to pomeni, da jih lahko ureja ali odstrani samo aplikacija lastnika naprave, ne pa tudi aplikacija Nastavitve).
Omogočanje podatkovnega gostovanja	Aktivacija podatkovnega gostovanja

Bluetooth	
Prepovedati Bluetooth	Določa, ali je bluetooth v napravi prepovedan. Zahteva operacijski sistem Android 8.0
Prepoved souporabe Bluetooth	Določa, ali je v napravi onemogočena odhodna souporaba bluetooth. Zahteva operacijski sistem Android 8.0
Prepovedati konfiguracijo Bluetooth	Določa, ali je uporabniku prepovedano konfigurirati bluetooth.

Upravljanje računa	
Prepoved dodajanja upravljanega profila	Določa, ali je uporabniku prepovedano dodajanje upravljanih profilov. Zahteva Android 8.0
Prepoved dodajanja uporabnikov	Določa, ali je uporabniku prepovedano dodajanje novih uporabnikov.
Prepoved Odstranitev upravljanega profila	Določa, ali je mogoče upravljane profile tega uporabnika odstraniti, razen če jih odstrani lastnik profila. Zahteva Android 8.0
Prepoved spreminjanja računa	Določa, ali je uporabniku prepovedano dodajanje in odstranjevanje računov, razen če jih programsko doda Authenticator.

Telefonija	
Prepoved odhodnih klicev	Določa, da uporabniku ni dovoljeno opravljati odhodnih telefonskih klicev.
Prepovedati sporočila SMS	Določa, da uporabnik ne sme pošiljati ali prejemati sporočil SMS.

Sistem	
Prepoved ustvarjanja oken	Določa, da se okna poleg oken aplikacije ne smejo ustvariti.
Prepovedati nastavitve ikone uporabnika	Določa, ali uporabnik ne sme spreminjati svoje ikone.
Prepoved nastavitve ozadja	Omejitev uporabnika, ki onemogoča nastavitve ozadja.
Onemogočite vrstico stanja	Onemogočanje vrstice stanja blokira obvestila, hitre nastavitve in druge prekrivne zaslone, ki omogočajo pobeg iz naprave za enkratno uporabo.
Omogoči samodejni čas	Samodejno nastavi čas.
Omogočanje samodejnega časovnega pasu	Samodejno nastavi časovno območje.
Ostanite vklopljeni, ko ste priključeni v električno omrežje	Naprava ostane aktivna, ko je priključena na vir napajanja.

Shranjevanje	
Onemogočanje onemogočanja preverjanja aplikacij	Določa, ali je uporabniku prepovedano onemogočiti preverjanje aplikacij.

Prepoved priklopa fizičnega medija	Določa, ali je uporabniku onemogočeno nameščanje fizičnih zunanjih medijev.
Omogočite storitev varnostnega kopiranja	Storitev varnostnega kopiranja upravlja vse mehanizme varnostnega kopiranja in obnovitve v napravi. Če to nastavite na false, preprečite varnostno kopiranje ali obnovitev podatkov. Storitev varnostnega kopiranja je privzeto izklopljena. Zahteva operacijski sistem Android 8.0
Omogočite masovni pomnilnik USB	Omogoča uporabo masovnega pomnilnika USB.

Tipkovnica

Prepovedati samodejno izpolnjevanje	Določa, ali uporabnik ne sme uporabljati storitev samodejnega izpolnjevanja. Zahteva Android 8.0
Prepoved kopiranja in lepljenja med profili	Določa, ali je mogoče kopirano v odložišče tega profila prilepiti v povezane profile.

Zvok

Prepoved prilagoditve obsega	Določa, ali je uporabniku prepovedano prilagajanje glavne glasnosti.
Prepoved izklopa mikrofona	Določa, ali je uporabniku onemogočeno prilagajanje glasnosti mikrofona.
Naprava za utišanje zvoka	Naprava za utišanje zvoka.

Politika posodabljanja sistema

Nadzor nad posodobitvami operacijskega sistema	Omogočite to možnost, če želite nastaviti obnašanje posodobitve na samodejno, okensko ali odloženo.
--	---

Zabojnik BYOD

Android Enterprise

Android Enterprise

Omogočanje sistema Android Enterprise	Omogočite Android Enterprise (AE). AE je podprta od različice Android 5.1 naprej.
Izvrševanje skladnosti	Način Poziv uporabniku - uporabnik bo pozvan, da izvede potrebna dejanja. Kontejner za zaklepanje načina - skrijte vse aplikacije, dokler niso izpolnjene vse zahteve
Pravilnik o dovoljenjih za izvajanje	Poziv uporabniku za nove zahteve za dovoljenja Vedno odobri nove zahtevke za nova dovoljenja Vedno zavrnite nove zahteve za dovoljenje Opozorilo: Nekatero aplikacije imajo težave s prepoznavanjem dovoljenj, če so ta nastavljena samodejno. Če vedno podeljujete dovoljenja in imate težave z aplikacijami, ki trdijo, da dovoljenja manjkajo, to nastavite na "pozvati uporabnika" in ponovno namestite aplikacijo.
Dovolite odhodno odložišče	Omogoča kopiranje in lepljenje iz notranjosti vsebnika na zunanjo stran
Omogočanje razreševanja ID klicatelja	Prikaže ime dohodnega klica na podlagi stikov v vsebniku
Omogočanje rešitve iskanja stikov	Omogoča iskanje imen v vsebniku za stike med klicanjem.
Omogočanje souporabe stikov Bluetooth	Omogoča dostop do stika z zabojnikom v avtomobilu
Prepovedati odhodni žarek NFC	Onemogoči NFC za zabojnik
Dovolite neznane vire	Če je ta možnost omogočena, lahko uporabniki z namestitvijo datoteke .apk prenesejo aplikacije na drugo stran.
Omogočanje razhroščevanja USB	Če je omogočeno, lahko uporabniki omogočijo razhroščevanje USB.
Prepoved spreminjanja računa	Prepoved ustvarjanja, brisanja in spreminjanja računov v vsebniku

Upoštevajte, da morajo nekatere aplikacije ustvariti ali spremeniti račune, da delujejo, kot je bilo pričakovano.

Gmail Exchange

Omogoča konfiguracijo storitve Gmail v vsebniku. Upoštevajte, da omogočanje te konfiguracije ne pomeni samodejne namestitve aplikacije. Še vedno morate to aplikacijo dodati kot obvezno aplikacijo.

Elektronski naslov	Elektronski naslov
Gostiteljsko ime strežnika	Gostiteljsko ime strežnika
Prijavno ime	Prijavno ime
Podpis	Podpis
Število prejšnjih dni za sinhronizacijo	Število prejšnjih dni za sinhronizacijo.
Identifikator naprave	Identifikator EAS. Pustite to polje prazno, če vaše okolje tega ne zahteva.
Uporabite Secure Sockets Layer (SSL)	Omogoča uporabo protokola SSL. Če to onemogočite, se lahko zmanjša varnost.
Sprejmite vsa potrdila	Sprejema vsa potrdila. Če to omogočite, se lahko zmanjša varnost
Dovoli neupravljanje račune	Uporabniku omogoča dodajanje dodatnih računov
Potrdilo stranke	Naložite potrdilo odjemalca, če strežnik Exchange to zahteva

Aplikacije sistema AE

Tu lahko omogočite sistemske aplikacije za zabojnik Android Enterprise Container. Upoštevajte, da mora biti določena aplikacija v shrambi sistema, sicer se ne zgodi nič.

Pristopna koda zabojnika

Samo za operacijski sistem Android 7.0 ali novejši

Omogoča nastavitve posebne zahteve za geslo za vsebnik.

Najmanjša dolžina gesla	določa najmanjše število simbolov, ki jih mora imeti geslo.
Kakovost gesla	Moč gesla Neopredeljeno = ni opredeljeno Vsako geslo je v redu = vsako geslo je sprejemljivo vsaj številčni znaki = vsebovati mora vsaj številčne znake vsaj kompleksni znaki = vsebovati mora vsaj posebne znake vsaj alfanumerični znaki = vsebovati mora vsaj alfanumerične znake vsaj abecedni znaki = vsebovati mora vsaj abecedne znake
Zaklepanje največjega časa neaktivnosti	Najdaljši čas do zaklepanja posode. S tem se nastavi samo največja vrednost, ki jo lahko izbere uporabnik.
Najmanjše število malih črk v geslu	Najmanjše število malih črk v geslu
Najmanjše število velikih tiskanih črk v geslu	Najmanjše število velikih tiskanih črk v geslu
Najmanjši zahtevani črkovni znaki v geslu	Najmanjši zahtevani črkovni znaki v geslu
Najmanjše število števil v geslu	Najmanjše število števil v geslu
Najmanjši zahtevani simboli v geslu	Najmanjši zahtevani simboli v geslu
Časovna omejitev izteka gesla	vzpostavi, po tem časovnem intervalu geslo preneha veljati in je treba izdati novo geslo.
Omejitev zgodovine gesel	Število predhodno uporabljenih gesel, ki niso dovoljena
Največ neuspešnih poskusov gesla	določa, kolikokrat je mogoče napačno vnesti geslo, preden se vsebnik izbriše.

Samsung KNOX

Aktivacija

Tu lahko omogočite vsebnik Samsung KNOX. Upoštevajte, da Samsung tega na operacijskem sistemu Android 10 ali novejšem ne podpira več. Uporaba vsebnika Android Enterprise Container v operacijskem sistemu Android 10 ali novejšem

Pristopna koda Knox

Določite smernice, ki se nanašajo na nastavitve gesla naprave

Najmanjša dolžina gesla	določa, koliko simbolov mora imeti geslo.
Kakovost gesla	Moč gesla Vsako geslo je v redu = Vsako geslo je v redu Vsaj številčni znaki = prisotni morajo biti najmanj številčni znaki Vsaj kompleksni znaki = prisotni morajo biti najmanj posebni znaki Vsaj alfanumerični znaki = prisotni morajo biti najmanj alfanumerični znaki Vsaj abecedni znaki = Najmanj abecednih znakov mora biti prisotnih
Najmanjši zahtevani kompleksni znaki	Prisotni morajo biti najmanj kompleksni znaki.
Največji čas neaktivnosti	Najdaljši čas nedejavnosti uporabnika pred zaklepanjem tipkovnice
Omogočite preverjanje pristnosti s prstnim odtisom	Omogočanje avtentikacije s prstnimi odtisi
Omogočanje avtentikacije Iris	Omogočanje avtentikacije s prepoznavo šarenice
Največja starost gesla	določa, po katerem času geslo poteče in je treba izdati novo geslo.
Zgodovina shranjenih gesel	Število nekdanjih gesel, ki niso dovoljena
Največ neuspešnih poskusov gesla	določa, kolikokrat je mogoče napačno predložiti geslo, preden se izvede popolno brisanje naprave.

Knox Security

Omejitev določenih funkcij naprave

Omogoči kamero	Dovolite uporabo fotoaparata
Dovolite trgovino z aplikacijami Samsung KNOX	Omogočanje uporabe trgovine Samsung KNOX App Store
Dovolite storitve Google Play	Dovolite storitve Google Play
Dovolite brskalnik	Omogočanje uporabe domačega brskalnika
Dovoli posnetke zaslona	Omogočanje ustvarjanja posnetkov zaslona
Dovoli uvoz stikov	Če je aktivirano, je omogočen dostop do stikov naprave iz vsebnika KNOX.

Omogočite izvoz stikov	Če je aktivirano, je omogočen dostop do stikov KNOX iz naprave.
Dovoli uvoz koledarja	Če je aktivirano, je dovoljen dostop do koledarja naprave iz vsebnika KNOX.
Omogočite izvoz koledarja	Če je aktivirano, je dovoljen dostop do koledarja KNOX iz naprave.
Dovoli nezaščiteno tipkovnico	Omogočanje uporabe nezavarovane tipkovnice
Omogočite uvoz datotek	Omogočanje uvoza datotek v vsebnik KNOX
Omogočite izvoz datotek	Omogočanje izvoza datotek iz vsebnika KNOX

Knox Exchange

Tukaj lahko konfigurirate profil Exchange za vsebnik KNOX

E-poštni naslov	e-poštni naslov uporabnika Upoštevajte "Namestnike", ki jih lahko uporabite za delo s poverilnicami in ne izvajate sprememb ročno v vsaki napravi. S klikom na Prikaži nadomestne elemente jih lahko prikažete sami.
Gostiteljsko ime strežnika	Strežniški naslov strežnikov Exchange
Prijavno ime	Prijavno ime za zadevno napravo končnega uporabnika, upoštevajte tudi "Namestna imena".
Domena	Naslov domene
Geslo (samo na ravni naprave)	Po želji lahko posamezni napravi določite geslo; če to ostane prazno, bo uporabnik pozvan, da vnese svoje geslo Exchange.
Število prejšnjih dni za sinhronizacijo	Število dni, ki določajo, kdaj se e-poštna sporočila sinhronizirajo nazaj
Podpis	Priloži se lahko podpis.
Privzeti račun	ugotovi, da je ta e-poštni račun standardni račun.
Uporabite Secure Sockets Layer (SSL)	Uporaba povezave SSL
Uporaba protokola TLS (Transport Layer Security)	Uporaba povezave TLS
Sprejmite vsa potrdila	Sprejemajo se vsa potrdila. Izberite to možnost, če vaš strežnik Exchange uporablja samopodpisano potrdilo.

Elektronska pošta Knox

E-poštni naslov	e-poštni naslov uporabnika Upoštevajte "Namestnike", ki jih lahko uporabite za delo s poverilnicami in ne izvajate sprememb ročno v vsaki napravi. S klikom na Prikaži nadomestne elemente jih lahko prikažete sami.
Protokol dohodnega strežnika	Protokol dohodnega strežnika IMAP ali POP
Naslov dohodnega strežnika	Naslov dohodnega strežnika
Vhodna vrata strežnika	Vhodna vrata strežnika
Prijavno/uporabniško ime dohodnega strežnika	Prijavno/uporabniško ime dohodnega strežnika
Geslo dohodnega strežnika	Geslo dohodnega strežnika
Dohodni strežnik uporablja SSL	Dohodni strežnik uporablja SSL
Dohodni strežnik uporablja TLS	Dohodni strežnik uporablja TLS
Dohodni strežnik sprejme vsa potrdila	Dohodni strežnik sprejema vse vrste potrdil
Protokol odhodnega strežnika	Protokol odhodnega strežnika SMTP
Odhodna vrata strežnika	Odhodna vrata strežnika
Odhodni strežnik uporablja dodatne poverilnice	Dodatne poverilnice za odhodni strežnik. Če je nastavljena na "izklopljeno", se uporabijo nastavitve dohodnega strežnika.
Prijava/uporabniško ime odhodnega strežnika	Prijava/uporabniško ime odhodnega strežnika
Geslo odhodnega strežnika	Geslo odhodnega strežnika
Odhodni strežnik uporablja SSL	Odhodni strežnik uporablja SSL
Odhodni strežnik uporablja TLS	Odhodni strežnik uporablja TLS
Odhodni strežnik sprejme vsa potrdila	Odhodni strežnik sprejema vse vrste potrdil
Podpis	Tu lahko priložite podpis.
Obveščanje uporabnika o prejemu nove e-pošte	Obveščanje uporabnika o prejemu nove e-pošte

Aplikacije Knox

Tu vzpostavite aplikacije, ki jih želite distribuirati v naprave končnih uporabnikov. Te bodo nato na voljo v vsebniku KNOX. Če želite dodati aplikacijo, postopajte kot v meniju Obvezne aplikacije

Ime aplikacije	Ime aplikacije
Obvezno od	Točka v času, ko je bila aplikacija dodana
Vir:	Vir aplikacije (Trgovina Play Lastni vir)

S klikom na simbol lahko zadevno aplikacijo ponovno odstranite.

Upravljanje povezav

Wifi

Za to nastavitve opravite predhodno konfiguracijo naprav končnega uporabnika za dostop do notranjih dostopnih točk.

Identifikator nabora storitev (SSID)	SSID za omrežje, ki ga želite povezati
Skrito omrežje	Aktiviraj, če AP ne oddaja SSID.
Vrsta varnosti	Določite varnostno vrsto AP

Vrsta varnosti

WEP

Geslo	Geslo za AP
-------	-------------

WPA/WPA2

Geslo	Geslo za AP
-------	-------------

802.1x EAP

Metoda EAP	
-------------------	--

PWD	Identiteta	Identiteta
	Geslo	Geslo

PEAP	Protokol za preverjanje pristnosti faze 2	ni	Brez dodatnega protokola
------	---	----	--------------------------

		MSCHAPV2	Protokol MSCHAPV2
		GTC	Protokol GTC
	Potrdilo CA	Potrdilo CA	
	Identiteta	Identiteta	
	Anonimna identiteta	Anonimna identiteta	
	Geslo	Geslo	

Metoda EAP	
-------------------	--

TTLS	Protokol preverjanja pristnosti v fazi 2	ni	Brez dodatnega protokola	
		PAP	Protokol PAP	
		MSCHAP	Protokol MSCHAP	
		MSCHAPV2	Protokol MSCHAPV2	
		GTC	Protokol GTC	
		Potrdilo CA	Potrdilo CA	
		Identiteta	Identiteta	
		Anonimna identiteta	Anonimna identiteta	
		Geslo	Geslo	

TLS	Potrdilo CA	Potrdilo CA	
	Identiteta	Identiteta	
	Geslo	Geslo	

VPN

Vrsta povezave	Vzpostavitev vrste povezave VPN
-----------------------	--

Če kot vrsto VPN izberete "Per-App VPN", se razpoložljivi odjemalci VPN spremenijo. Funkcija Per-App VPN omejuje VPN na določene aplikacije in samodejno zažene povezavo VPN, če se zažene določena aplikacija.

Odjemalec AppTec360 VPN	Uporablja odjemalca AppTec360 VPN v kombinaciji z univerzalnim prehodom
-------------------------	---

Ime povezave	Ime povezave VPN
Konfiguracija vrat	Izberite konfiguracijo VPN univerzalnega prehoda
Vedno vključen VPN	Prisili VPN, da je vedno aktiven, tako da ves promet poteka prek VPN.
Omogočanje funkcije Native Lockdown	Blokira vsa omrežja, kadar naprava ni povezana z omrežjem VPN. To uporabljajte previdno, saj lahko povzroči popolno izgubo povezave, če ni pravilno konfigurirana. Samo za podjetja z operacijskim sistemom Android 7 ali novejšim
Omogočite zaklepanje aplikacije AppTec360	Blokira uporabo vseh aplikacij, dokler se ne začne povezava VPN.

Cisco AnyConnect	
Ime povezave	Ime povezave VPN
Strežnik	Naslov strežnika
Način potrdila	Onemogočeno = deaktivirano Samodejno = samodejno

L2TP (samo KNOX)	Na voljo samo v napravah Samsung
Ime povezave	Ime povezave
Strežnik	Naslov strežnika
Omogočite L2TP Secret	
DNS Iskanje domen	Iskanje domen DNS

Vrsta povezave	Vzpostavitev vrste povezave VPN
-----------------------	--

PPTP (samo KNOX)	Na voljo samo v napravah Samsung
Ime povezave	Ime povezave VPN
Strežnik	Naslov strežnika
Omogoči šifriranje	Omogočite šifriranje
DNS Iskanje domen	Iskanje domen DNS

L2TP / IPSec PSK (samo KNOX)	Na voljo samo v napravah Samsung
Ime povezave	Ime povezave VPN
Strežnik	Naslov strežnika
Predhodni zaupni ključ IPSec	Predhodno zaupni ključ za preverjanje pristnosti
Omogočite L2TP Secret	
Skrivnost L2TP	
DNS Iskanje domen	Iskanje domen DNS

IPSec XAuth PSK (samo KNOX)	Na voljo samo v napravah Samsung
Ime povezave	Ime povezave VPN
Strežnik	Naslov strežnika
Identifikator IPSec	Uporabniško ime za povezavo
Predhodni zaupni ključ IPSec	Geslo za povezavo
DNS Iskanje domen	Iskanje domen DNS

OpenVPN	
Ime povezave	Ime povezave

Profil OpenVPN	Tu se kopira vsebina datoteke .ovpn
Aplikacija OpenVPN	Za uporabo OpenVPN obstajata dve različni aplikaciji Priporočamo aplikacijo OpenVPN za Android. Druga možnost je uporaba aplikacije "OpenVPN Connect".

| Omejitve

Tu lahko nastavite omejitve v zvezi z upravljanjem povezave.

Omogočanje podatkovnega gostovanja	Omogočanje mobilnih podatkov med gostovanjem
Prisiliti podatkovno gostovanje	Če je aktivirano, je gostovanje za mobilne podatke trajno aktivirano (ni priporočljivo!) Ta nastavev prepíše nastavev "Dovoli podatkovno gostovanje"!
Naslednje nastavitve so na voljo samo v sistemu Samsung KNOX 2.0 ali novejšem	
Dovolite samo klice v sili	Dovolite samo klice v sili
Omogočanje omrežja WiFi	Omogočanje omrežja WiFi
Najnižja stopnja varnosti omrežja WiFi	Najnižja stopnja varnosti omrežja WiFi Odprto = dovoljene so vse vrste brezžičnega interneta.
Prepoved dodajanja omrežij WiFi uporabniku	Uporabnik ne sme sam dodati omrežja WiFi. Ta nastavev je mogoča le, če je bil profil WiFi opredeljen v razdelku "Upravljanje povezav".
Dovolite sporočila SMS in MMS	Vse = dovoljen je ves promet SMS in MMS Samo dohodna sporočila SMS = dovoljena so samo dohodna sporočila SMS Samo odhodna sporočila SMS = dovoljena so samo odhodna sporočila SMS Ni = promet SMS/ MMS ni dovoljen.
Dovolite sinhronizacijo med gostovanjem	Dovolite sinhronizacijo med gostovanjem Vključeno = aktivirano Izklopljeno = deaktivirano Izbira uporabnika = izbira uporabnika
Omogočanje glasovnega gostovanja	Omogočanje glasovnega gostovanja Vključeno = aktivirano Izklopljeno = deaktivirano Izbira uporabnika = izbira uporabnika
Uporaba sistemskega strežnika http Proxy Server	Uporaba posredniškega strežnika HTTP, ki je na voljo v nastavitvah sistema, je odvisna od povezanega omrežja (WiFi ali APN).

APN

Naslednje nastavitve so na voljo samo v sistemu Samsung SAFE 2.0 ali novejšem!

Prikazno ime APN	Prikazno ime APN	
Ime dostopne točke	Ime APN	
Protokol odhodnega strežnika	Ni nastavljeno	
	Ni	
	PAP	Protokol PAP
	CHAP	Protokol CHAP
	PAP ali CHAP	Protokol PAP ali CHAP
MCC - koda mobilne države	Tukaj se vnese MCC, če se uporabi MCC vstavljene kartice SIM, pustite to polje prazno.	
MNC - koda mobilnega omrežja	Tu se vnese MNC, če se uporabi MCC vstavljene kartice SIM, pustite to polje prazno.	
Naslov strežnika	Naslov strežnika	
Številka vrat strežnika	Številka vrat strežnika	
Naslov strežnika proxy	Naslov strežnika proxy	
Naslov strežnika MMS	naslov strežnika MMS, za standardne pustite prazen	
Številka vrat MMS	Številka vrat MMS	
Naslov posredniškega strežnika MMS	Naslov posredniškega strežnika MMS	
Uporabniško ime	Uporabniško ime	
Geslo	Geslo	
Vrsta dostopne točke	Dovoljene vrste so: "default", "mms", "supl" Če to polje ostane prazno, se uporabi "default,supl,mms".	
Prednostna APN	APN je zaželen	

Bluetooth

Tu lahko izvedete različne nastavitve Bluetooth.

Naslednje nastavitve so na voljo samo v napravi Samsung KNOX 1.0 ali višji različici!

Omogočanje odkrivanja naprave prek povezave Bluetooth	Omogočanje odkrivanja naprave prek povezave Bluetooth
Omogočanje seznanjanja prek povezave Bluetooth	Omogočanje združevanja Bluetooth
Dovolite naprave s slušalkami Bluetooth	Dovolite naprave s slušalkami Bluetooth
Omogočanje naprav za prostoročno telefoniranje Bluetooth	Omogočanje naprav za prostoročno telefoniranje Bluetooth
Dovolite naprave Bluetooth A2DP	Omogočanje pretakanja zvoka Bluetooth A2DP med napravami
Dovolite odhodne klice	Omogočanje odhodnih klicev prek omrežja BT
Omogočanje prenosa podatkov prek povezave Bluetooth	Omogočanje prenosa podatkov prek povezave Bluetooth
Omogočanje povezovanja prek povezave Bluetooth	Omogoča uporabo naprave kot modema (internetna povezava Bluetooth)
Omogočanje povezave z računalnikom prek povezave Bluetooth	Omogočanje povezave z računalnikom prek povezave Bluetooth

Upravljanje PIM

Izmenjava

Na voljo samo za Samsung KNOX 1.0 ali višje!

E-poštni naslov	e-poštni naslov uporabnika Upoštevajte "Namestnike", ki jih lahko uporabite za delo s poverilnicami in ne izvajate sprememb ročno v vsaki napravi. S klikom na Prikaži nadomestne elemente jih lahko prikažete sami.
Gostiteljsko ime strežnika	Strežniški naslov strežnikov Exchange
Prijavno ime	Prijavno ime za zadevno napravo končnega uporabnika, upoštevajte tudi "Namestna imena tukaj".
Domena	Naslov domene
Geslo (samo na ravni naprave)	Po želji lahko posamezni napravi določite geslo; če to ostane prazno, bo uporabnik pozvan, da vnese svoje geslo Exchange.
Število prejšnjih dni za sinhronizacijo	Število dni, ki določajo, kdaj se e-poštna sporočila sinhronizirajo nazaj
Podpis	Priložite lahko podpis (namig: nekatere naprave zahtevajo oblikovanje HTML za podpis).
Privzeti račun	ugotovi, da je ta poštni račun standardni račun.
Uporabite Secure Sockets Layer (SSL)	Uporaba povezave SSL
Uporaba protokola TLS (Transport Layer Security)	Uporaba povezave TLS
Sprejmite vsa potrdila	Sprejemajo se vsa potrdila. Izberite to možnost, če vaš strežnik Exchange uporablja samopodpisano potrdilo.

Elektronska pošta

Tu lahko račune IMAP in POP razdelite v ustrezne naprave končnih uporabnikov.

Naslednje nastavitve so na voljo samo v napravi Samsung KNOX 1.0 ali višji različici!		
E-poštni naslov	e-poštni naslov uporabnika Upoštevajte "Namestnike", ki jih lahko uporabite za delo s poverilnicami in ne izvajate sprememb ročno v vsaki napravi. S klikom na Prikaži nadomestne elemente jih lahko prikažete sami.	
Protokol dohodnega strežnika	Protokol dohodnega strežnika	IMAP ali POP
Naslov dohodnega strežnika	Naslov dohodnega strežnika	
Vhodna vrata strežnika	Vhodna vrata strežnika	
Prijavno/uporabniško ime dohodnega strežnika	Prijavno/uporabniško ime dohodnega strežnika	
Geslo vhodnega strežnika (samo na ravni naprave)	Geslo vhodnega strežnika (samo na ravni naprave)	
Dohodni strežnik uporablja SSL	Dohodni strežnik uporablja SSL	
Dohodni strežnik uporablja TLS	Dohodni strežnik uporablja TLS	
Dohodni strežnik sprejme vsa potrdila	Dohodni strežnik sprejema vse vrste potrdil	
Protokol odhodnega strežnika	Protokol odhodnega strežnika	SMTP
Odhodna vrata strežnika	Odhodna vrata strežnika	
Odhodni strežnik uporablja dodatne poverilnice	Dodatne poverilnice za odhodni strežnik. Če je nastavljeno na "izklopljeno", se uporabijo nastavitve dohodnega strežnika.	
Prijava/uporabniško ime odhodnega strežnika	Prijava/uporabniško ime odhodnega strežnika	
Geslo odhodnega strežnika (samo na ravni naprave)	Geslo odhodnega strežnika	
Odhodni strežnik uporablja SSL	Odhodni strežnik uporablja SSL	
Odhodni strežnik uporablja TLS	Odhodni strežnik uporablja TLS	
Odhodni strežnik sprejme vsa potrdila	Odhodni strežnik sprejema vse vrste potrdil	

Podpis	Podpis lahko priložite tukaj (namig: nekatere naprave zahtevajo oblikovanje HTML za podpis).
Obveščanje uporabnika o prejemu nove e-pošte	obvesti uporabnika o prejemu nove e-pošte

AE Gmail Exchange

Informacije: Ta konfiguracija bo uporabljena za aplikacijo Gmail. Zato morate odobriti in namestiti aplikacijo Gmail.


E-poštni naslov	e-poštni naslov uporabnika Upoštevajte "Namestnike", ki jih lahko uporabite za delo s poverilnicami in ne izvajate sprememb ročno v vsaki napravi. S klikom na Prikaži nadomestne elemente jih lahko prikažete sami.
Gostiteljsko ime strežnika	Strežniški naslov strežnikov Exchange
Prijavno ime	Prijavno ime za zadevno napravo končnega uporabnika, upoštevajte tudi "Namestna imena tukaj".
Podpis	Priložite lahko podpis (namig: nekatere naprave zahtevajo oblikovanje HTML za podpis).
Število prejšnjih dni za sinhronizacijo	Število dni, ki določajo, kdaj se e-poštna sporočila sinhronizirajo nazaj
Identifikator naprave	Identifikator EAS. Pustite to polje prazno, če vaše okolje tega ne zahteva.
Uporabite Secure Sockets Layer (SSL)	Uporaba povezave SSL
Sprejmite vsa potrdila	Sprejemajo se vsa potrdila. Izberite to možnost, če vaš strežnik Exchange uporablja samopodpisano potrdilo.
Dovoli neupravljanje račune	Uporabniku omogoča dodajanje dodatnih računov
Potrdilo stranke	Naložite potrdilo odjemalca, če strežnik Exchange to zahteva



Upravljanje aplikacij










Upravitelj aplikacij za podjetja

Nameščene aplikacije (samo na ravni naprave)

Tu bodo prikazane vse aplikacije, ki so trenutno nameščene v napravi končnega uporabnika.

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	

Sistemske aplikacije (samo na ravni naprave)

V razdelku "Sistemske aplikacije" so navedeni vsi prednameščeni sistemi z imenom in različico paketa.

System Apps				
Application Name	Version	Size	Package Name	
AASAservice	7.0	67 kB	com.samsung.aasaservice	
ANT + DUT	01.00.05	74 kB	com.dsi.ant.sample.acquirechannels	
ANT Radio Service	4.14.20	178 kB	com.dsi.ant.service.socket	
ANT+ HAL-Dienst	4.0.0	138 kB	com.dsi.ant.server	
ANT+ Plugins Service	3.6.10	2.54 MB	com.dsi.ant.plugins.antplus	
Adapt Sound	5.3.04	3.92 MB	com.sec.hearingadjust	
Android Easter Egg	1.0	230 kB	com.android.egg	
Android Services Library	1	12 kB	com.google.android.ext.services	
Android Shared Library	1	6 kB	com.google.android.ext.shared	
Android System WebView	69.0.3497...	405 kB	com.google.android.webview	
Android-Einrichtung	227.5901558	7.52 MB	com.google.android.setupwizard	
Android-System	8.1.0	69.48 MB	android	
Anwendungs-Installer	8.1.0	86 kB	com.sec.android.preloadinstaller	

Obvezne aplikacije

V razdelku Obvezne aplikacije lahko določite, katere aplikacije morajo biti nameščene v napravi. Odvisno od konfiguracije in naprave se aplikacija namesti samodejno ali pa bo uporabnik pozvan, da jo namesti.

Zavedajte se, da je za lažje upravljanje aplikacij priporočljivo uporabiti program Android Enterprise.

Scenariji so navedeni spodaj:

Običajne aplikacije v Trgovini Play

Namestitve aplikacij v trgovini Playstore vedno zahtevajo interakcijo z uporabnikom. Poleg tega je treba v napravi konfigurirati Googlov račun.

Namestitev aplikacije v hiši

V napravah Samsung bodo te aplikacije nameščene tiho. Edina izjema je vsebnik, pri katerem mora uporabnik potrditi namestitev.

V vseh drugih primerih mora uporabnik potrditi namestitev aplikacije.

Android Podjetje Trgovina Play Aplikacije

Te aplikacije bodo vedno nameščene tiho, brez posredovanja uporabnika.

Če želite dodati obvezno aplikacijo, kliknite "+" in s seznama izberite želeno aplikacijo. Upoštevajte, da aplikacij z zavihka "Trgovina Google Play" ne morete namestiti, če je naprava konfigurirana s sistemom Android Enterprise kot popolnoma upravljana ali kot vsebnik.

Če uporabljate sistem Android Enterprise, izberite aplikacije v razdelku "AE Play Store". Če želite, da so aplikacije na voljo tukaj, jih potrdite v trgovini Google Enterprise Play tako, da greste v Splošne nastavitve → AE Play Store → Play Store Apps.

Ko odstranite obvezno aplikacijo, bo ta odstranjena tudi iz naprave.

Na seznamu obveznih aplikacij lahko kliknete ime aplikacije in odprete zavihek "konfiguracija", da jo konfigurirate. To zahteva uporabo sistema Android Enterprise, aplikacija pa mora to podpirati. Zato so možnosti, ki so na voljo, odvisne od izbrane aplikacije.

Aplikacije sistema AE

Tu lahko omogočite sistemske aplikacije za naprave Android Enterprise. Upoštevajte, da mora biti določena aplikacija v shrambi sistema, sicer se ne zgodi nič. 296

Omejitve in nastavitve

Črna in bela lista

Tu lahko določite črno ali belo listo. Vse aplikacije na črnem seznamu bodo blokirane. Vse aplikacije, ki niso na beli listi, bodo blokirane. Prazen črni seznam ne blokira ničesar, prazen beli seznam pa blokira vse*

**Vse obvezne aplikacije in aplikacije iz trgovine Enterprise App Store bodo samodejno uvrščene na beli seznam. Ni jih treba dodajati ročno.*

S klikom na "+" lahko poiščete aplikacijo, ki jo želite dodati na črni ali beli seznam, ali pa ročno vnesete ime paketa.

Omejitve aplikacij sistema

V razdelku "Omejitve aplikacij sistema" lahko med drugim po želji blokirate vnaprej nameščene aplikacije in storitve.

Onemogočite brskalnik	Onemogočite standardni brskalnik
Onemogočite koledar	Onemogočite domači koledar
Onemogočite kalkulator	Onemogočite kalkulator
Onemogočite brskalnik Chrome	Onemogočite brskalnik Chrome
Onemogoči uro	Onemogočite uro
Onemogočiti stike	Onemogočiti stike
Onemogočanje klicnega avtomata	Onemogočite izvirni klicnik
Onemogočite elektronsko pošto	Onemogočite e-pošto
Onemogočite izmenjavo	Onemogočanje računov Exchange
Onemogočite Facebook	Onemogočite aplikacijo Facebook
Onemogočite galerijo	Onemogočite izvorno aplikacijo Galerija
Onemogočite storitev Gmail	Onemogočite storitev Gmail
Onemogočite Google Books	Onemogočite Google Books
Onemogočanje kioska Google Play	Onemogočanje kioska Google Play
Onemogočite Google Maps	Onemogočite Google Maps
Onemogočanje storitve Google Glasba	Onemogočanje storitve Google Glasba
Onemogočanje Googlovih filmov	Onemogočanje Googlovih filmov
Onemogočanje trgovine Google Play	Onemogočite trgovino Google Play (javna trgovina App Store)
Onemogočanje storitve Google Plus	Onemogočanje storitve Google Plus
Onemogočite iskanje Google	Onemogočite iskanje Google
Onemogočanje storitve Google Talk / Google Hangouts	Onemogočanje storitve Google Talk / Google Hangouts
Onemogočite predvajalnik glasbe	Onemogočite domačo aplikacijo za predvajanje glasbe
Onemogočite nastavitve	Onemogočite nastavitve naprave
Onemogočite orodje Sim Toolkit	Onemogočite storitve Sim Toolkit
Onemogočite sporočila SMS / MMS	Onemogočite sporočila SMS / MMS
Onemogočite prikaz ulice	Onemogočite storitve Street View
Onemogočite Youtube	Onemogočite Youtube

Aplikacije Samsung

V razdelku "Samsung Apps" lahko določite dodatne nastavitve in/ali omejitve za naprave Samsung.

Onemogočite storitev AllShare Play / Samsung Link	Onemogočite storitev AllShare Play / Samsung Link
Onemogočite ChatON	Onemogočite ChatON
Onemogočite vozlišče za igre	Onemogočite vozlišče za igre
Onemogočanje skupinskega igranja	Onemogočanje skupinskega igranja
Onemogoči pomoč	Onemogočite pomoč družbe Samsung
Onemogočite KNOX	Onemogočite vsebnik Samsung KNOX
Onemogočite opomnik	Onemogočanje glasovnega zapiska
Onemogoči moje datoteke	Onemogoči moje datoteke
Onemogočite optični bralnik	Onemogočite optični bralnik
Onemogočite Polaris Office	Onemogočite Polaris Office
Onemogočite vozlišče bralnikov / Samsung Books	Onemogočite vozlišče bralnikov / Samsung Books
Onemogočite S Memo	Onemogočite aplikacijo Samsung Memo
Onemogočite prevajalnik S	Onemogočite aplikacijo Samsung Prevajalnik
Onemogočite funkcijo S Voice	Onemogočanje glasovnega pomočnika S
Onemogočanje aplikacij Samsung	Onemogočanje trgovine Samsung App Store
Onemogočite vozlišče Samsung Hub	Onemogočite trgovine Samsung Entertainment Store
Onemogočite predvajalnik videoposnetkov	Onemogočite predvajalnik videoposnetkov
Onemogočite diktafon	Onemogočite diktafon
Onemogočite storitev WatchON	Onemogočite funkcijo WatchON (simulira daljinski upravljalnik)

Aplikacije Huawei

V razdelku "Huawei Apps" lahko določite dodatne nastavitve in/ali omejitve v napravi Huawei.

Onemogočite DLNA	Onemogočite DLNA
Onemogočanje namestitvenega programa	Onemogočanje namestitvenega programa
Onemogočite upravitelja datotek	Onemogočite upravitelja datotek
Onemogočite upravitelja varnostnega kopiranja	Onemogočite upravitelja varnostnega kopiranja
Onemogočite posodobitev sistema	Onemogočite posodobitev sistema
Onemogočite polje z orodji	Onemogočite polje z orodji
Onemogočite vreme	Onemogočite vreme
Onemogočite radio FM	Onemogočite radio FM

Nastavitve upravljanja aplikacij

Tu lahko določite obnašanje posodobitev aplikacij InHouse Apps.

Pogostost preverjanja posodobitev določa, kako pogosto aplikacija AppTec360 išče posodobitve za aplikacije v hiši. Ko je zaznana nova različica, se prenese in namesti.

Prag Wi-Fi določa, ali naj se prenos omeji na povezave Wi-Fi, če je aplikacija večja od nastavljenega praga. Če je manjša ali če praga ne določite, bo aplikacija prenesena v omrežju Wi-Fi in v mobilnem omrežju.

Trgovina z aplikacijami za podjetja

Upoštevajte, da se aplikacije, ki so dodane tukaj (Enterprise App Store), NE bodo samodejno namestile v napravo(-e). Uporabnik mora v napravi odpreti trgovino Enterprise App Store in aplikacijo namestiti ročno.

Če želite v napravo samodejno namestiti aplikacije, pojdite v "Upravljanje aplikacij" → "Upravitelj aplikacij v podjetju" → "Obvezne aplikacije" in tam dodajte zelene aplikacije.

Na tej točki lahko uporabnikom razdelite izbirne aplikacije.

Trgovina Playstore

Če želite dodati aplikacijo iz trgovine Play v trgovino, kliknite na "+". Če uporabljate Android Enterprise, pojdite na "App Management Enterprise Play Store". Upoštevajte tudi, da mora biti v → napravi nastavljen račun Google, da lahko namestite tukaj opredeljene aplikacije.

Lastna spletna stran

Pod točko "Lastno" lahko naložite in distribuirate interno razvite aplikacije.

S klikom na "+" dodate aplikacijo InHouse v trgovino z aplikacijami za podjetja, ki jo lahko nato namesti uporabnik. V tem dialogu lahko naložite tudi novo aplikacijo InHouse.

Trgovina Play za podjetja

Upoštevajte, da se aplikacije, ki so dodane tukaj (Enterprise Play Store), NE bodo samodejno namestile v napravo(-e). Uporabnik mora v napravi odpreti Trgovino Play in aplikacijo namestiti ročno.

Če želite v napravo samodejno namestiti aplikacije, pojdite v "Upravljanje aplikacij" → "Upravitelj aplikacij v podjetju" → "Obvezne aplikacije" in tam dodajte zelene aplikacije.

Na tej točki lahko uporabnikom razdelite izbirne aplikacije.

Tu lahko dodate aplikacije v trgovino Android Enterprise Playstore. Upoštevajte, da morate aplikacije odobriti v splošnih nastavitvah → AE Play Store → Play Store Apps. Te Aplikacije bodo dodane v običajno trgovino Google Play.

Upoštevajte tudi, da morate najprej določiti postavitev z aplikacijami v Splošne nastavitve → Upravljanje aplikacij → AE Play Store → Postavitev trgovine.

Aplikacije morajo biti v postavitvi, preden jih lahko uspešno dodate v trgovino.

Način Kiosk in zaganjalnik

Način kioska

V načinu Kiosk lahko vnaprej določite aplikacijo ali naslov URL. Nato bo mogoče zagnati/obiskati izključno to aplikacijo ali URL.

Prav tako lahko različne strojne gumbе deaktivirate v načinu Kiosk Mode.

Samodejni zagon	Samodejno zažene način Kiosk, takoj ko profil doseže napravo končnega uporabnika.
Načrtovani način kioska?	Načrtujete lahko čas za način Kiosk, ki se bo nato samodejno začel in končal ob času, ki ga določite vi.
Čas začetka	Čas začetka
Čas v minutah	Čas v minutah, po katerem se mora način Kiosk ponovno končati

Vrsta uporabe

Posamezna aplikacija	Če želite aplikacijo zagnati v načinu Kiosk, v razdelku "Vrsta aplikacije" izberite možnost Paket.
Uporaba kioska	Kliknite tukaj, da izberete aplikacijo, ki naj se zažene v načinu Kiosk. Našli boste običajen pregled upravljanja aplikacij. Izbirate lahko med "Google Play Store", "Android In-House Apps" in "Packagename".

Vrsta uporabe

URL	Če želite v načinu Kiosk zagnati URL, v razdelku "Vrsta aplikacije" izberite "URL". Nato določite želeni naslov URL
Izbriši brskalnik po neaktivnosti	Tu lahko določite časovni interval v minutah, po katerem naj se način Kiosk ponovno zažene.
Izbriši spletni predpomnilnik in piškotke	Če aktivirate to funkcijo, se po ponovnem zagonu načina Kiosk izbriše spletni predpomnilnik (piškotki in slike v predpomnilniku).
Politika enakega izvora	Če je ta funkcija aktivna, lahko uporabnik brska le po podstraneh določenega naslova URL. Na primer, določili ste naslednji URL: www.mypage.com Potem lahko uporabnik brska po: www.mypage.com/subpage
URL-ji na belem seznamu	Tu lahko vzdržujete beli seznam, na katerem so dovoljeni vsi ti naslovi URL. Največ 1 URL na vrstico URL se mora začeti s http:/ ali https://.
URL-ji na črnem seznamu	Tu lahko vzdržujete črni seznam, vsi ti naslovi URL niso dovoljeni. Največ 1 URL na vrstico URL se mora začeti s http:/ ali https://.
Usmeritev zaslona	Ta nastavitvev se nanaša na prilagoditve zaslona Samodejno = samodejno Portret = navpični format Pokrajina = krajinski način

Več aplikacij	Če izberete način "Multi App" Kiosk Mode, se bo uveljavila uporaba zaganjalnika AppTec360.
Aplikacije	Uporaba: Kot aplikacijo za kiosk izberite aplikacijo iz trgovine Playstore ali lastno aplikacijo. Možno je vnesti tudi ime paketa. Izbrana aplikacija Kiosk Application mora biti nameščena v napravi. Ne pozabite nastaviti, da je aplikacija Kiosk Application obvezna. Bližnjica na domačem zaslonu: Če je nastavljeno na "Vklopljeno", se ustvari bližnjica na domačem zaslonu. Če je nastavljena na "Izklopljeno", se bo aplikacija še vedno prikazovala na seznamu aplikacij.

Izhodno geslo Omogočeno	Če aktivirate to funkcijo, lahko uporabnik z geslom, ki ste ga vnaprej določili, zaključí način Kiosk.
Izhodno geslo	To je geslo, ki ste ga vnaprej določili.
Samodejno zvišanje vrstice stanja	Če je omogočeno, se vrstica stanja samodejno obkroži. S to možnostjo lahko uporabniki vidijo informacije v vrstici stanja, vendar ne morejo dostopati do njenih funkcij.
Onemogočite vrstico stanja	Vrstica stanja vsebuje obvestila, bližnjice in informacije. Na voljo samo za naprave Samsung s KNOX 1.0 ali novejšo različico.
Onemogočanje tipk za glasnost	Onemogočite tipke za glasnost (na voljo samo v Samsungovih napravah s KNOX 1.0 ali novejšo različico)
Onemogočite stikalo za vklop/izklop	Onemogočite stikalo za vklop/izklop (na voljo samo v Samsungovih napravah s KNOX 1.0 ali novejšo različico)
Onemogočanje gumba Domov	Onemogočite gumb Domov. Če je ta funkcija aktivirana, lahko način Kiosk prekinete samo v konzoli AppTec360. (na voljo samo v Samsungovih napravah s KNOX 1.0 ali novejšo različico)
Onemogočite navigacijsko vrstico	S tem lahko onemogočite navigacijsko vrstico (Nazaj / Meni). Če je ta funkcija aktivirana, lahko način Kiosk prekinete samo v konzoli AppTec360. (na voljo samo v Samsungovih napravah s KNOX 1.0 ali novejšo različico)

Nastavitve posodabljanja aplikacij	
Omogočanje posodobitev aplikacij	Uporabniki bodo pozvani k posodobitvam aplikacij tudi, če je aktiven način Kiosk. V napravah s Samsung KNOX se bodo aplikacije posodabljale tiho.
Okno za posodabljanje	Nastavite interval, v katerem bodo uporabniki pozvani k namestitvi posodobitev aplikacije.

TeamViewer	
Omogočanje nenadzorovanega dostopa	Če je ta možnost omogočena, lahko skrbniki napravo nadzorujejo na daljavo brez interakcije z uporabnikom. V napravo je treba namestiti aplikacijo TeamViewer Host.

AppTec360 zaganjalnik

Omogočite zaganjalnik AppTec360	Na: Vklopi zaganjalnik AppTec360. Uporabnik ga mora enkrat nastaviti kot privzeti zaganjalnik. Opomba: Če je omogočen način Kiosk in je način Kiosk nastavljen na "Multi App", se bo uporabil zaganjalnik AppTec360.
Velike ikone	Na: Prikaže večjo različico ikon aplikacij v zaganjalniku
Skrivanje ikone aplikacije AppTec360	Na: Aplikacijo AppTec360 popolnoma skrije
Skrivanje ikone trgovine AppTec360	Na: AppTec360 Enterprise AppStore se popolnoma skrije.

Nastavitve AppTec360

Omogočite aplikacijo AppTec360 Settings	Aplikacija AppTec360 Settings omogoča nadzor nad povezavami WiFi in Bluetooth
Omogočanje nastavitve v več aplikacijah Način kioska	Če je omogočeno, lahko uporabniki dostopajo do aplikacije AppTec360 Settings, ko je aktiven način Multi App Kiosk Mode.

Daljinski upravljalnik

Splashtop

Prikazuje trenutno stanje nastavitve Splashtop. Tukaj so prikazani koraki, ki jih morate izvesti za oddaljen dostop do naprave prek Splashtop. Tu morate vnesti tudi svojo kodo za namestitev, ki jo lahko dobite na spletnem mestu Splashtop. Koda za namestitev je potrebna za vzpostavitev povezave z napravo.

Teamviewer

Prikazuje trenutno stanje nastavitve programa Teamviewer. Tu so prikazani koraki, ki jih morate izvesti za oddaljen dostop do naprave prek programa Teamviewer.

Upravljanje vsebine

Vsebinsko polje

Tukaj lahko omogočite polje vsebine za to napravo. Ko jo aktivirate, bo v napravo nameščena aplikacija Contentbox.

Varen brskalnik

Tu lahko omogočite varen brskalnik za to napravo. Ko jo aktivirate, bo v napravo nameščena aplikacija Varni brskalnik. Ta brskalnik lahko nastavite tako, da v napravi ponuja spletni brskalnik, ki je omejen na vaše potrebe.

Zahtevati geslo	Od uporabnika zahtevajte, da nastavi in uporablja geslo za dostop do brskalnika.
Omejitev prenosov / Odprite v	Blokira prenose s spletnih strani
Omejitev nalaganja	Omejuje nalaganje na določene URL-je. Če ne navedete nobenega URL-ja, boste nalaganje v celoti blokirali.
Dovoli kopiranje	Omogočite kopiranje, rezanje ali deljenje besedila na spletnih straneh.
Omogočite zajem zaslona	Omogočite zajemanje posnetkov zaslona.
Pogostost čiščenja podatkov	Izberite, s kakšno pogostostjo naj se samodejno odstranijo VSI uporabniški podatki (zgodovina, predpomnilnik itd.).
Zaznamki podjetja	Zaznamki bodo prikazani v mapi "Company bookmarks" (zaznamki podjetja) v zaznamkih brskalnikov. Uporabnik jih ne more urejati.
Skrij naslovno vrstico	Skrije naslovno vrstico, tako da uporabnik ne vidi naslova URL, ki ga obiskuje.
Bela lista v brskalniku (brez univerzalnega prehoda)	Omogoča beli seznam URL-jev na strani odjemalca. - Zaznamki podjetja so vedno uvrščeni na beli seznam - Podprto samo za 100 URL-jev - Za neomejeno črno in belo listo uporabite univerzalni prehod
Črni in beli seznam na podlagi prehodov	Za uvrstitev na črni seznam veljajo naslednje zahteve: - Delujoča univerzalna vrata AppTec360 ("Splošne nastavitve" → "Univerzalna vrata") - Delujoča konfiguracija VPN z določenim strežnikom DNS ("Splošne nastavitve" → "Univerzalna vrata" → "Nastavitve VPN") - Konfiguracija črne liste ("Splošne nastavitve" → "Univerzalna vrata" → "Črna lista domen") - Veljavna povezava VPN v profilu ("Upravljanje povezav" → "VPN")

Konfiguracija Računalnik z operacijskim sistemom Windows 10

Splošno

Pregled profila skupine (samo na ravni skupine)

Ko odprete profil skupine, dobite hiter pregled profila.

Profile Name	Default Group Profile
Operating System	Android
Created At	01.03.2021 09:52:54
Created By	John Doe
Last Change	31.08.2021 16:35:50
Changed By	John Doe
Current Profile Revision	16
Released Profile Revision (outdated)	14

Delete Profile
Reset Group Profile
Copy Profile

Ime profila	Ime profila (tukaj ga lahko spremenite)
Operacijski sistem	Operacijski sistem, za katerega je profil namenjen
Ustvarjeno na	Čas nastanka
Ustvaril je	Ustvarjalec profila
Zadnja sprememba	Čas zadnje spremembe profila
Spremenjeno s	Račun, ki je opravil zadnje spremembe
Trenutna revizija profila	Revizija stanja shranjenega profila
Objavljena revizija profila	Dodeljena revizija profila ("Assigned profile revision"). Če je za besedilom na etiketi "(zastarela)", to pomeni, da ste profil shranili, vendar ga še niste dodelili, zato bodo naprave še vedno dobile starejšo različico.

Pregled naprave (samo na ravni naprave)

Povzetek pregleda naprave, ki vsebuje naslednje:

Ime računalnika	Ime računalnika
Stranka	Naprave Tip sistema Windows
Zadnja znana lokacija	zemljepisna širina in dolžina zadnje znane lokacije naprave
Dodeljene obvezne aplikacije	Število obveznih aplikacij, dodeljenih napravi
UID RAČUNALNIKA	UID računalnika
Izdaja za operacijski sistem	Prikazuje vašo izdajo sistema Windows
Različica operacijskega sistema	Trenutno nameščena različica sistema Windows
Sestava operacijskega sistema	Trenutna sestava sistema Windows
Operacijski sistem	Trenutno nameščen operacijski sistem
Serijska številka	Serijska številka naprave
Lastništvo naprave	Konfigurirana vrsta lastništva
Vrsta naprave	Vrsta naprave
Ukoreninjen	Pokaže, ali je naprava zakoreninjena
V skladu s predpisi	Pokaže, ali je naprava skladna
Nazadnje videno	Datum in čas, ko so bile opravljene spremembe v profilu.
Dodelitev uporabnika	Prikaže uporabnika ali skupino, ki ji je ta naprava trenutno dodeljena. Napravo lahko premaknete tako, da s spustnega seznama izberete drugega uporabnika ali skupino.

Nastavitve

Omogoči samodejno posodabljanje	Dovolite ali onemogočite samodejne posodobitve OS.
---------------------------------	--

Revizija konfiguracije (samo na ravni naprave)

Tu boste dobili pregled nad tem, kateri profil skupine je dodeljen napravi.

Revision Overview			
	Installed Profile	Assigned Profile	Last Generated Profile
Device Profile	Device Profile: Revision 5	Device Profile: Revision 5	Device Profile: Revision 5
Group Profile	Default Group Profile: Revision 13	Default Group Profile: Revision 13 (Newer Revision available)	Default Group Profile: Revision 13

Če kliknete na profil skupine, boste neposredno dostopali do profila in opravili nastavitve.

S simbolom lahko dodeljene aplikacije vrnete v nastavitve skupinskega profila.

S tem simbolom lahko ponastavite profil naprave, tako da nima nobenih nastavitvev.

"Na voljo je novejša revizija" pomeni, da je bil profil skupine spremenjen in shranjen, vendar ni dodeljen. Profil skupine je treba dodeliti s funkcijo "Assign now" na ravni skupine, da se spremembe uporabijo v napravah.

Dnevnik naprave (samo na ravni naprave)

Dnevnik ukazov

Tu si lahko ogledate, kateri ukazi so bili izdani za napravo in kakšen je njihov status.

Command Log (last 250 commands)					
#	Created By	Date modified	Command	State	
1	jd@example.com	31.08.2021 12:21:37	Install assigned profiles	Device Pushed	
2	jd@example.com	31.08.2021 12:10:04	Get installed apps	Command Executed	
3	jd@example.com	31.08.2021 12:10:04	Get managed apps	Command Executed	
4	jd@example.com	31.08.2021 12:10:02	Get certificates	Command Executed	
5	jd@example.com	31.08.2021 12:10:02	Get asset data	Command Executed	
6	System Automated	31.08.2021 05:34:29	Update profile revision	Command Partially Failed	!
7	System Automated	31.08.2021 05:34:29	Apply device settings	Command Executed	
8	System Automated	31.08.2021 05:34:27	Install application	Command Failed	!
9	System Automated	31.08.2021 05:34:25	Get installed apps	Command Executed	
10	System Automated	31.08.2021 05:34:25	Get managed apps	Command Executed	
11	System Automated	31.08.2021 05:34:23	Get certificates	Command Executed	

Ukazi, ustvarjeni s "Sistemska avtomatizirano", se samodejno ustvarijo v sistemu.

Možni statusi ukazov

Potisnjena naprava	Storitvi za potiskanje (npr. APNS) je bila poslana potisna zahteva, da se naprava poveže nazaj s strežnikom EMM.
Ustvarjen ukaz	Ukaz je bil ustvarjen v sistemu.
Poslan ukaz	Ukaz je bil napravi poslan, ko se je povezala s strežnikom.
Izveden ukaz	Ukaz je bil uspešno izveden.
Ukaz ni uspel	Ukaz ni uspel. *
Ukaz delno ni uspel	Odvisno od operacijskega sistema naprave so lahko nekateri ukazi združeni. Pri tem nekateri deli te skupine ukazov niso bili uspešni. *
Ukaz se je izvršil, vendar je bil neuspešen	Ukaz je bil izveden, vendar morda ni bil.
Ukaz se ponovno premakne	Ukaz je ponovno poslal uporabnik.
Zavrženi	Ukaz je bil zavržen. Na primer zato, ker ga je nadomestil drug ukaz ali ker je bila naprava ponovno vpisana in so bili stari ukazi odstranjeni.

*Če je za sporočilom izklicnik, lahko več informacij dobite tako, da s kazalcem podrsate nad ikono.

Upravljanje sredstev (samo na ravni naprave)

Informacije o napravi

Proizvajalec	Proizvajalec naprave
Model	Model naprave
Številka modela	Številka modela
Operacijski sistem	Operacijski sistem
Različica operacijskega sistema	Različica operacijskega sistema
Serijska številka	Serijska številka
ExchangeID	ExchangeID
Skupni RAM	Skupni RAM
Ločljivost zaslona	Ločljivost zaslona
Jezik telefona	Jezik naprave
Različica strojne programske opreme	Različica vdelane programske opreme
Različica odjemalca DM	Različica odjemalca za upravljanje naprav
Različica strojne opreme	Različica strojne opreme naprave
Arhitektura procesorja	Arhitektura procesorja (vrsta procesorja)

Cellular

Omrežje operaterja SIM	Omrežje prevoznikov
Telefonska številka	Telefonska številka
Status gostovanja	Status gostovanja
IMEI	IMEI
IMSI	IMSI
Vdelana programska oprema modema	Vdelana programska oprema modema

Informacije o sinhronizaciji

Takojšnja DM povezava	Naprava mora takoj vzpostaviti povezavo z aplikacijo AppTec.
Začetni čas ponovitve	Začetni čas ponovnega poskusa za to prvo povezavo
Ponovitve povezave	Število ponovitev nove povezave po prekinitvi povezave s strani upravitelja povezav ali napaki na ravni Winlnet
Najdaljši čas spanja	Najdaljši čas mirovanja po napaki pri pošiljanju paketa
Prvi ponovni poskusi sinhronizacije	Čas za prvo fazo po vpisu
Interval prvega ponovnega poskusa	Čas za prvo fazo po vpisu
Drugi ponovni poskusi sinhronizacije	Čas za drugo fazo po vpisu
Drugi interval ponovitve	Čas za drugo fazo po vpisu
Redni ponovni poskusi sinhronizacije	Čas za dodatne faze po vpisu
Redni interval ponavljanja	Čas za dodatne faze po vpisu

Upravljanje varnosti

Zaščita pred krajo (samo na ravni naprave)

Informacije GPS (samo na ravni naprave)

Tu lahko določite trenutno/ zadnjo lokacijo naprave. Lokalizacijo lahko zaščitite z enim ali celo dvema gesloma - glejte: "Splošne nastavitve" > "Zasebnost" > "Dostop do GPS".

Nastavitve GPS

Omogočanje sledenja GPS	Omogočite redno sinhronizacijo informacij GPS.
Interval sledenja	Nastavite interval sinhronizacije informacij GPS.

Varnostna konfiguracija

Pristopna koda

Najmanjša dolžina gesla	Najmanjša dolžina gesla	
Sestava gesla	Določa število posebnih znakov, ki jih mora vsebovati geslo. Ti so sestavljeni iz velikih in malih črk, števil in posebnih simbolov.	
Kakovost gesla	Tu lahko nastavite kakovost gesla	
	Alfanumerični	Samo številke in črke
	Številčno	Samo številke
	Številčno ali alfanumerično	Številke ali številke in črke
Najdaljši čas neaktivnosti Zaklepanje	Število minut nedejavnosti uporabnika v napravi, po katerih se naprava zaklene. Po tem času mora uporabnik napravo odkleniti tako, da vnese geslo naprave.	
Potek veljavnosti gesla	Nastavitev časa, v katerem je treba nastaviti novo geslo	
Omejitev zgodovine gesel	Število predhodno uporabljenih gesel, ki niso dovoljena	
Največ neuspešnih poskusov gesla	Kolikokrat je mogoče napačno vnesti geslo, preden se izvede popolno brisanje naprave.	

Protivirusni program

Nastavitve protivirusnega programa - Nastavitev konfiguracije skeniranja	
Vrsta skeniranja	Izbira, ali naj se opravi hitro ali celotno pregledovanje.
Nastavitev začetka skeniranja	Izbira časa v dnevu, ko bo program Windows Defender začel s pregledovanjem.
Frekvenca skeniranja	Izbira dneva, ko naj se zažene pregledovanje programa Windows Defender.
Pogostost posodabljanja podpisa	Določa interval v urah, ki se bo uporabljal za preverjanje podpisov.

Konfiguracija vrste datotek za skeniranje	
Omogočanje skeniranja arhivskih datotek	Dovolite ali onemogočite pregledovanje arhivov (na primer .zip), ko do njih dostopate.
Omogočanje skeniranja skript	Omogoča ali onemogoča funkcionalnost skeniranja skript v programu Windows Defender.
Omogočanje skeniranja e-poštnih sporočil	Omogočite ali onemogočite skeniranje e-poštnih sporočil.
Omogočanje skeniranja omrežnih datotek	Dovolite ali onemogočite pregledovanje omrežnih datotek.
Omogočanje popolnega pregledovanja mapiranih omrežnih pogonov	Dovolite ali onemogočite pregledovanje mapiranih omrežnih pogonov (omogočeno le, če je omogočeno celovito pregledovanje).
Nadzor dvosmernega skeniranja	Nadzoruje, katere sklope datotek je treba spremljati.
Omogočanje popolnega pregledovanja izmenljivih diskov	Omogočite ali onemogočite popolno pregledovanje izmenljivih diskov. Začne se samo med popolnim pregledovanjem.

Vrsta datotek, ki jih je treba izključiti iz pregleda	
Ignoriranje vrst datotek za skeniranje	Opredelite niz vrst razširitev datotek. Vsaka razširitev datoteke za vsako polje.
Ignoriranje poti do imenikov	Opredelite niz poti do imenikov, da jih ne boste pregledovali. Ena pot na polje. Primeri: "C:\Example", "C:\Windows" ali "C:\Users".
Izključitev procesov iz pregleda	Izključitev datotek, ki so jih odprli določeni procesi, iz protivirusnih pregledov programa Microsoft Defender. . Ena pot na polje. Primeri: "C:\myFile.exe", "C:\Windows\myProcess.exe", "C:\myScript.bat

Dodatne nastavitve	
Omogočite spremljanje v realnem času	Omogočanje ali onemogočanje funkcije spremljanja v realnem času programa Windows Defender
Omogoči spremljanje vedenja	Omogočanje ali onemogočanje funkcionalnosti spremljanja vedenja sistema Windows
Omogočanje zaščite v oblaku	Dovolite ali onemogočite, da program Windows Defender Microsoftu pošlje informacije o vseh težavah, ki jih odkrije. Microsoft bo te informacije analiziral, izvedel več o težavi, ki vpliva na napravo, in ponudil izboljšane rešitve.
	Obnašanje pri pošiljanju vzorcev
Omogočanje zaščite Windows Defender IOAV	Omogočanje ali onemogočanje zaščite Windows Defender IOAV
Omogočanje dostopa do uporabniškega vmesnika "Zaščita pri dostopu" programa Defenders	
Povprečni faktor obremenitve procesorja	Predstavlja povprečni faktor obremenitve procesorja za pregledovanje programa Windows Defender (v odstotkih).

Ravnanje z zlonamerno programsko opremo	
Majhna resnost	Za vsako stopnjo resnosti lahko določite, kako naprava obravnava zlonamerno programsko opremo. Na voljo so naslednje možnosti: <ul style="list-style-type: none"> • Čisto • Karantena • Odstranite • Omogočite • Določeno s strani uporabnika • Blok
Zmerna resnost	
Velika resnost	
Huda resnost	
Dnevi za ohranitev očiščene škodljive programske opreme	Časovno obdobje v dnevih, v katerem bodo datoteke/predmeti v karanteni shranjeni v sistemu. Privzeta vrednost je 0, kar pomeni, da elementi

	ostanejo v karanteni in se ne odstranijo samodejno. Največja vrednost je 90.
--	--

Varnostni center

Windows Security Center - Nastavitve za Windows Security	
Onemogočite uporabniški vmesnik za zaščito pred virusi in grožnjami	
Skrij Ransomware Uporabniški vmesnik za obnovitev podatkov	
Onemogočanje uporabniškega vmesnika za zaščito računa	
Onemogočite požarni zid in zaščito omrežja Uporabniški vmesnik	
Onemogočite uporabniški vmesnik za nadzor aplikacij in brskalnika	
Prepoved sprememb zaščite pred izkoriščanjem	Uporabniku onemogočite spreminjanje nastavitve zaščite pred izkoriščanjem
Onemogočanje uporabniškega vmesnika za varnost naprave	
Skrijte odpravljanje težav s TPM	Skrievanje nastavitve za odpravljanje težav TPM
Onemogočite gumb Clear TPM	
Onemogočanje uporabniškega vmesnika za zmogljivost in zdravje naprave	
Onemogočite uporabniški vmesnik družinskih možnosti	

Prilagajanje toastov	
Omogočite informacije o podpori po meri	Omogočite prikaz prilagojenih kontaktnih informacij za podporo za vaše podjetje v spodnjem desnem kotu aplikacije varnostnega centra.
E-naslov	Nastavite e-poštni naslov podjetja
Ime podjetja	Nastavite ime podjetja
Telefon podjetja	Nastavitev telefona podjetja
URL pomoči	Nastavite URL pomoči podjetja

Dodatne nastavitve	
Onemogočanje obvestil	Onemogočite prikaz obvestil centra Windows Defender Security Center.
Skrijte priporočila za posodobitev vdelane programske opreme TPM	Skrijte priporočilo za posodobitev vdelane programske opreme TPM, ko odkrijete ranljivo vdelano programsko opremo.
Prikaz imena podjetja in možnosti za stik	Prikažite ime podjetja in možnosti za stike na izletni kartici stikov v varnostnem središču Windows Defender Security Center.
Skrievanje varnega zagona	Skrijte območje Varnostni zagon.
Skrievanje nadzora območja varnostnih obvestil	Skrijte nadzor varnostnega območja za obvestila sistema Windows.

Konfiguracija požarnega zidu

Konfiguracija požarnega zidu - Globalne nastavitve	
Ignoriranje nastavitve avtentikacije	prezreti celoten niz avtentikacij, če ne podpirajo vseh sklopov avtentikacij, določenih v nizu.
Vrsta čakalne vrste paketov	Določa, kako je omogočeno skaliranje programske opreme na strani prejema za šifriran sprejem in jasno pot naprej za scenarij tunela IPsec.
Onemogočite izvajanje stalne filtriranja FTP	Če je onemogočena, ne izvaja filtriranja FTP (Stateful File Transfer Protocol), da bi omogočila sekundarne povezave.
Čas mirovanja varnostnega združenja	To polje konfigurira čas mirovanja varnostnega združenja v sekundah. Varnostna združenja se izbrišejo, ko se omrežni promet ne pojavi v tem določenem časovnem obdobju.
Kodiranje vnaprej zaupanega ključa	Nastavitev kodiranja vnaprej zaupanega ključa
Izjeme IPsec	Konfiguracija izjem internetnega protokola
Preverjanje seznama preklicanih potrdil	

Profili požarnega zidu (domenski profil / zasebni profil / javni profil)	
Omogoči požarni zid za ta profil	
Onemogočanje obvestil	Onemogočite prikaz obvestila uporabniku, ko je aplikaciji onemogočeno poslušanje na vratih.
Blokiranje odzivov enosmernega oddajanja na večpredstavnostno oddajanje	
Izvajanje pravil požarnega zidu za pooblaščen aplikacije	Če ni uveljavljena, se pravila pooblaščenega požarnega zidu aplikacije v lokalni shrambi ne upoštevajo in se ne uveljavijo.
Uveljavljanje globalnih pravil zapornega zidu na vratih	Če ni uveljavljena, se pravila globalnega požarnega zidu vrat v lokalni shrambi ne upoštevajo in se ne uveljavijo. Nastavitev ima pomen le, če je nastavljena ali našteta v shrambi skupinske politike ali če je našteta iz shrambe GroupPolicyRSOPStore
Izvajanje pravil požarnega zidu	Če ni uveljavljena, se pravila požarnega zidu iz lokalne shrambe ne upoštevajo in se ne uveljavijo.
Uveljavljanje varnostnih pravil povezave	Če ni uveljavljena, se varnostna pravila povezave iz lokalne shrambe ne upoštevajo in se ne uveljavljajo.
Privzeto izhodno dejanje	Ukrep, ki ga požarni zid privzeto izvede pri odhodnih povezavah
Privzeto dohodno dejanje	Ukrep, ki ga požarni zid privzeto izvede pri vhodnih povezavah
Onemogočite način Stealth	Način Stealth je mehanizem v požarnem zidu Windows, ki pomaga preprečiti zlonamernim uporabnikom, da bi odkrili informacije o omrežnih računalnikih in storitvah, ki jih izvajajo.
Onemogočanje preprečevanja odzivanja na nezaželeni promet	Če je onemogočeno, pravila za prikriti način požarnega zidu gostiteljskemu računalniku ne smejo preprečiti odziva na nezaželeni omrežni promet, če je ta promet zaščiten s protokolom IPsec.

Pravila požarnega zidu

Pravila požarnega zidu	
Ime	Ime pravila
Opis	Opis pravila
Akcija	Določite, ali bo to pravilo promet blokiralo ali dovolilo. Upoštevajte, da lahko možnost Blokiraj blokira tudi promet (odvisno od preostale konfiguracije) med strežnikom MDM in napravo.
Smer	
Omogoči prehajanje robov (na voljo samo, če je smer nastavljena na dohodni promet)	Označuje, da je določenemu vhodnemu prometu dovoljeno tuneliranje skozi NAT in druge robne naprave z uporabo tehnologije tuneliranja Teredo.

Programi in storitve	
Opredelitev aplikacij, vse drugače	Če ta možnost ni omogočena, bodo upoštevane vse aplikacije.
Ime družine paketov	Ime družine paketov, za katero bo pravilo veljalo.
Pot do datoteke aplikacije	Celotna aplikacija, na primer C:\Windows\System\notepad.exe, za katero bo veljalo pravilo
Popolnoma kvalificirano binarno ime	Popolnoma kvalificirano binarno ime, za katero bo pravilo veljalo. FQBN je niz v naslednji obliki: {Izdajatelj\Produkt\Filensko ime,Različica}
Ime storitve	Vnesite ime storitve (npr. "EventLog"). Seznam imen storitev lahko dobite v programu Powershell z ukazom "Get-Service".

Protokoli in vrata				
Protokol	Protokol, ki ga uporablja pravilo.			
Razpoložljive vrednosti: - Katera koli - Po meri - HOPORT - ICMPv4 - IGMP - TCP - UDP - IPv6 - IPv6-usmeritev - IPv6-Frag - GRE - ICMPv6 - IPv6-NoNxt - Možnosti IPv6 - VRRP - PGM - L2TP	Ko je nastavljena vrednost Po meri	Vnesite številko protokola med 0 in 255	Številka protokola	
	Ko je nastavljena na TCP ali UDP	Navedite lokalna vrata, sicer se uporabijo vsa.	Lokalna vrata, ki jih bo pravilo uporabljalo, dovoljena so tudi vrata v obsegu.	
		Lokalno pristanišče	Posamezna vrata ali vrsta vrat. Npr. 100-120,200,300-320.	
		Navedite oddaljena vrata, sicer se uporabijo vsa.	Oddaljena vrata, ki jih bo pravilo uporabljalo, dovoljena so tudi vrata v obsegu.	
		Oddaljena vrata	Posamezna vrata ali vrsta vrat. Npr. 100-120,200,300-320.	

Področje uporabe	
Navedite lokalne IP-je, v nasprotnem primeru katerikoli IP.	Nabor lokalnih IP-jev, lahko tudi razpon IP-jev, ločenih z -
Lokalni naslov IP	Nabor posameznih IP-jev ali razpon IP-jev, ločenih z -
Navedite oddaljene IP-je, v nasprotnem primeru katerikoli oddaljeni IP	Določite niz oddaljenih IP-jev, lahko tudi razpon IP-jev, ločenih z "-".
Oddaljeni naslov IP	Določite posamezne IP-je ali razpon IP-jev
Žetoni	Žetoni, ki jih je mogoče nastaviti skupaj z oddaljenimi naslovi. Žetoni Intranet, RmtIntranet in Ply2Renders so podprti v operacijskem sistemu Windows 10, različica 1809 in novejša.

Napredne nastavitve	
Določite profile, sicer se uporabijo vsi.	Če je to onemogočeno, se uporabijo vsi profili.
Domena	Profil domene
Zasebno	Zasebni profil
Javna stran	Javni profil
Navedite vmesnike, sicer bodo uporabljeni vsi.	Če je to onemogočeno, se uporabijo vsi vmesniki.
Lokalno omrežje	Vmesnik lokalnega omrežja
Oddaljeni dostop	Vmesnik za oddaljeni dostop
Brezžični	Brezžični vmesnik

Lokalni ravnatelji	
Dodajanje pooblaščenih lokalnih uporabnikov	Dovolite dodati seznam lokalnih uporabnikov, ki bodo uporabljali to pravilo
Pooblašчени uporabniki	Seznam pooblaščenih lokalnih uporabnikov za to pravilo. Uporabnik mora biti v formatu SDDL (Security Description Definition language), npr. PC_NAME\USERNAME. To polje ne sme biti izpolnjeno, če je za uporabo tega pravila nastavljeno ime storitve

Nastavitve omejitev

Funkcionalnost naprave

Dovolite kartico SD	Omogočanje uporabe kartice SD
Dovolite kamero	Dovolite uporabo fotoaparata
Omogočanje lokacijske storitve	Dovolite storitev lokacije naprave
Omogočanje bočnega nalaganja aplikacij	Dovolite namestitvev aplikacij iz neznanih virov
Dovolite način za razvijalce	Omogoča način za razvijalce
Omogočanje mobilnega podatkovnega gostovanja	Omogočanje mobilnega podatkovnega gostovanja
Dovolite Cortani	Omogočanje glasovne pomočnice Cortana
Omogočanje iskanja z uporabo lokacije	Omogočanje iskanja z uporabo lokacije
Omogočanje dodajanja e-poštnega računa, ki ni Microsoftov e-poštni račun	Določite, ali je uporabniku dovoljeno dodajati e-poštne račune, ki niso MSA.
Omogočanje povezave z Microsoftovim računom	Določite, ali dovolite uporabo računa MSA za avtentikacijo in storitve, ki niso povezane z e-pošto.
Dovoli sinhronizacijo mojih nastavitev	Omogoča sinhronizacijo nastavitev v celotni napravi
Zaščitena domenska imena za podjetja	Določa imena domen podjetij, ki so ločena z ";".
Omogočite uporabniku, da onemogoči Obnovitev sistema	Uporabniku omogoča, da onemogoči obnovitev sistema. OPOZORILO! To funkcijo lahko uporabljate samo v napravah, ki so v lasti podjetja ali organizacije ali jih podjetje ali organizacija zagotovi, ali v napravi v lasti

	<p>uporabnika, če uporabnik dovoli, da napravo v celoti upravlja podjetje. Če to nastavitev politike onemogočite, je obnavljanje sistema izklopljeno, do čarovnika za obnavljanje sistema pa ni mogoče dostopati. Onemogočena je tudi možnost konfiguracije obnovitve sistema ali ustvarjanja obnovitvene točke prek sistemske zaščite.</p>
Omogočanje odjave uporabnika	<p>Uporabniku omogoča, da iz naprave odstrani korporativni del in se tako odklopi od strežnikov AppTec360. Če se to zgodi, naprave ne bo več mogoče upravljati.</p> <p>OPOZORILO!</p> <p>To funkcijo lahko uporabljate samo v napravah, ki so v lasti podjetja ali organizacije ali jih podjetje ali organizacija zagotovi, ali v napravi v lasti uporabnika, če uporabnik dovoli, da napravo v celoti upravlja podjetje. Če to nastavitev politike onemogočite, uporabniki ne bodo mogli odstraniti vpisov v MDM.</p> <p>Določite, ali lahko uporabnik prek nadzorne plošče delovnega mesta izbriše račun delovnega mesta. Strežnik MDM lahko vedno izbriše račun na daljavo.</p>

BitLocker

Konfiguracija programa BitLocker

Splošne nastavitve	
Zahteva za šifriranje naprave	Uporabnike pozovite, naj omogočijo šifriranje naprave. Odvisno od izdaje operacijskega sistema Windows in konfiguracije sistema se lahko od uporabnikov zahteva: <ul style="list-style-type: none"> - Če želite potrditi, da šifriranje drugega ponudnika ni omogočeno. - Izklop šifriranja pogona BitLocker in ponovni vklop programa BitLocker.
Metode šifriranja	
Metoda šifriranja pogonov operacijskega sistema	
Metoda šifriranja za fiksne podatkovne pogone	
Metoda šifriranja za izmenljive podatkovne pogone	
Onemogočite opozorilo o šifriranju diska tretje osebe	Onemogočite opozorilni poziv glede storitve šifriranja diska tretje osebe, ki se uporablja v napravi. Od različice 1803 operacijskega sistema Windows 10 je ta nastavev podprta samo za naprave, ki so pridružene Azure Active Directory.
Dovolite izvajanje šifriranja, ko je prijavljen uporabnik, ki ni upravitelj	Podprto samo za naprave, ki so pridružene Azure Active Directory

AppTec360 razširitve	
Tiho šifriranje	Če je izbrana možnost "Zahtevati šifriranje naprave", bo storitev AppTec360 Management Service izvedla samodejno tiho šifriranje pogonov naprave.
Samodejno ustvarjanje uporabniških poverilnic	Šifrirani pogon operacijskega sistema bo zaščiten s samodejno ustvarjenimi uporabniškimi poverilnicami. PIN TPM, če je na voljo TPM, ali šestmestno besedilno geslo. Ustvarjene poverilnice so poslane na e-poštni naslov, registriran za določeno napravo. Če je ta možnost izklopljena, je edina možna zaščita za tiho šifriranje uporaba TPM. V tem primeru pri napravah brez čipa TPM tiho šifriranje ne bo uspešno.
Šifriranje fiksnih diskov	Vsi razpoložljivi fiksni podatkovni pogoni bodo prav tako šifrirani in zaščiteni s funkcijo samodejnega odklepanja s ključem, shranjenim na pogonu operacijskega sistema.

Nastavitve pogona operacijskega sistema

Zahteva po dodatni avtentikaciji ob zagonu	S to nastavitvijo lahko nastavite, ali program BitLocker zahteva preverjanje pristnosti ob vsakem zagonu računalnika. Ta nastavev se uporabi med nastavitvijo programa BitLocker. Če omogočite to nastavev, lahko uporabniki v čarovniku za namestitev programa BitLocker nastavijo napredne možnosti zagona.
Blokiranje programa BitLocker brez združljivega TPM	
Samo TPM	
TPM in PIN	
TPM in ključ	
TPM, ključ in PIN	Če želite zahtevati uporabo kode PIN in pomnilnika USB (ključa), mora uporabnik nastaviti program BitLocker z orodjem ukazne vrstice "manage-bde" namesto s čarovnikom za nastavev šifriranja pogona BitLocker.

Zahteva Najmanjša dolžina kode PIN	
	Najmanj znakov

<p>Konfiguracija sporočila in URL-ja za obnovitev pred zagonom</p>	<p>Konfigurirajte celotno sporočilo za obnovitev ali zamenjajte obstoječi naslov URL, ki se prikaže na zaslonu za obnovitev pred zagonskim ključem, ko je pogon operacijskega sistema zaklenjen.</p> <p>Opomba: Vsi znaki in jeziki niso podprti pred zagonom. Priporočljivo je, da preizkusite, ali so znaki, ki jih uporabljate, pravilno prikazani na zaslonu za obnovitev pred zagonom.</p>
	<p>Možnost sporočila za obnovitev pred zagonom</p>
	<p>Sporočilo o obnovitvi po meri</p>
	<p>URL za obnovitev po meri</p>

<p>Možnosti obnovitve pogona OS</p>	<p>Ta nastavitev omogoča nadzor nad tem, kako se obnovijo pogoni operacijskega sistema, zaščiteni s programom BitLocker, če ni zahtevanih poverilnic.</p> <p>Ta nastavitev se uporabi med nastavitvijo programa BitLocker.</p> <p>Privzeto je dovoljen agent za obnovitev podatkov na podlagi certifikata, možnosti obnovitve lahko določi uporabnik, vključno z geslom za obnovitev in ključem za obnovitev, podatki za obnovitev pa niso varnostno kopirani v AD DS.</p>
<p>Agent za obnovitev podatkov na podlagi certifikata bloka</p>	<p>Določite, ali se lahko sredstvo za obnovitev podatkov uporablja z diski operacijskega sistema, zaščitenimi z orodjem BitLocker.</p> <p>Preden lahko uporabite agenta za obnovitev podatkov, ga je treba dodati iz elementa Politike javnih ključev v konzoli za upravljanje skupinskih politik ali v urejevalniku lokalnih skupinskih politik.</p> <p>Za več informacij o dodajanju agentov za obnovitev podatkov si oglejte Vodnik za uvajanje šifriranja diskov BitLocker v Microsoft TechNet.</p>
<p>Nastavitve gesla za obnovitev programa BitLocker</p>	
<p>Nastavitve obnovitvenega ključa programa BitLocker</p>	
<p>Shranjevanje informacij o obnovitvi programa BitLocker v domensko storitev Active Directory</p>	
<p>Konfiguracija shrambe za obnovitev AD DS BitLocker</p>	<p>Shranjevanje paketa ključev podpira obnovitev podatkov s fizično poškodovanega pogona.</p>
<p>Zahteva po shranjevanju podatkov za obnovitev v AD DS</p>	<p>Uporabnikom prepričajte, da bi omogočili BitLocker, razen če je računalnik povezan v domeno in</p>

Fiksne nastavitve pogona	
Možnosti obnovitve fiksnih diskov	S to nastavitvijo lahko nadzirate, kako se z BitLockerjem zaščiteni fiksni diski obnovijo, če ni zahtevanih poverilnic. Ta nastavev se uporabi med nastavitvijo programa BitLocker. Privzeto je dovoljen agent za obnovitev podatkov na podlagi certifikata, možnosti obnovitve lahko določi uporabnik, vključno z geslom za obnovitev in ključem za obnovitev, podatki za obnovitev pa niso varnostno kopirani v AD DS.
Agent za obnovitev podatkov na podlagi certifikata bloka	
Nastavitve gesla za obnovitev programa BitLocker	
Nastavitve obnovitvenega ključa programa BitLocker	
Shranjevanje informacij o obnovitvi programa BitLocker v domensko storitev Active Directory	
Konfiguracija shrambe za obnovitev AD DS BitLocker	Shranjevanje paketa ključev podpira obnovitev podatkov s fizično poškodovanega pogona.
Zahteva po shranjevanju podatkov za obnovitev v AD DS	Uporabnikom prepričite omogočanje programa BitLocker, razen če je računalnik povezan z domeno in je varnostna kopija informacij za obnovitev programa BitLocker v AD DS uspešna. Opomba: Geslo za obnovitev se ustvari samodejno.
zavrnitev dostopa do pisanja na nezaščitene fiksne pogone	

Nastavitve izmenljivega pogona	
Prepoved pisanja na nezaščitene izmenljive pogone	onemogočite pisanje na izmenljive podatkovne pogone, ki niso zaščiteni s programom Bitlocker. Opomba: Če "Removable Disks: Deny write access" je omogočena v politiki skupine, ta nastavev politike ne bo upoštevana.
zavrnitev dostopa do pisanja za naprave, konfigurirane v drugi organizaciji	Dostop za pisanje bo omogočen samo pogonom z identifikacijskimi polji, ki se ujemajo z identifikacijskimi polji računalnika. Ta polja so opredeljena z nastavitvijo skupinske politike "Zagotovite edinstvene identifikatorje za vašo organizacijo".

Stanje programa BitLocker

Tukaj si lahko ogledate trenutno stanje diskov, šifriranih s programom BitLocker

C [OS Drive]
Stanje šifriranja
Šifrirano (%)
Status zaščite
Metoda šifriranja
Zaščitniki za ključ
Geslo za obnovitev

S klikom na gumb "Obrnite geslo za obnovitev" lahko obrnete geslo za obnovitev programa BitLocker.

Upravljanje certifikatov

Seznam certifikatov

Tukaj je seznam certifikatov, ki so nameščeni v prikazani napravi.

Konfiguracija potrdila

Tu lahko konfigurirate certifikate in način njihove namestitve v napravo.

Zaupanja vredno potrdilo	
Opis	Opis certifikata
Področje uporabe	Obseg uvajanja certifikata: Trenutni uporabnik proti napravi
Hramba potrdil	"Nezaupanja vredni certifikati" so na voljo samo v operacijskem sistemu Windows 10, različica 1803
Datoteka s potrdilom	Prenos datoteke PKCS#1

Potrdilo o identiteti		
Opis	Opis certifikata	
Področje uporabe	Obseg uvajanja certifikata: Trenutni uporabnik proti napravi	
Ključna lokacija	Ponudnik za shranjevanje ključev, v katerega se namesti zasebni ključ.	
	TPM. Neuspešno, če TPM ni prisoten	
	TPM. Če TPM ni prisoten, se preklopi na programsko opremo KSP.	
	Ponudnik shranjevanja ključev programske opreme	Označi zasebni ključ kot izvozni
	Windows Hello za podjetja	Ime zabojnika
	Besedilo poziva PIN	Določa besedilo po meri, ki se prikaže na pozivu PIN v programu Windows Hello for Business med vpisom potrdila.
Pooblastilo	Prenos datoteke PKCS#12	

SCEP

Opis	Opis strežnika SCEP		
Področje uporabe	Obseg uvajanja certifikata: Trenutna naprava proti uporabniku		
URL-ji strežnika SCEP	Eden ali več strežnikov, ki izdajajo potrdila prek protokola SCEP.		
Zadeva	Predstavitev imena X.500. Npr. "C=US, O=Microsoft Corporation, CN=foo, 1.2.5.3=bar"		
Alternativna imena predmetov	Tip	E-poštni naslov	
		DNS	
		URI	
		Glavno ime uporabnika (UPN)	
Prstni odtis CA	Prstni odtis SHA1 potrdila overitelja. E.g. 31:8F:1E:78:5C:D5:12:9F:7E:3B:AD:F3:1C:C0:19:03:96:43:A9:E5		
Obdobje veljavnosti enote	Dnevi, meseci ali leta		
Obdobje veljavnosti			
Izziv	Uporablja se kot vnaprej zaupana skrivnost za samodejni vpis.		
Ponovitve	Število ponovnih poskusov naprave, če strežnik pošlje odgovor PENDING. Privzeta vrednost je 5. Največja vrednost je 30.		
Zakasnitev ponovitve	Število minut, ki jih je treba počakati pred ponovnim poskusom. Privzeta vrednost je 5. Najmanjša vrednost je 1.		
Velikost ključa	Velikost ključa v bitih		
Algoritem pomišljanja	Družina algoritmov za pomišljanje		
Ključna uporaba	Razširitev uporabe ključa opredeljuje namen (npr. šifriranje, podpis) ključa, ki ga vsebuje potrdilo. Izbrati je treba vsaj eno od možnosti "Digitalni podpis" ali "Encipherment ključa".		
Razširjena uporaba	Določa razširjeno uporabo ključev. Odvisno od konfiguracije strežnika SCEP. Navedite seznam ustreznih OID, npr. 1.3.6.1.5.5.7.3.2 (preverjanje pristnosti)		

ključev	odjemalca)	
Ključna lokacija	Ponudnik za shranjevanje ključev, v katerega se namesti zasebni ključ.	
		TPM. Neuspešno, če TPM ni prisoten
	TPM. Če TPM ni prisoten, se preklopi na programsko opremo KSP.	
	Ponudnik shranjevanja ključev programske opreme	
	Windows Hello za podjetja	Ime zabojnika
	Besedilo poziva PIN	Določa besedilo po meri, ki se prikaže na pozivu PIN v programu Windows Hello for Business med vpisom potrdila.

Upravljanje povezav

Wifi

Pri tej nastavitvi izvedite predhodno konfiguracijo naprav končnega uporabnika za dostop do notranjih dostopnih točk.

Identifikator nabora storitev (SSID)	SSID omrežja, s katerim bo vzpostavljena povezava.
Samodejno pridruževanje	Aktivacija samodejne vključitve v omrežje
Skrito omrežje	Aktiviraj, če AP ne oddaja SSID.

Vrsta varnosti

Vzpostavitev varnostne vrste AP

Odpri sistem WEP	
Geslo	Geslo za AP

WPA PSK	
Geslo	Geslo za AP

WPA EAP	
Vrsta preverjanja pristnosti	Vrsta avtentikacije, mogoča samo s "PEAP-MSCAHPv2".
Hitra ponovna povezava	Naprave lahko preklaplajo med dostopnimi točkami, ne da bi se morale ponovno avtentificirati.
Dostop za goste	Uporabnik nima računa, zato se mora registrirati kot gost
Pregledi v karanteni	Odjemalec mora opraviti preverjanje NAP (Network Access Protection) in rezultate posredovati sistemu, ki nato odloči, ali se lahko odjemalec poveže.
Zahtevajte kriptografsko vezavo	Preverjanje pristnosti je mogoče samo prek kriptografske vezave.
Potrjevanje strežnika	Odjemalec preveri, ali je potrdilo strežnika veljavno. Če je, se vzpostavi povezava.
Poziv za potrdila	Uporabniku omogoča, da sprejme nezaupanja vredna potrdila.
Imena strežnikov	Ponuja možnost prikaza imena strežnika RADIUS, ki omogoča preverjanje pristnosti in avtorizacijo v omrežju.

WPA2-PSK	
Geslo	Geslo AP

WPA2 EAP	
Vrsta preverjanja pristnosti	Vrsta avtentikacije, mogoča samo s "PEAP-MSCAHPv2".
Hitra ponovna povezava	
Dostop za goste	
Pregledi v karanteni	Aktivira zaščito dostopa do omrežja NAP
Zahtevajte kriptografsko vezavo	Preverjanje pristnosti je mogoče samo prek kriptografske vezave.
Potrjevanje strežnika	
Poziv za potrdila	Zahteva za potrjeno potrdilo strežnika, ime ali preverjanje pristnosti korenskega potrdila (CA).
Imena strežnikov	Seznam strežnikov, ki jim morajo naprave zaupati
Ni	Ni vzpostavljene varnosti
Uporaba strežnika proxy	Uporaba posredniškega strežnika
Naslov strežnika	Naslov strežnika proxy
Vrata strežnika	Strežniško pristanišče strežnika proxy

■ Uporaba strežnika proxy

Omogočite uporabo posredniškega strežnika.

Naslov strežnika	Naslov strežnika proxy, ki ga uporablja to omrežje.
Vrata strežnika	Vrata strežnika proxy, ki se uporabljajo v tem omrežju.

Omejitve brezžičnega interneta

Tu lahko določite različne omejitve za Wifi.

Omogočanje omrežja WiFi	Dovolite/zaklenite brezžično omrežje WiFi
Omogočanje souporabe interneta	Omogočanje uporabe vroče točke
Omogočanje samodejnega povezovanja z občutljivimi vročimi točkami WiFi	Omogočanje samodejnega povezovanja z občutljivimi vročimi točkami WiFi
Omogočanje ročne konfiguracije WiFi	Uporabniku omogočite povezavo z omrežji WiFi, ki jih AppTec ni opredelil.
Frekvenca skeniranja WLAN	Določi interval pregledovanja WLAN. Višja vrednost poveča sposobnost prepoznavanja omrežij WIFI.

VPN

Tukaj izvedite ustrezne nastavitve za konfiguracijo povezav VPN.

Ime povezave	Navedeno ime povezave		
Vrsta VPN	Povezava VPN za posamezno aplikacijo se uporablja za zaščito prometa določenih aplikacij.		
	VPN	Vedno vklopljeno	To bo samodejno povežalo omrežje VPN ob prijavi in bo ostalo povezano, dokler ga uporabnik ročno ne odklopi.
	VPN za posamezno aplikacijo	Aplikacije VPN	Opredelevanje aplikacij, ki uporabljajo to povezavo VPN
		Zaklepanje za posamezno aplikacijo	Z zaklepanjem na aplikacijo omogočite izbranim aplikacijam povezljivost samo prek te povezave VPN. Ta funkcija je odvisna od požarnega zidu Windows Defender.
Profil WIP	WIP domena za to povezavo	ID podjetja, ki je potreben za povezavo tega profila VPN s politiko Windows Information Protection (WIP).	

Vrsta povezave

AppTec360 VPN	
Za aplikacijo AppTec360 VPN je potrebno, da je dovoljeno sideloading aplikacij. Omogočite možnost "Allow App Sideloading" v "Security Management" → "Restriction Settings" → "Device Functionality".	
Konfiguracija vrat	Če želite konfigurirati povezavo VPN s črnim seznamom, izberite konfiguracijo VPN z določenim strežnikom DNS. Konfiguracijo VPN lahko nastavite v razdelku "Splošne nastavitve" → "Univerzalni prehod" → "Nastavitve VPN".

IKEv2		
Strežniki	Seznam strežnikov VPN	
Predor naprave	Omogoči povezavo pred prijavo uporabnika.	
Način preverjanja pristnosti	EAP	EAP XML
	Potrdila strojev	
Algoritem šifriranja		
Algoritem za preverjanje celovitosti		
Diffie-Hellmanova skupina		
Algoritem za transformacijo šifre		
Algoritem transformacije avtentikacije		
Skupina za popolno tajnost naprej (PFS)		

PPTP		
Strežniki	Seznam strežnikov VPN	
Način preverjanja pristnosti	EAP	EAP XML

L2TP		
Strežniki	Seznam strežnikov VPN	
Način preverjanja pristnosti	EAP	EAP XML
Algoritem šifriranja		
Algoritem za preverjanje celovitosti		
Diffie-Hellmanova skupina		
Algoritem za transformacijo šifre		
Algoritem transformacije avtentikacije		
Skupina za popolno tajnost naprej (PFS)		

Samodejno		
Strežniki	Seznam strežnikov VPN	
Način preverjanja pristnosti	EAP	EAP XML

Splošne konfiguracije VPN

Zapomnite si poverilnice ob vsaki prijavi	
Registracija naslovov IP z notranjim sistemom DNS	
Pravila za filtriranje omrežnega prometa	Omejite povezavo VPN na določen nabor pravil.
Seznam za iskanje končnic DNS	končnice DNS, ki jih dodamo na seznam iskanja DNS za usmerjanje kratkih imen.
Pravila tabele NRPT (Name Resolution Policy Table)	Pravila NRPT (Name Resolution Policy table) določajo, kako DNS razrešuje imena, ko je povezan z omrežjem VPN.
Zaznavanje zaupanja vrednega omrežja	Seznam končnic DNS za prepoznavanje zaupanja vrednega omrežja.
Razdeljeno tuneliranje	Razdeljeno tuneliranje pomeni, da lahko promet poteka prek kateregakoli vmesnika, ki ga določi omrežni niz.
Razdelitev poti za tuneliranje	Seznam poti, ki jih je treba dodati v usmerjevalno tabelo za vmesnik VPN.
Nastavitev posredniškega strežnika	Konfigurira proxy, ki se uporablja v tem omrežju
Naslov pooblaščenca	Naslov strežnika proxy kot polno kvalificirano ime gostitelja ali naslov IP.
Pristanišče	Vrata strežnika proxy.
URL za samodejno konfiguracijo proxyja	URL, da samodejno pridobi nastavitve proxyja.

Omejitve VPN

Tu lahko določite različne omejitve VPN.

Omogočanje nastavitve VPN	Ta smernica uporabniku omogoča/prepoveduje deaktiviranje in spreminjanje nastavitve VPN.
Omogočanje omrežja VPN prek mobilne telefonije	dovoli/prepoveduje napravi vzpostavitev povezave VPN, če naprava uporablja mobilne podatke.
Omogočanje gostovanja VPN prek mobilne telefonije	dovoli/prepoveduje napravi vzpostavitev povezave VPN, če naprava gostuje.

Bluetooth

Tu lahko določite, ali naj bo Bluetooth dovoljen/prepovedan.

Omogoči Bluetooth	Vključitev/izključitev povezave Bluetooth
-------------------	---

Upravljanje PIM

Exchange Active Sync

Nastavitev računa ActiveSync v napravi končnega uporabnika

Ime računa	Ime e-poštnega računa
Ime gostitelja strežnika	Naslov strežnika/FQDN
Ime domene	Domena strežnika
Elektronski naslov	E-poštni naslov
Uporabniško ime	Uporabniško ime
Uporabniško geslo	Po želji lahko tukaj uporabniku že pripnete geslo.
Uporaba protokola SSL	Uporaba povezave SSL
Interval sinhronizacije	Tu lahko določite interval sinhronizacije. Ročna sinhronizacija = Uporabnik mora prenesti e-pošto in opraviti ročno sinhronizacijo.
Filter starosti pošte	Čas, v katerem je treba e-pošto sinhronizirati Brez filtra = neomejeno
Raven dnevnika	Določitev ravni beleženja za promet ActiveSync
Sinhronizacija e-pošte	Aktivirano = e-poštna sporočila so sinhronizirana
Sinhronizacija stikov	Aktivirano = stiki so sinhronizirani
Sinhronizacija koledarja	Aktivirano = koledar je sinhroniziran
Sinhronizacija opravil	Aktivirano = naloge so sinhronizirane

Elektronska pošta

Vzpostavitev računov POP3/IMAP4 v napravi končnega uporabnika.

Opis računa	Ime e-poštnega računa
Ime pošiljatelja	Prikazano ime pošiljatelja
Ime domene	Ime domene za e-poštni račun
Elektronski naslov	Elektronski naslov uporabnika
Uporabniško ime	Uporabniško ime
Uporabniško geslo	Po želji lahko tukaj uporabniku že pripnete geslo.
Alternativna pooblastila za odhodni strežnik	Tu lahko določite, ali so za odhodni strežnik potrebne druge poverilnice.
Ime izhodne domene	Ime izhodne domene
Uporabniško ime odhodnega strežnika	Uporabniško ime odhodnega strežnika
Geslo za odhodni strežnik	Geslo odhodnega strežnika
Protokol e-pošte	POP3 ali IMAP4 se lahko uporablja kot protokol
Gostiteljsko ime strežnika dohodne pošte	Ime gostitelja strežnika dohodne pošte
Uporaba SSL za dohodno pošto	Uporaba SSL za dohodna e-poštna sporočila
Gostiteljsko ime strežnika odhodne pošte	Ime gostitelja strežnika odhodne pošte
Uporaba SSL za odhodno pošto	Uporaba SSL za odhodna e-poštna sporočila
Preverjanje pristnosti odhodnega strežnika	Potrebna je avtentikacija odhodnega strežnika.
Interval sinhronizacije	Tu lahko določite interval sinhronizacije. Ročna sinhronizacija = Uporabnik mora prenesti e-pošto in opraviti ročno sinhronizacijo.
Filter starosti pošte	Čas, v katerem je treba e-pošto sinhronizirati Brez filtra = neomejeno

Upravljanje aplikacij

Upravitelj aplikacij za podjetja

■ Nameščene aplikacije

Tukaj je seznam aplikacij, ki so trenutno nameščene v prikazani napravi.

■ Obvezne aplikacije

Tu lahko nastavite seznam aplikacij, ki so obvezne v napravi.

Ta seznam se preveri vsakič, ko se naprava poveže z MDM, in se namestijo vse aplikacije s tega seznama, ki niso nameščene v napravi, ne glede na to, ali je bila aplikacija odstranjena ali ni bila nikoli prej nameščena.

Prenesete lahko domače aplikacije Windows 10 in jih nato dodate na ta seznam ali pa dodate konfiguracije Microsoft Office, ki jih je treba predhodno konfigurirati v "Splošne nastavitve" > "Upravljanje aplikacij" > "Microsoft Office".

| Omejitve aplikacij sistema

Aplikacije Prejeto
Omogočanje alarmov in ure
Dovolite kalkulator
Dovolite kamero
Omogočite podporo za stike
Dovolite Cortani
Dovolite Raziskovalcu datotek
Dovolite, da začnete
Dovolite Groove Music
Omogočite zemljevide
Omogočanje sporočil
Dovolite Microsoft Edge
Dovolite filme in televizijo
Dovolite denar
Dovolite novice
Dovolite storitev OneDrive
Dovolite OneNote
Dovolite Outlookov koledar in pošto
Omogočite ljudem
Dovolite telefon
Dovolite fotografije
Dovolite Powerpoint
Dovolite nastavitve
Dovolite Skype
Dovolite športne aktivnosti
Dovolite trgovino
Dovolite glasovni snemalnik
Dovolite denarnico
Dovolite vreme

Dovolite vozlišče za povratne informacije Windows
Dovolite besedo
Omogočanje konzole Xbox

Nastavitev strani
Dovolite račune Delovno mesto
Omogoči napredne informacije
Omogočanje aplikacij v kotičku
Dovolite blokiranje in filtriranje
Omogoči barvni profil
Dovoli način vožnje
Dovolite e-pošto in račune
Dovolite izenačevalnik
Dovoli tipkovnico
Dovolite navigacijsko vrstico
Omogočanje načina letenja v omrežju
Dovolite skupno rabo interneta v omrežju
Dovolite omrežne storitve
Dovolite omrežje Wi-Fi
Omogočanje sistema Bluetooth v računalniku
Dovolite, da ocenite svojo napravo
Dovoli obnovitev Posodobitev
Omogočanje souporabe
Dovoli začetek
Dopustite čas Jezik
Dovoli čas Regija
Dovolite privzeto zaklepanje zaslona Windows
Dovolite delovni ali šolski račun

Črna in bela lista

V razdelku "Črna in bela lista" lahko izbirate med načinom "Bela lista" in načinom "Črna lista".

Bela lista	V napravo končnega uporabnika je mogoče namestiti samo aplikacije in storitve, ki so dodane na seznam. Če so te že predhodno nameščene v napravi končnega uporabnika, bodo aktivirane in nastavljene tako, da jih bo uporabnik lahko zagnal.
	Vseh drugih aplikacij, ki niso dodane na seznam, ni mogoče namestiti v napravo končnega uporabnika. Če so te aplikacije že predhodno nameščene v napravi končnega uporabnika, bodo deaktivirane in nastavljene tako, da jih uporabnik ne bo mogel zagnati.
Črni seznam	Aplikacij in storitev, ki so dodane na seznam, ni mogoče namestiti v napravo končnega uporabnika. Če so te že predhodno nameščene v napravi končnega uporabnika, bodo deaktivirane in nastavljene tako, da jih uporabnik ne bo mogel zagnati.
	Vse druge aplikacije, ki niso dodane na seznam, je mogoče namestiti v napravo končnega uporabnika. Če so te že predhodno nameščene v napravi končnega uporabnika, bodo aktivirane in nastavljene tako, da jih bo uporabnik lahko zagnal.

Prek gumba , na seznam trenutno uporabljenih aplikacij ali storitev dodajate dodatne aplikacije ali storitve.

Prek gumba , na trenutno neaktivni seznam dodate dodatne aplikacije ali storitve.

Aplikacijo lahko dodate iz trgovine Windows App Store ali neposredno vnesete "identifikator aplikacije" in jo dodate na črni ali beli seznam.

Konfiguracija sistema MacOS

Glede na to, ali ste izbrali profil ali napravo, se prikaz in njegove podtočke razlikujejo - na to bodite pozorni!

Splošno

Pregled profila skupine (samo na ravni skupine)

Ko odprete profil skupine, dobite hiter pregled profila.

Profile Name	Default Group Profile
Operating System	Android
Created At	01.03.2021 09:52:54
Created By	John Doe
Last Change	31.08.2021 16:35:50
Changed By	John Doe
Current Profile Revision	16
Released Profile Revision (outdated)	14

Delete Profile
Reset Group Profile
Copy Profile

Ime profila	Ime profila (tukaj ga lahko spremenite)
Operacijski sistem	Operacijski sistem, za katerega je profil namenjen
Ustvarjeno na	Čas nastanka
Ustvaril je	Ustvarjalec profila
Zadnja sprememba	Čas zadnje spremembe profila
Spremenjeno s	Račun, ki je opravil zadnje spremembe
Trenutna revizija profila	Revizija stanja shranjenega profila
Objavljena revizija profila	Dodeljena revizija profila ("Assigned profile revision"). Če je za besedilom na etiketi "(zastarela)", to pomeni, da ste profil shranili, vendar ga še niste dodelili, zato bodo naprave še vedno dobile starejšo različico.

Pregled naprave (samo na ravni naprave)

Povzetek pregleda naprave.

Ime naprave	Ime naprave
Model	Model
Operacijski sistem	Operacijski sistem
Serijska številka	Serijska številka naprave
Lastništvo naprave	Konfigurirana vrsta lastništva
Vrsta naprave	Vrsta naprave
V skladu s predpisi	Pokaže, ali je naprava skladna
Naslov IP	Naslov IP, s katerega je naprava povezana s strežnikom.
Nazadnje videno	Čas zadnje povezave iz naprave
Zadnji potisk	Čas zadnjega potiska, poslanega v napravo
Naloga	Tukaj lahko napravo premaknete k drugemu uporabniku ali skupini.

Revizija konfiguracije (samo na ravni naprave)

Tu boste dobili pregled nad tem, kateri profil skupine je dodeljen napravi.

Revision Overview			
	Installed Profile	Assigned Profile	Last Generated Profile
Device Profile	Device Profile: Revision 5	Device Profile: Revision 5	Device Profile: Revision 5
Group Profile	Default Group Profile: Revision 13	Default Group Profile: Revision 13 (Newer Revision available)	Default Group Profile: Revision 13

Če kliknete na profil skupine, boste neposredno dostopali do profila in opravili nastavitve.

S simbolom lahko dodeljene aplikacije vrnete v nastavitve skupinskega profila.

S tem simbolom lahko ponastavite profil naprave, tako da nima nobenih nastavitvev.

"Na voljo je novejša revizija" pomeni, da je bil profil skupine spremenjen in shranjen, vendar ni dodeljen. Profil skupine je treba dodeliti s funkcijo "Assign now" na ravni skupine, da se spremembe uporabijo v napravah.

Dnevnik naprave (samo na ravni naprave)

Dnevnik ukazov

Tu si lahko ogledate, kateri ukazi so bili izdani za napravo in kakšen je njihov status.

Command Log (last 250 commands)					
#	Created By	Date modified	Command	State	
1	jd@example.com	31.08.2021 12:21:37	Install assigned profiles	Device Pushed	
2	jd@example.com	31.08.2021 12:10:04	Get installed apps	Command Executed	
3	jd@example.com	31.08.2021 12:10:04	Get managed apps	Command Executed	
4	jd@example.com	31.08.2021 12:10:02	Get certificates	Command Executed	
5	jd@example.com	31.08.2021 12:10:02	Get asset data	Command Executed	
6	System Automated	31.08.2021 05:34:29	Update profile revision	Command Partially Failed	!
7	System Automated	31.08.2021 05:34:29	Apply device settings	Command Executed	
8	System Automated	31.08.2021 05:34:27	Install application	Command Failed	!
9	System Automated	31.08.2021 05:34:25	Get installed apps	Command Executed	
10	System Automated	31.08.2021 05:34:25	Get managed apps	Command Executed	
11	System Automated	31.08.2021 05:34:23	Get certificates	Command Executed	

Ukazi, ustvarjeni s "Sistemska avtomatizirano", se samodejno ustvarijo v sistemu.

Možni statusi ukazov

Potisnjena naprava	Storitvi za potiskanje (npr. APNS) je bila poslana potisna zahteva, da se naprava poveže nazaj s strežnikom EMM.
Ustvarjen ukaz	Ukaz je bil ustvarjen v sistemu.
Poslan ukaz	Ukaz je bil napravi poslan, ko se je povezala s strežnikom.
Izveden ukaz	Ukaz je bil uspešno izveden.
Ukaz ni uspel	Ukaz ni uspel. *
Ukaz delno ni uspel	Odvisno od operacijskega sistema naprave so lahko nekateri ukazi združeni. Pri tem nekateri deli te skupine ukazov niso bili uspešni. *
Ukaz se je izvršil, vendar je bil neuspešen	Ukaz je bil izveden, vendar morda ni bil.
Ukaz se ponovno premakne	Ukaz je ponovno poslal uporabnik.
Zavrženi	Ukaz je bil zavržen. Na primer zato, ker ga je nadomestil drug ukaz ali ker je bila naprava ponovno vpisana in so bili stari ukazi odstranjeni.

*Če je za sporočilom izklicnik, lahko več informacij dobite tako, da s kazalcem podrsate nad ikono.

Upravljanje sredstev (samo na ravni naprave)

Informacije o napravi

Številka modela	Številka modela
Ime gostitelja	Ime gostitelja
Lokalno gostiteljsko ime	Lokalno gostiteljsko ime
Operacijski sistem	Operacijski sistem
Različica operacijskega sistema	Različica operacijskega sistema
UDID	UDID
Prosti / skupni pomnilnik	Prosti / skupni pomnilnik

WiFi

Naslov IP	Naslov IP
WiFi MAC	WiFi MAC

Cellular

Telefonska številka	Telefonska številka
Status gostovanja	Status gostovanja
Gostovanje (glasovno/podatkovno)	Gostovanje (glasovno/podatkovno)
Naslov IP	Naslov IP
Operater/prevoznik	Operater/prevoznik
Omrežje operaterja SIM	Omrežje prevoznikov
Različica nosilca	Različica nosilca
ICCID	ICCID
Trenutni MCC/MNC	Trenutni MCC/MNC
SIM MCC/MNC	SIM MCC/MNC

Bluetooth

Bluetooth MAC	Bluetooth MAC
---------------	---------------

Upravljanje posodobitev (samo na ravni naprave)

Posodobitev informacij

Ta zavihek prikazuje informacije o nastavitvah posodobitve sistema v napravi.

Omogočen samodejni pregled	Če sistem samodejno preverja posodobitev.
Omogočeno samodejno posodabljanje aplikacij	Če bo sistem samodejno namestil posodobitve aplikacij.
Omogočene samodejne posodobitve operacijskega sistema	Če bo sistem samodejno namestil posodobitve OS.
Omogočene samodejne varnostne posodobitve	Če bo sistem samodejno namestil varnostne posodobitve.
Posodabljanje aplikacij v ozadju - Prenos je omogočen	Če bo sistem prenesel posodobitve aplikacij v ozadju.
URL kataloga	URL do kataloga posodobitev programske opreme, ki ga uporablja odjemalec.
Je privzeti katalog	Če je odgovor "da", je Katalog privzeti katalog.
Izvedite redni pregled	Če je odgovor "da", začnite novo pregledovanje.
Datum prejšnjega skeniranja	Datum zadnjega pregleda posodobitve programske opreme.
Rezultat prejšnjega skeniranja	Koda rezultata zadnjega pregleda posodobitve programske opreme.

Upravljanje varnosti

Boj proti kraji

Brisanje in zaklepanje

Celotno brisanje	Pošljite ukaz za tovarniško ponastavitev naprave
Izbris podjetja	Odstranite MDM iz naprave in odstranite vse podatke MDM (npr. račune, aplikacije).
Zaklepanje zaslona	Vrnitev naprave na zaklenjeni zaslon

Varnostna konfiguracija

Pristopna koda

Dovoljena deaktivacija kode	Določa, ali mora uporabnik nastaviti kodo PIN. S preprosto nastavitvijo te vrednosti (in ne z drugimi) uporabnik vnese geslo, ne da bi določil njegovo dolžino ali kakovost.
Dovolite preprosto vrednost	Uporabniku omogočite uporabo enakih, naraščajočih in zmanjšanih nizov števil (npr. 1234, 1111).
Zahtevajte črkovno-številčno vrednost	Gesla morajo vsebovati vsaj eno črko.
Najmanjša dolžina gesla	Minimalna dolžina gesla
Najmanjše število zapletenih znakov	Najmanjše število alfanumeričnih simbolov v geslu
Najvišja starost gesla	Število dni, po katerih je treba geslo spremeniti
Največja samodejna zapora	Najdaljši čas, po katerem se naprava zaklene
Najdaljše obdobje odloga za zaklepanje naprave	Koliko časa je lahko naprava zaklenjena, ne da bi se ob odklepanju zahtevala geselska koda
Največja starost gesla (1-730 dni ali nič)	Dnevi, po katerih je treba spremeniti geslo
Zgodovina geselskih kod (1-50 geselskih kod ali nobene)	Število edinstvenih geselskih kod pred ponovno uporabo

Potrdilo

PKCS#1	
Opis	Vnesite opis potrdila
Pooblastilo	Prenos datoteke pkcs1

PKCS#12	
Opis	Vnesite opis potrdila
Pooblastilo	Naložite datoteko pkcs12

Nastavitve omejitev

Funkcionalnost naprave

Dovolite kamero	Dovolite uporabo fotoaparata
Omogočite storitev Game Center	Če je vrednost napačna, je program Game Center onemogočen, njegova ikona pa je odstranjena z začetnega zaslona.
Omogočite igranje iger za več igralcev	Če je napačno, prepove igranje iger za več igralcev.
Omogočanje dodajanja prijateljev v storitvi Game Center	Če je vrednost napačna, prepove dodajanje prijateljev v storitev Game Center.
Omogočanje fototeke iCloud	Če je nastavljena na false, onemogoči knjižnico iCloud Photo Library. Vse fotografije, ki niso v celoti prenesene iz Fototeke iCloud v napravo, bodo odstranjene iz lokalne shrambe.
Dovoli ID dotika	Če je napačno, prepreči odklepanje naprave z ID-jem dotika.

iCloud

Blokiranje nekaterih funkcij med seznanjanjem z iCloudom

Omogočite sinhronizacijo dokumentov	Omogočite sinhronizacijo dokumentov
Omogočanje sinhronizacije iCloud Keychain	Omogočanje sinhronizacije iCloud Keychain
Omogočanje beležk iCloud	Če je napačno, onemogoči storitve MacOS iCloud Notes
Dovolite iCloud BTMM	Če je napačno, onemogoči storitev iCloud v operacijskem sistemu MacOS Back to My Mac.
Dovolite iCloud FMM	Če je vrednost lažna, onemogoči storitev iCloud v sistemu MacOS Find My Mac.
Dovolite zaznamke iCloud	Če je napačno, onemogoči sinhronizacijo zaznamka iCloud za MacOS.
Dovolite pošto iCloud	Če je vrednost napačna, onemogoči storitve iCloud v storitvi MacOS Mail.
Dovolite koledar iCloud	Če je vrednost napačna, onemogoči storitve iCloud v oblaku MacOS Cloud.

Omogočanje opomnikov iCloud	Če je napačno, onemogoči storitve opomnika iCloud.
Omogočanje imenika iCloud	Če je vrednost napačna, onemogoči storitve imeniške knjige iCloud v sistemu MacOS.

Upravljanje medijev

Izbriši ob odjavi	Izbrišite vse izmenljive medije ob odjavi
Dovolite omrežje	Dovolite dostop za omrežne medije
Dovolite notranji disk	Dovolite dostop do notranjega diska.
Zahteva za preverjanje pristnosti	Zahtevati preverjanje pristnosti za uporabo tega medija
Samo za branje	Uporabnik lahko bere podatke samo z medija.
Dovolite zunanji disk	Dovolite dostop do zunanjega diska.
Zahteva za preverjanje pristnosti	Zahtevati preverjanje pristnosti za uporabo tega medija
Samo za branje	Uporabnik lahko bere podatke samo z medija.
Dovolite uporabo slik diska	Dovolite dostop za slike.
Zahteva za preverjanje pristnosti	Zahteva za avtentikacijo za uporabo tega medija
Samo za branje	Uporabnik lahko bere podatke z medija samo
Omogočanje uporabe plošč DVD-RAM	Dovolite dostop do diska DVD-RAM.
Zahteva za preverjanje pristnosti	Zahteva za avtentikacijo za uporabo tega medija
Samo za branje	Uporabnik lahko bere podatke z medija samo
Dovolite uporabo DVD-jev	Dovolite dostop do diska DVD.
Zahteva za preverjanje pristnosti	Zahteva za avtentikacijo za uporabo tega medija
Dovolite uporabo zgoščenk	Dovolite dostop za disk CD.
Zahteva za preverjanje pristnosti	Zahteva za avtentikacijo za uporabo tega medija

Upravljanje povezav

Wi-Fi

Tu lahko dodate in konfigurirate povezave Wi-Fi

Identifikator nabora storitev (SSID)	SSID omrežja, s katerim bo vzpostavljena povezava
Samodejno pridruževanje	Omogočite samodejno pridružitve za omrežje
Skrito omrežje	Omogoči, če AP ne oddaja SSID.
Nastavitev posredniškega strežnika	Konfiguracija posredniškega strežnika za vsako dostopno točko
Ni	Ne uporabljajte strežnika proxy
Priročnik	Vzpostavitev ročnega pooblaščenca
URL strežnika proxy	Naslov za dostop do nastavitev posredniškega strežnika
Pristanišče	Določite vrata za posrednika
Preverjanje pristnosti	Uporabniško ime za preverjanje pristnosti v posredniškem strežniku
Geslo	Geslo za preverjanje pristnosti v posredniškem strežniku
Samodejno	Samodejna vzpostavitev pooblaščenca
URL strežnika proxy	URL za datoteko z nastavitvami posredniškega strežnika
Vrsta varnosti	Vzpostavitev varnostne vrste za AP
WEP	
Geslo	Geslo za AP
WPA/WPA2	
Geslo	Geslo za AP
WEP Enterprise - WPA / WPA2 Enterprise / Vsako podjetje	Glej tabelo Napaka: Ni mogoče najti referenčnega vira v nadaljevanju
Ni	Ne vzpostavi varnosti
Onemogočite naključno določanje naslovov MAC	Onemogoči naključno izbiranje naslovov MAC za to omrežje Wi-Fi, ko je povezano z omrežjem. To prikaže tudi opozorilo o zasebnosti v nastavitvah, ki označuje, da ima omrežje zmanjšano zaščito zasebnosti.

Konfiguracija omrežja Wi-Fi v podjetju

Opomba: Na voljo je samo, če je možnost "Vrsta varnosti" nastavljena na vrsto podjetja.

Protokoli	Protokol avtentikacije, ki ga podpira ciljno omrežje
TLS	Omogoči / onemogoči uporabo
TTLS	Omogoči / onemogoči uporabo
Notranje preverjanje pristnosti	Protokol za preverjanje pristnosti, ki ga je treba uporabiti: PAP, CHAP, MSCHAP, MSCHAPv2
LEAP	Omogoči / onemogoči uporabo
PEAP	Omogoči / onemogoči uporabo
EAP-FAST	Omogoči / onemogoči uporabo
EAP-SIM	Omogoči / onemogoči uporabo
Uporaba PAC	Uporaba sistema PAC (zaščitena nadzora dostopa)
Določba PAC	Konfiguracija sistema Provision PAC
Anonimno zagotavljanje PAC	Anonimno zagotavljanje PAC
Preverjanje pristnosti	
Uporabniško ime	Uporabniško ime za preverjanje pristnosti
Ne uporabljajte Na povezavo Geslo	Ne uporabljajte gesla na povezavo
Geslo	Uporabljeno geslo
Potrdilo o identiteti	Prenos/izbira potrdila za preverjanje pristnosti
Zunanja identiteta	Identiteta, ki je vidna navzven
Zaupanje	
Zaupanja vredno potrdilo 1	Prenesite prvo zaupanja vredno potrdilo
Zaupanja vredno potrdilo 2	Naložite drugo zaupanja vredno potrdilo
Zaupanja vredno potrdilo 3	Prenos tretjega zaupanja vrednega potrdila
Zaupanja vreden strežnik	Imena pričakovanih strežniških potrdil

Imena potrdil	(na seznamu, ločenem z vejico)
---------------	--------------------------------

VPN

Glede na izbrano vrsto povezave so lahko vidna različna polja.

Ime povezave	Ime profila VPN
Vrsta VPN	
VPN	Ves omrežni promet naprave bo usmerjen prek povezave VPN.
Vrsta povezave	Vzpostavitev vrste povezave VPN
IPsec (cisco)	Protokol IPsec podjetja cisco
L2TP	Protokol L2TP
SSL po meri	Povezava prek SSL po meri
IKEv2	Protokol IKEv2
Nastavitev posredniškega strežnika	Konfiguracija posredniškega strežnika za povezavo VPN
Ni	Vzpostavitev brez pooblaščenca
Priročnik	Ročna vzpostavitev posredniškega strežnika
URL strežnika proxy	Naslov za dostop do nastavitev posredniškega strežnika
Pristanišče	Določite vrata za posrednika
Preverjanje pristnosti	Uporabniško ime za preverjanje pristnosti v posredniškem strežniku
Geslo	Geslo za preverjanje pristnosti v posredniškem strežniku
Samodejno	Samodejna vzpostavitev pooblaščenca
URL strežnika proxy	URL za dostop do nastavitev posredniškega strežnika

Proxy strežnik HTTP

Vrsta pooblaščenca	
Priročnik	Ročno vzpostavite proxy strežnik
URL strežnika proxy	Naslov za dostop do nastavitve posredniškega strežnika
Pristanišče	Vzpostavitev pristanišča posredniškega strežnika
Preverjanje pristnosti	Uporabniško ime za preverjanje pristnosti v posredniškem strežniku
Geslo	Geslo za preverjanje pristnosti v posredniškem strežniku
Samodejno	Samodejna vzpostavitev pooblaščenca
URL naslov proxy PAC	URL naslov proxy PAC
Omogoči neposredno povezavo, če je PAC nedosegljiv	Omogočite neposredno povezavo (brez VPN), če PAC ni dosegljiv
Omogočanje izogibanja posredniškemu strežniku za dostop do omrežij v ujetništvu	Omogočanje izogibanja posredniškemu strežniku za dostop do notranjih omrežij v ujetništvu

AirPrint

Naslov IP	Naslov IP tiskalnika
Pot virov	Določena pot do naprave AirPrint

AirPlay

Ime naprave	Ime naprave
Geslo	Geslo za seznanjanje
Bela lista	Opredelitev seznama naprav, s katerimi se lahko naprava izključno poveže

Upravljanje PIM

Exchange Active Sync

Ime računa	Ime računa.
E-poštni naslov	Naslov računa (npr. max@company.com)
Gostiteljsko ime strežnika	Notranje gostiteljsko ime
Prijavno ime	"Domain" in "Login Name" morata biti prazna, da naprava pozove k prijavi uporabnika.
Domena	"Domain" in "Login Name" morata biti prazna, da naprava pozove k prijavi uporabnika. Če je omogočena konfiguracija vrat ACL in polje Domain ni prazno, bo AppTec360 Universal Gateway avtentificiral napravo z naslednjim imenom "Domain\Login Name".
Geslo	Geslo za račun (npr. secretUserPassword)
Pretekli dnevi programa Mail to Sync	Število preteklih dni pošte za sinhronizacijo
Uporaba protokola SSL	Uporaba SSL za notranje gostitelje Exchange Host
Napredna možnost	Prikaži napredne možnosti
Vrata strežnika	Notranja vrata
Pot strežnika	Notranja pot
Zunanje gostiteljsko ime	Zunanji gostitelj
Zunanja vrata	Zunanja vrata
Zunanja pot	Zunanja pot
Uporaba SSL za zunanje Gostitelj izmenjave	Uporaba SSL za zunanje gostitelje Exchange Host

Elektronska pošta

Nastavitev računov POP3 / IMAP v napravi končnega uporabnika

Opis računa	Ime des E-poštni računi
Vrsta računa	
IMAP	
Predpona poti	Predpona poti za posebne mape
POP	
Prikazno ime uporabnika	Prikazno ime uporabnika
Elektronski naslov	Elektronski naslov uporabnika

Dohodna pošta	Nastavitve dohodnega strežnika
Naslov poštnega strežnika	Naslov poštnega strežnika
Vrata poštnega strežnika	Vrata poštnega strežnika
Uporabniško ime	Ustrezno uporabniško ime
Vrsta preverjanja pristnosti	Vrsta preverjanja pristnosti
Ni	Ne Vrsta preverjanja pristnosti
Geslo (samo na ravni naprave)	Poziv za geslo
MDM izziv-odgovor	
NTLM	Preverjanje pristnosti NTLM
HTTP MD5 Digest	
Uporaba protokola SSL	Po potrebi uporabite SSL

Odhodna pošta	Nastavitve odhodnega strežnika
Naslov poštnega strežnika	Naslov poštnega strežnika
Vrata poštnega strežnika	Vrata poštnega strežnika
Uporabniško ime	Ustrezno uporabniško ime
Vrsta preverjanja pristnosti	
Ni	Ni metode avtentikacije
Geslo (samo na ravni naprave)	Poziv za geslo
MDM izziv-odgovor	
NTLM	Preverjanje pristnosti NTLM
HTTP MD5 Digest	
Uporaba protokola SSL	Po potrebi uporabite SSL
Odhodno geslo enako kot dohodno	Odhodno geslo enako kot vhodno
Uporabljajte samo v pošti	Aktivirajte, če naj se vsa odhodna e-poštna sporočila pošiljajo prek aplikacije Mail-App.

CalDav

Konfiguracija vzpostavitve in distribucije računa CalDav

Opis računa	Prikazno ime računa
Ime gostitelja	Ime gostitelja in/ali naslov IP
Pristanišče	Pristanišče računa CalDav
Glavni naslov URL	Glavni naslov URL računa
Uporabniško ime	Ustrezno uporabniško ime CalDav
Geslo (samo na ravni naprave)	Ustrezno geslo CalDav
Uporaba protokola SSL	Po potrebi uporabite SSL

CardDav

Konfiguracija vzpostavitve in distribucije računa CardDav

Opis računa	Prikazno ime računa
Ime gostitelja	Ime gostitelja in/ali naslov IP
Pristanišče	Pristanišče računa CardDav
Glavni naslov URL	Glavni naslov URL računa
Uporabniško ime	Ustrezno uporabniško ime CardDav
Geslo (samo na ravni naprave)	Ustrezno geslo CardDav
Uporaba protokola SSL	Po potrebi uporabite SSL

LDAP

Na tem področju nastavite povezavo LDAP, da omogočite dinamično izmenjavo potrdil med napravo končnega uporabnika in imenikom Active Directory.

Upoštevajte, da izbrani uporabnik potrebuje ustrezno dovoljenje za branje.

Opis računa	Opis računa
Uporabniško ime računa	Uporabnik za dostop do protokola LDAP
Geslo računa	Geslo za dostop do protokola LDAP
Ime gostitelja računa	Gostiteljsko ime/IP naslov strežnika LDAP
Uporaba protokola SSL	Po potrebi uporabite SSL

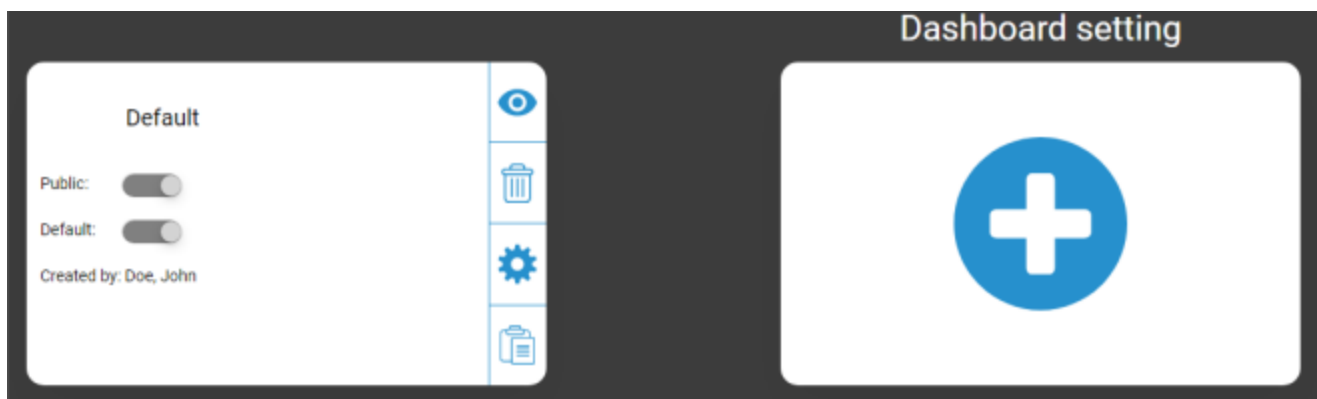
V drugem delu lahko določite posamezne filtre za iskanje v registru LDAP.

Opis	Področje uporabe	Osnova za iskanje
Opis filtra	Raven iskanja v registru LDAP	Opredelitev posameznega filtra

Nadzorna plošča in poročanje

Nastavitve armaturne plošče

Tu lahko vidite, katere nadzorne plošče obstajajo, jih urejate ali ustvarite nove. Vsaka nadzorna plošča ima svoj nabor podatkov za prikaz in konfiguracijo grafikona.



Nadzor nastavitve armaturne plošče

Javna stran	Nadzorno ploščo nastavi kot javno, tako da jo lahko vidijo tudi drugi uporabniki. Uporabniki morajo seveda imeti možnost prijave in ogleda nadzornih plošč. Če možnost "Javno" ni aktivirana, jo lahko vidi samo ustvarjalec.
Privzeto	Privzeto nastavi armaturno ploščo, tako da se samodejno odpre ob naslednjem dostopu do pogleda armaturne plošče.
	Prikaz nadzorne plošče in njenih grafov
	Brisanje armaturne plošče
	Urejanje imena in nastavitve nadzorne plošče
	Naredite kopijo nadzorne plošče
	Dodajanje popolnoma nove armaturne plošče

Pogled na armaturno ploščo

Prikaže podatke in grafe izbrane nadzorne plošče ter omogoča njihovo spreminjanje.



Nadzor armaturne plošče

Določite, kateri podatki se prikažejo na nadzorni plošči, koliko podatkov se prikaže in v kakšni velikosti se ti podatki prikažejo.
Vrne vas nazaj na pregled armaturne plošče
Ponastavitev trenutno odprte armaturne plošče na privzeto nastavitev
shrani vse spremembe, ki ste jih naredili na trenutno odprti nadzorni plošči (npr. katere podatke želite prikazati).
Spremeni vrsto grafikona na grafikon stebrov
Spremeni vrsto grafikona na pitasti grafikon
Spremeni vrsto grafikona na diagram krofa
Spremeni vrsto grafikona na polarni diagram območja
Spreminjanje vrstnega reda razvrščanja

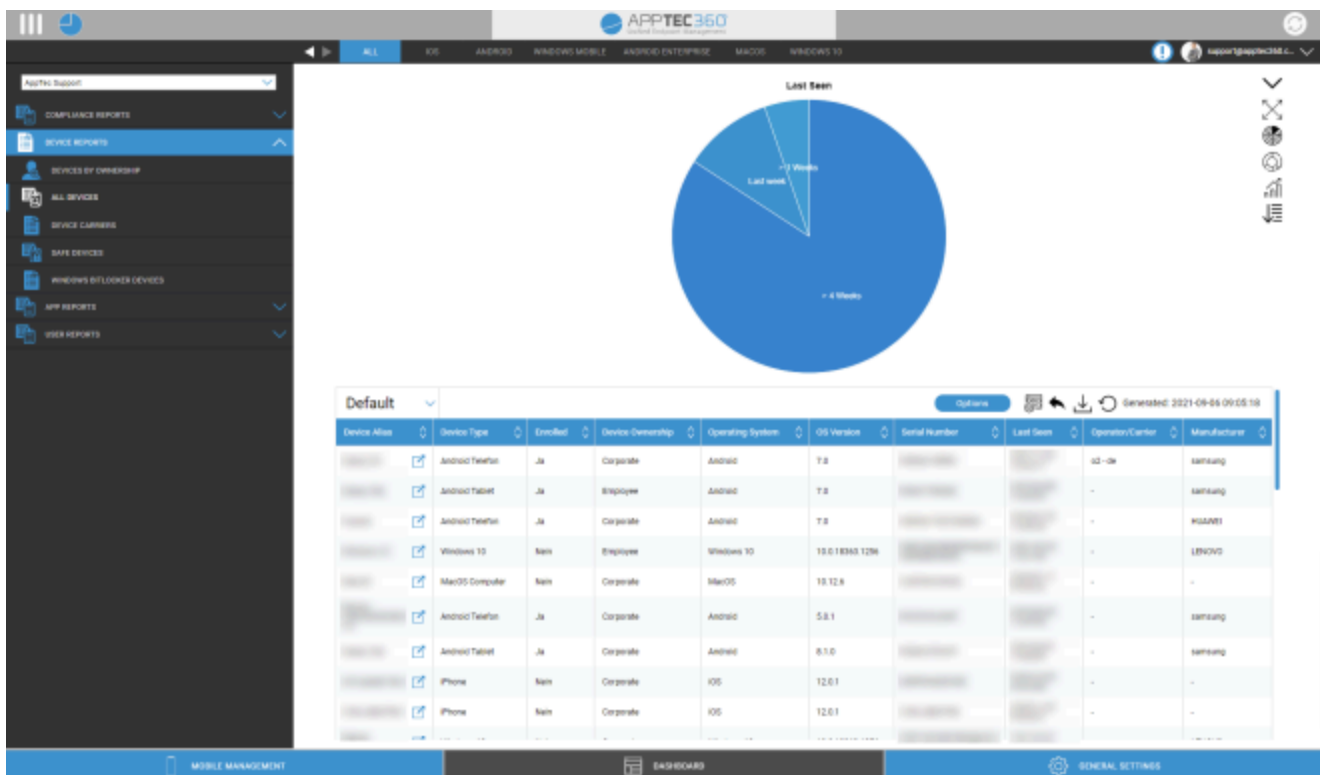
Razširjeno poročanje

"Razširjeno poročanje" ponuja podrobne preglede in grafe informacij o napravah in uporabnikih.

Obstaja nekaj privzetih poročil, vendar lahko vsa poročila ročno spremenite in dodate ali odstranite podatke, ki jih želite prikazati.

Upoštevajte, da lahko samo ročno spremenite prikazane podatke. Izbrana kategorija poročila določa, na katerih podatkih temelji. Npr. v poročilu o napravah z operacijskim sistemom iOS nikoli ne boste mogli prikazati naprav z operacijskim sistemom Android v Poročilih o napravah Vse naprave z operacijskim sistemom iOS

V zgornjem levem kotu lahko podatke poročanja omejit na določeno skupino (in vse njene podskupine). Privzeto je to nastavljeno na korensko vozlišče, zato so upoštevane VSE naprave in uporabniki.



Razširjen nadzor nad poročanjem

V vsakem pregledu lahko z naslednjimi funkcijami spreminjate poročilo na poljuben način:

Skrij grafikon (Če je grafikon prikazan)
Prikaži grafikon (Če je grafikon skrit)
Razširite grafikon (Če je grafikon zložen)
Zbrišite grafikon (Če je grafikon razširjen)
Spremeni vrsto grafikona na grafikon stebrov
Spremeni vrsto grafikona na pitasti grafikon
Spremeni vrsto grafikona na diagram krofa
Spremeni vrsto grafikona na polarni diagram območja
Spreminjanje vrstnega reda razvrščanja
Spremenite naslednje dele prikazanega pregleda: <ul style="list-style-type: none"> • Dodajanje/odstranjevanje stolpcev • Določite vrstni red prikaza stolpcev • Prikaži/skrij graf nad tabelo • Izberite stolpec, ki se uporablja za graf • Filtriranje podatkov v tabeli
Odprite upravitelja nastavitev, da shranite in naložite različna poročila.
Ponastavitev trenutno odprtega poročila na privzeto vrednost
Izvozite trenutno poročilo kot datoteko .csv
Ponovno generiranje podatkov in ponovno nalaganje trenutnega poročila

Seznam vseh privzetih poročil najdete na naslednjih straneh.

Poročila o skladnosti

Ukoreninjene naprave

Pregled naprav, ki so bile zakoreninjene/spremembe za zagon.

Privzeti stolpci tega poročila:

Vzdevek naprave
Lastnik naprave
E-naslov
Operacijski sistem
Telefonska številka
Nazadnje videno
Proizvajalec

Naprave za gostovanje

Pregled vseh naprav, ki gostujejo

Privzeti stolpci tega poročila:

Vzdevek naprave
Lastnik naprave
E-naslov
Vrsta naprave
Operacijski sistem
Telefonska številka
Nazadnje videno

Naprave z omogočenim gostovanjem

Pregled vseh naprav, ki so aktivirale gostovanje, vendar ni nujno, da trenutno gostujejo.

Privzeti stolpci tega poročila:

Vzdevek naprave
Lastnik naprave
E-naslov
Vrsta naprave
Operacijski sistem
Telefonska številka
Nazadnje videno

Nadzorovane naprave

Pregled vseh naprav, ki so nadzorovane v nadzorovanem načinu (samo iOS)

Privzeti stolpci tega poročila:

Vzdevek naprave
Lastnik naprave
E-naslov
Vrsta naprave
Nazadnje videno

Neaktivne naprave

Pregled vseh naprav, ki se v zadnjih 7 dneh niso povezale s strežnikom.

Privzeti stolpci tega poročila:

Vzdevek naprave
Lastnik naprave
E-naslov
Vrsta naprave
Operacijski sistem
Nazadnje videno

Poročila o napravah

Naprave po lastništvu

Tukaj si lahko ogledate, koliko naprav je trenutno nameščenih kot naprave za podjetja (službene naprave) in naprave za zaposlene (zasebne naprave).

Privzeti stolpci tega poročila:

Vzdevek naprave
Lastnik naprave
Vrsta naprave
Lastništvo naprave
Operacijski sistem

Vse naprave

Tu si lahko ogledate pregled vseh naprav z najpomembnejšimi informacijami.

Privzeti stolpci tega poročila:

Vzdevek naprave
Vrsta naprave
Vpisano na
Lastništvo naprave
Operacijski sistem
Različica operacijskega sistema
Serijska številka
Nazadnje videno
Operater/prevoznik
Proizvajalec

Nosilci naprav

Tu si lahko ogledate pregled operaterja (ponudnika mobilnih storitev).

Privzeti stolpci tega poročila:

Vzdevek naprave
Lastnik naprave
E-naslov
Operacijski sistem
Različica operacijskega sistema
Operater/prevoznik

Naprave SAFE

Tukaj si lahko ogledate pregled naprav, ki uporabljajo različico SAFE.

Ker je pregled in/ali SAFE na voljo samo za naprave Samsung, pod to točko ne boste videli običajnih zavihkov.

Privzeti stolpci tega poročila:

Vzdevek naprave
Lastnik naprave
E-naslov
Vrsta naprave
Nazadnje videno
Različica SAFE

Naprave Windows BitLocker

Tukaj si lahko ogledate pregled naprav Windows, ki uporabljajo program BitLocker.

Privzeti stolpci tega poročila:

Vzdevek naprave
Lastnik naprave
E-naslov

Stanje programa BitLocker

Poročila o aplikacijah

Tu so na voljo različni pregledi aplikacij. V vseh teh poročilih lahko kliknete na vnos in si ogledate, katere različice so nameščene v napravah in kako pogosto. V tem pogledu lahko ponovno kliknete na določeno različico, da vidite, v katerih napravah je ta različica nameščena.

Opomba: Lahko traja nekaj časa, dokler sistem ne dobi posodobljenih informacij iz naprave. Poleg tega se poročila ne posodablja vsako minuto. Morda boste morali biti potrpežljivi, da boste videli trenutno stanje, če ste pravkar dodelili novo aplikacijo ali različico. Z ročnim ponovnim nalaganjem poročila se bodo v poročilu prikazali najnovejši podatki, ki so na voljo

Nameščene aplikacije

Tu dobite pregled vseh nameščenih aplikacij.

Privzeti stolpci tega poročila:

Ime	Ime zadevne aplikacije in/ali storitve
Identifikator	Določen ID aplikacije/storitve
Skupno število	Kako pogosto je bila ta aplikacija/storitev nameščena v naprave končnega uporabnika.

Najbolj nameščene aplikacije

Tu dobite pregled aplikacij, ki so bile največkrat nameščene.

Privzeti stolpci tega poročila:

Ime	Ime zadevne aplikacije in/ali storitve
Identifikator	Določen ID aplikacije/storitve
Skupno število	Kako pogosto je bila ta aplikacija/storitev nameščena v naprave končnega uporabnika.

Obvezne aplikacije

Tu je na voljo pregled obveznih (obveznih zahtevanih) aplikacij.

Privzeti stolpci tega poročila:

Ime	Ime zadevne aplikacije in/ali storitve
Identifikator	Določen ID aplikacije/storitve
Vir aplikacije	Katera trgovina AppStore je vključena: <ul style="list-style-type: none"> • Trgovina Google PlayStore (Android) • Trgovina z aplikacijami iTunes (iOS)
OS	Operacijski sistem

Aplikacije na črnem seznamu

Tu dobite pregled vseh opredeljenih aplikacij na črni listi.

Privzeti stolpci tega poročila:

Ime	Ime zadevne aplikacije in/ali storitve
Identifikator	Določen ID aplikacije/storitve
Vir aplikacije	Katera trgovina AppStore je vključena: <ul style="list-style-type: none"> • Trgovina Google PlayStore (Android) • Trgovina z aplikacijami iTunes (iOS)
OS	Operacijski sistem

Poročila uporabnikov

Tarifa

Tu dobite pregled telefonskih tarif in kartic SIM svojih uporabnikov.

Privzeti stolpci tega poročila:

E-naslov
Ime
phoneNumber
nosilec
tarifa
možnost
cena
pogodbaOdpovedana
contractStart
duringTime
mobileAndData
dataVolume
multiSIM
vrsta
simCardSerial1
simCardSerial2
simCardSerial3
pin1
pin2
puk1
puk2
Opomba

Upravljanje več najemnikov

AppTec360 EMM lahko gosti več ločenih najemnikov, vsak s svojimi uporabniki in skupinami, dovoljenji in globalnimi nastavitvami.

Če želite omogočiti večpredstavnostne zmogljivosti, jih morate omogočiti v konfiguracijskem vmesniku naprave v tretjem koraku - Nastavitve strežnika.

Maximum Upload Size (e.g for In-House Apps)	20	Megabyte
Enable Debug Logging	<input type="checkbox"/>	
If you want to run multiple clients (e.g different Accounts for different Companies) on this appliance, enable this setting. After enabling, please set the Server Manager Credentials below. Keep in mind, that you need an additional license for each client. If you don't want to run multiple clients on this appliance, you can ignore this setting.		
Use Appliance as a Multitenant System	<input checked="" type="checkbox"/>	

License- & Servermanager Settings

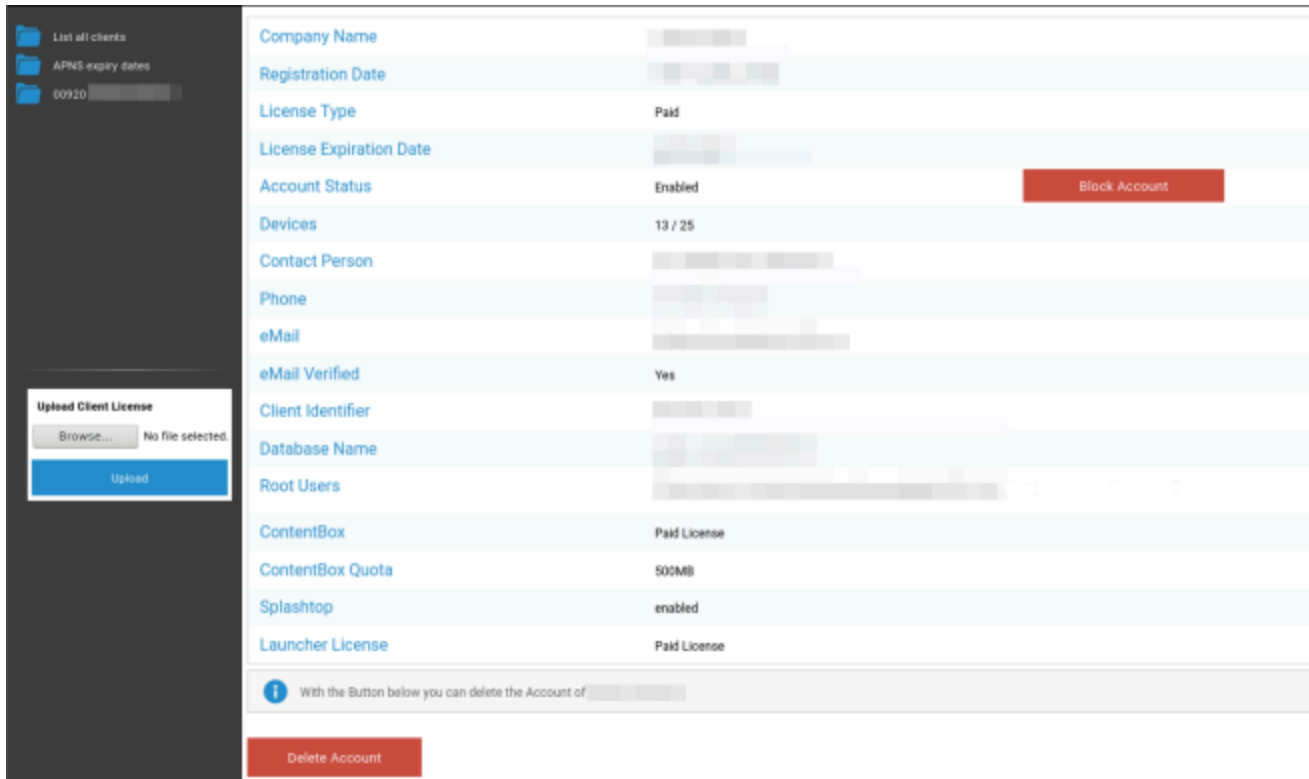
Attention:
The credentials entered here are not for managing devices.
To manage your devices please use your e-mail address as username and the password sent to you by E-Mail.
The password gets send from your appliance when running "Configure Appliance" for the first time.
Make sure you enter your e-mail settings correctly in the "E-Mail Settings" below.
The Server Manager is used in Multitenant Environments. If you don't run multiple clients on one appliance, you can ignore this setting.

Username	24ab311995775e921216d4f0d0a06ddb942f80d6
Password	●●●●●●
Repeat Password	●●●●●●

V novem meniju nastavite uporabniško ime in geslo za upravitelja strežnika. Shranite nastavitve in zaženite "Configure Appliance" v "Petem koraku - Licenčna pogodba", da uporabite nastavitve.

Ko je konfiguracija končana, se lahko z nastavljenimi poverilnicami prijavite v običajni vmesnik za upravljanje mobilnih naprav.

Po prijavi lahko vidite naslednji pogled.



The screenshot displays the AppTec360 management interface. On the left, a dark sidebar contains navigation options: 'List all clients', 'APNS expiry dates', and '90920'. Below these is an 'Upload Client License' section with a 'Browse...' button (showing 'No file selected') and an 'Upload' button. The main area shows account details for client ID 920:

Company Name	[Redacted]
Registration Date	[Redacted]
License Type	Paid
License Expiration Date	[Redacted]
Account Status	Enabled Block Account
Devices	13 / 25
Contact Person	[Redacted]
Phone	[Redacted]
eMail	[Redacted]
eMail Verified	Yes
Client Identifier	[Redacted]
Database Name	[Redacted]
Root Users	[Redacted]
ContentBox	Paid License
ContentBox Quota	500MB
Splashtop	enabled
Launcher License	Paid License

At the bottom, an information icon and text state: 'With the Button below you can delete the Account of [Redacted]'. Below this is a red 'Delete Account' button.

Na levi strani so prikazani vsi najemniki (v tem primeru samo eden z id 920), na desni strani pa informacije o tej stranki. Na voljo imate tudi možnost blokiranja dostopa do računa in izbrisa stranke (POZOR: s tem bodo odstranjeni vsi podatki, povezani s to stranko).

Na levi strani lahko naložite novo licenco stranke, ki je lahko posodobitev licence za obstoječo stranko ali nova licenca, ki samodejno ustvari novo stranko. Ob ustvarjanju nove stranke se na e-poštni naslov, za katerega je bila izdana licenca, samodejno pošlje e-poštno sporočilo z geslom za prijavo.

Če želite pridobiti novo ali posodobljeno licenco odjemalca (npr. če potrebujete več licenc za naprave), se obrnite na prodajnega zastopnika.

Dodatni pogledi

Navedite vse stranke

Prikaže pregled vseh odjemalcev v sistemu.

ID stranke	ID stranke
Identifikator	Identifikator stranke
Podatkovna zbirka	Podatkovna zbirka
Ime podjetja	Ime podjetja
Elektronska pošta	Kontaktna oseba eMail
Preverjeno	Ali je e-pošta kontaktne osebe preverjena ali ne
Država	Država
Naprave	Število registriranih naprav
Datum registracije	Trenutek dodelitve licence
Zadnja prijava	Zadnja prijava v administratorski račun
Licenca	Prikaz vrste licence (brezplačna plačljiva)
Licenca CB	Vrsta licence ContentBox (Brezplačna plačljiva)
Status	Trenutni status odjemalca AppTec
Pretekla veljavnost	Prikaže, če je licenca potekla
iOS	Število naprav iOS
Android	Število naprav s sistemom Android
Windows Mobile	Število naprav Windows Mobile
MacOS	Število naprav MacOS
Windows 10	Število naprav s sistemom Windows 10
Android Enterprise	Število naprav z operacijskim sistemom Android v podjetjih
IOS BYOD (prijava uporabnikov)	Število naprav IOS BYOD (vpis uporabnikov)
IoT	Število naprav IoT

Datumi izteka veljavnosti APNS

Prikaže pregled vseh datumov izteka veljavnosti potrdil APNS vseh odjemalcev.

ID stranke	ID stranke
Ime podjetja	Ime podjetja
Datum izteka veljavnosti	Datum poteka veljavnosti certifikata Apple APNS
Info	Informacije o poteku veljavnosti

Pišite na

Dodatna vprašanja? Obrnite se na nas pod naslovom:

Za splošna tehnična vprašanja

support@apptec360.com

+41 61 511 3210

Za vprašanja v zvezi z namestitvijo navidezne naprave

consulting@apptec360.com

+41 61 511 3214

Izjava o omejitvi odgovornosti

© AppTec GmbH

Ta dokumentacija je zaščitena z avtorskimi pravicami. Vse pravice pripadajo podjetju AppTec GmbH. Prepovedana je vsakršna druga uporaba, zlasti prenos na tretjo osebo, shranjevanje v podatkovnem sistemu, distribucija, urejanje, izvajanje, prikazovanje in oddajanje. To ne velja le za celoten dokument, temveč tudi za njegove dele. Spremembe se lahko izvedejo kadar koli.

Druga imena podjetij, blagovnih znamk in izdelkov so blagovne znamke ali registrirane blagovne znamke, ki na tej točki niso bile izrecno navedene, so zaščitene z zakoni o blagovnih znamkah in pripadajo zadevnemu lastniku. Spremembe in popravki se lahko izvedejo kadar koli.