AppTec360 Enterprise Mobile Manager & ContentBox

Administrationshåndbog | Version 5.0 (202110)

Indholdsfortegnelse

- Begrænsninger og indstillinger
  - Sortlistede / hvidlistede apps
  - SysApp-begrænsninger
  - App-VPN
  - App-indstillinger
- Enterprise App Store
  - iTunes-apps
  - Internt
- Kiosk-tilstand
  - Applikationstype
    - Pakke
    - URL
  - Indstillinger for kiosktilstand

Android Enterprise – Fuldt administreret enhedskonfiguration

Generelt

- Oversigt over gruppeprofiler (kun på gruppeniveau)
- Enhedsoversigt (kun på enhedsniveau)
- Config Revision (kun på enhedsniveau)
- Enhedslog (kun på enhedsniveau)
  - Kommando-log
  - Mulige kommandostatusser
- Enhedsindstillinger
  - Konfiguration af klienter
  - Baggrund

Asset Management (kun på enhedsniveau)

- Enhedsinfo
  - Wi-Fi
- Cellulær
- Bluetooth

Sikkerhedsstyring

- Tyverisikring (kun på enhedsniveau)
  - GPS-information (kun på enhedsniveau)
  - Tør og lås (kun på enhedsniveau)
  - Besked (kun på enhedsniveau)

- Besked (kun på enhedsniveau)
- Sikkerhedskonfiguration
  - Adgangskode
  - Kryptering
  - AntiVirus
- End of Life (kun på enhedsniveau)
  - Tør (kun på enhedsniveau)
- Begrænsningsindstillinger
  - Begrænsninger
  - Ejer af AE-enhed

BYOD-container

- Android Enterprise
  - Android Enterprise
  - Gmail-udveksling
  - AE System Apps
  - Adgangskode til container
- Samsung KNOX
  - Aktivering
  - Knox-adgangskode
  - Knox Sikkerhed
  - Knox-udveksling
  - Knox eMail
  - Knox-apps

Håndtering af forbindelser

- Wifi
  - Sikkerhedstype
    - WEP
    - WPA/WPA2
    - 802.1x EAP
- VPN
- Begrænsninger
- APN
- Bluetooth

PIM-styring

- Udveksling

Generelt overblik

Introduktion til AppTec360

AppTecs Enterprise-Mobile-Management-Solution giver mulighed for at administrere og konfigurere alle mobile enheder med sin intuitive administrationskonsol. I dette scenarie kan EMM-serveren enten køre i dine egne omgivelser, eller du kan bruge vores cloudbaserede løsning.

Selv når det drejer sig om en central installation af virksomhedsapplikationer på smartphones, er du kommet til det rette sted. Med Enterprise Mobile Manager kan du distribuere virksomhedens applikationer og dokumenter til enheder på få sekunder eller blokere uønskede applikationer med white/blacklisting.

Brugen af private enheder i virksomheder udgør en ny udfordring for sikring af smartphones og tablets. Da medarbejderne ønsker at bruge deres smartphones mere og mere, skal it-administratorer beskytte et stort antal forskellige typer enheder. Vi hjælper dig med at sikre alle enheder og de følsomme data, der er gemt på dem, og administrerer dem fra en intuitiv konsol.

Understøttede enhedsoperativsystemer

AppTec360 tilbyder support til iOS-, Android- og Windows-enheder. Vær opmærksom på, at funktionerne på de nævnte platforme kan være forskellige fra det ene operativsystem til det andet.

- Apple iOS 11.0 eller nyere*.
- Apple macOS 10.11 eller nyere
- Google Android 4.4 eller nyere** på Cloud-versionen
- Google Android 4.1 eller nyere** på OnPrem-versionen
- MS Windows 10 eller nyere*** (stationær computer, bærbar computer og tablet)

**Bemærk, at enheder med iOS 10 eller tidligere ikke kan tilmeldes på grund af drastiske ændringer, som Apple har foretaget i tilmeldingsprocessen.*

***Enheder kan tilsluttes og konfigureres, selv om de bruger en version, der ikke længere understøttes af producenten. Bemærk, at der kan være funktioner, der kræver en bestemt Android-version. I supporttilfælde følger vi producentens officielle support. I tilfælde af problemer eller fejl, der skyldes en forældet version, som ikke længere understøttes af producenten, forbeholder vi os ret til kun at tilbyde begrænset support.*

****Home-versionen af Windows understøttes ikke på grund af begrænsninger i operativsystemet. Vi anbefaler på det kraftigste at bruge en OS-version, som stadig understøttes af producenten. Ikke kun af hensyn til kompatibilitet, men også af sikkerhedsmæssige årsager. Derfor anbefaler vi iOS 12 eller højere og Android 9 eller højere.*

Understøttede LDAP-biblioteker

- Microsoft Active Directory
- Åbn LDAP

Opdaterede oplysninger om "Understøttede enhedsoperativsystemer" og "Understøttede LDAP-biblioteker" kan findes her:

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

Forklaring af „Supervised-Mode“ på Apple-enheder

Supervised-Mode repræsenterer en udvidet grænseflade til iOS-enheder.

På den respektive konfigurerede enhed kan der anvendes yderligere begrænsninger, som vedrører slutbrugerenhedens funktionalitet. Disse findes også i administrationshåndbogen og er markeret med et banner.

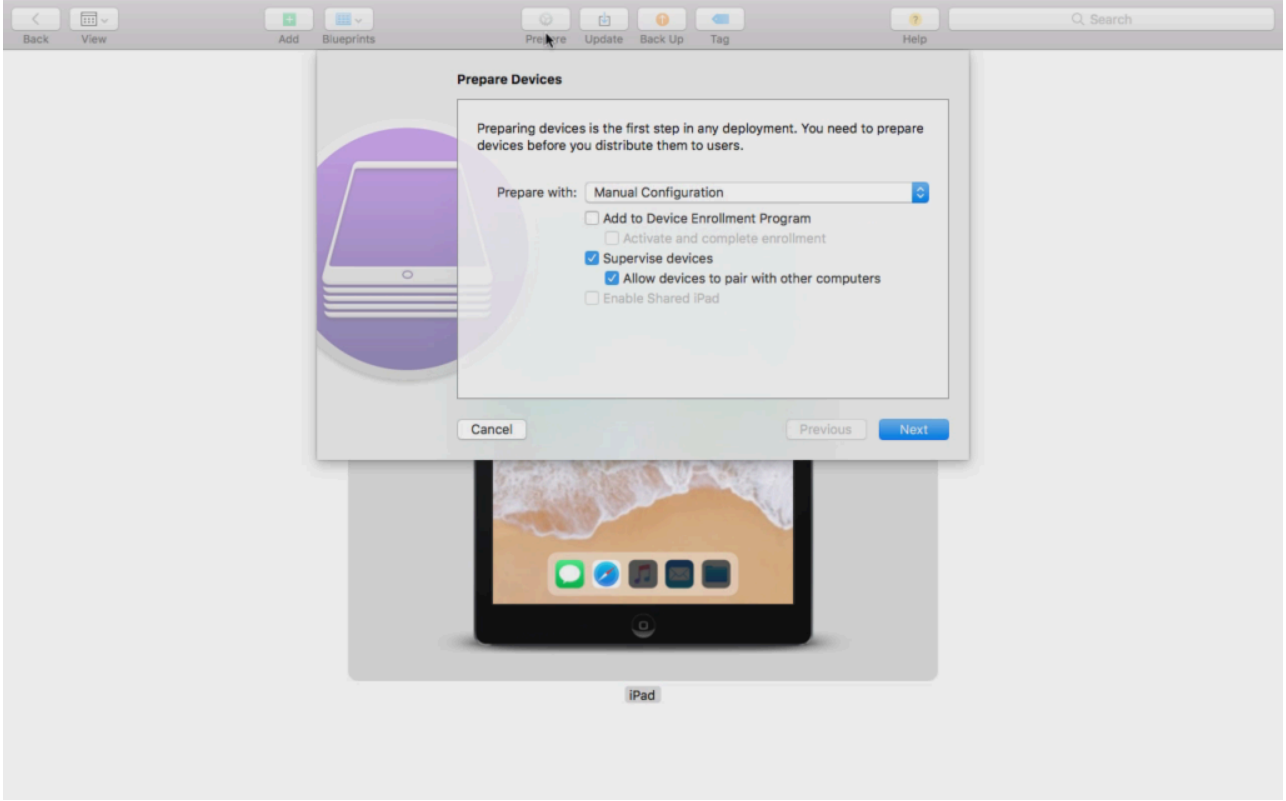
Tilgængelig i overvåget tilstand

"Supervised-Mode" kan aktiveres med programmet "Apple Configurator". Apple Configurator kan indstille standardindstillingerne på nye iOS-enheder som et konfigurationsværktøj (via USB-grænsefladen).

Værktøjet kan ikke kun installere konfigurationsprofiler, men også apps. Det er gratis, men kræver en Mac-computer.

Aktivér den overvågede tilstand

1. Åbn Apple Configurator



2. Klik på enheden, og vælg "Forbered"
3. Vælg "Manuel konfiguration" og "Overvåg enheder"
4. Klik på "Næste"
5. (valgfrit) Nu kan du tilføje en MDM-server, hvor enheden skal tilmeldes. Linket til dette kan findes i "Generelle indstillinger - iOS-konfiguration - Konfigurator og URL" Vælg din organisation, eller opret en ny
6. Vælg din organisation, eller opret en ny
7. Vælg, hvilke trin der skal springes over i den indledende opsætning, og klik på "Næste" (FORSIGTIG: Hvis du fortsætter, slettes din enhed!).

Nu vil din enhed blive sat i overvåget tilstand. Det kan tage nogle minutter. Når det er gjort, genstarter enheden.

Nu er din enhed under opsyn!

Tilføjelse af en enhed til DEP

Du kan også tilføje enheder til DEP (Device Enrollment Programm) ved hjælp af Apple Configurator, hvis dine enheder er på iOS 11 eller højere.

Mere information om DEP: https: //www.apple.com/business/dep/

Følg de samme trin, som når du overvåger en enhed, og marker desuden "Add to Device Enrollment Programm". Du vil blive bedt om dine DEP-login-data, hvis du aldrig før har logget ind på DEP med Apple Configurator.

Når processen er afsluttet, kan enheden findes på DEP-serveren "Devices Added by Apple Configurator 2". Du kan nu bruge denne server og forbinde den med administrationskonsollen eller overføre enheden til en allerede eksisterende server.

Du har nu tilføjet en enhed til DEP!

Forklaring af Android Enterprise

Hvad er Android Enterprise?

Android Enterprise giver bedre kontrol over arbejdsenheder, der administreres med en MDM. Det gør det muligt for administratorer enten at have fuld kontrol over deres Android-enheder eller at adskille virksomhedsdata fra private data på containerenheder. Derudover giver Android Enterprise mulighed for en nemmere registrering af enhederne og en nem app-distribution.

Hvad er kravene til at bruge Android Enterprise?

Android Enterprise kan bruges gratis af alle. Du behøver kun at forbinde en Google-konto til MDM'en for at aktivere alle Android Enterprise-funktioner. Du kan læse mere om dette i afsnittet om Android Enterprise.

Android Enterprise kan bruges på enheder med Android 5.1 eller nyere, med undtagelse af Enhanced Work Profile (se nedenfor). Vi anbefaler mindst Android 7 eller nyere for at gøre det nemmere at tilmelde sig eller Android 11 for at udnytte alle tilgængelige funktioner.

Hvad er de tilgængelige tilstande med Android Enterprise?

Der er 3 forskellige tilstande at bruge, når man bruger Android Enterprise.

AE Fuldt administreret enhed (arbejdsadministreret): En fuldt administreret enhed, der kun bruges til arbejde. Dette giver administratoren fuld kontrol over enheden. Det tillader ikke privat brug af enheden. For at tilmelde enheder i denne tilstand skal enhederne nulstilles og tilmeldes med en QR-kode (se AE-tilmelding) eller tilmeldes via Knox-tilmelding eller Zero Touch.

AE BYOD-container: BYOD-containeren (bring your own device) giver brugerne adgang til virksomhedsdata på deres private telefon i en separat container. I denne tilstand kan private apps ikke se virksomhedens data og apps og vice versa. For at tilmelde enheder i denne tilstand skal AppTec-appen downloades, og en QR-kode kan scannes. Opret en enhed i konsollen, og vælg "AE Container (BYOD & Enahnced Work Profile)" som enhedstype. Klik på QR-koden på den nyoprettede enhed for at få QR-koden, og indstil den første kontakt til "Legacy & BYOD".

AE Enhanced Work Profile: (kræver Android 11 eller nyere) Mens ovennævnte BYOD-container bringer virksomhedsdata over på en privat enhed, gør Enhanced Work Profile det samme, men for en virksomhedsejet enhed. Den opretter den samme container, men giver administratoren lidt mere kontrol over enheden, så brugeren ikke bare kan fjerne MDM fra enheden. Opret en enhed i konsollen, og vælg "AE Container (BYOD & Enahnced Work Profile)" som enhedstype. Klik på QR-koden på den nyoprettede enhed for at få QR-koden, og indstil den første kontakt til "Enhanced Work

Profile". Denne QR-kode kan scannes, når du har nulstillet enheden og trykket 6 gange på skærmen som forklaret i metode 1 i AE-tilmelding.

Hvordan kan jeg tildele apps til Android Enterprise-enheder?

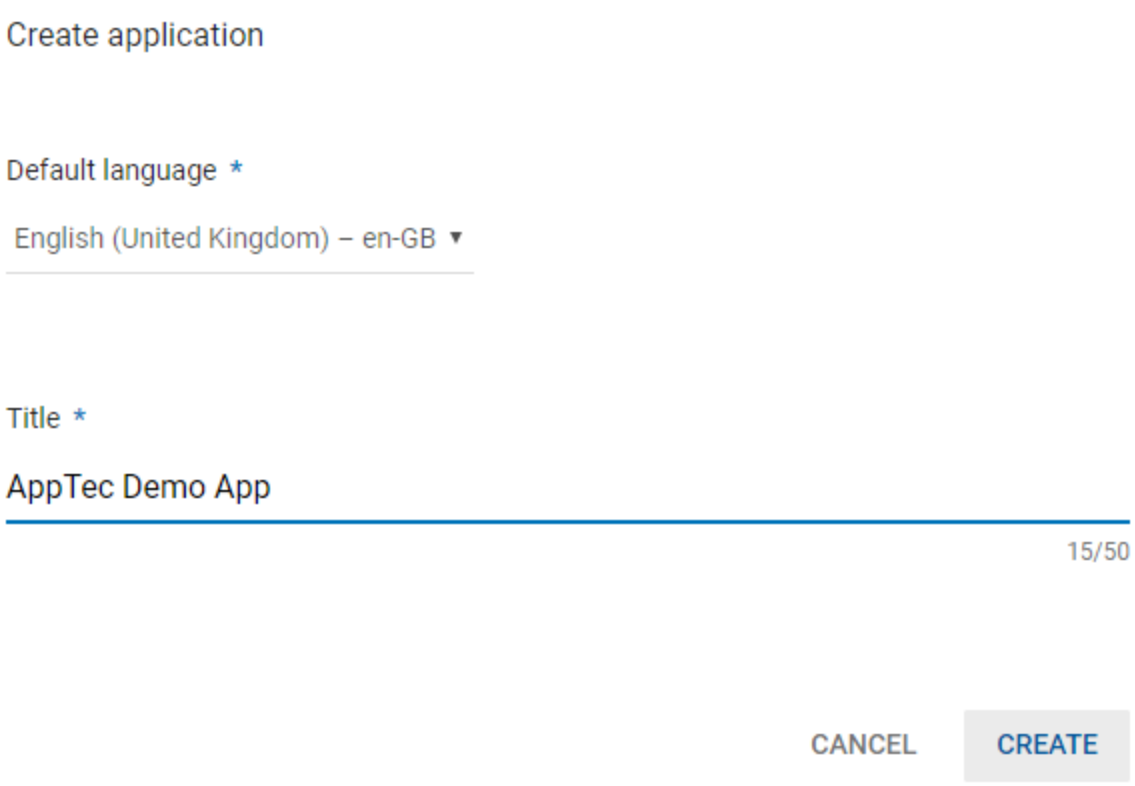
Først skal du godkende de apps, du vil bruge, i Generelle indstillinger → Appadministration → AE Play Store → Play Store-apps. Når du har godkendt en app, kan du tildele den til den obligatoriske appliste → i din profil ved at klikke på "+" og vælge appen fra fanen "AE Play Store". Så downloades og installeres appen automatisk. Der kræves ingen Google-konto på enheden, og brugeren behøver ikke at bekræfte eller tillade dette.

Upload dine egne apps til Google Play Store

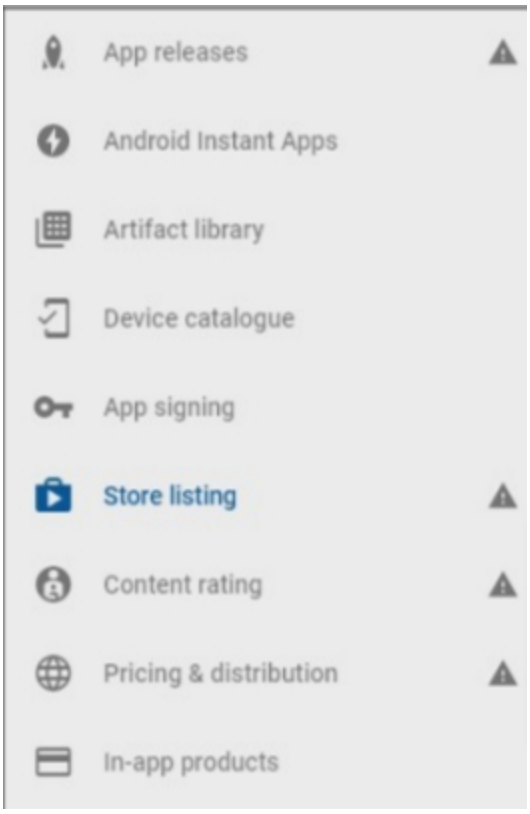
Det er muligt at uploade dine interne apps til Google Play Store. På den måde kan du drage fordel af forskellige fordele som f.eks. opdateringsmekanismen i Play Store.

For at gøre det skal du have en Google Developer Account. Log ind ved hjælp af Google Play Console(https://play.google.com/apps/publish)

Klik på "Opret applikation". Vælg dit standardsprog og appens titel.



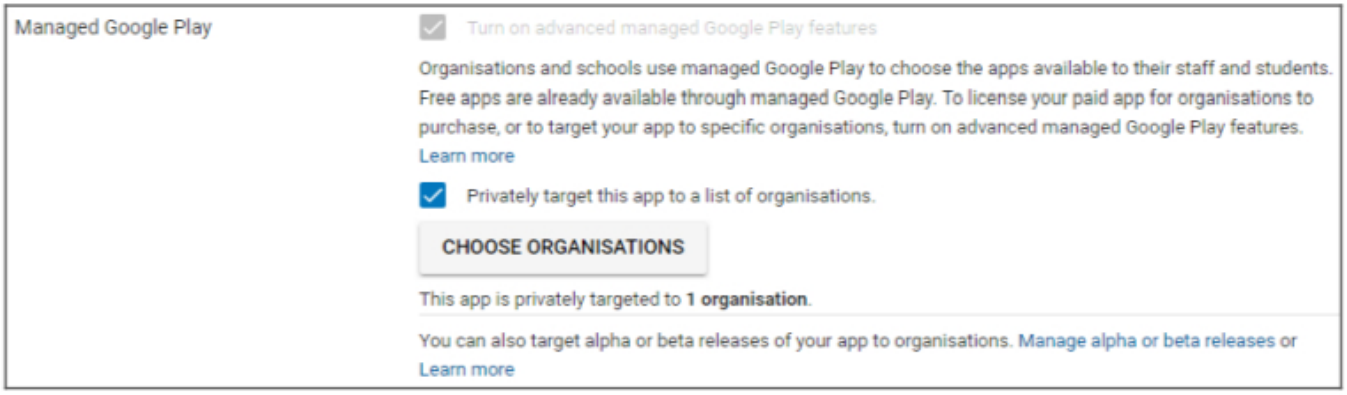
På den følgende side bliver du bedt om at indtaste forskellige oplysninger om din app.



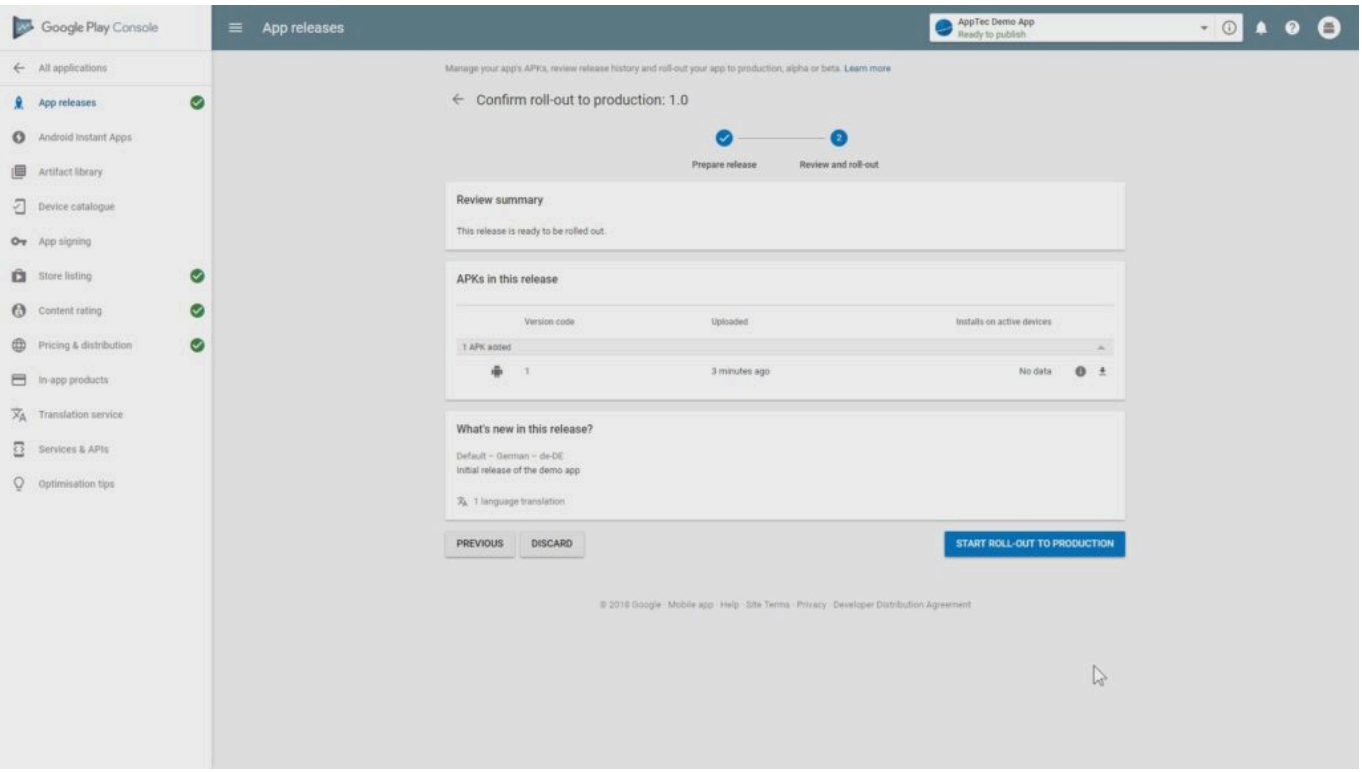
Når du har indtastet alle oplysninger, vil du se forskellige hintsymboler i venstre side.

Hold musen over dem for at se, hvilke trin der er tilbage, og følg dem i den rækkefølge, du ønsker.

Bemærk: Sørg for at markere de to afkrydsningsfelter ved "Managed Google Play" under "Pricing & Distribution". Ellers bliver appen offentlig og kan tilgås af alle. Sørg også for at vælge land for distribution.



Når du har gennemført alle trin, kan du gå til "App-udgivelser". Klik på "Review" og "Start Roll-Out to Production" for at færdiggøre dit udkast og udgive appen.



Det kan tage lidt tid, før appen er tilgængelig i Play Store. Når processen er færdig, kan du søge efter din app i Play for Work-butikken og godkende den. Derefter kan du bare tildele appen til enheder ved hjælp af EMM-konsollen, ligesom du gør det med andre apps.

Krav og installation

Kravene

Systemkrav

Det virtuelle apparat er tilgængeligt i Open Virtualization Format (VMWare, VirtualBox, Citrix Xen Server) og som komprimeret .vhdx (Hyper-V)-fil*.

*Bemærk: Maskinen skal oprettes med Generation 1, når man bruger Hyper-V.

Den virtuelle disk har en målstørrelse på 20 GB, og maskinen kræver 4 GB RAM.

Apparatet er baseret på Debian 9 64bit.

Opgrader den importerede maskine til den nyeste kompatibilitet (f.eks. i VMWare), og sørg for, at maskinens OS-type er indstillet korrekt i din hypervisor.

Licensnøgle

For at kunne aktivere og installere serveren skal du bruge en gyldig licensfil. Du kan få en fra AppTec360 direkte og/eller fra din respektive forhandler.

IP-adresse og DNS-opløsning

AppTec360-apparatet skal kunne nås af enheden ved hjælp af det værtsnavn, som licensen er udstedt til.

For at tilmelde Windows 10-enheder skal du også oprette et ekstra underdomæne i form af "enterpriseenrollment.", der peger på apparatet.

SSL-certifikat

Da alle forbindelser til og fra enhederne skal sikres ved hjælp af SSL, skal du have et gyldigt certifikat for værtsnavnet udstedt af en certifikatmyndighed, som enheden har tillid til. Den private nøgle til certifikatet skal uploades uden adgangskodebeskyttelse. I de fleste tilfælde kræves der et mellemliggende certifikat for CA, for at enhederne kan genkende servercertifikatet.

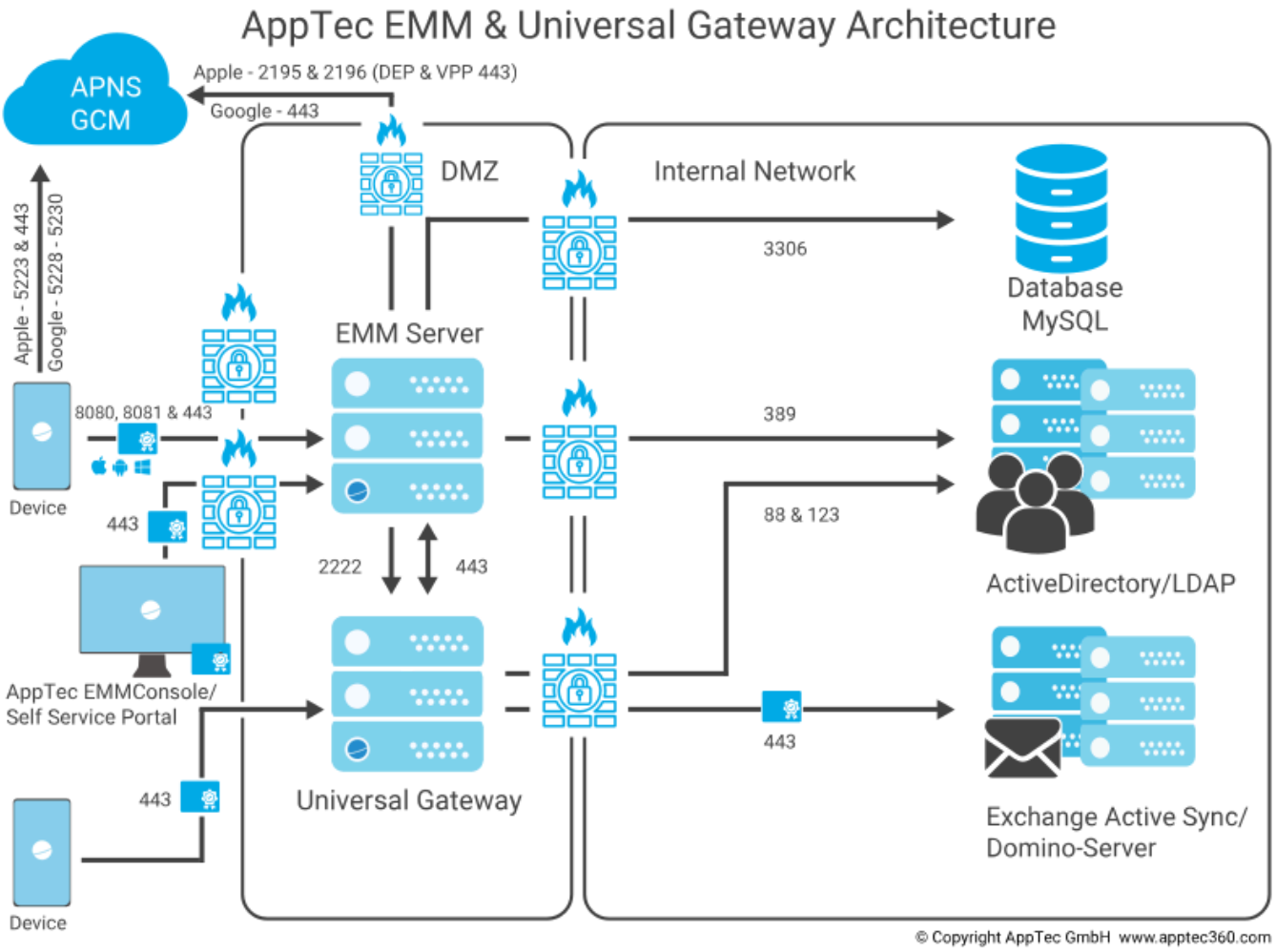
Windows 10-enheder kræver et specifikt certifikat til dit enterpriseenrollment-underdomæne.

Fra og med appliance-version 202104 kan du også bruge Let's Encrypt-certifikater, som genereres automatisk (beskrevet i Trin 2 - SSL-certifikat).

SMTP-server

Der kræves en e-mailserver og/eller et e-mailrelæ, så AppTec360 EMM kan sende e-mails (f.eks. til enhedsregistrering og kontovalidering).

Firewall-regler



Dette diagram viser, hvilken forbindelse der er nødvendig, afhængigt af hvilke tjenester du vil bruge.

Se tabellen på næste side for en mere detaljeret beskrivelse.

Alle (eksterne/enheder)	→	**AppTec360 Apparat / emmconsole.com**
Havne	443	Ledelse, Enterprise AppStore og Windows Phone-kommunikation
	8080	Android- og iOS-kommunikation
	80	Førstegangsopsætning af Let´s Encrypt. Bruger 443 bagefter.
Enhver (enheder)	→	**Enhver (ekstern)**
Havne	5223, 443	Apple Push Service, skal kunne nås uden proxy, 443 som fallback, se https://support.apple.com/en-us/HT203609
	5228-5230	Android Push Service (FCM), skal kunne nås uden proxy
AppTec360 Apparat	→	**Domænecontroller**
Havne	389, (LDAPS 636)	Brugersynkronisering med LDAP
AppTec360-apparat	→	**Enhver**
Havn	443	Bruges til Android Push Service (GCM) Søgning i AppStore / Play Store
AppTec360-apparat	→	**emmconsole.com**
Havne	443	AppTec360 Appliance-opdateringer, generering af APNS-certifikater
AppTec360-apparat	→	**Apple-netværk (17.0.0.0/8)**
Havne	2195, 2196	Apple Push Service & Feedback Service
	443	DEP & VPP

Sikkerhedsopdateringer

Debian-operativsystemet bør opdateres regelmæssigt for at få de nyeste sikkerhedsrettelser. Sørg dog for, at du ikke opgraderer til en nyere hovedversion af Debian manuelt. Når AppTec360 EMM er kompatibel med en nyere hovedversion, vil vi tilføje en måde at opgradere på i en appliance-opdatering.

Standardadgangskoder for det virtuelle apparat

Login-bruger (Root-login er deaktiveret. Brug "sudo" til administrationsopgaver)

apptec

Login-adgangskode

apptec

MySQL-rodbruger

rod

MySQL-rodadgangskode

apptec

MySQL standardbruger

AppTec

MySQL Standard brugeradgangskode

AppTec

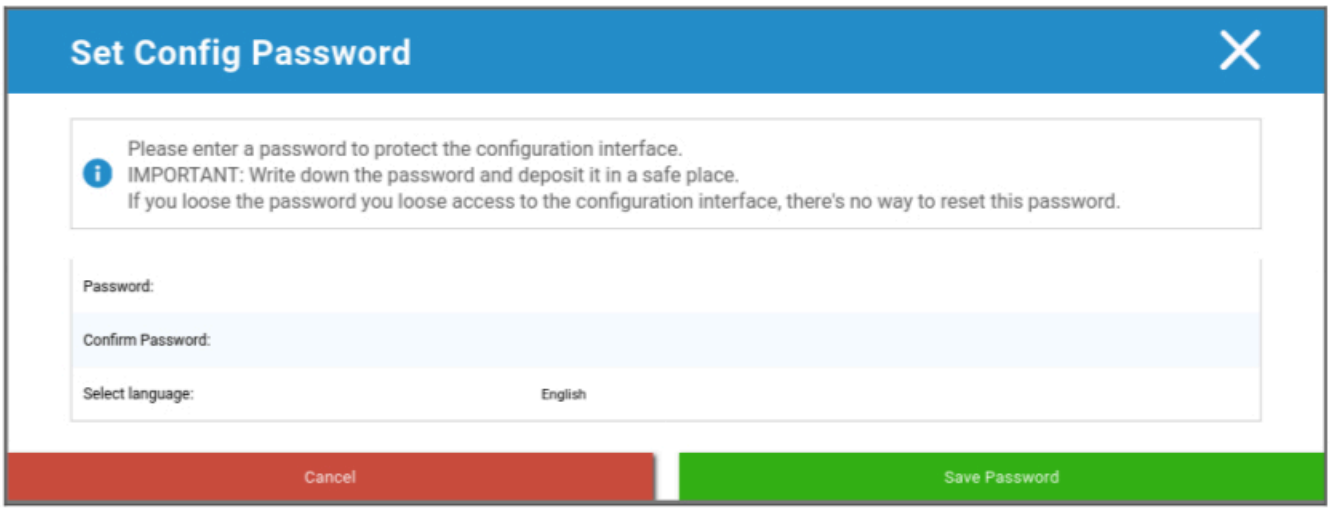
Konfiguration af den virtuelle appliance

Vigtigt: Før du begynder at konfigurere det virtuelle apparat, skal skærmopløsningen være indstillet til mindst 1280 x 800 pixels.

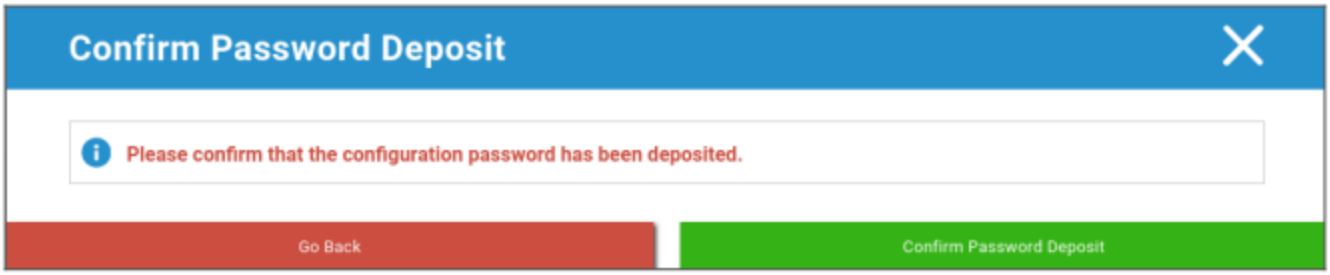
Når du har logget ind på apparatet, bør Firefox automatisk starte og vise konfigurationsgrænsefladen.

Forberedelse

Først skal du angive en adgangskode til konfigurationsgrænsefladen. Denne adgangskode bruges til at kryptere alle oplysninger og filer, der indtastes i konfigurationsgrænsefladen. Her kan du også indstille det sprog, som grænsefladen skal vises på (kan ændres senere).

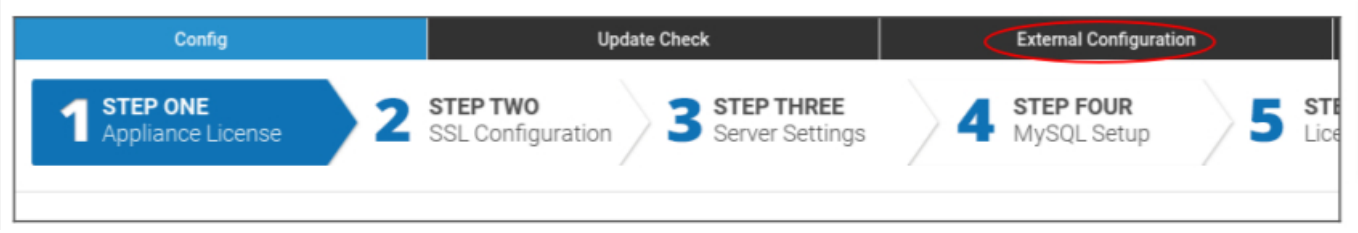


Adgangskoden kan kun nulstilles af AppTec360 Support, så sørg for at gemme den et sikkert sted og bekræft den kommende popup.



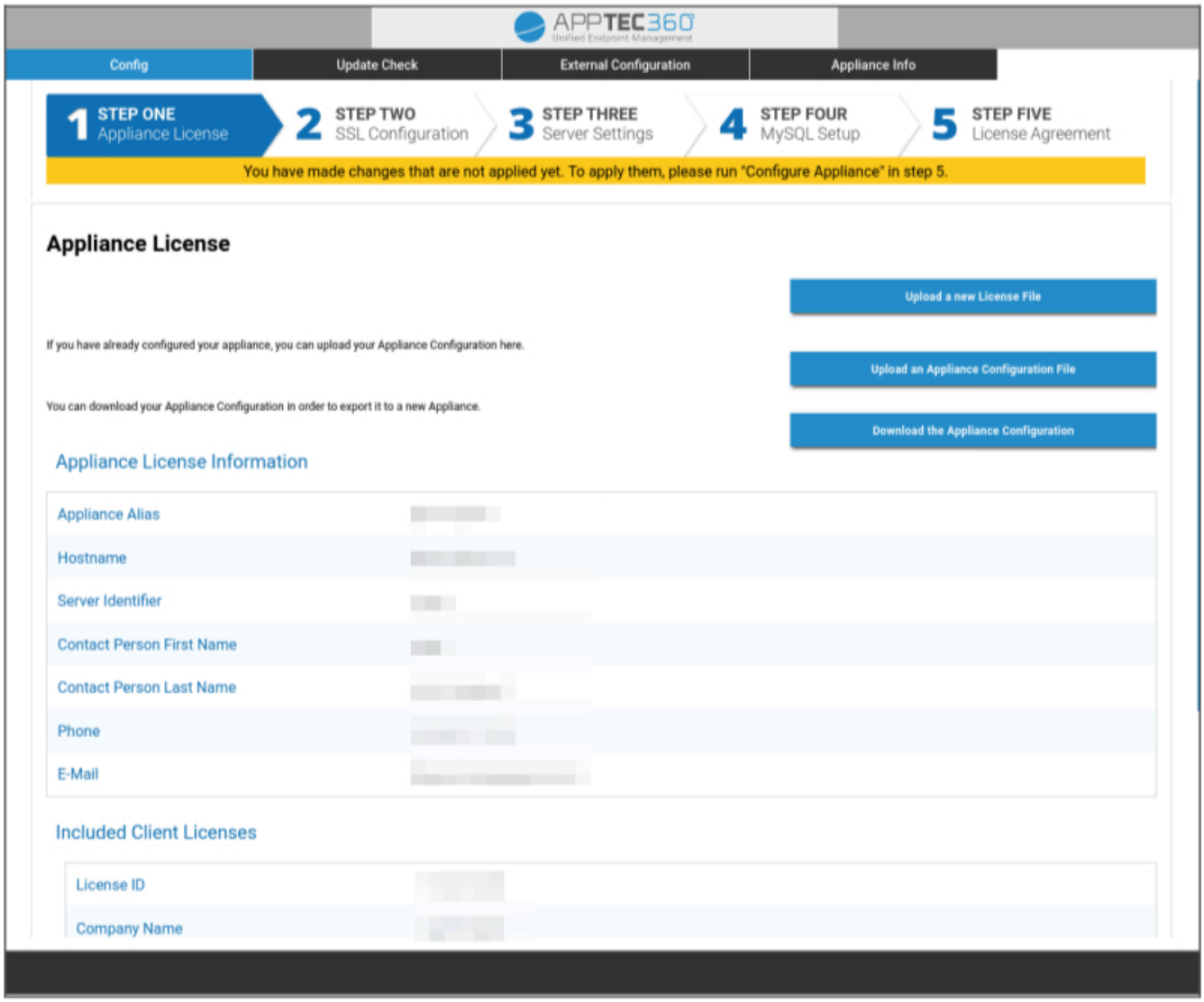
Konfigurer fra ekstern vært

For at lette opsætningsprocessen kan du gøre konfigurationssiden tilgængelig fra en fjernbetjening. For at gøre det skal du følge trinnene i "Konfigurer fra ekstern vært".



Trin 1 – Licens til apparat

1. Upload venligst den licensfil, som du har modtaget fra AppTec.
2. Hvis licensfilen er blevet uploadet korrekt, kan du se apparatets licensoplysninger som i skærmbilledet nedenfor.



Trin to – SSL-certifikat

Du kan enten bruge den automatiske certifikatopsætning ved hjælp af Let's Encrypt eller selv sørge for certifikaterne (se SSL-certifikat for mere information).

Automatisk

Certifikatet genereres automatisk ved hjælp af Let's Encrypt-tjenesten.

AppTec360 EMM bruger HTTP-01-udfordringen til validering af domænet, hvilket betyder, at HTTP-porten skal være åben fra internettet for den første anmodning om et certifikat. Efterfølgende fornyelsesanmodninger kan valideres via HTTPS.

Skift radioknapperne til "Automatic (Let's Encrypt)", og tryk på "SAVE VALUES". Certifikatet vil automatisk blive anmodet om, når du anvender konfigurationen i trin fem - Licensaftale. Certifikatet fornyes automatisk, hvis det er nødvendigt, og du vil modtage en e-mail, hvis certifikatet er ved at udløbe (hvilket betyder, at fornyelsen måske er mislykkedes).

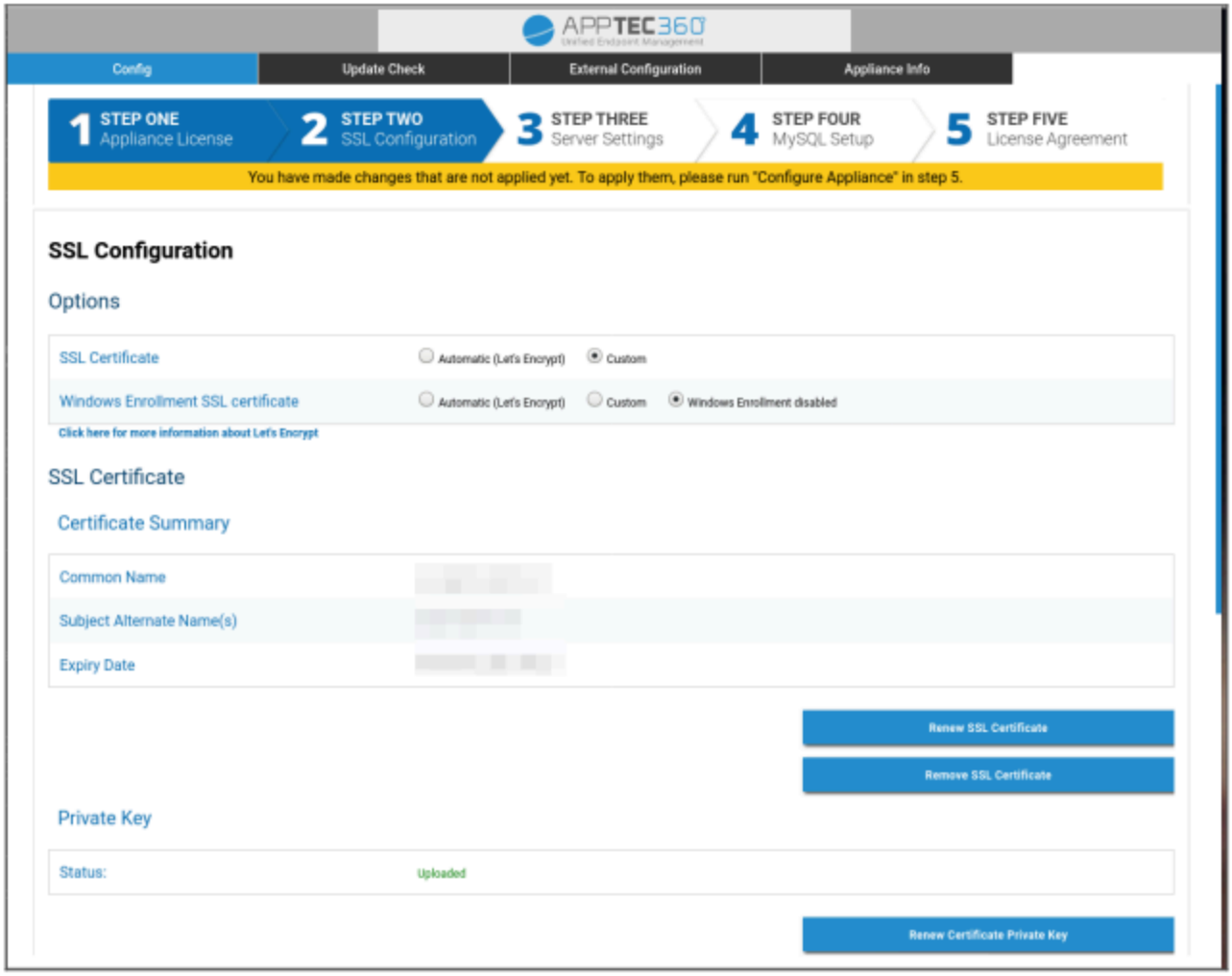
Brugerdefineret

1. Upload SSL-certifikatet for dit licenserede værtsnavn. Du kan se værtsnavnet i Trin 1 - Apparatlicens.

2. Upload også den private nøgle til certifikatet og om nødvendigt det mellemliggende certifikat.

Vigtigt: Nøglen må ikke være beskyttet med en adgangskode. Hvis den er, skal du fjerne adgangskoden, før du uploader den.

Tip: Hvis du også vil bruge Windows 10-enheder, skal du aktivere "Windows Enrollment SSL certificate" og uploade certifikatet, den private nøgle og det mellemliggende certifikat til dit underdomæne (beskrevet i IP-Address and DNS Resolution) nederst på siden.



Trin tre – Serverindstillinger

1. Indtast venligst en e-mailadresse til global support. Denne adresse vil blive brugt i e-mails til dine brugere, så de ved, hvem de skal kontakte i tilfælde af problemer med deres enhed.
2. Angiv de e-mailindstillinger, som systemet skal bruge til at sende e-mails. Indstillingerne vil blive brugt til at sende e-mails til brugeren og også til at sende fejlrapporter og funktionsanmodninger til"support@apptec360.com".Når du har gemt dine e-mailindstillinger, skal du bekræfte dem ved at klikke på "Test E-Mail Configuration" og følge instruktionerne.

Trin fire – opsætning af MySQL

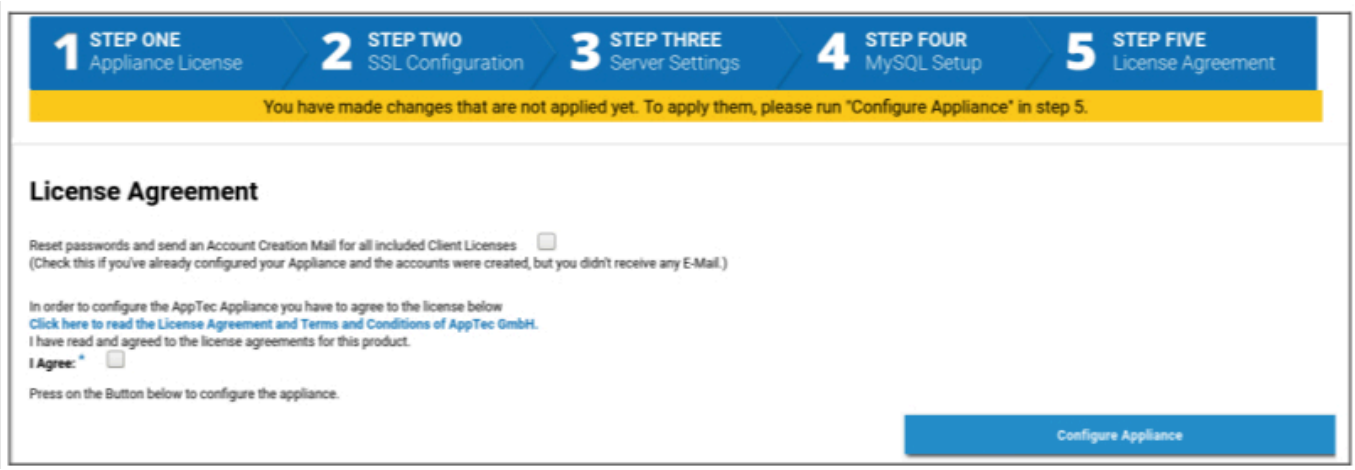
1. Hvis du vil bruge den interne database, kan du springe dette trin over. Ellers kan du indtaste forbindelsesoplysningerne til din eksterne databaseserver.


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

Trin fem – Licensaftale

1. Læs venligst licensaftalen.
2. Marker "I Agree", og tryk på knappen "Configure Appliance" for at anvende indstillingerne.

Tip: Du skal køre "Configure Appliance", hver gang du ændrer indstillinger i de 5 trin for at anvende indstillingerne.



Tillykke med det!

Du er færdig med at konfigurere den virtuelle appliance.

En e-mail med din adgangskode blev sendt til den adresse, du har angivet for licensen (kan ses under "Inkluderede klientlicenser" i Trin 1 - Apparatlicens).

Du kan nu logge ind på konsollen ved hjælp af denne adgangskode og den e-mailadresse, du har modtaget den på.

For at logge ind på konsollen skal du indtaste konsollens værtsnavn i adresselinjen i din browser.

Du kan finde værtsnavnet på dit apparat i Trin 1 - Apparatlicens.

Fejlfinding

1. Du modtog ikke en e-mail, da du konfigurerede apparatet i trin fem - Licensaftale:

Sørg for, at dine e-mailindstillinger i Trin 3 - Serverindstillinger er korrekte. For at sende adgangskoden igen skal du tjekke "Nulstil adgangskoder og send en mail om kontooprettelse for alle inkluderede klientlicenser" i Trin fem - Licensaftale, før du kører "Konfigurer apparat" igen.

2. Du har fået en fejl med hensyn til Let's Encrypt under konfigurationen i trin fem - Licensaftale:

Sørg for, at apparatet kan nås med sit domænenavn på port 80. Let's encrypt skriver også en log til "/var/log/letsencrypt", som kan hjælpe med yderligere fejlfinding.

Anbefalinger om sikkerhed

Det anbefales at udføre følgende trin for at sikre din AppTec360-appliance.

Dette er ikke et komplet sæt instruktioner, det er bare en anbefaling til en grundlæggende konfiguration.

- Skift adgangskode for AppTec360-brugeren
- Skift adgangskode for MySQL-brugerne "root" og "AppTec", og opdater trin fire - MySQL-opsætning i overensstemmelse hermed.
- Skift SSH-serverens standardport
- Bloker port 80 i din konsol, og afvis indgående HTTP-trafik, brug kun HTTPS. Når det er konfigureret, er det også muligt at foretage en ekstern konfiguration via HTTPS.
- Begræns adgangen til administrationsgrænsefladen til kun visse IP'er i bunden af Trin tre - Serverindstillinger
- Konfigurer firewallen

Generelle indstillinger

Oversigt over konti

Kontooplysninger

Oversigt

Her kan du se en oversigt over din AppTec360-konto.

Virksomhedens navn	Dit firmanavn
Oprettelsesdato	Dato for oprettelse af din konto
Licenstype	Betalt = betalt licens Gratis = ubetalt licens Bemærk: Konti på en OnPremise Appliance vil altid blive vist som betalt af tekniske årsager.
Klient-identifikator	Identifikator for din konto (dette er IKKE dit kundenummer)
Licensens udløbsdato	Udløbsdato for din AppTec360-licens
ContentBox-licens	Gratis = gratis licens til 25 enheder Betalt = betalt licens for x enheder
Launcher	Viser, om du kan bruge den brugerdefinerede launcher til Android eller ej
Enheder	Antal aktuelt anvendte / samlede licenser
Kontaktperson	Udleveret kontaktperson
Telefon	Oplyst telefonnummer
E-mail*	Oplyst e-mailadresse
Rodbruger	Root-brugere, der kan logge ind
Software-version	Nuværende softwareversion

**Bemærk: Den e-mailadresse, der vises her, er den, du indtastede for at registrere kontoen. Baseret på dette oprettes en bruger i bruger-/enhedstræet, som kan ændres. Hvis du redigerer denne bruger, ændres den e-mailadresse, du skal bruge til at logge ind, men ikke oplysningerne i kontooversigten. .*

Fejlrapport

En fejlrapport kan sendes direkte til support for at rapportere problemer eller fejl og indeholder oplysninger og logfiler om din konto og opsætning.

Emne	Emnet for fejlrapporten. Medtag et supportnummer, hvis du vil føje dette til en eksisterende supportrapport.
Forventet adfærd	Beskriv i detaljer, hvad du gjorde, og hvad du forventede, der ville ske.
Faktisk adfærd	Beskriv i detaljer, hvad der præcist sker. Citer venligst fejlmeddelelser PRÆCIS. Det hjælper også, hvis du tilføjer skærmbilleder til den vedhæftede fil.
På hvilket tidspunkt oplevede du problemet?	Angiv venligst et præcist tidspunkt, hvor du fik en specifik fejlmeddelelse/et specifikt problem. I bedste fald medtages også sekunder, f.eks. 18:55:27
Kan problemet replikeres? Hvis ja, hvordan (i detaljer)?	Beskriv i detaljer, hvordan du kan genskabe problemet.
Har denne funktion tidligere fungeret, som du forventede? Hvis ja, indtil hvornår?	Lad det være tomt, hvis du ikke ved det.
Blev der foretaget nogen specifikke ændringer i systemet, før dette problem opstod? Hvis ja, hvilke ændringer (i detaljer)?	Nævn altid, hvad din sidste ændring eller handling var, før problemet dukkede op, også selv om du synes, det er irrelevant.
Hvis det er relevant: Hvilke enhedsmodeller og OS-versioner er berørt?	Angiv altid den nøjagtige OS-version (f.eks. iOS 14.7.1 eller Android 11).
Hvis det er relevant: Hvad er enhedens offentlige IP-adresse og/eller serienummer?	Nævn mindst én, selv om alle enheder er berørt.
Inkluder logfiler	Marker dette for at sende logfilen med fejlrapporten. Dette anbefales at gøre.
Hent den aktuelle VPP-tilstand fra Apple og inkluder den i fejlrapporten	Indeholder oplysninger om VPP-licenstildelinger. Aktivér kun dette, hvis du bliver bedt om det af supporten, eller hvis dit problem handler om VPP.
Vedhæftet fil	Vedhæft enhver fil, der kan være nyttig (f.eks. skærmbilleder af en fejlmeddelelse).

Anmodning om funktion

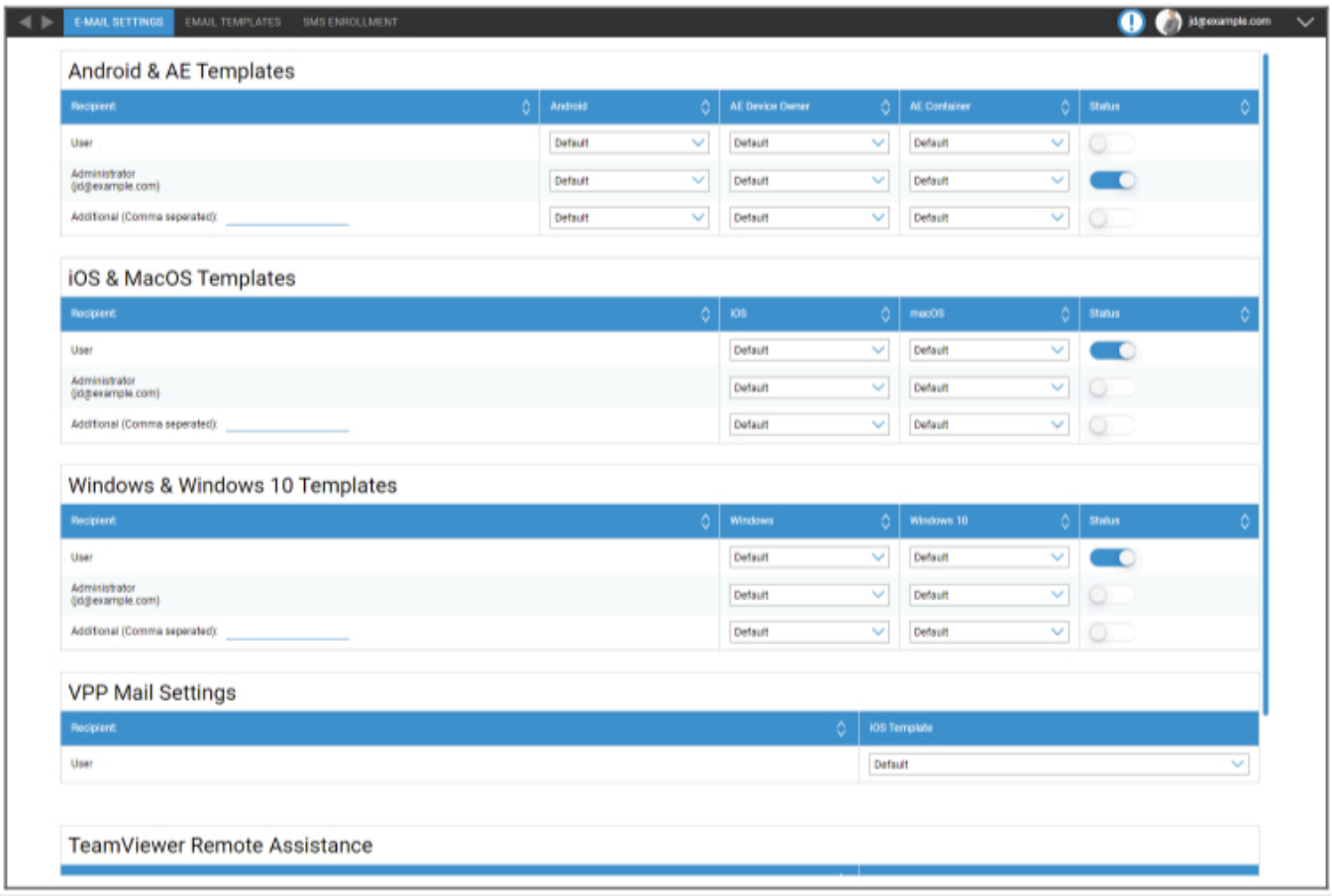
En funktionsanmodning kan sendes direkte til support. Den kan indeholde en anmodning om en specifik funktion eller en forbedring af

Sammenfatning	En kort opsummering af dit problem
Beskrivelse	En detaljeret beskrivelse af dit problem, vær så specifik som muligt
Vedhæftet fil	Vedhæft filer til fejlrapporten

Global konfiguration

Indstillinger for e-mail

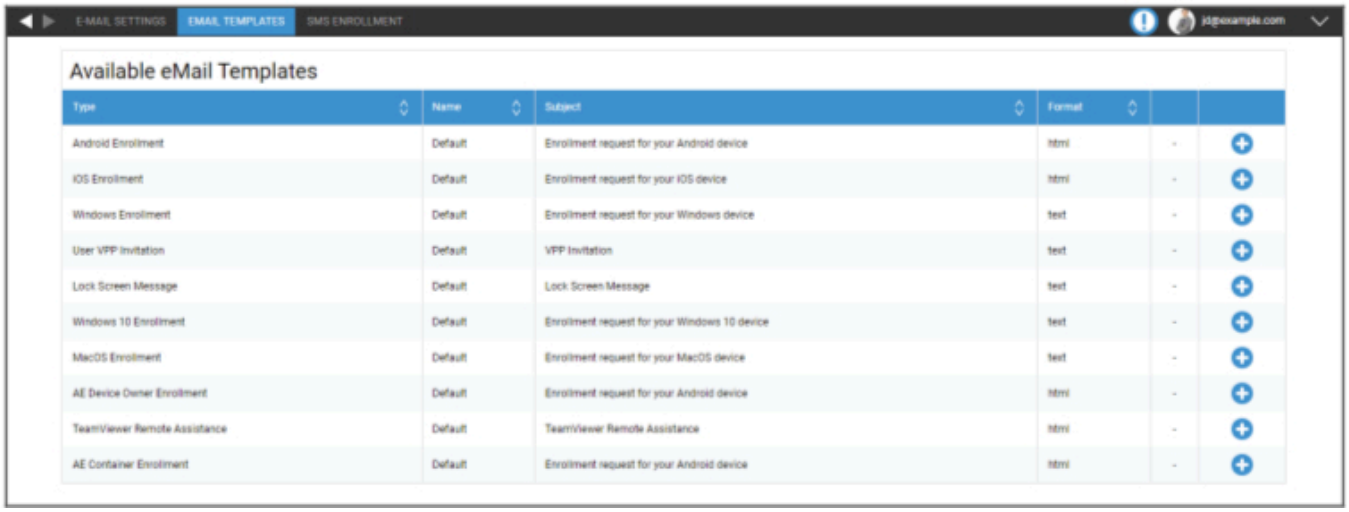
Her kan du definere, hvem der får en mail, når der genereres en tilmeldingsanmodning, og hvilken tekstskabelon der bruges til den mail.



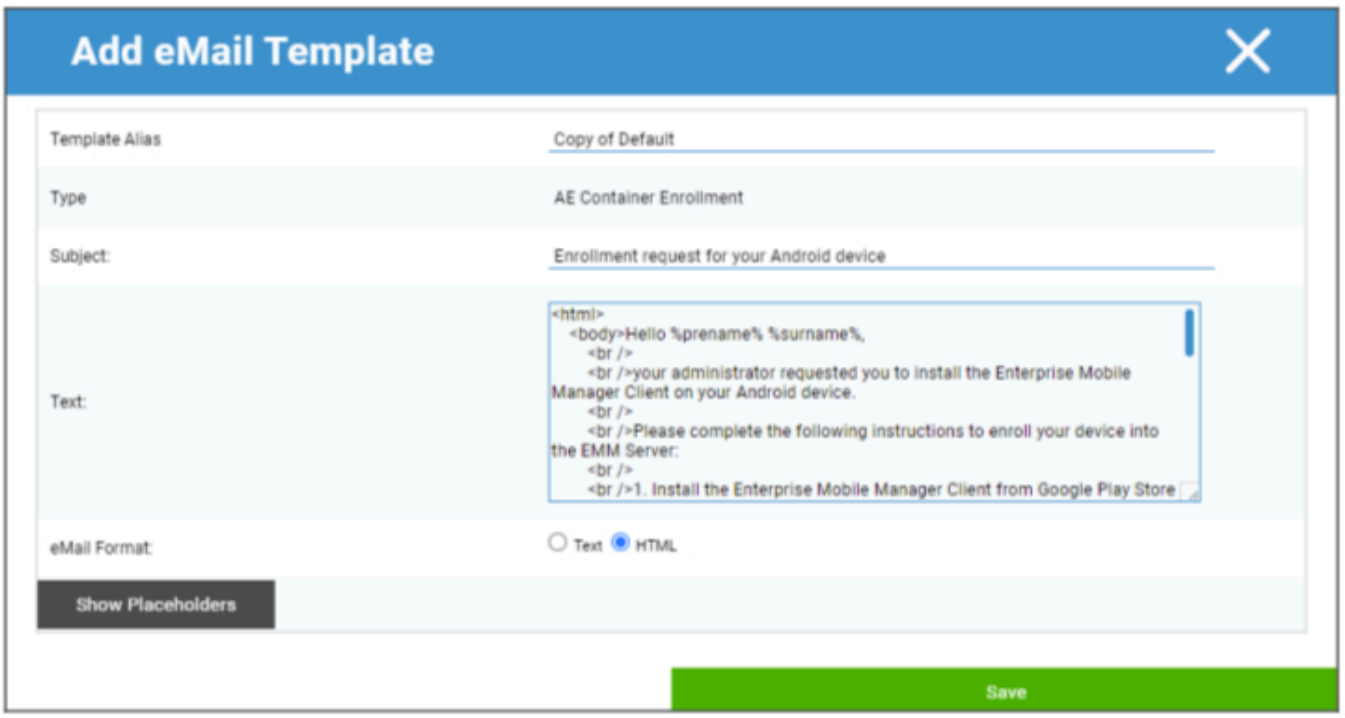
eMail-skabeloner

Her kan du generere og redigere dine skabeloner til forskellige scenarier. De kan være i normal tekstform eller i HTML. Med HTML kan du bedre kontrollere formateringen af din tekst.

Standardskabelonerne kan ikke redigeres eller slettes.



Du kan også bruge pladsholdere som variabler, der automatisk bliver erstattet. Klik på "Vis pladsholdere" under redigering for at se tilgængelige pladsholdere. Forskellige kategorier har forskellige pladsholdere.



SMS-tilmelding

Her kan du de-/aktivere SMS-tilmeldingsprocessen.

(Standard: deaktiveret)

Du vil også se et display, der viser, hvor mange SMS-kreditter der stadig er til rådighed.

SMS-kreditter skal købes separat.

Privatlivets fred

GPS-adgang

Her kan du beskytte GPS-visningen for hver enhed med 1 eller 2 adgangskoder (fire øjne-princippet). Du vil blive bedt om at indtaste din(e) adgangskode(r), hver gang du forsøger at få adgang til en enheds placering.

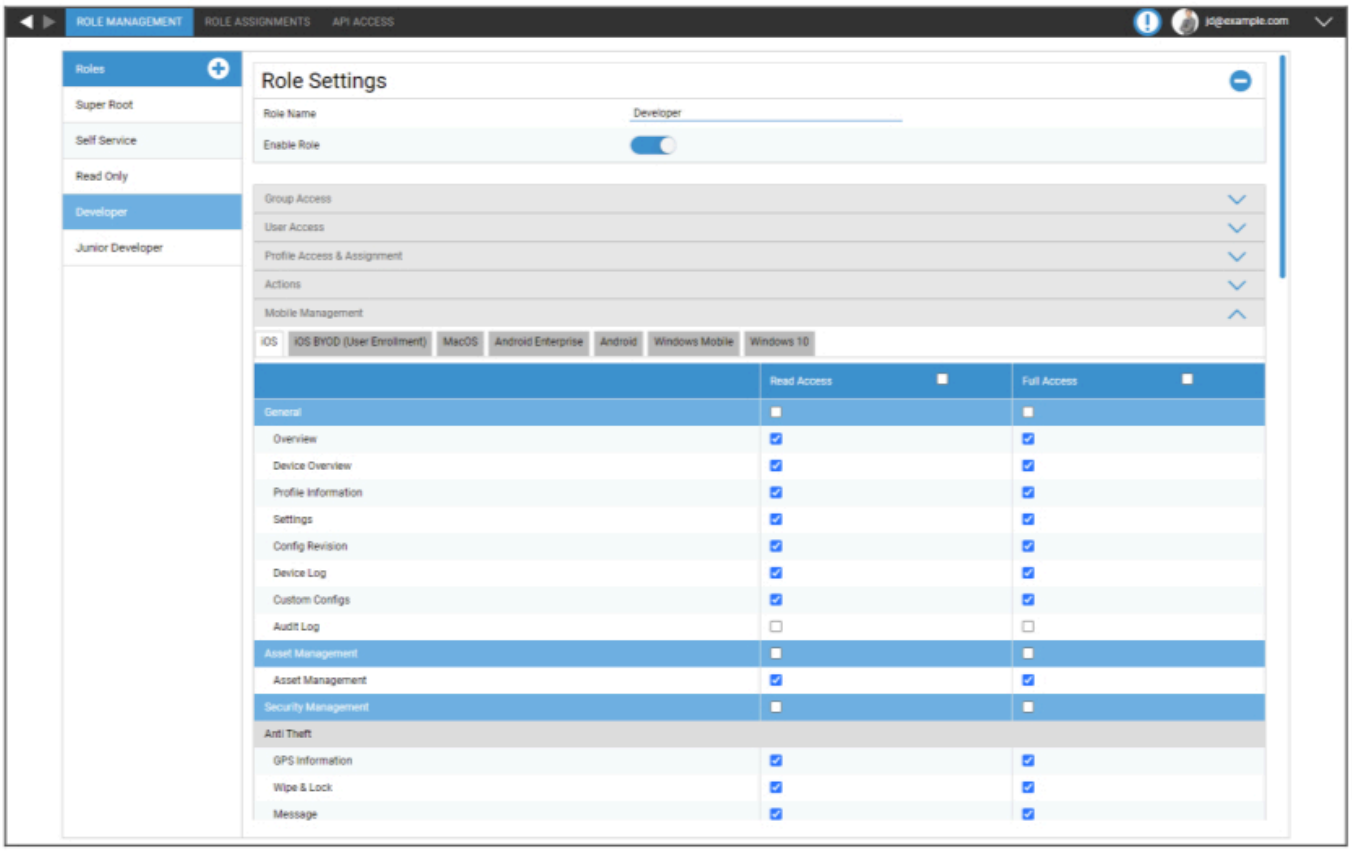
Begræns adgang til GPS-indstillinger	Off = funktionen er slået fra, og der kræves ingen adgangskode til lokalisering
	On = funktionen er slået til, og der kræves en adgangskode til lokalisering
Beskyttelsesmetode	Brug én adgangskode = brug én adgangskode til lokalisering
	Brug to adgangskoder = brug to adgangskoder til lokalisering
Indtast adgangskode (1)	Indtast den valgte adgangskode
Gentag adgangskode (1)	Indtast den valgte adgangskode igen
valgfrit: Indtast adgangskode 2	Indtast den anden valgte adgangskode
valgfrit: Gentag adgangskode 2	Indtast den anden valgte adgangskode igen

Bemærk: Når du har indstillet din(e) adgangskode(r), skal du indtaste den igen, før den er helt aktiveret.

Rollebaseret adgang

Ledelse af roller

Rollerne definerer, hvad en bruger kan se og gøre, når han logger ind på administrationskonsollen. Det gør det muligt at oprette brugere, som kan logge ind, men som har begrænset funktionalitet.



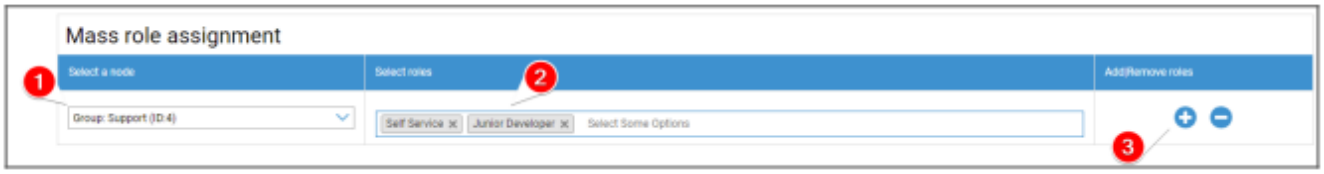
Super Root-rollen er en standardrolle, som altid kan se og ændre alt. Den kan ikke ændres eller slettes. Selvbetjeningsrollen kan kun se sine egne brugere og enheder. Du kan kombinere selvbetjening og en brugerdefineret rolle for f.eks. at give brugerne mulighed for at logge ind og tilmelde enheder alene og kun for deres egen bruger.

Brugerdefinerede roller kan aktiveres eller deaktiveres manuelt. Nye roller er som standard deaktiveret. Brugere med en deaktiveret rolle arbejder, som om de ikke har rollen. Dette giver dig mulighed for f.eks. midlertidigt at begrænse en given rolle fra deres handlinger.

Alle tilladelser er opdelt i "Læseadgang" og "Fuld adgang". Ved at give en rolle læseadgang kan de se den specifikke del af konsollen. Ved at give dem fuld adgang kan rollen se og ændre den specifikke del af konsollen.

Tildeling af roller

Her får du en oversigt over alle brugere, der har en rolle, og kan se, hvilken rolle de har. Du kan også tildele en rolle til brugere eller hele grupper her:

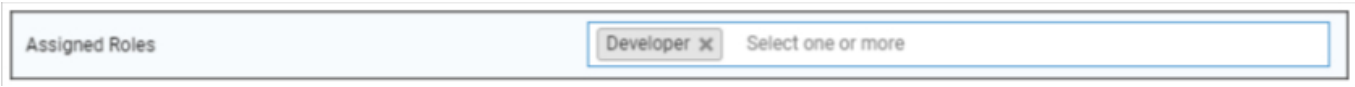


1. Vælg, hvilken gruppe eller bruger du vil tilføje eller fjerne roller for. Du kan enten vælge en enkelt bruger eller en gruppe. Når du vælger en gruppe, vil din ændring påvirke alle brugere i den gruppe og alle brugere af undergrupper i den valgte gruppe.
2. Vælg, hvilken rolle du vil tilføje eller fjerne. Du kan vælge en eller flere roller.
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. Gem for at afslutte processen. Brugere, som tidligere ikke havde nogen rolle og "Kan logge ind" deaktiveret, vil automatisk modtage en mail med et link til at angive en adgangskode.

Under masse-rolletildelingen kan du finde en oversigt over de tildelte roller. Du kan også manuelt ændre roller for specifikke brugere.

Tildeling af en rolle

For at tildele en rolle til en bruger skal du gå til Mobile Management, hvor du finder træet med dine grupper, brugere og enheder. Rediger brugeren for at tildele en rolle. Alternativt kan du også bruge ovennævnte metode til enkelte brugere.



API-adgang

Få adgang til AppTec360 REST API

AppTec360 REST API kræver et autentificeringstoken (API-nøgle) og en privat nøgle, som skal genereres i Managment Console.

For at gøre det skal du logge ind på AppTec360 EMM og gå til

Generelle indstillinger → Rollebaseret adgang → API-adgang, og tilføj en ny nøgle.

Du skal vælge en bruger, hvis tilladelser skal gælde for API-nøglen.

Den private nøgle kan kun downloades én gang. Når downloadet er startet, slettes nøglen, og knappen "Download" forsvinder.

Hvis du mister din private nøgle, skal du generere en ny API-nøgle.

Generelle regler

- REST-API'en er tilgængelig under basis-URL'en:

/public/external/api

- Alle anmodninger skal sendes via POST.
- REST API'en understøtter kun anmodninger via HTTPS.
- Anmodninger skal indeholde følgende overskrifter:

Overskriftsnavn	Overskriftsværdi	Beskrivelse
Indholdstype	applikation/json	fast
godkendelse	123...xyz	API-nøgle fra fanen "API-adgang"
underskrift	Base64-kodet signatur	Signatur af nyttelasten genereret med privat nøgle fra fanen "API-adgang"

- Anmodningskroppen skal være et json-kodet objekt, som skal indeholde følgende værdier:

Felt	Felt Eksempel Værdi	Beskrivelse
api	v2/enhed/listeenheder	Navn på API'en
tid	1529662725	Unix-tidsstempel (UTC) for klientmaskinen. Den maksimalt tilladte tidsforskel mellem klienten og serveren er 30 minutter.

- Hvis det lykkes, returnerer API'en de ønskede data (se forespørgslerne nedenfor) og en HTTP-statuskode 200.
- Hvis der opstår en fejl, vil HTTP-statuskoden være mellem 4xx og 5xx afhængigt af fejlen, og svarobjektet vil indeholde et array med nøglen "errors", som indeholder en liste over menneskeligt læsbare fejlmeddelelser.
- Hvis der ikke er nogen matchende data for en enhed, returneres et tomt array.
- Hvis en enheds-id ikke findes, vil dens returdata være null.

Eksempel på anmodning

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

Forespørgsler

Liste over alle enheder

Funktionalitet: Returnerer en liste over alle enheder, der indeholder enheds-ID, IMEI og serie
API URI: v2/device/listdevices
Obligatoriske parametre: ingen
Valgfrie parametre: ingen

Eksempel på anmodningskrop


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


Eksempel på svartekst


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

Hent en liste over (GPS)-positioner

Funktionalitet: Returnerer en liste over alle gemte positionslogposter for enheds-id'er
API URI: v2/device/listposition
Obligatoriske parametre: "ids" - Array af enheds-id'er
Valgfrie parametre: ingen

Eksempel på anmodningskrop


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


Eksempel på svartekst


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

Hent kort over aktiver

Funktionalitet:
Returnerer en liste over alle gemte mulige aktiver, der kan anmodes om ved hjælp af Hent alle aktivdata.
Du kan enten bruge den menneskeligt læsbare form eller aktivtagget til at anmode om dataene.
API URI: v2/device/getassetmap
Obligatoriske parametre: ingen
Valgfrie parametre: ingen

Eksempel på anmodningskrop

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

Eksempel på svartekst

Dette svar blev forkortet af hensyn til læsbarheden.

{
"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": []
}

Hent alle aktivdata

Funktionalitet: Returnerer en liste over anmodede aktivdata for enheds-id'er
API URI: v2/device/getassetdata
Obligatoriske parametre: "ids" - Array af enheds-id'er
Valgfrie parametre:
"assetkeys" - nøgler til aktivdata, der skal returneres. Hvis det ikke specificeres, returneres alle tilgængelige aktivdata
. Du kan få en liste over aktivnøgler ved hjælp af Get asset map.

Eksempel på anmodningskrop

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

Eksempel på svartekst

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

Eksempel på kode i Python3

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

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

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

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

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

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

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

Apple-konfiguration

APNS-certifikat

Her kan du uploade et APNS-certifikat. Det er nødvendigt for at administrere iOS- og MacOS-enheder.

Bemærk: APNS-certifikatet er kun gyldigt i et år. Det skal fornyes, før det udløber.
Fornyelsesprocessen er identisk med oprettelsen (se nedenfor) og tager kun et par minutter.

Hvis du glemmer at forny den i tide, kan du ikke foretage ændringer på dine allerede tilmeldte enheder **og du er nødt til at tilmelde alle enhederne igen**.

Trin 1

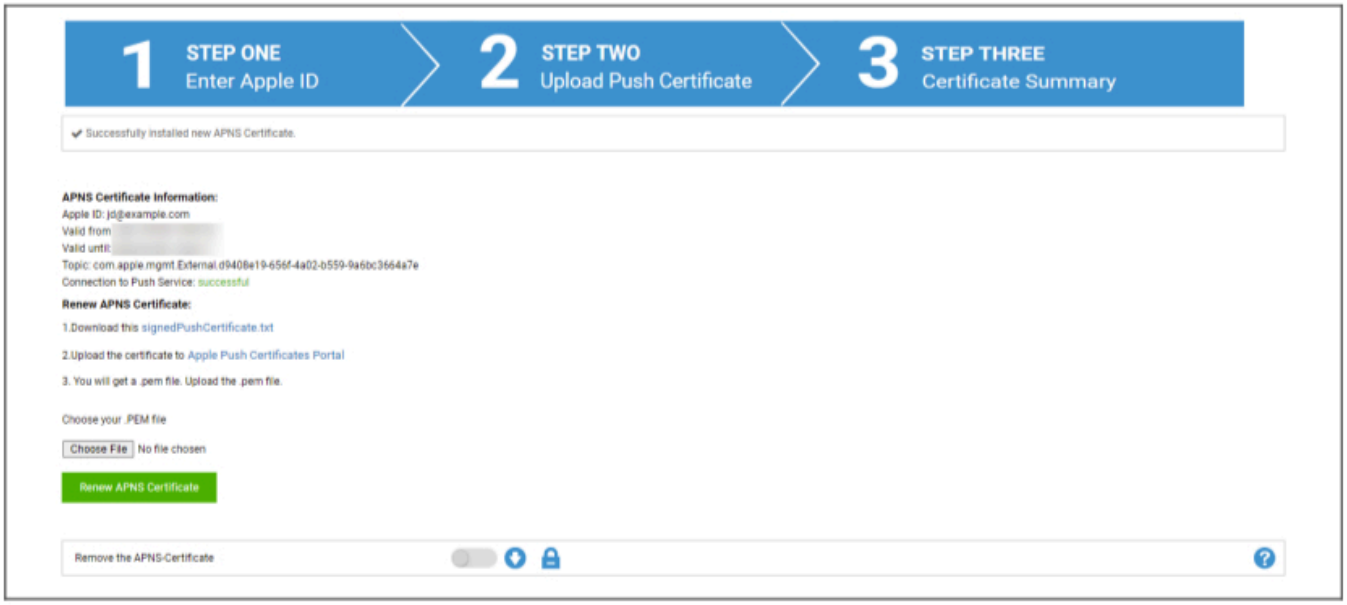
- Indtast først dit Apple-id, som du vil bruge til at oprette APNS-certifikatet.

Bemærk: Dette Apple-id bruges kun til oprettelse af APNS-certifikater. Dette Apple-id har intet at gøre med enhederne, og enhederne kender ikke til dette Apple-id. Derudover skal du også have adgang til dette Apple-id for at forny APNS-certifikatet. Derfor anbefales det at bruge et generisk Apple-id og dokumentere login-dataene. Der sendes en påmindelse til den anvendte mailadresse for Apple-id'et, før APNS-certifikatet udløber.

- Klik på "Næste trin" for at fortsætte.
- (valgfrit) Du kan også gendanne det tidligere slettede APNS-certifikat, hvis du slettede det ved et uheld

Trin 2

- Download signedPushCertificate.txt
- Gå til https://identity.apple.com/pushcert/, og log ind med Apple-id'et fra trin 1.
- Klik på "Opret et certifikat"
- (valgfrit) indtast en note. Dette kan være nyttigt, hvis du administrerer flere lejere, så du nemt kan identificere dem.
- Klik på "Choose File" for at vælge den tidligere downloadede signedPushCertificate.txt
- Klik på "Upload".
- Du vil nu se en bekræftelse på, at du har oprettet et APNS-certifikat.
- Klik på "Download", og gem den.
- Gå tilbage til administrationskonsollen.
- Klik på "Choose File", og vælg det APNS-certifikat, du vil uploade.
- Klik på "Upload"



Trin 3

Du har nu opsat APNS-certifikatet og kan nu administrere iOS- og MacOS-enheder.

I trin 3 vil du se en oversigt over dit aktuelt anvendte APNS-certifikat.

Du har også mulighed for at forny APNS-certifikatet ved at følge de trin, der vises på skærmen. Husk at forny det, før det udløber.

Når du fornyer APNS-certifikatet, skal du huske at logge ind med det Apple-id, der vises i trin 3, og også at forny det tidligere anvendte certifikat og IKKE oprette et nyt. Du vil se "emnet" for APNS-certifikatet i trin 3, og når du klikker på "i" i Apple Push Certificate Portal. Dette er det unikke ID, som identificerer certifikatet. Det hjælper dig med at identificere det korrekte og forny det korrekte.

Når du får "Fejl: Push-certifikatet har et andet emne!" under fornyelsen, betyder det, at du har fornyet et andet certifikat eller oprettet et nyt.

Hvis du vil uploade et nyt certifikat, f.eks. hvis du ikke længere kan få adgang til det tidligere anvendte Apple ID, skal du først slette det aktuelt uploadede certifikat.

Under alle omstændigheder betyder sletning af APNS-certifikatet, at du ikke længere kan foretage ændringer for de aktuelt tilmeldte enheder, før du tilmelder dem igen. Så vær sikker på, at du er forberedt på dette, og fjern kun certifikatet, hvis der ikke er andre muligheder.

Administreret adgang

Her kan du aktivere brugertilmelding for iOS-enheder og delt iPad for iOS-enheder.

Brugertilmelding

'User Enrollment' aktiverer en særlig tilstand for BYOD-enheder.

For hver bruger skal der oprettes et administreret Apple-ID i Apple Business Portal.

Under tilmeldingsprocessen vil brugerne blive bedt om deres Apple-ID-oplysninger.

"User Enrollment" garanterer maksimal sikkerhed for brugeren, da den kun tillader et begrænset sæt indstillinger og begrænsninger, der kan konfigureres af MDM.

Administreret domæne:

Det domæne, der bruges til at mappe brugerens e-mailadresse til deres administrerede Apple-ID (skal være i formatet: '@appleid.company.com'), f.eks. vil john.doe@example.com blive mappet til john.doe@appleid.company.com.

Tjek Apple Business Manager for at se dit Managed Domain

Fælles iPad

En delt iPad er en DEP-enhed, der er konfigureret med en særlig DEP-profil.

Dette gør det muligt for flere brugere at logge ind på enheden ved hjælp af deres administrerede Apple-ID.

Det administrerede Apple-ID skal oprettes i Apple Business Portal eller Apple School Manager.

Brugere, der logger ind på en delt iPad, bliver bedt om at angive deres administrerede Apple-ID-oplysninger.

Administreret domæne:

Det domæne, der bruges til at mappe brugerens e-mailadresse til deres administrerede Apple-ID (skal være i formatet: '@appleid.company.com'), f.eks. vil john.doe@example.com blive mappet til john.doe@appleid.company.com.

Tjek Apple Business Manager for at se dit Managed Domain

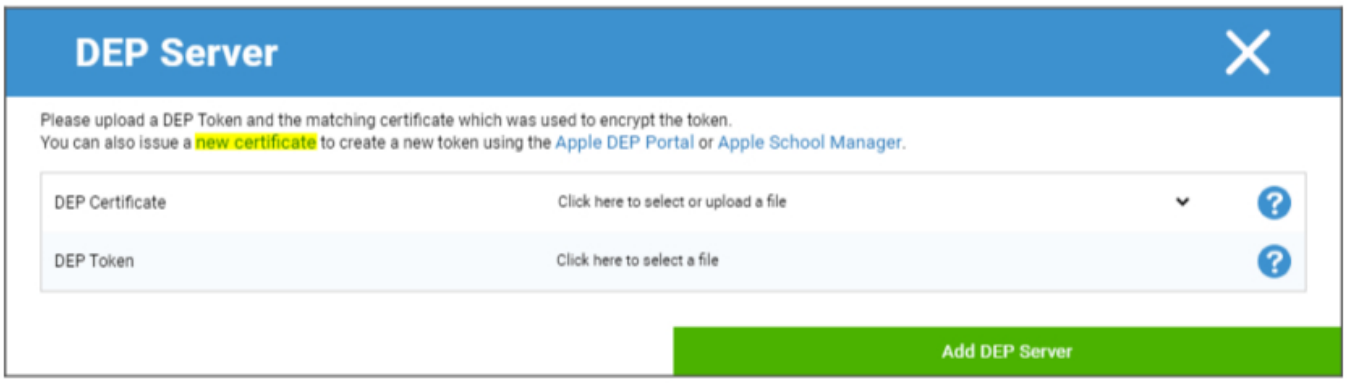
DEP

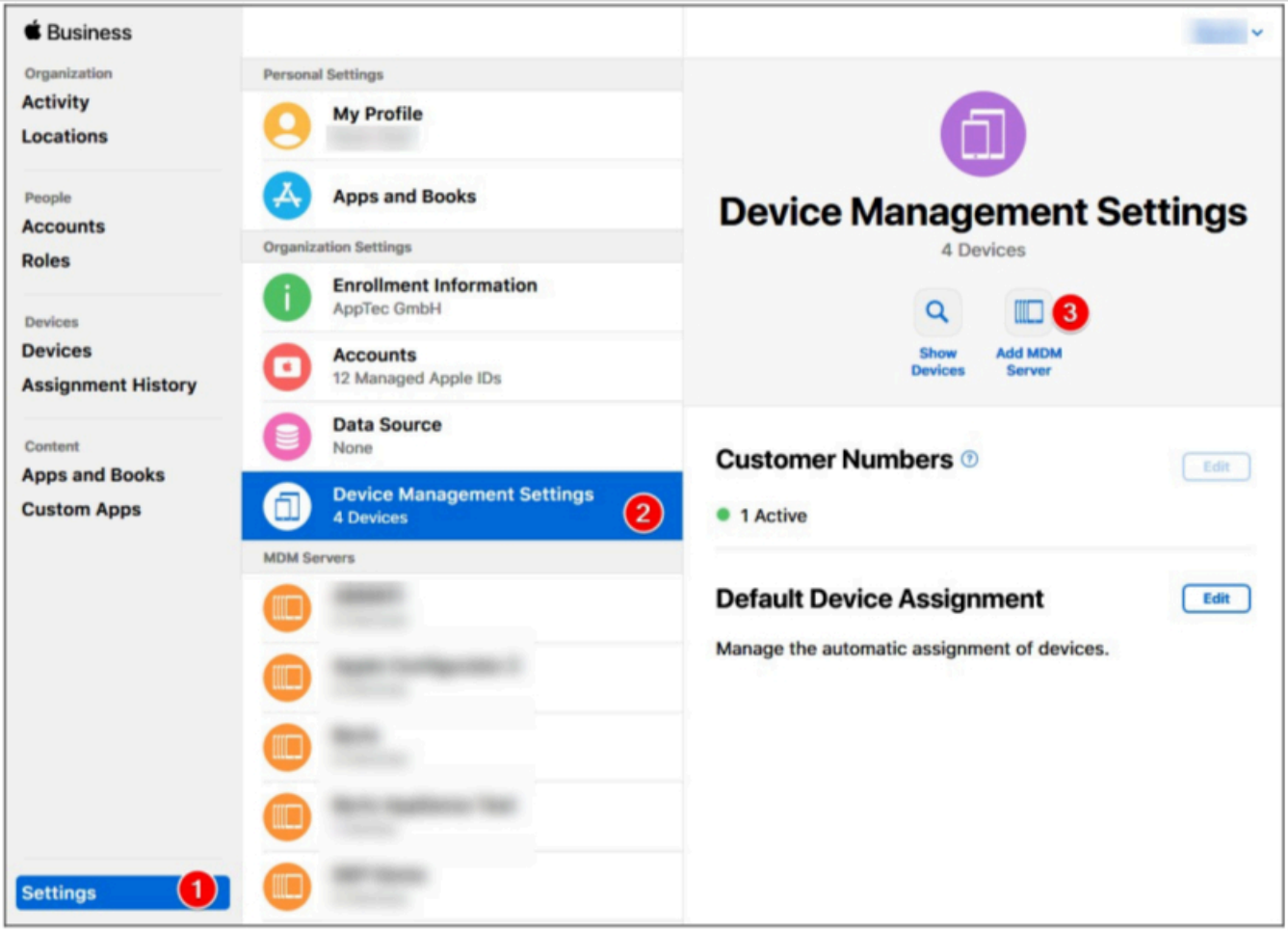
DEP (Device Enrollment Program) giver dig mulighed for nemt at tilmelde enheder til MDM. Når du bruger DEP, bliver enhederne automatisk forbundet til MDM, når du opsætter enheden. Du kan også springe næsten alle de opsætningstrin over, som normalt er obligatoriske på iOS.

Husk, at du skal købe enhederne hos en forhandler, der understøtter DEP. Kontakt din forhandler eller Apple for at få flere oplysninger.

Mere information om DEP: https: //www.apple.com/business/dep/

Klik på "+" for at tilføje et DEP-token. I pop op-vinduet skal du klikke på "nyt certifikat" i teksten (markeret med gult på billedet nedenfor). Dette vil generere og downloade et DEP certifikat. Gå derefter til Apple Business Manager(https://business.apple.com/) eller Apple School Manager(https://school.apple.com/).

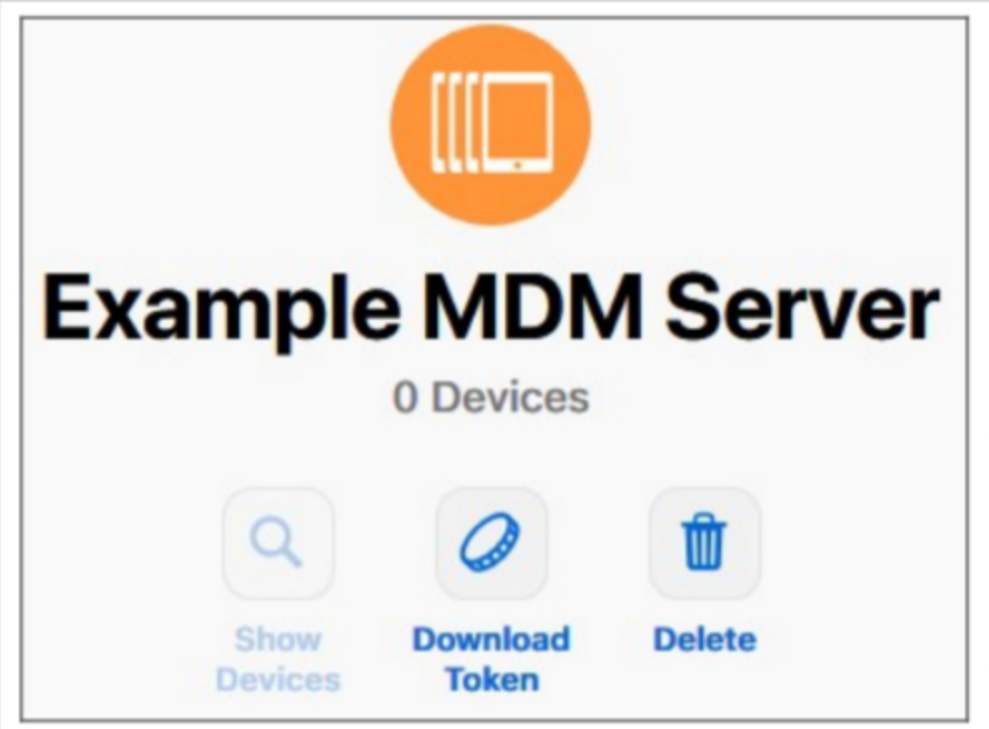




I Apple Business Manager skal du følge trinnene som vist på billedet ovenfor. Indstillinger → Indstillinger for enhedshåndtering → Tilføj MDM-server.

Giv serveren det navn, du ønsker, og upload det tidligere downloadede DEP certifikat under MDM Server Settings → Upload Public Key, og klik på "Save".

Du vil nu få muligheden "Download Token". Klik på den, og gem den. Tokenet er kun gyldigt i 1 år. Men hvis du klikker på "Download Token" igen, får du et nyt, hvilket gør det meget nemt at forny tokenet.



Du kan nu gå tilbage til MDM, hvor du tidligere har downloadet DEP-certifikatet. Hvis du ikke lukkede fanen, bør popup-vinduet til tilføjelse af en DEP-server stadig være åbnet, og DEPcertifikatet bør allerede være valgt. Du kan nu uploade dit Token i feltet "DEP Token" og klikke på DEP Server.

I kolonnen "**Enheder**" kan du se antallet af enheder, der er tildelt denne DEP-server. Enheder, der føjes til denne DEP-server, oprettes automatisk i DEP-puljen i Mobile Management.

Du kan klikke på dette nummer for at få et overblik over alle dine DEP-enheder og deres status.

Bemærk: Afhængigt af din arbejdsgang eller konfiguration i Business Manager kan det være, at du manuelt skal tildele disse enheder til DEP-serveren. Du kan også indstille en standard DEP-server i Apple Business Manager for nye enheder.

I kolonnen "**Profiler**" kan du se, hvor mange DEP-profiler du har. Du kan også klikke på dette tal for at se detaljer om dine DEP-profiler, og du kan slette gamle/ubrugte profiler her. Det er i øjeblikket ikke muligt at ændre disse. Hvis du vil foretage en ændring, skal du oprette en ny.

I kolonnen "**Sidste synkronisering**" kan du manuelt synkronisere DEP-serveren (f.eks. hvis du lige har tilføjet en ny enhed til DEP) og se datoen for den sidste vellykkede synkronisering.

I kolonnen "**Auto Profile**" kan du indstille en DEP-profil som automatisk standard. Denne profil vil automatisk blive tildelt nye enheder. Hvis du ikke indstiller en automatisk profil, skal du manuelt tildele en profil til nye enheder hver gang.

I kolonnen "**Tilføj**profil" kan du tilføje en ny DEP-profil. Enheden vil modtage denne i begyndelsen af opsætningen af enheden. DEP-profilen definerer, hvordan enheden sættes op, og hvilke opsætningstrin der springes over.

Bemærk: Når en enhed er tilmeldt, kan disse indstillinger kun ændres ved at udføre en fabriksnulstilling og tilmelde enheden med en ny profil. Dette er især relevant for "**Flytbar**" og "**Tillad parring**". I tilfælde af "**Tillad par**ring" anbefales det at slå dette til, da det kan deaktiveres via MDM-restriktioner, men det kan ikke aktiveres igen, hvis det er deaktiveret i DEP-profilen.

I kolonnen "**Rediger**" kan du uploade et nyt token, f.eks. når du fornyer tokenet.

Konfigurator og URL

URL'er til tilmelding til puljen

Her kan du oprette en tilmeldings-URL og en tilmeldings-QR-kode, som er gyldig i et bestemt antal tilmeldinger og indtil en bestemt dato. Dette giver dig mulighed for at tilmelde flere enheder med kun ét link eller én QR-kode.

Enheder, der er tilmeldt med denne URL eller QR-kode, vil være i puljen i Mobile Management, og du skal manuelt tildele dem til en gruppe eller bruger bagefter.

Bemærk: Dette er kun til manuel tilmelding. Brug ikke denne URL, hvis du tilmelder enhederne via Apple Configurator.

MDM-profil – Apple Configurator

Her kan du få den URL, du skal bruge, når du tilmelder enheder via Apple Configurator. Når du forbereder enheder med Apple Configurator, kan du tilføje enhederne til MDM i samme proces. Apple Configurator kræver denne URL til dette.

Enheder, der tilføjes via Apple Configurator, vil være i puljen i Mobile Management, og du skal manuelt tildele dem til en gruppe eller bruger bagefter.

Du finder også en .mobileconfig-fil her, som kan bruges til at tilmelde enhederne via Apple Configurator. Under alle omstændigheder anbefales det at bruge URL'en.

Android-konfiguration

Android-konfiguration

Fjern beskyttelse	Hvis denne funktion er aktiveret, kan brugeren ikke deaktivere enhedsadministratoren uden at indtaste den adgangskode, der er indstillet af MDM-administratoren. Adgangskoden indstilles under tilmeldingen, så enhederne skal tilmeldes igen for at opdatere adgangskoden. Der er to muligheder for at fjerne enhedsadministratorerne: 1. Manuelt på enheden ◦ Åbn EMM-appen på enheden ◦ Skift til fanen Status ◦ Tryk på "Fjern beskyttelse" ◦ Indtast adgangskoden Du kan bruge Revision til at få den korrekte adgangskode fra "Adgangskodehistorik" i konsollen. ◦ Rul ned, og tryk på det nyligt tilføjede punkt, "Tryk for at afinstallere AppTec360 MDM App" (du har 20 sekunder til at udføre denne opgave). ◦ Bekræft dialogen "Afinstaller AppTec360 MDM App" med "ok". Dette vil afmelde enheden fra konsollen. ◦ For at fjerne appen fra enheden skal du bekræfte dialogen "AppTec360 MDM vil blive afinstalleret" med "UNINSTALL". 2. den automatiske (konsol) ◦ Vælg enheden i konsollen ◦ Klik på det blå tandhjulsikon, og vælg "Enterprise Wipe" Bemærk: Kun tilgængelig med Android 4.x og lavere versioner eller på enheder med KNOX API (Samsung-enheder).
Fjern adgangskode (revision x)	Den etablerede adgangskode, som brugeren kan fjerne enhedsadministratoren med

	Revision x = tæller, hvor ofte adgangskoden allerede er blevet ændret Det er vigtigt, hvilken adgangskode brugeren har brug for, fordi det er muligt, at enheden ikke har kommunikeret med AppTec360-serveren, og derfor er den nyeste adgangskode ikke blevet overført endnu.
Adgangskode-historik	Når du klikker på den blå knap ("Vis historik"), kan du se de tidligere oprettede adgangskoder
Udvidet beskyttelse mod afinstallation	Denne mulighed giver beskyttelse mod ikke-SAFE-enheder Så længe denne indstilling er aktiveret, er det ikke muligt nemt at deaktivere enhedens administrator.
Opfordre brugeren til at afinstallere blokerede apps?	Hvis det er muligt, vil blokerede apps ikke kun blive blokeret, men også afinstalleret automatisk. Brugeren bliver bedt om at afinstallere blokerede apps, hvis det ikke er muligt at afinstallere dem automatisk.
Intelligent system-app-blokering	Hvis Whitelisting er aktiveret, blokerer Android MDM-klienten alle brugerinstallerede apps. Aktivér denne indstilling for at blokere alle systemapps, der kan startes i hvidlistningstilstand.

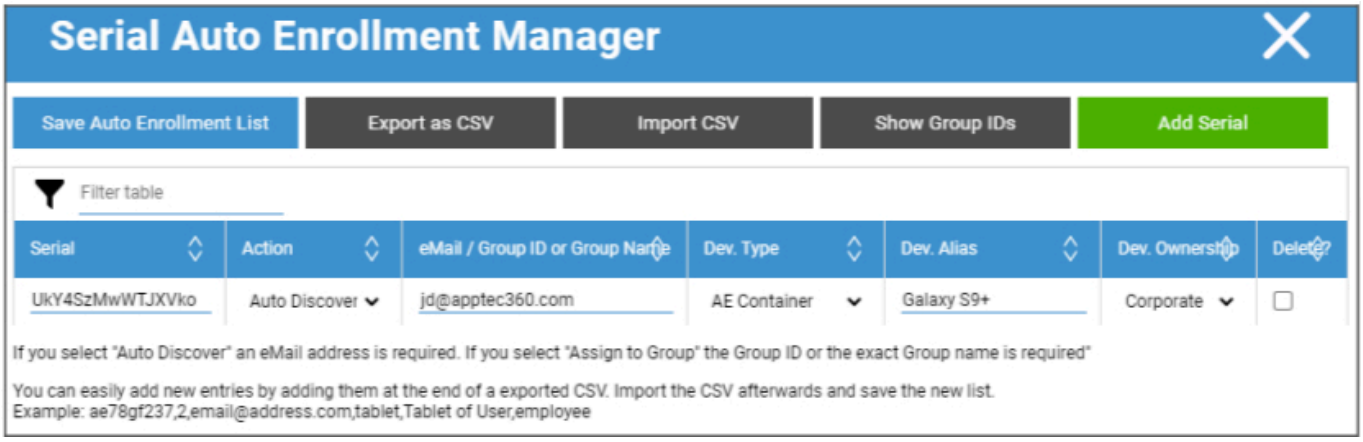
Automatisk tilmelding

Her kan du aktivere funktionen Autotilmelding for at tilmelde dine enheder automatisk, når AppTec360 MDM Client åbnes på enheden.

Vigtigt: Denne tilmeldingsmetode er forældet og fungerer ikke længere på Android 10 eller nyere. Når du bruger Android 7 eller nyere, skal du under alle omstændigheder tilmelde enheder som Android Enterprise fully managed. Hvis du vil bruge Android Enterprise BYOD-containeren, og du bruger Android 10 eller nyere, skal du tilmelde enheden manuelt via legitimationsoplysninger, QR-kode eller SMS. Under alle omstændigheder bruges Auto Enrollment List stadig til at automatisere tilmeldingsprocessen til f.eks. AE Enrollment, Knox Enrollment osv.

Under alle omstændigheder bruges den automatiske tilmeldingsliste stadig til at automatisere tilmeldingsprocessen for fx AE-tilmelding, Knox-tilmelding osv.

Ved enten at klikke på "Serial Manager" eller "IMEI Manager" kan du tilføje henholdsvis Serial eller IMEI for dine enheder. Det er ikke nødvendigt at gøre begge dele for dine enheder, kun én er nok.



Handling definerer, om enhederne skal tilmeldes puljen, en bruger eller en gruppe.

Du kan også eksportere og importere en .csv-fil og filtrere dine poster efter nøgleord.

Android Enterprise

Her kan du opsætte Android Enterprise. Dette er nødvendigt for at bruge alle Android Enterprise-funktioner.

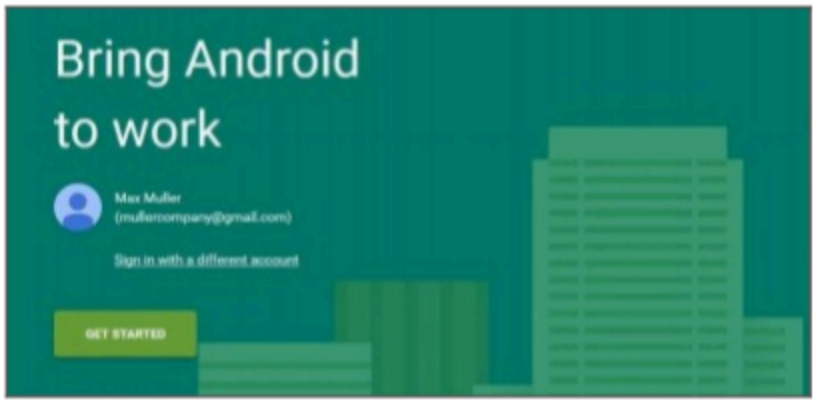
Første metode: Android Enterprise-konto (Google-konto)

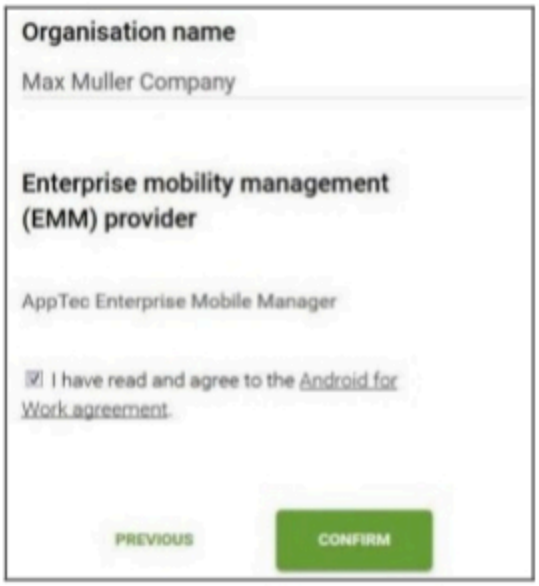
Tryk først på "Prepare Setup", og efter et kort øjeblik skal der være en knap til "Start Setup".

Dette vil bringe dig til Googles Android Enterprise-opsætningsside.

Log ind med den Google-konto, du vil bruge, hvis du ikke allerede er logget ind, og tryk på "Kom i gang".

Nu kan du indtaste navnet på din virksomhed. Når du har gjort det, skal du markere afkrydsningsfeltet og trykke på "Bekræft".





I det sidste trin kan du afslutte din registrering og bør vende tilbage til konsollen. Hvis alt har fungeret, bør det se sådan ud:

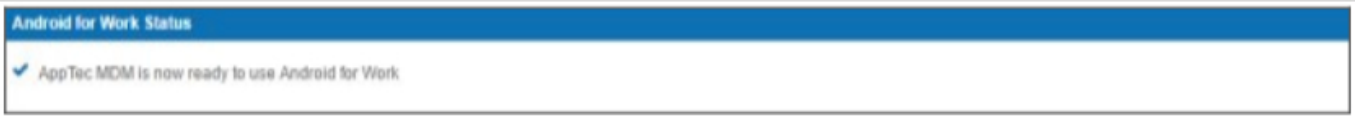
Nu kan du begynde at konfigurere din Android Enterprise Container.

Anden metode: G-Suite-konto

Tryk på "Brug G-Suite", og log ind på din Google Admin-konto. Der skal du gå til "Sikkerhed" -> "Vis mere" -> "Administrer EMM-udbyder til Android" og generere et token. Bemærk: Hvis du ikke kan se Android Enterprise Settings i din G-Suite-konto, skal du gå til "Få flere apps og tjenester" og tilføje Android-enhedsstyring. Indtast nu tokenet og dit primære domæne i vores konsol, og klik på "Gem ændringer". Når du er færdig, skal du klikke på "Brug Android Enterprise-konto".

Nu bør du se knappen "Opret servicekonto". Klik på den. Denne proces kan tage et par øjeblikke.

Hvis alt fungerede, skulle det se sådan ud:



Nu kan du begynde at konfigurere din Android Enterprise Container.

Beskyttelse mod fabriksnulstilling

Med Factory Reset Protection kan du binde din enhed til en Google-konto efter eget valg, hvilket også tilsidesætter enhver eksisterende binding til en Google-konto. For at bruge Factory Reset Protection skal du først konfigurere det her og derefter aktivere det i dine profiler.

For at indstille Factory Reset Protection skal du klikke på "FRP Setup" og følge instruktionerne på skærmen.

BEMÆRK: Læs og udfør trinnene omhyggeligt. Vi anbefaler, at du gør det i et nyt inkognito-browservindue for at undgå, at du automatisk logger ind på den forkerte Google-konto. Du kan låse dig selv helt ude af enheden, hvis du skulle indtaste et forkert ID eller miste adgangen til den brugte Google-konto!

AE-tilmelding

Her kan du aktivere Android Enterprise Ernollment. Ved at bruge denne metode tilmelder du dine enheder til Android Enterprise Device Owner Mode. I denne tilstand har du fuld kontrol over enheden.

Aktiver AE-tilmelding	Aktiverer AE-registrering Forsigtig: Hvis du deaktiverer AE Enrollment, vil eksisterende QR-koder og allerede konfigurerede NFC-programmeringsenheder holde op med at virke. Hvis du aktiverer AE Enrollment igen, skal du sende NFC-push-konfigurationer / generere nye QR-koder.
Aktivér automatisk opdagelse	Når en enhed tilmelder sig selv via "AE Enrollment", vil systemet forsøge at tildele den til en bruger baseret på de oplysninger, der er angivet i Serial / IMEI Whitelist ("General Settings" > "Android Configuration" > "Auto Enrollment").
Bloker ukendte enheder	Kun enheder, der er blevet hvidlistet i Serial / IMEI Whitelist ("General Settings" > "Android Configuration" > "Auto Enrollment"), har lov til at tilmelde sig.

Bemærk om metode 1 og 2: "Velkomstskærm" henviser til den første skærm, du ser efter fabriksnulstillingen. Den kan se anderledes ud afhængigt af den Android-version og/eller enhedsmodel, du bruger.

Metode 1: Tilmelding med QR-kode

(kræver Android 7.0 eller nyere) Vi anbefaler, at du altid bruger denne metode, hvis du kører Android 7 eller nyere.

1. Nulstil enheden til fabriksindstillinger
2. Generer QR-koden til indskrivningen ved hjælp af en af de to følgende metoder:
    - Klik i "Generelle indstillinger -> Android-konfiguration -> AE-tilmelding" på "Generer QR-kode". Vælg, om du vil springe lagerkrypteringen over, og/eller om alle systemapps skal fjernes.
    - (alternativt) Vælg en eksisterende enhed. Klik på den QR-kode, der vises i "Enhedsoversigt". Vælg, om du vil springe lagerkrypteringen over, og/eller om alle systemapps skal fjernes.
3. Tryk nu 6 gange på velkomstskærmen på din enhed. Dette burde starte QR-tilmeldingsfunktionen.
4. Opret nu forbindelse til et trådløst netværk, og vent kort tid, indtil QR-kodelæseren er installeret.
5. Scan nu QR-koden
6. Sådan er det. Din enhed er nu tilmeldt Android Enterprise Device Mode.
    - a. Hvis du har brugt QR-koden i "Generelle indstillinger", kan du finde din enhed i "Pool -> AE Device Owner Devices". (Tip: Det er muligt, at du skal genindlæse siden for at se

enhederne). Hvis du har markeret "Aktivér automatisk opdagelse", kan du finde den under din Auto Discover-bruger.

- Hvis du har brugt QR-koden for en eksisterende enhedsprofil, vil enheden blive registreret i denne profil.

Metode 2: NFC-tilmelding

(kræver NFC og Android 6.0 eller nyere)

Forberedelse: Indtast dine WiFi-oplysninger i "Generelle indstillinger -> Android-konfiguration -> AE-tilmelding -> Data til NFC-tilvejebringelse". Brug nu "NFC Device" til at søge efter den enhed, der skal være programmør. Denne enhed vil blive brugt til at sende tilmeldingsoplysningerne til de andre enheder via NFC.

1. Fabriksindstil din enhed
2. Åbn NFC-parringsappen fra AppTec360 på din programmeringsenhed
3. Vælg, om du vil springe lagerkrypteringen over, og/eller om alle systemapps skal fjernes.
4. Hold begge enheder ryg mod ryg
5. Nu skal Android Enterprise Enrollment være skarp
6. Du finder nu din enhed i konsollen
    - a. I puljen, hvis du ikke har konfigureret Auto Discover
    - b. Inden for den bruger, du har konfigureret til Auto Discover
    - c. Tip: Det er muligt, at du er nødt til at genindlæse siden for at se enhederne

Metode 3: Google-konto

(kræver Android 5.1 eller nyere)

(Bemærk: Hvis du bruger denne metode, bliver enheden ikke automatisk tilmeldt. I stedet skal du tilmelde den manuelt eller automatisere processen ved at bruge Auto Enrollment).

1. Fabriksindstil din enhed
2. Gå gennem opsætningstrinnene, indtil du kan logge ind med en Google-konto
3. Indtast "afw#apptec" som brugernavn/mail
4. Tryk på "Næste"
5. Din enhed er nu en Android Enterprise-enhed

KNOX Indskrivning

Her kan du aktivere KNOX Enrollment og finde de oplysninger, du skal bruge for at oprette en KNOX Enrollment Profile i KNOX Deployment Portal. Du skal have en konto på KNOX Deployment Portal for at konfigurere og bruge dette.

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

Aktiver KNOX-tilmelding	Aktiverer KNOX-tilmelding. Vær opmærksom: Hvis du deaktiverer KNOX Enrollment, vil eksisterende MDM-profiler holde op med at fungere. Hvis du aktiverer KNOX Enrollment igen, skal du opdatere feltet "Custom JSON Data" i din MDM-profil.
Aktivér automatisk opdagelse	Når en enhed tilmelder sig selv via "KNOX Enrollment", vil systemet forsøge at tildele den til en bruger baseret på de oplysninger, der er angivet i Serial / IMEI Whitelist ("General Settings" > "Android Configuration" > "Auto Enrollment").

1. Log ind på Samsung KNOX Mobile Enrollment Portal https://eukme.samsungknox.com/itadmin
2. Gå til "MDM-profiler"
3. Klik på "Tilføj"
4. Vælg "Server URI not required for my MDM", og klik på "Next".
5. Opret nu en profil med de oplysninger, der vises i administrationskonsollen

Nu kan denne KNOX Enrollment Profile installeres direkte på enheden af Samsung, hvis du køber enhederne direkte fra Samsung.

Alternativt kan du downloade KNOX Deployment App, logge ind med din KNOX Deployment Account og sende KNOX Enrollment Profile via NFC til andre enheder.

Hvis enheden har en KNOX-tilmeldingsprofil installeret, vil den downloade vores app og tilmelde enheden, hvis den har en fungerende internetforbindelse.

Enheder, der tilmeldes via KNOX Enrollment, kan findes i "Pool -> KNOX Enrollment" eller i den bruger, du har angivet i Auto Discover.

Nul berøring

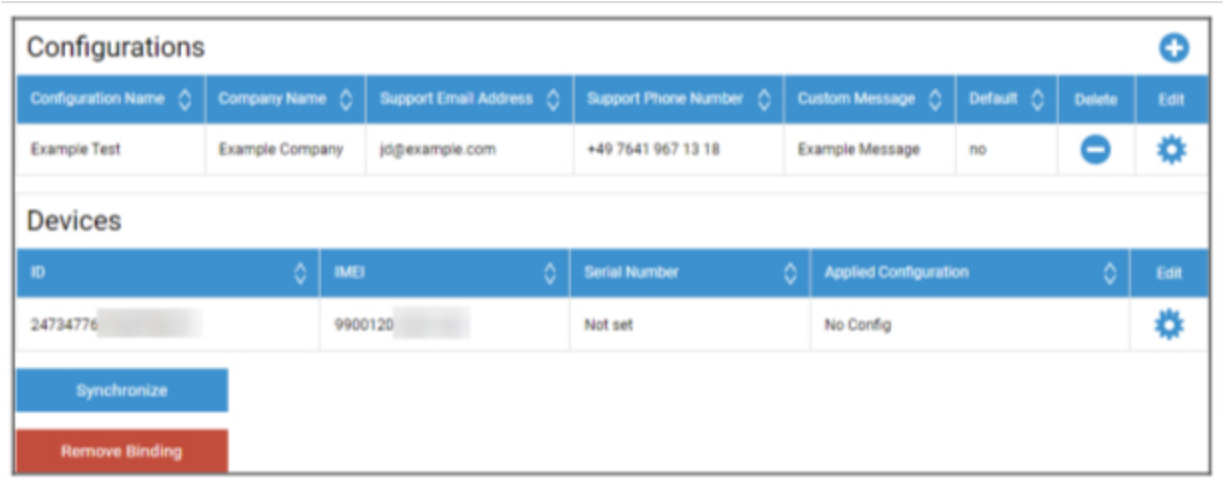
Med Zero-Touch kan du nemt tilmelde dine enheder uden at skulle røre ved dem eller konfigurere noget på selve enheden. Du skal bare tænde den, fortsætte gennem konfigurationen som normalt, og enheden vil helt automatisk modtage alle oplysninger om, hvordan den skal opsættes og forbindes til MDM.

For at bruge Zero-Touch skal du købe dine enheder hos en forhandler, der understøtter Zero-Touch. Den samme forhandler opretter også en konto til dig i Zero-Touch-portalen. Kontakt din forhandler for at få mere information om proceduren, eller hvis du har problemer med at få adgang til Zero-Touch-portalen.

Klik på "Start opsætning" for at starte opsætningen. Du vil blive omdirigeret til en login-side, hvor du skal vælge din Google-konto, som har adgang til Zero-Touch Portal.

BEMÆRK: Det er muligt at vælge en hvilken som helst konto. Så sørg for at vælge den rigtige konto i dette trin. Hvis du ikke kan se dine enheder/konfigurationer, har du højst sandsynligt brugt den forkerte konto.

Når du er færdig med at logge ind, ser det sådan ud:



Klik på "+" for at tilføje en konfiguration, og udfyld felterne som vist på skærmen. Hvis du aktiverer konfigurationen som standardkonfiguration, vil den automatisk blive tildelt de nye enheder. Oprettelse eller indstilling af en standardkonfiguration tildeler den ikke til allerede eksisterende enheder.

Hvis en enhed ikke har fået tildelt en konfiguration, vil den blive konfigureret som en normal enhed og ikke oprette forbindelse til MDM. Sørg derfor for, at dine enheder har fået tildelt en konfiguration.

Når du har tilsluttet din konto, dine enheder er synlige, og du har tildelt en konfiguration til dem, kan du begynde at konfigurere enhederne.

Du kan tilføje enhederne til den automatiske tilmeldingsliste, så de automatisk bliver tilmeldt en bestemt gruppe eller bruger. Hvis du ikke har konfigureret noget på listen over automatisk tilmelding, vil enhederne blive tilmeldt puljen.

Windows-konfiguration

Windows-konfiguration

Her har du mulighed for at aktivere følgende konfigurationer på din Windows 10-pc:

Øjeblikkelig DM-forbindelse	
Første forsøgstid	Opretter det første forbindelsesforsøg til enheden, denne værdi stiger eksponentielt
Forbindelsesforsøg	Angiver, hvor mange forbindelsesforsøg DM-klienten skal udføre i tilfælde af en forbindelsesfejl.
Maksimal søvntid	Angiver den maksimale hviletid efter en forbindelsesfejl
Første synkroniseringsforsøg	Intervaller, hvor enheden skal kommunikere med serveren efter den første forbindelse
Første forsøgsinterval	Relaterer til "Første synkroniseringsforsøg" Her er tiderne angivet i minutter For eksempel under "First Sync Retries" er værdien "2" angivet, og under "First Retry Interval" er værdien "4 Minutes" angivet, på denne måde kommunikerer enheden 2 gange hvert 4. minut efter den første forbindelse.
Andet synkroniseringsforsøg	Intervaller, hvor enheden skal kommunikere med serveren efter at have gennemført "Første synkroniseringsforsøg"
Andet gentagelsesinterval	Samme princip som for "First Retry Interval" - bare at det her gælder for "Second Sync Retries".
Regelmæssige synkroniseringsforsøg	Intervaller for, hvor ofte enheden skal kommunikere med serveren i fremtiden Standard: "Uendelig" Vi anbefaler, at du ikke ændrer denne værdi, for hvis du indtaster "10", vil enheden kommunikere med serveren 10 gange og derefter stoppe. Derfor afbrydes kommunikationen med AppTec360-serveren!
Regelmæssigt gentagelsesinterval	Samme princip som for "First/Second Retry Interval" - bare at her gælder indstillingerne for fremtiden.
Regelmæssigt gentagelsesinterval	Samme princip som for "First/Second Retry Interval" - bare at her gælder indstillingerne for fremtiden.

Indholdsboks

Konfiguration

Her kan du konfigurere ContentBoxen. Du kan placere filer til grupper i ContentBox, som du kan få adgang til med ContentBox-appen på enheden.

Aktivér indholdsboks	Aktivér ContentBox. Hvis du deaktiverer dette, hvis du ikke bruger ContentBox, kan du spare ressourcer på OnPremise-maskiner.
Brug ekstern ContentBox-installation	ContentBox kan også betjenes med din egen Nextcloud.
URL	Komplet URL til Nextcloud-enheden
Rodbruger	Root-bruger af Nextcloud-kontoen
Adgangskode til roden	Root-adgangskode til Nextcloud-kontoen
Standardtilladelser til gruppemapper	Standardtilladelser til gruppemapper, kan ændres individuelt af gruppen (i Mobile Management)
Del gruppemappe med undergrupper	Hvis den er aktiv, kan hver undergruppe læse alle hovedgruppens mapper, kan også konfigureres individuelt for hver gruppe (Mobile Management).
Tilladelser til undergrupper	Tilladelser til undergrupper kan konfigureres individuelt for hver gruppe (Mobile Management)
Tillad deling	Giver brugeren mulighed for at dele indholdet via links, kan konfigureres individuelt for hver gruppe
Maksimal størrelse på filupload i MB	Maksimal størrelse på en fil Standard: 512 MB Maksimal konfiguration: 2048
WebDAV-legitimationsoplysninger	
WebDAV-URL	Du kan også åbne ContentBox med WebDAV. Du må under ingen omstændigheder slette følgende mapper: /apptecgroups /apptecgroups/AppTecGroup-X
Rodbruger	Navn på rodbrugerne
Adgangskode	Root-brugernes adgangskode

Synkroniseringen med ContentBox sker automatisk. Du kan dog udføre en manuel synkronisering med "Synkroniser ContentBox".

Her kan du desuden aktivere/deaktivere ContentBox på hver enkelt enhed.

Dette er kun relevant, hvis du ikke har licenseret ContentBox yderligere, så har du stadig adgang til 25 enheder, som du kan teste ContentBox med - her kan du aktivere dette for de respektive enheder.

LDAP-konfiguration

Oversigt over LDAP

Her kan du oprette en forbindelse til dit Active Directory via LDAP for at masseimportere brugere og grupper. Synkroniseringen skal udføres manuelt. Du kan konfigurere flere LDAP-forbindelser til forskellige systemer eller med forskellige konfigurationer/filtre.

Serverens navn	Serverens visningsnavn
Type	I øjeblikket understøttes kun Active Directories, der understøtter LDAP.
LDAP-domæne	Det primære LDAP-domæne (f.eks. example.com)
LDAP-vært	Kun nødvendigt, hvis LDAP-værten ikke kan nås under det givne LDAP-domæne.
Havn	Lad det være tomt for at bruge standardport (389 eller 636 for SSL)
Brugernavn	F.eks. CN=John,OU=Users,DC=EXAMPLE,DC=COM Bemærk: De fleste systemer kræver brugernavnet i dette format og accepterer ikke "John" som brugernavn.
Adgangskode	
Bekræft adgangskode	
Forbindelsessikkerhed	Bemærk: Når du bruger SSL eller TLS, vil certifikatet fra Active Directory blive kontrolleret. Hvis det er selvsigneret, skal du tilføje rod-CA'en til tillidslageret på den lokale maskine. Hvis du er i skyen, skal Active Directory levere et betroet certifikat, ellers vil forbindelsen kun fungere uden kryptering.
Automatisk synkronisering.	Aktiverer automatisk synkronisering af LDAP-biblioteket i det tidsinterval, der er angivet i de generelle LDAP-indstillinger.
Base DN	Hvis du ikke ønsker at synkronisere hele biblioteket, kan du angive en OU her, f.eks. OU=AndroidUsers,OU=Users,DC=EXAMPLE,DC=COM.
Medlem af	Alle importerede brugere tilføjes til den valgte gruppe
Kun aktiverede brugere?	Når den er aktiveret, vil attributten userAccountControl blive taget i betragtning, og brugere uden denne attribut vil ikke blive importeret.
LDAP-filter	Du kan bruge LDAP-filter til at filtrere, hvilke brugere der bliver importeret
Regex-filter	Du kan bruge Regex Filter til at filtrere, hvilke brugere der bliver importeret
Testforbindelse	Tester forbindelsen, når du gemmer konfigurationen

Nulstil mappestruktur ved synkronisering?	Hvis true, flyttes alle LDAP-poster tilbage til deres oprindelige placering i LDAP-træet. Anbefales at være aktiveret.
Genimportere slettede brugere og grupper?	Når den er aktiveret, vil brugere og grupper, der er blevet slettet, blive genskabt. Anbefales at være aktiveret.
Synkronisere sletninger?	Når det er aktiveret, slettes grupper og brugere, når de slettes på LDAP-serveren. Også slettede brugeres enheder slettes.

Under listen over dine LDAP-konfigurationer kan du definere den periode, hvor systemet skal synkronisere automatisk. Bruger kun de LDAP-konfigurationer til automatisk synkronisering, som har den pågældende indstilling aktiveret.

App-administration

In-house app DB

Android

Her kan du uploade de Android-apps, som din virksomhed har udviklet, og distribuere dem senere i Mobile Management i enheds- eller gruppeprofiler.

Vær opmærksom på, at vi kun anbefaler at distribuere apps på denne måde, som ikke er tilgængelige i Google Play Store.

Klik på "+" for at uploade APK'en for den app, du vil uploade. Kun APK-formatet understøttes i øjeblikket.

Uploadgrænsen på OnPremise-apparater kan øges i trin 3 i apparatets konfiguration. Hvis du gerne vil øge uploadgrænsen på Cloud, bedes du kontakte supporten for at få flere oplysninger.

Vær opmærksom på, at APK'er normalt er lidt mindre end deres indhold. Det er muligt, at en upload mislykkes på grund af dette, da APK'en pakkes ud i processen. Det er f.eks. muligt, at en APK på 95 MB fejler med en uploadgrænse på 100 MB. I dette tilfælde skal du øge uploadgrænsen som nævnt ovenfor.

Vi anbefaler også, at man først manuelt flytter APK'en til en testenhed (f.eks. via USB) og prøver at installere den manuelt med enhedens Files-app. Hvis dette af en eller anden grund ikke virker, vil det også mislykkes via MDM.

Opdater målet

Med funktionen "Update Target" kan du vælge, hvilken version af en app der skal installeres, eller hvilken version en app skal opdateres til, hvis du har aktiveret "Keep up to date" for en app.

Hvis du ikke har valgt et opdateringsmål, vil den højeste version blive brugt.

Husk, at Android ikke kan nedgradere apps. Vær også opmærksom på, at "Versionskoden" afgør, om en version er højere, lavere eller den samme. Så sørg for at øge denne version korrekt i din app, når du bygger en opdatering.

iOS

Her kan du uploade de iOS-apps, du har udviklet, og distribuere dem senere i Mobile Management i din enheds- eller gruppeprofil.

Klik på "+" for at uploade IPA'en for den app, du vil uploade. Kun IPA-formatet er understøttet indtil videre.

Uploadgrænsen på OnPremise-apparater kan øges i trin 3 i apparatets konfiguration. Hvis du gerne vil øge uploadgrænsen på Cloud, bedes du kontakte supporten for at få flere oplysninger.

Opdater målet

Med funktionen "Update Target" kan du vælge, hvilken version af en app der skal installeres, eller hvilken version en app skal opdateres til, hvis du har aktiveret "Keep up to date" for en app.

Hvis du ikke har valgt et opdateringsmål, vil den højeste version blive brugt.

MacOS

Her kan du uploade de MacOS-apps, du har udviklet, og distribuere dem senere i Mobile Management i din enheds- eller gruppeprofil.

Klik på "+" for at uploade PKG'en for den app, du vil uploade. Kun PKG-formatet understøttes lige nu.

Uploadgrænsen på OnPremise-apparater kan øges i trin 3 i apparatets konfiguration. Hvis du gerne vil øge uploadgrænsen på Cloud, bedes du kontakte supporten for at få flere oplysninger.

Opdater målet

Med funktionen "Update Target" kan du vælge, hvilken version af en app der skal installeres, eller hvilken version en app skal opdateres til, hvis du har aktiveret "Keep up to date" for en app.

Hvis du ikke har valgt et opdateringsmål, vil den højeste version blive brugt.

Windows 10

Her kan du uploade Windows 10-apps og distribuere dem senere i Mobile Management i din enheds- eller gruppeprofil.

Klik på "+" for at uploade APPX, APPXBUNDLE eller MSI for en app, du vil uploade. Kun APPX-, APPXBUNDLE- eller MSI-formatet understøttes på nuværende tidspunkt.

Du kan også uploade og definere afhængigheder for en app, som automatisk distribueres og installeres, før du installerer den ønskede app.

Uploadgrænsen på OnPremise-apparater kan øges i trin 3 i apparatets konfiguration. Hvis du gerne vil øge uploadgrænsen på Cloud, bedes du kontakte supporten for at få flere oplysninger.

Opdater målet

Med funktionen "Update Target" kan du vælge, hvilken version af en app der skal installeres, eller hvilken version en app skal opdateres til, hvis du har aktiveret "Keep up to date" for en app.

Hvis du ikke har valgt et opdateringsmål, vil den højeste version blive brugt.

Win32-pakke (.exe)

Du kan også distribuere .exe-filer/installationsprogrammer til dine enheder.

Navnet på pakken	Det navn, der vil blive vist i MDM.
Beskrivelse	Beskrivelse vist i MDM
Pakke-fil	Kun .zip-filer er tilladt. Placer de filer, du vil distribuere, i denne zip-fil.
Implementeringskontekst	**System**: Installationskommandoen kører med systemprivilegier, som er højere end "Bruger". Når man bruger "System", har processen heller ingen brugergrænseflade, så den vil være lydløs, og brugerprofilen, f.eks. miljøvariabler som %AppDat%, er ikke tilgængelig. **Bruger**: Installationskommandoen har adgang til brugerprofilen og kan vise brugergrænsefladen, hvis det er nødvendigt. Bemærk: Nogle processer arbejder måske kun i én kontekst. Hvis en software f.eks. installerer sig selv i AppData, vil den kun fungere, når man vælger "User".
Installer kommando	Den kommando, der bruges til at installere programmet. For eksempel vil installationskommandoen for en zip-fil, der indeholder "setup.exe" i roden, og som understøtter parameteren "/s" for en lydløs installation, være "setup.exe /s". Vær opmærksom på, at forskellig software kan have forskellige parametre.
Fjern kommandoen	Den kommando, der skal køres for at afinstallere softwaren via MDM. Normalt peger dette på afinstallationsprogrammet. For eksempel "C:\Program Files\ExampleSoftware\uninstall.exe".
Kravene	
Bemærk: Alle de opstillede krav skal være opfyldt, for at softwaren kan installeres. Ellers vil den ikke blive installeret. Nogle felter kan være obligatoriske. Hvis der ikke er angivet nogen værdi for et krav, vil kravet blive ignoreret.	
OS-arkitektur	OS-arkitektur
Min. OS-version	Min. OS-version
Min. ledig diskplads (MB)	Min. ledig diskplads (MB)
Min. fysisk hukommelse (MB)	Min. fysisk hukommelse (MB)
Min. antal logiske processorer	Min. antal logiske processorer
Min. CPU-hastighed (MHz)	Min. CPU-hastighed (MHz)

Yderligere krav	Du kan også manuelt definere regler eller uploade et script her for at udføre yderligere kravkontrol, hvis du ønsker det.
Regler for detektion	
Detektionsmetode	Her kan du definere, hvordan du registrerer, om appen er installeret på enheden. Installationskommandoer køres kun, når disse regler registrerer, at appen IKKE er installeret. Afinstallationskommandoer kører kun, når disse regler registrerer, at appen ikke er installeret. **Definér regler manuelt**: Giver dig mulighed for manuelt at definere en eller flere regler for f.eks. at kontrollere, om en bestemt fil, mappe, MSI eller registreringsdatabasenøgle er til stede. Hvis alle de givne regler er sande, vil appen blive anset for at være til stede. **Brug** et **script**: Upload dit eget script med dine egne kontroller. Hvis scriptet returnerer "$TRUE", vil appen blive anset for at være til stede.
Regler for detektion	

App-indstillinger

Indstillinger for iOS-appen

Her kan du definere standardindstillingerne for tilføjelse af en app til de obligatoriske apps eller virksomhedens app-butik.

Bemærk: Dette indstiller kun, hvad der er valgt som standard, når du tilføjer apps. Det ændrer IKKE eksisterende indstillinger for apps, som allerede er tilføjet i de obligatoriske apps eller enterprise app store.

Hold dig opdateret	Holder automatisk appen opdateret. Vær opmærksom på, at det kan tage op til 7 dage, efter at en opdatering er udgivet, før appen er opdateret.
Overhaler, når den ikke er styret	Hvis en app allerede er installeret som ikke-administreret (af brugeren), vil appen blive overtaget og administreret af MDM.
Fjern appen, når MDM-profilen fjernes	Afinstallerer appen, når MDM fjernes.
Forhindre sikkerhedskopiering af app-data	Forhindrer sikkerhedskopiering af app-data.

Indstillinger for Android-appen

Her kan du definere standardindstillingerne for tilføjelse af en app til de obligatoriske apps eller virksomhedens app-butik.

Bemærk: Dette indstiller kun det, der er valgt som standard ved tilføjelse. Det ændrer IKKE indstillingerne for apps, der allerede er tilføjet i de obligatoriske apps eller enterprise app store.

Hold dig opdateret	Holder automatisk appen opdateret. Kun tilgængelig for InHouse-apps.
Opdatering af kontrolleret AppTec360 EMM-klient	Hvis det er aktiveret, kan administratorer angive opdateringsmålet for AppTec360 EMM Client. En liste over alle tilgængelige versioner af AppTec360 EMM Client vil blive vist i "Generelle indstillinger" → "App Management" → "In-House App DB" → "Android".

Apps fra tredjeparter

Android

Her kan du indstille din aktiveringskode til Ikarus.

Sæt denne til "Brug aktiveringskode", og indtast din aktiveringskode her.

Bemærk: Når du har indtastet koden og gemt den, er den endnu ikke føjet til den profil, der sendes til enheden. Du skal foretage en ændring i din profil, for at koden kan blive føjet til profilen. Ændr f.eks. en kontakt i profilen fra slukket → tændt → slukket - Gem → Tildel nu.

iOS

Her kan du indtaste din SecurePIM-licens. Når du har indtastet licensen, skal du trykke på "Gem ændringer", og så kan du bruge SecurePIM-indstillingerne.

VPP / KNOX Premium

Apples Volume Purchase Program (VPP) giver dig mulighed for nemt at distribuere betalte og gratis apps til dine enheder. Det kan varmt anbefales, da du ikke behøver et Apple-id på enhederne, brugerne behøver ikke at bekræfte installationen (overvåget), brugerne behøver ikke at indtaste adgangskoden til Apple-id'et, og du kan nemt distribuere betalte apps uden at købe dem på hver enhed igen.

For at bruge VPP skal du registrere dig i Apple Business Manager.

VPP-licenser

Her kan du få et overblik over dine VPP-apps, hvor mange licenser der er brugt, og hvor mange der er tilgængelige.

Ved at klikke på hjulet kan du se, hvilke enheder der har fået tildelt en licens, og hvad status for denne tildeling er.

Ved at klikke på opdateres VPP-cachen, som sammenligner de licenser, der er tildelt i MDM, med de licenser, der er tildelt på Apples side. Dette kan i nogle tilfælde løse licensproblemer.

VPP-token

Her kan du uploade dit VPP-token, som du kan finde i Apple Business Manager under Indstillinger → Apps & Bøger. Du kan uploade flere VPP-tokens.

Du kan forny en Token ved blot at downloade en ny i Apple Business Manager, klikke på "Edit"-hjulet og uploade den nye.

"VPP Mode" bestemmer, hvordan licenstildelingen håndteres. Afhængigt af dit scenarie skal du bruge forskellige tilstande:

"Enhedsbaseret" skal bruges, når du tilmelder enhederne via QR-kode, Link, Apple Configurator eller DEP.

"Brugerbaseret" er påkrævet, hvis enhederne er tilmeldt med brugertilmelding eller som delt iPad.

Hvis du aktiverer "Automated License Management", vil brugere, der flyttes fra en gruppe til en anden, automatisk få tildelt Apple VPP-licenser baseret på den gruppeprofil, de flyttes til.

Eksisterende Apple VPP-licenser fra den gruppe, de er flyttet fra, vil ikke blive tilbagekaldt.

Nye brugere, der føjes til en gruppe, får automatisk tildelt Apple VPP-licenser baseret på den respektive gruppeprofil.

KNOX Premium-nøgle

Her kan du indtaste din KNOX Premium Key for at bruge Samsung KNOX Container.

Vær opmærksom på, at dette ikke længere understøttes siden Android 10. Brug i stedet Android Enterprise Container.

Indstillinger for App Store

Region og sprog

Her kan du indstille standardsproget og -regionen for app-søgningen i App Management.

Vær opmærksom på, at indstillingen for iTunes også definerer, hvordan systemet henter oplysninger om bestemte apps. Hvis du støder på apps i dine lister, som vises på en underlig måde (f.eks. manglende ikon), har du måske indstillet et område, hvor den specifikke app ikke er tilgængelig.

AE Play Store

Her kan du finde alle mulighederne for Play Store til Android Enterprise-enheder for at godkende apps, uploade egne apps til Play Store eller oprette dine egne webapps.

Godkendte apps

Her kan du få et overblik over alle de apps, du har godkendt.

Apps i Play Store

Dette vil indlæse en iFrame, der viser Play Store. Søg efter en hvilken som helst app, klik på den, og godkend den. Når du godkender appen, kan du også definere, at godkendelsen skal tilbagekaldes, hvis de krævede tilladelser ændres. Vi anbefaler, at du lader disse indstillinger være standard, når du godkender apps.

Når en app er blevet godkendt, kan du tilføje den til dine profiler.

Knappen "Godkend" ændres til "Tilbagekald godkendelse", når du har godkendt den, så du altid kan fjerne apps, hvis du ikke længere har brug for dem.

Private apps

Her kan du uploade din egen app som en privat app til Google Play Store. Det giver dig mulighed for at distribuere appen gennem Googles tjenester og opdatere den gennem dem. Det har også den fordel, at dine egne apps kan installeres uden brugerbekræftelse, som normalt er nødvendig.

Web-apps

Her kan du oprette webapps, som er links til bestemte websider, der kan tildeles som apps.

Du kan også give det et brugerdefineret ikon og yderligere definere, hvordan det skal vises.

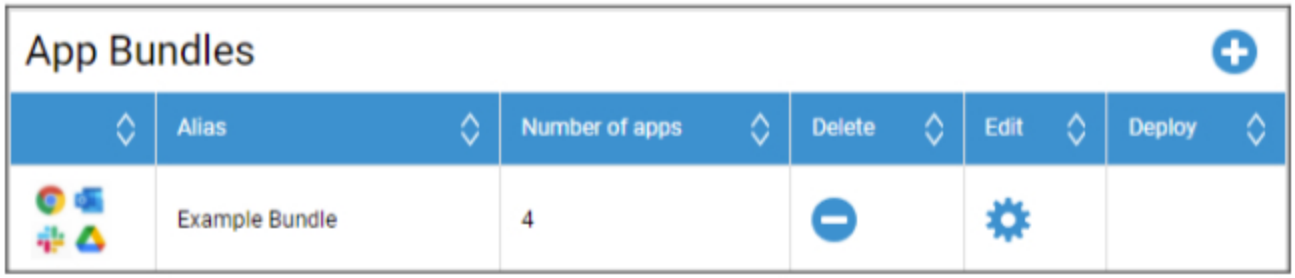
Butikslayout

Butikslayoutet definerer, hvordan apps vises i Play Butik, eller om de overhovedet vises.

Husk, at hvis du vil vise apps i Play Store, som brugeren kan installere manuelt, skal de tilføjes her i layoutet. **OG** i profilen til Enterprise Play Store. Hvis du kun tilføjer en app til én af dem, vil den ikke blive vist.

App-pakke

Med App Bundles kan du definere grupper af apps, som kan tildeles enheds- eller gruppeprofiler med et enkelt klik.



Klik på "+" for at oprette et nyt App Bundle. Når du har oprettet et App Bundle, kan du klikke på "Edit" for at tilføje apps fra forskellige kilder til Bundle.

Et bundt kan føjes til profiler som alle andre apps. Når du tilføjer apps, får du en ekstra fane med navnet "App Bundles", hvor du har dine Bundles.

Hvis du foretager en ændring i et App Bundle, vises en knap i kolonnen "Deploy". Det giver dig mulighed for at skubbe disse ændringer til alle profiler, der indeholder dette bundt. Så husk, at du skal gøre det manuelt, når du har tilføjet eller fjernet apps i et bundt.

Fjernbetjening

TeamViewer

TeamViewer-stik

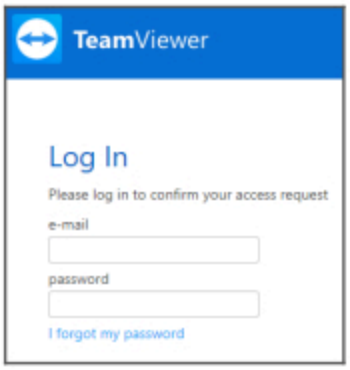
Bemærk: I den gratis prøveperiode på vores cloud-version kan du ikke forbinde din TeamViewer-konto. Du får i stedet automatisk tilknyttet en gratis demokonto.

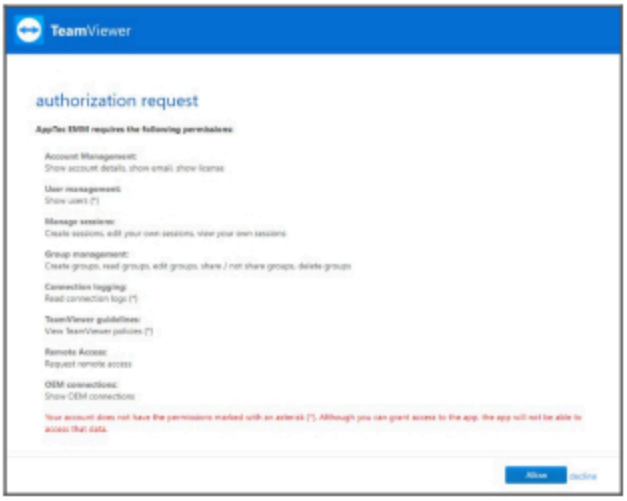
Gå til Generelle indstillinger -> Fjernbetjening -> TeamViewer. Her kan du forbinde din TeamViewer-konto med konsollen eller se oplysninger om din aktuelt tilsluttede konto. Du kan også se alle aktive sessioner, hvis du går til "Aktive sessioner".

Klik på "Start opsætning" for at forbinde din konto.

Hvis du gør det, kommer du til en ny side, hvor du skal logge ind med din TeamViewer-konto.

Når du har logget ind, skal du give AppTec360 MDM tilladelse til at bruge denne konto. Når du har bekræftet dette, skal du vente et par sekunder, og kontoen er tilsluttet.


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


TeamViewer
authorization request

Installer TeamViewer QuickSupport

Tilføj appen "TeamViewer QuickSupport" til de obligatoriske apps i din enhedsprofil eller gruppeprofil, og klik på "Tildel nu". Vent, indtil appen er installeret på enheden.

Hvis du forsøger at få adgang til en enhed, hvor appen ikke er installeret, vil den blive installeret, eller du vil blive bedt om at installere den, afhængigt af enhedens konfiguration.

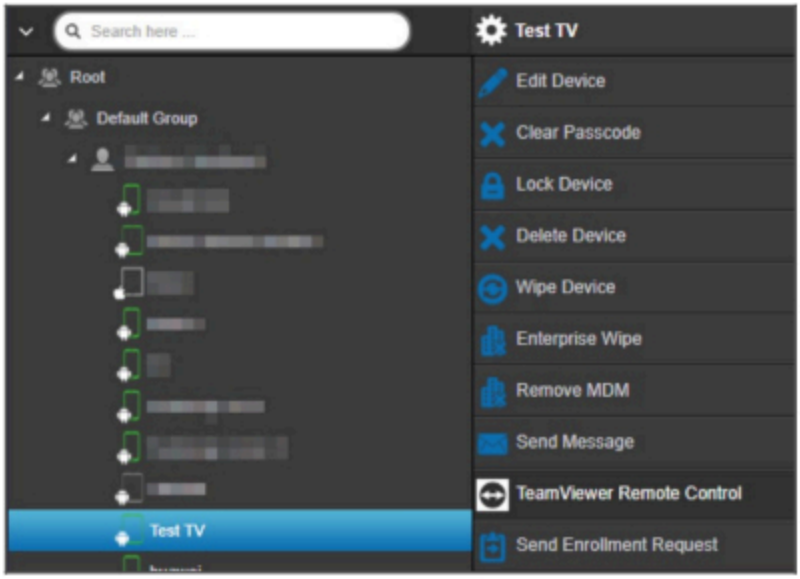
Fjernbetjen din enhed

For at fjernstyre din enhed skal du vælge enheden, klikke på hjulet og vælge "TeamViewer Remote Control"

Hvis der allerede er en aktiv session, kan du enten bruge den gamle session eller oprette en ny.

Bekræft, at du vil oprette en ny TeamViewer-session.

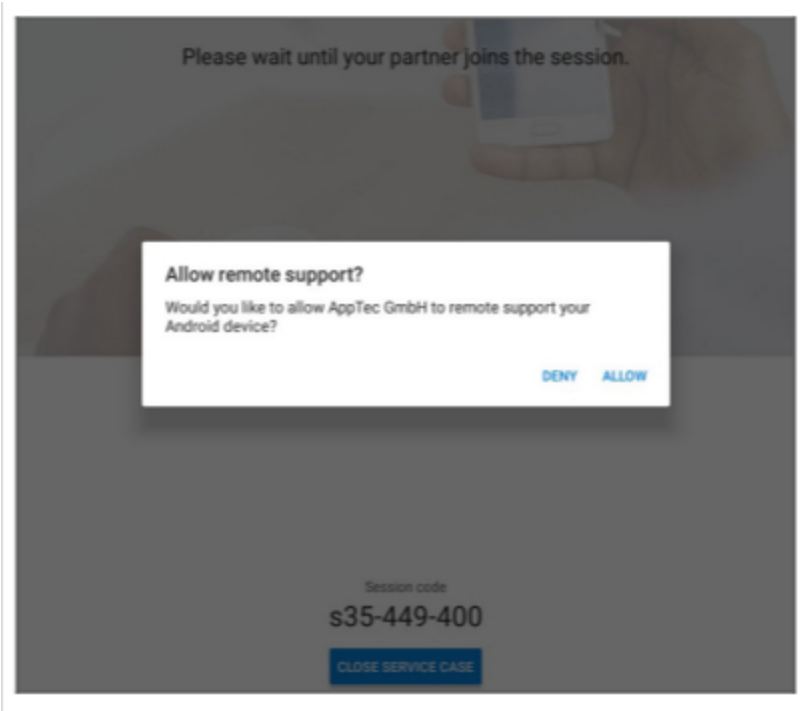
Efter et par sekunder får du et link til din TeamViewer-session. Du kan klikke på "Start" for at åbne dette link i et nyt vindue.


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


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

Dette link åbner din installerede TeamViewer og forbinder dig til din enhed.

Nu skal du bekræfte forbindelsen på selve enheden for at kunne fjernbetjene den.

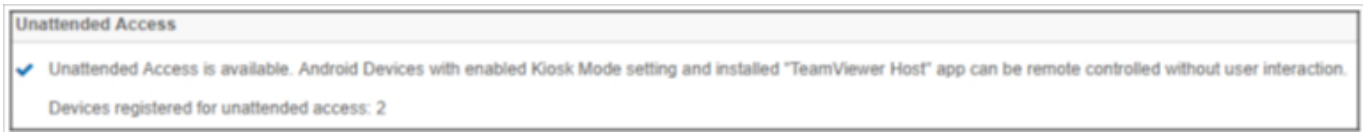


Hvis du bruger iOS, vil du få en besked i AppTec360 MDM Client. Med dette link vil enheden deltage i fjernsessionen. Afhængigt af enhedens notifikationsindstillinger er det muligt, at du ikke modtager en notifikation og skal åbne AppTec360 MDM Client manuelt.

På nogle Android-enheder (f.eks. Samsung) er det nødvendigt at installere en ekstra app som addon. TeamViewer-appen på enheden vil informere dig om det, hvis det er nødvendigt på din enhed.

Uovervåget adgang

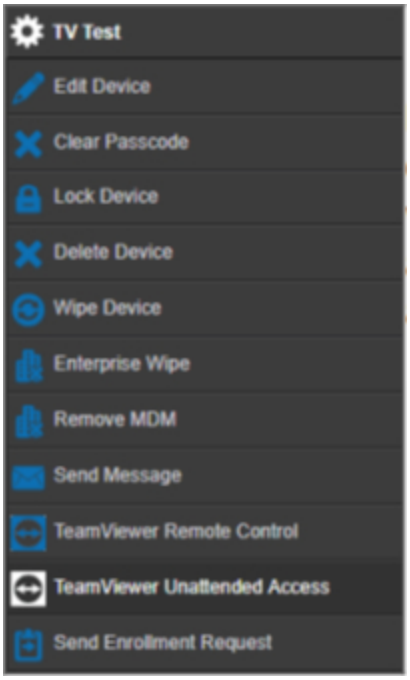
Bemærk: Uovervåget adgang er kun mulig på Android-enheder.



Du kan kun oprette forbindelse til dine enheder uden at acceptere forbindelsen på enheden, hvis din TeamViewer-konto bruger en "Tensor"- eller "Corporate"-licens.

Du kan tjekke dette, når du har linket din konto, i "Generelle indstillinger".

For at bruge den uovervågede adgang skal du installere appen "TeamViewer Host" og aktivere "Aktiver uovervåget adgang" under "Kiosktilstand & Launcher" i din profil. Vær opmærksom på, at dette kun er muligt, hvis du bruger Kiosk Mode.



Nu kan du vælge uovervåget adgang, hvis du vælger din enhed og klikker på hjulet. Dette vil forbinde dig til din enhed uden behov for bekræftelse på selve enheden. Vær opmærksom på, at det kan tage nogle øjeblikke, før du får linket til at få adgang til din enhed.

Splashtop

Hvis du aktiverer Splashtop-indstillingen, ser du Splashtop-konfigurationsindstillingerne i dine profiler.

For at bruge Splashtop skal du indstille Splashtop Streamer (com.splashtop.streamer.csrs) som obligatorisk app i din profil. Bagefter kan du aktivere Splashtop-konfigurationen i din profil under "Fjernbetjening". Aktivering af dette vil konfigurere Splashtop Streamer-appen. Hvis du bruger Splashtop Streamer, men ikke i kombination med MDM, skal du lade dette være slået fra.

I din profil under "Remote Control" skal du også angive en implementeringskode. Gå til https://my.splashtop.com og log ind på din Splashtop-konto. Klik på "Add Computer", og kopier den 12-cifrede implementeringskode fra den resulterende side.

Uden implementeringskoden er fjernbetjening IKKE mulig.

Når du har gjort det, kan du højreklikke på din enhed og starte en fjernsession ved at klikke på "Splashtop Remote Control".

Håndtering af sim-kort

CSV-masseimport

Dette viser en oversigt over dine tildelte sim-kort og alle oplysninger om dem. Dette hjælper dig med at have alle oplysninger, ikke kun om dine enheder, men også om dine sim-kort i ét system.

BEMÆRK: Dette er en manuel styring/dokumentation. Det er ikke muligt at få disse data automatisk fra enhederne på grund af operativsystemernes privatlivs-/sikkerhedsmekanismer.

Du kan også ex- og importere denne liste som CSV.

Transportør og takst

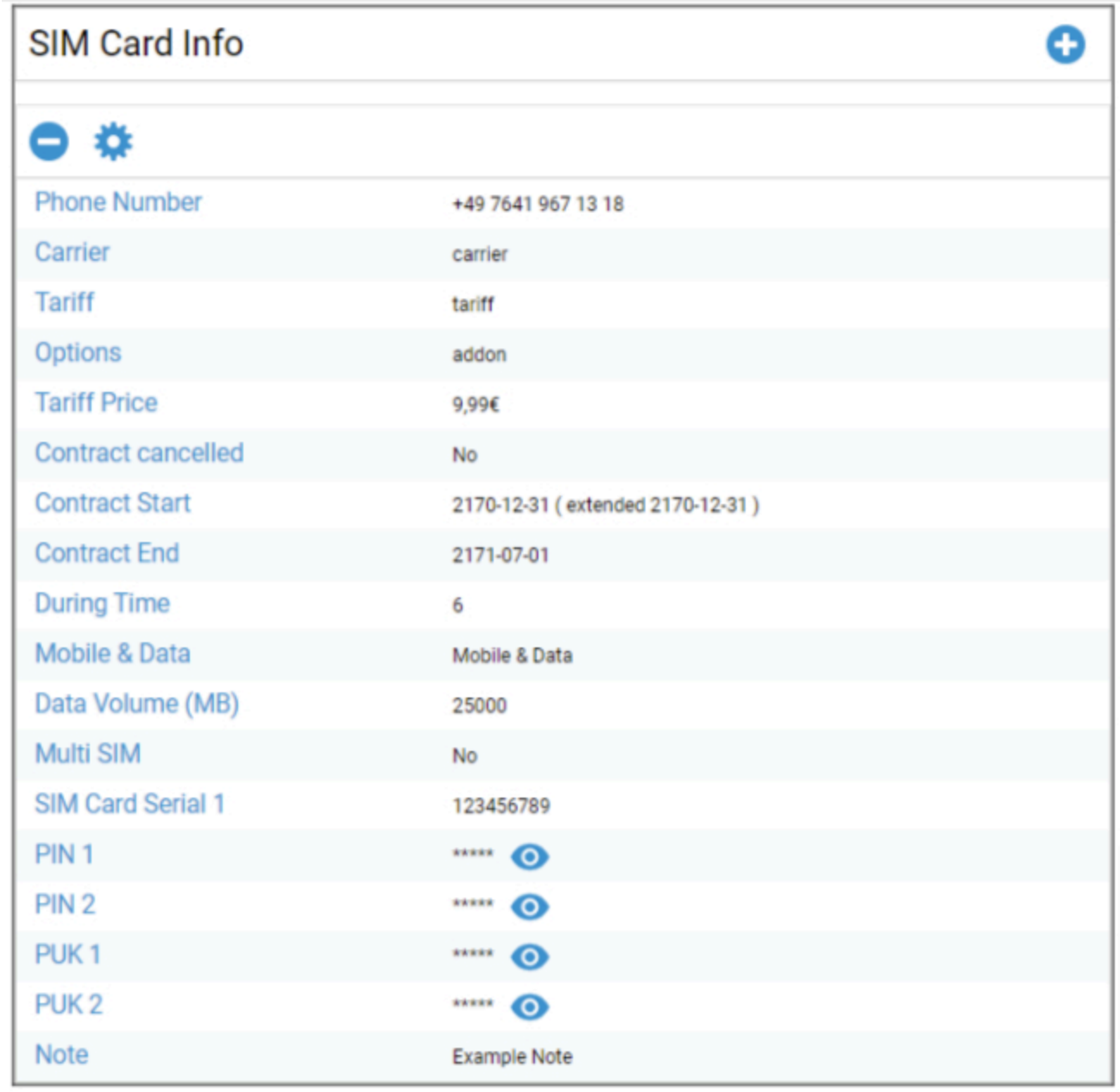
For at tilføje et sim-kort skal du først klikke på knappen for at tilføje en eller flere operatører.

Klik derefter på "+" i "Tariff Information" for at tilføje en tarif til en transportør.

Du kan eventuelt tilføje valgfrie Add-Ons nedenfor, hvis du har noget lignende.

Dette forberedte alt, hvad du behøver for at tilføje et egentligt sim-kort. Sim-kort er i øjeblikket tildelt en bruger. Gå derfor til Mobile Management, vælg en bruger, og gå til "Sim Card Overview".

Her kan du se denne brugers sim-kort. Hvis der er et, kan du redigere eller fjerne det. Brugere kan have flere sim-kort.

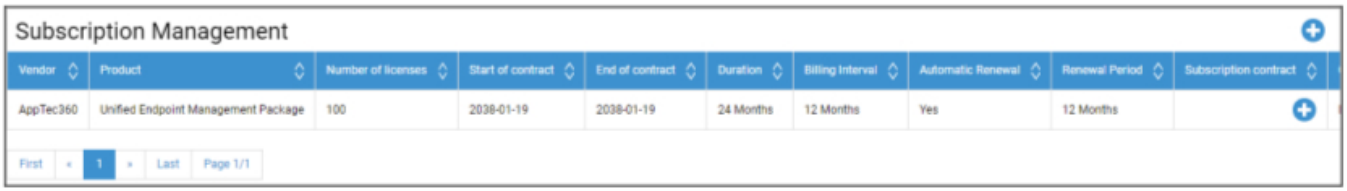


Klik på "+" for at tilføje et sim-kort, og tilføj alle de oplysninger, du har brug for. Disse sim-kort vil også blive vist på listen over alle dine sim-kort i Generelle indstillinger → Sim-kortadministration.

Administration af abonnementer

Administration af abonnementer

Her kan du dokumentere løbende abonnementer, deres detaljer og også gemme forskellige filer, f.eks. underskrevet kontrakt, opsigelsesbrev osv. Du kan også oprette påmindelser, som minder dig om det pr. mail, før abonnementet slutter og måske forlænges automatisk.



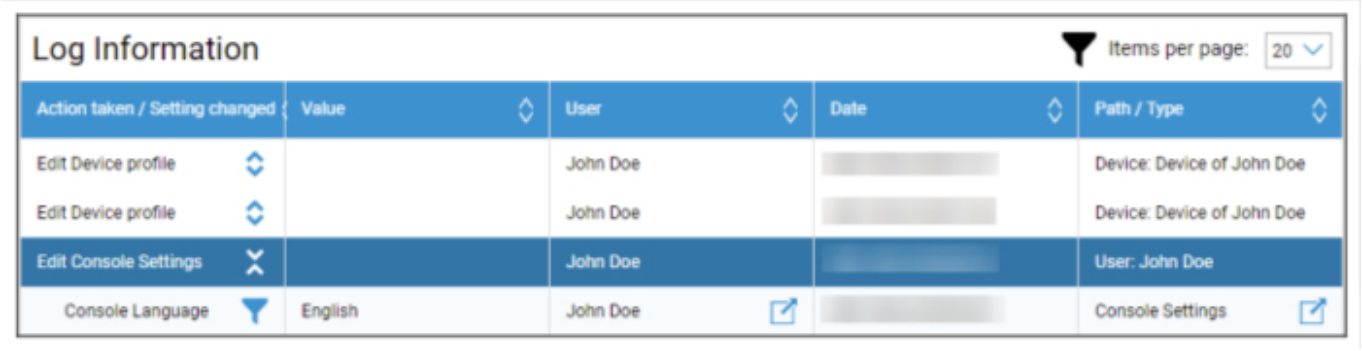
Klik på "+" øverst for at tilføje et abonnement. Du kan tilføje så mange abonnementer, som du vil.

Klik på "+" i de forskellige felter for at uploade filer vedrørende dette abonnement. Du kan teknisk set uploade alle filtyper, men vær opmærksom på, at ikke alle filtyper kan forhåndsvises i browseren.

Generel revisionslog

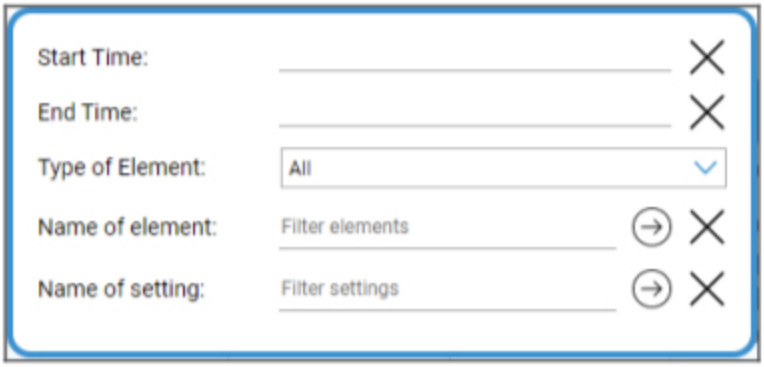
Audit-log

Her har du en generel revisionslog, som viser alle ændringer, der er foretaget. Mens Audit Log i en bruger eller gruppe kun viser ændringer for denne bruger eller gruppe, viser denne ALLE ændringer, der er foretaget overalt i konsollen.



Du kan se, hvad der er blevet ændret, af hvem, hvornår og hvor. I nogle tilfælde kan du også udvide indgangen for at se flere detaljer.

Det er muligt at klikke på brugeren eller på posten i "Path / Type" for at komme til det sted, hvor ændringen er foretaget.



Øverst til højre kan man også definere et filter, som kan hjælpe med at finde bestemte ændringer i et miljø, hvor der sker mange ændringer.

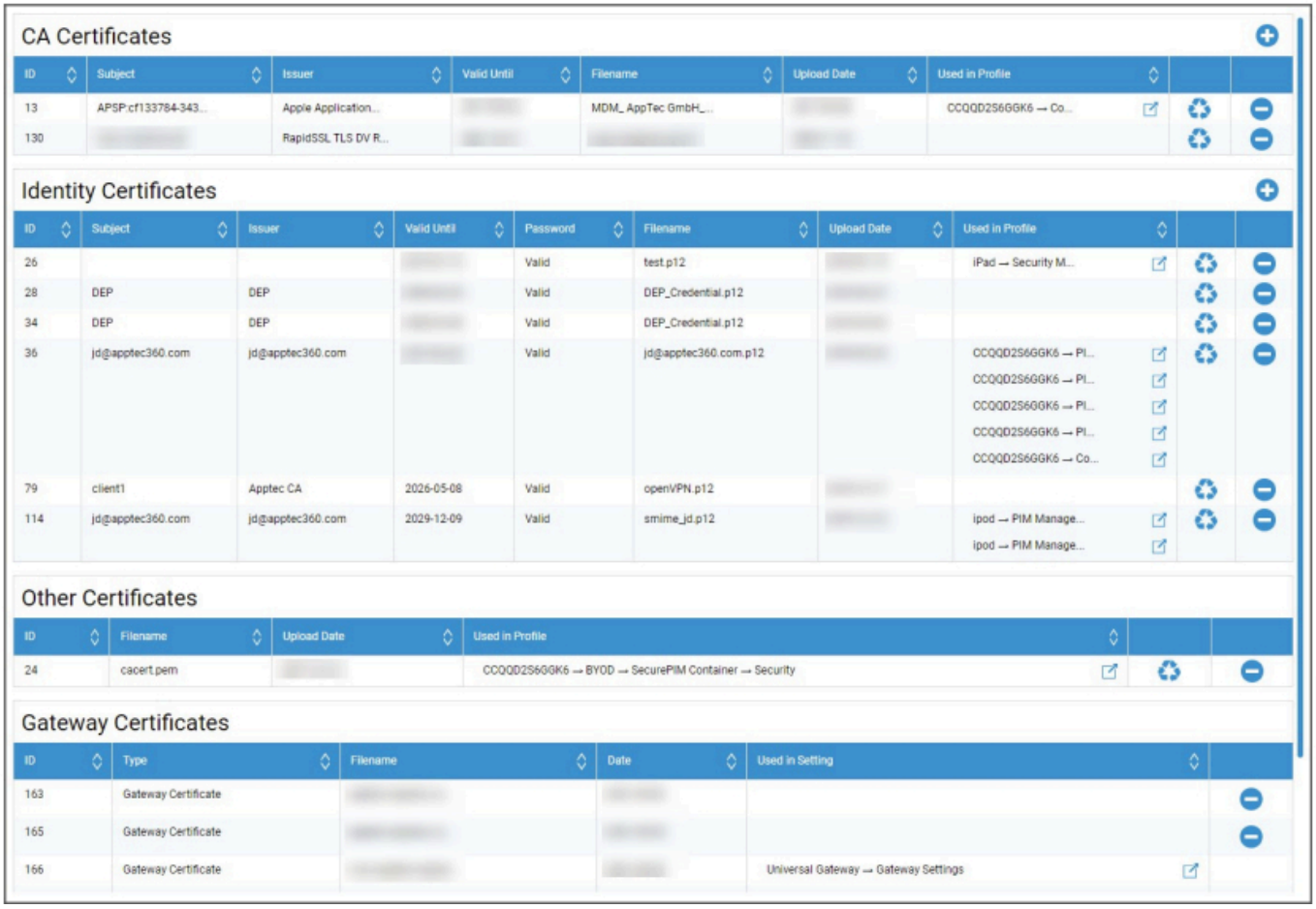
Indstillinger for revisionslog

"Audit Log Retention Period" definerer, hvor længe Audit Logs skal opbevares, før de slettes.

Administration af certifikater

Her får du en oversigt over alle certifikater, der er uploadet og brugt i konsollen. Dette er kun en oversigt. Den faktiske konfiguration af f.eks. wi-fi-certifikater foretages stadig i profilen på den tilsvarende placering.

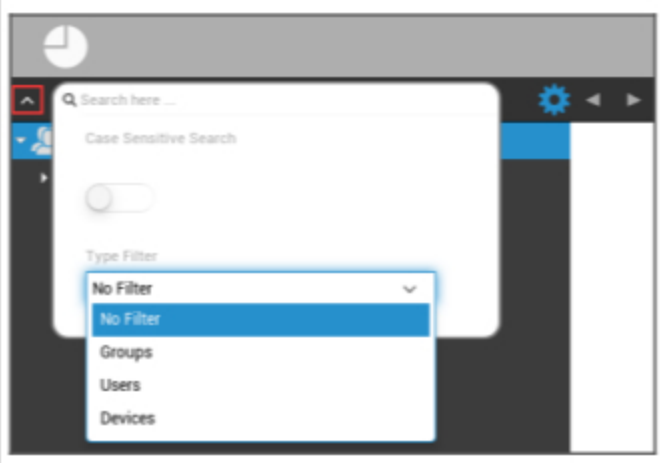
Her kan du også fjerne eller opdatere certifikater, hvilket automatisk vil blive afspejlet i de berørte profiler. Klik på oplysningerne i "Brugt i profil" for at se, præcis hvor et certifikat stadig er tildelt.



Mobil ledelse

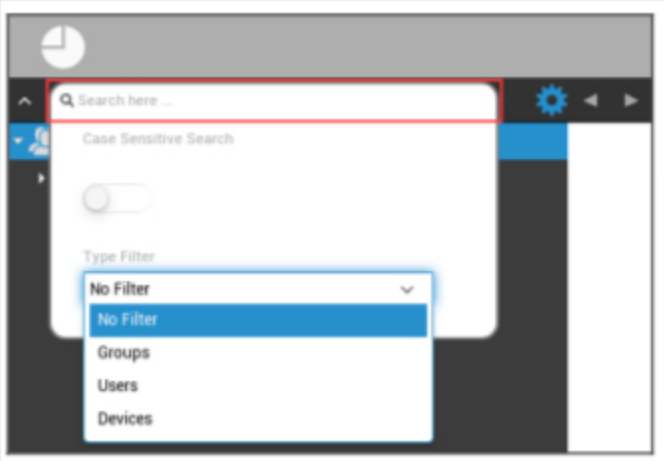
Skærm til mobil administration

Enhedsfilter



Med et klik i øverste venstre hjørne af skærmen kan du finde en række filtre til visning af enheder.

Søg i vindue



I søgevinduet kan du søge på alle enheder og/eller brugere med et bestemt søgeord.

Ekstraudstyr gear

Når du har klikket på det pågældende symbol, vises en liste over de muligheder, du har til rådighed.

Disse ændres for hvert aktuelt vindue og forklares i de respektive kapitler.

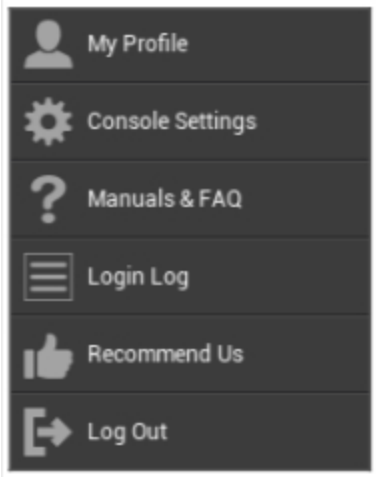
Navigationspile

Med et klik på pilen til venstre kommer du til den forrige side.

Bagefter kommer du med et klik på højre pil tilbage til den side, du lige har forladt.

Administration kontoindstillinger

Hvis du klikker på e-mailadressen som vist ovenfor, får du følgende menu frem:



Min profil	Rediger administratorens kontooplysninger
Konsolindstillinger	Konfigurer konsolindstillinger for Admins-kontoen
Manualer og ofte stillede spørgsmål	Se siden "Manualer og ofte stillede spørgsmål" i "Generelle indstillinger"
Log ind	Få adgang til "login-loggen"
Anbefal os	Se siden "Anbefal os" i "Generelle indstillinger"
Log ud	Log ud af MDM-konsollen

Brugeroplysninger

Her kan du redigere kontooplysningerne for den aktuelt indloggede administrator.

Brugernavn	Brugernavn og/eller e-mailadresse på kontoen
Navn	Administratorernes fornavn
Efternavn	Administratorernes efternavn
Login-navn	Administratorernes login-navn
E-mail-adresse	Administratorernes e-mailadresse
Alternativ e-mail-adresse	Administratorernes alternative e-mailadresse
Billede	Profilbillede
Telefonnummer	Administratorernes telefonnummer
Mobilnummer	Administratorernes mobilnummer
Telefonudvidelse	Telefonudvidelse
Beliggenhed	Beliggenhed
Position	Position i virksomheden
Brugergruppe	Vælg, hvilken brugergruppe du vil tildele administratorkontoen til
Kommentar	Skriv en kommentar
Indtast ny adgangskode	Indtast adgangskoden for en ændring af adgangskoden
Gentag ny adgangskode	Gentag den nye adgangskode for at bekræfte

Bemærk, at administrationsadgangen også kan arkiveres som en lokal brugerkonto i hierarkistrukturen. Uden oprettelse af en ekstra administrator bør denne ikke slettes!

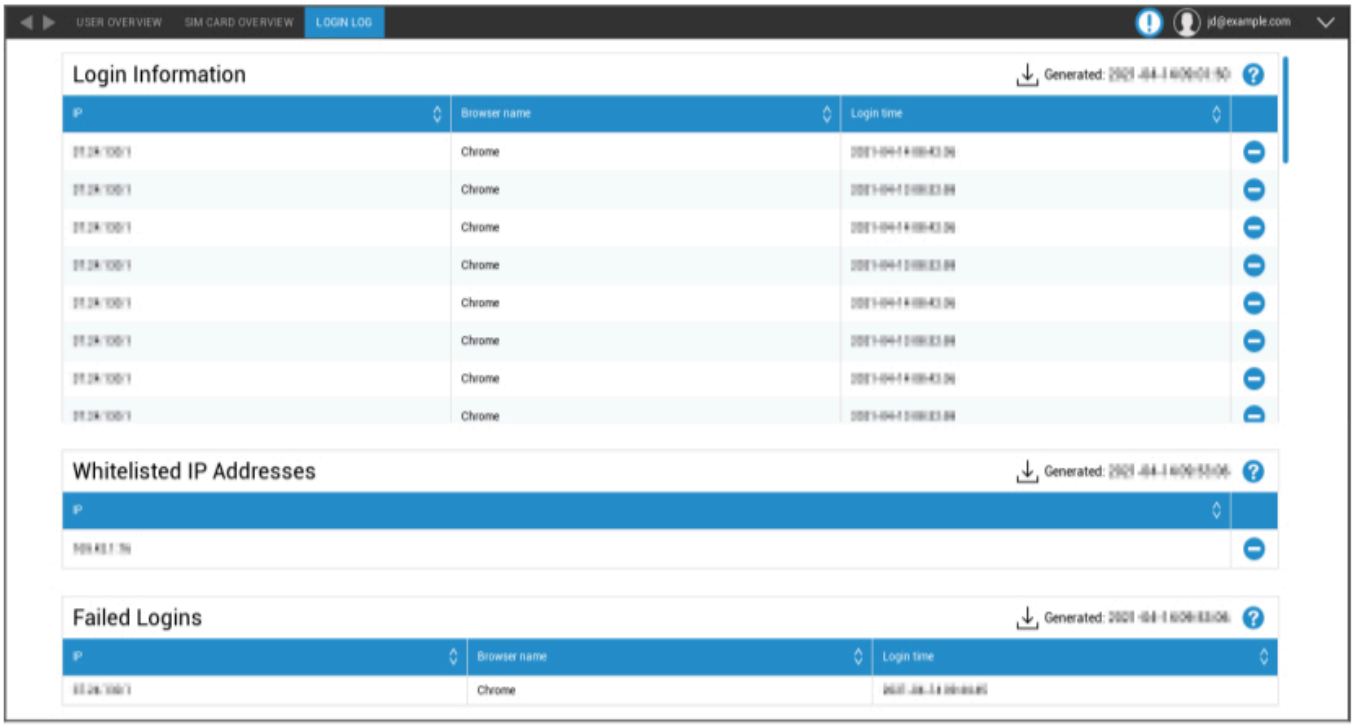
Konsolindstillinger

Her kan du konfigurere følgende konsolindstillinger for Admins-kontoen:

Indstillinger for visning af katalogbruger	Definer, hvordan brugere skal mærkes i træet
Indstillinger for visning af katalogenheder	Definer, hvordan enheder skal mærkes i træet
Sessionens timeout	Hvis brugeren ikke gør noget inden for den angivne tid, bliver brugeren logget ud. Standardværdien er 60 minutter. Log ud og log på igen, når du har ændret denne indstilling.
Tidszone	Vælg den tidszone, der skal bruges
Tidsformat	Vælg, hvordan tidsstempler skal vises
Konsolsprog	Vælg det sprog, som konsollen skal vises på. Engelsk og tysk er tilgængelige.
Hovedfarve	Du kan indstille en farve, som skal bruges som basis for konsollens farveskema. Du kan enten bruge farvevælgeren eller indtaste en farve i HTML HEX-notation. RGB-formatorer som 'pink', 'gul' fungerer også.
Gem kommandoen	Tastekombinationen til at udløse en lagring uden at trykke på "Gem"-knappen.
Brug to-faktor-autentificering	Aktivér brugen af to-faktor-autentificering, når du logger ind. Du modtager en e-mail ved login med en kode, som du skal indtaste for at logge ind.
Timeout for to-faktor-autentificering	Indstil en tidsperiode, hvor du ikke vil blive bedt om en to-faktor-godkendelse efter en allerede vellykket godkendelse.
Send bekræftelseskode via	Bekræftelseskoden sendes til de valgte indstillinger. Enhedsmeddelelsen vil blive vist i AppTec360 MDM-appen på alle Android- og iOS-enheder, der tilhører dig.
Send login-meddelelse efter login	Hvis den er aktiveret, sendes der en e-mail for hvert login fra en ip-adresse, der ikke er på hvidlisten. E-mailen indeholder oplysninger om login (f.eks. IP, browser).

Log ind

Her kan du se oplysninger om logins for den aktuelt indloggede administratorkonto.



Oplysninger om login	En liste, der indeholder logins for den aktuelt indloggede administratorkonto, som blev registreret af konsollen. Denne liste viser alle dine vellykkede logins i de sidste 30 dage.
IP-adresser på hvidlisten	Dette er listen over alle dine hvidlistede IP-adresser. Hvis du logger ind fra en IP, der er angivet her, får du ikke login-meddelelsen. Du kan tilføje en IP-adresse til denne liste ved at klikke på knappen ved siden af en post i listen "Loginoplysninger" ovenfor. Du kan fjerne en IP-adresse fra denne liste ved at klikke på knappen ved siden af en post på denne liste eller på listen "Loginoplysninger" ovenfor.
Mislykkede logins	Dette er en liste over alle mislykkede loginforsøg i de sidste 30 dage. Hvis du ikke har indtastet den korrekte adgangskode mindst 3 gange på 20 minutter, vises der en post på denne liste. Du vil også blive informeret om mislykkede loginforsøg via e-mail.

Virksomhedsadministration (Root-Node) i Mobile Management

Når du er nået til Root-Node (første gruppe), kan du foretage en række indstillinger for din virksomhed med hensyn til Mobile Management.

Opret en undergruppe	Opret en undergruppe
Omdøb rodknudepunktet	Omdøbning af Root-Node (f.eks. dit firmanavn)
Masseindskrivning	Tilmeld flere enheder/brugere på samme tid
Masseopgave	Tildel en profil til de respektive grupper, med ét blik
Hurtig app-administration	Send (af)installationsanmodninger for en applikation til de respektive grupper af enheder
CSV-brugerimport	Importer brugere fra CSV til den respektive gruppe

Opret en undergruppe

Med "Opret en undergruppe" kan du oprette en ekstra undergruppe.

Du kan bestemme, hvilken gruppe undergruppen skal høre under.

(Som standard oprettes en ny gruppe, der tildeles som en undergruppe i rodknuden)

Omdøb rodknudepunktet

Her kan du omdøbe dit rodnavn. Det er almindeligt, at firmanavnet bruges i dette tilfælde.

Masseindskrivning

Med "Mass Enrollment" kan du tilmelde flere enheder og brugere.

Du kan vælge direkte, hvordan brugeren skal modtage tilmeldingen (e-mail; alternativ e-mail; SMS).

Afhængigt af hvilken enhed brugeren skal modtage (iOS, Android, Windows Phone), kan du markere det direkte her.

Om det er en smartphone eller en tablet, kan også konfigureres her, hvilket du skal vælge korrekt med et flueben.

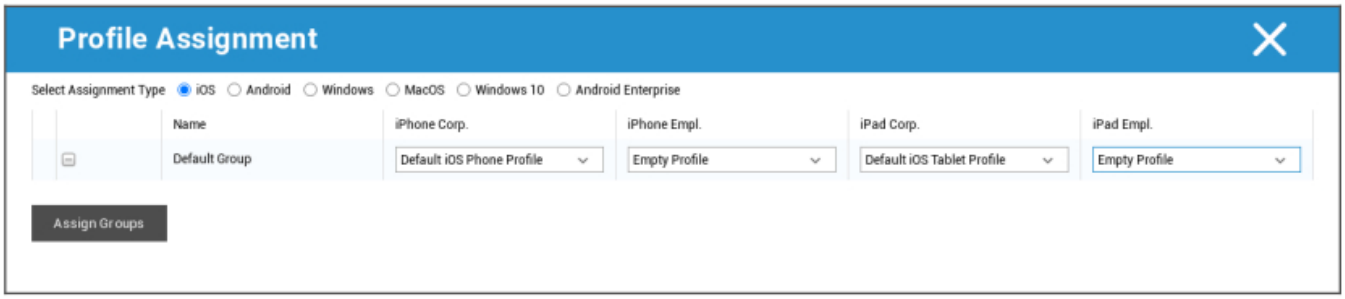
Som et sidste trin kan du afgøre, om den pågældende enhed er en virksomhedsenhed eller en privat enhed (BYOD).

Med "Eksporter som CSV" kan du eksportere oplysningerne som en CSV-datafil. Til gengæld kan du også importere CSV-datafilen med "Import CSV", og filen skal se ud som i eksemplet nedenfor:

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

Masseopgave

Under Mass Assignment kan du tildele en profil til alle grupper, dette er opdelt i iOS - Android - Windows - MacOS - Windows 10 - Android Enterprise.

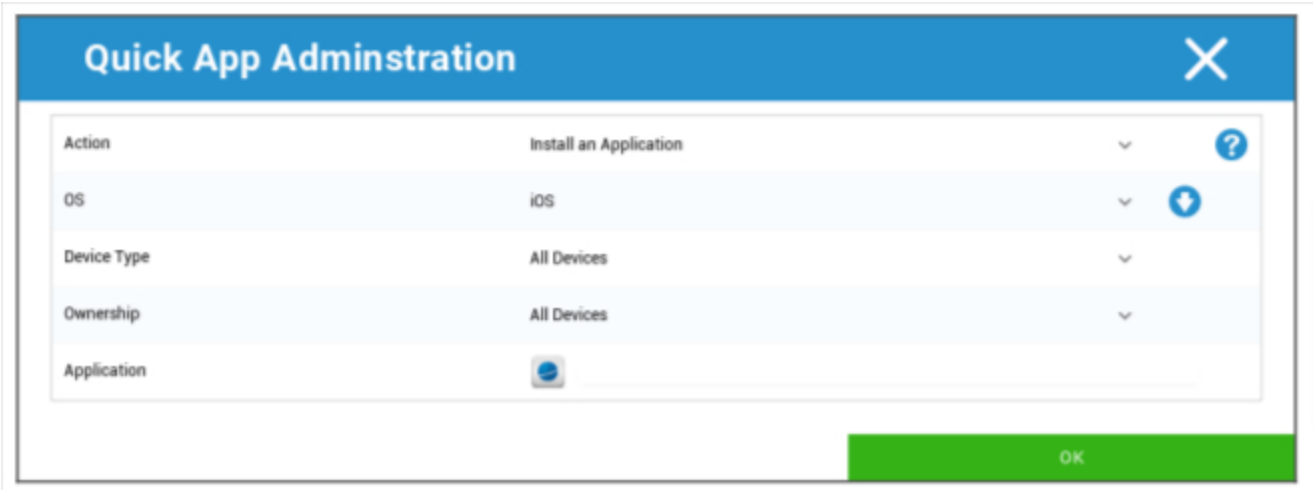


Windows - MacOS - Windows 10 - Android Enterprise

Hurtig app-administration

Under Quick App Administration kan du sende anmodninger om installation eller afinstallation af en bestemt applikation til et operativsystem efter eget valg.

Du kan også definere, om anmodningen skal sendes til alle enhedstyper i det valgte operativsystem eller kun til en bestemt enhedstype.



CSV-brugerimport

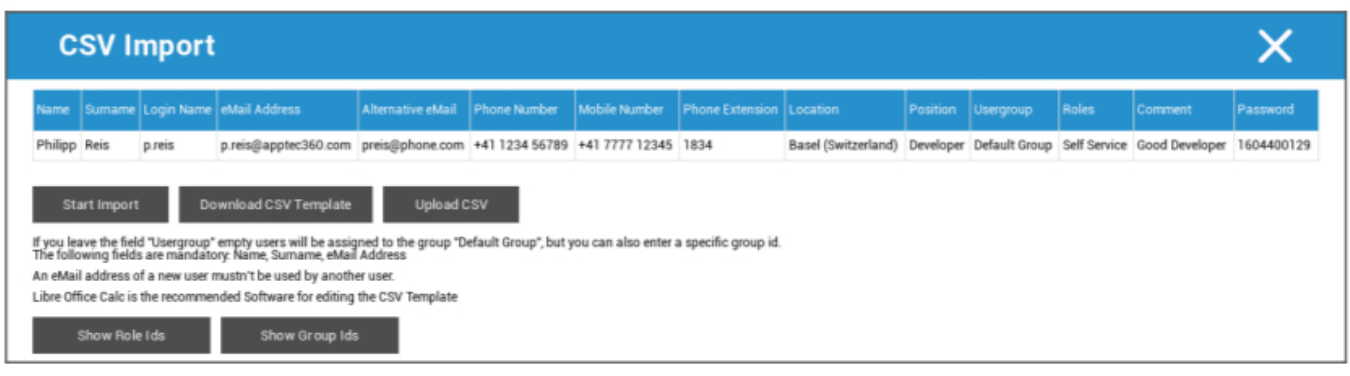
Importer brugere fra CSV til den respektive gruppe.

Med "Download CSV Template" kan du eksportere en CSV-skabelonfil, som kan udfyldes (eller den kan bruges som reference).

Du kan også bruge indstillingerne "Vis rolle-id'er" og "Vis gruppe-id'er" som reference til at oprette din egen CSV-fil.

CSV-filen kan uploades til MDM med "Upload CSV".

Som sidste trin kan du starte importen ved at klikke på "Start import".



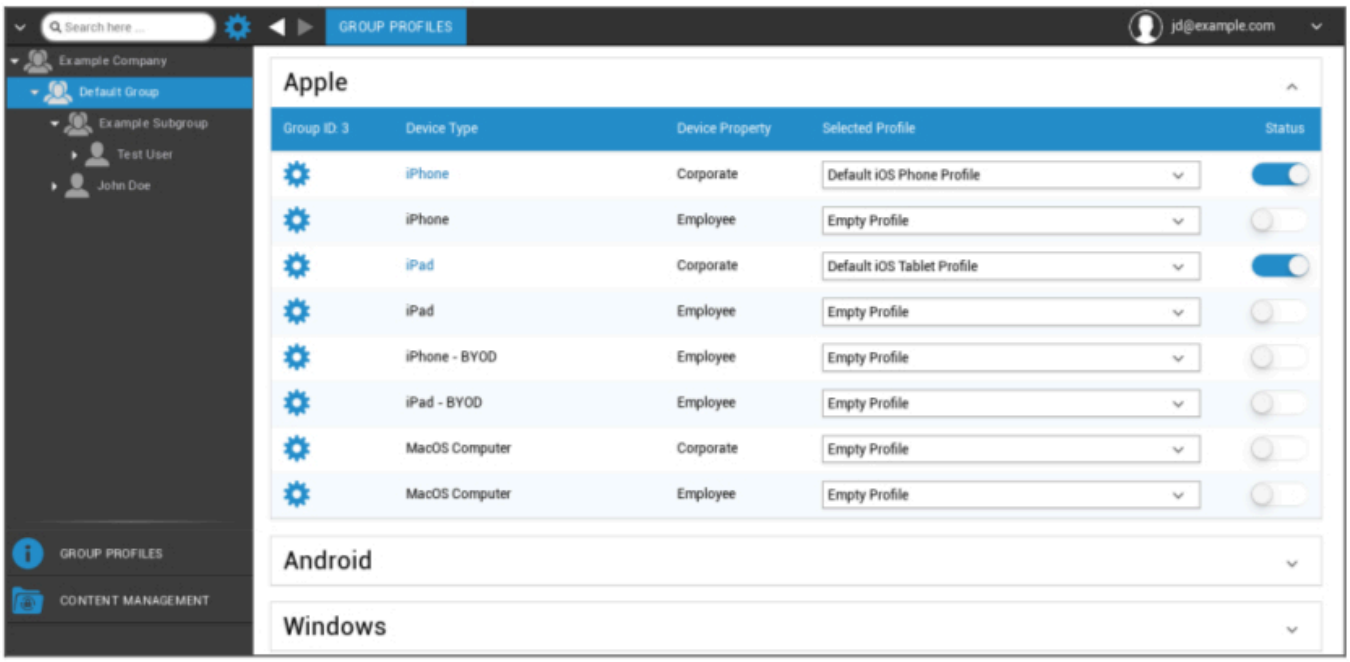
Gruppestyring i Mobile Management

Et klik på oversigten viser de forskellige konfigurationsprofiler for de respektive platforme.

En profil indeholder alle indstillingsmuligheder, der kan etableres med AppTec360 på forhånd på slutbrugerens enhed. På hver platform kan du oprette profiler for virksomhedsenheder (Corporate) eller Bring-Your-Own-Device-enheder (Employee).

For at kunne differentiere konfigurationer for enhedsgrupper, f.eks. baseret på placering eller funktion, anbefales det at oprette flere undergrupper.

Vær opmærksom på profilstyring i Mobile Management



Med gearmenuen kan du foretage en række indstillinger for den respektive (under)gruppe.

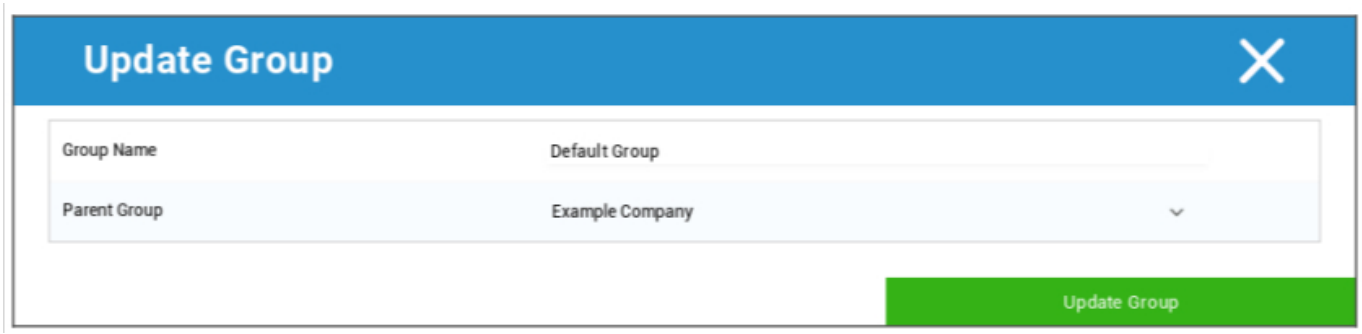
Opret en undergruppe	Opret undergruppe for den respektive (under)gruppe
Rediger den valgte gruppe	Rediger den valgte gruppe
Slet den valgte gruppe	Slet den valgte gruppe
Masseindskrivning	Tilmeld mange enheder/brugere på én gang til den valgte profil
Masseopgave	Tildel profiler til den gruppe, der er valgt i øjeblikket
Opret en undergruppe	Opret undergruppe for den respektive (under)gruppe
Opret en bruger	Opret en bruger til den respektive (under)gruppe

Opret en undergruppe

Med "Opret en undergruppe" kan du oprette en ekstra undergruppe.

Du kan bestemme, hvilken gruppe undergruppen skal tilknyttes (som standard tilknyttes undergruppen den gruppe, der er valgt i øjeblikket).

Rediger den valgte gruppe



Her kan du redigere profilen - her er følgende indstillinger mulige:

- Gruppens navn kan ændres
- Forældregruppen kan ændres

Slet den valgte gruppe

Under "Slet den valgte gruppe" vises alle de brugere og enheder, der er i den pågældende gruppe. Her har du mulighed for at slette dem.

For en bruger kan du udføre følgende slettekommandoer:

Slet bruger	Brugeren er slettet
Flyt bruger til gruppe:	Du kan flytte brugeren til en anden gruppe (følgende kolonne, f.eks. "Admins")

For en enhed kan du udføre følgende slettekommandoer:

Tør og slet	Tør og slet enheden
Slet fra systemet	Fjern kun enheden fra AppTec

Reference: Masseindskrivning

Reference: Masseopgave

Opret en bruger

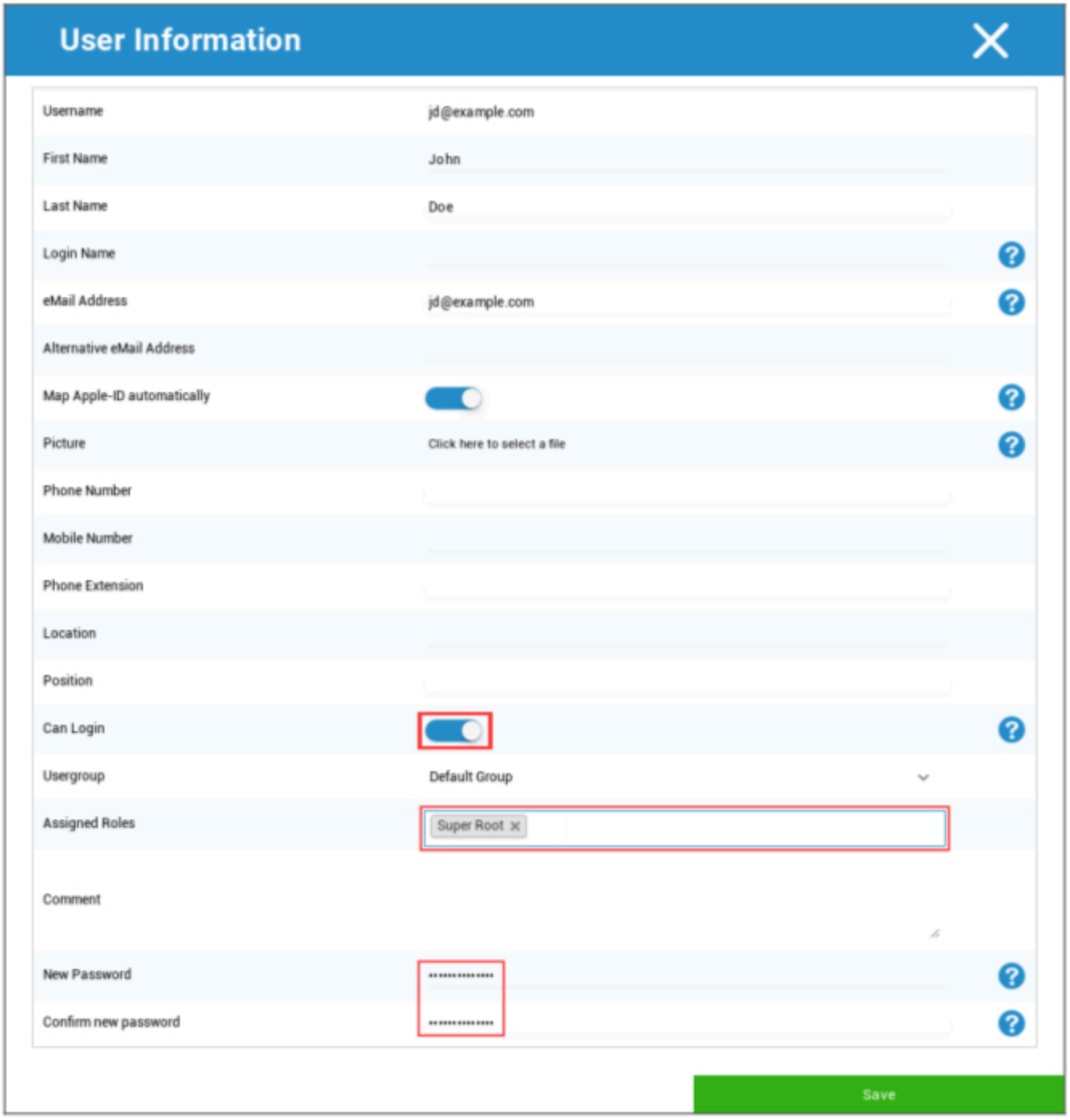
Med "Create a User" kan du tilføje en ny bruger.

Opret en ny administrator-bruger

Du kan indstille en bruger som admin-bruger. Det vil give ham tilladelse til at logge ind på konsollen og også ændre brugere/grupper/enheder.

Opret en normal bruger, eller brug en eksisterende bruger. Vælg den bruger, du vil give administratorrettigheder, klik på hjulet, og vælg "Rediger bruger":

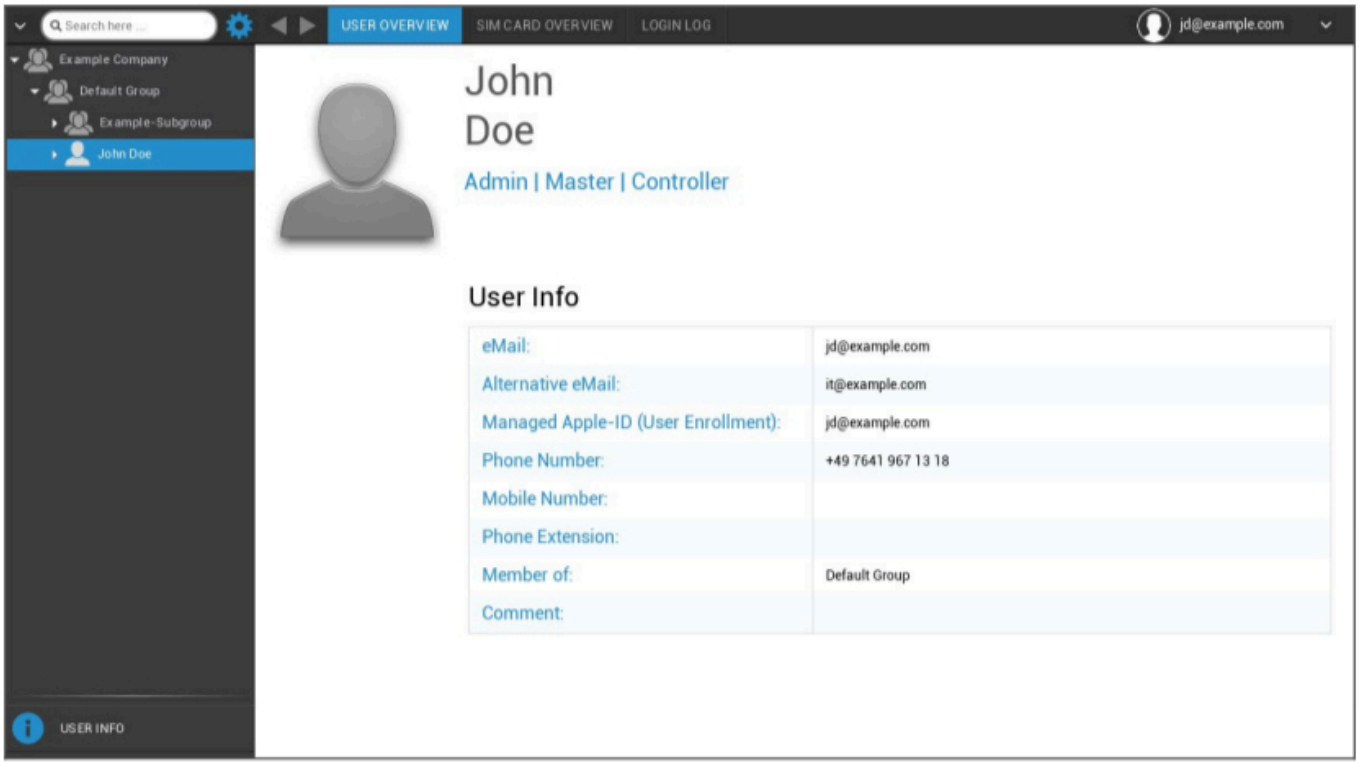
Aktivér kontakten til "Kan logge ind", tildel brugeren rollen "Super-Root", og angiv en adgangskode.



Gem dette, og brugeren kan nu logge ind med brugernavn og adgangskode.

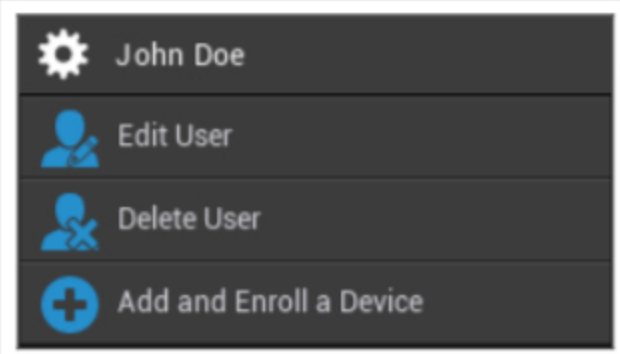
Brugerstyring i Mobile Management

Når du vælger en bestemt bruger, ser du følgende oversigt:



Du får en oversigt over alle de oplysninger, du tidligere har indtastet i "Opret en bruger".

Med det udstyr, der er installeret øverst, kan du udføre følgende konfigurationer:



Brugernavn	Brugernavn på den valgte bruger
Rediger bruger	Rediger brugeroplysninger
Slet bruger	Slet bruger • Slet fra system = Enheden vil blive fjernet fra AppTec

	• Wipe & Delete = Enheden gendannes til fabriksindstillingerne og fjernes fra AppTec
Tilføj og tilmeld en enhed	Tilmeld en enhed til den valgte bruger

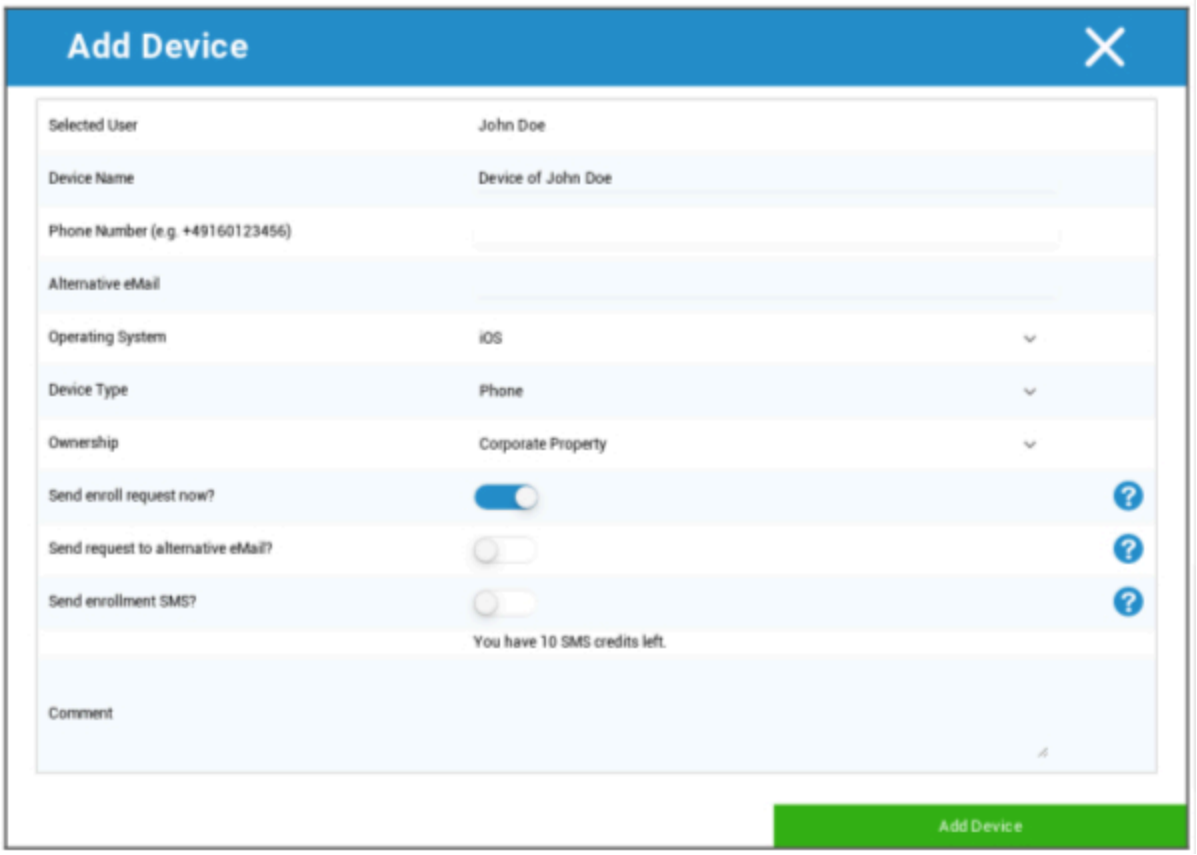
Bemærk, at administrationsadgangen også kan arkiveres som en lokal brugerkonto i hierarkistrukturen. Uden oprettelse af en ekstra administrator bør denne ikke slettes!

Tilføj og tilmeld en enhed

Her kan du vælge en enhed til den valgte brug.

Alternativt kan du tilmelde enheder til en gruppe direkte. Det gør du ved at klikke på gruppen, klikke på hjulet og vælge "Tilføj og tilmeld en enhed".

Du bør se følgende oversigt:



Afhængigt af hvilken type enhed du vil tilmelde, skal du udføre følgende konfigurationer:

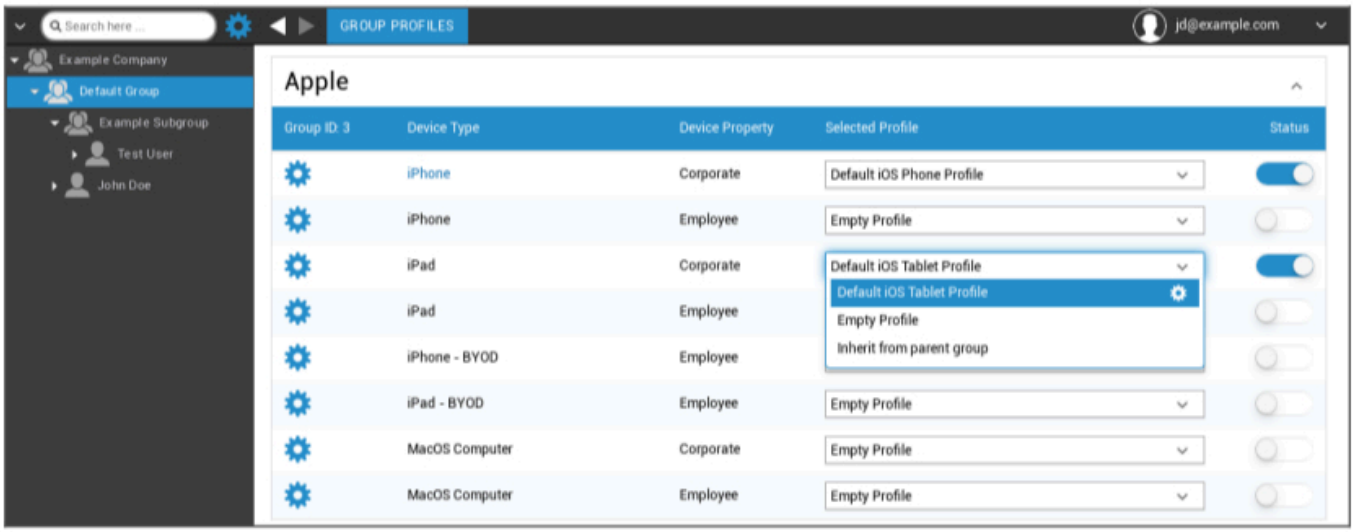
Udvalgt bruger	Valgt bruger (udfyldes automatisk)
Enhedens navn	Udfyldes automatisk (enhed til "brugerens navn") - kan dog ændres
Telefonnummer	Telefonnummer, udfyldes automatisk (så længe det er oplyst af brugeren) - her kan det dog tilføjes eller ændres.
Alternativ e-mail	Alternativ e-mail, udfyldes automatisk (så længe den er angivet af brugeren) - her kan den dog tilføjes eller ændres
Enhedens ejer	Virksomhedsejendom = virksomhedsenhed Medarbejderens ejendom = BYOD-enhed
Vælg betjeningssystem	Her kan du vælge mellem følgende operativsystemer: • iOS • iOS BYOD (brugertilmelding) • MacOS • Android Enterprise • Android • Windows Mobile • Windows 10
Send anmodning om indskrivning?	E-mailen sendes straks til hoved-e-mailadressen, og brugeren bliver bedt om at tilslutte sin enhed.
Send anmodning til alternativ e-mail?	Send e-mailen yderligere eller udelukkende (hvis "Send tilmeldingsanmodning?" er deaktiveret) til den alternative e-mailadresse (e-mailen er forskellig fra den "normale" e-mail med tilmeldingsanmodning).
Sende tilmeldings-SMS?	Send en tilmeldingsanmodning via SMS (telefonnummeret skal indtastes)

Når tilmeldingsanmodningen er sendt, vil enheden blive vist (markeret med rødt) med det samme.

Så snart enheden er blevet tilsluttet, vil den kort efter blive markeret med grøn og er dermed klar til at modtage begrænsninger, apps osv.

Profilstyring i Mobile Management

Når du har klikket på en gruppe, får du en oversigt over alle de enhedsplatforme, der skal konfigureres, og de respektive tildelte profiler.



	Udfør konfigurationen for den valgte profil
Enhedstype	Enhedstype og/eller -model
Enhedens egenskaber	Enhedens ejer (virksomhed = virksomhedens ejendom, medarbejder = privat medarbejders enhed)
Udvalgt profil	Valgt profil (tandhjulet åbner profilens konfigurationsdialog)
Status	On/Off (profilen er aktiveret/deaktiveret)

Når du vælger gearet, får du følgende muligheder:

Opret en profil

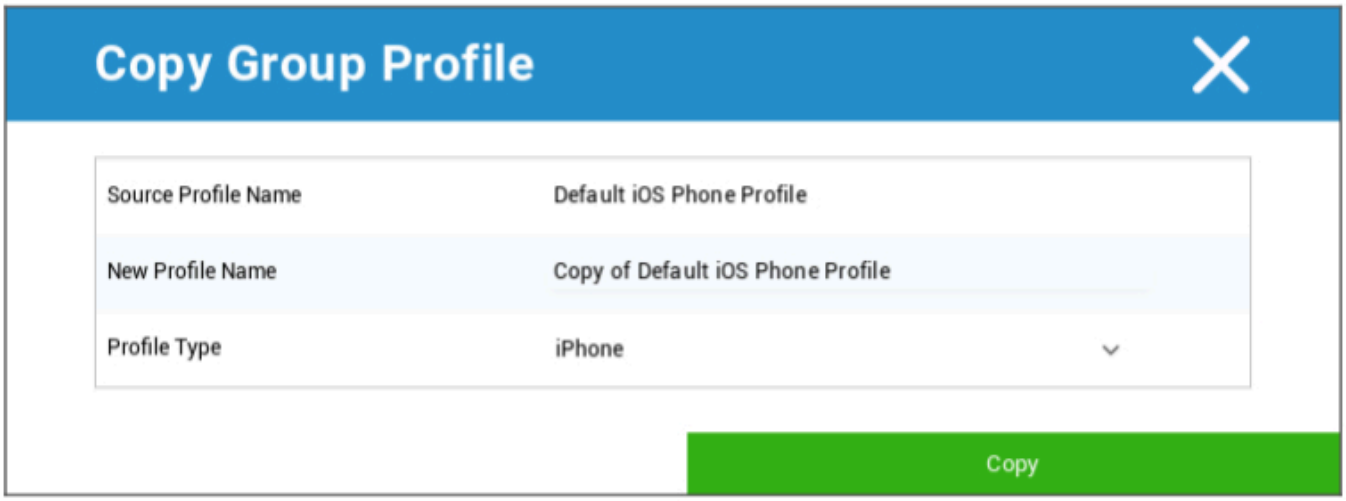
Du kan oprette og konfigurere en ny profil for hver indgang og/eller platform. Når du har klikket på dette underpunkt, oprettes profilen med det samme, og du kan begynde at konfigurere iOS, Android og Windows Phone med det samme.

Rediger profil

Når du har klikket på "Rediger profil", kommer du til konfigurationsdisplayet for den pågældende profil, hvor du kan indstille konfigurationerne.

Kopier profil

Ved hjælp af funktionen "Copy Profile" kan du kopiere opsætninger/konfigurationer fra en allerede eksisterende profil og tilføje dem til en ny profil.

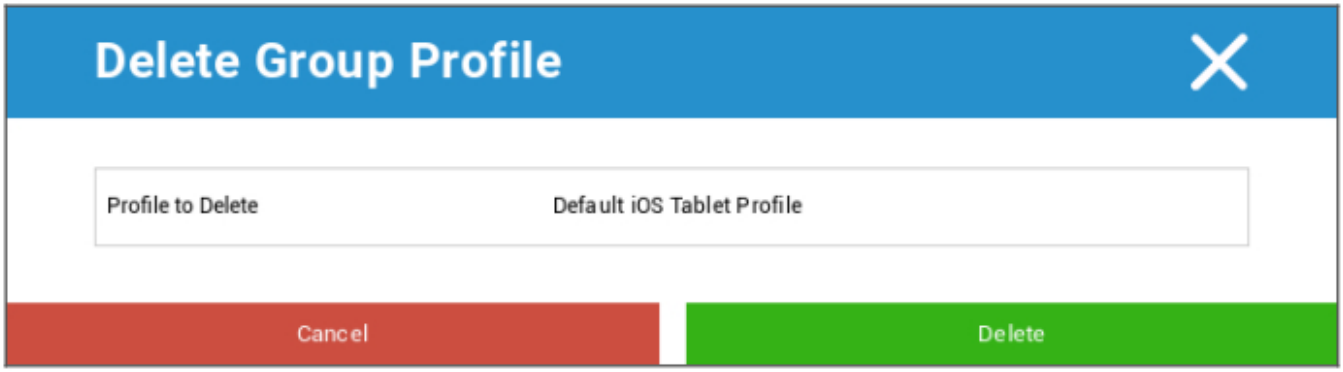


Navn på kildeprofil	Navnet på den profil, der skal kopieres
Nyt profilnavn	Navnet på den nye profil
Profiltype	Profiltype (telefon/tablet)

Når du klikker på "Kopier", bliver profilen oprettet og kan nu tildeles gruppen.

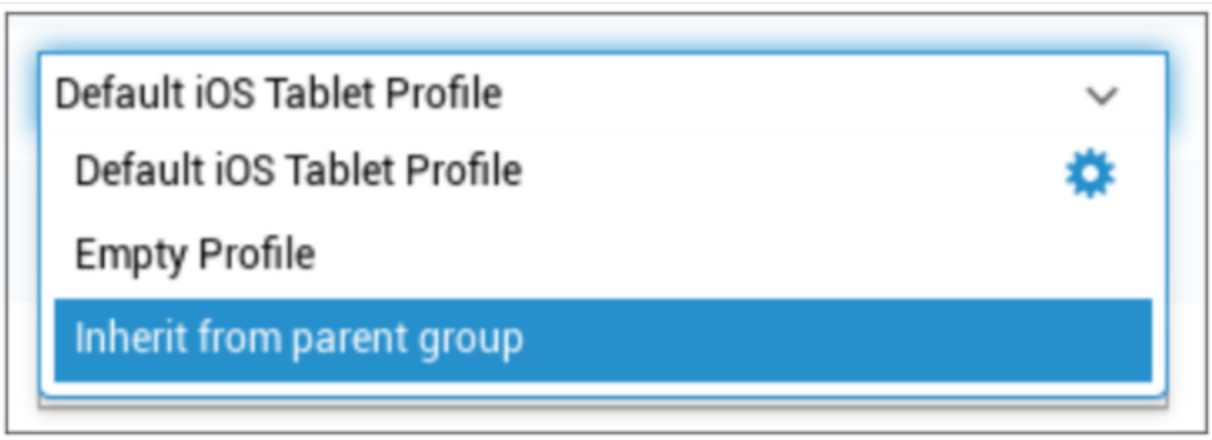
Slet profil

Her kan du slette en profil permanent. Bemærk, at under sletningsprocessen og den følgende "Tildel nu"-proces for profilen forsvinder konfigurationen på de respektive enheder i en berørt gruppe og kan ikke gendannes!


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

Nedarvning af profiler

Under valget af profiler er muligheden "Arv fra forældregruppe" tilgængelig.



Når profilen er aktiveret, vil den overordnede gruppes profil blive brugt til den valgte enhed (og den respektive enhedstype). Bemærk også, at ændringer i denne profil muligvis kan påvirke adskillige grupper.

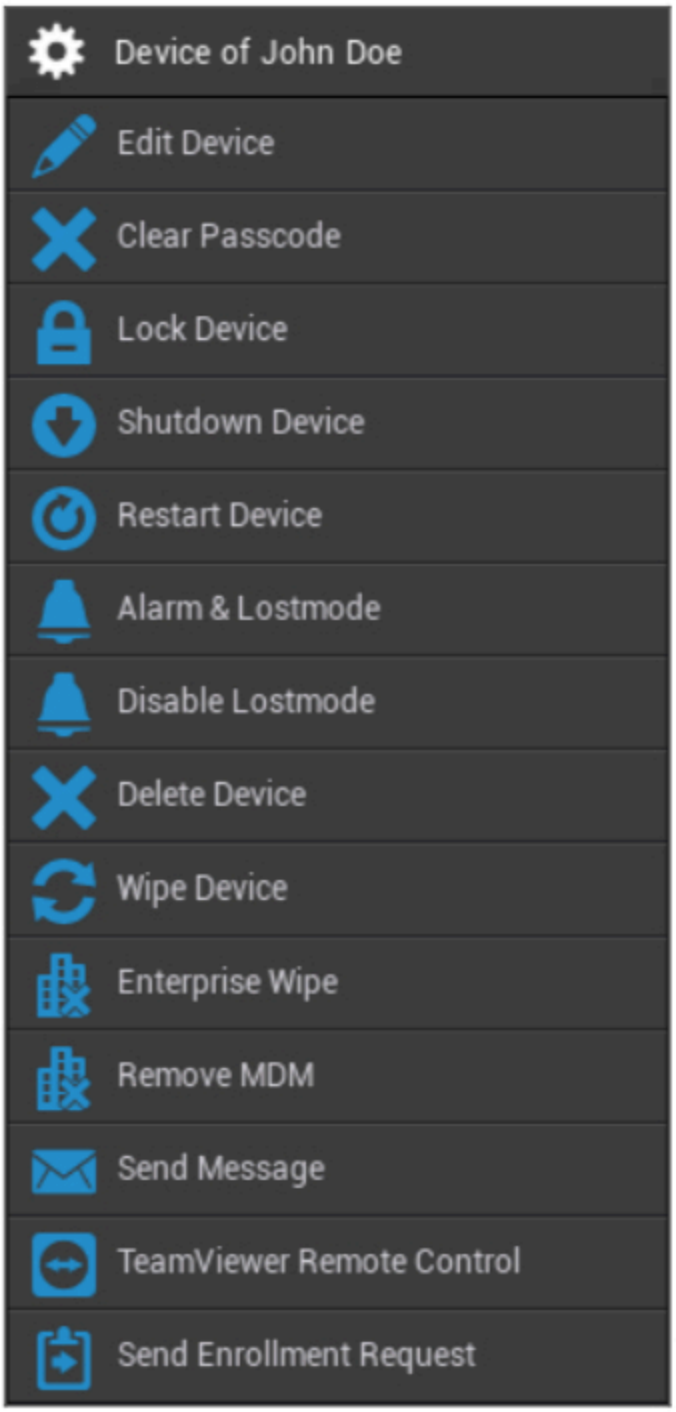
Denne konfiguration indstilles som standardværdi, når en ny undergruppe oprettes.

Konfigurationen "Empty Profile" er også tilgængelig, hvilket svarer til en tom profil, hvilket betyder, at der i sidste ende ikke vil blive udført nye konfigurationer på slutbrugerens enhed.

Enhedshåndtering i Mobile Management

Når du vælger en enhed, kan du udføre en række opgaver via "gearet". Disse er forskellige afhængigt af OS-platformene (iOS, Android Enterprise, Android, Windows Mobile, Windows 10).

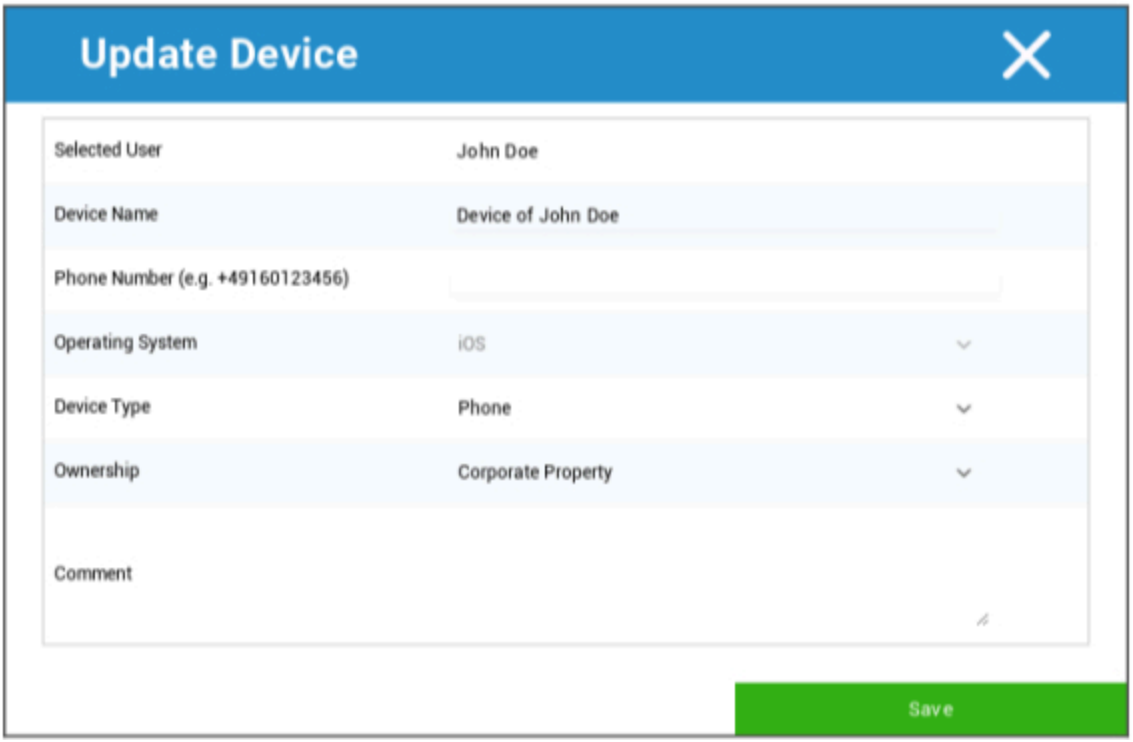
IOS



Rediger enhed	Rediger enhed
Slet adgangskode	Enhedens adgangskode slettes
Lås enhed	Lås enhed (låseskærm)
Nedlukningsenhed	Nedlukningsenhed

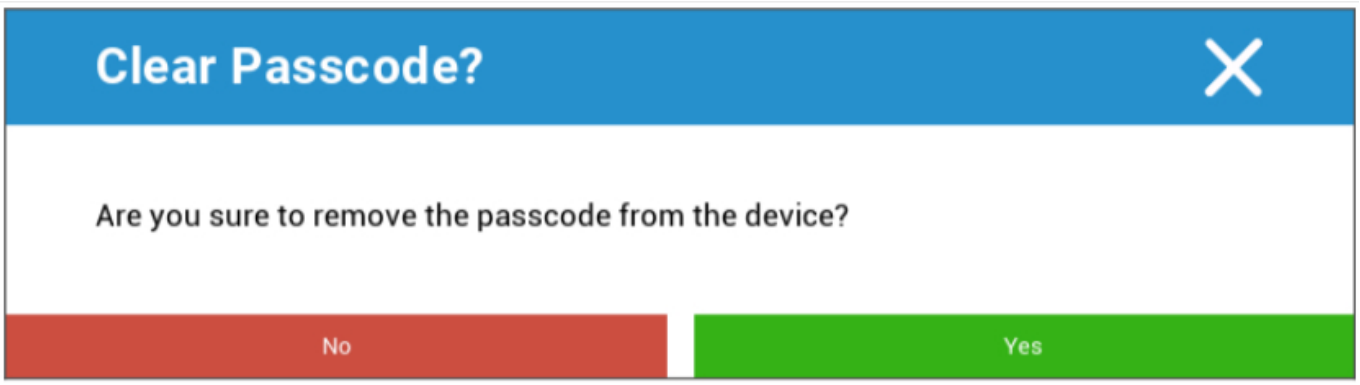
Genstart enheden	Genstart enheden
Alarm og tabt tilstand	Start alarm og tabt tilstand
Deaktiver Lostmode	Deaktiver Lostmode
Slet enhed	Fjern enheden fra AppTec
Tør enhed af	Gendan enheden til fabriksindstillingerne
Enterprise Wipe	De oplysninger, apps og profiler, der leveres af AppTec360, slettes (enheden adskilles fra MDM).
Fjern MDM	
Send besked	Send push-meddelelser til enheden Beskeden vil blive vist i AppTec360-appen (fanen Besked).
TeamViewer-fjernbetjening	Start en fjernbetjeningssession med TeamViewer
Send tilmeldingsanmodning	Send (gentagen) tilmeldingsanmodning

Rediger enhed



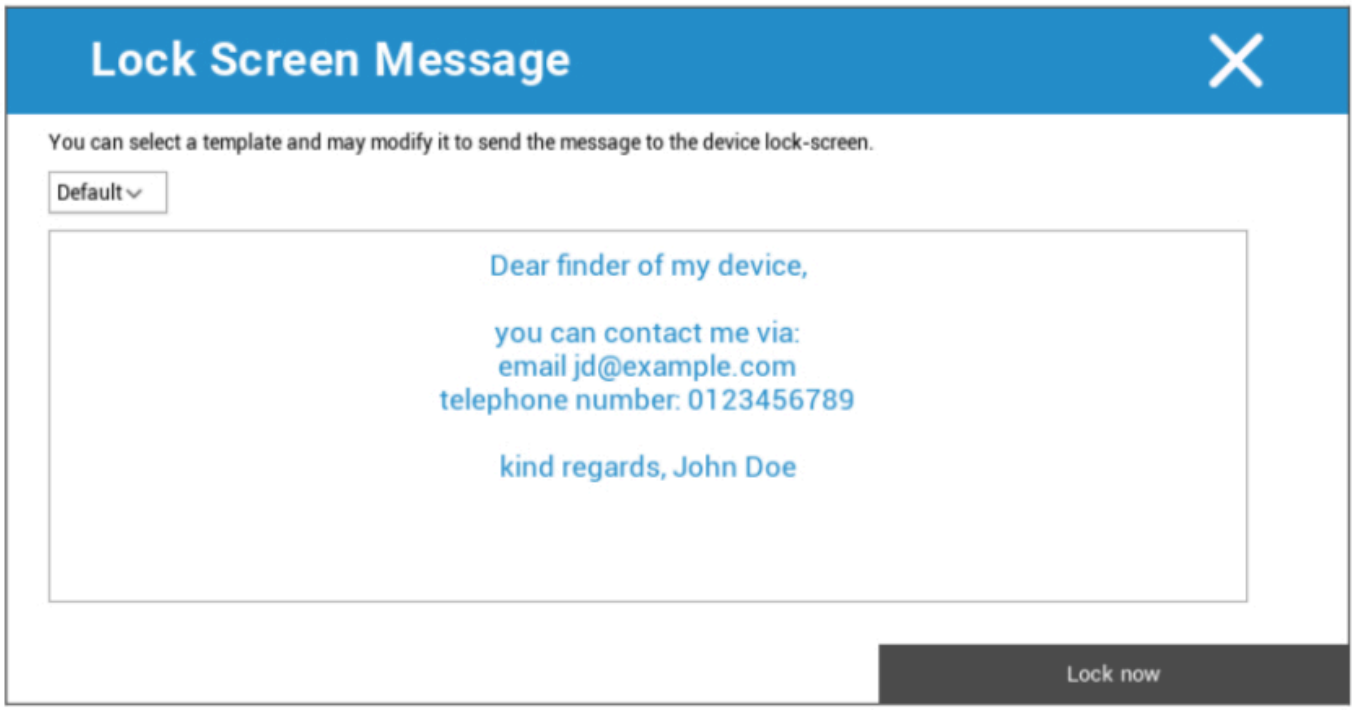
Her kan du opdatere en række oplysninger om enheden.

Slet adgangskode



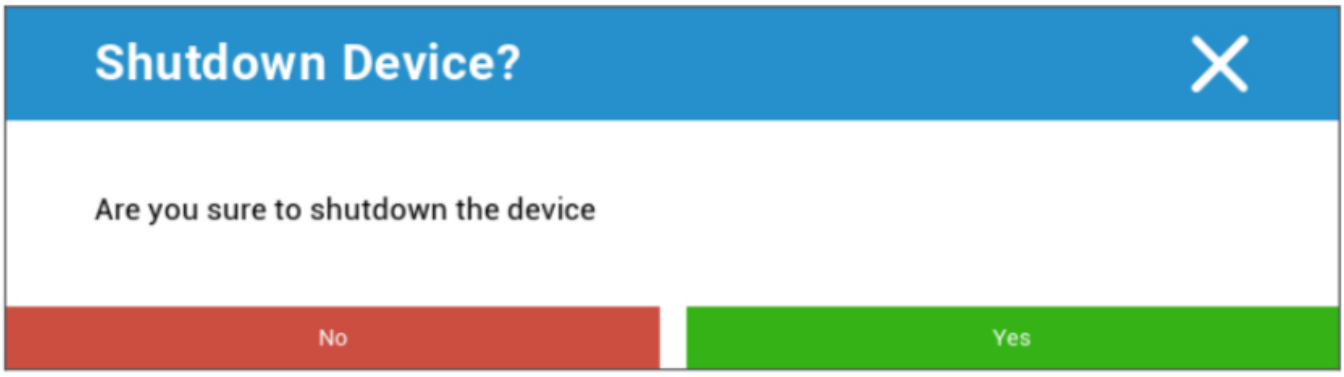
Under "Clear Passcode" kan du fjerne adgangskoden fra enheden. Efterfølgende vil brugeren blive bedt om at udstede en ny adgangskode (afhængigt af retningslinjerne for adgangskoden).

Lås enhed



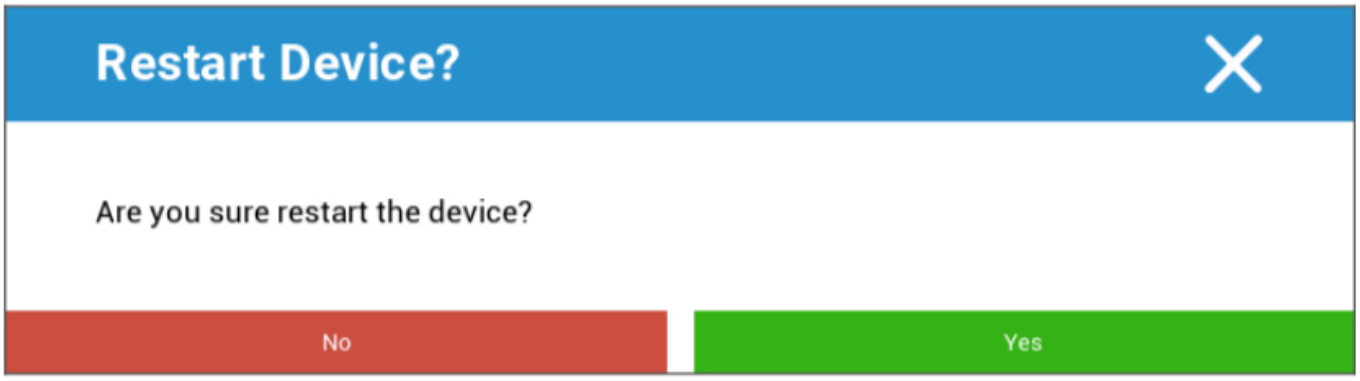
Her sendes en låsekommando til slutbrugerens enhed (låseskærm).

Nedlukningsenhed



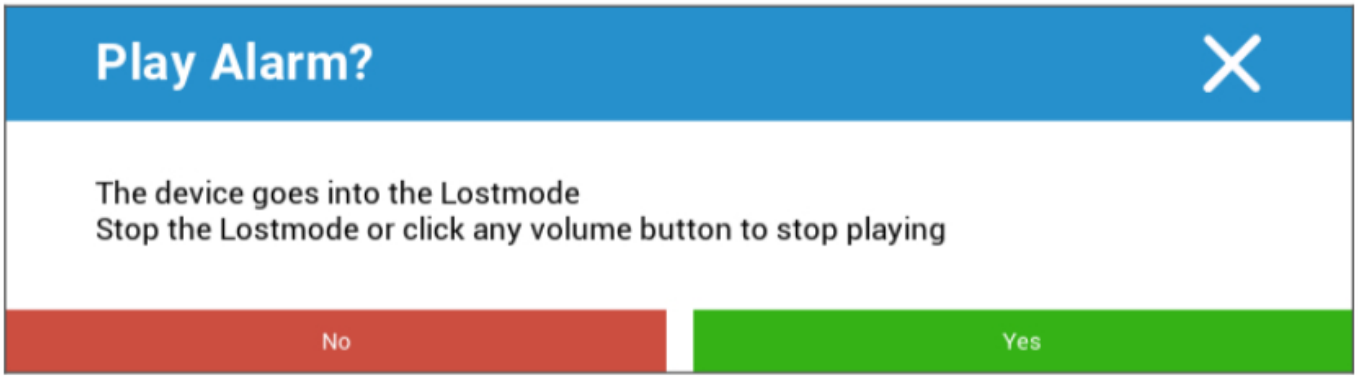
Her sendes en nedlukningskommando til slutbrugerens enhed.

Genstart enheden

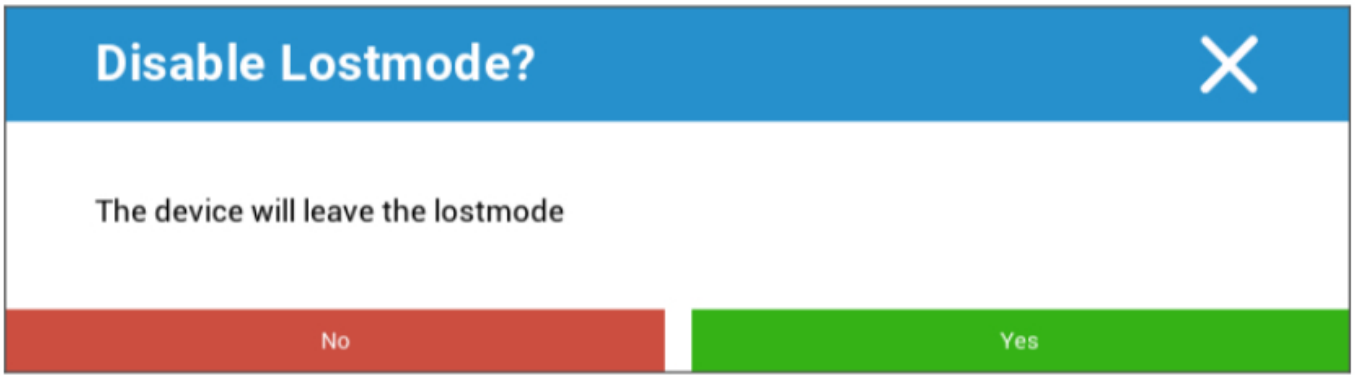


Her sendes en genstartskommando til slutbrugerens enhed.

Alarm & Lostmode | Deaktiver Lostmode



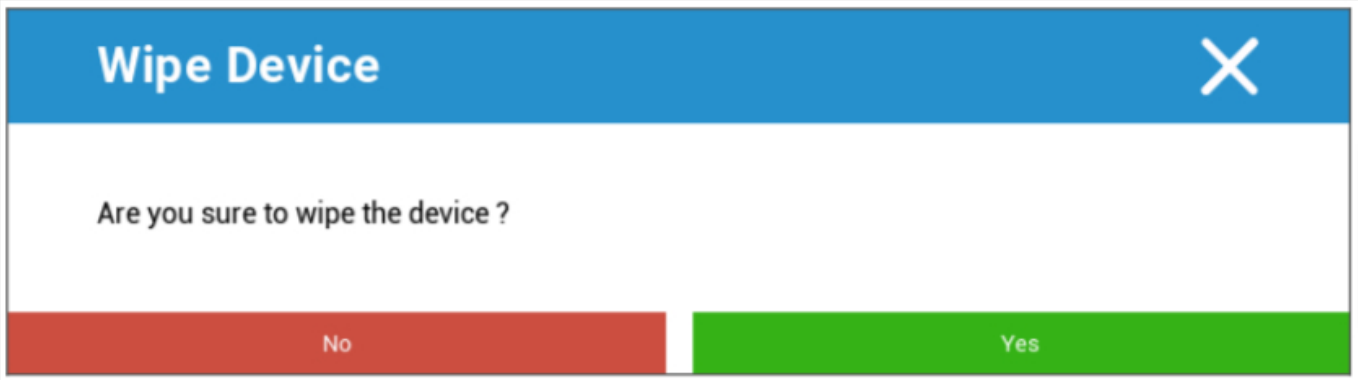
Her kan enheden indstilles til Lostmode, som indstiller enheden til konstant at afspille en alarmlyd. Lostmode kan stoppes ved at trykke på en hvilken som helst lydstyrkeknap på enheden eller eksternt ved at klikke på "Disable Lostmode":



Slet enhed

Her kan slettekommandoen udføres. Du kan igen vælge, om enheden kun skal fjernes fra AppTec360 ("Delete from System"), eller om enheden skal fjernes fra AppTec360 og også gendannes til fabriksindstillingerne ("Wipe & Delete").

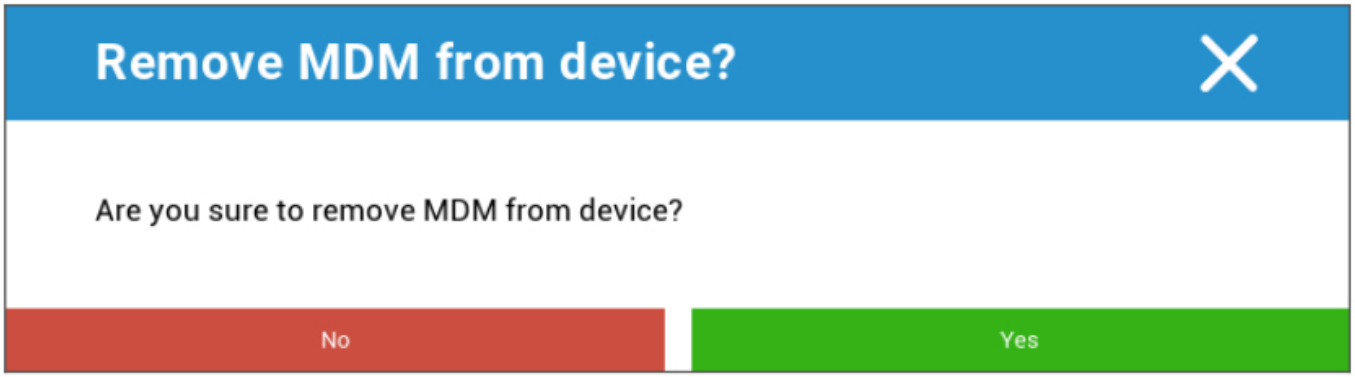
Tør enhed af



Under "Slet enhed" kan du udføre en komplet sletning af enheden. Enheden gendannes til fabriksindstillingerne.

Enterprise Wipe | Fjern MDM

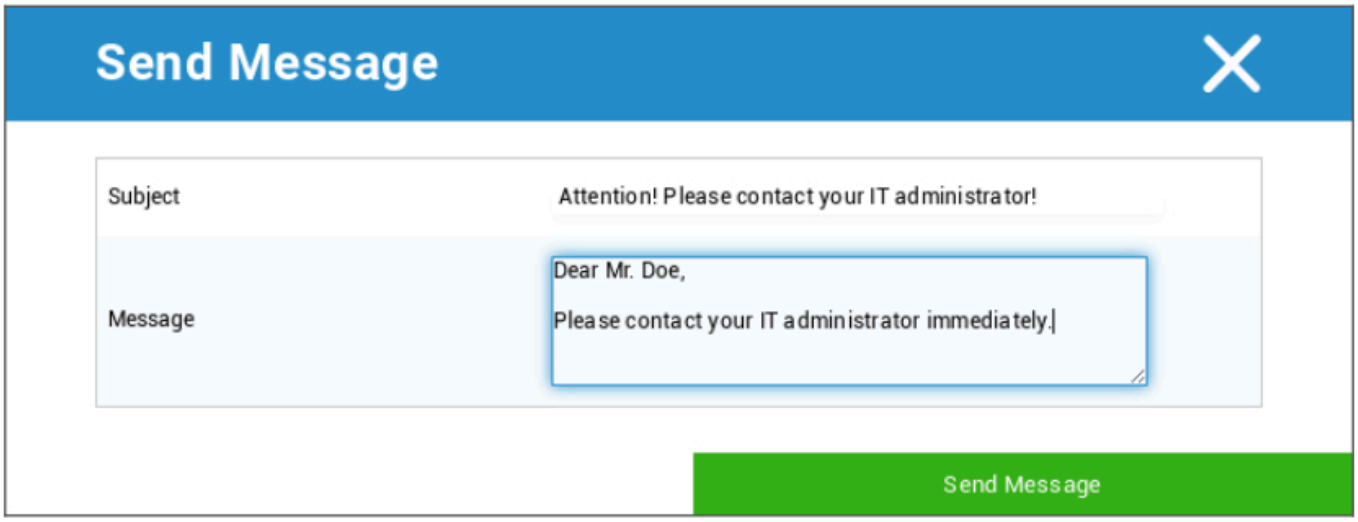
Kun de oplysninger, apps og profiler, der leveres af AppTec360, slettes. På denne måde vil virksomhedsdataene ikke længere være tilgængelige på slutbrugerens enhed. Det private område påvirkes ikke og forbliver fortsat på slutbrugerens enhed.



Med "Fjern MDM" kan du fjerne MDM-profilen på slutbrugerens enhed og alle andre elementer, der leveres af AppTec.

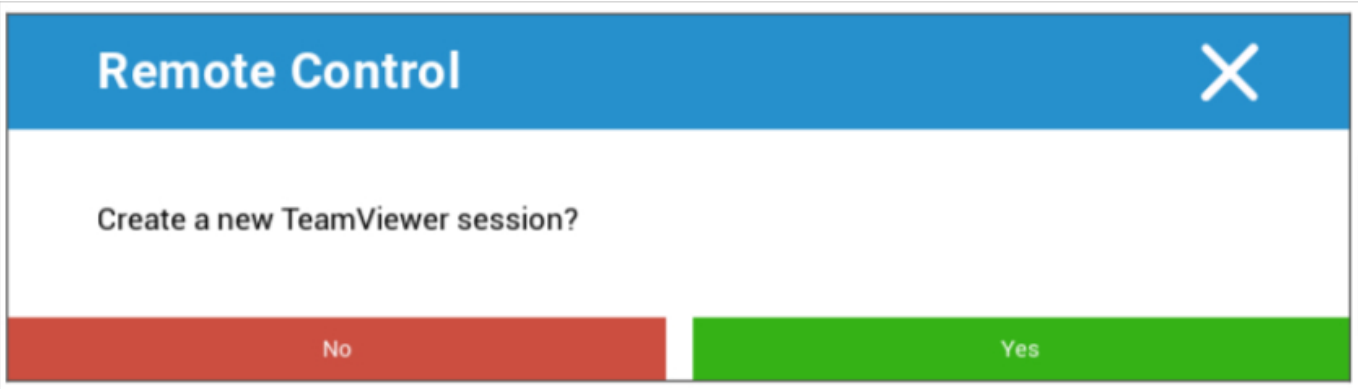
Denne kommando udfører samme handling som "Enterprise Wipe".

Send besked



Her kan du sende en push-meddelelse til den pågældende enhed.

TeamViewer-fjernbetjening



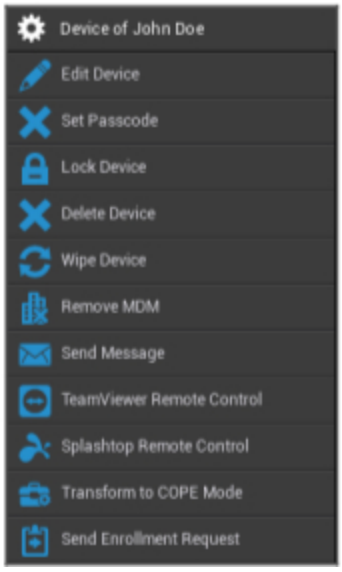
Her kan man starte en Teamviewer Remote Control-session.

Send tilmeldingsanmodning

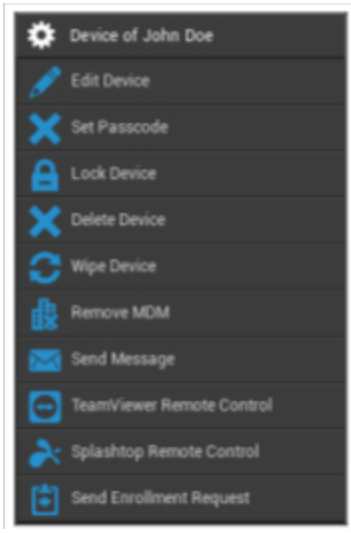
Med "Send tilmeldingsanmodning" kan du sende en tilmeldingsanmodning (igen) til den pågældende bruger.

Android

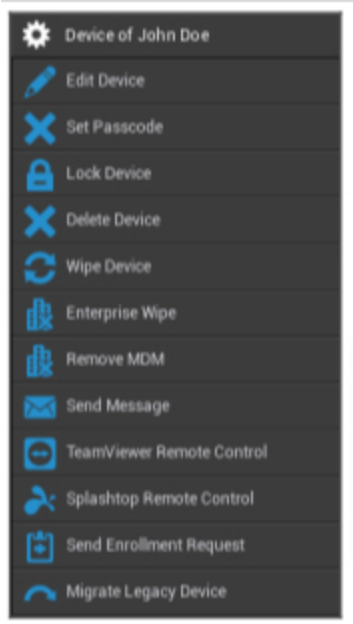
AE Fuldt administreret enhed (arbejdsadministreret)



AE-arbejdsprofil (container)



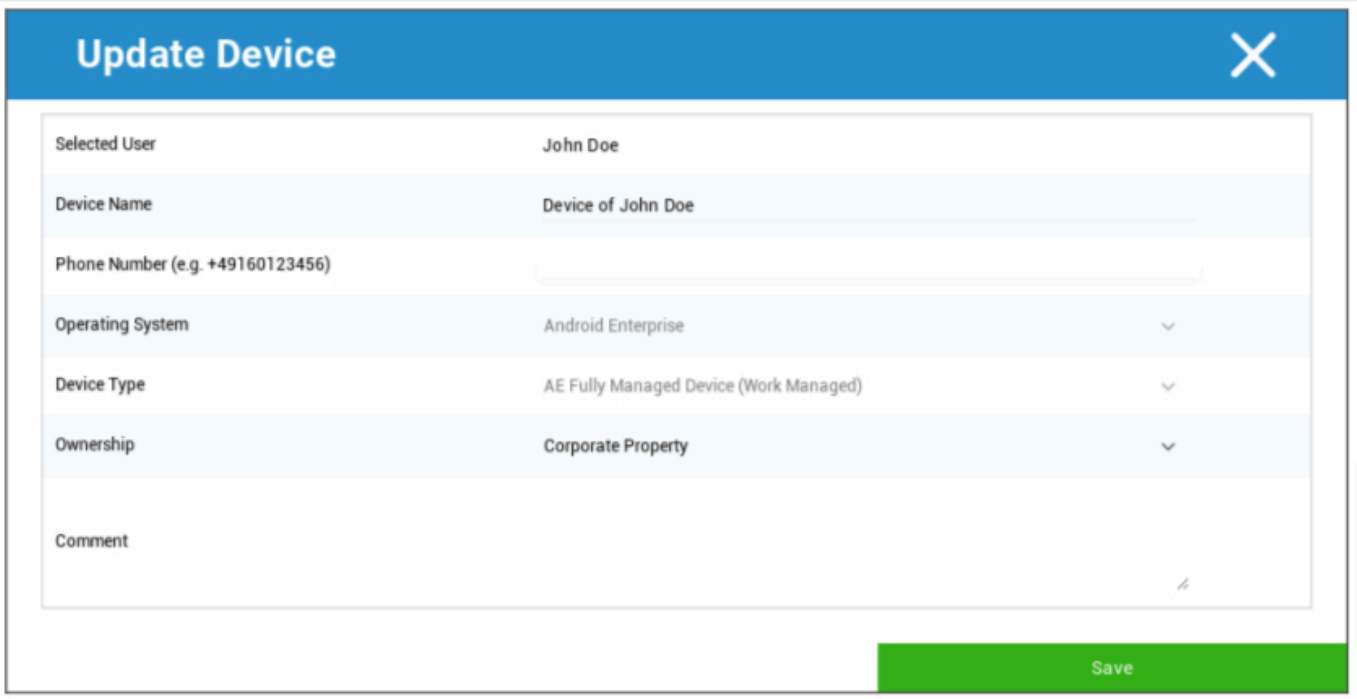
Android-telefon | Tablet



Rediger enhed	Rediger oplysninger om enheden
Indstil adgangskode	Indstil enhedens adgangskode
Lås enhed	Lås enhed (låseskærm)
Slet enhed	Slet enheden fra AppTec
Tør enhed af	Gendan enheden til fabriksindstillingerne
Enterprise Wipe	Oplysninger, apps og profiler, der leveres af AppTec360, slettes (enheden adskilles fra MDM).
Fjern MDM	
Send besked	Send push-meddelelser til enheden Beskeden vil blive vist i AppTec360-appen (fanen Besked).
TeamViewer-fjernbetjening	Start en fjernbetjeningssession for denne enhed ved hjælp af TeamViewer
Splashtop fjernbetjening	Start en fjernbetjeningssession for denne enhed ved hjælp af Splashtop
Skift til COPE-tilstand (kun på AE Fully Managed Device (Work Managed))	Opret en arbejdsprofil på denne AE Fully Managed (Work Managed) enhed
Send tilmeldingsanmodning	Send (gentagen) tilmeldingsanmodning
Migrer ældre enhed (kun på Android-telefon/tablet, når den er tilmeldt ved hjælp af Device Owner Mode Provisioning)	Overfør Android-telefon/tablet-profil til AE Fully Managed Device (Work Managed)-profil

Rediger enhed

Her kan du opdatere en række oplysninger om enheden.



Udvalgt bruger	Bruger af enhed
Enhedens navn	Enhedens navn
Telefonnummer	Enhedens telefonnummer
Operativsystem	Android Enterprise Android
Enhedstype	Android Enterprise: • AE Fuldt administreret enhed (arbejdsadministreret) • AE-arbejdsprofiltilstand (kun container) • AE Fuldt administreret enhed med arbejdsprofil (COPE) Android: • Telefon • Tablet
Ejerskab	Corporate = virksomhedsejendom

	Medarbejder = medarbejderegenskab
Kommentar	Yderligere beskrivelser af enheden

Slet adgangskode

Her kan du fjerne enhedens adgangskode på den valgte enhed. På Android er adgangskoden som standard indstillet til "123456" - dette kan og bør ændres af brugeren bagefter.

Lås enhed

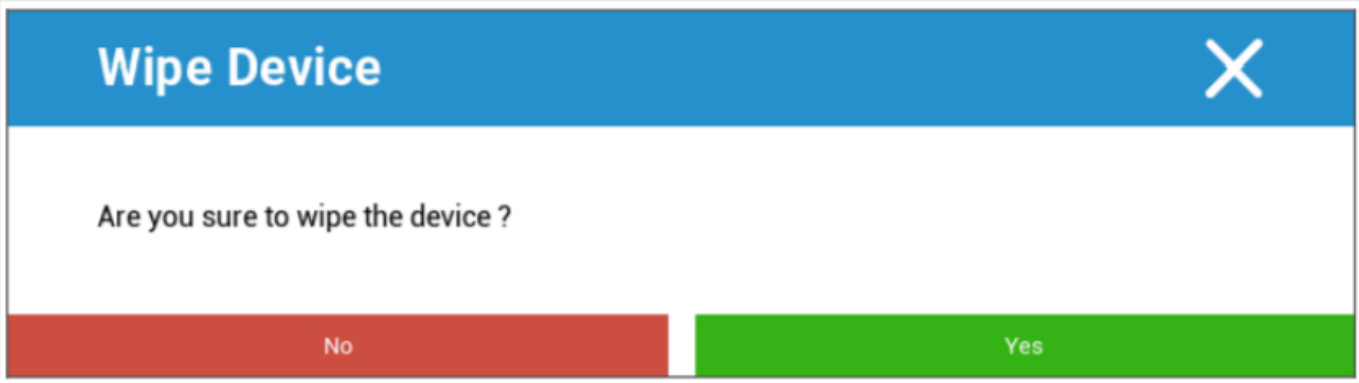
Her sendes en kommando til at låse enheden (låseskærm).

Slet enhed

Her kan der udføres en slettekommando. Du kan igen vælge, om enheden kun skal fjernes fra AppTec360 ("Delete from System"), eller om enheden skal fjernes fra AppTec360 og desuden gendannes til fabriksindstillingerne ("Wipe & Delete").

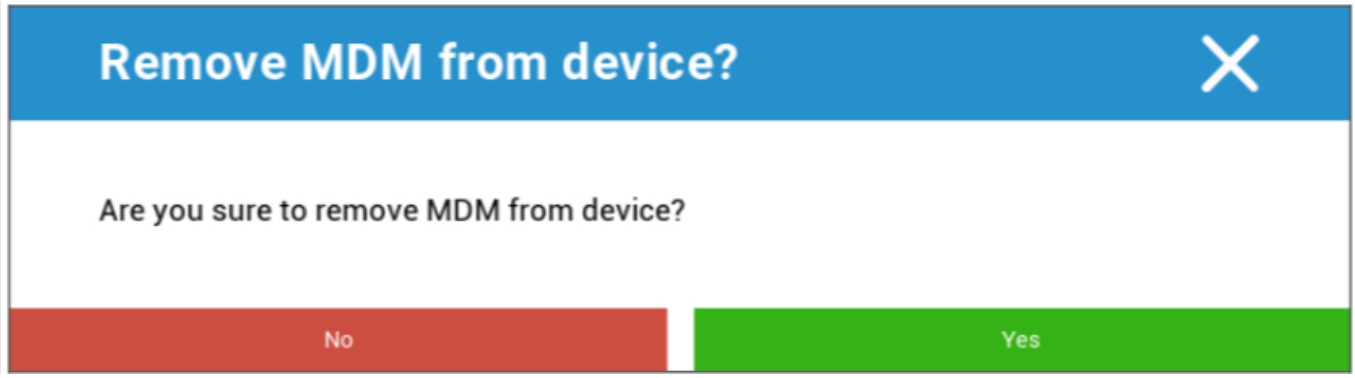
Tør enhed af

Under "Wipe Device" kan du udføre en komplet sletning af enheden. Enheden vil derefter blive gendannet til fabriksindstillingerne.



Hvis enheden indeholder et SD-kort, kan du desuden slette SD-kortet. Det kan du gøre ved at indstille "Wipe SD Card too? " til "On".

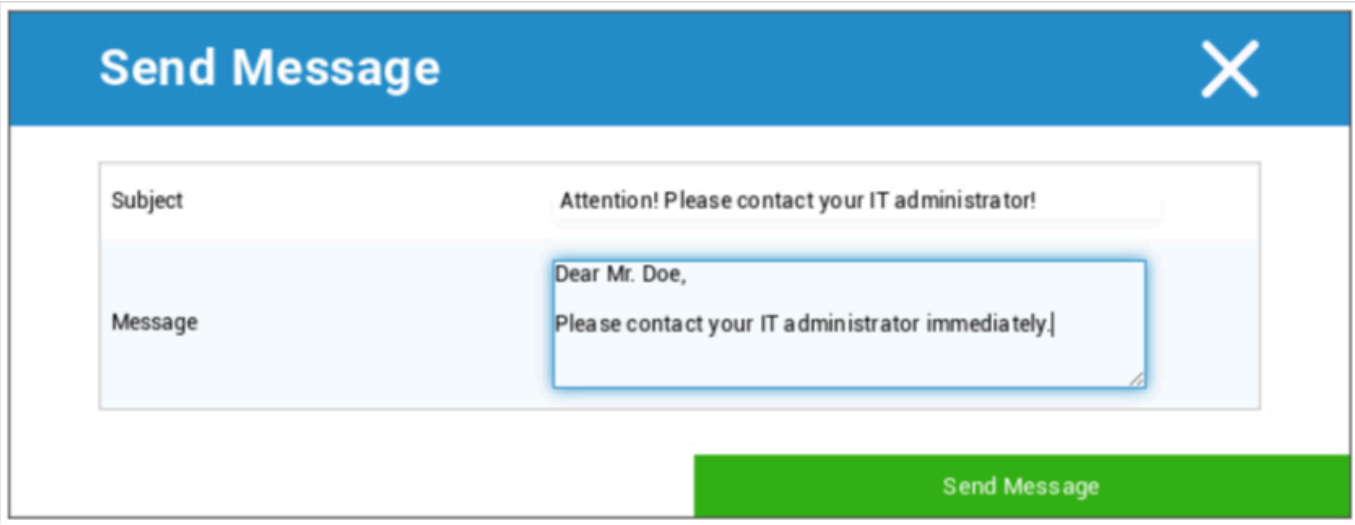
Fjern MDM



Dette er den anbefalede metode til at skabe en adskillelse fra MDM.

Kun de oplysninger, apps og profiler, der leveres af AppTec360, slettes, hvilket betyder, at alle virksomhedsdata ikke længere vil være tilgængelige på slutbrugerens enhed. Den private sfære påvirkes dog ikke og forbliver fortsat på slutbrugerens enhed.

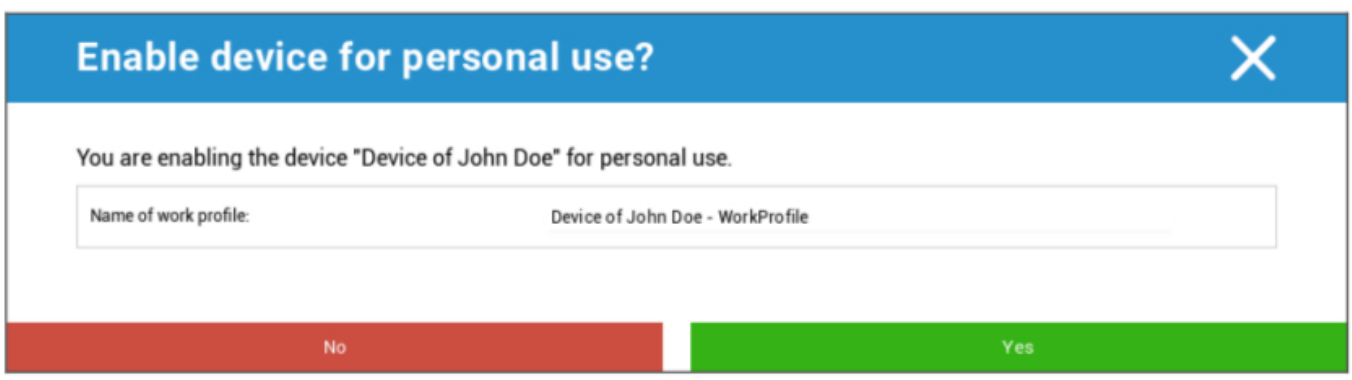
Send besked



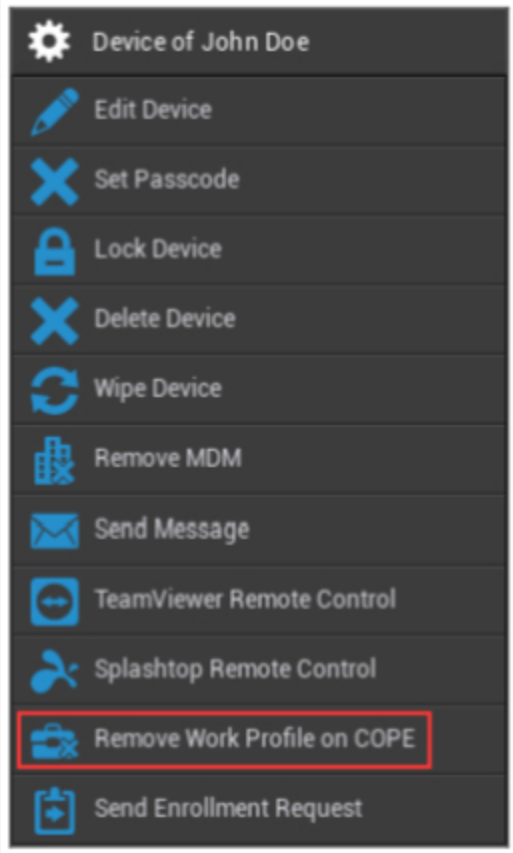
Her kan du sende en push-meddelelse til den pågældende slutbrugers enhed.

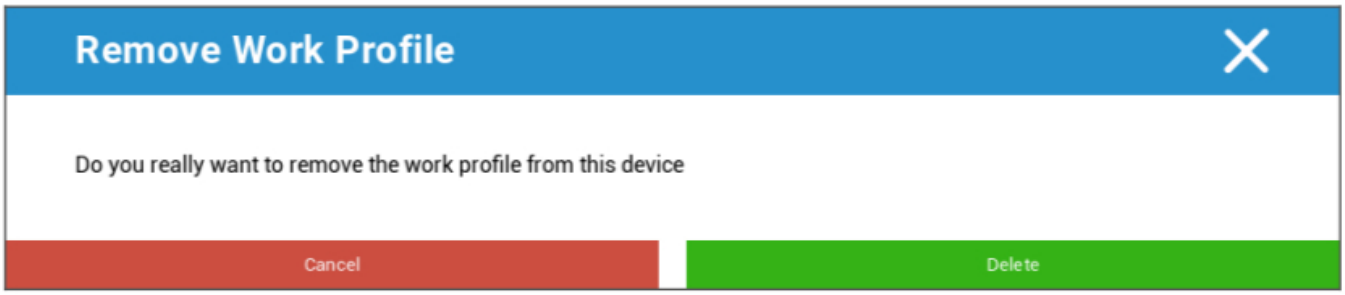
Skift til COPE-tilstand

Opret en arbejdsprofil på denne AE Fully Managed (Work Managed) enhed



Når du har omdannet enheden til COPE-tilstand, kan du fjerne arbejdsprofilen ved at klikke på tandhjulet **Fjern arbejdsprofil på COPE**:




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

Send tilmeldingsanmodning

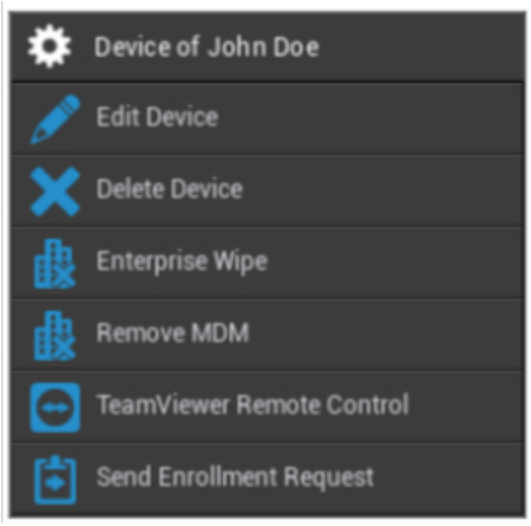
Med "Send tilmeldingsanmodning" kan du sende en tilmeldingsanmodning (igen) til den pågældende bruger.

Bemærk, at kun den nyeste tilmeldingsanmodning er gyldig.

Overfør ældre enheder

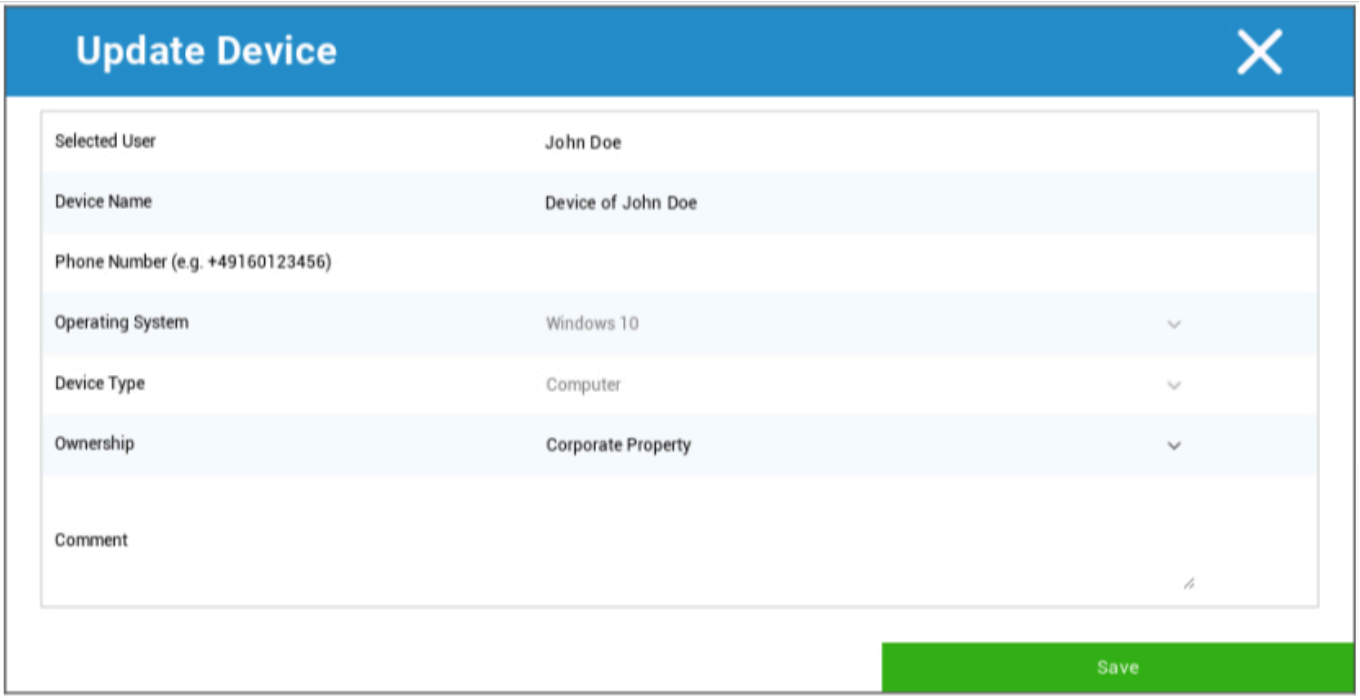
Overfør Android-telefon/tablet-profil til AE Fully Managed Device (Work Managed)-profil

Vinduer



Enhedens navn	Navnet på den valgte enhed
Rediger enhed	Rediger enhed
Slet enhed	Fjern enheden fra AppTec
Enterprise Wipe	Oplysninger, apps og profiler leveret af AppTec360 slettes
Fjern MDM	
TeamViewer-fjernbetjening	Fjernstyr enheden med TeamViewer
Send tilmeldingsanmodning	Send tilmeldingsanmodning (igen)

Rediger enhed

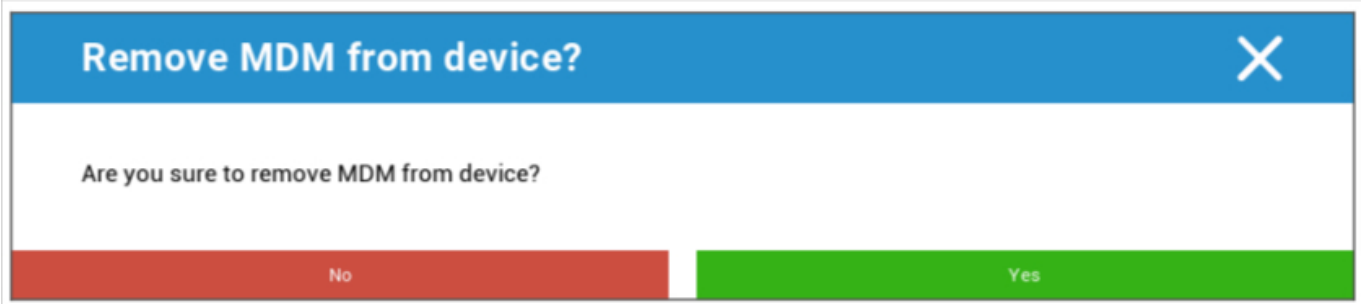


Her kan du opdatere en række oplysninger om enheden.

Slet enhed

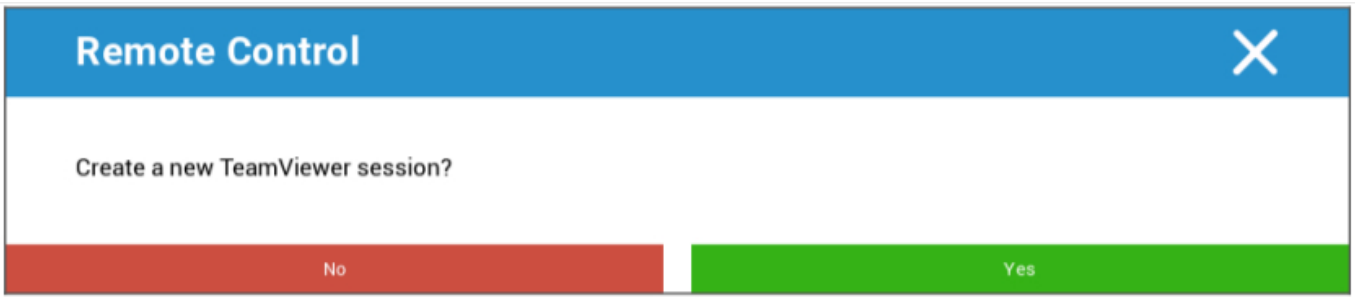
Her kan delete-kommandoen, som kun fjerner enheden fra AppTec360, udføres.

Enterprise Wipe | Fjern MDM



Kun de oplysninger, apps og profiler, der leveres af AppTec360, slettes. På denne måde vil virksomhedsdataene ikke længere være tilgængelige på slutbrugerens enhed. Det private område påvirkes ikke og forbliver fortsat på slutbrugerens enhed.

TeamViewer-fjernbetjening



Her kan du starte en TeamViewer-fjernbetjeningssession for denne enhed.

Send tilmeldingsanmodning

Med "Send tilmeldingsanmodning" kan du sende en tilmeldingsanmodning (igen) til den pågældende bruger.

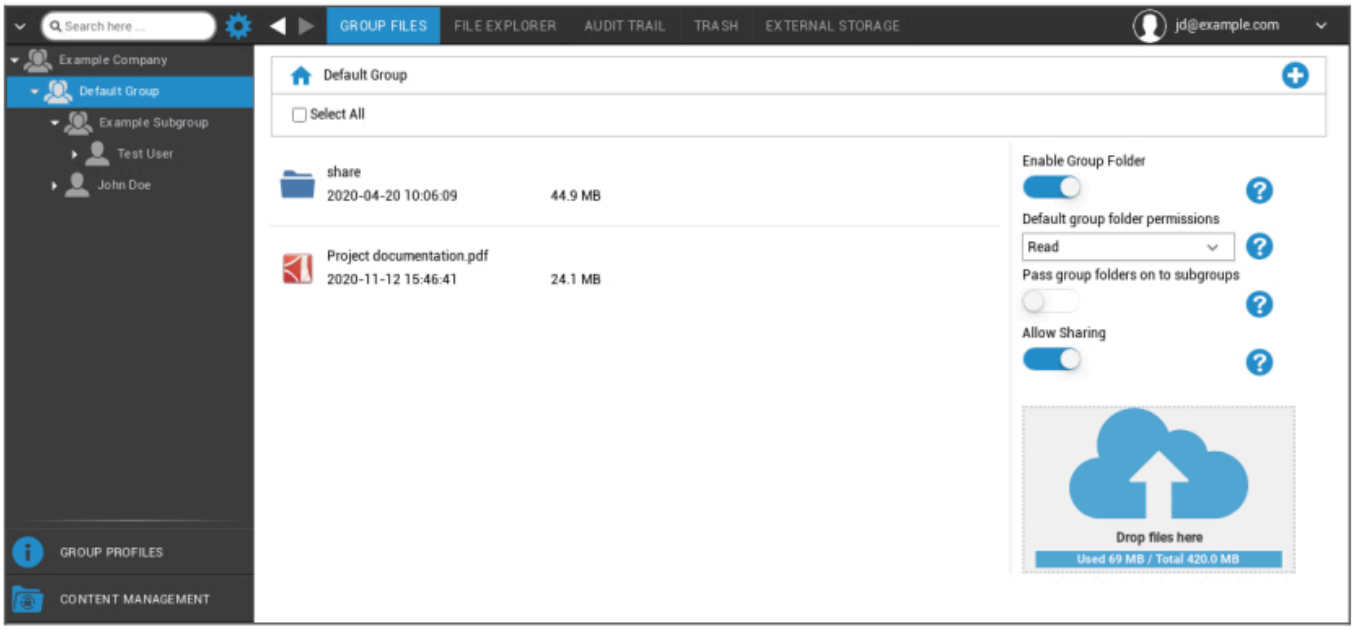
Styring af indhold

Når du er i en gruppe, kan du administrere AppTecs ContentBox med "Content Management".

Med Content Box kan du sikkert distribuere dokumenter og andre virksomhedsdata til slutbrugernes enheder.

Gruppefiler

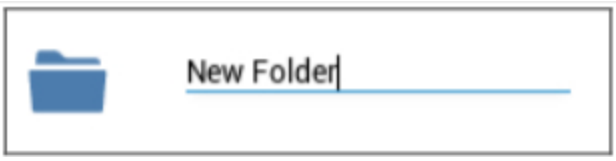
"Group Files" er en grundlæggende del af ContentBox. Her foretager du indstillinger, uploader dokumenter, opretter nye mapper osv.



Med symbolet i øverste højre hjørne kan du oprette nye mapper, som tilknyttes den pågældende gruppe med "Tilføj mappe".

Med symbolet i øverste højre hjørne kan du oprette en ny mappe via "Tilføj mappe", som skal tilknyttes den pågældende gruppe.

Du kan navngive mappen, som du vil.



Via "Upload Files" kan du uploade data. Her vil din Standard-Explorer blive åbnet. Du kan selvfølgelig udføre disse to handlinger i alle (under)mapper.

Med symbolet i øverste venstre hjørne kan du vende tilbage til hovedmenuen.

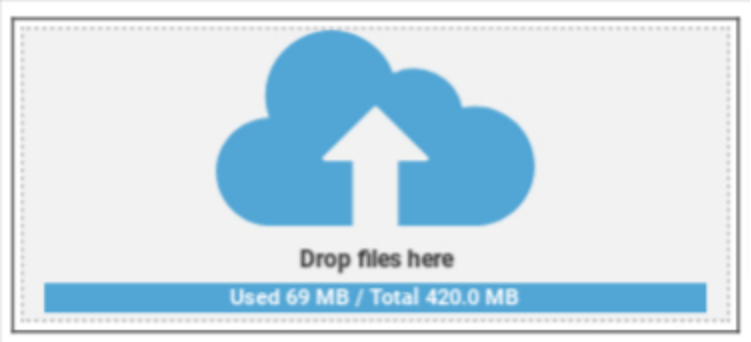
Du kan vælge flere mapper og filer og downloade dem med "Download", eller du kan slette dem ved at klikke på "Delete".

Du kan også vælge alle filer og mapper med og udføre kommandoerne "Download" og "Slet".

Når du fører musen hen over en mappe eller fil, ser du følgende oversigt:

- Med "Omdøb" kan du omdøbe mappen/filen
- Med "Download" kan du downloade mappen/filen
- Med "Slet" kan du slette mappen/filen

Aktivér gruppemappe	Hvis den er aktiveret, har alle medlemmer af gruppen adgang til den pågældende mappe.
Standardtilladelser til gruppemapper	Rettigheder for brugerne i den valgte gruppe: Read = kun læsetilladelse Update = opdateringstilladelse Create = tilladelse til at oprette Delete = slet tilladelse
Send gruppemapper videre til undergrupper	Hvis den er aktiveret, kan de respektive undergrupper få adgang til de overordnede datafiler
Tilladelser til undergrupper	Rettigheder for brugerne i den valgte undergruppe: Read = kun læsetilladelse Update = opdateringstilladelse Create = tilladelse til at oprette Delete = slet tilladelse
Tillad deling	Hvis den er aktiveret, kan brugeren dele filer via et link



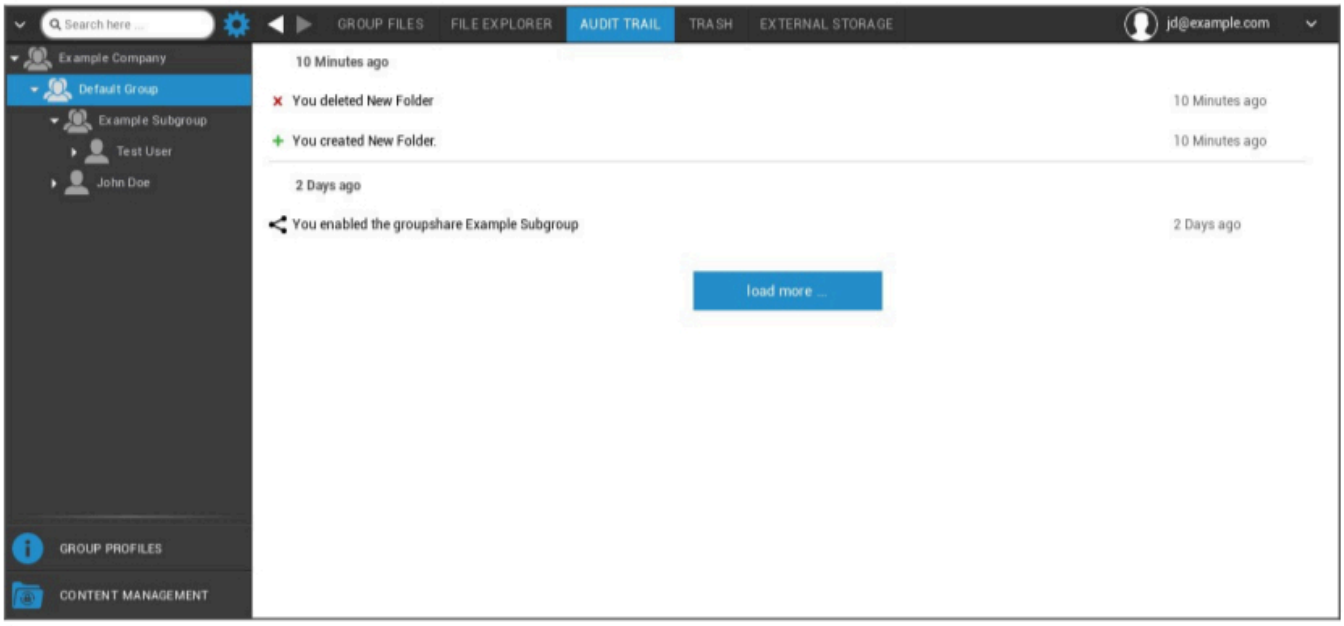
For at uploade filer kan du bruge dette felt ved at trække en fil via Drag & Drop til dette vindue. Du kan også klikke på dette felt for at vælge og uploade en fil ved hjælp af Internet Explorer.

Stifinder

Med "File Explorer" kan du administrere alle mapper og filer - uanset hvilken gruppe de er arkiveret i.

Du finder også de indstillinger og knapper, som du lærte om i "Gruppefiler".

Revisionsspor



I "Audit Trail" kan du ud fra historikken se, hvilken bruger der har oprettet, slettet eller delt hvad. På den måde kan du til enhver tid finde ud af, hvad der er sket med virksomhedens data.

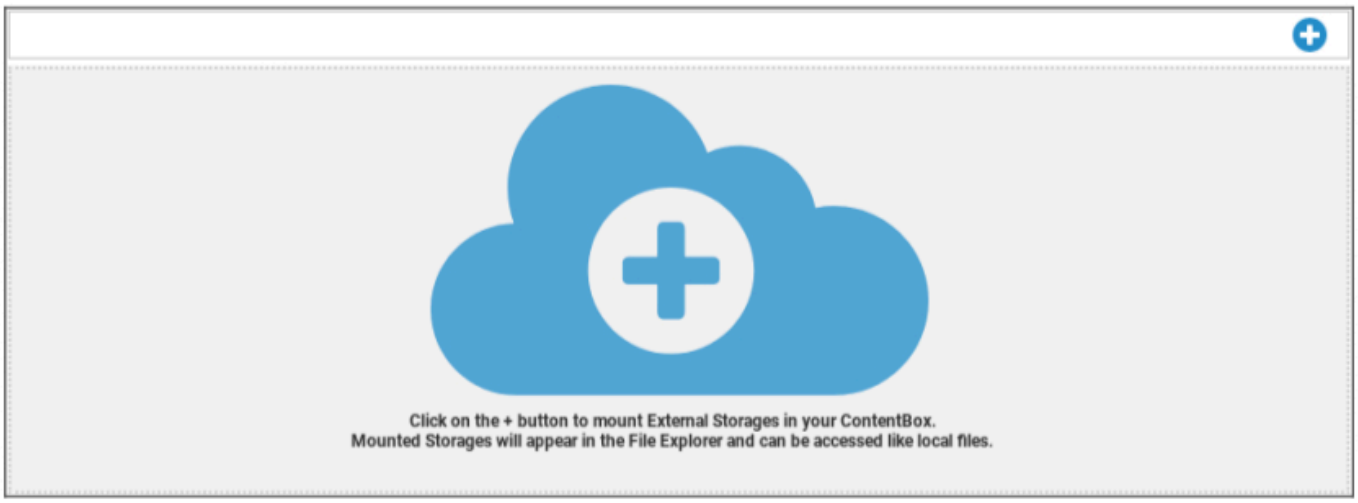
Affald

Hvis du har slettet noget (ved et uheld), kan du se mapperne og filerne under "Papirkurv" og gendanne dem, som du ønsker det.

- Med "Undelete" kan du gendanne data/mapper.
- Med "Delete" kan du slette data/mappen permanent - du skal bekræfte dele-kommandoen en gang til.

Bemærk, at den lagerkapacitet, der bruges i papirkurven, reducerer den "samlede plads", der er til rådighed - det er et krav fra ownCloud.

Eksternt lager



Under overskriften "Eksternt lager" kan du tilslutte eksternt lager.

Med symbolet kan der tilføjes (ekstra) lagerplads.

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

Amazon S3	
Vis navn	Vis navn
Adgangsnøgle	Adgangsnøgle
Hemmelig nøgle	Sikkerhedsnøgle
Spand	Definitiv identitet på den undermappe, der er blevet tildelt dig
Værtsnavn (valgfrit)	Værtsnavn (valgfrit)
Port (valgfrit)	Port (valgfrit)
Region	Region (valgfrit)
Aktivér SSL	Aktivér SSL
Aktiver sti-stil	Clear Path-adresse, der er blevet tildelt dig

FTP	
Vis navn	Vis navn
Vært	Værts-adresse
Brugernavn	Brugernavn
Adgangskode	Adgangskode
Rod	Hovedmenu
Sikker ftps://.	

SFTP	
Vis navn	Vis navn
Vært	Værts-adresse
Brugernavn	Brugernavn
Adgangskode	Adgangskode
Rod	Hovedmenu

ownCloud	
Vis navn	Vis navn
URL	ownCloud URL
Brugernavn	Brugernavn
Adgangskode	Adgangskode
Ekstern undermappe	Standardmappe
Sikker https://	

WebDAV	
Vis navn	Vis navn
URL	WebDAV-URL
Brugernavn	Brugernavn
Adgangskode	Adgangskode
Rod	Hovedmenu
Sikker https://	
Windows Share	Understøttelse af Windows Share vil snart være tilgængelig
SharePoint	Understøttelse af Microsoft SharePoint vil snart være tilgængelig

Audit-log

Her kan du finde en log, der registrerer oplysninger om handlinger, der udføres i MDM-konsollen.

Med filterikonet kan du anvende filtre på den viste liste.

Med rullemenuen Elementer **pr. side**: kan du vælge, hvor mange elementer der skal vises på én side af listen.

Handling foretaget / indstilling ændret	Den handling, der blev foretaget / Den indstilling, der blev ændret
Værdi	Værdien af den udførte handling/ændrede indstilling
Bruger	Navnet på den bruger, der har foretaget handlingen/ændret indstillingen
Dato	Tidsstemplet for, hvornår denne handling blev foretaget / denne indstilling blev ændret
Sti / type	Stien til, hvor denne handling blev udført / denne indstilling blev ændret

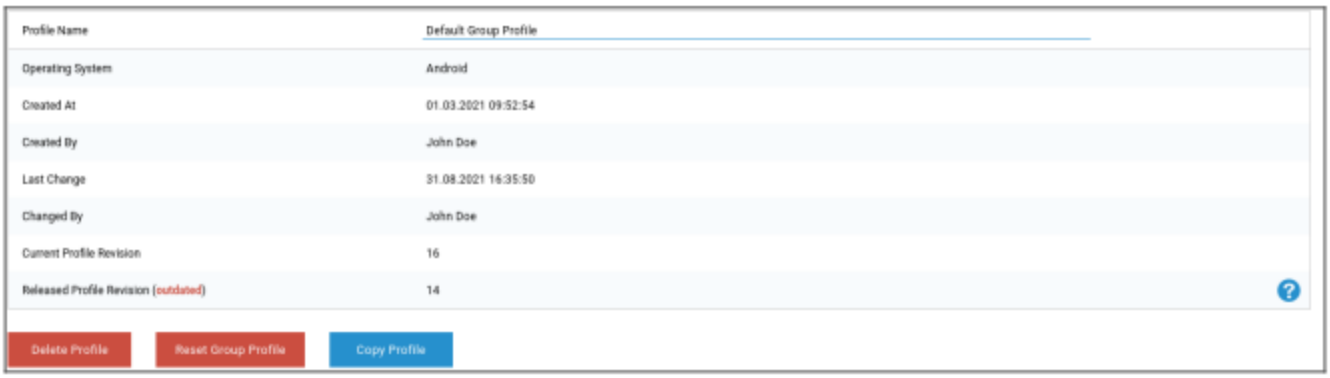
iOS-konfiguration

Generelt

Afhængigt af om du i øjeblikket har valgt en gruppe eller en enhed, er displayet og dets underpunkter forskellige - vær meget opmærksom på dette!

Oversigt over gruppeprofiler (kun på gruppeniveau)

Når du åbner en gruppeprofil, får du et hurtigt overblik over profilen



Navn på profil	Navn på profilen (kan ændres her)
Operativsystem	Operativsystem, som profilen er til
Oprettet på	Tidspunkt for skabelse
Oprettet af	Profilens skaber
Sidste ændring	Tidspunkt for sidste ændring af profilen
Ændret af	Konto, der foretog de sidste ændringer
Nuværende profilrevision	Revision af gemt profiltilstand
Udgivet profilrevision	Tildelt profilrevision ("Tildel nu"). Hvis etiketten viser "(forældet)" bag teksten, betyder det, at du har gemt profilen, men ikke tildelt den endnu, så enhederne vil stadig få en ældre version.

Generel information

Hvis du er direkte på enheden, får du en kort oversigt over din valgte enhed.

Enhedens navn	Enhedens navn
Telefonnummer	Enhedens telefonnummer
Model	Model nummer
Operativsystem	OS
Serienummer	Enhedens serienummer
Ejerskab af enhed	Virksomheds- eller privat enhed Corporate = virksomhedsenhed Medarbejder = privat enhed
Enhedstype	Enhedstype (tablet eller telefon)
Jailbroken	Hvis der er et jailbreak på enheden
Overvåget	Angiver, om dette er en overvåget enhed
Overensstemmende	Hvis nogen retningslinjer blev overtrådt
Sidst set	Status for, hvornår enheden sidst kommunikerede med AppTec360-serveren

Indstillinger

Disse indstillinger indeholder enhedens navn og en foruddefineret baggrund.

Navngiv enhed til systemnavn	Det navn, der udstedes i AppTec360-konsollen (i venstre hierarkistruktur), vil være det samme som på den respektive slutbrugerenhed (kan ses i enhedsindstillingerne).
Brug brugerdefineret baggrund (kun overvågede enheder)	Her kan du foruddefinere den baggrund, der skal vises på slutbrugerens enhed (f.eks. til en form for virksomhedsbranding for enheden). Er kun tilgængelig i overvåget tilstand!
Automatiske OS-opdateringer	Fremtvinger OS-opdateringer, hvis de er tilgængelige. Kun for DEP-enheder i overvåget tilstand.
Tilpassede skrifttyper	Her kan du tilføje brugerdefinerede skrifttyper.
Navn	Valgfrit. Det synlige navn for skrifttypen. Dette felt erstattes af det faktiske navn på skrifttypen efter installationen.
Skrifttype	Upload skrifttypefilen (.otf eller .ttf).

Config Revision

Her får du en oversigt over, hvilken gruppeprofil der er tildelt enheden.

Hvis du klikker på gruppeprofilen, får du direkte adgang til profilen, og du kan foretage indstillinger.

Med symbolet kan du gendanne de tildelte apps til gruppeprofilens indstillinger.

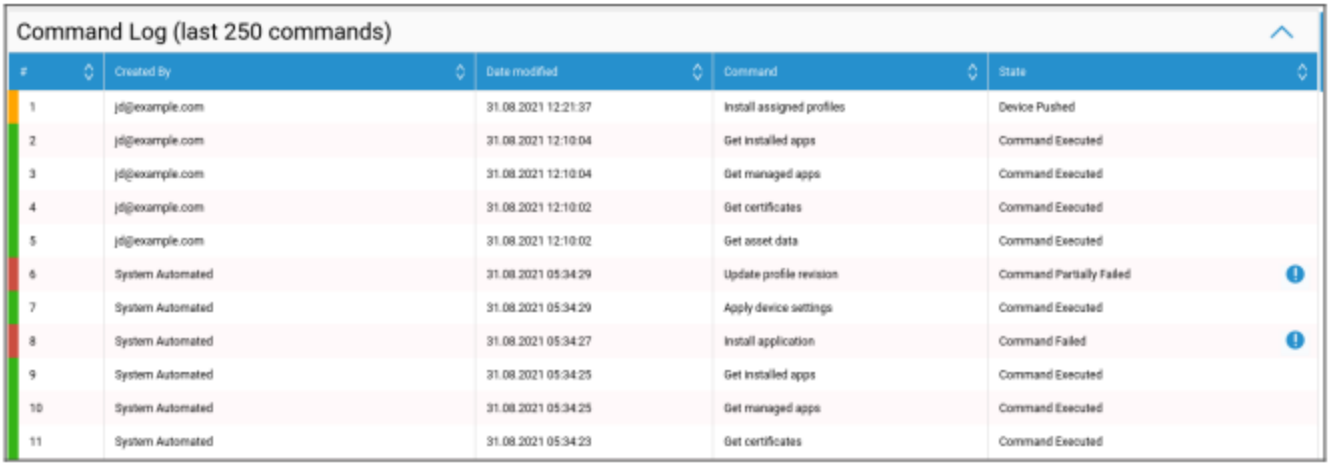
Med symbolet kan du nulstille enhedens profil, så den slet ikke har nogen indstillinger.

"Nyere revision tilgængelig" angiver, at gruppeprofilen er blevet ændret og gemt, men ikke tildelt. Gruppeprofilen skal tildeles med "Tildel nu" på gruppeniveau for at anvende ændringerne på enhederne.

Enhedslog (kun på enhedsniveau)

Kommando-log

Her kan du se, hvilke kommandoer der er udstedt til enheden, og hvad deres status er.



Kommandoer, der er oprettet af "System Automated", oprettes automatisk af systemet.

Mulige kommandostatusser

Enhed skubbet	Der er sendt en push-anmodning til push-tjenesten (f.eks. APNS) for at fortælle enheden, at den skal oprette forbindelse tilbage til EMM-serveren.
Kommando oprettet	Kommandoen blev oprettet i systemet.
Kommando sendt	Kommandoen blev sendt til enheden, efter at den havde oprettet forbindelse til serveren.
Kommando udført	Kommandoen blev udført med succes.
Kommando mislykkedes	Kommandoen mislykkedes. *
Kommando delvist mislykket	Afhængigt af enhedens operativsystem kan nogle kommandoer blive grupperet sammen. Nogle dele af denne kommandogruppe mislykkedes. *
Kommandoen blev udført, men mislykkedes til sidst	Kommandoen blev udført, men måske blev den ikke.
Kommando genindført	Kommandoen blev repushed af en bruger.
Kasseret	Kommandoen blev kasseret. For eksempel fordi den blev erstattet af en anden kommando, eller fordi enheden blev genindskrevet, og gamle kommandoer blev fjernet.

Hvis der er et udråbstegn bag beskeden, kan du få flere oplysninger ved at holde markøren over ikonet.

Asset Management (kun på enhedsniveau)

Asset Management (kun på enhedsniveau)

Enhedsinfo

Model	Enhedens modelnummer
Operativsystem	OS
OS-version	OS-version
Serienummer	Serienummer
UDID	Enhedens UDID
Enhedens navn	Enhedens navn
Overvåget	Viser, om enheden er overvåget
Batteristatus	Batteristatus

Wi-Fi

IP-adresse	Enhedens IP-adresse
WiFi MAC	WiFi MAC-adresse

Cellulær

Status	Status (SIM-kort til stede)
Telefonnummer	Telefonnummer
Roaming-status	Aktuel roaming-status
Roaming (tale/data)	Roaming-status for tale/data
IP-adresse	IP-adresse
IMEI	IMEI-nummer
Operatør/transportør	Udbyder af mobiltjenester
SIM-bærerens netværk	SIM-operatørens netværk
Transportør-version	Bærende version
Modem-firmware	Modemets firmware
Nuværende MCC/MNC	Se "SIM MCC/MNC"
SIM MCC/MNC	Mobile Country Code er en etableret landeidentifikation af ITU i henhold til E.212-standarden, som sammen med Mobile Network Code (MNC) bruges til at identificere et mobilnetværk (= landekode). Når du går ind på et andet mobilnetværk, er "Current MCC/MNC" og "SIM MCC/MNC" derfor forskellige.

Bluetooth

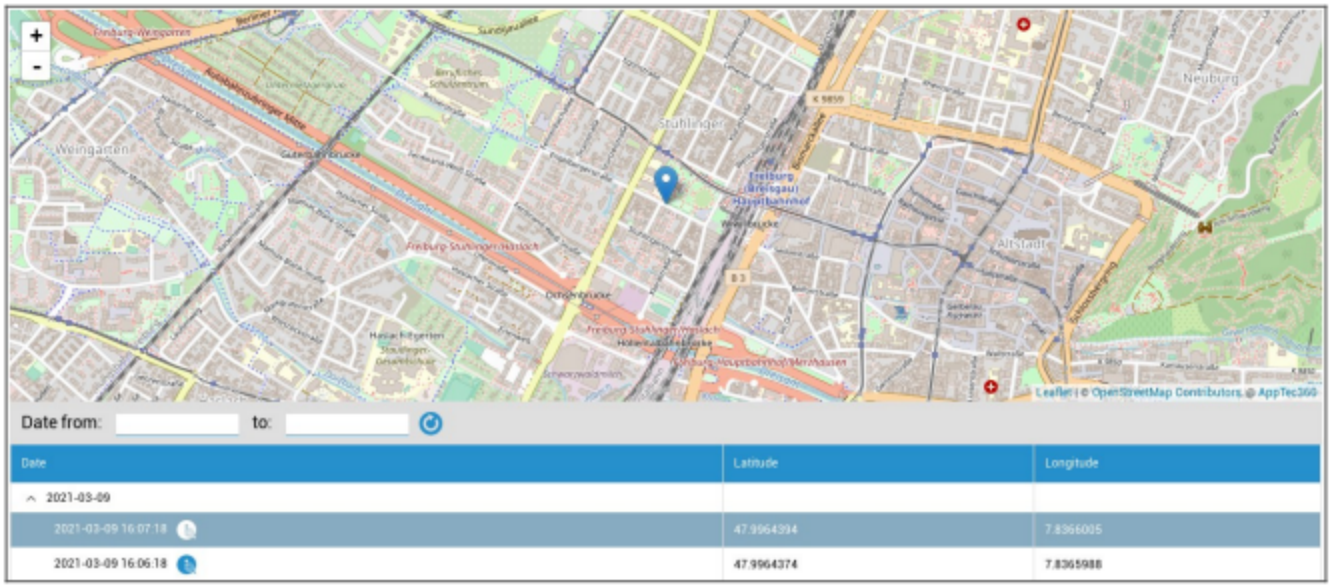
Bluetooth MAC	Bluetooth MAC-adresse

Sikkerhedsstyring

Tyverisikring (kun på enhedsniveau)

GPS-information (kun på enhedsniveau)

Her kan du vurdere enhedens nuværende/sidste placering. Lokaliseringen kan enten beskyttes med en eller endda to adgangskoder - se: Generelle indstillinger - Privatliv - GPS-adgang



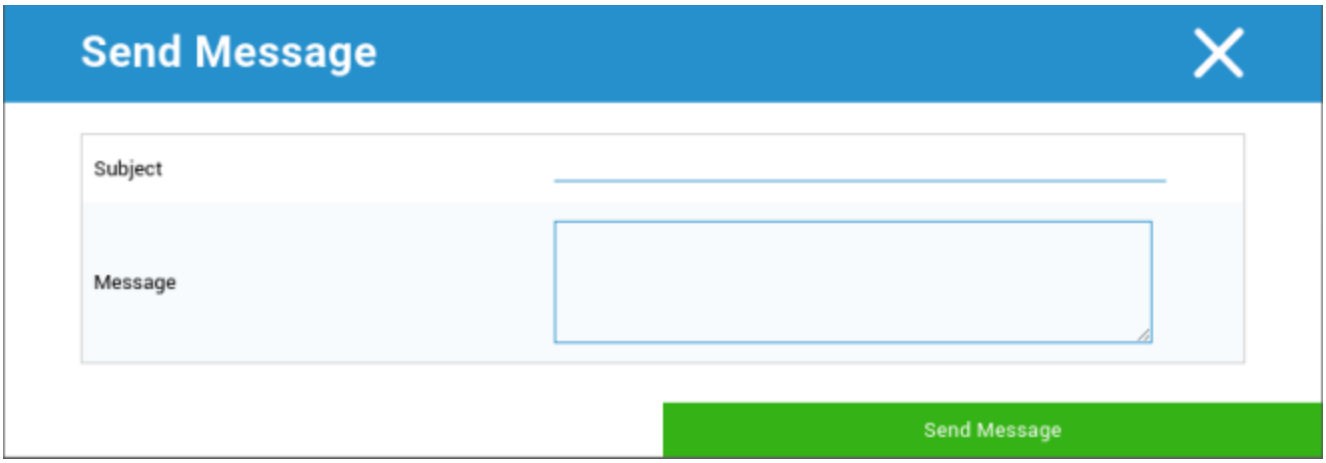
Tør og lås (kun på enhedsniveau)

Under "Wipe & Lock" kan du udføre følgende tre handlinger:

Fuld aftørring	Enheden gendannes til fabriksindstillingerne (både virksomhedsdata og personlige data slettes).
Enterprise Wipe	Kun virksomhedsdata fjernes fra slutbrugerens enhed (alle apps, data osv., der blev leveret af AppTec).
Låseskærm	Skærmlås er aktiveret, det er tilstrækkeligt at låse enheden op med enhedens adgangskode/PIN.
Retsmedicinsk nedlukning (kun overvågede enheder)	Hvis denne funktion aktiveres med symbolet  , låses enheden ved at vise en besked, som ikke kan lukkes. Medarbejderen kan heller ikke låse enheden op. Kun administratoren kan låse enheden op i konsollen med oplåsningssymbolet  .
Tillad aktiveringslås (kun overvågede enheder)	Hvis denne funktion er aktiveret, bliver enheden låst, så snart "Find min iPhone" er aktiveret i iCloud-indstillingerne.

Besked (kun på enhedsniveau)

I det følgende vindue kan du udfylde emnet og en besked og sende den til en slutbrugerenhed:



Sikkerhedskonfiguration

Adgangskode

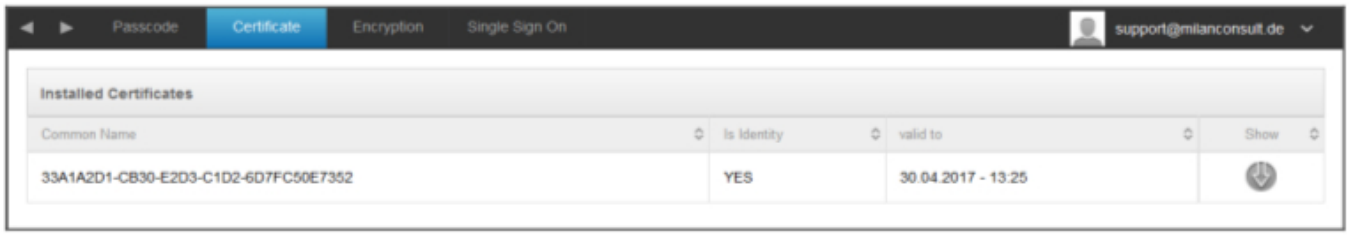
Her foretager du indstillingerne for enhedens adgangskode

Deaktivering af kode tilladt	Når denne indstilling er aktiveret, bliver man ikke bedt om at indtaste en adgangskode. Så snart en adgangskode er etableret, kan den ikke deaktiveres.
Tillad simpel værdi	Tillad brugeren at bruge de samme, eskalerende og reducerende talstrenge (f.eks. 1234, 1111)
Kræver alfanumerisk værdi	Adgangskoder skal indeholde mindst ét bogstav
Minimumslængde på adgangskoden	Minimal længde på adgangskode
Minimum antal komplekse tegn	Minimalt antal alfanumeriske symboler i adgangskoden
Maksimal alder på adgangskoden	Antal dage, hvorefter adgangskoden skal ændres
Maksimal autolås	Maksimal tid, hvorefter enheden er låst
Maksimal afdragsfri periode for enhedslås	Tid, hvorefter enheden går ind i låst Stand-By
Maksimalt antal mislykkede forsøg	Fastsætter, hvor ofte en adgangskode kan indtastes forkert, før en komplet sletning af enheden vil blive udført
Maksimal alder på adgangskoden (1-730 dage)	Maksimal alder på adgangskode
Adgangskodehistorik (1-50 adgangskoder)	Det er tilladt at bruge en gammel adgangskode efter dette nummer.

Et klik på papirkurven åbner dialogen Password-Reset, hvor en glemt adgangskode til enheden kan slettes.

Certifikat (kun på enhedsniveau)

Viser de certifikater, der er tilgængelige på enheden


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

Kryptering

Kræv kryptering af lagerplads	Aktivér den installerede enheds krypteringsfunktion

Enkelt sign-on

Under punktet "Single Sign-On" kan du konfigurere Kerberos-godkendelsen.

Her opretter du adgangsoplysningerne og de respektive URL'er/apps, der har tilladelse til at bruge Kerberos-tokens.

Tilgængelig i overvåget tilstand	
Kontonavn	Kontonavn
Hovednavn	Unik identitet, som Kerberos-billetter kan distribueres til
Riget	Din Kerberos Realm, der skal bruges (f.eks. dit domæne)

Med symbolet kan du oprette flere URL'er.

URL-mønster brugt til at begrænse denne konto	URL'er, som Kerberos-billetter kan distribueres til, skal fastlægges

Med symbolet kan du oprette flere apps.

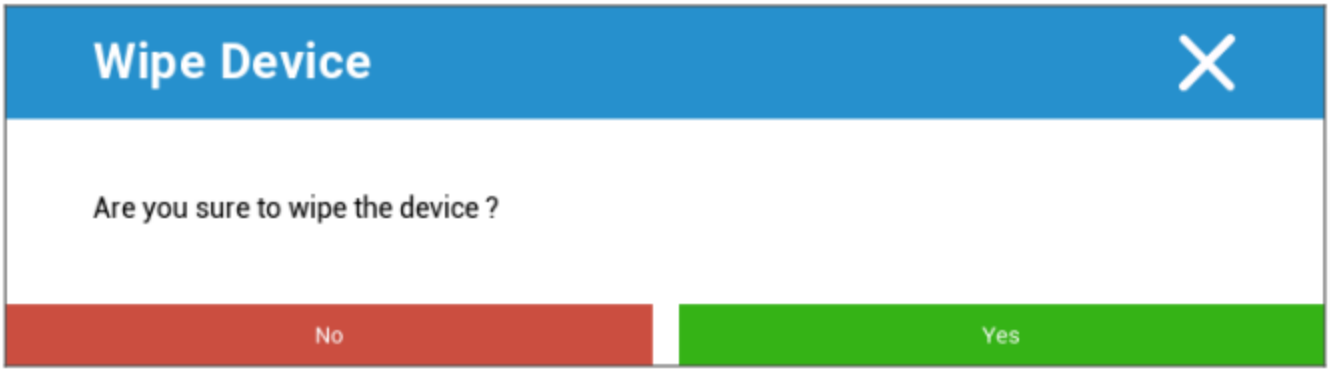
Apps til at begrænse denne konto	Skal bestemmes Apps, som Kerberos-billetter kan distribueres til

End of Life (kun på enhedsniveau)

Tør (kun på enhedsniveau)

Under "Wipe" kan du gendanne enheden til dens fabriksindstillinger. Her slettes både virksomhedsdata og private data på slutbrugerens enhed.

Med et klik på "Minus-symbolet" bør du få følgende besked



Med "Ja" kan du udføre aftørringen.

Under "Wipe Report" kan følgende elementer vises

Slettet af	Historien om, hvem der udførte tørringen
Dato	Dato
Status	Status (f.eks. hvis Wipe blev udført med succes)

Begrænsningsindstillinger

Enhedens funktionalitet

Her kan du blokere individuelle funktioner på slutbrugerens enhed

Tillad installation af apps	Tillad installation af apps
Tillad kamera	Tillad brug af kameraet
Tillad FaceTime	Tillad FaceTime
Tillad skærmoptagelse	Tillad skærmoptagelse
Tillad automatisk synkronisering under roaming	Tillad automatisk synkronisering under roaming
Tillad Siri	Tillad Siri
Tillad stemmeopkald	Tillad stemmeopkald
Tillad køb i appen	Tillad køb i appen
Kræv adgangskode til iTunes Store for alle køb	Kræv adgangskode til iTunes Store for alle køb
Tillad multiplayer-spil	Tillad multiplayer-spil
Tillad tilføjelse af Game Center-venner	Tillad tilføjelse af Game Center-venner
Tillad åbning fra managed til unmanaged	Tillad åbning af indhold i administrerede apps i ikke-administrerede apps
Tillad åbning fra unmanaged til managed	Tillad åbning af indhold i ikke-administrerede apps i administrerede apps
Tillad visning af i dag på låseskærmen	Når denne indstilling er aktiv, vises visningen "I dag" i meddelelsescentret på låseskærmen.
Tillad kontrolcenter på låseskærmen	Tillad Kontrolcenter på låseskærmen
Tillad TouchID	Tillad TouchID
Tillad over-the-air PKI-opdateringer	Tillad over-the-air PKI-opdateringer
Tillad passbook, mens den er låst	Tillad passbook, mens enheden er låst

Begræns sporing af annoncer	Denne funktion deaktiverer Ad Tracking (f.eks. kan annoncører ikke bruge Ad Tracking til at distribuere personaliserede annoncer)
Tillad overdragelse	Tillad overdragelse
Tillad internetresultater i spotlight	Tillad internetresultater i spotlight (f.eks. Bing eller Wikipedia)
Kræver adgangskode ved første AirPlay-parring	Kræver adgangskode ved første AirPlay-parring
Force Watch håndledsbeskyttelse	Hvis den er aktiveret, tvinges Apple Watch til at bruge "Wrist Protection" (håndledsgenkendelse).
Tillad iCloud Photo Library	Tillader iCloud Photo Library. Hvis det ikke er tilladt, slettes alle billeder, der ikke blev downloadet fuldstændigt fra iCloud, på det lokale lager.
Tilgængelig i overvåget tilstand	
Tillad ændring af konto	Tillad ændring af "mail, kontakter, kalender"
Tillad AirDrop	Tillad AirDrop
Tillad ændring af appen på mobilen	Denne indstilling blokerer indstillingen for, hvilke apps der har lov til at bruge mobildata Denne indstilling kan f.eks. indstilles manuelt på slutbrugerens enhed, og derefter kan denne begrænsning aktiveres.
Tillad Siri at spørge efter brugergenereret indhold fra nettet	Websøgning på visse hjemmesider er blokeret, f.eks. Wikipedia, fordi alle kan lave ændringer, som de vil.
Aktivér Siri-filter for bandeord	Bandeord, der er rettet mod Siri, bliver censureret
Tillad iBook Store	Tillad iBook Store
Tillad erotik i iBook Store	Tillad erotik i iBook Store
Tillad ændring af indstillinger for Find mine venner	Tillad ændring af indstillinger for Find mine venner
Tillad Game Center	Tillad Game Center
Tillad parring af værter	Parring af kontrolcomputer
Tillad installation af konfigurationsprofiler	Tillad installation af konfigurationsprofiler
Tillad fjernelse af app	Fjernelse af kontrolapps
Tillad iMessage	Tillad iMessage

Tillad sletning af alt indhold og alle indstillinger	Tillad sletning af alt indhold og alle indstillinger
Tillad konfiguration af begrænsninger	Tillad konfiguration af begrænsninger
Tillad podcast	Tillad podcast
Tillad opslag i definition	Tillad opslag i definition
Tillad prædiktivt tastatur	Tillad prædiktivt tastatur
Tillad automatisk korrektion	Tillad automatisk korrektion
Tillad installation af UI-apps	Hvis den er deaktiveret, kan der ikke installeres apps fra den offentlige AppStore (ikonet vises ikke længere). Apps kan dog stadig installeres via iTunes og Configurator.
Tillad tastaturgenveje	Tillad tastaturgenveje, hvis enheden er tilsluttet et fysisk tastatur
Tillad parring af Apple Watch	Forhindrer en parring mellem enheden og Apple Watch, eksisterende forbindelser vil blive afbrudt
Tillad ændring af adgangskode	Hvis det ikke er tilladt, kan ingen adgangskode til enheden tilføjes, ændres eller fjernes.
Tillad ændring af devicenavn	Retningslinje for at afgøre, om enhedens navn kan ændres
Tillad ændring af tapet	Retningslinje for at afgøre, om tapetet kan ændres
Tillad automatiske app-downloads	Hvis den er deaktiveret, vil en købt app ikke automatisk blive installeret på andre enheder. Gælder ikke for opdateringer til eksisterende apps
Tillad nyheder	Tillad nyheder på iOS-enheden
Tillad tillid til Enterprise-apps	Hvis indstillet til false, forhindrer det tillid til virksomhedsapps

iCloud

Bloker visse funktioner under iCloud-parring

Tillad sikkerhedskopiering	Tillad sikkerhedskopiering
Tillad synkronisering af dokumenter	Tillad synkronisering af dokumenter
Tillad fotostream	Tillad fotostream
Tillad delt fotostream	Tillad delt fotostream
Tillad synkronisering af nøgleringe i skyen	Tillad synkronisering af nøgleringe i skyen
Tillad administrerede apps at gemme data	Tillad administrerede apps at gemme data
Tillad synkronisering af noter og højdepunkter for virksomhedsbøger	Tillad synkronisering af noter og højdepunkter for virksomhedsbøger
Tillad backup af virksomhedens bøger	Tillad backup af virksomhedens bøger

Sikkerhed og privatliv

Bloker disse funktioner i forbindelse med diagnostiske data

Gør det muligt at sende diagnostiske data til Apple	Gør det muligt at sende diagnostiske data til Apple
Tillad brugeren at acceptere ikke-betroede TLS-certifikater	Tillad brugeren at acceptere ikke-betroede TLS-certifikater
Fremtving krypterede sikkerhedskopier	Fremtving krypterede sikkerhedskopier

BYOD

Indbygget iOS-sikkerhed (container)

iOS har altid været i stand til at skelne mellem managed (business) og unmanaged (private). Alt, hvad der kommer fra MDM-systemet, behandles som administreret. Hvis du f.eks. installerer en app via MDM eller konfigurerer en Exchange-konto, vil dette blive behandlet som administreret af iOS.

Alt andet, der bliver konfigureret/installeret manuelt på enheden, vil blive behandlet som ikke-administreret. F.eks. hvis brugeren selv installerer WhatsApp, eller hvis han tilføjer en Exchange-konto. Denne adskillelse har dog aldrig påvirket kontakterne. Men siden iOS 11.3 (og nyere) er dette også blevet tilføjet for kontakterne.

Da dette er en grundlæggende funktion i operativsystemet, behøver du ikke at installere noget eller opsætte en særlig container.

Aktivér den indbyggede funktion til at adskille private og forretningsmæssige apps/informationer/filer. Denne indstilling vil også deaktivere nogle andre funktioner, som ellers kunne slå dele af denne adskillelse fra ved en fejltagelse.

Aktivering

Aktivér de container-løsninger, der understøttes af AppTec360

Aktivér Google Divide Container	Aktivér Google Divide Container
Aktivér SecurePIM Container	Aktivér SecurePIM Container

Hvis du har aktiveret SecurePIM Container, finder du også følgende punkt under "Aktivering". Derudover åbnes der med det samme fire faner mere, som beskrives nedenfor.

E-mail-adresse til support	Support-e-mailadresse, hvor en bruger kan henvende sig med problemer

SecurePIM-adgangskode

Under "SecurePIM Password" kan du fastlægge retningslinjerne for passwordets sikkerhedsstyrke.

Sessionens timeout	Her kan du bestemme, efter hvor mange minutter en ny adgangskode skal indtastes igen, når SecurePIM kører i baggrunden.
Længde på adgangskode	Længde på adgangskode til adgang til SecurePIM Container
Store bogstaver	Minimum store bogstaver
Små bogstaver	Minimum små bogstaver
Særlige tegn	Minimum af specialtegn
Cifre	Mindste antal cifre
Tørre applikation	Antal gange, en adgangskode kan indtastes forkert, før SecurePIM-indholdet slettes (Appen forbliver dog stadig på slutbrugerens enhed)

SecurePIM-sikkerhed

Under "SecurePIM Security" kan du foretage en række forskellige sikkerhedsindstillinger.

Opdag jailbreakede enheder	Hvis denne indstilling er aktiveret, vil adgangen til SecurePIM Container blive blokeret, så snart enheden registreres som jailbreaket.
Sikre tekstfelter	Indholdet af indsendelsesfelterne bliver krypteret, så ingen oplysninger når frem til operativsystemet (iOS). Bemærk: Så længe denne indstilling er aktiv, er autokorrektur ikke længere tilgængelig.
Eksporter kontaktdata til enhed	Hvis denne indstilling er aktiveret, kan brugeren eksportere Exchange-kontakterne til sin lokale enhed. Bemærk: Kun navn og telefonnummer eksporteres.
Vis arrangementets placering	Hvis denne indstilling er aktiveret, vil placeringen af de kommende begivenheder blive vist i meddelelseslinjen.
Vis begivenhedens titel	Hvis denne indstilling er aktiveret, vises placeringen af titlen på den kommende begivenhed i meddelelseslinjen.

SecurePIM-browser

Her kan du konfigurere browseren til SecurePIM.

Med symbolet kan du definere en ny URL.

Med symbolet kan du fjerne en defineret URL igen.

"Hvidlistede URL'er" er URL'er, der kan indlæses.

"Blacklistede URL'er" er URL'er, der ikke kan indlæses og derfor er blokeret.

Vær opmærksom på, at hvidlisteposter har højere prioritet end sortlisteposter. Under "Bogmærketitel" kan du udstede en titel. Med "Bogmærke-URL" kan du knytte en URL-adresse til bogmærketitlen - på den måde kan du distribuere individualiserede bogmærker til de respektive brugere.

Udveksling

Under "Exchange" kan du konfigurere en Exchange-konto.

ActiveSync e-mailadresse	Exchange-e-mailadresse (bemærk "pladsholderne")
ActiveSync Exchange-login	Udveksl brugernavne (læg mærke til "pladsholderne")
ActiveSync Exchange Server	Exchange Server-adresse (FQDN)
ActiveSync Exchange-domæne	Exchange-domæneadresse
Brugercertifikat	Brugercertifikat
Certifikatbaseret autentificering	Brugeren autentificerer sig selv med et certifikat
Tillad S/MIME-kryptering	Giver brugeren mulighed for at kryptere sin mail
Tillad S/MIME-signering	Giver brugeren mulighed for at underskrive sin mail
CRL-kontrol	Hvis det er aktivt, vil det private certifikat blive sammenlignet med CRL (Certificate Revocation List).

Håndtering af forbindelser

Wi-Fi

Identifikator for servicesæt (SSID)	SSID for det netværk, der skal tilsluttes
Automatisk tilslutning	Aktivér automatisk tilslutning, når du tilslutter dig et netværk
Skjult netværk	Aktivér, hvis AP'et ikke udsender SSID'et

Proxy-opsætning

Konfiguration af en proxy for hvert adgangspunkt

Ingen		Opret ingen fuldmagt
Manuel		Opret en manuel proxy
	URL til proxyserver	Adresse for adgang til proxyindstillinger
	Havn	Fastlæg porten til proxyen
	Autentificering	Brugernavn til godkendelse på proxyen
	Adgangskode	Adgangskode til godkendelse på proxyen
Automatisk		Opret automatisk en proxy
URL til proxyserver		URL til adgang til proxyindstillingerne

Sikkerhedstype

Etablering af sikkerhedstype for AP'et

WEP	
Adgangskode	Adgangskode til AP'et

WPA/WPA2	
Adgangskode	Adgangskode til AP'et

WEP Enterprise - WPA / WPA2 Enterprise - Any Enterprise			
	Protokoller		
	TLS	Aktiver/Deaktiver	
	TTLS	Aktiver/Deaktiver	
	LEAP	Aktiver/Deaktiver	
	PEAP	Aktiver/Deaktiver	
	EAP-FAST	Aktiver/Deaktiver	
	EAP-SIM	Aktiver/Deaktiver	
	Brug PAC		Brug af PAC (Protected Access Controll)
	Tilvejebringelse af PAC	Konfiguration af Provision PAC	
	Tilvejebringelse af PAC anonymt	Anonym levering af PAC	
	Indre godkendelser	Autentificeringsprotokol, der skal bruges: PAP, CHAP, MSCHAP, MSCHAPv2	
	Brugernavn	Brugernavn til autentificering	
	Brug ikke adgangskode pr. forbindelse	Brug ikke adgangskode pr. forbindelse	
	Identitetscertifikat	Upload/vælg godkendelsescertifikat	
	Ydre identitet	Identitet, der kan ses udefra	
	Tillid		
	Betroet certifikat 1	Upload det første betroede certifikat	
	Betroet certifikat 2	Upload det andet betroede certifikat	
	Betroet certifikat 3	Upload et tredje betroet certifikat	
	Navne på betroede servercertifikater	Navnene på de forventede servercertifikater (i en kommasepareret liste)	

Ingen	Etablerer ingen sikkerhed

VPN

Navn på forbindelse	Navn på VPN-profilen

VPN-type

VPN

Al enhedens netværkstrafik vil blive dirigeret via en VPN-forbindelse.

Tilslutningstype	Etablering af VPN-forbindelsestype
IPsec (cisco)	IPsec-protokol fra Cisco
PPTP	PPTP-protokol
L2TP	L2TP-protokol
Cisco AnyConnect	AnyConnect-protokol
Juniper SSL	Juniper SSL-protokol
F5 SSL	F5 SSL-protokol
SonicWall mConnect	SonicWall mobile Connect
Aruba VIA	Aruba VIA-protokol
Brugerdefineret SSL	Forbindelse via brugerdefineret SSL
OpenVPN	OpenVPN-protokol

VPN pr. app

Når du åbner en bestemt app, vil der blive oprettet en VPN-forbindelse

Start automatisk VPN-forbindelse pr. app		Start automatisk VPN-forbindelse pr. app
Tilslutningstype		Etablering af VPN-forbindelsestype
	Cisco AnyConnect	AnyConnect-protokol
	Juniper SSL	Juniper SSL-protokol
	F5 SSL	F5 SSL-protokol
	SonicWall mConnect	SonicWall mobile Connect
	Aruba VIA	Aruba VIA-protokol
	Brugerdefineret SSL	Forbindelse via brugerdefineret SSL
	OpenVPN	OpenVPN-protokol

Proxy-opsætning

Konfiguration af en proxy til VPN-forbindelsen

Ingen	Opret ingen fuldmagt
Manuel	Opret en proxy manuelt
URL til proxyserver	Adresse for adgang til proxyindstillinger
Havn	Fastlæg porten til proxyen
Autentificering	Brugernavn til autentificering på proxyen
Adgangskode	Adgangskode til autentificering på proxyen
Automatisk	Opret automatisk en proxy
URL til proxyserver	URL til adgang til proxyindstillingerne

Vis pladsholdere	Viser alle tilgængelige brugervariabler, som AppTec360 kan bruge

APN

Navn på adgangspunkt	Navn på adgangspunkt
Adgangspunktets brugernavn	Adgangspunktets brugernavn
Adgangspunktets adgangskode	Adgangspunktets adgangskode
Proxy-server	Proxyserver-adresse
Havn	Den respektive proxy-port

Cellulær

Aktivér dataroaming	Aktivér dataroaming
Aktivér stemme-roaming	Aktivér stemme-roaming
Aktivér hotspot	Aktivér hotspot

HTTP-proxy

Proxy-type	
Manuel	Opret en proxy manuelt
URL til proxyserver	Adresse for adgang til proxyindstillingerne
Havn	Etablering af proxy-port
Autentificering	Brugernavn til autentificering på proxyen
Adgangskode	Adgangskode til autentificering på proxyen
Automatisk	Opret automatisk en proxy
Proxy PAC-URL	Proxy PAC-URL
Tillad direkte forbindelse, hvis PAC ikke kan nås	Tillad direkte forbindelse (uden VPN), hvis PAC ikke kan nås
Tillad omgåelse af proxy for at få adgang til lukkede netværk	Tillad omgåelse af proxy for at få adgang til lukkede interne netværk

AirPrint

IP-adresse	Printerens IP-adresse
Ressource-sti	En klar vej til AirPrint-enheden

AirPlay

Enhedens navn	Enhedens navn
Adgangskode	Adgangskode til parring
Hvidliste	Definer en liste over enheder, som enheden udelukkende kan parre sig med

PIM-styring

Aktiv synkronisering af Exchange

Kontonavn	Navn på e-mailkonto
Exchange ActiveSync-vært	Adresse/FQDN på serveren
Tillad bevægelse	Tillad flytning af e-mails
Brug kun i mail	Interaktioner kan kun forekomme i den oprindelige Mail-app
Brug SSL	Brug SSL-kryptering
Domæne	Server-domæne
Bruger	Brugernavn
E-mail-adresse	e-mailadresse (kun på enhedsniveau)
Adgangskode (kun på enhedsniveau)	Brugerens adgangskode
Identitetscertifikat	Vælg det respektive certifikat til godkendelse på serveren
Tidligere dage med Mail to Sync	Antal dage, indtil e-mails skal synkroniseres tilbage. Ingen grænse = ubegrænset
Aktivér S/MIME	Aktivér S/MIME-kryptering
Signering af certifikat	Upload det respektive signeringscertifikat
Krypteringscertifikat	Upload det respektive krypteringscertifikat

E-mail

Opsætning af POP3/IMAP-konti på slutbrugerens enhed

Beskrivelse af konto	Navn på e-mail-konti		
Kontotype	IMAP	Stipræfiks	Stipræfikset for særlige mapper
	POP		
Brugerens visningsnavn	Brugerens visningsnavn		
E-mail-adresse	Brugerens e-mailadresse		
Tillad bevægelse	Tillad flytning af e-mails		
Aktivér S/MIME	Aktivér S/MIME-kryptering		
Signering af certifikat	Upload det respektive signeringscertifikat		
Krypteringscertifikat	Upload det respektive krypteringscertifikat		

Indgående post

Indstillinger for indgående server

Mailserver-adresse	Mailserver-adresse
Port til mailserver	Mailserver-port
Brugernavn	Respektive brugernavn
Autentificeringstype	Autentificeringstype
Ingen	Ingen godkendelsestype
Adgangskode (kun på enhedsniveau)	Adgangskode-prompt
MDM-udfordring-svar	
NTLM	NTLM-autentificering
HTTP MD5-digest	
Brug SSL	Brug SSL, hvis det er nødvendigt

Udgående post

Indstillinger for udgående server

Mailserver-adresse	Mailserver-adresse
Port til mailserver	Port til mailserver
Brugernavn	Respektive brugernavn
Autentificeringstype	
Ingen	Ingen godkendelsesmetode
Adgangskode (kun på enhedsniveau)	Adgangskode-prompt
MDM-udfordring-svar	
NTLM	NTLM-autentificering
HTTP MD5-digest	
Brug SSL	Brug SSL, hvis det er nødvendigt
Udgående adgangskode samme som indgående	Udgående adgangskode samme som indgående
Brug kun i mail	Aktivér, hvis alle udgående e-mails skal sendes via Mail-appen

CalDav

Konfigurer opsætning og distribution af en CalDav-konto

Beskrivelse af konto	Visningsnavn på kontoen
Værtsnavn	Værtsnavn og/eller IP-adresse
Havn	Port til CalDav-kontoen
Hoved-URL	Kontoens primære URL
Brugernavn	Respektive CalDav-brugernavn
Adgangskode (kun på enhedsniveau)	Respektive CalDav-adgangskode
Brug SSL	Brug SSL, hvis det er nødvendigt

Abonnerede kalendere

Opsætning og distribution af abonnerede kalendere

Beskrivelse	Visningsnavn på kontoen
URL	URL til kalenderdatabasen
Brugernavn	Brugernavn på kalenderabonnementet
Adgangskode (kun på enhedsniveau)	Adgangskode til kalenderabonnementet
Brug SSL	Brug SSL, hvis det er nødvendigt

LDAP

I dette område skal du oprette en LDAP-forbindelse for at muliggøre en dynamisk certifikatudveksling mellem slutbrugerenheden og Active Directory.

Vær opmærksom på, at den valgte bruger skal have læserettigheder.

Beskrivelse af konto	Beskrivelse af konto
Brugernavn til konto	Bruger til LDAP-adgang
Adgangskode til konto	Adgangskode til LDAP-adgang
Kontoens værtsnavn	LDAP-serverens værtsnavn/IP-adresse
Brug SSL	Brug SSL, hvis det er nødvendigt

I den anden del kan du definere individuelle filtre til søgning i LDAP-registret.

Beskrivelse	Omfang	Søg i basen
Beskrivelse af filter	Søgeniveau i LDAP-registret	Definer det enkelte filter

Webadministration

Webklip

Her kan man definere bogmærker med links til websider, intranetportaler osv., som vil være synlige som en applikation på slutbrugerens enhed.

Etiket	Navn på forbindelsen på slutbrugerens enhed
URL	Link til den respektive hjemmeside
Aftagelig	Hvis den er aktiveret, kan brugeren fjerne webclippet
Ikon	Via denne dialog kan du uploade et logo til forbindelsen: Mål 180x180, png-format
Forudkomponeret ikon	Hvis den er aktiveret, vises der ingen yderligere effekter (skygge, refleksion) på ikonet.
Fuld skærm	Når du åbner webclips, åbnes browseren i fuldskærmstilstand

Filter til webindhold

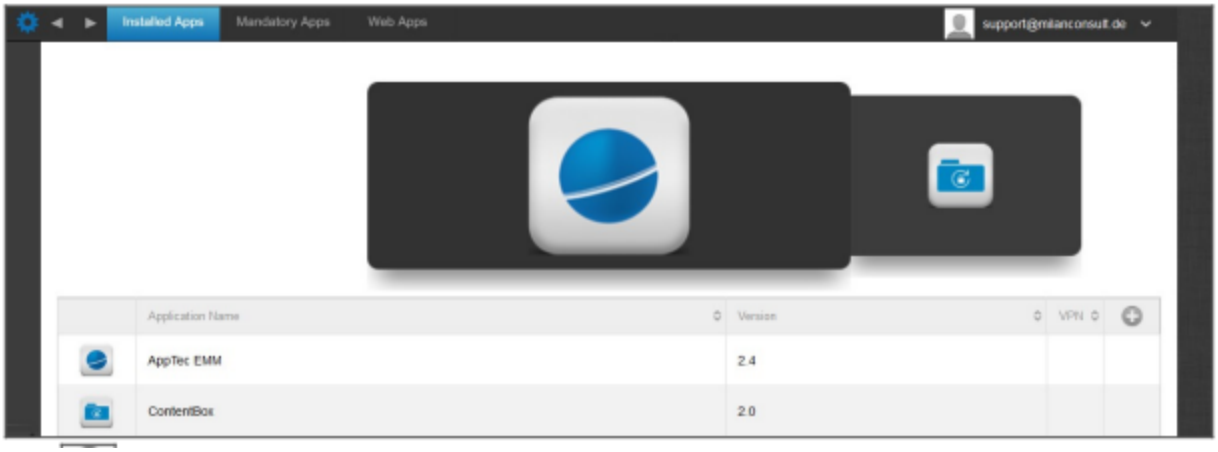
Web Content Filter gør det muligt at begrænse adgangen til bestemte internetsider.

Tilladte hjemmesider	
Begræns voksent indhold	Webfilter anvendes automatisk til voksenindhold
Tilladte URL'er	Tilføj tilladte sider med +-symbolet
Sortlistede webadresser	Tilføj blokerede sider med +-symbolet
Kun specifikke hjemmesider	Der kan kun vises specifikt indhold, som du kan tilføje med +-symbolet.

App-administration

Enterprise App Manager

Installerede apps (kun på enhedsniveau)



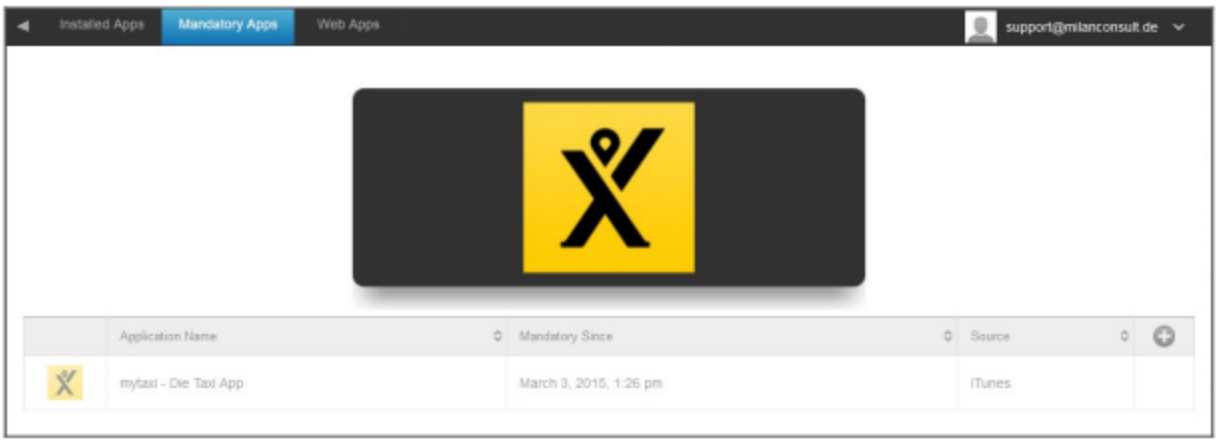
Her kan du se de apps, der i øjeblikket er installeret på enheden.

Obligatoriske apps

Under Obligatoriske apps kan du give tilladelse til nødvendige apps.

Brugeren vil løbende blive mindet om at installere denne app.

Via kan den mandaterede app defineres.



Det kan være en Apple App Store-app, men også en intern app.

Hvis det drejer sig om en overvåget enhed, installeres appen automatisk.

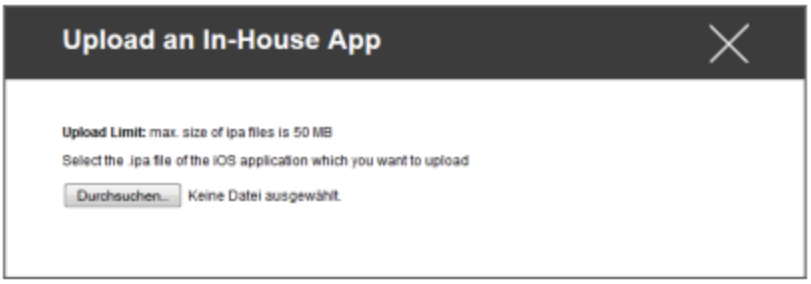
Du kan skubbe en "Apple AppStore"-app fra den offentlige AppStore til enheden, såvel som en internt udviklet In-House-app.

Eller du kan vælge fra kategorien "iOS In-House Apps" og vælge en In-House App, som du har uploadet under Generelle indstillinger.

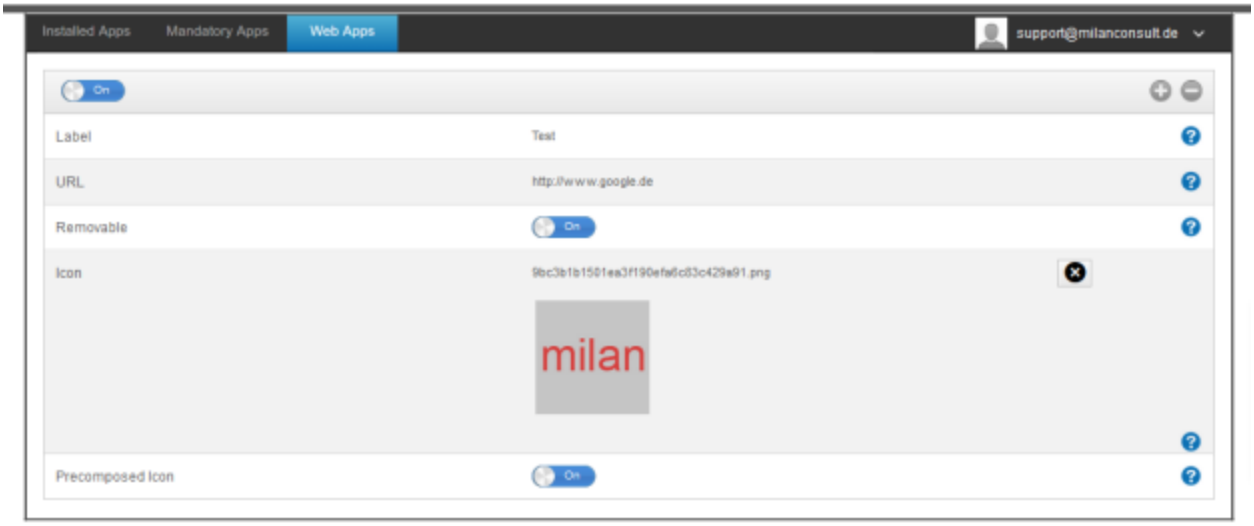
Installations-optioner

Hold dig opdateret (understøttes kun for VPP pr. enhed)	En gang om ugen afgøres det, om der er en opdatering til appen. Hvis ja, vil denne opdatering blive installeret. For interne apps vil det opdateringsmål, du har konfigureret i Generelle indstillinger, blive brugt til opdateringsprocessen.
Overhaler, når den ikke er styret	Hvis appen allerede er installeret, vil MDM overtage appen og administrere den.
Fjern appen, når MDM-profilen fjernes	I tilfælde af fjernelse af enhedshåndtering vil appen blive afinstalleret.
Forhindre sikkerhedskopiering af app-data	Der oprettes ikke en sikkerhedskopi af app-specifikke data
App-indstilling	Under "Appindstillinger" kan du tildele appen visse værdier i forgrunden (så længe appen understøtter det, spørg om nødvendigt appens udvikler).

Du kan også vælge og uploade en ipa-fil direkte via "Upload In-House App".



Web-apps



Under punktet "Web Apps" kan du, på samme måde som med "Web Clips", skubbe internetsider eller intranetportaler som en applikation til slutbrugerens enhed i området Web Management. Som standard vises Web Apps i fuldskærmstilstand, hvilket kan konfigureres under Webclips.

Etiket	Navn på forbindelsen på slutbrugerens enhed
URL	Link til den respektive hjemmeside
Aftagelig	Hvis den er aktiveret, kan brugeren fjerne webclippet
Ikon	Via denne dialog kan du uploade et logo til forbindelsen: Mål 180x180, png-format
Forudkomponeret ikon	Hvis den er aktiveret, vises der ingen yderligere effekter (skygge, refleksion) på ikonet.

Begrænsninger og indstillinger

Sortlistede / hvidlistede apps

Her kan du indstille de apps, der er blokeret (eller tilladt), afhængigt af dine indstillinger i "Generelle indstillinger". Et klik på bringer den kendte app-søgning frem. Her kan du søge efter de apps, du vil tilføje.

Bemærk, at en overvåget enhed er nødvendig for denne funktion.

SysApp-begrænsninger

Bloker specifikke apps eller funktioner på din enhed

Tillad brug af YouTube	Tillad brug af YouTube
Tillad brug af iTunes Store	Tillad brug af iTunes Store
Tillad brug af Safari	Tillad brug af Safari
Aktivér automatisk udfyldning	Tillader automatisk udfyldning
Advarsel om svindel med magt	Styrker advarslen om svindel
Aktivér JavScript	Gør det muligt at bruge JavaScript
Bloker pop-ups	Blokerer alle former for pup-ups
Tillad cookies	Vælg, hvornår Safari skal acceptere cookies

App-VPN

Via symbolet kan du definere programmer, som automatisk starter den valgte VPN-forbindelse ved opstart.

App-indstillinger

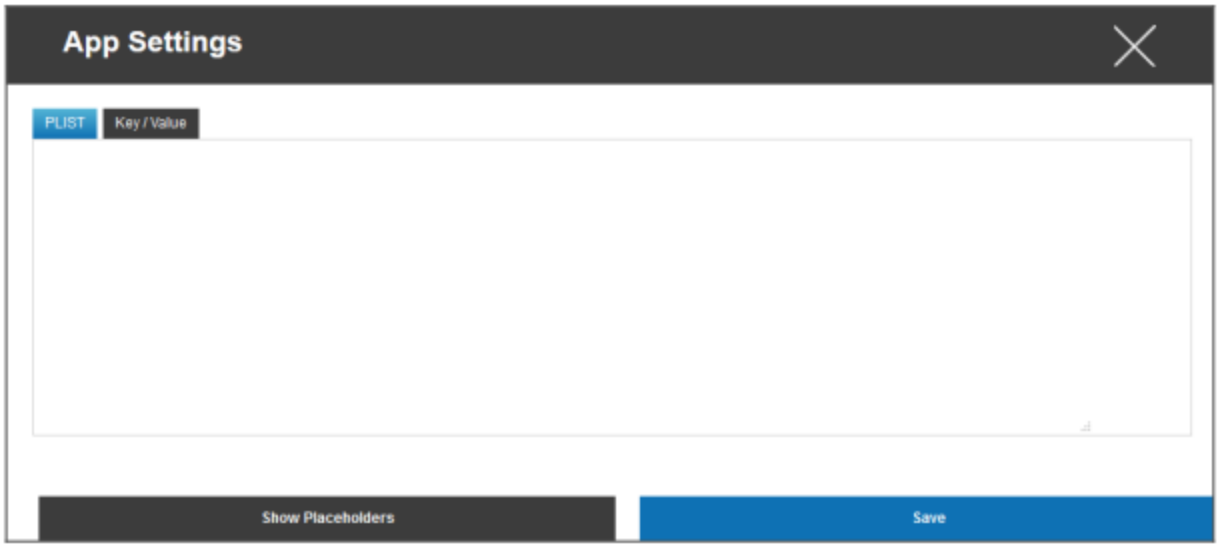
Under "Appindstillinger" kan du tildele appen visse værdier i forgrunden (så længe appen understøtter det, spørg om nødvendigt appens udvikler).

Via symbolet tilføjer du en (ekstra) app. Du vil igen finde den velkendte AppTec360-repræsentation af en App-Import.

Søg her efter den app, du gerne vil konfigurere, og vælg den. Indstillingerne gælder kun for administrerede apps.

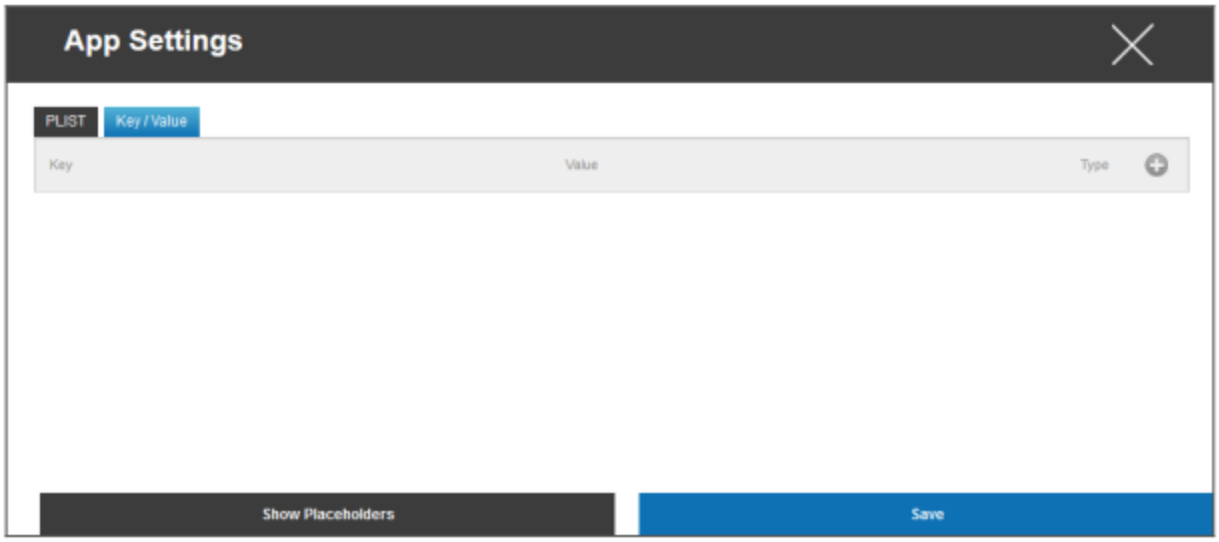
Hvis importen er lykkedes, vil du se følgende display:

Nu kan du med et klik på udføre en række konfigurationer. Du får derefter følgende oversigt:

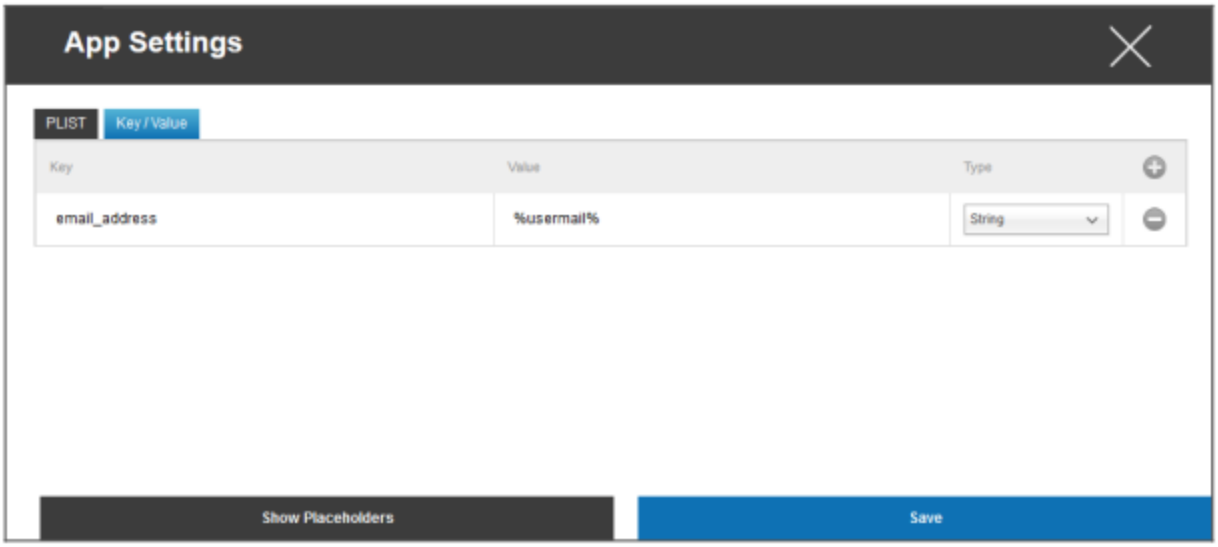


Hvis du allerede har en PLIST (kildetekst til konfigurationen), kan du tilføje den her og gemme det hele med "Save".

Under "Nøgle/værdi" kan du knytte specifikke konfigurationer til appen



Her kan du oprette en ny nøgle og dens værdi med symbolet.



Naturligvis står alle AppTecs pladsholdere til din rådighed

"Type"-forklaring:

Streng	Tekst
Boolsk	Sandt/falsk
Antal	Antal

Med symbolet kan du fjerne en app igen.

Enterprise App Store

iTunes-apps

Under dette punkt kan du distribuere valgfrie apps til din bruger.

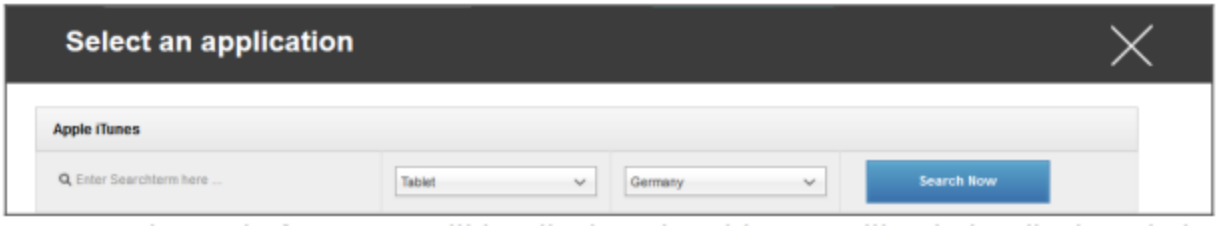
Hvis der er en app her, vil den automatisk blive installeret på AppTec360 Stores slutbrugerenhed.

Det er blot links til den officielle Apple App Store. Af denne grund skal hver slutbrugerenhed være udstyret med et Apple ID.

På dette tidspunkt anbefaler vi, at hver bruger har sit eget Apple ID.

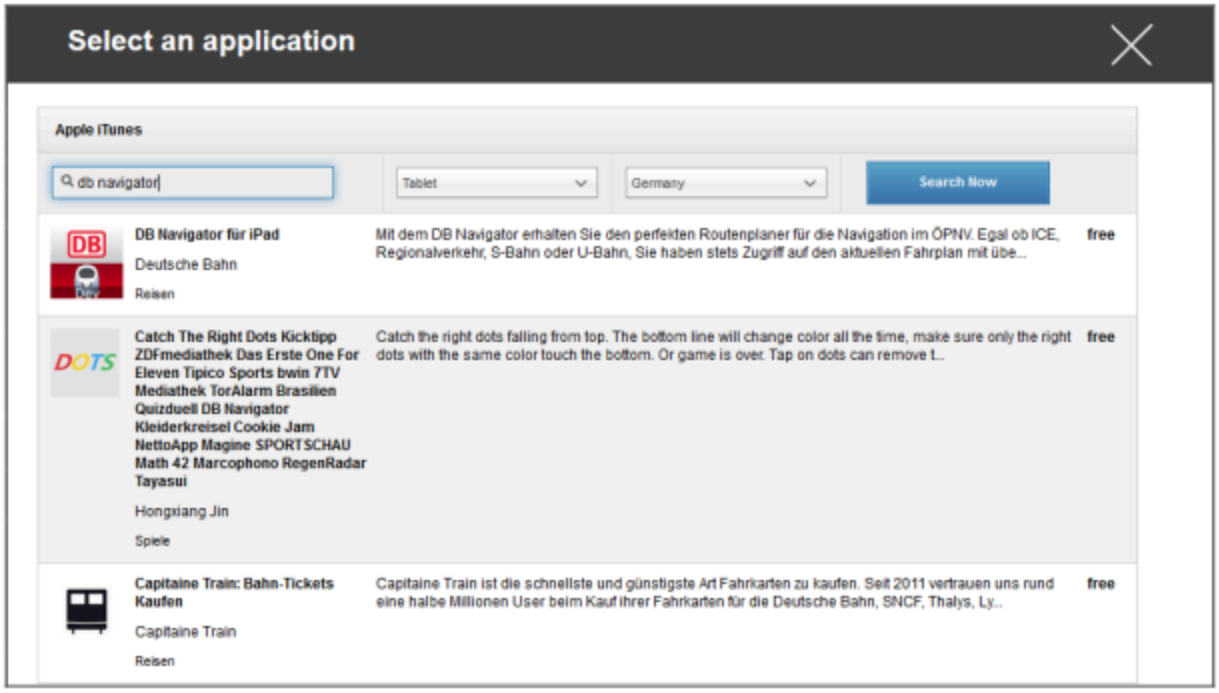
Med symbolet kan du tilføje yderligere apps.

Derefter åbnes et vindue med følgende oversigt.



Bemærk, at kun gratis apps vil blive vist, betalte apps vil kun blive vist via VPN.

Under "Enter Search Term here ..." kan du søge efter en app, der findes i Apple App Store.



Når du klikker på ikonet eller på appens navn, bliver du igen bedt om at udføre yderligere konfigurationer.

Hold dig opdateret	En gang om ugen afgøres det, om der er en opdatering til appen. Hvis ja, vil denne opdatering blive installeret.
Fjern appen, når MDM-profilen fjernes	I tilfælde af fjernelse af enhedshåndtering vil appen blive afinstalleret.
Forhindre sikkerhedskopiering af app-data	Der oprettes ikke en sikkerhedskopi af app-specifikke data
App-VPN	Vælg en VPN-forbindelse, som starter, når du åbner appen

Efter et klik på "Installer" tilføjes appen til Enterprise App Store og kan derefter installeres på slutbrugerens enhed via AppTec360 AppStore.

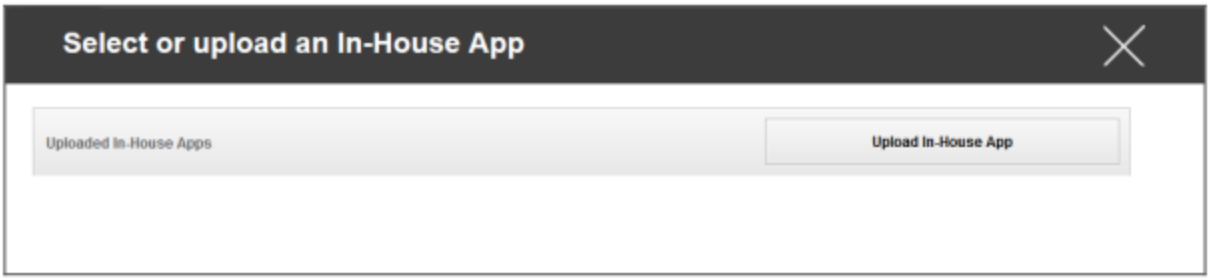
Hvis App-Store-importen er gennemført, får du følgende oversigt:

Internt

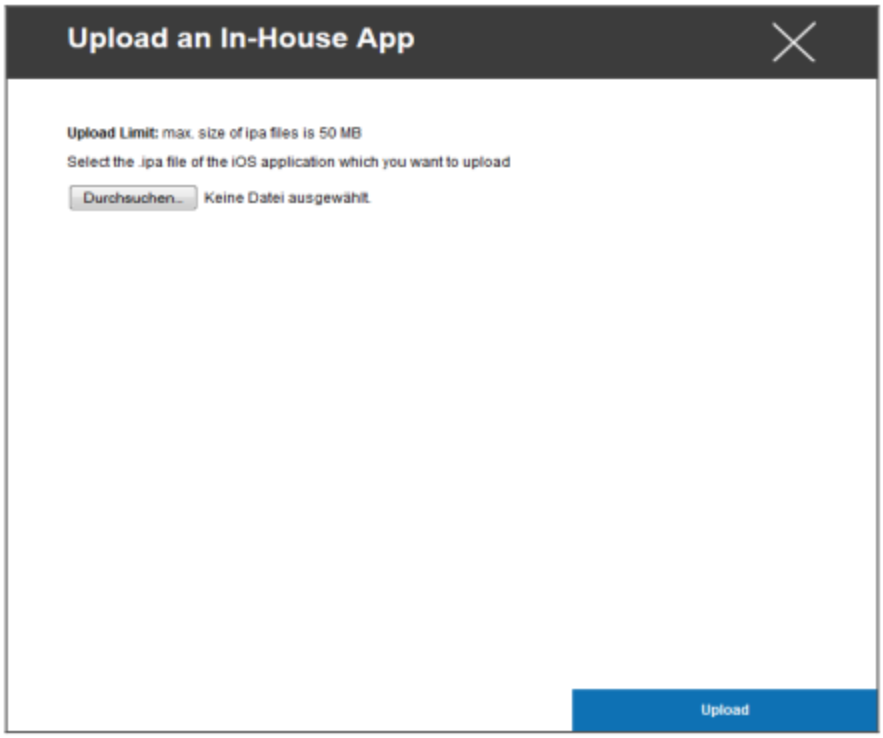
Under punktet "In-House" kan du uploade internt udviklede apps og distribuere dem.

Med symbolet kan du distribuere yderligere In-House Apps.

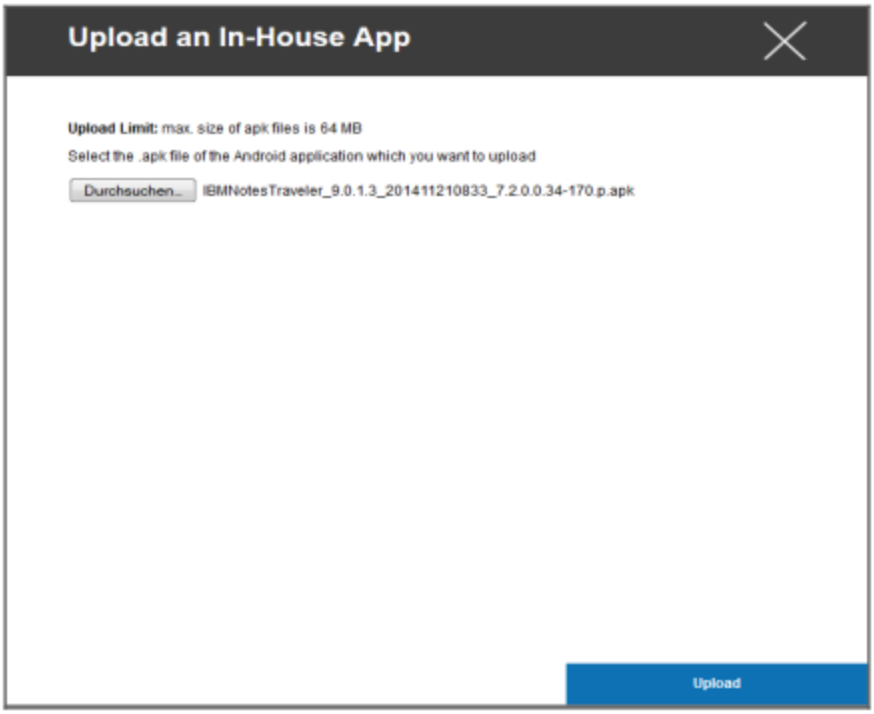
Hvis du aldrig har distribueret In-House App, får du følgende oversigt:



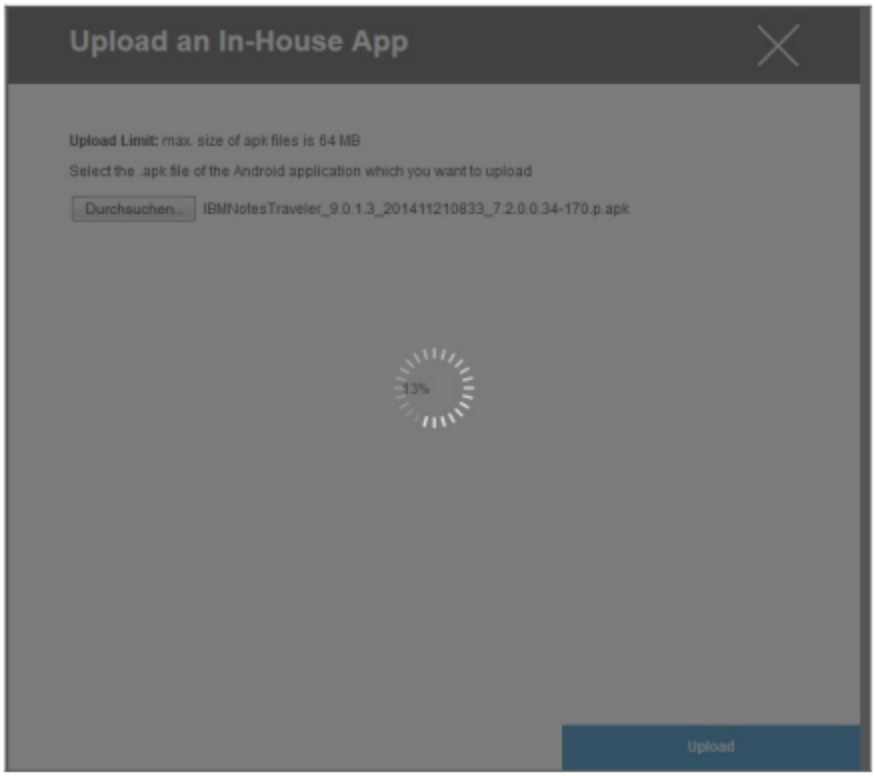
Klik på "Upload In-House App", så får du følgende oversigt:



Vælg nu en .ipa-fil med "Søg...", og klik derefter på "Upload".



Din app vil nu blive uploadet. I midten af cirklen kan du se procentdelen af, hvor meget af din app, der allerede er uploadet.



Hvis uploaden af den interne app er lykkedes, vil du se den nyligt uploadede app i dit app-katalog.

Brugeren har nu mulighed for at se og installere denne app i AppTec360 Store på slutbrugerens enhed under kategorien "In-House".

Da der ikke er tale om en offentlig Apple AppStore-app, har brugeren ikke brug for et gemt Apple-id på slutbrugerens enhed.

Kiosk-tilstand

iOS Kiosk Mode er kun tilgængelig i Supervised Mode

Kiosk-tilstanden giver dig mulighed for at forhåndsdefinere en app eller URL, så det udelukkende er muligt at køre/besøge denne app/URL.

Derudover kan du deaktivere forskellige hardwareknapper i Kiosk Mode.

Applikationstype

Pakke

Hvis du vil starte appen i kiosktilstand, skal du vælge "Pakke" under "Applikationstype".

Kiosk-applikation	Klik her for at vælge en app, der skal starte i Kiosk Mode Her finder du den aktuelle oversigt over App Management Du kan vælge mellem "Apple iTunes Apps" og "iOS In-House Apps"

URL

Hvis du vil starte en URL i kiosktilstand, skal du vælge "URL" under "Applikationstype".

URL	Nu skal du definere den ønskede URL-adresse
Politik for samme oprindelse	Hvis denne funktion er aktiv, kan brugeren kun surfe på undersiderne til den foruddefinerede URL. Hvis du for eksempel har defineret følgende URL: www.mypage.com, så kan brugeren surfe på www.mypage.com/subpage
Hvidlistede webadresser	Her kan du vedligeholde en hvidliste, hvor alle disse URL'er er tilladt Maksimalt 1 URL pr. linje En URL skal starte med http:/ eller https://
Sortlistede webadresser	Her kan du vedligeholde en sortliste, hvor alle disse webadresser ikke er tilladt Maksimalt 1 URL pr. linje En URL skal starte med http:/ eller https://
Ryd browseren efter inaktivitet	Efter inaktivitet vil browserens cache blive tømt
Afslut adgangskode aktiveret	Hvis du aktiverer denne funktion, har brugeren mulighed for at afslutte Kiosk Mode med en adgangskode, som du har defineret på forhånd.
Afslut adgangskode	Dette er den adgangskode, som du har defineret på forhånd.

Indstillinger for kiosktilstand

Planlagt kiosktilstand	Baseret på tidspunktet på dagen kan du indstille kiosktilstanden, så den starter og slutter automatisk på et tidspunkt, der er forudbestemt.
Starttidspunkt	Starttidspunkt
Tid i minutter	Tid i minutter, hvorefter Kiosk Mode skal afsluttes igen
Deaktiver berøring	Hvis aktiveret, er berøringsskærmen deaktiveret
Deaktiver enhedens rotation	Hvis den er aktiveret, deaktiveres den automatiske skærmtilpasning.
Deaktivering af ringetone	Hvis den er aktiveret, vil ringekontakten blive deaktiveret. Fra da af afhænger adfærden af den tidligere indstillede funktion
Deaktiver lydstyrkeknapper	Hvis den er aktiveret, deaktiveres lydstyrkeknapperne.
Deaktiver knappen Sleep Wake	Hvis den er aktiveret, vil tænd/sluk-kontakten blive deaktiveret.
Deaktiver automatisk låsning	Hvis den er aktiveret, skifter enheden ikke til standby.
Aktivér Voice Over	Hvis den er aktiveret, vil Voice Over-assistenten blive aktiveret
Aktivér zoom	Hvis den er aktiveret, vil zoomen blive aktiveret
Aktivér inverterede farver	Hvis den er aktiveret, vil den omvendte visningstilstand blive aktiveret.
Aktivér assisterende berøring	Hvis den er aktiveret, vil AssistiveTouch blive aktiveret
Aktiver valg af tale	Hvis aktiveret, vil talevalget blive aktiveret
Aktivér monolyd	Hvis den er aktiveret, vil Mono Audio blive aktiveret.
VoiceOver	Hvis den er aktiveret, kan brugeren aktivere VoiceOver
Zoom	Hvis den er aktiveret, kan brugeren aktivere Zoom
Inverter farver	Hvis den er aktiveret, kan brugeren aktivere inverterede farver
Hjælpende berøring	Hvis den er aktiveret, kan brugeren aktivere assisterende berøring

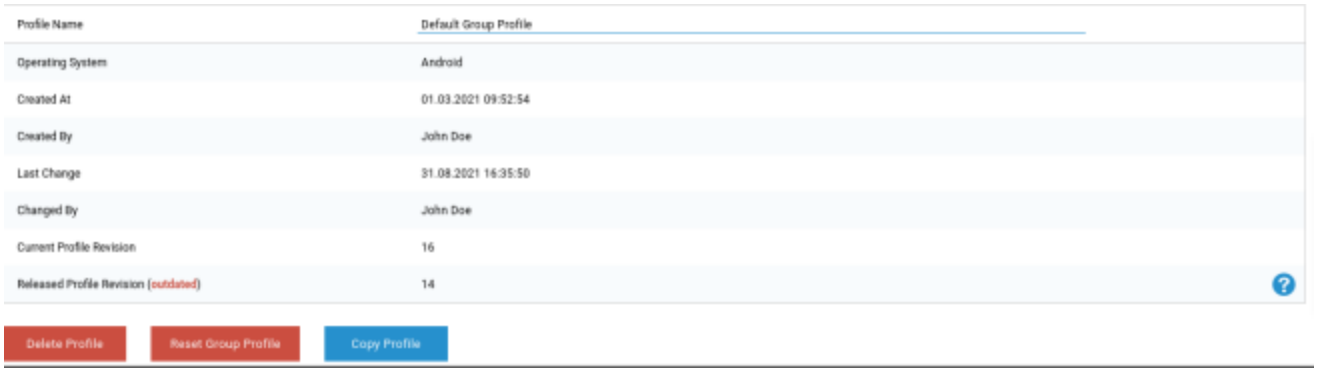
Android Enterprise – Fuldt administreret enhedskonfiguration

Afhængigt af om du i øjeblikket har valgt en gruppeprofil eller en enhed, er oversigten og dens underpunkter forskellige - vær opmærksom på dette!

Generelt

Oversigt over gruppeprofiler (kun på gruppeniveau)

Når du åbner en gruppeprofil, får du et hurtigt overblik over profilen.



Navn på profil	Navn på profilen (kan ændres her)
Operativsystem	Operativsystem, som profilen er til
Oprettet på	Tidspunkt for skabelse
Oprettet af	Profilens skaber
Sidste ændring	Tidspunkt for sidste ændring af profilen
Ændret af	Konto, der foretog de sidste ændringer
Nuværende profilrevision	Revision af gemt profiltilstand
Udgivet profilrevision	Tildelt profilrevision ("Tildel nu"). Hvis etiketten viser "(forældet)" bag teksten, betyder det, at du har gemt profilen, men ikke tildelt den endnu, så enhederne vil stadig få en ældre version.

Enhedsoversigt (kun på enhedsniveau)

Hvis du er på en enhed, får du en oversigt over den valgte enhed, som indeholder følgende:

Enhedens navn	Enhedens navn
Beliggenhed	Koordinater for placering
Telefonnummer	Telefonnummer
Tildelte obligatoriske apps	Antal tildelte obligatoriske apps
OS-version	Enhedens OS-version
Operativsystem	Operativsystem (Android Enterprise)
Serienummer	Enhedens serienummer
Ejerskab af enhed	Virksomheds- eller privat enhed
Enhedstype	AE-arbejdsstyret enhed
Rodfæstet	Status, der angiver, om enheden er blevet rootet
Overensstemmende	Overholder retningslinjerne
IP-adresse	Enhedens IP-adresse
Sidst set	Tidspunkt, hvor enheden sidst havde forbindelse til AppTec
Sidste skub	Tidspunkt, hvor det sidste push blev sendt til enheden
AE Enhedsejertilstand	Ja
Brugertildeling	Den bruger eller gruppe, som denne enhed er tildelt

Config Revision (kun på enhedsniveau)

Her får du en oversigt over, hvilken gruppeprofil der er tildelt enheden.

Hvis du klikker på gruppeprofilen, får du direkte adgang til denne profil, og du kan foretage indstillinger.

Med dette symbol kan du gendanne de distribuerede apps til gruppeprofilens indstillinger.

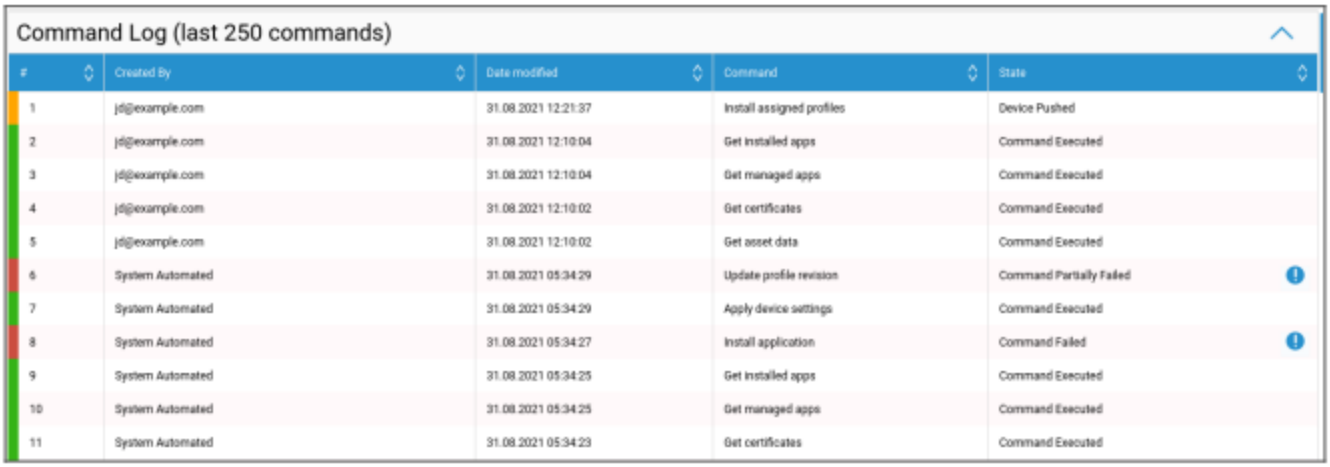
Med dette symbol kan du sætte alle de anvendte apps tilbage til gruppeprofilens indstillinger.

"Nyere revision tilgængelig" angiver, at gruppeprofilen er blevet ændret og gemt, men ikke tildelt. Gruppeprofilen skal tildeles med "Tildel nu" på gruppeniveau for at anvende ændringerne på enhederne.

Enhedslog (kun på enhedsniveau)

Kommando-log

Her kan du se, hvilke kommandoer der er udstedt til enheden, og hvad deres status er.



Kommandoer, der er oprettet af "System Automated", oprettes automatisk af systemet.

Mulige kommandostatusser

Enhed skubbet	Der er sendt en push-anmodning til push-tjenesten (f.eks. APNS) for at fortælle enheden, at den skal oprette forbindelse tilbage til EMM-serveren.
Kommando oprettet	Kommandoen blev oprettet i systemet.
Kommando sendt	Kommandoen blev sendt til enheden, efter at den havde oprettet forbindelse til serveren.
Kommando udført	Kommandoen blev udført med succes.
Kommando mislykkedes	Kommandoen mislykkedes. *
Kommando delvist mislykket	Afhængigt af enhedens operativsystem kan nogle kommandoer blive grupperet sammen. Nogle dele af denne kommandogruppe mislykkedes. *
Kommandoen blev udført, men mislykkedes til sidst	Kommandoen blev udført, men måske blev den ikke.
Kommando genindført	Kommandoen blev repushed af en bruger.
Kasseret	Kommandoen blev kasseret. For eksempel fordi den blev erstattet af en anden kommando, eller fordi enheden blev genindskrevet, og gamle kommandoer blev fjernet.

Hvis der er et udråbstegn bag beskeden, kan du få flere oplysninger ved at holde markøren over ikonet.

Enhedsindstillinger

Konfiguration af klienter

Her kan du udføre følgende konfigurationer på din Android-enhed:

Tid for manglende overholdelse	Tidsgrænsen for brugersvar, efter hvilken håndhævelseshandlingen anvendes.
Håndhævelse efter timeout for overholdelse	Håndhævelseshandling, når en bruger ikke udfører handlinger, der fører til en kompatibel enhedsstatus
Dataindsamlingsfrekvens	Hyppighed, hvormed enhedens/GPS-information skal indsamles
Enhedens hjerteslagsfrekvens	Interval, hvor enheden skal kontakte AppTec360-serveren Min. 1 minut Maks. 24 timer
Aktivér opdateringer af placering	Hvis den er aktiveret, sender enheden placeringsopdateringer til AppTec360 Server.
Placering Opdateringstidspunkt	Bestemmer, i hvilke tidsintervaller enheden sender placeringsopdateringer til AppTec360
Brug Google Location Accuracy til opdatering af placering	Hvis den er aktiveret, vil netværksplaceringen blive brugt til placeringsopdateringer (hvis den var deaktiveret under "Begrænsninger", vil denne indstilling ikke påvirke noget).
Brug GPS-placering til opdatering af placering	Hvis den er aktiveret, vil GPS'en blive brugt til at opdatere positionen.
Tillad falske lokationer	Tillader forfalskning af placeringsoplysninger via tredjepartsapps
Handling ved mistet forbindelse	Hvis det er aktiveret, kan du angive en handling for det tilfælde, at en enhed ikke får forbindelse til MDM-serveren inden for heartbeat-intervallet. Hvis enheden f.eks. har en heartbeat-tid på 5 minutter, opretter den forbindelse til serveren kl. 10:35. Derefter forlader enheden Wi-Fi-området. Det næste hjerteslag kl. 10:40 vil mislykkes, og den angivne handling vil blive udført.
Handling	Den handling, der skal foretages, så snart en enhed ikke overholder kravene.

	• Lock Device = låseenhed • Wipe Device = enheden gendannes til fabriksindstillingerne • Wipe Device & SD Card = enheden gendannes til fabriksindstillingerne, og SD-kortets lager slettes
Tærskel	Du kan angive en tærskelværdi for mislykkede hjerteslag, som er nødvendig for at udløse den angivne handling.

Politisk håndhævelsestilstand	Standard:	Brugere vil med jævne mellemrum blive bedt om at udføre udestående handlinger
	Lazy Policy Enforcement:	Brugere vil aldrig blive bedt om at udføre udestående handlinger. Alle åbne handlinger vil blive vist i AppTec360-klienten.
	Aggressiv håndhævelse af politikker:	Brugerne bliver hele tiden bedt om at udføre udestående handlinger
AppTec360 Version Lock	Hvis det er aktiveret, kan der angives en versionskode for AppTec360 MDM-klienten. AppTec360-klienten vil kun opdatere til den angivne version. Nyere versioner vil blive ignoreret. En nedgradering er IKKE mulig.	
Versionskode	Versionskode for AppTec360 MDM-klienten, der skal låses på.	
Deaktiver AppTec360 Notifikation	Hvis den er deaktiveret, vil AppTec360-klienten ikke vise en notifikation i notifikationslinjen. Brugere kan således lukke AppTec360-klienten via task manager. Hvis AppTec360-klienten er lukket, vil flere funktioner, herunder Kiosk Mode og App Black/Whitelisting, ikke fungere korrekt. Samsung-enheder tilbyder en beskyttelsesmekanisme for AppTec360-klienten. Meddelelsen er som standard deaktiveret på Samsung-enheder, der understøtter KNOX API'er. Meddelelsen bør ikke være deaktiveret på enheder med Android 8.0 eller nyere.	

Baggrund

Indstil brugerdefineret baggrund	Aktiver/deaktiver det brugerdefinerede tapet
Baggrund	Indstil baggrundstilstanden til at bruge en farvekode eller et billede
Angiv en farve	Angiv en baggrundsfarve som hex-værdi, f.eks. #000000 for sort eller #ffffff for hvid.
Indstil billede som baggrund	Upload den billedfil, du vil bruge som baggrund

Asset Management (kun på enhedsniveau)

Enhedsinfo

Model	Enhedens modelbetegnelse
Operativsystem	OS
OS-version	OS-version
Serienummer	Serienummer
Enhedens navn	Enhedens navn
Batteristatus	Batteristatus
Fri / samlet hukommelse	Fri / samlet hukommelse
Samsung Safe	Samsung SAFE-grænseflade, nødvendig for en række indstillingsmuligheder
SD-kort tilgængeligt	SD-kort tilgængeligt
Emuleret SD-kort	SD-kort emuleret
SD-kort kan tages ud	SD-kort kan tages ud
SD Fri / Samlet hukommelse	SD-fri / samlet SD-kort-hukommelse

Wi-Fi

IP-adresse	Enhedens IP-adresse
WiFi MAC	WiFi MAC-adresse

Cellulær

Status	Status (SIM-kort installeret)
Telefonnummer	Telefonnummer
Roaming (tale/data)	Roaming til tale/data
Roaming-status	Aktuel roaming-status
IP-adresse	IP-adresse
Operatør/transportør	Operatør/transportør
Cellulær teknologi	Cellulær teknologi
IMEI	IMEI-nummer
ICCID	Dette er ID'et for SIM-kortet, ofte også et Smartcard eller Integrated Circuit Card (ICC).
IMSI	International Mobile Subscriber Identity (IMSI) giver i GSM- og UMTS-mobilnetværk en definitiv identifikation af netværksbrugerne. IMSI består af maksimalt 15 cifre og konfigureres på følgende måde: • Mobil landekode (MCC), 3 cifre • Mobilnetværkskode (MNC), 2 eller 3 cifre • Identifikationsnummer for mobilabonnenter (MSIN), 1-10 cifre
Nuværende MCC/MNC	Se "SIM MCC/MNC"
SIM MCC/MNC	Den mobile landekode er en etableret landeidentifikation, der er fastsat af ITU i henhold til E.212-standarden. Den fungerer sammen med mobilnetværkskoden (MNC) til identifikation af mobilnetværket. Betyder SIM-kortets landekode/mobilnetværkskode. Hvis du roamer til et andet mobilnetværk, vil "Current MCC/MNC" og "SIM MCC/MNC" logisk nok være forskellige.

Bluetooth

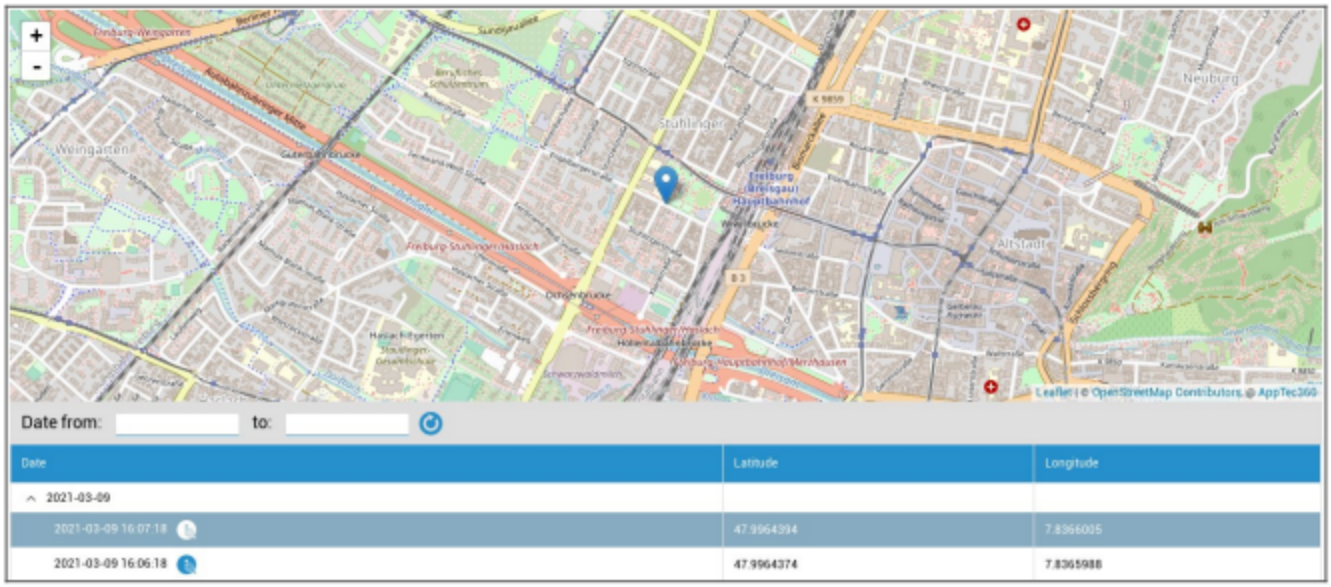
Bluetooth MAC	Bluetooth MAC-adresse

Sikkerhedsstyring

Tyverisikring (kun på enhedsniveau)

GPS-information (kun på enhedsniveau)

Her kan du fastlægge enhedens aktuelle/sidste placering. Lokaliseringen kan beskyttes med en eller endda to adgangskoder - se: Generelle indstillinger - Privatliv - GPS-adgang



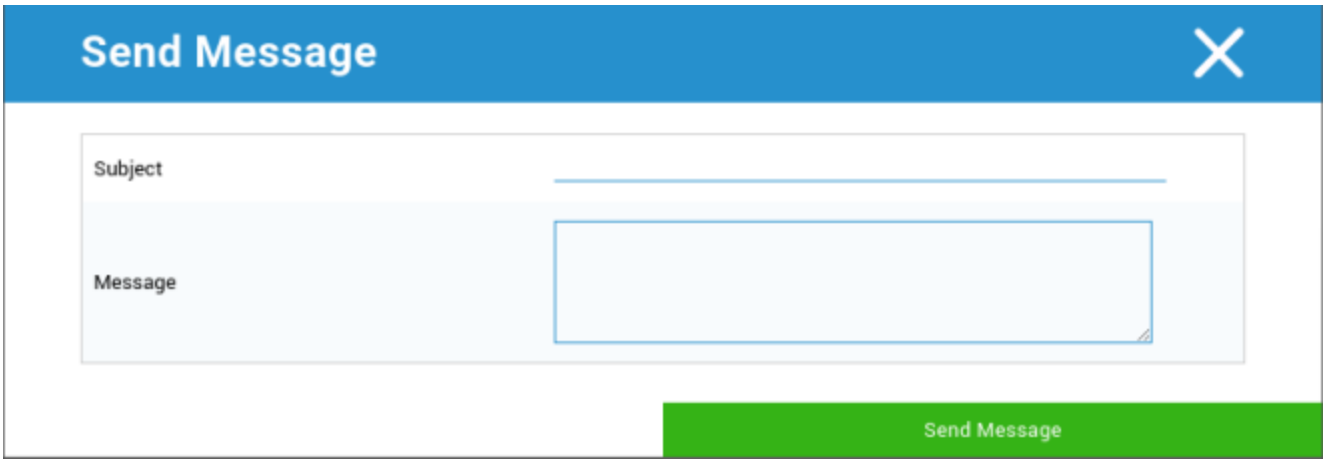
Tør og lås (kun på enhedsniveau)

Under "Wipe & Lock" kan du udføre følgende tre handlinger:

Fuld aftørring	Enheden gendannes til fabriksindstillingerne (både virksomhedsdata og personlige data slettes).
Enterprise Wipe	Kun virksomhedsdata fjernes fra slutbrugerens enhed (alle apps, data osv., der blev leveret af AppTec360).
Låseskærm	Skærmlås er aktiveret, det er tilstrækkeligt at låse enheden op med enhedens adgangskode/PIN.

Besked (kun på enhedsniveau)

Her kan du udfylde emnet og en besked og sende den til en slutbrugerenhed.



Sikkerhedskonfiguration

Enhedens adgangskode

Under "Adgangskode" kan du angive en adgangskode til enheden, og følgende indstillingsmuligheder er tilgængelige for dig

Minimumslængde for adgangskode	Fastsætter, hvor mange symboler en adgangskode som minimum skal indeholde	
Kvalitet af adgangskode	Uspecificeret	Denne politik har ingen krav til adgangskoden.
	Biometrisk svaghed	Denne politik tillader biometrisk genkendelsesteknologi med lav sikkerhed. Dette indebærer teknologier, der kan genkende en persons identitet til omkring en 3-cifret PIN-kode (falsk registrering er mindre end 1 ud af 1.000).
	Et eller andet	Denne politik kræver, at der indstilles en form for adgangskode eller et mønster, men den håndhæver ikke nogen specifikke regler.
	Alfabetisk	Brugeren skal have indtastet en adgangskode, der mindst indeholder alfabetiske tegn (eller andre symboler).
	Alfanumerisk	Brugeren skal have indtastet en adgangskode, der indeholder mindst både numeriske og alfabetiske tegn (eller andre symboler).
	Kompleks	Brugeren skal have indtastet en adgangskode, der som standard indeholder mindst et bogstav, et tal og et specialsymbol. Med denne adgangskodekvalitet kan adgangskoder begrænses til at indeholde forskellige sæt af tegn, f.eks. mindst et stort bogstav osv.
Minimumslængde for adgangskode	Indstil det krævede antal tegn for adgangskoden. Du kan f.eks. kræve, at PIN-koder eller adgangskoder skal indeholde mindst seks tegn.	
Minimum antal cifre, der kræves i adgangskoden	Minimum antal cifre, der kræves i adgangskoden	
Mindst små bogstaver kræves i adgangskoden	Mindst små bogstaver kræves i adgangskoden	
Minimum store bogstaver kræves i adgangskoden	Minimum store bogstaver kræves i adgangskoden	

Minimum af tegn, der ikke er bogstaver, i adgangskoden	Minimum af tegn, der ikke er bogstaver, i adgangskoden
Minimum af symboler i adgangskoden	Minimum af symboler i adgangskoden

Lås for maksimal inaktivitetstid	Maksimal brugerinaktivitet indtil tidslås
Timeout for udløb af adgangskode	Fastsætter, efter hvilket tidsinterval adgangskoden udløber, og en ny adgangskode skal udstedes
Begrænsning af adgangskodehistorik	Antal tidligere anvendte adgangskoder, der ikke er tilladt
Maksimalt antal mislykkede adgangskodeforsøg	Fastsætter, hvor ofte en adgangskode kan indtastes forkert, før en komplet sletning af enheden vil blive udført
Tillad biometrisk godkendelse	Muliggør godkendelse via fingeraftryk eller irisscanning. Kun til Samsung KNOX 2.1 og nyere

AntiVirus

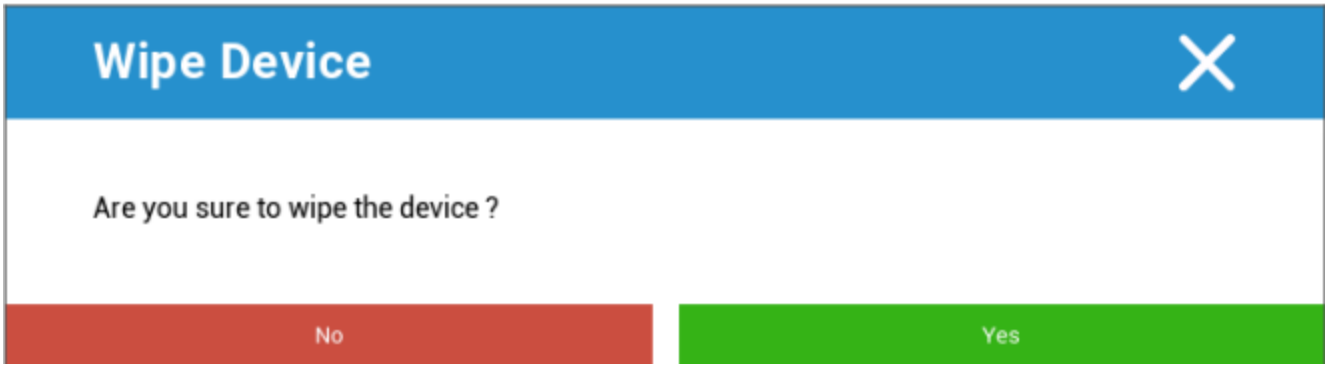
Automatisk scanning	Aktivér periodiske automatiske scanninger
Scanningsinterval	Interval for undersøgelse (hurtig/fuld)
Fuld automatisk scanning	Aktivér fuldautomatiske scanninger
Automatiske opdateringer	Aktivér automatiske opdateringer
Interval for opdateringskontrol	Hvor ofte appen og dens database skal opdateres (virus/beskadiget kode)
App-beskyttelse	Aktivér automatisk app-scanning
Beskyttelse af SD-kort	Aktivér automatisk SD-kort-scanning
Kun Wi-Fi-opdatering	Når det er aktiveret, vil opdateringer kun blive anvendt, når enheden har forbindelse til et Wi-Fi-netværk.

End of Life (kun på enhedsniveau)

Tør (kun på enhedsniveau)

Under "Wipe" kan du gendanne enheden til dens fabriksindstillinger. Her slettes både virksomhedsdata og private data på slutbrugerens enhed.

Når du klikker på "Minus-symbolet", får du følgende besked:



Med "Ja" kan du udføre aftørringen.

Under "Wipe Report" kan følgende elementer vises

Slettet af	Historien om, hvem der udførte tørringen
Dato	Dato
Status	Status (f.eks. hvis Wipe blev udført med succes)

Begrænsningsindstillinger

Begrænsninger

Her kan en lang række ting begrænses og blokeres.

Aktivér kamera	Tillad brug af kamera	
Fremtving automatisk synkronisering	På	Synkronisering er permanent aktiveret
	Fra	Synkronisering er permanent deaktiveret
	Brugerens valg	Valgt af brugeren
Force Bluetooth	På	Bluetooth er permanent aktiveret
	Fra	Bluetooth er permanent deaktiveret
	Brugerens valg	Valgt af brugeren
Force GPS	På	GPS er permanent aktiveret
	Fra	GPS er permanent deaktiveret
	Brugerens valg	Valgt af brugeren
Force-netværkets placering	På	Permanent internet-lokalisering
	Fra	Permanent deaktivering af internetlokalisering
	Brugerens valg	Valgt af brugeren

Sikkerhed		
Forbyd deling af placering	Angiver, om en bruger ikke må slå deling af placering til.	
Forbyd sikker opstart	Angiver, om brugeren ikke må genstarte enheden i sikker opstartstilstand.	
Forbyd nulstilling af netværk	Angiver, om en bruger ikke må nulstille netværksindstillinger fra Indstillinger.	
Tillad ikke fabriksnulstilling	Angiver, om en bruger ikke må nulstille enheden.	
Aktivér ADB	Giver mulighed for tilslutning til en pc via ADB	
Deaktiver nøglebeskyttelse	Deaktiverer Keyguard	
Enhedsejer Info om låseskærm	Indstiller de oplysninger om enhedens ejer, der skal vises på låseskærmen.	
Håndhævelse af overholdelse	Mode Prompt User	Brugeren bliver bedt om at udføre de nødvendige handlinger.
	Mode Lock-Down Container	Skjul alle apps, indtil alle krav er opfyldt

App-administration	
Tillad app-linking på tværs af profiler	Giver apps i den overordnede profil mulighed for at håndtere weblinks fra den administrerede profil.
Forbud mod app-kontrol	Angiver, om en bruger ikke må ændre programmer i indstillinger eller launchers.
Forbyd installation af app	Angiver, om en bruger ikke må installere programmer.
Forbyd afinstallation af apps	Angiver, om en bruger ikke må afinstallere programmer.
Politik for runtime-tilladelser	Angiver, hvordan nye anmodninger om tilladelse fra apps skal håndteres.
Tillad ukendte kilder	Hvis det er aktiveret, kan brugerne sideloade apps ved at installere en .apk-fil.

Forbindelse	
Afvis konfiguration af mobilnetværk	Angiver, om en bruger ikke må konfigurere mobilnetværk.
Forbyd tethering-konfiguration	Angiver, om en bruger ikke har tilladelse til at konfigurere Tethering og bærbare hotspots.
Forbyd VPN-konfiguration	Angiver, om en bruger ikke må konfigurere en VPN.
Forbyd Wifi-konfiguration	Angiver, om en bruger ikke må ændre WiFi-adgangspunkter.
Forbyd udgående NFC-beam	Angiver, om brugeren ikke må bruge NFC til at sende data fra apps.
Lås WiFi-konfiguration	Denne indstilling styrer, om WiFi-konfigurationer, der er oprettet af en enhedsejer-app, skal være låst (dvs. kun kunne redigeres eller fjernes af enhedsejer-appen, ikke engang af Indstillinger-appen).
Aktivér dataroaming	Aktiverer dataroaming

Bluetooth	
Forbyd Bluetooth	Angiver, om Bluetooth ikke er tilladt på enheden. Kræver Android 8.0
Forbyd Bluetooth-deling	Angiver, om udgående Bluetooth-deling ikke er tilladt på enheden. Kræver Android 8.0
Forbyd Bluetooth-konfiguration	Angiver, om en bruger ikke må konfigurere Bluetooth.

Kontoadministration	
Forbyd tilføjelse af administreret profil	Angiver, om en bruger ikke må tilføje administrerede profiler. Kræver Android 8.0
Forbyd tilføjelse af brugere	Angiver, om en bruger ikke må tilføje nye brugere.
Afvis Fjern administreret profil	Angiver, om administrerede profiler for denne bruger kan fjernes af andre end profilens ejer. Kræver Android 8.0
Forbud mod ændring af konto	Angiver, om en bruger ikke må tilføje og fjerne konti, medmindre de er tilføjet programmatisk af Authenticator.

Telefoni	
Forbyd udgående opkald	Angiver, at brugeren ikke må foretage udgående telefonopkald.
Forbyd SMS	Angiver, at brugeren ikke må sende eller modtage SMS-beskeder.

System	
Forbyd oprettelse af vinduer	Angiver, at der ikke skal oprettes andre vinduer end app-vinduer.
Forbud mod at indstille brugerikon	Angiver, om en bruger ikke må ændre sit ikon.
Tillad ikke Set Wallpaper	Brugerbegrænsning for ikke at tillade indstilling af et tapet.
Deaktiver statuslinje	Ved at deaktivere statuslinjen blokeres meddelelser, hurtigindstillinger og andre skærmoverlejringer, der gør det muligt at flygte fra en enhed til engangsbrug.
Aktivér automatisk tid	Indstiller tiden automatisk.
Aktivér automatisk tidszone	Indstiller tidszonen automatisk.
Bliv ved med at være tændt, mens du er tilsluttet	Enheden forbliver aktiv, mens den er tilsluttet en strømkilde.

Opbevaring	
Afvis deaktivering af app-verifikation	Angiver, om en bruger ikke må deaktivere programverifikation.
Forbyd montering af fysiske medier	Angiver, om en bruger ikke må montere fysiske eksterne medier.
Aktivér backup-service	Backupservice administrerer alle backup- og gendannelsesmekanismer på enheden. Hvis du sætter den til false, forhindres data i at blive sikkerhedskopieret eller gendannet. Backup-tjenesten er som standard slået fra. Kræver Android 8.0
Aktivér USB-masselager	Aktiverer brugen af USB-masselager.

Tastatur	
Forbyd automatisk udfyldning	Angiver, om en bruger ikke må bruge Autofill Services. Kræver Android 8.0
Forbud mod at kopiere og indsætte mellem profiler	Angiver, om det, der kopieres til udklipsholderen i denne profil, kan indsættes i relaterede profiler.

Lyd	
Afvis justering af volumen	Angiver, om en bruger ikke må justere mastervolumen.
Tillad ikke Slå mikrofonen fra	Angiver, om en bruger ikke må justere mikrofonens lydstyrke.
Mute-enhed	Mute-enhed.

Administration af certifikater

Her kan du distribuere Trusted Certificates og Identity Certificates til dine enheder.

Android 8 eller nyere er påkrævet for at distribuere Trusted Certificates, og Android 9 eller nyere er påkrævet for at distribuere Identity Certificates.

Med "+" kan du tilføje flere certifikater.

Betroede certifikater skal være i PEM-format.

Identitetscertifikater skal være i PKCS12-format

Håndtering af forbindelser

Wifi

For denne indstilling skal du udføre forudgående konfiguration af slutbrugerenhederne for at få adgang til interne adgangspunkter

Identifikator for servicesæt (SSID)	SSID for det netværk, der skal tilsluttes
Skjult netværk	Aktivér, hvis AP'et ikke udsender SSID'et

Sikkerhedstype

Fastlæg AP'ets sikkerhedstype

WEP

Adgangskode	Adgangskode til AP'et

WPA/WPA2

Adgangskode	Adgangskode til AP'et

802.1x EAP

EAP-metode

PWD	Identitet	Identitet
	Adgangskode	Adgangskode

PEAP	Fase 2-godkendelsesprotokol	ingen	Ingen yderligere protokol
		MSCHAPV2	MSCHAPV2-protokol
		GTC	GTC-protokol
	CA-certifikat	CA-certifikat	
	Identitet	Identitet	
	Anonym identitet	Anonym identitet	
	Adgangskode	Adgangskode	

TTLS	Fase 2-godkendelsesprotokol	ingen	Ingen yderligere protokol
		PAP	PAP-protokol
		MSCHAP	MSCHAP-protokol
		MSCHAPV2	MSCHAPV2-protokol
		GTC	GTC-protokol
	CA-certifikat	CA-certifikat	
	Identitet	Identitet	
	Anonym identitet	Anonym identitet	
	Adgangskode	Adgangskode	

TLS	CA-certifikat	CA-certifikat
	Identitet	Identitet
	Adgangskode	Adgangskode

VPN

Navn på forbindelse	Navn på VPN-forbindelsen

VPN-type

VPN

VPN-klient

AppTec360 VPN-klient	
Gateway-konfiguration	Vælg Gateway VPN-konfiguration (se **Generelle indstillinger > Universal Gateway > VPN-indstillinger**)
Altid tændt VPN	Aktiver Native Lockdown
Aktivér AppTec360 Lockdown	Aktivér AppTec360 Lockdown

Indbygget (kun tilgængelig på Samsung-enheder)			
Tilslutningstype	PPTP	Server	Server
		Aktivér PPTP-kryptering	Aktivér PPTP-kryptering
	L2TP / IPSec PSK	Server	Server
		IPSec forhåndsdelt nøgle	IPSec forhåndsdelt nøgle
		Aktivér L2TP-hemmelighed	Aktivér L2TP-hemmelighed
		L2TP-hemmelighed	L2TP-hemmelighed
	IPSec XAuth PSK	Server	Server
		IPSec-identifikator	IPSec-identifikator
		IPSec forhåndsdelt nøgle	IPSec forhåndsdelt nøgle
Domæner til DNS-søgning	Domæner til DNS-søgning		
Ekspertindstillinger	DNS-servere	DNS-servere	
	Videresendelse af ruter	Videresendelse af ruter	

Åben VPN		
Server	Server	
OpenVPN-profil	OpenVPN-profil	
OpenVPN-app	OpenVPN til Android (anbefales)	
	OpenVPN-forbindelse	
Ekspertindstillinger	DNS-servere	DNS-servere
	Videresendelse af ruter	Videresendelse af ruter

Samsung / Stærk svane			
Tilslutningstype	PPTP	Server	Server
		Brugernavn	Brugernavn
		Adgangskode	Adgangskode
		Aktivér PPTP-kryptering	Aktivér PPTP-kryptering
	L2TP / IPSec PSK	Server	Server
		IPSec forhåndsdelt nøgle	IPSec forhåndsdelt nøgle
		Brugernavn	Brugernavn
		Adgangskode	Adgangskode
		Aktivér L2TP-hemmelighed	L2TP-hemmelighed
	IPSec XAuth PSK	Server	Server
		IPSec-identifikator	IPSec-identifikator
		IPSec forhåndsdelt nøgle	IPSec forhåndsdelt nøgle
		Brugernavn	Brugernavn
		Adgangskode	Adgangskode
Ekspertindstillinger	DNS-servere	DNS-servere	
	Videresendelse af ruter	Videresendelse af ruter	

Cisco Any Connect		
Server	Server	
Certifikat-tilstand	Handicappet	Handicappet
	Automatisk	Automatisk
Ekspertindstillinger	DNS-servere	DNS-servere
	Videresendelse af ruter	Videresendelse af ruter

VPN pr. app

VPN-klient

AppTec360 VPN-klient		
Gateway-konfiguration	Vælg Gateway VPN-konfiguration (se **Generelle indstillinger > Universal Gateway > VPN-indstillinger**)	
VPN-apps	VPN-apps	
Altid tændt VPN	Aktiver Native Lockdown	Altid tændt VPN
Aktivér AppTec360 Lockdown	Aktivér AppTec360 Lockdown	

Samsung / Stærk svane			
Tilslutningstype	PPTP	Server	Server
		VPN-apps	VPN-apps
		Brugernavn	Brugernavn
		Adgangskode	Adgangskode
		Aktivér PPTP-kryptering	Aktivér PPTP-kryptering
	L2TP / IPSec PSK	Server	Server
		VPN-apps	VPN-apps
		IPSec forhåndsdelt nøgle	IPSec forhåndsdelt nøgle
		Brugernavn	Brugernavn
		Adgangskode	Adgangskode
		Aktivér L2TP-hemmelighed	L2TP-hemmelighed
	IPSec XAuth PSK	Server	Server
		VPN-apps	VPN-apps
		IPSec-identifikator	IPSec-identifikator
		IPSec forhåndsdelt nøgle	IPSec forhåndsdelt nøgle
		Brugernavn	Brugernavn
		Adgangskode	Adgangskode
Ekspertindstillinger	DNS-servere	DNS-servere	
	Videresendelse af ruter	Videresendelse af ruter	

Begrænsninger

Her kan du indstille begrænsningerne i forhold til forbindelsesstyring.

Tillad dataroaming	Tillad mobildata under roaming
Tving til dataroaming	Hvis den er aktiveret, er roaming for mobildata permanent aktiveret (anbefales ikke!). Denne indstilling overskriver indstillingen "Tillad dataroaming"!
Følgende indstillinger er kun tilgængelige på SAFE 2.x eller højere	
Tillad kun nødopkald	Tillad kun nødopkald
Tillad WiFi	Tillad WiFi
Minimum sikkerhedsniveau for WiFi-netværk	WiFi-netværkets mindste sikkerhedsniveau Åben = alle typer WiFi er tilladt
Forbyd brugeren at tilføje WiFi-netværk	Brugeren kan ikke selv tilføje et WiFi-netværk Denne indstilling er kun mulig, hvis der er defineret en WiFi-profil under "Connection Management".
Tillad SMS og MMS	Alle = Al SMS- og MMS-trafik er tilladt Kun indgående SMS = Kun indgående SMS-beskeder er tilladt Kun udgående SMS = Kun udgående SMS-beskeder er tilladt Ingen = Ingen SMS/MMS-trafik er tilladt
Tillad synkronisering under roaming	Tillad synkronisering under roaming On = aktiveret Off = deaktiveret Brugervalg = brugerens valg
Tillad stemme-roaming	Tillad stemme-roaming On = aktiveret Off = deaktiveret User Choice = brugerens valg
Brug systemets http-proxyserver	Brugen af en HTTP-proxyserver, som leveres af systemets indstillinger i indstillinger, er afhængig af det tilsluttede netværk (WiFi eller APN).

PIM-styring

Gmail-udveksling

Info: Denne konfiguration vil blive anvendt på Gmail-appen. Så du skal godkende og installere Gmail.

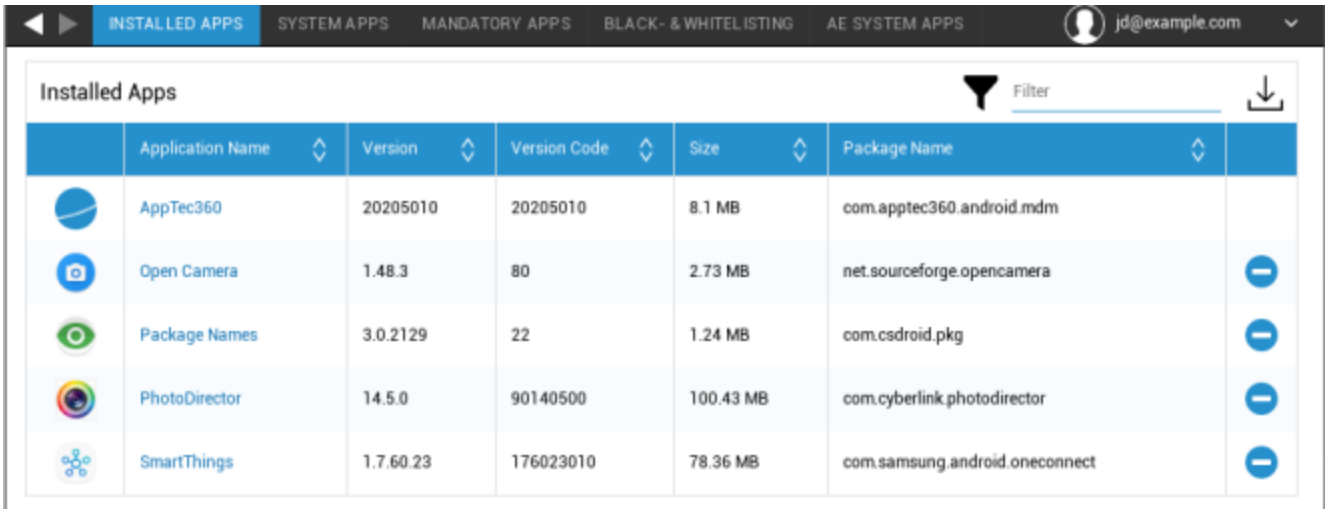
E-mail-adresse	Den angivne brugers e-mailadresse Bemærk "pladsholderne", som du kan bruge til at arbejde med legitimationsoplysninger, og du behøver ikke foretage ændringer manuelt på alle enheder. Med et klik kan du se dem for dig selv
Serverens værtsnavn	Serveradresse på dine Exchange-servere
Login-navn	Login-navnet for den respektive slutbrugerenhed, bemærk også "Placeholders here".
Underskrift	En underskrift kan vedhæftes (tip: Nogle enheder kræver HTML-formatering af underskriften).
Antal foregående dage, der skal synkroniseres	Antal dage, der bestemmer, hvornår e-mails synkroniseres tilbage
Enhedsidentifikator	En streng, der indeholder EAS DeviceID. Dette er en del af EAS-protokollerne og er nødvendigt i nogle områder.
Brug Secure Sockets Layer (SSL)	Brug en SSL-forbindelse
Accepter alle certifikater	Alle certifikater accepteres. Vælg denne indstilling, hvis din Exchange Server bruger et selvsigneret certifikat.

App-administration

Enterprise App Manager

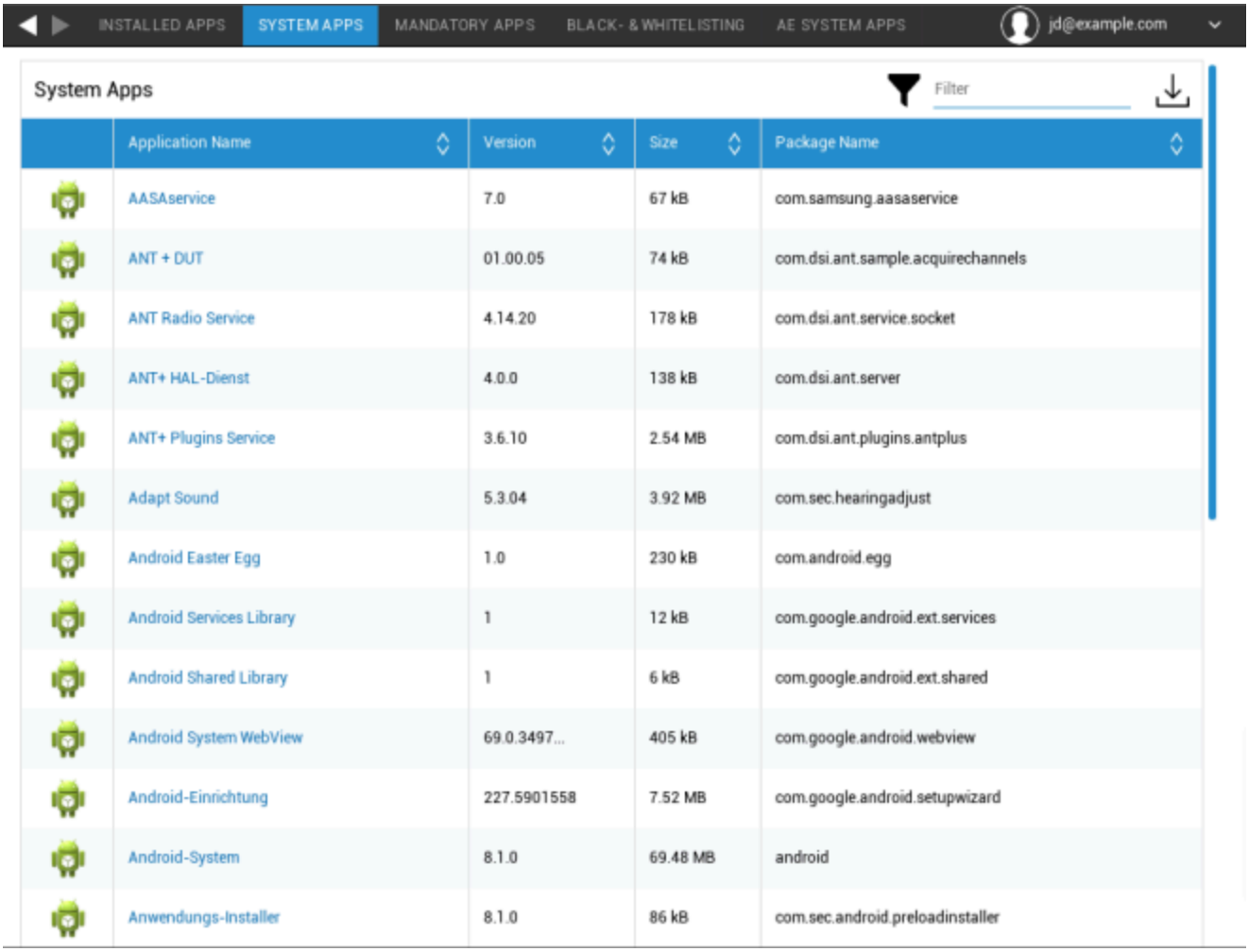
Installerede apps (kun på enhedsniveau)

Her vises alle de apps, der i øjeblikket er installeret på slutbrugerens enhed.



System-apps (kun på enhedsniveau)

Under "System Apps" vil alle de apps og tjenester, der allerede er installeret på slutbrugerens enhed af enhedens producent, blive vist for dig.

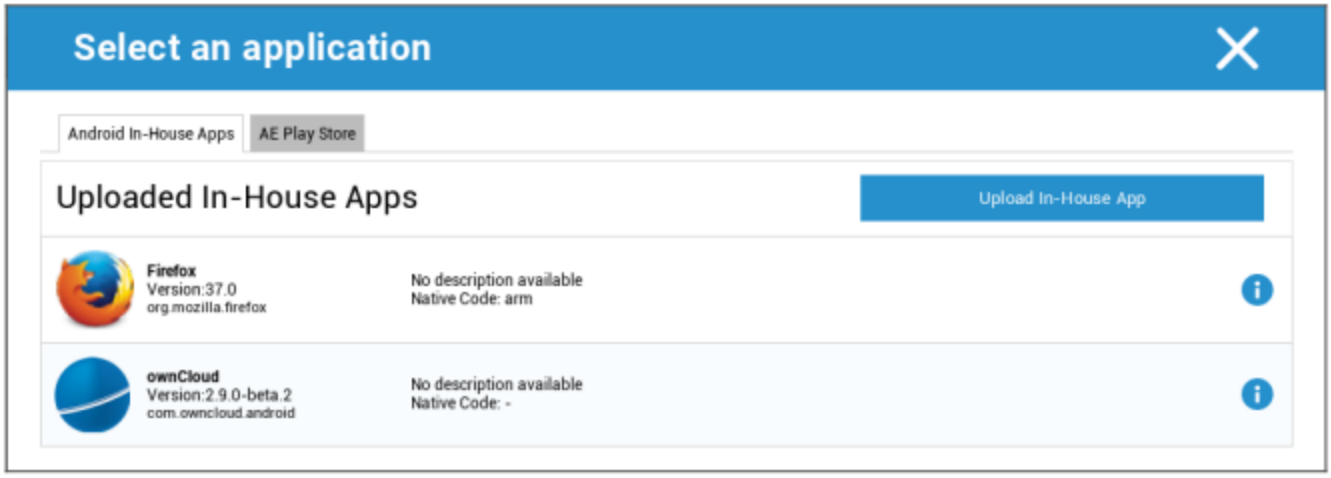


Obligatoriske apps

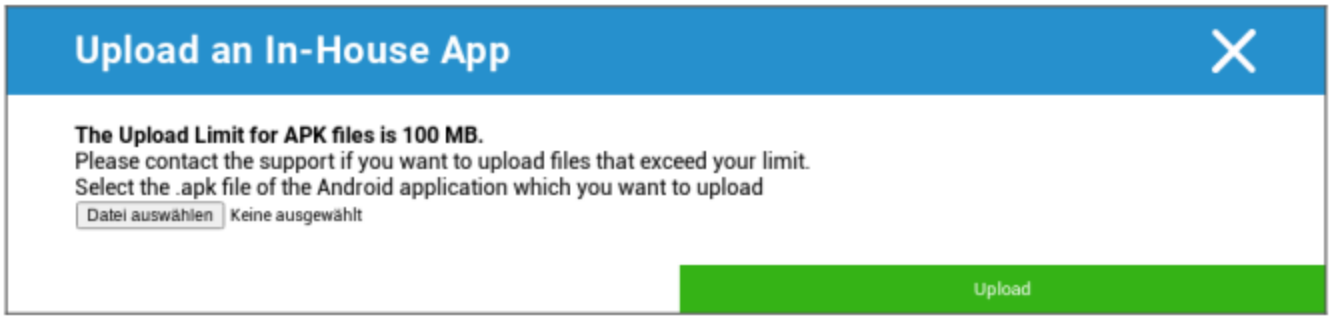
Under Obligatoriske apps kan du oprette de obligatoriske apps. Brugeren vil løbende blive bedt om at installere denne udpegede app.

Via kan den påkrævede app defineres.

Det kan være en intern app fra "Android In-House Apps", som du har uploadet i Generelle indstillinger.

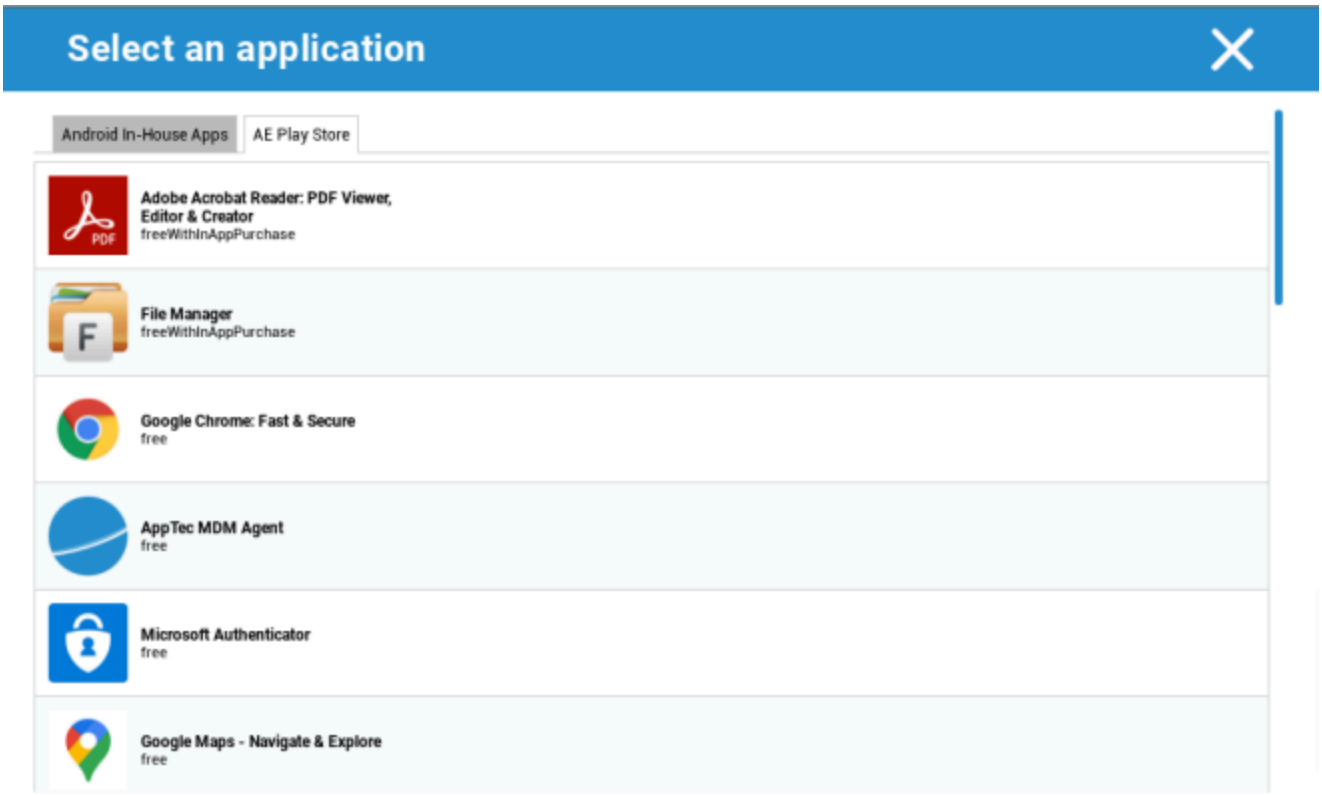


Du kan også vælge og uploade en apk-fil direkte med "Upload In-House App".



Hvis du installerer en In-House App, har du mulighed for at aktivere "Keep up to date". Hvis dette er aktiveret, og du har defineret en nyere version i In-House App DB, vil appen blive opdateret på enheden.

Eller det kan være en "AE Play Store"-app fra Google Work Play Store.



Kun godkendte "AE Play Store Apps" vil blive vist på denne fane.

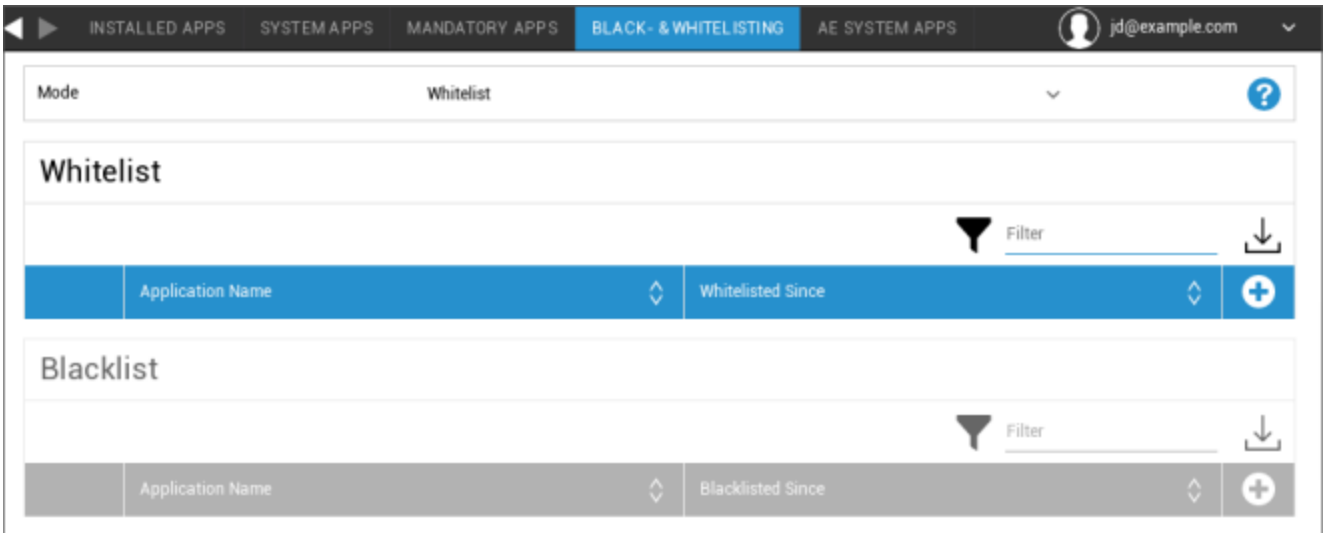
For at godkende en "AE Play Store-app" skal du gå til "Generelle indstillinger" > "Appadministration" > "AE Play".

Store" og tilføj en app via knappen, som sender dig videre til fanen "Play Store Apps" (eller du kan gå direkte til fanen "Play Store Apps").

På fanen "Play Store Apps" kan du søge efter apps. Når du klikker på en app, åbnes app-siden , og her kan du godkende appen ved at klikke på "Approve".

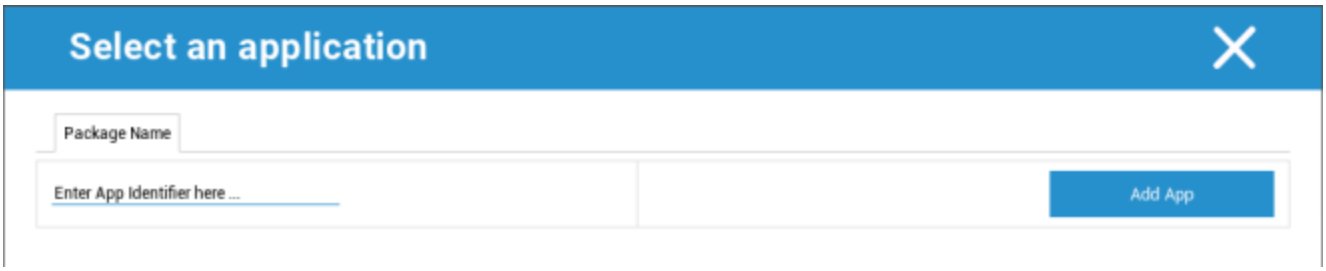
Sort- og hvidlistning

Under "Black- & Whitelisting" kan du vælge mellem tilstanden "Whitelist" og tilstanden "Blacklist".



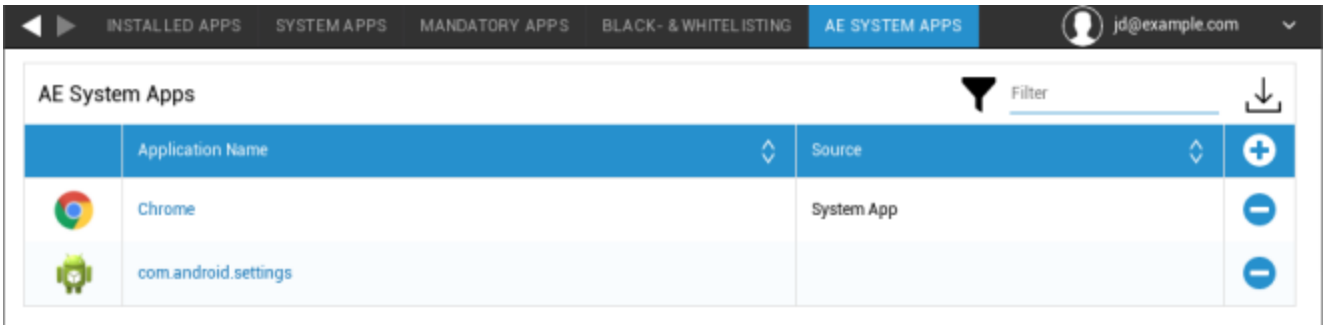
Hvidliste	Kun apps og tjenester, der er føjet til listen, kan installeres på slutbrugerens enhed. Hvis de allerede er forudinstalleret på slutbrugerens enhed, vil de blive aktiveret og indstillet, så brugeren kan køre dem.
	Alle andre apps, der ikke er føjet til listen, kan ikke installeres på slutbrugerens enhed. Hvis de allerede er forudinstalleret på slutbrugerens enhed, vil de blive deaktiveret og indstillet, så brugeren ikke kan køre dem.
Sortliste	Apps og tjenester, der føjes til listen, kan ikke installeres på slutbrugerens enhed. Hvis de allerede er forudinstalleret på slutbrugerens enhed, vil de blive deaktiveret og indstillet, så brugeren ikke kan køre dem.
	Alle andre apps, der ikke er føjet til listen, kan installeres på slutbrugerens enhed. Hvis de allerede er forudinstalleret på slutbrugerens enhed, vil de blive aktiveret og indstillet, så brugeren kan køre dem.

Via , tilføjer du yderligere apps eller tjenester til den aktuelt anvendte liste.
Via , tilføjer du yderligere apps eller tjenester til den aktuelt inaktive liste.
Du kan definere et "pakkenavn":

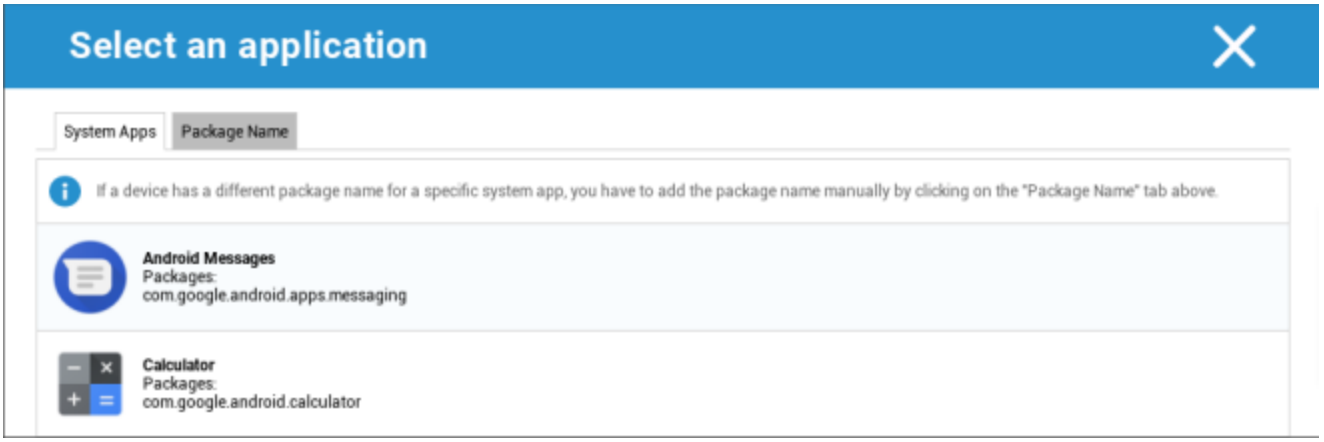

Select an application
Package Name
Enter App Identifier here ...
Add App

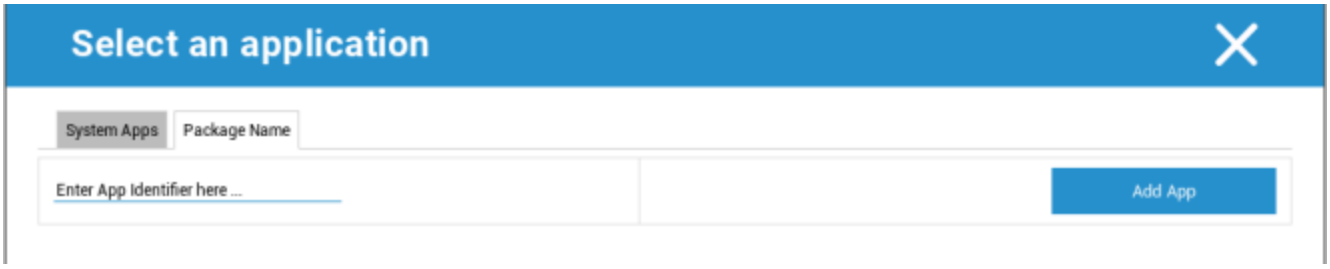
AE System Apps

Her kan du definere en liste, der indeholder specifikke systemapps, som skal aktiveres på enhederne.



Hvis du klikker på knappen, kan du vælge fra en liste over mulige systemapps fra Google eller direkte indtaste pakkenavnet på en systemapp, der skal aktiveres.





Husk, at systemapps på listen fra Google kun er apps, der kan være systemapps, men ikke nødvendigvis behøver at være systemapps på dine enheder.

Denne liste påvirker dog kun apps, der allerede er forudinstalleret.

Tilføjelse af apps, der ikke er forudinstalleret på dine enheder, vil ikke påvirke dine enheder, uanset om appen er fra listen fra Google, eller om appens pakkenavn indtastes direkte.

Begrænsninger og indstillinger

Indstillinger for app-administration

Her kan du konfigurere enhedens adfærd i forhold til app-opdateringer.

Hyppighed af opdateringstjek	Angiv, i hvilket interval AppTec360-klienten skal søge efter app-opdateringer. Standardværdien er 24 timer.
Wi-Fi-tærskel	Apps, der er større end den angivne størrelse, downloades via Wi-Fi. Hvis "Kun Wi-Fi" er valgt, vil alle apps blive downloadet via Wi-Fi.

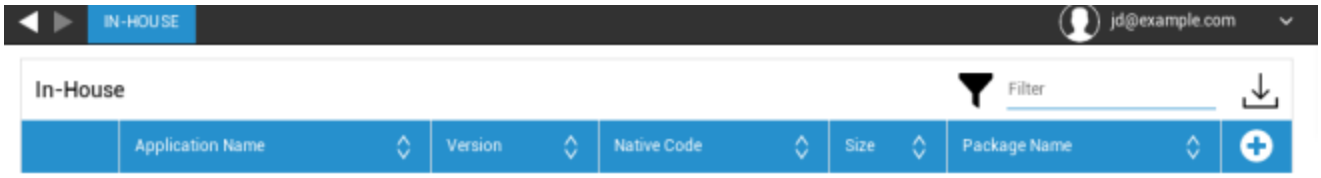
Enterprise App Store

Internt

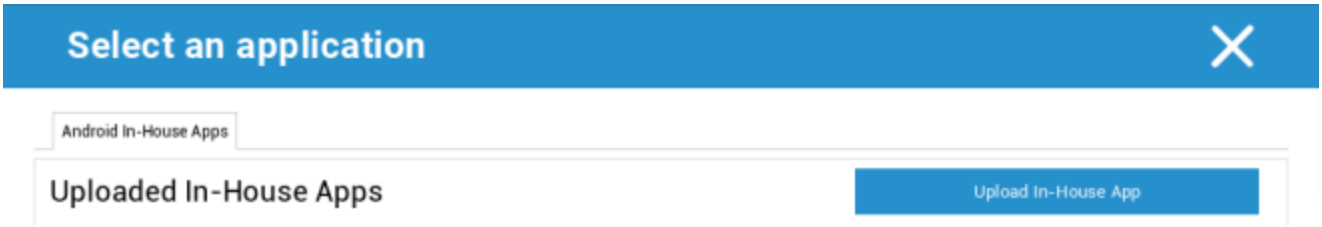
Under punktet "In-House" kan du uploade og distribuere internt udviklede apps.

Med symbolet kan du distribuere yderligere In-House Apps.

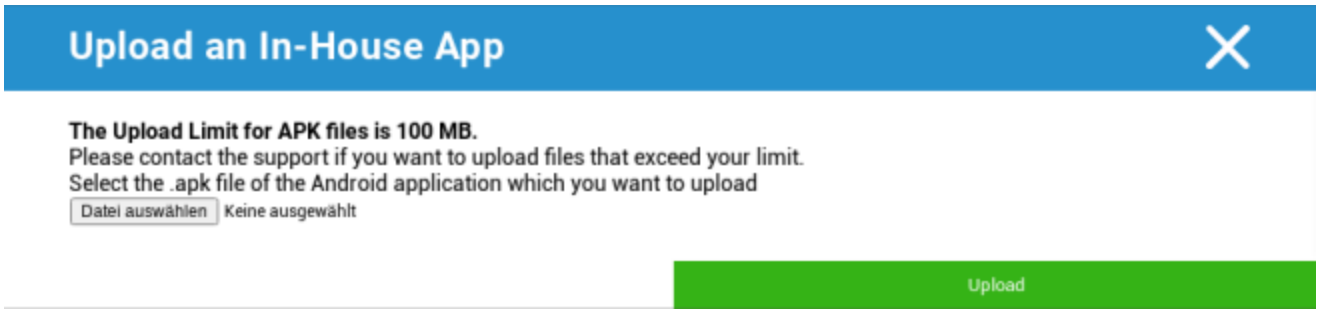
Hvis du installerer en In-House App, har du mulighed for at aktivere "Keep up to date". Hvis er aktiveret, og du har defineret en nyere version i In-House App DB, vil appen blive opdateret på på enheden.



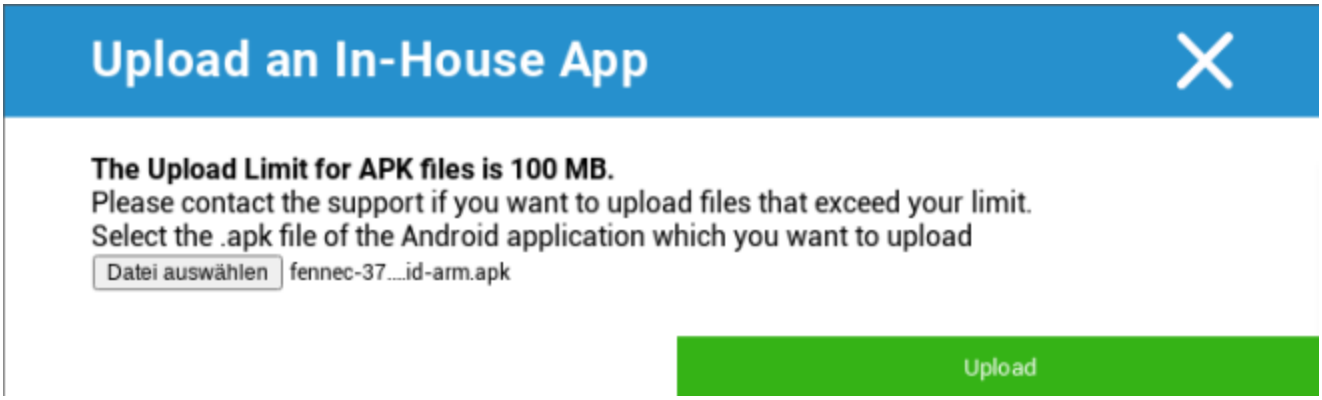
Hvis du ikke har distribueret In-House Apps, vil du modtage følgende oversigt:



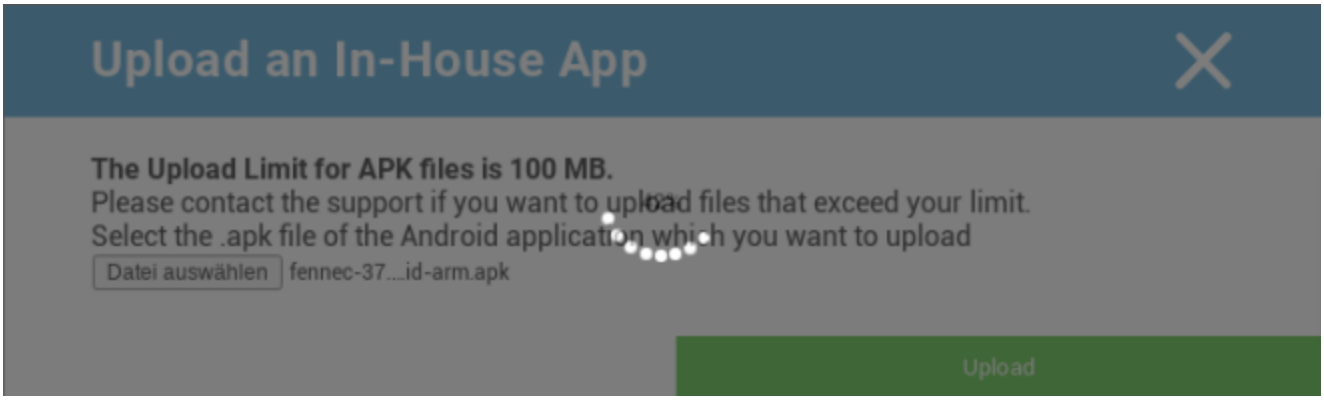
Klik på "Upload In-House App", så får du følgende oversigt:



Vælg nu med "Søg ..." en .apk-fil, og klik derefter på "Upload".



Din app vil nu blive uploadet, og i midten af cirklen vil du se en procentindikator,
, som viser, hvor meget af din app, der allerede er uploadet.



Hvis uploaden af din interne app har været vellykket, kan du finde den uploadede app i dit app-katalog.

Brugeren har nu mulighed for at se og installere denne app i AppTec360 Store på slutbrugerens enhed under kategorien "In-House".

Da dette ikke involverer en Google PlayStore-app, har brugeren ikke brug for et gemt Google ID på sin respektive slutbrugerenhed.

Enterprise Play Store

AE Play Store

Her kan du tilføje apps til Android Enterprise Playstore. Bemærk, at du skal godkende apps med din AE-administratorkonto, før du kan tilføje dem.

For at godkende en app, se venligst instruktionerne i Obligatoriske apps.

Kiosk-tilstand og launcher

Kiosk-tilstand

Kiosk Mode giver dig mulighed for at forhåndsdefinere en app eller en URL. Derefter vil det udelukkende være muligt at køre/besøge denne app eller URL på

.

På samme måde kan forskellige hardwareknapper deaktiveres i Kiosk Mode diverse.

Automatisk start	Starter automatisk Kiosk Mode, så snart profilen når frem til slutbrugerens enhed
Planlagt kiosktilstand?	Du kan planlægge et tidspunkt for Kiosk Mode, som så starter og slutter automatisk på et tidspunkt, du har indstillet.
Starttidspunkt	Starttidspunkt
Tid i minutter	Tid i minutter, hvorefter Kiosk Mode skal afsluttes igen

Applikationstype

Enkelt app	Hvis du vil starte appen i kiosktilstand, skal du vælge "Pakke" under "Applikationstype".
Kiosk-applikation	Klik her for at vælge en app, der skal startes i Kiosk Mode Du finder den sædvanlige oversigt over App Management Du kan vælge mellem en "Google Play Store", "Android In-House Apps" og et "Packagename"

Applikationstype

URL	Hvis du vil starte en URL i kiosktilstand, skal du vælge "URL" under "Applikationstype". Definer derefter din ønskede URL-adresse
Ryd browseren efter inaktivitet	Her kan du definere et tidsinterval i minutter, hvorefter Kiosk Mode skal genstartes.
Ryd webcache og cookies	Hvis du aktiverer denne funktion, vil webcachen (cookies og cachelagrede billeder) blive slettet efter en genstart af Kiosk Mode.
Politik for samme oprindelse	Hvis denne funktion er aktiv, kan brugeren kun surfe på undersiderne i en defineret URL. Du har f.eks. defineret følgende URL:www.mypage.com Så kan brugeren surfe på: www.mypage.com/subpage
Hvidlistede webadresser	Her kan du vedligeholde en hvidliste, hvor alle disse URL'er er tilladt Maksimalt 1 URL pr. linje En URL skal starte med http:/ eller https://
Sortlistede webadresser	Her kan du vedligeholde en sortliste, hvor alle disse URL'er ikke er tilladt Maksimalt 1 URL pr. linje En URL skal starte med http:/ eller https://
Skærm-orientering	Denne indstilling vedrører skærmjusteringerne Automatisk = automatisk Portræt = lodret format Landscape = landskabstilstand

Multi-app	Hvis du vælger "Multi App"-kiosktilstand, vil brugen af AppTec360 Launcher blive gennemtvunget.
Apps	Applikation: Vælg en Playstore eller en intern app som kiosk-applikation. Det er også muligt at indtaste et pakkenavn. Den valgte kiosk-applikation skal være installeret på enheden. Husk at indstille Kiosk-applikationen som obligatorisk. Genvej på startskærmen: Hvis den er sat til "On", oprettes der en genvej på startskærmen. Hvis den er indstillet til "Fra", vises appen stadig på applisten.

Afslut adgangskode aktiveret	Hvis du aktiverer denne funktion, er det muligt for brugeren at afslutte kiosktilstanden med en adgangskode, som du har defineret på forhånd.
Afslut adgangskode	Dette er den adgangskode, som du har defineret på forhånd.
Skjul statuslinjen automatisk	Hvis den er aktiveret, bliver statuslinjen automatisk udtonet. Med denne indstilling kan brugerne se oplysningerne på statuslinjen, men ikke få adgang til dens funktioner.
Deaktiver statuslinje	Statuslinjen indeholder meddelelser, genveje og information. Kun tilgængelig for Samsung-enheder med SAFE 4.0 eller nyere.
Deaktiver lydstyrketaster	Deaktiver lydstyrketaster (kun tilgængelig på Samsung-enheder med SAFE 3.0 eller højere)
Deaktiver tænd/sluk-kontakt	Deaktiver tænd/sluk-kontakt (kun tilgængelig på Samsung-enheder med SAFE 3.0 eller højere)
Deaktiver Home-knap	Deaktiver Hjem-knap. Hvis denne funktion er blevet aktiveret, kan kiosktilstanden kun afsluttes i AppTec360-konsollen. (kun tilgængelig på Samsung-enheder med SAFE 3.0 eller højere)
Slå navigationslinjen fra	Med denne funktion kan du deaktivere navigationslinjen (Tilbage/Menu). Hvis denne funktion er aktiveret, kan kiosktilstanden kun afsluttes i AppTec360-konsollen. (kun tilgængelig på Samsung-enheder med SAFE 3.0 eller højere)

AppTec360 Launcher

Aktivér AppTec360 Launcher	Tændt: Aktiverer AppTec360 Launcher. Brugeren skal indstille den som standardstarter én gang. Bemærk: Hvis Kiosk Mode er aktiveret, og Kiosk Mode er indstillet til "Multi App", vil brugen af AppTec360 launcher blive gennemtvunget.
Store ikoner	Til: Viser en større version af app-ikonerne i launcheren
Skjul AppTec360-appikonet	På: Skjuler AppTec360-appen fuldstændigt
Skjul AppTec360 Store-ikonet	På: Skjuler AppTec360 Enterprise AppStore helt.

AppTec360-indstillinger

Aktivér AppTec360-indstillingsappen	AppTec360-indstillingsappen giver kontrol over WiFi- og Bluetooth-forbindelser
Aktivér indstillinger i Multi App Kiosk-tilstand	Hvis det er aktiveret, kan brugerne få adgang til AppTec360 Settings-appen, mens Multi App Kiosk Mode er aktiv.

Fjernbetjening

Splashtop

For at starte en fjernbetjeningssession til din enhed skal appen "Splashtop Streamer" installeres på enheden ved at tilføje appen til App **Management** → **Enterprise App Manager** → **Obligatoriske apps**.

Derefter skal du konfigurere følgende indstillinger for Splashtop:

Aktivér Splashtop	Hvis det er aktiveret, vil AppTec360 konfigurere Splashtop-appen til at tillade fjernbetjening
Implementer kode	Gå til https://my.splashtop.com og log ind på din Splashtop-konto. Klik på "Add Computer", og kopier den 12-cifrede implementeringskode fra den resulterende side.
Indstil brugerdefineret implementeringsgateway?	Implementer Gateway
Implementer Gateway-domæne/vært	Implementer Gateway
Bekræftelse af certifikat	Bekræftelse af certifikat

Derefter kan du bruge indstillingen Splashtop Remote Control i kontekstmenuen (tandhjulet ved siden af søgefeltet, når enheden er valgt, eller højreklik på enheden i træet) til at starte fjernbetjeningssessionen.

TeamViewer

For at starte en fjernbetjeningssession til din enhed skal appen "TeamViewer QuickSupport" installeres på enheden ved at tilføje appen til App **Management** → **Enterprise App Manager** → **Obligatoriske apps**.

Derefter kan du bruge indstillingen **TeamViewer Remote Control** i kontekstmenuen (tandhjulet ved siden af søgefeltet, når enheden er valgt, eller højreklik på enheden i træet) til at starte fjernbetjeningssessionen.

Styring af indhold

Indholdsboks

Her kan du aktivere indholdsboksen.

Så snart du sætter "Enable ContentBox" til "On", installeres der automatisk en separat ContentBox-app
på slutbrugerens enhed.

Sikker browser

Her kan du konfigurere indstillinger for AppTec360 Secure Browser.

Så snart du skifter sektionen i "Secure Browser" til "On", installeres der automatisk en separat browser-app på
på slutbrugerens enhed.

Kræver adgangskode	Kræv, at brugeren opretter og bruger en adgangskode for at få adgang til browseren.
Mindste krævede password-længde	Indstil det krævede antal tegn for adgangskoden
Nødvendig adgangskodekvalitet	Indstil den krævede adgangskodekvalitet
Begræns downloads / åbn i	
Begræns uploads	
Upload hvidliste	En liste over URL'er, som det altid er tilladt at uploade til.
Tillad kopiering	Tillad at kopiere, klippe eller dele tekst inde på websiderne.
Tillad skærmoptagelse	Tillad optagelse af skærmbilleder.
Hyppighed af dataoprydning	Vælg, hvor ofte ALLE brugerdata (historik, cache osv.) skal fjernes automatisk.
Bogmærker til virksomheder	Bogmærkerne vil dukke op i mappen "Company bookmarks" i browserens bogmærker. De kan ikke redigeres af brugeren.
Skjul adresselinjen	
Whitelisting i browseren (uden Universal Gateway)	Aktiverer URL-whitelisting på klientsiden. • Virksomhedens bogmærker er altid whitelistet • Understøttes kun for 100 URL'er • Brug Universal Gateway til ubegrænset black- og whitelisting.
Hvidlistede webadresser	En liste over tilladte URL'er.
Gateway-baseret black- og whitelisting	Sortlistning har følgende krav: • En fungerende AppTec360 Universal Gateway ("Generelle indstillinger" → "Universal Gateway")

	• En fungerende VPN-konfiguration med en specificeret DNS-server ("Generelle indstillinger" → "Universal Gateway" → "VPN-indstillinger") • En sortlistekonfiguration ("Generelle indstillinger" → "Universal Gateway" → "Sortliste over domæner") • En gyldig VPN-forbindelse i profilen ("Forbindelsesstyring" → "VPN")

Yderligere API

Samsung KNOX

Begrænsninger

Tillad SD-kort	
Tillad skrivning på SD-kort	
Tillad skærmoptagelse	
Tillad udklipsholder	
Sikkerhedskopier indstillinger og app-data i Google Cloud	
Gendan indstillinger fra Google Cloud, når du geninstallerer en app	
Tillad USB-fejlfinding	
Tillad Google Crash Report	
Tillad fabriksnulstilling	
Tillad OTA-opgradering	
Tillad USB-værtslagring	Hvis det er aktiveret, kan en bruger tilslutte et hvilket som helst pen-drev (bærbart USB-lager), ekstern HD eller Secure Digital (SD)-kortlæser, og det bliver monteret som et lagerdrev på enheden.
Tillad USB Media Player (MTP,PTP)	
Tillad mikrofon	Deaktiverer mikrofonen for tredjepartsapplikationer
Tillad NFC (Near Field Communication)	
Tillad ukendte kilder (APK Sideloading)	Hvis det er aktiveret, er side-loading af apps (APK-filer) tilladt. Når denne indstilling er deaktiveret, skal brugeren aktivere den manuelt, når du tillader installation af APK'er fra ukendte kilder.
Tillad oprettelse af brugere	Hvis det er aktiveret, kan brugeren oprette flere konti på enheden, f.eks. gæstekonti.

E-mail

E-mail-adresse	
Indgående serverprotokol	
Adresse på indgående server	
Indgående serverport	
Login/brugernavn til indgående server	
Adgangskode til indgående server	
Indgående server bruger SSL	
Indgående server bruger TLS	
Indkommende server accepterer alle certifikater	
Udgående serverprotokol	
Adresse på udgående server	
Udgående serverport	
Udgående server bruger ekstra legitimationsoplysninger	Hvis den er deaktiveret, bruger systemet også de indgående legitimationsoplysninger til den udgående server.
Login/brugernavn til udgående server	
Adgangskode til udgående server	
Udgående server bruger SSL	
Udgående server bruger TLS	
Udgående server accepterer alle certifikater	
Sæt signatur	
Underskrift	Bemærk: På nogle enheder skal signaturen angives i HTML-format.
Giv brugeren besked ved modtagelse af ny e-mail	

Udveksling

E-mail-adresse	
Serverens værtsnavn	Værtsnavnet på Exchange-serveren
Login-navn	Det brugernavn, der bruges til at logge ind på Exchange Server.
Domæne	Hvis en ACL Gateway-konfiguration er aktiveret, og feltet Domæne ikke er tomt, vil AppTec360 Universal Gateway godkende enheden med følgende navn "Domæne\Loginnavn
Adgangskode	
Antal foregående dage, der skal synkroniseres	
Frekvens for synkronisering af eMail	
Synkronisering under roaming	
Sæt signatur	
Underskrift	Bemærk: På nogle enheder skal signaturen angives i HTML-format.
Standardkonto	
Brug Secure Sockets Layer (SSL)	
Brug Transport Layer Security (TLS)	
Accepter alle certifikater	

APN

APN-visningsnavn	
Navn på adgangspunkt	Navnet på APN'en
Udgående serverprotokol	
MCC - Mobil landekode	Lad det være tomt for at bruge mmc fra installeret SIM
MNC - Mobilnetværkskode	Lad det være tomt for at bruge mnc fra det installerede SIM-kort
Serveradresse	
Serverens portnummer	
Serverens proxy-adresse	
Adresse på MMS-server	Lad det være tomt som standard
MMS-portnummer	Lad det være tomt som standard
MMS-proxy-adresse	Lad det være tomt som standard
Brugernavn	
Adgangskode	
Type adgangspunkt	Accepterede typer er "default", "mms", "supl".
	Hvis der sendes null eller empty, bruges som standard "default,supl,mms".
	Lad den være tom som standard.
Foretrukket APN	

Bluetooth

Tillad enhedsopdagelse via Bluetooth	
Tillad Bluetooth-parring	
Tillad Bluetooth-headset-enheder	
Tillad Bluetooth-håndfri enheder	
Tillad Bluetooth A2DP-enheder	A2DP, Advanced Audio Distribution Profile giver mulighed for lydstreaming mellem enheder
Tillad udgående opkald	
Tillad dataoverførsel via Bluetooth	
Tillad Bluetooth-tethering	
Tillad forbindelse til computeren via Bluetooth	

Forbindelse

Tillad kun nødopkaldTillad Wi-Fi	
Wi-Fi-netværkets mindste sikkerhedsniveau	
Forbyd brugeren at tilføje Wi-Fi-netværk	Denne begrænsning kan kun aktiveres, hvis mindst én aktiv wi-fi-profil er defineret under Connection Management.
Tillad SMS og MMS	
Tillad synkronisering under roaming	
Tillad stemme-roaming	

Android Enterprise – Fuldt administreret enhed med arbejdsprofil (COPE)

Generel forklaring af COPE

COPE er en forkortelse for **Corporate Owned Personally Enabled**.

COPE-tilstanden gør det muligt at tilmelde en Android-enhed som en **Android Enterprise - Fully Managed Device** med integreret **Android Enterprise - Container-profil**.

Dette kan enten være en Android-enhed, der allerede er tilmeldt som en **Android Enterprise - Fully Managed Device**, og som Android **Enterprise - Container** desuden er sat op på, eller en nytilmeldt Android-enhed, der er direkte tilmeldt som en Android **Enterprise - Fully Managed Device** sammen med **Android Enterprise - Container** oven på den.

COPE-tilstanden er kun tilgængelig for enheder med Android 8, 9 og 10

Konfiguration af profiler for COPE-enheder

Da der ikke er nogen konfigurationsprofil for selve COPE-tilstanden, er konfigurationen af **Android Enterprise - Fully Managed Device** og **Android Enterprise - Container** opdelt i to profiler inden for COPE-profilen. Det er muligt at skifte mellem de to profiler for konfigurationen af hver profil ved at klikke på den respektive knap i venstre side af konsollen:

Begge profiler kan konfigureres som beskrevet for hver enkelt profil:

Android Enterprise - Fuldt administreret enhed

Android Enterprise - Container

Tilbage til AE Fully Managed Device

Android Enterprise - Container-profilen kan fjernes som beskrevet i **Mobile Management**.

Ved at fjerne containerprofilen bliver COPE-profilen omdannet til en **Android Enterprise - Fully Managed Device-profil**.

Android Enterprise – Container-konfiguration

Afhængigt af om du i øjeblikket har valgt en gruppeprofil eller en enhed, er oversigten og dens underpunkter forskellige - vær opmærksom på dette!

Generelt

Profiloversigt (kun på profilniveau)

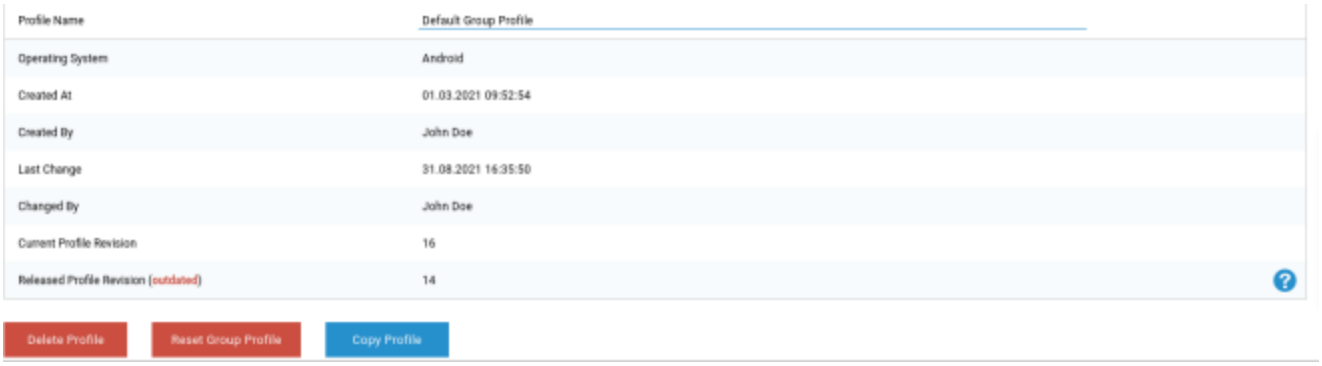
Hvis du er i en profil, får du en kort oversigt over profilen med hensyn til navn, operativsystem, oprettelsesdato, forfatter osv.

Navn på profil	Profilnavn - kan omdøbes direkte her
Operativsystem	Gyldigt operativsystem for profilen
Oprettet på	Dato for oprettelse
Oprettet af	Oprettet af
Sidste ændring	Sidste ændringsdato
Ændret af	Den bruger, der foretog de sidste ændringer i denne profil
Nuværende profilrevision	Antal gange profilen allerede er blevet opdateret
Udgivet profilrevision	Antal gange profilen allerede er blevet opdateret og har fået tildelt enheder

Slet profil	Slet profil
Nulstil gruppeprofil	Nulstil gruppeprofil
Kopier profil	Kopier profil

Oversigt over gruppeprofiler (kun på gruppeniveau)

Når du åbner en gruppeprofil, får du et hurtigt overblik over profilen.



Navn på profil	Navn på profilen (kan ændres her)
Operativsystem	Operativsystem, som profilen er til
Oprettet på	Tidspunkt for skabelse
Oprettet af	Profilens skaber
Sidste ændring	Tidspunkt for sidste ændring af profilen
Ændret af	Konto, der foretog de sidste ændringer
Nuværende profilrevision	Revision af gemt profiltilstand
Udgivet profilrevision	Tildelt profilrevision ("Tildel nu"). Hvis etiketten viser "(forældet)" bag teksten, betyder det, at du har gemt profilen, men ikke tildelt den endnu, så enhederne vil stadig få en ældre version.

Enhedsoversigt (kun på enhedsniveau)

Hvis du er på en enhed, får du en oversigt over den valgte enhed, som indeholder følgende:

Enhedens navn	Enhedens navn
Beliggenhed	Koordinater for placering
Telefonnummer	Telefonnummer
Tildelte obligatoriske apps	Antal tildelte obligatoriske apps
OS-version	Enhedens OS-version
Operativsystem	Operativsystem (Android Enterprise)
Serienummer	Enhedens serienummer
Ejerskab af enhed	Virksomheds- eller privat enhed
Enhedstype	AE-arbejdsstyret enhed
Rodfæstet	Status, der angiver, om enheden er blevet rootet
Overensstemmende	Overholder retningslinjerne
IP-adresse	Enhedens IP-adresse
Sidst set	Tidspunkt, hvor enheden sidst havde forbindelse til AppTec
Sidste skub	Tidspunkt, hvor det sidste push blev sendt til enheden
Brugertildeling	Den bruger eller gruppe, som denne enhed er tildelt

Config Revision

Her får du en oversigt over, hvilken gruppeprofil der er tildelt enheden.

Hvis du klikker på gruppeprofilen, får du direkte adgang til denne profil, og du kan foretage indstillinger.

Med dette symbol kan du gendanne de distribuerede apps til gruppeprofilens indstillinger.

Med dette symbol kan du sætte alle de anvendte apps tilbage til gruppeprofilens indstillinger.

"Nyere revision tilgængelig" angiver, at gruppeprofilen er blevet ændret og gemt, men ikke tildelt. Gruppeprofilen skal tildeles med "Tildel nu" på gruppeniveau for at anvende ændringerne på

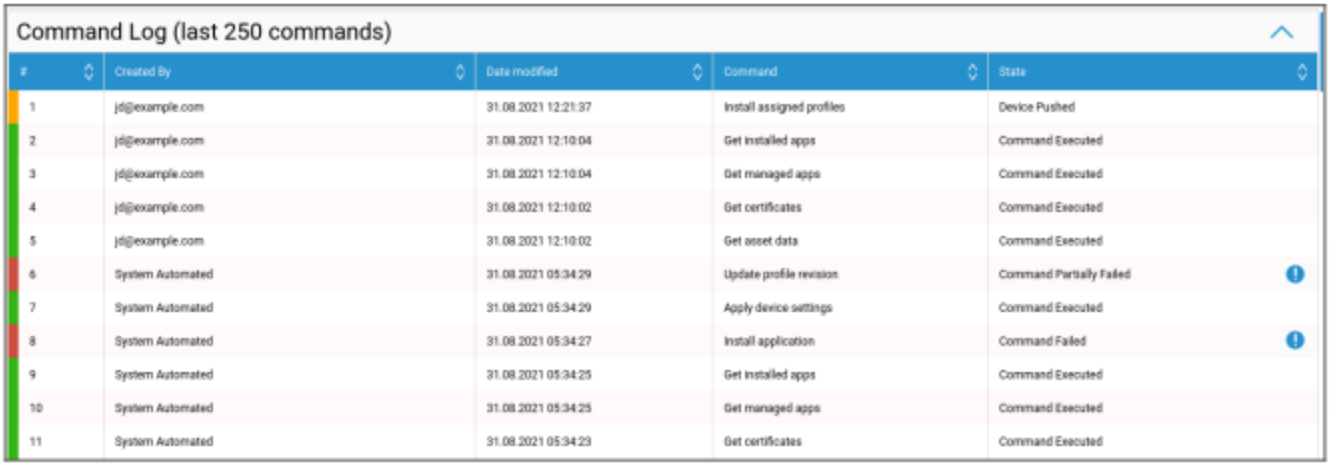
enhederne.

Enhedslog (kun på enhedsniveau)

Her vil du modtage forskellige enhedslogs. Hvis det er nødvendigt, kan du finde årsagen til en fejl direkte her.

Kommando-log

Her kan du se, hvilke kommandoer der er udstedt til enheden, og hvad deres status er.



Mulige kommandostatusser

Enhed skubbet	Der er sendt en push-anmodning til push-tjenesten (f.eks. APNS) for at fortælle enheden, at den skal oprette forbindelse tilbage til EMM-serveren.
Kommando oprettet	Kommandoen blev oprettet i systemet.
Kommando sendt	Kommandoen blev sendt til enheden, efter at den havde oprettet forbindelse til serveren.
Kommando udført	Kommandoen blev udført med succes.
Kommando mislykkedes	Kommandoen mislykkedes. *
Kommando delvist mislykket	Afhængigt af enhedens operativsystem kan nogle kommandoer blive grupperet sammen. Nogle dele af denne kommandogruppe mislykkedes. *
Kommandoen blev udført, men mislykkedes til sidst	Kommandoen blev udført, men måske blev den ikke.
Kommando genindført	Kommandoen blev repushed af en bruger.
Kasseret	Kommandoen blev kasseret. For eksempel fordi den blev erstattet af en anden kommando, eller fordi enheden blev genindskrevet, og gamle kommandoer blev fjernet.

*Hvis der er et udråbstegn bag beskeden, kan du få flere oplysninger ved at holde markøren over ikonet.

Enhedsindstillinger

Konfiguration af klienter

Her kan du udføre følgende konfigurationer på din Android-enhed:

Tid for manglende overholdelse	Tidsgrænsen for brugersvar, efter hvilken håndhævelseshandlingen anvendes.
Håndhævelse efter timeout for overholdelse	Håndhævelseshandling, når en bruger ikke udfører handlinger, der fører til en kompatibel enhedsstatus
Dataindsamlingsfrekvens	Hyppighed, hvormed enhedens/GPS-information skal indsamles
Enhedens hjerteslagsfrekvens	Interval, hvor enheden skal kontakte AppTec-serveren Min. 1 minut Maks. 24 timer
Aktivér opdateringer af placering	Hvis den er aktiveret, sender enheden placeringsopdateringer til AppTec Server.
Placering Opdateringstidspunkt	Bestemmer, i hvilke tidsintervaller enheden sender placeringsopdateringer til AppTec
Brug Google Location Accuracy til opdatering af placering	Hvis den er aktiveret, vil netværksplaceringen blive brugt til placeringsopdateringer (hvis den var deaktiveret under "Begrænsninger", vil denne indstilling ikke påvirke noget).
Brug GPS-placering til opdatering af placering	Hvis den er aktiveret, vil GPS'en blive brugt til at opdatere positionen.
Tillad falske lokationer	Tillader forfalskning af placeringsoplysninger via tredjepartsapps
Handling ved mistet forbindelse	Hvis det er aktiveret, kan du angive en handling for det tilfælde, at en enhed ikke får forbindelse til MDM-serveren inden for heartbeat-intervallet. Hvis enheden f.eks. har en heartbeat-tid på 5 minutter, opretter den forbindelse til serveren kl. 10:35. Derefter forlader enheden Wi-Fi-området. Det næste hjerteslag kl. 10:40 vil mislykkes, og den angivne handling vil blive udført.
Handling	Den handling, der skal foretages, så snart en enhed ikke overholder kravene.

	• Lock Device = låseenhed • Wipe Device = enheden gendannes til fabriksindstillingerne • Wipe Device & SD Card = enheden gendannes til fabriksindstillingerne, og SD-kortets lager slettes
Tærskel	Du kan angive en tærskel for mislykkede hjerteslag, som er nødvendige for at udløse den angivne handling.

Politisk håndhævelsestilstand	Standard:	Brugere vil med jævne mellemrum blive bedt om at udføre udestående handlinger
	Lazy Policy Enforcement:	Brugerne vil aldrig blive bedt om at udføre udestående handlinger. Alle åbne handlinger vil blive vist i AppTec Client
	Aggressiv håndhævelse af politikker:	Brugerne bliver hele tiden bedt om at udføre udestående handlinger
AppTec Version Lock	Hvis det er aktiveret, kan der angives en versionskode for AppTec-appen. AppTec-klienten vil kun opdatere til den angivne version. Nyere versioner vil blive ignoreret. En nedgradering er IKKE mulig.	
Versionskode	Versionskode for den AppTec-app, der skal låses på.	
Deaktiver AppTec Notification	Hvis den er deaktiveret, vil AppTec-klienten ikke vise en notifikation i notifikationslinjen. Brugere kan således lukke AppTec-klienten via task manager. Hvis AppTec-klienten er lukket, vil flere funktioner, herunder Kiosk Mode og App Black/Whitelisting, ikke fungere korrekt. Samsung-enheder tilbyder en beskyttelsesmekanisme for AppTec Client. Meddelelsen er som standard deaktiveret på Samsung-enheder, der understøtter KNOX API'er. Meddelelsen bør ikke være deaktiveret på enheder med Android 8.0 eller nyere.	

Baggrund

Indstil brugerdefineret baggrund	Aktiver/deaktiver det brugerdefinerede tapet
Baggrund	Indstil baggrundstilstanden til at bruge en farvekode eller et billede
Angiv en farve	Angiv en baggrundsfarve som hex-værdi, f.eks. #000000 for sort eller #ffffff som hvid.
Indstil billede som baggrund	Upload den billedfil, du vil bruge som baggrund

Asset Management (kun på enhedsniveau)

Enhedsinfo

Model	Enhedens modelbetegnelse
Operativsystem	OS
OS-version	OS-version
Serienummer	Serienummer
Enhedens navn	Enhedens navn
Batteristatus	Batteristatus
Fri / samlet hukommelse	Fri / samlet hukommelse
Samsung Safe	Samsung SAFE-grænseflade, nødvendig for en række indstillingsmuligheder
SD-kort tilgængeligt	SD-kort tilgængeligt
Emuleret SD-kort	SD-kort emuleret
SD-kort kan tages ud	SD-kort kan tages ud
SD Fri / Samlet hukommelse	SD-fri / samlet SD-kort-hukommelse

Wi-Fi

IP-adresse	Enhedens IP-adresse
WiFi MAC	WiFi MAC-adresse

Cellulær

Status	Status (SIM-kort installeret)
Telefonnummer	Telefonnummer
Roaming (tale/data)	Roaming til tale/data
Roaming-status	Aktuel roaming-status
IP-adresse	IP-adresse
Operatør/transportør	Operatør/transportør
Cellulær teknologi	Cellulær teknologi
IMEI	IMEI-nummer
ICCID	Dette er ID'et for SIM-kortet, ofte også et Smartcard eller Integrated Circuit Card (ICC).
IMSI	International Mobile Subscriber Identity (IMSI) giver i GSM- og UMTS-mobilnetværk en definitiv identifikation af netværksbrugerne. IMSI består af maksimalt 15 cifre og konfigureres på følgende måde: • Mobil landekode (MCC), 3 cifre • Mobilnetværkskode (MNC), 2 eller 3 cifre • Identifikationsnummer for mobilabonnenter (MSIN), 1-10 cifre
Nuværende MCC/MNC	Se "SIM MCC/MNC"
SIM MCC/MNC	Den mobile landekode er en etableret landeidentifikation, der er fastsat af ITU i henhold til E.212-standarden. Den fungerer sammen med mobilnetværkskoden (MNC) til identifikation af mobilnetværket. Betyder SIM-kortets landekode/mobilnetværkskode. Hvis du roamer til et andet mobilnetværk, vil "Current MCC/MNC" og "SIM MCC/MNC" logisk nok være forskellige.

Bluetooth

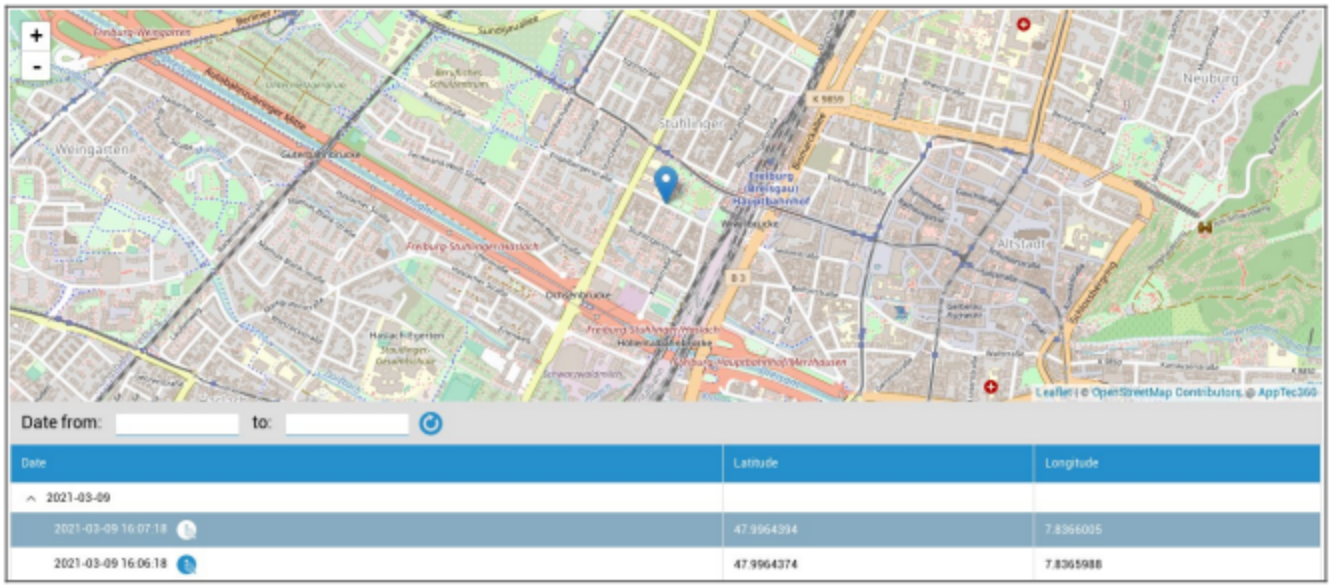
Bluetooth MAC	Bluetooth MAC-adresse

Sikkerhedsstyring

Tyverisikring (kun på enhedsniveau)

GPS-information (kun på enhedsniveau)

Her kan du fastlægge enhedens aktuelle/sidste placering. Lokaliseringen kan beskyttes med en eller endda to adgangskoder - se: Generelle indstillinger - Privatliv - GPS-adgang



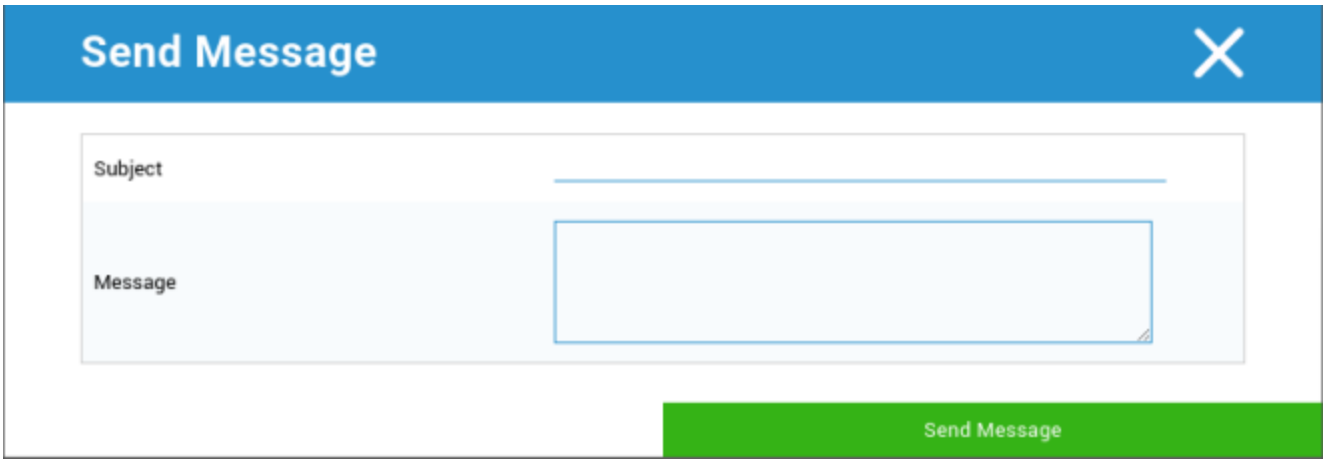
Tør og lås (kun på enhedsniveau)

Under "Wipe & Lock" kan du udføre følgende tre handlinger:

Fuld aftørring	Enheden gendannes til fabriksindstillingerne (både virksomhedsdata og personlige data slettes). Virker kun for Enhanced Work Profile
Enterprise Wipe	Kun virksomhedsdata fjernes fra slutbrugerens enhed (alle apps, data osv., der blev leveret af AppTec).
Låseskærm	Skærmlås er aktiveret, det er tilstrækkeligt at låse enheden op med enhedens adgangskode/PIN.

Besked (kun på enhedsniveau)

Her kan du udfylde emnet og en besked og sende den til en slutbrugerenhed



Sikkerhedskonfiguration

Enhedens adgangskode

Under "Adgangskode" kan du angive en adgangskode til enheden, og følgende indstillingsmuligheder er tilgængelige for dig

Minimumslængde for adgangskode	Fastsætter, hvor mange symboler en adgangskode som minimum skal indeholde	
Kvalitet af adgangskode	Uspecificeret	Denne politik har ingen krav til adgangskoden.
	Biometrisk svaghed	Denne politik tillader biometrisk genkendelsesteknologi med lav sikkerhed. Dette indebærer teknologier, der kan genkende en persons identitet til omkring en 3-cifret PIN-kode (falsk registrering er mindre end 1 ud af 1.000).
	Et eller andet	Denne politik kræver, at der indstilles en form for adgangskode eller et mønster, men den håndhæver ikke nogen specifikke regler.
	Alfabetisk	Brugeren skal have indtastet en adgangskode, der mindst indeholder alfabetiske tegn (eller andre symboler).
	Alfanumerisk	Brugeren skal have indtastet en adgangskode, der indeholder mindst både numeriske og alfabetiske tegn (eller andre symboler).
	Kompleks	Brugeren skal have indtastet en adgangskode, der som standard indeholder mindst et bogstav, et tal og et specialsymbol. Med denne adgangskodekvalitet kan adgangskoder begrænses til at indeholde forskellige sæt af tegn, f.eks. mindst et stort bogstav osv.
Minimumslængde for adgangskode	Indstil det krævede antal tegn for adgangskoden. Du kan f.eks. kræve, at PIN-koder eller adgangskoder skal indeholde mindst seks tegn.	
Minimum antal cifre, der kræves i adgangskoden	Minimum antal cifre, der kræves i adgangskoden	
Mindst små bogstaver kræves i adgangskoden	Mindst små bogstaver kræves i adgangskoden	
Minimum store bogstaver kræves i adgangskoden	Minimum store bogstaver kræves i adgangskoden	

Minimum af tegn, der ikke er bogstaver, i adgangskoden	Minimum af tegn, der ikke er bogstaver, i adgangskoden
Minimum af symboler i adgangskoden	Minimum af symboler i adgangskoden

Lås for maksimal inaktivitetstid	Maksimal brugerinaktivitet indtil tidslås
Timeout for udløb af adgangskode	Fastsætter, efter hvilket tidsinterval adgangskoden udløber, og en ny adgangskode skal udstedes
Begrænsning af adgangskodehistorik	Antal tidligere anvendte adgangskoder, der ikke er tilladt
Maksimalt antal mislykkede adgangskodeforsøg	Fastsætter, hvor ofte en adgangskode kan indtastes forkert, før en komplet sletning af enheden vil blive udført
Tillad biometrisk godkendelse	Muliggør godkendelse via fingeraftryk eller irisscanning. Kun til Samsung KNOX 2.1 og nyere

Adgangskode til container

Under "Adgangskode" kan du angive en adgangskode til containeren, og følgende indstillingsmuligheder er tilgængelige for dig

Minimumslængde for adgangskode	Fastsætter, hvor mange symboler en adgangskode som minimum skal indeholde	
Kvalitet af adgangskode	Uspecificeret	Denne politik har ingen krav til adgangskoden.
	Biometrisk svaghed	Denne politik tillader biometrisk genkendelsesteknologi med lav sikkerhed. Dette indebærer teknologier, der kan genkende en persons identitet til omkring en 3-cifret PIN-kode (falsk registrering er mindre end 1 ud af 1.000).
	Et eller andet	Denne politik kræver, at der indstilles en form for adgangskode eller et mønster, men den håndhæver ikke nogen specifikke regler.
	Alfabetisk	Brugeren skal have indtastet en adgangskode, der mindst indeholder alfabetiske tegn (eller andre symboler).
	Alfanumerisk	Brugeren skal have indtastet en adgangskode, der indeholder mindst både numeriske og alfabetiske tegn (eller andre symboler).
	Kompleks	Brugeren skal have indtastet en adgangskode, der som standard indeholder mindst et bogstav, et tal og et specialsymbol. Med denne adgangskodekvalitet kan adgangskoder begrænses til at indeholde forskellige sæt af tegn, f.eks. mindst et stort bogstav osv.
Minimumslængde for adgangskode	Indstil det krævede antal tegn for adgangskoden. Du kan f.eks. kræve, at PIN-koder eller adgangskoder skal indeholde mindst seks tegn.	
Minimum antal cifre, der kræves i adgangskoden	Minimum antal cifre, der kræves i adgangskoden	
Mindst små bogstaver kræves i adgangskoden	Mindst små bogstaver kræves i adgangskoden	
Minimum store bogstaver kræves i adgangskoden	Minimum store bogstaver kræves i adgangskoden	
Minimum af tegn, der ikke er bogstaver, i	Minimum af tegn, der ikke er bogstaver, i adgangskoden	

adgangskoden	
Minimum af symboler i adgangskoden	Minimum af symboler i adgangskoden

Lås for maksimal inaktivitetstid	Maksimal brugerinaktivitet indtil tidslås
Timeout for udløb af adgangskode	Fastsætter, efter hvilket tidsinterval adgangskoden udløber, og en ny adgangskode skal udstedes
Begrænsning af adgangskodehistorik	Antal tidligere anvendte adgangskoder, der ikke er tilladt
Maksimalt antal mislykkede adgangskodeforsøg	Fastsætter, hvor ofte en adgangskode kan indtastes forkert, før en komplet sletning af enheden vil blive udført

AntiVirus

Automatisk scanning	Aktivér periodiske automatiske scanninger
Scanningsinterval	Interval for undersøgelse (hurtig/fuld)
Fuld automatisk scanning	Aktivér fuldautomatiske scanninger
Automatiske opdateringer	Aktivér automatiske opdateringer
Interval for opdateringskontrol	Hvor ofte appen og dens database skal opdateres (virus/beskadiget kode)
App-beskyttelse	Aktivér automatisk app-scanning
Beskyttelse af SD-kort	Aktivér automatisk SD-kort-scanning
Kun Wi-Fi-opdatering	Når det er aktiveret, vil opdateringer kun blive anvendt, når enheden har forbindelse til et Wi-Fi-netværk.

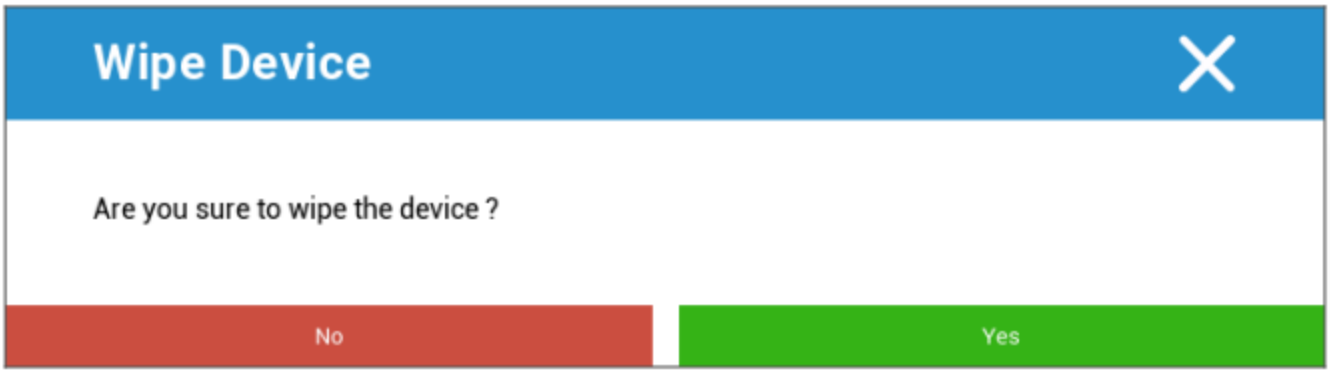
End of Life (kun på enhedsniveau)

Tør (kun på enhedsniveau)

Under "Wipe" kan du gendanne enheden til dens fabriksindstillinger (kun på Enhanced Work Profile).

Her slettes både virksomhedsdata og private data på slutbrugerens enhed.

Når du klikker på "Minus-symbolet", får du følgende besked:



Med "Ja" kan du udføre aftørringen.

Under "Wipe Report" kan følgende elementer vises

Slettet af	Historien om, hvem der udførte tørringen
Dato	Dato
Status	Status (f.eks. hvis Wipe blev udført med succes)

Begrænsningsindstillinger

Begrænsninger

Her kan en lang række ting begrænses og blokeres.

Håndhævelse af overholdelse	Mode Prompt User - Brugeren vil blive bedt om at udføre de nødvendige handlinger. Mode Lock-Down Container - Skjul alle apps, indtil alle krav er opfyldt
Politik for runtime-tilladelser	Spørg brugeren om nye tilladelser Giv altid nye anmodninger om tilladelse Afvis altid nye anmodninger om tilladelse Advarsel: Nogle apps har problemer med at genkende tilladelserne, hvis de er indstillet automatisk. Hvis du altid giver tilladelser og støder på problemer med apps, der siger, at der mangler tilladelser, skal du indstille dette til "spørg brugeren" og geninstallere appen.
Tillad udgående udklipsholder	Giver mulighed for at kopiere og indsætte indefra beholderen til ydersiden
Tillad opløsning af opkalds-id	Viser navnet på et indgående opkald baseret på kontakter i containeren
Tillad opløsning af kontaktsøgning	Giver mulighed for at søge efter navne i containerens kontakter, når du foretager opkald
Tillad deling af Bluetooth-kontakter	Giver adgang til beholderkontakt i en bil
Forbyd udgående NFC-beam	Deaktiverer NFC for containeren
Tillad ukendte kilder	Hvis det er aktiveret, kan brugerne sideloade apps ved at installere en .apk-fil.
Tillad USB-fejlfinding	Hvis den er aktiveret, kan brugerne aktivere USB-fejlfinding.
Forbud mod ændring af konto	Forbyder oprettelse, sletning og ændring af konti i containeren Husk, at nogle apps skal oprette eller ændre konti for at fungere som forventet.

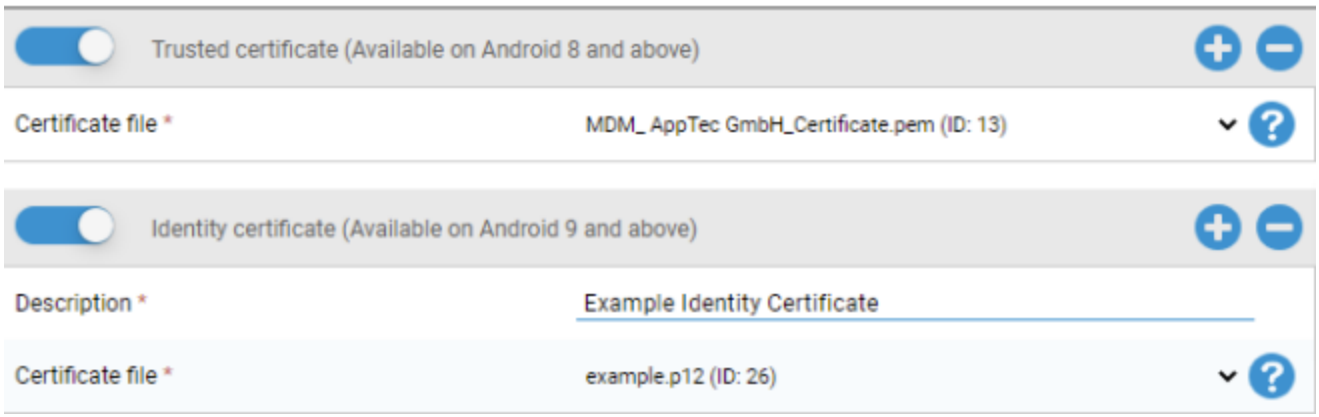
Begrænsninger i arbejdsprofilen. Kun tilgængelig på Android 11-enheder og nyere, med Enhanced Work Profile	
Forbyd kamera	Angiver, om kameraet ikke er tilladt i arbejdsprofilen.
Forbyd Bluetooth	Angiver, om Bluetooth ikke er tilladt i arbejdsprofilen.

Aktivér beskyttelse mod fabriksnulstilling	Aktiver dette for at tilsidesætte beskyttelsen mod fabriksnulstilling af Android til den Google-konto, du har defineret i "Generelle indstillinger" → "Android-konfiguration" → "Android Enterprise" → "Beskyttelse mod fabriksnulstilling" Hvis dette er aktiveret, og du nulstiller enheden, skal du angive den konfigurerede Google-konto for at opsætte enheden igen.
Kontrol af OS-opdatering	Aktivér dette for at indstille opdateringsadfærden til automatisk, med vindue eller udskudt.
Opdatering af politik	Automatisk: Installer automatisk, så snart en opdatering er tilgængelig. Med vindue: Installer automatisk inden for et dagligt vedligeholdelsesvindue. Dette konfigurerer også Play-apps til at blive opdateret inden for vinduet. Dette anbefales på det kraftigste til kioskenheder, fordi det er den eneste måde, hvorpå apps, der er fastgjort til forgrunden, kan opdateres af Play. Udsæt: Udsæt automatisk installation i op til 30 dage.

Begrænsninger for personlig profil. Kun tilgængelig på Android 11-enheder og nyere, med Enhanced Work Profile	
Forbyd kamera	Angiver, om kameraet ikke er tilladt i den personlige profil.
Forbyd Bluetooth	Angiver, om Bluetooth ikke er tilladt i den personlige profil.
Tillad ukendte kilder	Hvis det er aktiveret, kan brugere af arbejdsprofiler sideloade apps ved at installere en .apk-fil.

Administration af certifikater

Her kan du distribuere Trusted Certificates og Identity Certificates til dine enheder. Android 8 eller nyere kræves for at distribuere Trusted Certificates, og Android 9 eller nyere kræves for at distribuere Identity Certificates.



Med "+" kan du tilføje flere certifikater.

Betroede certifikater skal være i PEM-format.

Identitetscertifikater skal være i PKCS12-format.

Håndtering af forbindelser

Wifi

For denne indstilling skal du udføre forudgående konfiguration af slutbrugerenhederne for at få adgang til interne adgangspunkter

Identifikator for servicesæt (SSID)	SSID for det netværk, der skal tilsluttes
Skjult netværk	Aktivér, hvis AP'et ikke udsender SSID'et

Sikkerhedstype

Fastlæg AP'ets sikkerhedstype

WEP

Adgangskode	Adgangskode til AP'et

WPA/WPA2

Adgangskode	Adgangskode til AP'et

802.1x EAP

EAP-metode

PWD	Identitet	Identitet
	Adgangskode	Adgangskode

PEAP	Fase 2-godkendelsesprotokol	ingen	Ingen yderligere protokol
		MSCHAPV2	MSCHAPV2-protokol
		GTC	GTC-protokol
	CA-certifikat	CA-certifikat	
	Identitet	Identitet	
	Anonym identitet	Anonym identitet	
	Adgangskode	Adgangskode	

TTLS	Fase 2-godkendelsesprotokol	ingen	Ingen yderligere protokol
		PAP	PAP-protokol
		MSCHAP	MSCHAP-protokol
		MSCHAPV2	MSCHAPV2-protokol
		GTC	GTC-protokol
	CA-certifikat	CA-certifikat	
	Identitet	Identitet	
	Anonym identitet	Anonym identitet	
	Adgangskode	Adgangskode	

TLS	CA-certifikat	CA-certifikat
	Identitet	Identitet
	Adgangskode	Adgangskode

VPN

Navn på forbindelse	Navn på VPN-forbindelsen

VPN-type

VPN

VPN-klient

AppTec VPN-klient	
Gateway-konfiguration	Vælg Gateway VPN-konfiguration (se **Generelle indstillinger > Universal Gateway > VPN-indstillinger**)
Altid tændt VPN	Aktiver Native Lockdown
Aktivér AppTec Lockdown	Aktivér AppTec Lockdown

Indbygget (kun tilgængelig på Samsung-enheder)			
Tilslutningstype	PPTP	Server	Server
		Aktivér PPTP-kryptering	Aktivér PPTP-kryptering
	L2TP / IPSec PSK	Server	Server
		IPSec forhåndsdelt nøgle	IPSec forhåndsdelt nøgle
		Aktivér L2TP-hemmelighed	Aktivér L2TP-hemmelighed
		L2TP-hemmelighed	L2TP-hemmelighed
	IPSec XAuth PSK	Server	Server
		IPSec-identifikator	IPSec-identifikator
		IPSec forhåndsdelt nøgle	IPSec forhåndsdelt nøgle
Domæner til DNS-søgning	Domæner til DNS-søgning		
Ekspertindstillinger	DNS-servere	DNS-servere	
	Videresendelse af ruter	Videresendelse af ruter	

Åben VPN		
Server	Server	
OpenVPN-profil	OpenVPN-profil	
OpenVPN-app	OpenVPN til Android (anbefales)	
	OpenVPN-forbindelse	
Ekspertindstillinger	DNS-servere	DNS-servere
	Videresendelse af ruter	Videresendelse af ruter

Samsung / Stærk svane			
Tilslutningstype	PPTP	Server	Server
		Brugernavn	Brugernavn
		Adgangskode	Adgangskode
		Aktivér PPTP-kryptering	Aktivér PPTP-kryptering
	L2TP / IPSec PSK	Server	Server
		IPSec forhåndsdelt nøgle	IPSec forhåndsdelt nøgle
		Brugernavn	Brugernavn
		Adgangskode	Adgangskode
		Aktivér L2TP-hemmelighed	L2TP-hemmelighed
	IPSec XAuth PSK	Server	Server
		IPSec-identifikator	IPSec-identifikator
		IPSec forhåndsdelt nøgle	IPSec forhåndsdelt nøgle
		Brugernavn	Brugernavn
		Adgangskode	Adgangskode
Ekspertindstillinger	DNS-servere	DNS-servere	
	Videresendelse af ruter	Videresendelse af ruter	

Cisco Any Connect		
Server	Server	
Certifikat-tilstand	Handicappet	Handicappet
	Automatisk	Automatisk
Ekspertindstillinger	DNS-servere	DNS-servere
	Videresendelse af ruter	Videresendelse af ruter

VPN pr. app

VPN-klient

AppTec VPN-klient		
Gateway-konfiguration	Vælg Gateway VPN-konfiguration (se **Generelle indstillinger > Universal Gateway > VPN-indstillinger**)	
VPN-apps	VPN-apps	
Altid tændt VPN	Aktiver Native Lockdown	Altid tændt VPN
Aktivér AppTec Lockdown	Aktivér AppTec Lockdown	

Samsung / Stærk svane			
Tilslutningstype	PPTP	Server	Server
		VPN-apps	VPN-apps
		Brugernavn	Brugernavn
		Adgangskode	Adgangskode
		Aktivér PPTP-kryptering	Aktivér PPTP-kryptering
	L2TP / IPSec PSK	Server	Server
		VPN-apps	VPN-apps
		IPSec forhåndsdelt nøgle	IPSec forhåndsdelt nøgle
		Brugernavn	Brugernavn
		Adgangskode	Adgangskode
		Aktivér L2TP-hemmelighed	L2TP-hemmelighed
	IPSec XAuth PSK	Server	Server
		VPN-apps	VPN-apps
		IPSec-identifikator	IPSec-identifikator
		IPSec forhåndsdelt nøgle	IPSec forhåndsdelt nøgle
		Brugernavn	Brugernavn
		Adgangskode	Adgangskode
Ekspertindstillinger	DNS-servere	DNS-servere	
	Videresendelse af ruter	Videresendelse af ruter	

Begrænsninger

Her kan du indstille begrænsningerne i forhold til forbindelsesstyring

Tillad dataroaming	Tillad mobildata under roaming
Tving til dataroaming	Hvis den er aktiveret, er roaming for mobildata permanent aktiveret (anbefales ikke!). Denne indstilling overskriver indstillingen "Tillad dataroaming"!
Brug systemets http-proxyserver	Brugen af en HTTP-proxyserver, som leveres af systemets indstillinger i indstillinger, er afhængig af det tilsluttede netværk (WiFi eller APN).

PIM-styring

Gmail-udveksling

Info: Denne konfiguration vil blive anvendt på Gmail-appen. Så du skal godkende og installere Gmail.

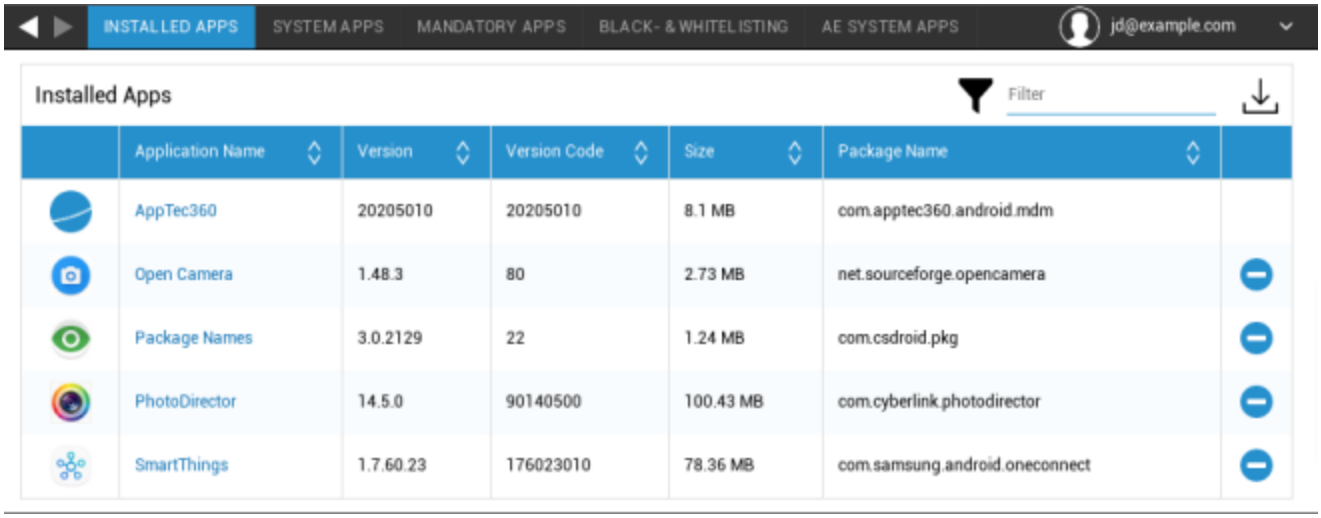
E-mail-adresse	Den angivne brugers e-mailadresse Bemærk "pladsholderne", som du kan bruge til at arbejde med legitimationsoplysninger, og du behøver ikke foretage ændringer manuelt på alle enheder. Med et klik kan du se dem for dig selv
Serverens værtsnavn	Serveradresse på dine Exchange-servere
Login-navn	Login-navnet for den respektive slutbrugerenhed, bemærk også "Placeholders here".
Underskrift	En underskrift kan vedhæftes (tip: Nogle enheder kræver HTML-formatering af underskriften).
Antal foregående dage, der skal synkroniseres	Antal dage, der bestemmer, hvornår e-mails synkroniseres tilbage
Enhedsidentifikator	En streng, der indeholder EAS DeviceID. Dette er en del af EAS-protokollerne og er nødvendigt i nogle områder.
Brug Secure Sockets Layer (SSL)	Brug en SSL-forbindelse
Accepter alle certifikater	Alle certifikater accepteres. Vælg denne indstilling, hvis din Exchange Server bruger et selvsigneret certifikat.
Tillad ikke-administrerede konti	Tillad brugere at tilføje eller fjerne enhver anden Exchange-konto end den konto, der er angivet i denne administrerede konfiguration. Hvis denne indstilling er aktiveret, kan du ikke forhindre brugere i at tilføje andre Exchange-konti til Gmail. Du kan heller ikke kontrollere datadeling mellem andre apps og Exchange-konti, som brugerne har tilføjet. Denne indstilling bør kun aktiveres, hvis dine brugere har brug for at vedligeholde mere end én arbejdsrelateret Exchange-konto i Gmail.
Klientcertifikat	Klientcertifikat. Kun påkrævet, hvis din mailserver forventer, at det er til stede.

App-administration

Enterprise App Manager

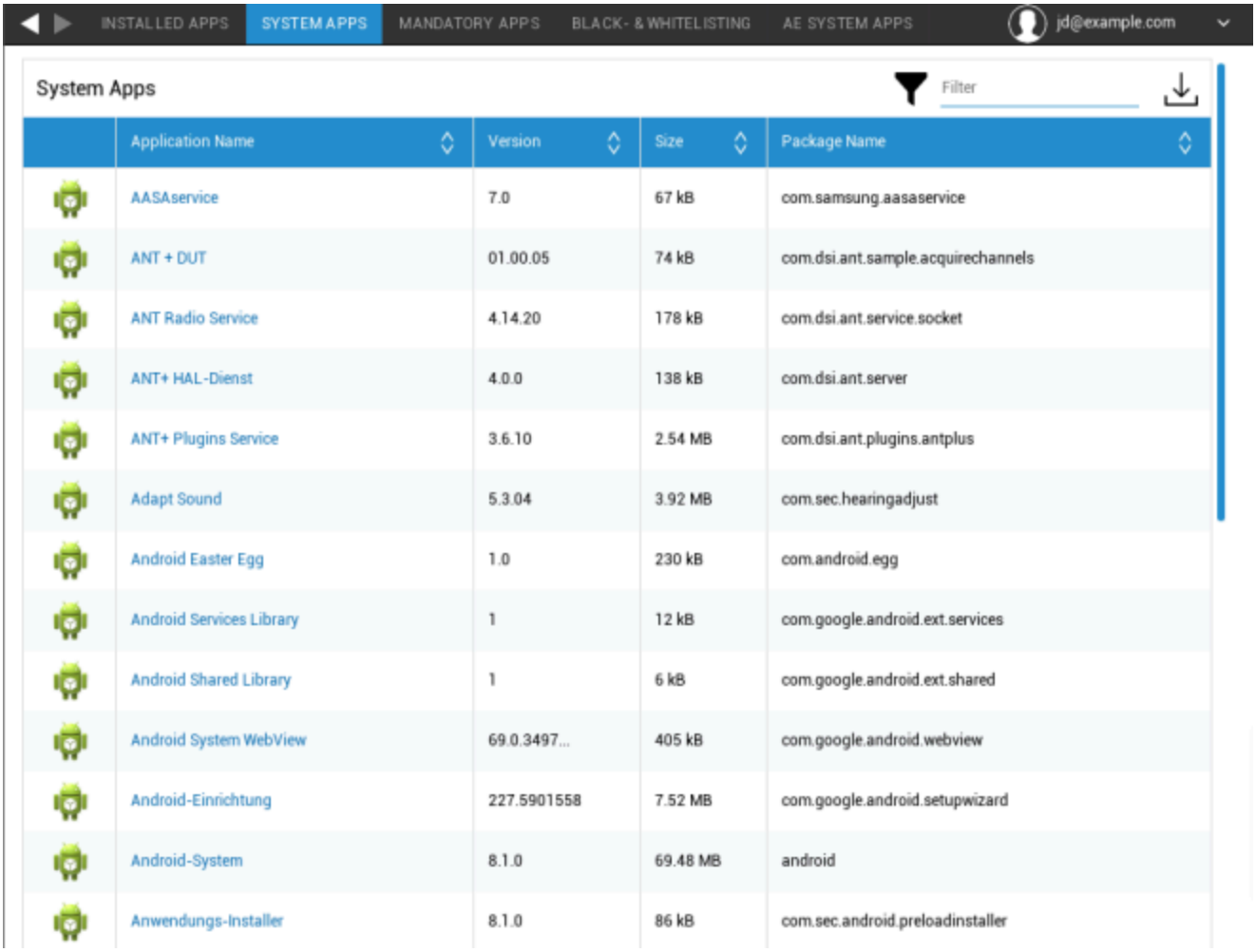
Installerede apps (kun på enhedsniveau)

Her vises alle de apps, der i øjeblikket er installeret i containeren.



System-apps (kun på enhedsniveau)

Under "System Apps" vil alle de apps og tjenester, der allerede er installeret på slutbrugerens enhed af enhedens producent, blive vist for dig.

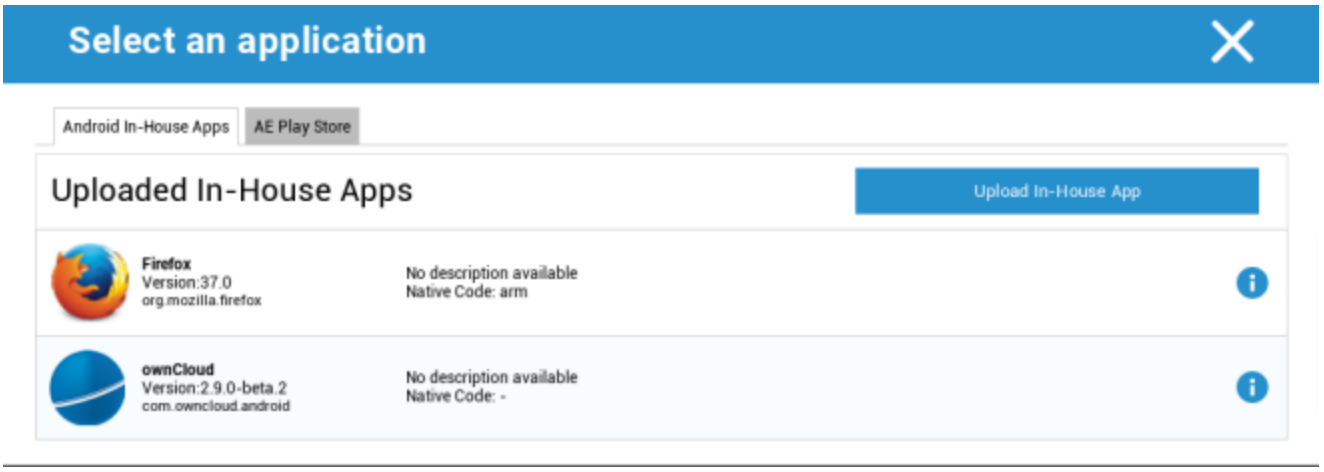


Obligatoriske apps

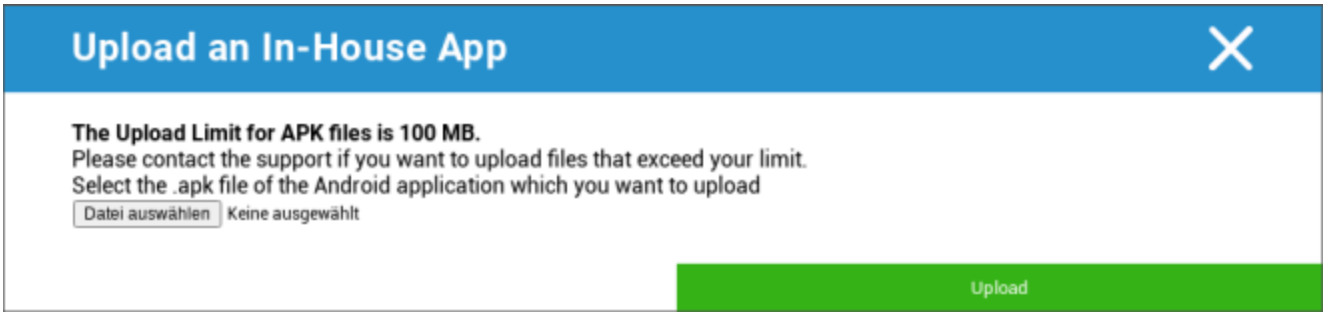
Under Obligatoriske apps kan du oprette de obligatoriske apps. Brugeren vil løbende blive bedt om at installere denne udpegede app, hvis det er en InHouse-app. Play Store-apps installeres automatisk.

Via kan den påkrævede app defineres.

Det kan være en intern app fra "Android In-House Apps", som du har uploadet i Generelle indstillinger.

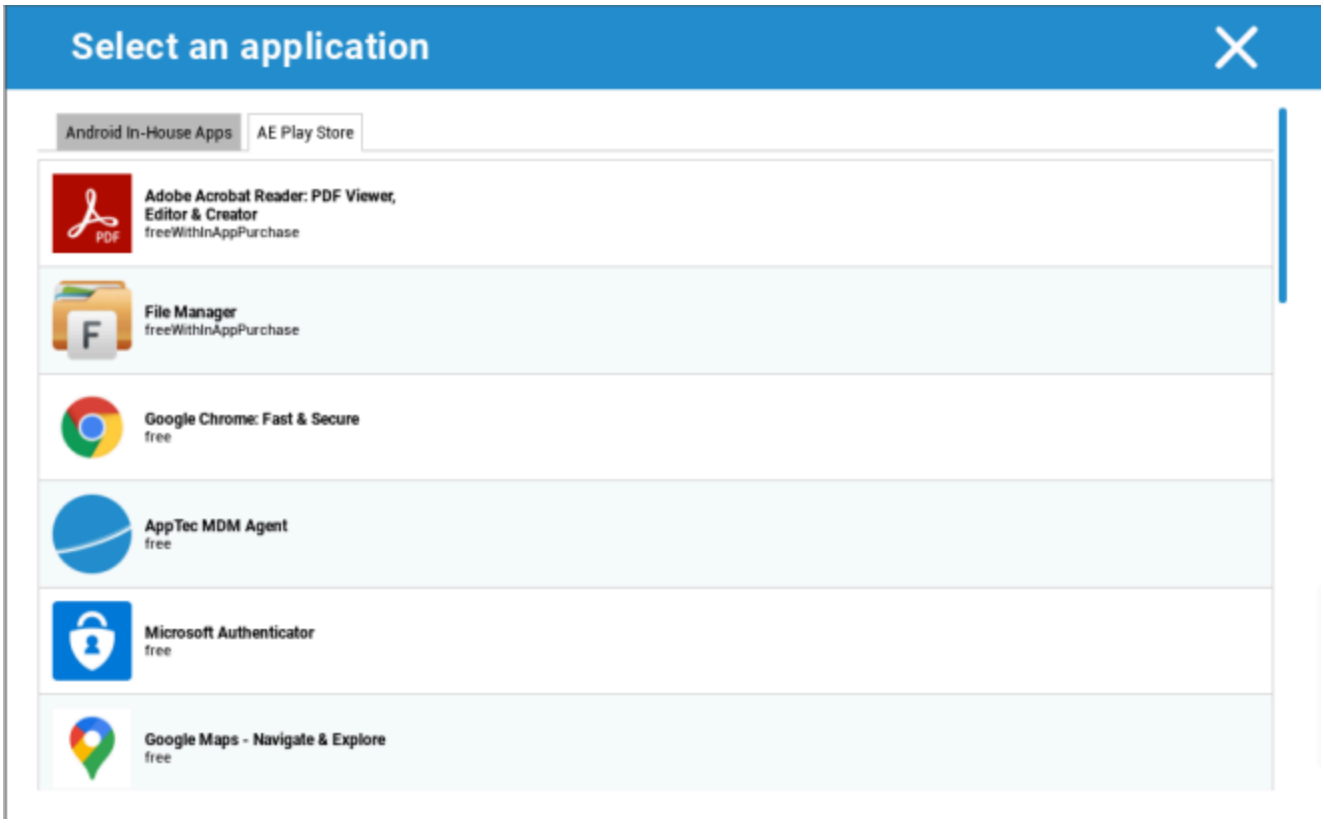


Du kan også vælge og uploade en apk-fil direkte med "Upload In-House App".



Hvis du installerer en In-House App, har du mulighed for at aktivere "Keep up to date". Hvis dette er aktiveret, og du har defineret en nyere version i In-House App DB, vil appen blive opdateret på enheden.

Eller det kan være en "AE Play Store"-app fra Google Work Play Store.



Kun godkendte "AE Play Store Apps" vil blive vist på denne fane.

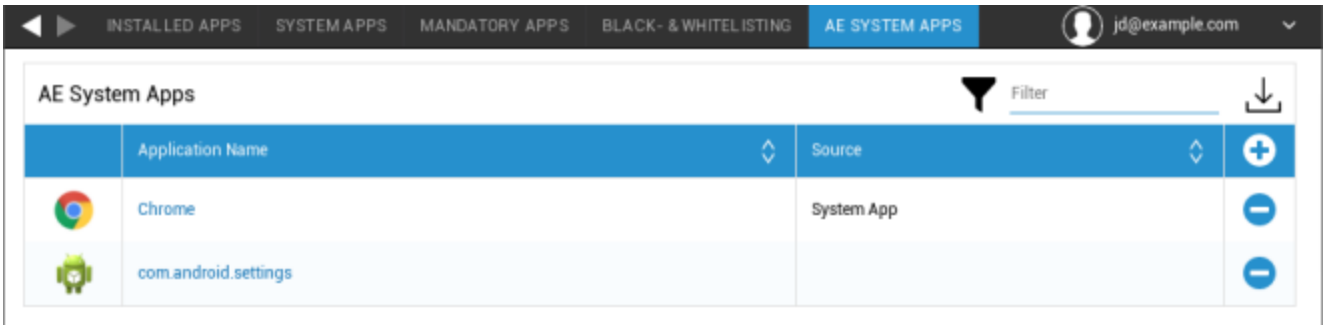
For at godkende en "AE Play Store-app" skal du gå til "Generelle indstillinger" > "Appadministration" > "AE Play".

Store" og tilføj en app via knappen, som sender dig videre til fanen "Play Store Apps" (eller du kan gå direkte til fanen "Play Store Apps").

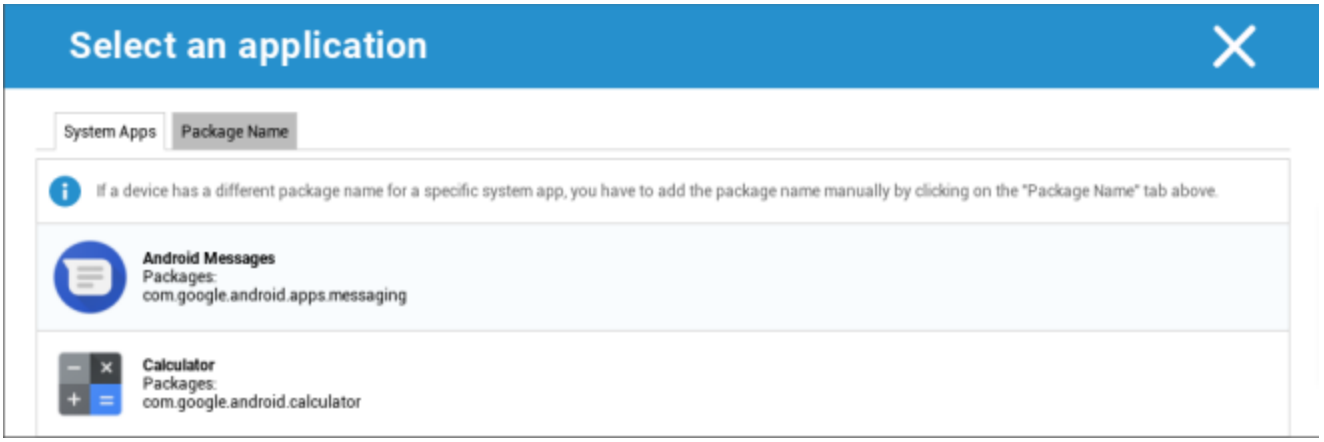
På fanen "Play Store Apps" kan du søge efter apps. Når du klikker på en app, åbnes app-siden, og her kan du godkende appen ved at klikke på "Approve".

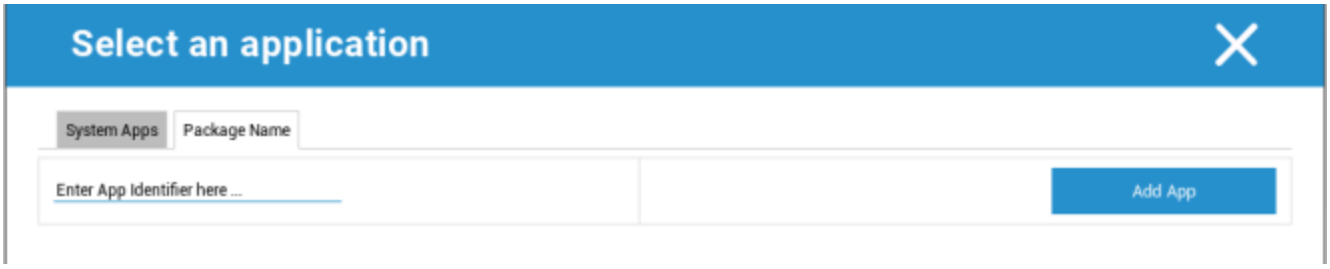
AE System Apps

Her kan du definere en liste, der indeholder specifikke systemapps, som skal aktiveres på enhederne.



Hvis du klikker på knappen, kan du vælge fra en liste over mulige systemapps fra Google eller direkte indtaste pakkenavnet på en systemapp, der skal aktiveres.





Husk, at systemapps på listen fra Google kun er apps, der kan være systemapps, men ikke nødvendigvis behøver at være systemapps på dine enheder.

Denne liste påvirker dog kun apps, der allerede er forudinstalleret.

Tilføjelse af apps, der ikke er forudinstalleret på dine enheder, vil ikke påvirke dine enheder, uanset om appen er fra listen fra Google, eller om appens pakkenavn indtastes direkte.

Begrænsninger og indstillinger

Indstillinger for app-administration

Her kan du konfigurere enhedens adfærd i forhold til app-opdateringer.

Hyppighed af opdateringstjek	Angiv, i hvilket interval AppTec-klienten skal søge efter app-opdateringer. Standardværdien er 24 timer.
Wi-Fi-tærskel	Apps, der er større end den angivne størrelse, downloades via Wi-Fi. Hvis "Kun Wi-Fi" er valgt, vil alle apps blive downloadet via Wi-Fi.

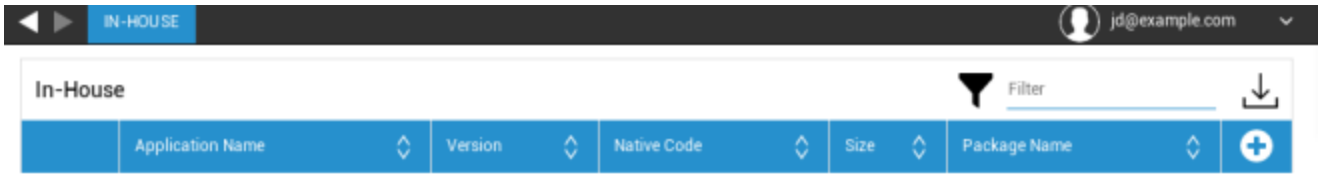
Enterprise App Store

Internt

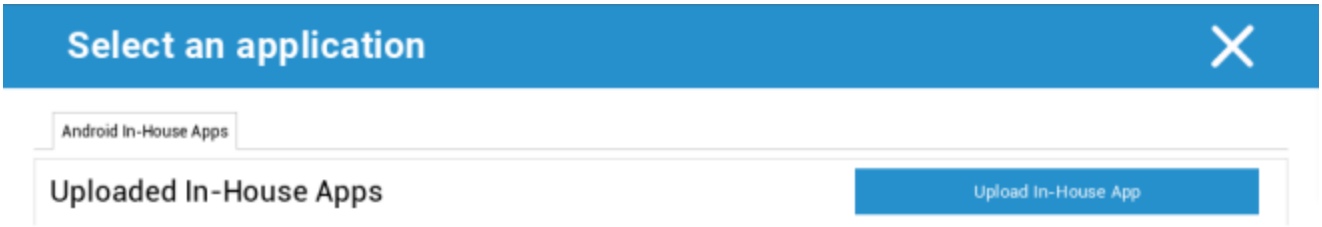
Under punktet "In-House" kan du uploade og distribuere internt udviklede apps.

Med symbolet kan du distribuere yderligere In-House Apps.

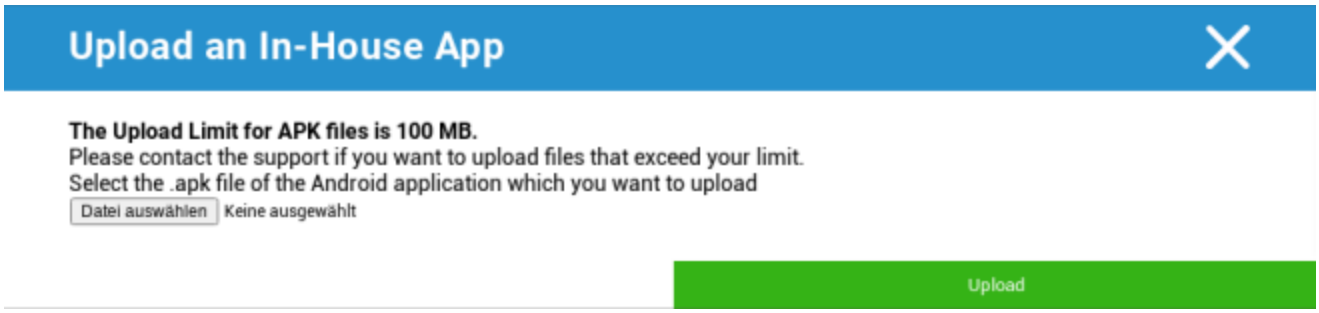
Hvis du installerer en In-House App, har du mulighed for at aktivere "Keep up to date". Hvis dette er aktiveret, og du har defineret en nyere version i In-House App DB, vil appen blive opdateret på enheden.



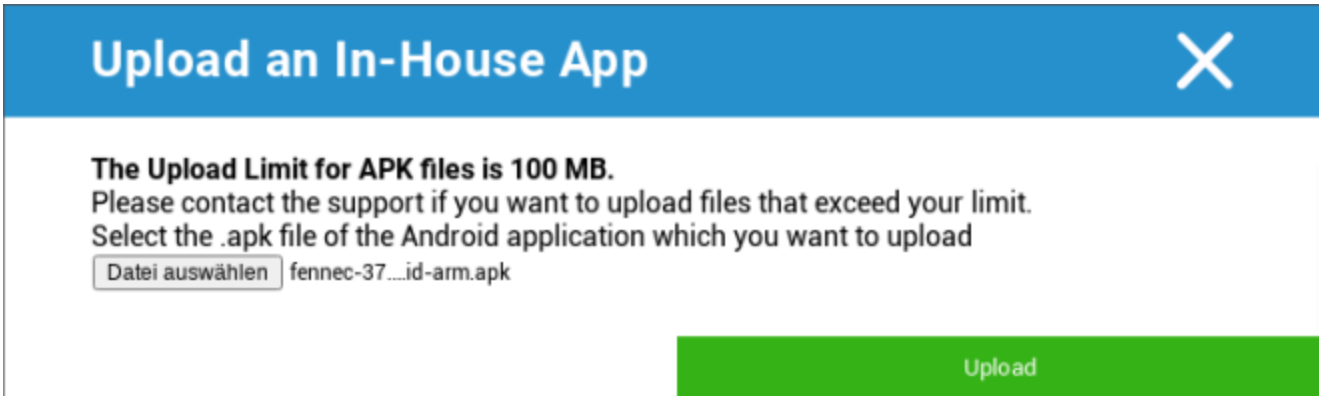
Hvis du ikke har distribueret In-House Apps, vil du modtage følgende oversigt:



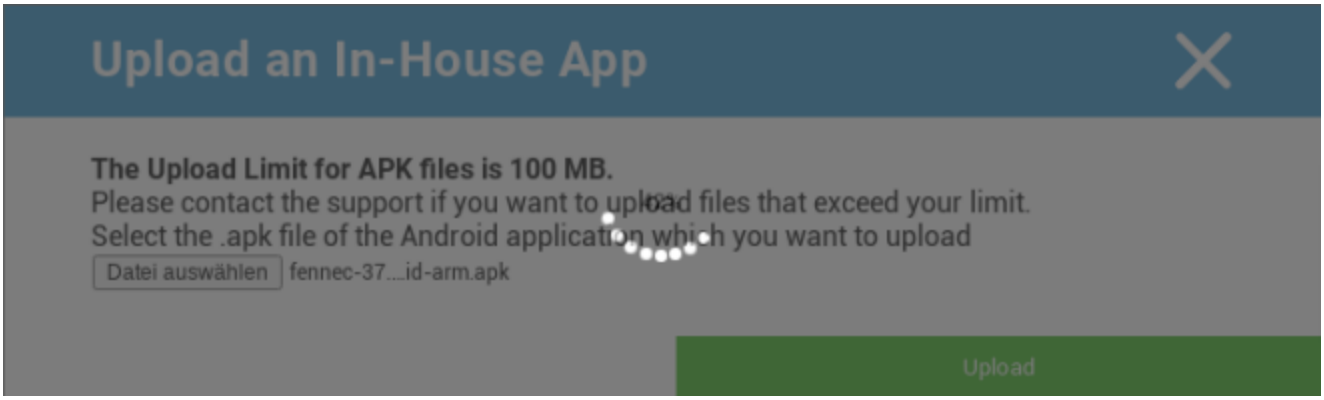
Klik på "Upload In-House App", så får du følgende oversigt:



Vælg nu med "Søg ..." en .apk-fil, og klik derefter på "Upload".



Din app vil nu blive uploadet, og i midten af cirklen vil du se en procentindikator, der viser, hvor meget af din app, der allerede er blevet uploadet.



Hvis uploaden af din interne app har været vellykket, kan du finde den uploadede app i dit app-katalog.

Brugeren har nu mulighed for at se og installere denne app i AppTec Store på slutbrugerens enhed under kategorien "In-House".

Da dette ikke involverer en Google PlayStore-app, har brugeren ikke brug for et gemt Google-id på sin respektive slutbrugerenhed.

Enterprise Play Store

AE Play Store

Her kan du tilføje apps til Android Enterprise Playstore. Bemærk, at du skal godkende apps med din AE-administratorkonto, før du kan tilføje dem.

For at godkende en app, se venligst instruktionerne i Obligatoriske apps.

Styring af indhold

Indholdsboks

Her kan du aktivere indholdsboksen.

Så snart du sætter "Enable ContentBox" til "On", installeres der automatisk en separat ContentBox-app på slutbrugerens enhed.

Sikker browser

Her kan du konfigurere indstillinger for AppTec Secure Browser.

Så snart du skifter sektionen i "Sikker browser" til "Til", installeres der automatisk en separat browser-app på slutbrugerens enhed.

Kræver adgangskode	Kræv, at brugeren opretter og bruger en adgangskode for at få adgang til browseren.
Mindste krævede password-længde	Indstil det krævede antal tegn for adgangskoden
Nødvendig adgangskodekvalitet	Indstil den krævede adgangskodekvalitet
Begræns downloads / åbn i	
Begræns uploads	
Upload hvidliste	En liste over URL'er, som det altid er tilladt at uploade til.
Tillad kopiering	Tillad at kopiere, klippe eller dele tekst inde på websiderne.
Tillad skærmoptagelse	Tillad optagelse af skærmbilleder.
Hyppighed af dataoprydning	Vælg, hvor ofte ALLE brugerdata (historik, cache osv.) skal fjernes automatisk.
Bogmærker til virksomheder	Bogmærkerne vil dukke op i mappen "Company bookmarks" i browserens bogmærker. De kan ikke redigeres af brugeren.
Skjul adresselinjen	
Whitelisting i browseren (uden Universal Gateway)	Aktiverer URL-whitelisting på klientsiden. • Virksomhedens bogmærker er altid whitelistet • Understøttes kun for 100 URL'er • Brug Universal Gateway til ubegrænset black- og whitelisting.
Hvidlistede webadresser	En liste over tilladte URL'er.
Gateway-baseret black- og whitelisting	Sortlistning har følgende krav: • En fungerende AppTec Universal Gateway ("Generelle indstillinger" → "Universal Gateway")

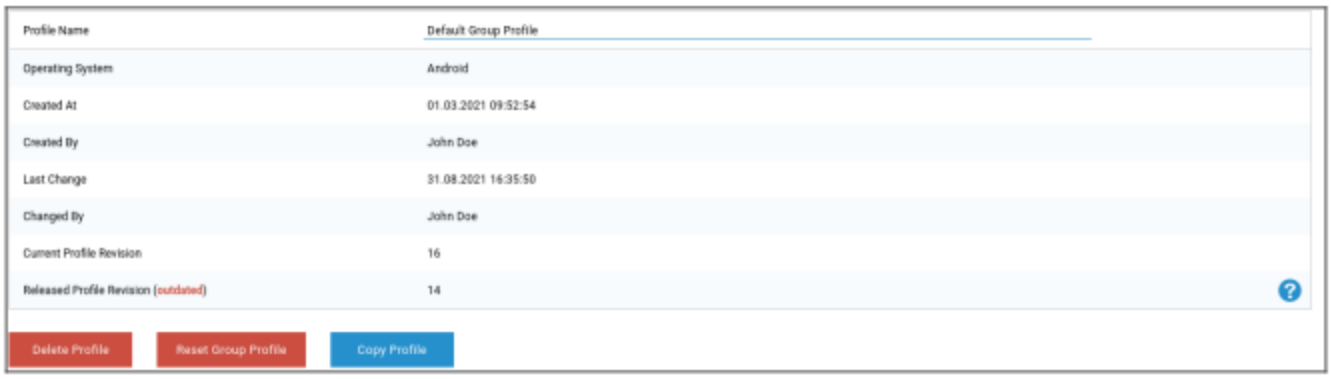
	• En fungerende VPN-konfiguration med en specificeret DNS-server ("Generelle indstillinger" → "Universal Gateway" → "VPN-indstillinger") • En sortlistekonfiguration ("Generelle indstillinger" → "Universal Gateway" → "Sortliste over domæner") • En gyldig VPN-forbindelse i profilen ("Forbindelsesstyring" → "VPN")

Android-konfiguration

Generelt

Oversigt over gruppeprofiler (kun på gruppeniveau)

Når du åbner en gruppeprofil, får du et hurtigt overblik over profilen.



Navn på profil	Navn på profilen (kan ændres her)
Operativsystem	Operativsystem, som profilen er til
Oprettet på	Tidspunkt for skabelse
Oprettet af	Profilens skaber
Sidste ændring	Tidspunkt for sidste ændring af profilen
Ændret af	Konto, der foretog de sidste ændringer
Nuværende profilrevision	Revision af gemt profiltilstand
Udgivet profilrevision	Tildelt profilrevision ("Tildel nu"). Hvis etiketten viser "(forældet)" bag teksten, betyder det, at du har gemt profilen, men ikke tildelt den endnu, så enhederne vil stadig få en ældre version.

Enhedsoversigt (kun på enhedsniveau)

Hvis du er på en enhed, får du en oversigt over den valgte enhed, som indeholder følgende:

Enhedens navn	Enhedens navn
Sidste kendte placering	De sidst kendte GPS-koordinater
Telefonnummer	Telefonnummer
Tildelte obligatoriske apps	Antallet af tildelte obligatoriske apps
OS-version	Enhedens OS-version
Operativsystem	Operativsystem (Android / iOS / Windows Phone)
Serienummer	Enhedens serienummer
Ejerskab af enhed	Virksomheds- eller privat enhed
Enhedstype	Telefon eller tablet
Rodfæstet	Status, der angiver, om enheden er blevet rootet
Overensstemmende	Overholder retningslinjerne
IP-adresse	IP-adresse
Sidst set	Tidspunkt, hvor enheden sidst havde forbindelse til AppTec
Sidste skub	Tidspunkt, hvor serveren sendte et push til enheden
Brugertildeling	En dropdown til at tildele enheden til en anden bruger

Config Revision (kun på enhedsniveau)

Her får du en oversigt over, hvilken gruppeprofil der er tildelt enheden.

Hvis du klikker på gruppeprofilen, får du direkte adgang til profilen, og du kan foretage indstillinger.

Med symbolet kan du gendanne de tildelte apps til gruppeprofilens indstillinger.

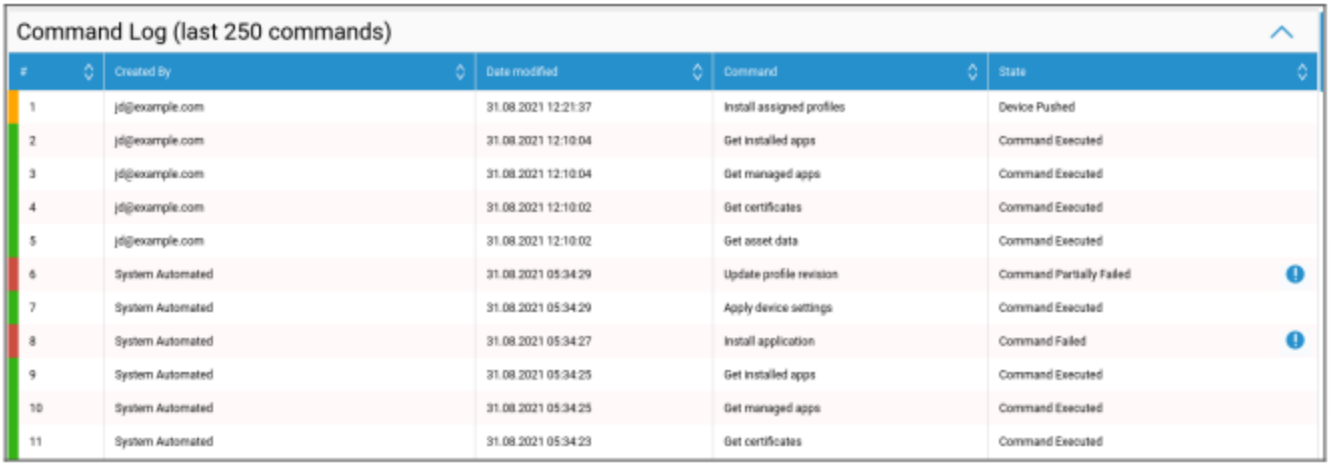
Med symbolet kan du nulstille enhedens profil, så den slet ikke har nogen indstillinger.

"Nyere revision tilgængelig" angiver, at gruppeprofilen er blevet ændret og gemt, men ikke tildelt. Gruppeprofilen skal tildeles med "Tildel nu" på gruppeniveau for at anvende ændringerne på enhederne.

Enhedslog (kun på enhedsniveau)

Kommando-log

Her kan du se, hvilke kommandoer der er udstedt til enheden, og hvad deres status er.



Kommandoer, der er oprettet af "System Automated", oprettes automatisk af systemet.

Mulige kommandostatusser

Enhed skubbet	Der er sendt en push-anmodning til push-tjenesten (f.eks. APNS) for at fortælle enheden, at den skal oprette forbindelse tilbage til EMM-serveren.
Kommando oprettet	Kommandoen blev oprettet i systemet.
Kommando sendt	Kommandoen blev sendt til enheden, efter at den havde oprettet forbindelse til serveren.
Kommando udført	Kommandoen blev udført med succes.
Kommando mislykkedes	Kommandoen mislykkedes. *
Kommando delvist mislykket	Afhængigt af enhedens operativsystem kan nogle kommandoer blive grupperet sammen. Nogle dele af denne kommandogruppe mislykkedes. *
Kommandoen blev udført, men mislykkedes til sidst	Kommandoen blev udført, men måske blev den ikke.
Kommando genindført	Kommandoen blev repushed af en bruger.
Kasseret	Kommandoen blev kasseret. For eksempel fordi den blev erstattet af en anden kommando, eller fordi enheden blev genindskrevet, og gamle kommandoer blev fjernet.

*Hvis der er et udråbstegn bag beskeden, kan du få flere oplysninger ved at holde markøren over ikonet.

Enhedsindstillinger

Konfiguration af klienter

Her kan du udføre følgende konfigurationer på din Android-enhed:

Advarselsmeddelelse efter deaktivering af Device Management	Etableret advarselsmeddelelse efter deaktivering af Device Management
Tid for manglende overholdelse	Tidsgrænse, efter hvilken "Håndhævelseshandling efter overholdelse" vil blive udført, hvis enheden ikke overholder kravene. Min. 1 minut Maks. 24 timer
Håndhævelse efter timeout for overholdelse	Den handling, der skal foretages, så snart en enhed ikke overholder kravene. • gør ingenting = ingen handling • Lock Device = låseenhed • Wipe Device = enheden gendannes til fabriksindstillingerne
Dataindsamlingsfrekvens	Hyppighed, hvormed enhedens/GPS-information skal indsamles
Enhedens hjerteslagsfrekvens	Interval, hvor enheden skal kontakte AppTec360-serveren Min. 1 minut Maks. 24 timer
Aktivér opdateringer af placering	Hvis den er aktiveret, sender enheden placeringsopdateringer til AppTec360 Server.
Placering Opdateringstidspunkt	Bestemmer, i hvilke tidsintervaller enheden sender placeringsopdateringer til AppTec
Brug Google Location Accuracy til opdatering af placering	Hvis den er aktiveret, vil Google Location Accuracy (tidligere kendt som netværksplacering) blive brugt til placeringsopdateringer (hvis den var deaktiveret under "Begrænsninger", vil denne indstilling ikke påvirke noget).
Brug GPS-placering til opdatering af placering	Hvis den er aktiveret, vil GPS'en blive brugt til at opdatere positionen.
Tillad falske lokationer	Tillader forfalskning af placeringsoplysninger via tredjepartsapps

Handling ved mistet forbindelse	Giver dig mulighed for at indstille en bestemt handling, som vil blive udført efter et bestemt antal mislykkede hjerteslag
Politisk håndhævelsestilstand	Definerer, hvor aggressivt AppTec360-klienten beder brugeren om at udføre visse handlinger, som kræver brugerinput. Interval (Standard) = Spørg i intervaller, så brugeren kan lade det køre i baggrunden i et stykke tid. Ingen advarsel = ingen popup for påkrævet interaktion. Du skal åbne AppTec360 Client manuelt for at kontrollere, om der er en påkrævet handling. Konstant alarm = Brugeren kan kun udføre den nødvendige handling. AppTec360-klienten vil tvinge sig selv i forgrunden, hvis brugeren forsøger at undgå den.
AppTec360 Version Lock	Lader dig definere en version af AppTec360-klienten, som er den maksimale version, klienten opdaterer sig selv til.

Baggrund

Her kan du definere et brugerdefineret tapet.

Med "Specify a Color" kan du definere en farve i hex-format (f.eks. #000000). Kun hex-værdier er tilladt.

Med "Sæt billede som baggrund" kan du uploade et billede. Vær opmærksom på, at forskellige enheder med forskellige launchers og OS-versioner fungerer forskelligt. Der er ingen generelle retningslinjer for størrelse og forhold, da det afhænger af enheden.

Brug JPG (eller JPEG) eller PNG som filformat.

Asset Management (kun på enhedsniveau)

Forvaltning af aktiver

Enhedsinfo

Model	**Enhedens modelbetegnelse**
Operativsystem	OS
OS-version	OS-version
AE-support	Understøttelse af Android Enterprise (container og fuldt administreret)
Serienummer	Serienummer
Enhedens navn	Enhedens navn
Batteristatus	Batteristatus
Fri / samlet hukommelse	Fri / samlet hukommelse
Samsung KNOX	Samsung KNOX API-niveau
SD-kort tilgængeligt	SD-kort tilgængeligt
Emuleret SD-kort	SD-kort emuleret
SD-kort kan tages ud	SD-kort kan tages ud
SD Fri / Samlet hukommelse	SD-fri / samlet SD-kort-hukommelse

Wi-Fi

IP-adresse	Enhedens IP-adresse
WiFi MAC	WiFi MAC-adresse

Cellulær

Status	Status (SIM-kort installeret)
Telefonnummer	Telefonnummer
Roaming (tale/data)	Roaming til tale/data
Roaming-status	Aktuel roaming-status
IP-adresse	IP-adresse
Operatør/transportør	Operatør/transportør
Cellulær teknologi	Cellulær teknologi
IMEI	IMEI-nummer
ICCID	Dette er ID'et for SIM-kortet, ofte også et Smartcard eller Integrated Circuit Card (ICC).
IMSI	International Mobile Subscriber Identity (IMSI) giver i GSM- og UMTS-mobilnetværk en definitiv identifikation af netværksbrugerne. IMSI består af maksimalt 15 cifre og konfigureres på følgende måde: • Mobil landekode (MCC), 3 cifre • Mobilnetværkskode (MNC), 2 eller 3 cifre • Identifikationsnummer for mobilabonnenter (MSIN), 1-10 cifre
Nuværende MCC/MNC	Se "SIM MCC/MNC"
SIM MCC/MNC	Den mobile landekode er en etableret landeidentifikation, der er fastsat af ITU i henhold til E.212-standarden. Den fungerer sammen med mobilnetværkskoden (MNC) til identifikation af mobilnetværket. Betyder SIM-kortets landekode/mobilnetværkskode. Hvis du roamer til et andet mobilnetværk, vil "Current MCC/MNC" og "SIM MCC/MNC" logisk nok være forskellige.

Bluetooth

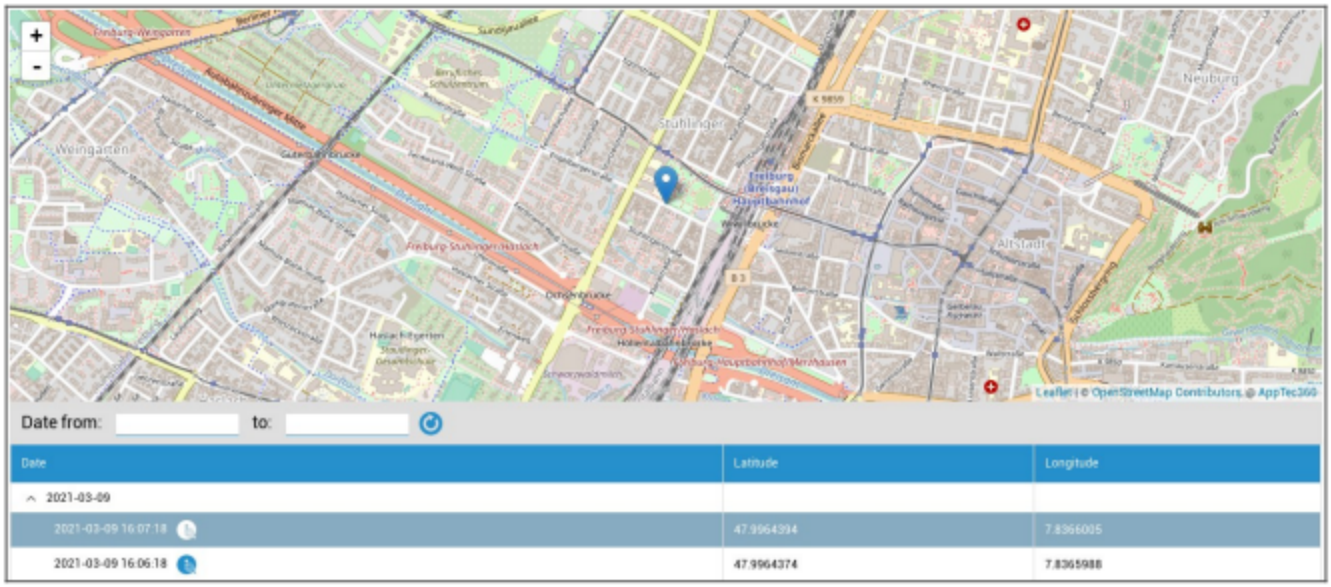
Bluetooth MAC	Bluetooth MAC-adresse

Sikkerhedsstyring

Tyverisikring (kun på enhedsniveau)

GPS-information (kun på enhedsniveau)

Her kan du fastlægge enhedens aktuelle/sidste placering. Lokaliseringen kan beskyttes med en eller endda to adgangskoder - se: Generelle indstillinger - Privatliv - GPS-adgang



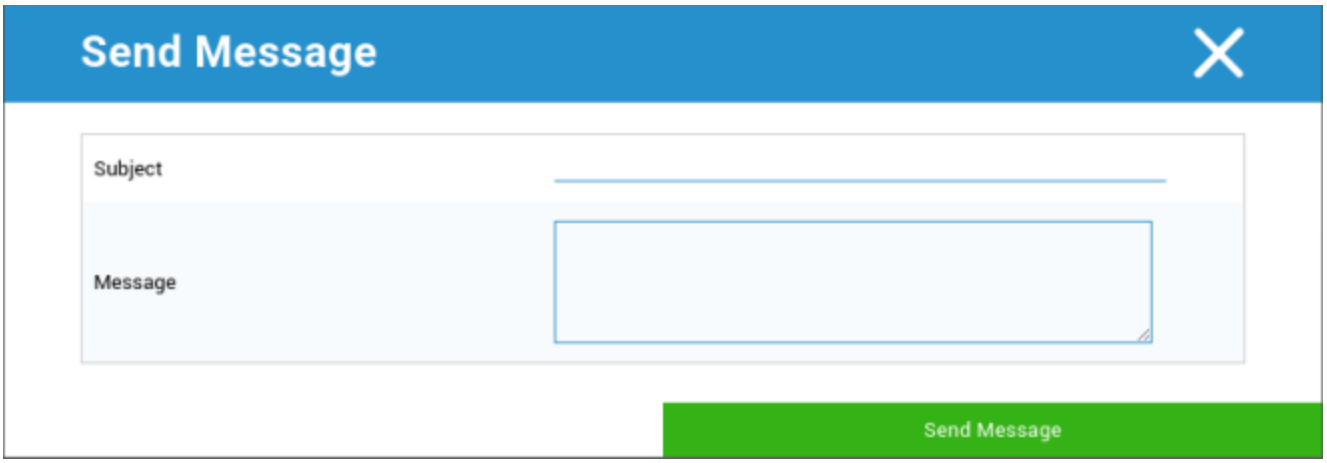
Tør og lås (kun på enhedsniveau)

Under "Wipe & Lock" kan du udføre følgende tre handlinger:

Fuld aftørring	Enheden gendannes til fabriksindstillingerne (både virksomhedsdata og personlige data slettes).
Enterprise Wipe	Kun virksomhedsdata fjernes fra slutbrugerens enhed (alle apps, data osv., der blev leveret af AppTec360).
Låseskærm	Skærmlås er aktiveret, det er tilstrækkeligt at låse enheden op med enhedens adgangskode/PIN.

Besked (kun på enhedsniveau)

Du kan udfylde emnet og en besked og sende den til en slutbrugerenhed. Denne besked vil blive vist i AppTec360 Client.



Sikkerhedskonfiguration

Adgangskode

Under "Adgangskode" kan du angive en adgangskode til enheden, og følgende indstillingsmuligheder er tilgængelige for dig

Minimumslængde for adgangskode	Fastsætter, hvor mange symboler en adgangskode som minimum skal indeholde
Kvalitet af adgangskode	Styrke af adgangskode Uspecificeret = ikke specificeret Alle adgangskoder er ok = alle adgangskoder er acceptable mindst numeriske tegn = skal indeholde mindst numeriske tegn mindst komplekse tegn = skal indeholde mindst specialtegn at least alphanumerical characters = skal indeholde mindst alfanumeriske tegn at least alphabetic characters = skal indeholde mindst alfabetiske tegn
Lås for maksimal inaktivitetstid	Maksimal timeout for skærmen. Dette konfigurerer kun den maksimale værdi, som kan vælges af brugeren.
Mindst små bogstaver kræves i adgangskoden	Mindst små bogstaver kræves i adgangskoden
Minimum store bogstaver kræves i adgangskoden	Minimum store bogstaver kræves i adgangskoden
Minimum af tegn, der ikke er bogstaver, i adgangskoden	Minimum af tegn, der ikke er bogstaver, i adgangskoden
Minimum antal cifre, der kræves i adgangskoden	Minimum antal cifre, der kræves i adgangskoden
Minimum af symboler i adgangskoden	Minimum af symboler i adgangskoden
Timeout for udløb af adgangskode	Fastsætter, efter hvilket tidsinterval adgangskoden udløber, og en ny adgangskode skal udstedes
Begrænsning af adgangskodehistorik	Antal tidligere anvendte adgangskoder, der ikke er tilladt
Maksimalt antal mislykkede adgangskodeforsøg	Fastsætter, hvor ofte en adgangskode kan indtastes forkert, før en komplet sletning af enheden vil blive udført

Kryptering

Under dette punkt kan du kryptere enhedens interne hukommelse såvel som SD-kortets hukommelse.

Kræv kryptering af opbevaring	Hvis denne indstilling er aktiveret, vil enhedens hukommelse blive krypteret, så længe enheden understøtter denne funktion. Når enhedens hukommelse er blevet krypteret første gang, er det ikke længere muligt at afkryptere den. Ligeledes vil adgangskodepolitikken automatisk blive ændret til 6 alfanumeriske symboler
Kræv kryptering af SD-kort	Denne indstilling gælder kun for Samsung-enheder! Hvis denne indstilling er aktiveret, kan det eksterne SD-kort krypteres og kan kun afkrypteres manuelt på slutbrugerens enhed. Ligeledes vil adgangskodepolitikken automatisk blive ændret til 6 alfanumeriske symboler

AntiVirus

Hvis du aktiverer AntiVirus, installeres Ikarus på enhederne. Vær opmærksom på, at dette kræver en separat licens, som kan indtastes i Generelle indstillinger → Appadministration → Tredjepartsapps.

Automatisk scanning	Definerer, om Ikarus skal scanne automatisk eller ej, og hvor ofte den skal scanne. Hvis du aktiverer "Fuld automatisk scanning", udføres en fuld scanning. Ellers vil der blive udført en hurtig scanning
Automatiske opdateringer	Aktiverer automatiske opdateringer af virusdatabasen og indstiller, hvor ofte det skal ske
App-beskyttelse	Aktiverer scanning af apps i tillæg til den almindelige scanning, der kun scanner filer
Beskyttelse af SD-kort	Aktiverer SD-kortbeskyttelse. Uden dette er scanningen begrænset til det lokale lager.
Kun Wi-Fi-opdatering	Begrænser opdatering til Wi-Fi

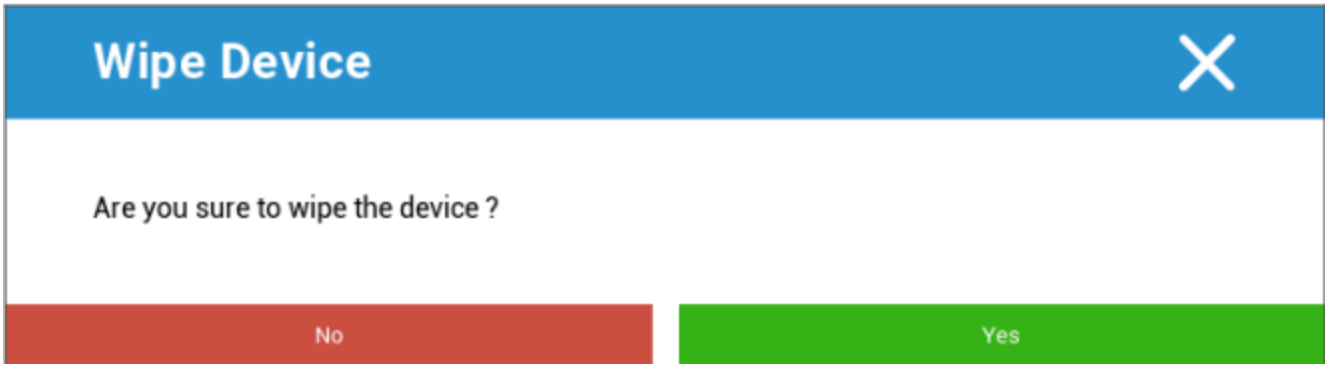
End of Life (kun på enhedsniveau)

Tør (kun på enhedsniveau)

Under "Wipe" kan du gendanne enheden til dens fabriksindstillinger. Her slettes både virksomhedsdata og private data på slutbrugerens enhed.

Når du klikker på "Minus-symbolet", bør du få følgende besked

Sletter du også SD-kortet?	SD-kortets hukommelse vil også blive slettet



Med "Ja" kan du udføre aftørringen.

Under "Wipe Report" kan følgende elementer vises

Slettet af	Historien om, hvem der udførte tørringen
Dato	Dato
Status	Status (f.eks. hvis Wipe blev udført med succes)

Begrænsningsindstillinger

Begrænsninger

Her kan en lang række ting begrænses og blokeres.

Aktivér kamera	Tillad brug af kamera
Fremtving automatisk synkronisering	Forholder sig til "Sync"-grænsefladen On = synkronisering er permanent aktiveret Off = synkronisering er permanent deaktiveret Brugervalg = valgt af brugeren
Force Bluetooth	On = Bluetooth er permanent aktiveret Off = Bluetooth er permanent deaktiveret Brugervalg = valgt af brugeren
Force GPS	On = GPS er permanent aktiveret Off = GPS er permanent deaktiveret Brugervalg = valgt af brugeren
Tving Googles placeringsnøjagtighed	On = Permanent internet-lokalisering Off = Permanent deaktivering af internetlokalisering Brugervalg = valgt af brugeren

For Samsung-enheder med KNOX 1.0 eller højere interface er følgende indstillingsmuligheder tilgængelige.

Tillad SD-kort	Tillad SD-kort
Tillad skrivning på SD-kort	Tillad "skrivning" på SD-kortet
Tillad skærmoptagelse	Tillad skærmoptagelse
Tillad udklipsholder	Tillad udklipsholder
Sikkerhedskopier indstillinger og app-data i Google Cloud	Off = deaktiverer Google Backup On = aktiver Google Backup Brugervalg = valgt af brugeren
Tillad USB-fejlfinding	Tillad USB-fejlfinding (bruges f.eks. til at oprette enhedslogs (ADB))
Tillad Google Crash Report	Tillad, at Google Crash Report sendes fra apps
Tillad fabriksnulstilling	Giver brugeren mulighed for at gendanne enheden til dens fabriksindstillinger
Tillad OTA-opgradering	Tillad "over-the-air"-opdateringer
Tillad USB-værtslagring	Hvis den er aktiveret, kan der tilsluttes USB-hukommelse i form af en HD eller en SD-kortlæser.
Tillad USB Media Player (MTP,PTP)	Tillad USB Media Player (MTP,PTP)
Tillad mikrofon	On = tillad mikrofon til tredjepartsapps Fra = blokér mikrofonen for tredjepartsapps Brugervalg = brugerne kan vælge, om tredjepartsappen har adgang til mikrofonen
Tillad NFC (Near Field Communication)	Tillad NFC
Tillad ukendte kilder (APK Sideloading)	Hvis det er aktiveret, er side-loading af apps (APK-filer) tilladt. Når denne indstilling er deaktiveret, skal brugeren aktivere den manuelt, når du tillader installation af APK'er fra ukendte kilder.
Tillad oprettelse af brugere	Tillader oprettelse af flere brugere

Ejer af AE-enhed

(Enheden skal være i Android Enterprise Device Owner Mode) Det anbefales at oprette enhederne som "Android Enterprise"-enhed og ikke som "Android"-enhed.

Sikkerhed	
Forbyd deling af placering	Angiver, om en bruger ikke må slå deling af placering til.
Forbyd sikker opstart	Angiver, om brugeren ikke må genstarte enheden i sikker opstartstilstand.
Forbyd nulstilling af netværk	Angiver, om en bruger ikke må nulstille netværksindstillinger fra Indstillinger.
Tillad ikke fabriksnulstilling	Angiver, om en bruger ikke må nulstille enheden.
Aktivér ADB	Giver mulighed for tilslutning til en pc via ADB
Deaktiver nøglebeskyttelse	Deaktiverer Keyguard
Enhedsejer Info om låseskærm	Indstiller de oplysninger om enhedens ejer, der skal vises på låseskærmen.
Håndhævelse af overholdelse	Mode Prompt User - Brugeren vil blive bedt om at udføre de nødvendige handlinger. Mode Lock-Down Container - Skjul alle apps, indtil alle krav er opfyldt

App-administration	
Tillad app-linking på tværs af profiler	Giver apps i den overordnede profil mulighed for at håndtere weblinks fra den administrerede profil.
Forbud mod app-kontrol	Angiver, om en bruger ikke må ændre programmer i indstillinger eller launchers.
Forbyd installation af app	Angiver, om en bruger ikke må installere programmer.
Forbyd afinstallation af apps	Angiver, om en bruger ikke må afinstallere programmer.
Politik for runtime-tilladelser	Angiver, hvordan nye anmodninger om tilladelse fra apps skal håndteres.
Tillad ukendte kilder	Hvis det er aktiveret, kan brugerne sideloade apps ved at installere en .apk-fil.

Forbindelse	
Afvis konfiguration af mobilnetværk	Angiver, om en bruger ikke må konfigurere mobilnetværk.
Forbyd tethering-konfiguration	Angiver, om en bruger ikke har tilladelse til at konfigurere Tethering og bærbare hotspots.
Forbyd VPN-konfiguration	Angiver, om en bruger ikke må konfigurere en VPN.
Forbyd Wifi-konfiguration	Angiver, om en bruger ikke må ændre WiFi-adgangspunkter.
Forbyd udgående NFC-beam	Angiver, om brugeren ikke må bruge NFC til at sende data fra apps.
Lås WiFi-konfiguration	Denne indstilling styrer, om WiFi-konfigurationer, der er oprettet af en enhedsejer-app, skal være låst (dvs. kun kunne redigeres eller fjernes af enhedsejer-appen, ikke engang af Indstillinger-appen).
Aktivér dataroaming	Aktiverer dataroaming

Bluetooth	
Forbyd Bluetooth	Angiver, om Bluetooth ikke er tilladt på enheden. Kræver Android 8.0
Forbyd Bluetooth-deling	Angiver, om udgående Bluetooth-deling ikke er tilladt på enheden. Kræver Android 8.0
Forbyd Bluetooth-konfiguration	Angiver, om en bruger ikke må konfigurere Bluetooth.

Kontoadministration	
Forbyd tilføjelse af administreret profil	Angiver, om en bruger ikke må tilføje administrerede profiler. Kræver Android 8.0
Forbyd tilføjelse af brugere	Angiver, om en bruger ikke må tilføje nye brugere.
Afvis Fjern administreret profil	Angiver, om administrerede profiler for denne bruger kan fjernes af andre end profilens ejer. Kræver Android 8.0
Forbud mod ændring af konto	Angiver, om en bruger ikke må tilføje og fjerne konti, medmindre de er tilføjet programmatisk af Authenticator.

Telefoni	
Forbyd udgående opkald	Angiver, at brugeren ikke må foretage udgående telefonopkald.
Forbyd SMS	Angiver, at brugeren ikke må sende eller modtage SMS-beskeder.

System	
Forbyd oprettelse af vinduer	Angiver, at der ikke skal oprettes andre vinduer end app-vinduer.
Forbud mod at indstille brugerikon	Angiver, om en bruger ikke må ændre sit ikon.
Tillad ikke Set Wallpaper	Brugerbegrænsning for ikke at tillade indstilling af et tapet.
Deaktiver statuslinje	Ved at deaktivere statuslinjen blokeres meddelelser, hurtigindstillinger og andre skærmoverlejringer, der gør det muligt at flygte fra en enhed til engangsbrug.
Aktivér automatisk tid	Indstiller tiden automatisk.
Aktivér automatisk tidszone	Indstiller tidszonen automatisk.
Bliv ved med at være tændt, mens du er tilsluttet	Enheden forbliver aktiv, mens den er tilsluttet en strømkilde.

Opbevaring	
Afvis deaktivering af app-verifikation	Angiver, om en bruger ikke må deaktivere programverifikation.

Forbyd montering af fysiske medier	Angiver, om en bruger ikke må montere fysiske eksterne medier.
Aktivér backup-service	Backupservice administrerer alle backup- og gendannelsesmekanismer på enheden. Hvis du sætter den til false, forhindres data i at blive sikkerhedskopieret eller gendannet. Backup-tjenesten er som standard slået fra. Kræver Android 8.0
Aktivér USB-masselager	Aktiverer brugen af USB-masselager.

Tastatur	
Forbyd automatisk udfyldning	Angiver, om en bruger ikke må bruge Autofill Services. Kræver Android 8.0
Forbud mod at kopiere og indsætte mellem profiler	Angiver, om det, der kopieres til udklipsholderen i denne profil, kan indsættes i relaterede profiler.

Lyd	
Afvis justering af volumen	Angiver, om en bruger ikke må justere mastervolumen.
Tillad ikke Slå mikrofonen fra	Angiver, om en bruger ikke må justere mikrofonens lydstyrke.
Mute-enhed	Mute-enhed.

Politik for systemopdatering	
Kontroller OS-opdateringer	Aktivér dette for at indstille opdateringsadfærden til automatisk, med vindue eller udskudt.

BYOD-container

Android Enterprise

Android Enterprise

Aktivér Android Enterprise	Aktivér Android Enterprise (AE). AE er understøttet fra Android 5.1 og opefter.
Håndhævelse af overholdelse	Mode Prompt User - Brugeren vil blive bedt om at udføre de nødvendige handlinger. Mode Lock-Down Container - Skjul alle apps, indtil alle krav er opfyldt
Politik for runtime-tilladelser	Spørg brugeren om nye tilladelser Giv altid nye anmodninger om tilladelse Afvis altid nye anmodninger om tilladelse Advarsel: Nogle apps har problemer med at genkende tilladelserne, hvis de er indstillet automatisk. Hvis du altid giver tilladelser og støder på problemer med apps, der siger, at der mangler tilladelser, skal du indstille dette til "spørg brugeren" og geninstallere appen.
Tillad udgående udklipsholder	Giver mulighed for at kopiere og indsætte indefra beholderen til ydersiden
Tillad opløsning af opkalds-id	Viser navnet på et indgående opkald baseret på kontakter i containeren
Tillad opløsning af kontaktsøgning	Giver mulighed for at søge efter navne i containerens kontakter, når du foretager opkald
Tillad deling af Bluetooth-kontakter	Giver adgang til beholderkontakt i en bil
Forbyd udgående NFC-beam	Deaktiverer NFC for containeren
Tillad ukendte kilder	Hvis det er aktiveret, kan brugerne sideloade apps ved at installere en .apk-fil.
Tillad USB-fejlfinding	Hvis den er aktiveret, kan brugerne aktivere USB-fejlfinding.
Forbud mod ændring af konto	Forbyder oprettelse, sletning og ændring af konti i containeren Husk, at nogle apps skal oprette eller ændre konti for at fungere som forventet.

Gmail-udveksling

Giver dig mulighed for at konfigurere Gmail i containeren. Vær opmærksom på, at aktivering af denne konfiguration ikke automatisk installerer appen. Du skal stadig tilføje denne app som obligatorisk app.

E-mail-adresse	E-mail-adresse
Serverens værtsnavn	Serverens værtsnavn
Login-navn	Login-navn
Underskrift	Underskrift
Antal foregående dage, der skal synkroniseres	Antal foregående dage, der skal synkroniseres.
Enhedsidentifikator	EAS-identifikator. Lad den være tom, hvis dit miljø ikke kræver dette.
Brug Secure Sockets Layer (SSL)	Aktiverer brug af SSL. Deaktivering af dette kan sænke sikkerheden
Accepter alle certifikater	Accepterer alle certifikater. Aktivering af dette kan sænke sikkerheden
Tillad ikke-administrerede konti	Giver brugeren mulighed for at tilføje yderligere konti
Klientcertifikat	Upload klientcertifikat, hvis din Exchange-server kræver dette

AE System Apps

Her kan du aktivere systemapps for Android Enterprise Container. Husk, at den angivne app skal være i systemets lager, ellers sker der ikke noget.

Adgangskode til container

Kun til Android 7.0 eller nyere

Giver dig mulighed for at indstille et specifikt krav til adgangskode for containeren.

Minimumslængde for adgangskode	Fastsætter, hvor mange symboler en adgangskode som minimum skal indeholde
Kvalitet af adgangskode	Styrke af adgangskode Uspecificeret = ikke specificeret Alle adgangskoder er ok = alle adgangskoder er acceptable mindst numeriske tegn = skal indeholde mindst numeriske tegn mindst komplekse tegn = skal indeholde mindst specialtegn at least alphanumerical characters = skal indeholde mindst alfanumeriske tegn at least alphabetic characters = skal indeholde mindst alfabetiske tegn
Lås for maksimal inaktivitetstid	Maksimal tid, indtil containeren bliver låst. Dette konfigurerer kun den maksimale værdi, som kan vælges af brugeren.
Mindst små bogstaver kræves i adgangskoden	Mindst små bogstaver kræves i adgangskoden
Minimum store bogstaver kræves i adgangskoden	Minimum store bogstaver kræves i adgangskoden
Minimum af tegn, der ikke er bogstaver, i adgangskoden	Minimum af tegn, der ikke er bogstaver, i adgangskoden
Minimum antal cifre, der kræves i adgangskoden	Minimum antal cifre, der kræves i adgangskoden
Minimum af symboler i adgangskoden	Minimum af symboler i adgangskoden
Timeout for udløb af adgangskode	Fastsætter, efter hvilket tidsinterval adgangskoden udløber, og en ny adgangskode skal udstedes
Begrænsning af adgangskodehistorik	Antal tidligere anvendte adgangskoder, der ikke er tilladt
Maksimalt antal mislykkede adgangskodeforsøg	Fastlægger, hvor ofte en adgangskode kan indtastes forkert, før containeren slettes.

Samsung KNOX

Aktivering

Her kan du aktivere Samsung KNOX Container. Vær opmærksom på, at dette ikke længere understøttes af Samsung på Android 10 eller nyere. Brug Android Enterprise Container på Android 10 eller nyere

Knox-adgangskode

Fastlæg de retningslinjer, der vedrører indstillingerne for enhedens adgangskode

Minimumslængde for adgangskode	Fastlægger, hvor mange symboler adgangskoden skal have
Kvalitet af adgangskode	Styrke af adgangskode Alle adgangskoder er ok = Alle adgangskoder er ok Mindst numeriske tegn = Mindst numeriske tegn skal være til stede Mindst komplekse tegn = Der skal mindst være specialtegn til stede Mindst alfanumeriske tegn = Mindst alfanumeriske tegn skal være til stede Mindst alfabetiske tegn = Mindst alfabetiske tegn skal være til stede
Minimumskrav til komplekse tegn	Minimum komplekse tegn skal være til stede
Maksimal timeout for inaktivitet	Maksimal timeout for brugerinaktivitet, før tastaturlås
Tillad godkendelse af fingeraftryk	Tillad godkendelse af fingeraftryk
Tillad iris-godkendelse	Tillad godkendelse med irisgenkendelse
Maks. alder på adgangskode	Fastlægger, efter hvilken tid adgangskoden udløber, og en ny adgangskode skal udstedes
Gemt adgangskodehistorik	Antal tidligere adgangskoder, der ikke er tilladt
Maksimalt antal mislykkede adgangskodeforsøg	Fastlægger, hvor ofte adgangskoden må indtastes forkert, før en komplet sletning af enheden finder sted.

Knox Sikkerhed

Begræns specifikke enhedsfunktioner

Aktivér kamera	Tillad brug af kameraet
Tillad Samsung KNOX App Store	Tillad brug af Samsung KNOX App Store
Tillad Google Play Services	Tillad Google Play Services

Tillad browser	Tillad brug af den oprindelige browser
Tillad skærmbilleder	Tillad oprettelse af skærmbilleder
Tillad import af kontakter	Hvis den er aktiveret, er det tilladt at få adgang til enhedens kontakter fra KNOX-containeren.
Tillad eksport af kontakter	Hvis den er aktiveret, er der adgang til KNOX-kontakterne fra enheden.
Tillad import af kalender	Hvis den er aktiveret, er det tilladt at få adgang til enhedens kalender fra KNOX-containeren.
Tillad eksport af kalender	Hvis den er aktiveret, er der adgang til KNOX-kalenderen fra enheden.
Tillad ikke-sikkert tastatur	Tillad brug af et ikke-sikkert tastatur
Aktivér filimport	Aktivér filimport til KNOX-containeren
Aktivér fileksport	Aktivér fileksport fra KNOX-containeren

Knox-udveksling

Her kan du konfigurere Exchange-profilen for KNOX-containeren

E-mail-adresse	Den angivne brugers e-mailadresse Bemærk "pladsholderne", som du kan bruge til at arbejde med legitimationsoplysninger, og du behøver ikke foretage ændringer manuelt på alle enheder. Med et klik på **Show Placeholders** kan du vise dem for dig selv
Serverens værtsnavn	Serveradresse på dine Exchange-servere
Login-navn	Login-navnet for den respektive slutbrugerenhed, bemærk også "pladsholderne" her
Domæne	Domæneadresse
Adgangskode (kun på enhedsniveau)	En individuel enhed kan eventuelt forsynes med en adgangskode, og hvis denne forbliver tom, vil brugeren blive bedt om at indtaste sin Exchange-adgangskode.
Antal foregående dage, der skal synkroniseres	Antal dage, der bestemmer, hvornår e-mails synkroniseres tilbage
Underskrift	En underskrift kan vedhæftes
Standardkonto	Fastslår, at denne e-mailkonto er standardkontoen
Brug Secure Sockets Layer (SSL)	Brug en SSL-forbindelse
Brug Transport Layer Security (TLS)	Brug en TLS-forbindelse
Accepter alle certifikater	Alle certifikater accepteres. Vælg denne indstilling, hvis din Exchange Server bruger et selvsigneret certifikat.

Knox eMail

E-mail-adresse	Den angivne brugers e-mailadresse Bemærk "pladsholderne", som du kan bruge til at arbejde med legitimationsoplysninger, og du behøver ikke foretage ændringer manuelt på alle enheder. Med et klik på **Show Placeholders** kan du vise dem for dig selv
Indgående serverprotokol	Indgående serverprotokol IMAP eller POP
Adresse på indgående server	Adresse på indgående server
Indgående serverport	Indgående serverport
Login/brugernavn til indgående server	Login/brugernavn til indgående server
Adgangskode til indgående server	Adgangskode til indgående server
Indgående server bruger SSL	Indgående server bruger SSL
Indgående server bruger TLS	Indgående server bruger TLS
Indkommende server accepterer alle certifikater	Indgående server accepterer alle typer certifikater
Udgående serverprotokol	Udgående serverprotokol SMTP
Udgående serverport	Udgående serverport
Udgående server bruger ekstra legitimationsoplysninger	Yderligere legitimationsoplysninger for den udgående server. Hvis den er sat til "off", bruges indstillingerne for den indgående server.
Login/brugernavn til udgående server	Login/brugernavn til udgående server
Adgangskode til udgående server	Adgangskode til udgående server
Udgående server bruger SSL	Udgående server bruger SSL
Udgående server bruger TLS	Udgående server bruger TLS
Udgående server accepterer alle certifikater	Udgående server accepterer alle typer certifikater
Underskrift	Her kan en underskrift vedhæftes
Giv brugeren besked ved modtagelse af ny e-mail	Giv brugeren besked ved modtagelse af ny e-mail

Knox-apps

Opret apps her, som du ønsker at distribuere til slutbrugernes enheder. Disse vil derefter være tilgængelige i KNOX-containeren. For at tilføje en app skal du gøre som i menuen Obligatoriske apps

Ansøgningens navn	Ansøgningens navn
Obligatorisk siden	Tidspunkt, hvor appen blev tilføjet
Kilde	Appens kilde (Play Store | Internt)

Ved at klikke på symbolet kan den pågældende app fjernes igen

Håndtering af forbindelser

Wifi

For denne indstilling skal du udføre forudgående konfiguration af slutbrugerenhederne for at få adgang til interne adgangspunkter

Identifikator for servicesæt (SSID)	SSID for det netværk, der skal tilsluttes
Skjult netværk	Aktivér, hvis AP'et ikke udsender SSID'et
Sikkerhedstype	Fastlæg AP'ets sikkerhedstype

Sikkerhedstype

WEP

Adgangskode	Adgangskode til AP'et

WPA/WPA2

Adgangskode	Adgangskode til AP'et

802.1x EAP

EAP-metode	

PWD	Identitet	Identitet
	Adgangskode	Adgangskode

PEAP	Fase 2-godkendelsesprotokol	ingen	Ingen yderligere protokol
		MSCHAPV2	MSCHAPV2-protokol
		GTC	GTC-protokol
	CA-certifikat	CA-certifikat	
	Identitet	Identitet	
	Anonym identitet	Anonym identitet	
	Adgangskode	Adgangskode	

EAP-metode	

TTLS	Fase 2-godkendelsesprotokol	ingen	Ingen yderligere protokol
		PAP	PAP-protokol
		MSCHAP	MSCHAP-protokol
		MSCHAPV2	MSCHAPV2-protokol
		GTC	GTC-protokol
	CA-certifikat	CA-certifikat	
	Identitet	Identitet	
	Anonym identitet	Anonym identitet	
	Adgangskode	Adgangskode	

TLS	CA-certifikat	CA-certifikat
	Identitet	Identitet
	Adgangskode	Adgangskode

VPN

Tilslutningstype	**Etablering af VPN-forbindelsestype**

Hvis du vælger "Per-App VPN" som VPN-type, ændres de tilgængelige VPN-klienter. Per-App VPN begrænser VPN'en til bestemte apps og starter VPN-forbindelsen automatisk, hvis en bestemt app startes.

AppTec360 VPN-klient	Bruger AppTec360 VPN Client i kombination med Universal Gateway
Navn på forbindelse	Navn på VPN-forbindelse
Gateway-konfiguration	Vælg VPN-konfigurationen for Universal Gateway
Altid på VPN	Tvinger VPN'en til altid at være aktiv, så hele trafikken går gennem VPN'en.
Aktiver Native Lockdown	Blokerer alt netværk, når enheden ikke er forbundet til VPN. Brug dette med omtanke, da det kan medføre, at hele forbindelsen går tabt, hvis det ikke er konfigureret korrekt. Kun for Android Enterprise på Android 7 eller nyere
Aktivér AppTec360 Lockdown	Blokerer brugen af alle apps, indtil VPN-forbindelsen er startet

Cisco AnyConnect	
Navn på forbindelse	Navn på VPN-forbindelse
Server	Serverens adresse
Certifikat-tilstand	Deaktiveret = deaktiveret Automatisk = automatisk

L2TP (kun KNOX)	Kun tilgængelig på Samsung-enheder
Navn på forbindelse	Navn på forbindelse
Server	Server-adresse
Aktivér L2TP-hemmelighed	
Domæner til DNS-søgning	Domæner til DNS-søgning

Tilslutningstype	**Etablering af VPN-forbindelsestype**

PPTP (kun KNOX)	Kun tilgængelig på Samsung-enheder
Navn på forbindelse	Navn på VPN-forbindelse
Server	Server-adresse
Aktivér kryptering	Aktivér kryptering
Domæner til DNS-søgning	Domæner til DNS-søgning

L2TP / IPSec PSK (kun KNOX)	Kun tilgængelig på Samsung-enheder
Navn på forbindelse	Navn på VPN-forbindelse
Server	Serveradresse
IPSec forhåndsdelt nøgle	Forhåndsdelt nøgle til autentificering
Aktivér L2TP-hemmelighed	
L2TP-hemmelighed	
Domæner til DNS-søgning	Domæner til DNS-søgning

IPSec XAuth PSK (kun KNOX)	Kun tilgængelig på Samsung-enheder
Navn på forbindelse	Navn på VPN-forbindelse
Server	Serveradresse
IPSec-identifikator	Brugernavn til forbindelsen
IPSec forhåndsdelt nøgle	Adgangskode til forbindelsen
Domæner til DNS-søgning	Domæner til DNS-søgning

OpenVPN	

Navn på forbindelse	Navn på forbindelse
OpenVPN-profil	Det er her, indholdet af .ovpn-filen bliver kopieret
OpenVPN-app	Der findes to forskellige apps til brug af OpenVPN Vi anbefaler appen "OpenVPN for Android". Men alternativt kan appen "OpenVPN Connect" bruges.

Begrænsninger

Her kan du indstille begrænsningerne i forhold til forbindelsesstyring.

Tillad dataroaming	Tillad mobildata under roaming
Tving til dataroaming	Hvis den er aktiveret, er roaming for mobildata permanent aktiveret (anbefales ikke!). Denne indstilling overskriver indstillingen "Tillad dataroaming"!
Følgende indstillinger er kun tilgængelige på Samsung KNOX 2.0 eller højere	
Tillad kun nødopkald	Tillad kun nødopkald
Tillad WiFi	Tillad WiFi
Minimum sikkerhedsniveau for WiFi-netværk	WiFi-netværkets mindste sikkerhedsniveau Åben = alle typer WiFi er tilladt
Forbyd brugeren at tilføje WiFi-netværk	Brugeren kan ikke selv tilføje et WiFi-netværk Denne indstilling er kun mulig, hvis der er defineret en WiFi-profil under "Connection Management".
Tillad SMS og MMS	Alle = Al SMS- og MMS-trafik er tilladt Kun indgående SMS = Kun indgående SMS-beskeder er tilladt Kun udgående SMS = Kun udgående SMS-beskeder er tilladt Ingen = Ingen SMS/MMS-trafik er tilladt
Tillad synkronisering under roaming	Tillad synkronisering under roaming On = aktiveret Off = deaktiveret Brugervalg = brugerens valg
Tillad stemme-roaming	Tillad stemme-roaming On = aktiveret Off = deaktiveret User Choice = brugerens valg
Brug systemets http-proxyserver	Brugen af en HTTP-proxyserver, som leveres af systemets indstillinger i indstillinger, er afhængig af det tilsluttede netværk (WiFi eller APN).

APN

Følgende indstillinger er kun tilgængelige på Samsung SAFE 2.0 eller nyere!

APN-visningsnavn	APN-visningsnavn	
Navn på adgangspunkt	APN's navn	
Udgående serverprotokol	Ikke indstillet	
	Ingen	
	PAP	PAP-protokol
	CHAP	CHAP-protokol
	PAP eller CHAP	Enten PAP- eller CHAP-protokollen
MCC - Mobil landekode	MCC indtastes her, lad dette felt være tomt, hvis det isatte SIM-korts MCC skal bruges.	
MNC - Mobilnetværkskode	MNC indtastes her, lad dette felt være tomt, hvis det isatte SIM-korts MCC skal bruges.	
Serverens adresse	Serverens adresse	
Serverens portnummer	Serverens portnummer	
Serverens proxy-adresse	Serverens proxy-adresse	
Adresse på MMS-server	MMS-serveradresse, lad den være tom for Standard	
MMS-portnummer	MMS-portnummer	
MMS-proxy-adresse	MMS-proxy-adresse	
Brugernavn	Brugernavn	
Adgangskode	Adgangskode	
Type adgangspunkt	Tilladte typer er: "standard", "mms", "supl" Hvis dette felt er tomt, vil "default,supl,mms" blive brugt.	
Foretrukket APN	APN foretrækkes	

Bluetooth

Her kan man foretage en række forskellige Bluetooth-indstillinger.

Følgende indstillinger er kun tilgængelige på Samsung KNOX 1.0 eller højere!

Tillad enhedsopdagelse via Bluetooth	Tillad opdagelse af enheder via Bluetooth
Tillad Bluetooth-parring	Tillad Bluetooth-parring
Tillad Bluetooth-headset-enheder	Tillad Bluetooth-headset-enheder
Tillad Bluetooth-håndfri enheder	Tillad Bluetooth-håndfri enheder
Tillad Bluetooth A2DP-enheder	Tillad Bluetooth A2DP-lydstreaming mellem enheder
Tillad udgående opkald	Tillad udgående opkald viaBT
Tillad dataoverførsel via Bluetooth	Tillad dataoverførsel via Bluetooth
Tillad Bluetooth-tethering	Giver mulighed for at bruge enheden som modem (Bluetooth-internetforbindelse)
Tillad forbindelse til computeren via Bluetooth	Tillad forbindelse til computer via Bluetooth

PIM-styring

Udveksling

Kun tilgængelig for Samsung KNOX 1.0 eller højere!

E-mail-adresse	Den angivne brugers e-mailadresse Bemærk "pladsholderne", som du kan bruge til at arbejde med legitimationsoplysninger, og du skal ikke udføre ændringer manuelt på alle enheder. Med et klik på **Show Placeholders** kan du vise dem for dig selv
Serverens værtsnavn	Serveradresse på dine Exchange-servere
Login-navn	Login-navnet for den respektive slutbrugerenhed, bemærk også "Placeholders here".
Domæne	Domæneadresse
Adgangskode (kun på enhedsniveau)	En individuel enhed kan eventuelt forsynes med en adgangskode, og hvis denne forbliver tom, vil brugeren blive bedt om at indtaste sin Exchange-adgangskode.
Antal foregående dage, der skal synkroniseres	Antal dage, der bestemmer, hvornår e-mails synkroniseres tilbage
Underskrift	En underskrift kan vedhæftes (tip: Nogle enheder kræver HTML-formatering af underskriften).
Standardkonto	Fastslår, at denne mailkonto er standardkontoen
Brug Secure Sockets Layer (SSL)	Brug en SSL-forbindelse
Brug Transport Layer Security (TLS)	Brug en TLS-forbindelse
Accepter alle certifikater	Alle certifikater accepteres. Vælg denne indstilling, hvis din Exchange Server bruger et selvsigneret certifikat.

E-mail

Her kan du distribuere IMAP- og POP-konti til de respektive slutbrugeres enheder.

Følgende indstillinger er kun tilgængelige på Samsung KNOX 1.0 eller højere!		
E-mail-adresse	Den angivne brugers e-mailadresse Bemærk "pladsholderne", som du kan bruge til at arbejde med legitimationsoplysninger, og du behøver ikke foretage ændringer manuelt på alle enheder. Med et klik på **Show Placeholders** kan du vise dem for dig selv	
Indgående serverprotokol	Indgående serverprotokol	IMAP eller POP
Adresse på indgående server	Adresse på indgående server	
Indgående serverport	Indgående serverport	
Login/brugernavn til indgående server	Login/brugernavn til indgående server	
Adgangskode til indgående server (kun på enhedsniveau)	Adgangskode til indgående server (kun på enhedsniveau)	
Indgående server bruger SSL	Indgående server bruger SSL	
Indgående server bruger TLS	Indgående server bruger TLS	
Indkommende server accepterer alle certifikater	Indgående server accepterer alle typer certifikater	
Udgående serverprotokol	Udgående serverprotokol	SMTP
Udgående serverport	Udgående serverport	
Udgående server bruger ekstra legitimationsoplysninger	Yderligere legitimationsoplysninger for den udgående server. Hvis den er sat til "off", bruges indstillingerne for den indgående server.	
Login/brugernavn til udgående server	Login/brugernavn til udgående server	
Adgangskode til udgående server (kun på enhedsniveau)	Adgangskode til udgående server	
Udgående server bruger SSL	Udgående server bruger SSL	
Udgående server bruger TLS	Udgående server bruger TLS	
Udgående server accepterer alle certifikater	Udgående server accepterer alle typer certifikater	

Underskrift	En underskrift kan vedhæftes her (Tip: Nogle enheder kræver HTML-formatering af underskriften).
Giv brugeren besked ved modtagelse af ny e-mail	Underretter brugeren om modtagelse af ny e-mail

AE Gmail-udveksling

Info: Denne konfiguration vil blive anvendt på Gmail-appen. Så du skal godkende og installere Gmail.

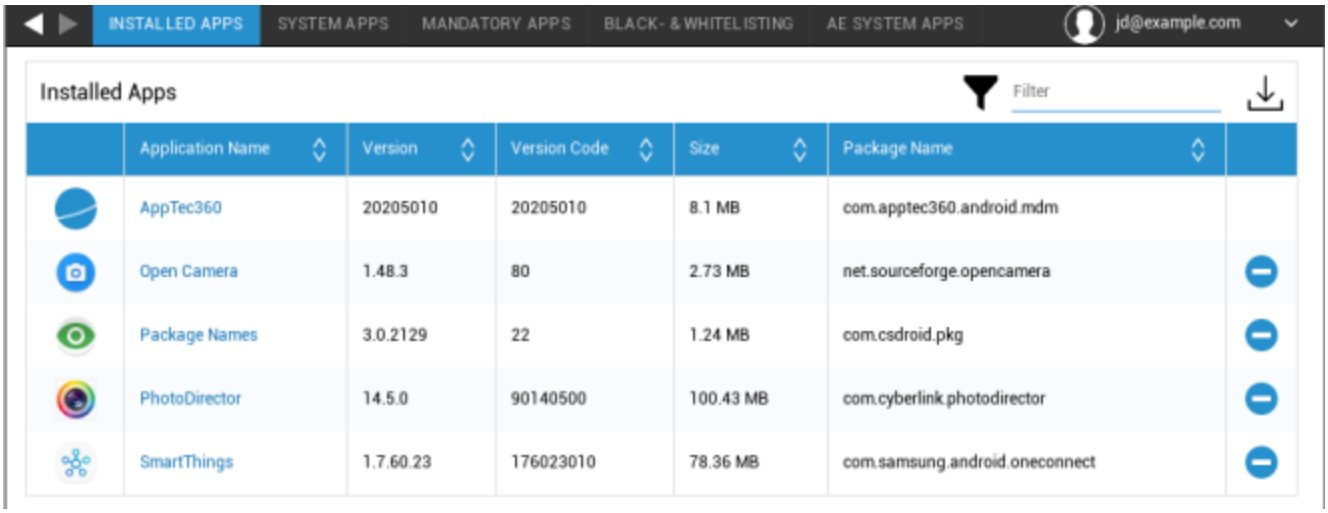
E-mail-adresse	Den angivne brugers e-mailadresse Bemærk "pladsholderne", som du kan bruge til at arbejde med legitimationsoplysninger, og du skal ikke udføre ændringer manuelt på alle enheder. Med et klik på Show Placeholders kan du vise dem for dig selv
Serverens værtsnavn	Serveradresse på dine Exchange-servere
Login-navn	Login-navnet for den respektive slutbrugerenhed, bemærk også "Placeholders here".
Underskrift	En underskrift kan vedhæftes (tip: Nogle enheder kræver HTML-formatering af underskriften).
Antal foregående dage, der skal synkroniseres	Antal dage, der bestemmer, hvornår e-mails synkroniseres tilbage
Enhedsidentifikator	EAS-identifikator. Lad den være tom, hvis dit miljø ikke kræver dette.
Brug Secure Sockets Layer (SSL)	Brug en SSL-forbindelse
Accepter alle certifikater	Alle certifikater accepteres. Vælg denne mulighed, hvis din Exchange Server bruger et selvsigneret certifikat.
Tillad ikke-administrerede konti	Giver brugeren mulighed for at tilføje yderligere konti
Klientcertifikat	Upload klientcertifikat, hvis din Exchange-server kræver dette

App-administration

Enterprise App Manager

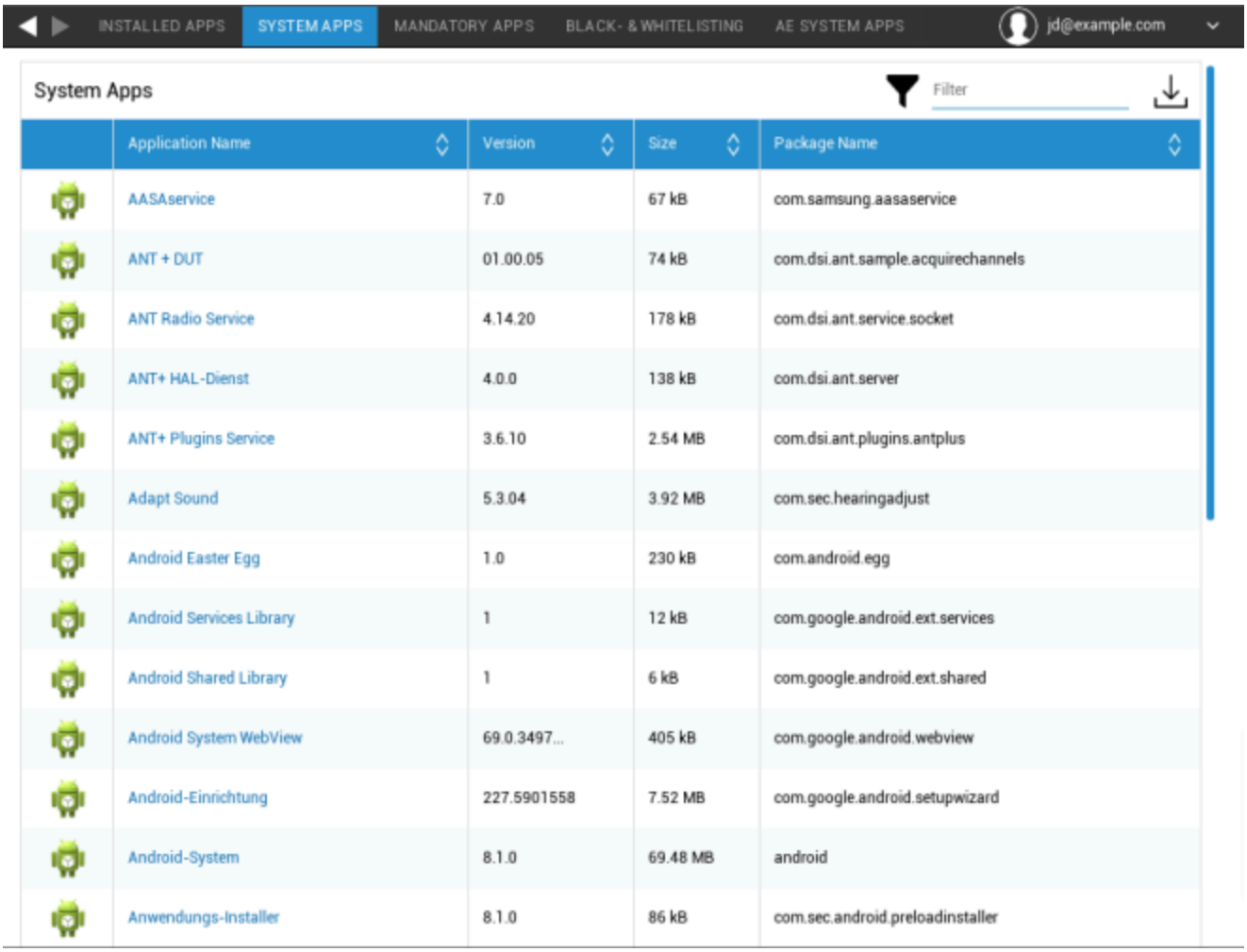
Installerede apps (kun på enhedsniveau)

Her vises alle de apps, der i øjeblikket er installeret på slutbrugerens enhed.


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

System-apps (kun på enhedsniveau)

Under "System Apps" vises alle de forudinstallerede systemer med deres pakkenavn og version.



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

Obligatoriske apps

I Obligatoriske apps kan du definere, hvilke apps der skal installeres på enheden. Afhængigt af din konfiguration og enhed vil appen blive installeret automatisk, eller brugeren vil blive bedt om at installere den.

Vær opmærksom på, at det anbefales at bruge Android Enterprise for at gøre det nemmere at administrere apps.

Scenarierne er som anført nedenfor:

Normale Play Store-apps

Playstore-appinstallationer kræver altid en brugerinteraktion. Derudover skal der konfigureres en Google-konto på enheden.

Installation af egen app

På Samsung-enheder vil disse apps blive installeret lydløst. Eneste undtagelse er containeren, hvor brugeren skal bekræfte installationen.

I alle andre scenarier skal brugeren bekræfte installationen af appen.

Android Enterprise Play Store Apps

Disse apps vil altid blive installeret lydløst uden brugerinteraktion.

For at tilføje en obligatorisk app skal du klikke på "+" og vælge den ønskede app fra listen. Vær opmærksom på, at du ikke kan installere apps fra fanen "Google Play Butik", hvis enheden er konfigureret med Android Enterprise enten som fuldt administreret eller som container.

Hvis du bruger Android Enterprise, skal du vælge apps fra afsnittet "AE Play Store". For at gøre apps tilgængelige her skal du bekræfte dem i Google Enterprise Play Store ved at gå til Generelle indstillinger → AE Play Store → Play Store Apps.

Når du fjerner en obligatorisk app, bliver den også afinstalleret fra enheden.

Du kan klikke på navnet på en app i listen over obligatoriske apps og gå til fanen "konfiguration" for at konfigurere en app. Dette kræver brug af Android Enterprise, og appen skal understøtte dette. Derfor afhænger de tilgængelige muligheder af den valgte app.

AE System Apps

Her kan du aktivere systemapps for Android Enterprise-enheder. Husk, at den angivne app skal være i systemets lager, ellers sker der ikke noget. 296

Begrænsninger og indstillinger

Sort- og hvidlistning

Her kan du definere en sort- eller hvidliste. Alle apps på sortlisten vil blive blokeret. Alle apps, som ikke er på hvidlisten, bliver blokeret. En tom sortliste blokerer intet, mens en tom hvidliste blokerer alt*.

**Alle obligatoriske apps og apps fra Enterprise App Store bliver automatisk hvidlistet. Du behøver ikke at tilføje dem manuelt.*

Når du klikker på "+", kan du enten søge efter en app, du vil føje til din sort- eller hvidliste, eller indtaste et pakkenavn manuelt.

Begrænsninger for systemapper

Under "Sys App Restrictions" kan du blandt andet blokere præinstallerede apps og tjenester, som du ønsker.

Slå browseren fra	Deaktiver standardbrowser
Deaktiver kalender	Deaktiver indbygget kalender
Deaktiver lommeregner	Deaktiver lommeregner
Deaktiver Chrome-browseren	Deaktiver Chrome-browseren
Deaktiver ur	Deaktiver uret
Deaktiver kontakter	Deaktiver kontakter
Slå dialer fra	Deaktiver indbygget dialer
Slå e-mail fra	Slå e-mail fra
Slå Exchange fra	Deaktiver Exchange-konti
Deaktiver Facebook	Deaktiver Facebook-appen
Deaktiver galleri	Deaktiver den oprindelige galleri-app
Deaktiver Gmail	Deaktiver Gmail
Deaktiver Google Bøger	Deaktiver Google Bøger
Deaktiver Google Play Kiosk	Deaktiver Google Play Kiosk
Deaktiver Google Maps	Deaktiver Google Maps
Deaktiver Google Music	Deaktiver Google Music
Deaktiver Google Film	Deaktiver Google Film
Deaktiver Google Play Butik	Deaktiver Google Play Store (offentlig App Store)
Deaktiver Google Plus	Deaktiver Google Plus
Deaktiver Google-søgning	Deaktiver Google-søgning
Deaktiver Google Talk / Google Hangouts	Deaktiver Google Talk / Google Hangouts
Deaktiver musikafspiller	Deaktiver indbygget musikafspiller-app
Deaktiver indstillinger	Deaktiver enhedens indstillinger
Deaktiver Sim Toolkit	Deaktiver Sim Toolkit-tjenester
Deaktiver SMS/MMS	Deaktiver SMS/MMS
Slå Street View fra	Slå Street View-tjenester fra
Slå Youtube fra	Slå Youtube fra

Samsung-apps

Under "Samsung Apps" kan du definere yderligere indstillinger og/eller begrænsninger for Samsung-enheder.

Deaktiver AllShare Play / Samsung Link	Deaktiver AllShare Play / Samsung Link
Slå ChatON fra	Slå ChatON fra
Deaktiver Game Hub	Deaktiver Game Hub
Slå gruppespil fra	Slå gruppespil fra
Deaktiver hjælp	Deaktiver Samsung-hjælp
Slå KNOX fra	Deaktiver Samsung KNOX Container
Slå memo fra	Slå stemmememo fra
Deaktiver mine filer	Deaktiver mine filer
Deaktiver optisk læser	Deaktiver optisk læser
Deaktiver Polaris Office	Deaktiver Polaris Office
Deaktiver Readers Hub / Samsung Books	Deaktiver Readers Hub / Samsung Books
Deaktiver S Memo	Deaktiver Samsung Memo-appen
Deaktiver S Translator	Deaktiver Samsung Translator-appen
Deaktiver S Voice	Deaktiver S Voice-assistent
Deaktiver Samsung-apps	Deaktiver Samsung App Store
Deaktiver Samsung Hub	Deaktiver Samsung Entertainment Stores
Deaktiver videoafspiller	Deaktiver videoafspiller
Deaktiver stemmeoptager	Deaktiver stemmeoptager
Slå WatchON fra	Deaktiver WatchON (simulerer en fjernbetjening)

Huawei Apps

Under "Huawei Apps" kan du definere yderligere indstillinger og/eller begrænsninger på Huawei-enheden.

Deaktiver DLNA	Deaktiver DLNA
Deaktiver app-installer	Deaktiver app-installer
Deaktiver filhåndtering	Deaktiver filhåndtering
Deaktiver Backup Manager	Deaktiver Backup Manager
Deaktiver systemopdatering	Deaktiver systemopdatering
Deaktiver værktøjskasse	Deaktiver værktøjskasse
Slå vejret fra	Slå vejret fra
Deaktiver FM-radio	Deaktiver FM-radio

Indstillinger for app-administration

Her kan du definere opdateringsadfærden for InHouse Apps.

Update Check Frequency definerer, hvor ofte AppTec360-appen leder efter opdateringer til InHouse-apps. Når en ny version er fundet, bliver den downloadet og installeret.

Wi-Fi Threshold definerer, om download skal begrænses til Wi-Fi-forbindelser, hvis appen er større end din konfigurerede Threshold. Hvis den er mindre, eller du ikke definerer en tærskel, vil appen blive downloadet via Wi-Fi og et mobilnetværk.

Enterprise App Store

Vær opmærksom på, at apps, der tilføjes her (Enterprise App Store), IKKE bliver installeret automatisk på enheden/enhederne. Brugeren skal åbne Enterprise App Store på enheden og installere appen manuelt.

Hvis du vil installere apps automatisk på enheden, skal du gå til "App Management" → "Enterprise App Manager" → "Mandatory Apps" og tilføje de ønskede apps der.

Under dette punkt kan du distribuere valgfrie apps til dine brugere.

Playstore

Klik på "+" for at tilføje en Play Store-app til butikken. Hvis du bruger Android Enterprise, skal du gå til "App Management Enterprise Play Store". Vær også opmærksom på, at der skal være konfigureret en Google-konto på → enheden for at installere de apps, der er defineret her.

Internt

Under punktet "In-House" kan du uploade og distribuere internt udviklede apps.

Klik på "+" for at tilføje en InHouse-app til virksomhedens app-butik, som derefter kan installeres af brugeren. I denne dialog kan du også uploade en ny InHouse-app.

Enterprise Play Store

Vær opmærksom på, at apps, der tilføjes her (Enterprise Play Store), IKKE bliver installeret automatisk på enheden/enhederne. Brugeren skal åbne Play Store på enheden og installere appen manuelt.

Hvis du vil installere apps automatisk på enheden, skal du gå til "App Management" → "Enterprise App Manager" → "Mandatory Apps" og tilføje de ønskede apps der.

Under dette punkt kan du distribuere valgfrie apps til dine brugere.

Her kan du tilføje apps til Android Enterprise Playstore. Bemærk, at du skal godkende apps i Generelle indstillinger → AE Play Store → Play Store-apps. Disse apps vil blive tilføjet til den normale Google Play Store.

Vær også opmærksom på, at du først skal definere et layout med apps i Generelle indstillinger → Appadministration → AE Play Store → Butikslayout.

Apps skal være i et layout, før du kan tilføje dem til butikken.

Kiosk-tilstand og launcher

Kiosk-tilstand

Kiosk-tilstanden giver dig mulighed for at forhåndsdefinere en app eller en URL. Derefter vil det udelukkende være muligt at køre/besøge denne app og/eller URL.

På samme måde kan forskellige hardwareknapper deaktiveres i Kiosk Mode diverse.

Automatisk start	Starter automatisk Kiosk Mode, så snart profilen når frem til slutbrugerens enhed
Planlagt kiosktilstand?	Du kan planlægge et tidspunkt for Kiosk Mode, som så starter og slutter automatisk på et tidspunkt, du har indstillet.
Starttidspunkt	Starttidspunkt
Tid i minutter	Tid i minutter, hvorefter Kiosk Mode skal afsluttes igen

Applikationstype

Enkelt app	Hvis du vil starte appen i kiosktilstand, skal du vælge "Pakke" under "Applikationstype".
Kiosk-applikation	Klik her for at vælge en app, der skal startes i Kiosk Mode Du finder den sædvanlige oversigt over App Management Du kan vælge mellem en "Google Play Store", "Android In-House Apps" og et "Packagename"

Applikationstype

URL	Hvis du vil starte en URL i kiosktilstand, skal du vælge "URL" under "Applikationstype". Definer derefter din ønskede URL-adresse
Ryd browseren efter inaktivitet	Her kan du definere et tidsinterval i minutter, hvorefter Kiosk Mode skal genstartes.
Ryd webcache og cookies	Hvis du aktiverer denne funktion, vil webcachen (cookies og cachelagrede billeder) blive slettet efter en genstart af Kiosk Mode.
Politik for samme oprindelse	Hvis denne funktion er aktiv, kan brugeren kun surfe på undersiderne i en defineret URL. Du har f.eks. defineret følgende URL:www.mypage.com Så kan brugeren surfe på: www.mypage.com/subpage
Hvidlistede webadresser	Her kan du vedligeholde en hvidliste, hvor alle disse URL'er er tilladt Maksimalt 1 URL pr. linje En URL skal starte med http:/ eller https://
Sortlistede webadresser	Her kan du vedligeholde en sortliste, hvor alle disse URL'er ikke er tilladt Maksimalt 1 URL pr. linje En URL skal starte med http:/ eller https://
Skærm-orientering	Denne indstilling vedrører skærmjusteringerne Automatisk = automatisk Portræt = lodret format Landscape = landskabstilstand

Multi-app	Hvis du vælger "Multi App"-kiosktilstand, vil brugen af AppTec360 Launcher blive gennemtvunget.
Apps	Applikation: Vælg en Playstore eller en intern app som kiosk-applikation. Det er også muligt at indtaste et pakkenavn. Den valgte kiosk-applikation skal være installeret på enheden. Husk at indstille Kiosk-applikationen som obligatorisk. Genvej på startskærmen: Hvis den er sat til "On", oprettes der en genvej på startskærmen. Hvis den er indstillet til "Fra", vises appen stadig på applisten.

Afslut adgangskode aktiveret	Hvis du aktiverer denne funktion, er det muligt for brugeren at afslutte kiosktilstanden med en adgangskode, som du har defineret på forhånd.
Afslut adgangskode	Dette er den adgangskode, som du har defineret på forhånd.
Skjul statuslinjen automatisk	Hvis den er aktiveret, bliver statuslinjen automatisk udtonet. Med denne indstilling kan brugerne se oplysningerne på statuslinjen, men ikke få adgang til dens funktioner.
Deaktiver statuslinje	Statuslinjen indeholder notifikationer, genveje og information. Kun tilgængelig for Samsung-enheder med KNOX 1.0 eller nyere.
Deaktiver lydstyrketaster	Deaktiver lydstyrketaster (kun tilgængelig på Samsung-enheder med KNOX 1.0 eller højere)
Deaktiver tænd/sluk-kontakt	Deaktiver tænd/sluk-kontakt (kun tilgængelig på Samsung-enheder med KNOX 1.0 eller højere)
Deaktiver Home-knap	Deaktiver Hjem-knap. Hvis denne funktion er blevet aktiveret, kan kiosktilstanden kun afsluttes i AppTec360-konsollen. (kun tilgængelig på Samsung-enheder med KNOX 1.0 eller højere)
Slå navigationslinjen fra	Med denne funktion kan du deaktivere navigationslinjen (Tilbage/Menu). Hvis denne funktion er aktiveret, kan kiosktilstanden kun afsluttes i AppTec360-konsollen. (kun tilgængelig på Samsung-enheder med KNOX 1.0 eller højere)

Indstillinger for app-opdatering	
Tillad app-opdateringer	Brugerne vil blive bedt om at udføre app-opdateringer, selv når Kiosk Mode er aktiv. På enheder med Samsung KNOX vil apps blive opdateret lydløst.
Opdateringsvindue	Indstil et interval, hvor brugerne bliver bedt om at installere app-opdateringer.

TeamViewer	
Aktivér uovervåget adgang	Hvis det er aktiveret, kan administratorer fjernstyre enheden uden brugerinteraktion. Appen TeamViewer Host skal være installeret på enheden.

AppTec360 Launcher

Aktivér AppTec360 Launcher	Tændt: Aktiverer AppTec360 Launcher. Brugeren skal indstille den som standardstarter én gang. Bemærk: Hvis Kiosk Mode er aktiveret, og Kiosk Mode er indstillet til "Multi App", vil brugen af AppTec360 launcher blive gennemtvunget.
Store ikoner	Til: Viser en større version af app-ikonerne i launcheren
Skjul AppTec360-appikonet	På: Skjuler AppTec360-appen fuldstændigt
Skjul AppTec360 Store-ikonet	På: Skjuler AppTec360 Enterprise AppStore helt.

AppTec360-indstillinger

Aktivér AppTec360-indstillingsappen	AppTec360-indstillingsappen giver kontrol over WiFi- og Bluetooth-forbindelser
Aktivér indstillinger i Multi App Kiosk-tilstand	Hvis det er aktiveret, kan brugerne få adgang til AppTec360 Settings-appen, mens Multi App Kiosk Mode er aktiv.

Fjernbetjening

Splashtop

Viser den aktuelle status for Splashtop-opsætningen. Her kan du se de trin, du skal udføre for at få fjernadgang til enheden via Splashtop. Her skal du også indtaste din implementeringskode, som du kan få fra Splashtops hjemmeside. Implementeringskoden er nødvendig for at oprette forbindelse til enheden.

Teamviewer

Viser den aktuelle status for Teamviewer-opsætningen. Her kan du se de trin, du skal udføre for at få fjernadgang til enheden via Teamviewer.

Styring af indhold

Indholdsboks

Her kan du aktivere Contentbox for denne enhed. Når den er aktiveret, vil Contentbox-appen blive installeret på enheden.

Sikker browser

Her kan du aktivere Secure Browser for denne enhed. Når den er aktiveret, vil Secure Browser-appen blive installeret på enheden. Denne browser kan konfigureres til at tilbyde en webbrowser på enheden, som er begrænset til dine behov.

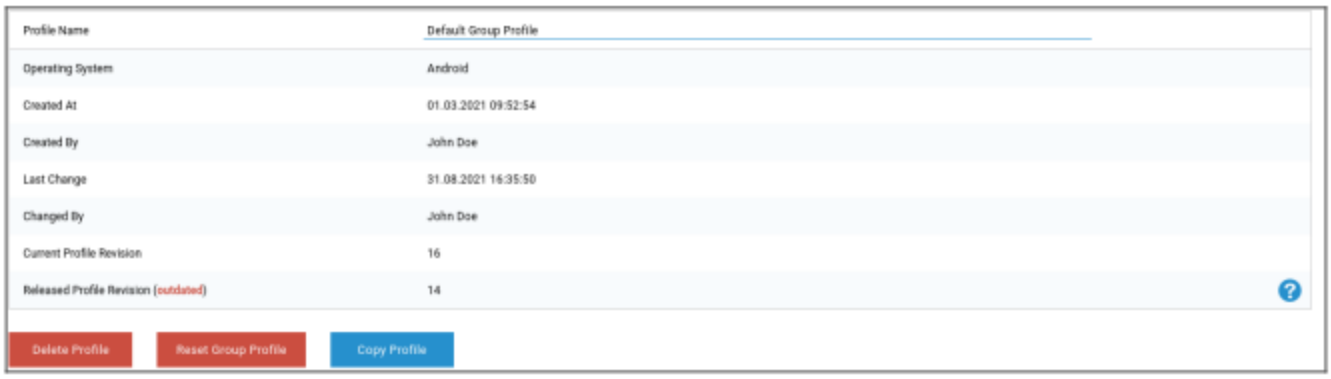
Kræver adgangskode	Kræv, at brugeren opretter og bruger en adgangskode for at få adgang til browseren.
Begræns downloads / åbn i	Blokerer downloads fra hjemmesider
Begræns uploads	Begrænser uploads til bestemte URL'er. Angiv ingen URL for at blokere uploaden helt
Tillad kopiering	Tillad at kopiere, klippe eller dele tekst inde på websiderne.
Tillad skærmoptagelse	Tillad optagelse af skærmbilleder.
Hyppighed af dataoprydning	Vælg, hvor ofte ALLE brugerdata (historik, cache osv.) skal fjernes automatisk.
Bogmærker til virksomheder	Bogmærkerne vil dukke op i mappen "Company bookmarks" i browserens bogmærker. De kan ikke redigeres af brugeren.
Skjul adresselinjen	Skjuler adresselinjen, så brugeren ikke kan se den URL, han besøger
Whitelisting i browseren (uden Universal Gateway)	Aktiverer hvidlistning af URL'er på klientsiden. - Virksomhedens bogmærker er altid whitelistet - Understøttes kun for 100 URL'er - Brug Universal Gateway til ubegrænset sort- og whitelisting
Gateway-baseret black- og whitelisting	Blacklisting har følgende krav: - En fungerende AppTec360 Universal Gateway ("Generelle indstillinger" → "Universal Gateway") - En fungerende VPN-konfiguration med en specificeret DNS-server ("Generelle indstillinger" → "Universal Gateway" → "VPN-indstillinger") - En blacklist-konfiguration ("Generelle indstillinger" → "Universal Gateway" → "Domain Blacklist") - En gyldig VPN-forbindelse i profilen ("Connection Management" → "VPN")

Konfiguration af Windows 10-pc

Generelt

Oversigt over gruppeprofiler (kun på gruppeniveau)

Når du åbner en gruppeprofil, får du et hurtigt overblik over profilen.



Navn på profil	Navn på profilen (kan ændres her)
Operativsystem	Operativsystem, som profilen er til
Oprettet på	Tidspunkt for skabelse
Oprettet af	Profilens skaber
Sidste ændring	Tidspunkt for sidste ændring af profilen
Ændret af	Konto, der foretog de sidste ændringer
Nuværende profilrevision	Revision af gemt profiltilstand
Udgivet profilrevision	Tildelt profilrevision ("Tildel nu"). Hvis etiketten viser "(forældet)" bag teksten, betyder det, at du har gemt profilen, men ikke tildelt den endnu, så enhederne vil stadig få en ældre version.

Enhedsoversigt (kun på enhedsniveau)

Enhedens sammenfattede oversigt, som indeholder følgende:

PC-navn	Navn på pc'en
Kunde	Enhedernes Windows-type
Sidste kendte placering	Breddegrad og længdegrad for enhedens sidst kendte placering
Tildelte obligatoriske apps	Antal obligatoriske apps, der er tildelt enheden
PC UID	UID for pc'en
OS-udgave	Viser din Windows-udgave
OS-version	Aktuelt installeret Windows-version
OS-bygning	Nuværende Windows-bygning
Operativsystem	Aktuelt installeret operativsystem
Serienummer	Enhedens serienummer
Ejerskab af enhed	Den konfigurerede ejerskabstype
Enhedstype	Enhedens type
Rodfæstet	Viser, om enheden er rodfæstet
Overensstemmende	Viser, om enheden er kompatibel
Sidst set	Dato og klokkeslæt, hvor der blev foretaget ændringer på profilen
Brugertildeling	Viser den bruger eller gruppe, som denne enhed i øjeblikket er tildelt. Du kan flytte enheden ved at vælge en anden bruger eller gruppe fra rullelisten.

Indstillinger

Tillad automatisk opdatering	Tillad eller afvis automatiske systemopdateringer.

Config Revision (kun på enhedsniveau)

Her får du en oversigt over, hvilken gruppeprofil der er tildelt enheden.

Hvis du klikker på gruppeprofilen, får du direkte adgang til profilen, og du kan foretage indstillinger.

Med symbolet kan du gendanne de tildelte apps til gruppeprofilens indstillinger.

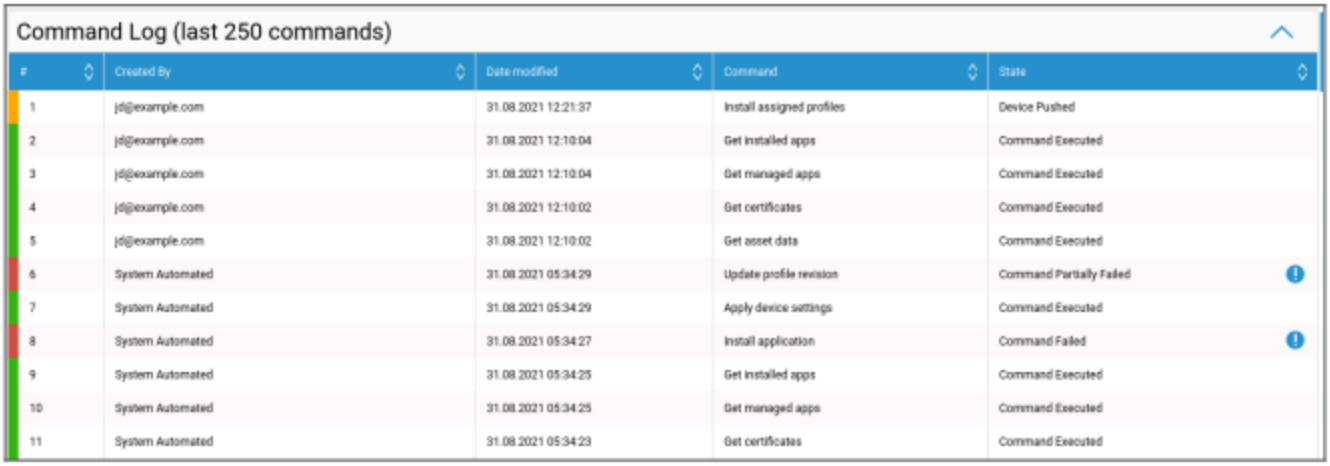
Med symbolet kan du nulstille enhedens profil, så den slet ikke har nogen indstillinger.

"Nyere revision tilgængelig" angiver, at gruppeprofilen er blevet ændret og gemt, men ikke tildelt. Gruppeprofilen skal tildeles med "Tildel nu" på gruppeniveau for at anvende ændringerne på enhederne.

Enhedslog (kun på enhedsniveau)

Kommando-log

Her kan du se, hvilke kommandoer der er udstedt til enheden, og hvad deres status er.



Kommandoer, der er oprettet af "System Automated", oprettes automatisk af systemet.

Mulige kommandostatusser

Enhed skubbet	Der er sendt en push-anmodning til push-tjenesten (f.eks. APNS) for at fortælle enheden, at den skal oprette forbindelse tilbage til EMM-serveren.
Kommando oprettet	Kommandoen blev oprettet i systemet.
Kommando sendt	Kommandoen blev sendt til enheden, efter at den havde oprettet forbindelse til serveren.
Kommando udført	Kommandoen blev udført med succes.
Kommando mislykkedes	Kommandoen mislykkedes. *
Kommando delvist mislykket	Afhængigt af enhedens operativsystem kan nogle kommandoer blive grupperet sammen. Nogle dele af denne kommandogruppe mislykkedes. *
Kommandoen blev udført, men mislykkedes til sidst	Kommandoen blev udført, men måske blev den ikke.
Kommando genindført	Kommandoen blev repushed af en bruger.
Kasseret	Kommandoen blev kasseret. For eksempel fordi den blev erstattet af en anden kommando, eller fordi enheden blev genindskrevet, og gamle kommandoer blev fjernet.

*Hvis der er et udråbstegn bag beskeden, kan du få flere oplysninger ved at holde markøren over ikonet.

Asset Management (kun på enhedsniveau)

Enhedsinfo

Producent	Producent af enheden
Model	Enhedsmodel
Modelnummer	Modelnummer
Operativsystem	Operativsystem
OS-version	OS-version
Serienummer	Serienummer
ExchangeID	ExchangeID
Samlet RAM	Samlet RAM
Skærmopløsning	Skærmopløsning
Sprog i telefonen	Enhedens sprog
Firmware-version	Firmware-version
DM-klientversion	Version af Device Management Client
Hardware-version	Enhedens hardwareversion
CPU-arkitektur	CPU-arkitektur (processortype)

Cellulær

SIM-bærerens netværk	Bærende netværk
Telefonnummer	Telefonnummer
Roaming-status	Roaming-status
IMEI	IMEI
IMSI	IMSI
Modem-firmware	Modem-firmware

Info om synkronisering

Øjeblikkelig DM-forbindelse	Enheden bør straks oprette en forbindelse til AppTec
Første forsøgstid	Første forsøgstid for denne første forbindelse
Forbindelsesforsøg	Antal nye forbindelsesforsøg efter en afbrydelse af forbindelsen fra Connection Manager eller en fejl på WinInet-niveau
Maksimal søvntid	Maksimal hviletid efter fejl i pakkesending
Første synkroniseringsforsøg	Tid til den første fase efter indskrivningen
Første forsøgsinterval	Tid til den første fase efter indskrivningen
Andet synkroniseringsforsøg	Tid til anden fase efter indskrivningen
Andet gentagelsesinterval	Tid til anden fase efter indskrivningen
Regelmæssige synkroniseringsforsøg	Tid til de yderligere faser efter indskrivningen
Regelmæssigt gentagelsesinterval	Tid til de yderligere faser efter indskrivningen

Sikkerhedsstyring

Tyverisikring (kun på enhedsniveau)

GPS-information (kun på enhedsniveau)

Her kan du fastlægge enhedens aktuelle/sidste placering. Lokaliseringen kan beskyttes med en eller endda to adgangskoder - se: "Generelle indstillinger" > "Privatliv" > "GPS-adgang"

GPS-indstillinger

Aktivér GPS-sporing	Aktivér regelmæssig synkronisering af GPS-information.
Sporingsinterval	Indstil intervallet for synkronisering af GPS-information.

Sikkerhedskonfiguration

Adgangskode

Minimum længde på adgangskode	Minimumslængde for adgangskode	
Sammensætning af kodeord	Angiver antallet af specifikke tegn, som adgangskoden skal indeholde De består af store og små bogstaver, tal og specialsymboler.	
Adgangskodekvalitet	Her kan du indstille adgangskodekvaliteten	
	Alfanumerisk	Kun tal og bogstaver
	Numerisk	Kun tal
	Numerisk eller alfanumerisk	Tal eller tal og bogstaver
Maksimal inaktivitetstid Lås	Antal minutter, hvor brugeren ikke har været aktiv på enheden, hvorefter enheden låses. Brugeren skal låse enheden op efter dette tidsrum ved at indtaste enhedens adgangskode.	
Udløb af adgangskode	Indstil tiden, indtil en ny adgangskode skal indstilles	
Begrænsning af adgangskodehistorik	Antal tidligere anvendte adgangskoder, der ikke er tilladt	
Maksimalt antal mislykkede adgangskodeforsøg	Antal gange, adgangskoden kan indtastes forkert, før en komplet sletning af enheden udføres	

Antivirus

Antivirusindstillinger - Indstil scanningskonfiguration	
Type af scanning	Vælger, om der skal udføres en hurtig scanning eller en fuld scanning
Indstil scanningsstart	Vælger det tidspunkt på dagen, hvor Windows Defender skal starte scanningen
Scanningsfrekvens	Vælger den dag, hvor Windows Defender-scanningen skal køre
Opdateringsfrekvens for signaturer	Angiver det interval i timer, der skal bruges til at tjekke for underskrifter

Konfigurer type af filer til scanning	
Tillad scanning af arkivfiler	Tillad eller afvis scanning af arkiver (f.eks. .zip), når de åbnes.
Tillad scanning af scripts	Tillader eller afviser Windows Defender Script Scanning-funktionalitet.
Tillad scanning af e-mails	Tillad eller afvis scanning af e-mails.
Tillad scanning af netværksfiler	Tillad eller afvis scanning af netværksfiler.
Tillad fuld scanning af mappede netværksdrev	Tillad eller afvis scanning af kortlagte netværksdrev (kun aktiveret, når fuld scanning er aktiveret).
Kontroller tovejs scanning	Styrer, hvilke sæt filer der skal overvåges.
Tillad fuld scanning af flytbare drev	Tillad eller afvis fuld scanning af flytbare drev. Kun når fuld scanning er påbegyndt.

Type af filer, der skal udelukkes fra scanning	
Ignorer filtyper til scanning	Definer et sæt filtypenavne. Hver filtype for hvert felt.
Ignorer mappestier	Definer et sæt katalogstier for ikke at scanne dem. En sti pr. felt. Eksempler: "C:\Example", "C:\Windows" eller "C:\Users".
Udeluk processer fra scanning	Udeluk filer, der er blevet åbnet af specifikke processer, fra Microsoft Defender Antivirus-scanninger. . En sti pr. felt. Eksempler på dette: "C:\myFile.exe", "C:\Windows\myProcess.exe", "C:\myScript.bat".

Ekstra indstillinger	
Tillad overvågning i realtid	Tillad eller afvis Windows Defender Realtime Monitoring-funktionalitet
Tillad overvågning af adfærd	Tillad eller afvis Windows Behavior Monitoring-funktionalitet
Tillad beskyttelse af skyen	Tillad eller afvis, at Windows Defender sender oplysninger til Microsoft om ethvert problem, den finder. Microsoft vil analysere disse oplysninger, lære mere om det problem, der påvirker enheden, og tilbyde forbedrede løsninger.
	Adfærd ved afsendelse af prøver
Tillad Windows Defender IOAV-beskyttelse	Tillad eller afvis Windows Defender IOAV-beskyttelse
Giv adgang til Defenders "On Access protection" UI	
Gennemsnitlig CPU-belastningsfaktor	Repræsenterer den gennemsnitlige CPU-belastningsfaktor for Windows Defender-scanningen (i procent).

Håndtering af malware	
Lav sværhedsgrad	Du kan definere for hvert alvorlighedsniveau, hvordan enheden skal håndtere malware. Tilgængelige muligheder er: • Ren • Karantæne • Fjerne • Tillad det • Brugerdefineret • Blok
Moderat sværhedsgrad	
Høj sværhedsgrad	
Alvorlig sværhedsgrad	
Dage til at bevare renset malware	Tidsperiode i dage, hvor karantænefiler/emner gemmes på systemet. Standardværdien er 0, som holder elementer i karantæne og ikke automatisk fjerner dem. Den maksimale værdi er 90.

Sikkerhedscenter

Windows Sikkerhedscenter - Indstillinger for Windows-sikkerhed	
Deaktiver UI til beskyttelse mod virus og trusler	
Hide Ransomware Data Recovery UI	
Deaktiver brugergrænsefladen for kontobeskyttelse	
Deaktiver firewall og netværksbeskyttelse UI	
Deaktiver brugergrænsefladen for app- og browserkontrol	
Forbyd ændringer i Exploit-beskyttelse	Forbyd brugeren at foretage ændringer i indstillingerne for Exploit-beskyttelse
Deaktiver enhedens sikkerhedsgrænseflade	
Skjul TPM-fejlfinding	Skjul indstillinger for TPM-fejlfinding
Deaktiver knappen Ryd TPM	
Deaktiver enhedens ydeevne og sundhed UI	
Deaktiver familieindstillinger UI	

Tilpas dine toasts	
Aktivér tilpasset supportinformation	Gør det muligt at vise tilpassede supportkontaktoplysninger for din virksomhed nederst til højre i sikkerhedscenter-appen.
E-mail-adresse	Indstil virksomhedens e-mailadresse
Virksomhedens navn	Indstil virksomhedens navn
Firmaets telefon	Indstil virksomhedens telefon
Hjælp til URL	Indstil virksomhedens hjælpe-URL

Ekstra indstillinger	
Slå notifikationer fra	Deaktiver visning af meddelelser fra Windows Defender Security Center.
Anbefalinger til opdatering af TPM-firmware	Skjul anbefalingen om at opdatere TPM-firmware, når der opdages en sårbar firmware.
Vis firmanavn og kontaktmuligheder	Vis dit firmanavn og dine kontaktmuligheder i et kontaktkort, der flyver ud i Windows Defender Security Center.
Skjul Secure Boot	Skjul området Security Boot.
Skjul kontrol af sikkerhedsmeddelelsesområde	Skjul kontrol af Windows Security-meddelelsesområde.

Konfiguration af firewall

Konfiguration af firewall - Globale indstillinger	
Ignorer indstillet autentificering	Ignorer hele godkendelsessættet, hvis de ikke understøtter alle de godkendelsessuiter, der er angivet i sættet
Type af pakkekø	Angiver, hvordan skalering af softwaren på modtagersiden aktiveres for både den krypterede modtagelse og clear the forward path for IPsec-tunnelgatewayscenariet.
Deaktiver udfør stateful FTP-filtrering	Hvis den er deaktiveret, vil den ikke udføre stateful File Transfer Protocol (FTP)-filtrering for at tillade sekundære forbindelser.
Inaktivitetstid for sikkerhedsassociation	Dette felt konfigurerer sikkerhedstilknytningens inaktivitetstid i sekunder. Sikkerhedstilknytninger slettes, når der ikke er set netværkstrafik i den angivne tidsperiode.
Kodning af forhåndsdelt nøgle	Indstil den forhåndsdelte nøglekodning
Undtagelser fra IPSec	Konfigurer undtagelser fra internetprotokollen
Kontrol af liste over tilbagekaldte certifikater	

Firewall-profiler (domæneprofil / privat profil / offentlig profil)	
Aktivér firewall for denne profil	
Slå notifikationer fra	Deaktiver visning af besked til brugeren, når et program er blokeret fra at lytte på en port.
Bloker unicast-svar på multicast-udsendelser	
Håndhæv autoriserede firewall-regler for applikationer	Hvis den ikke håndhæves, ignoreres autoriserede applikationsfirewallregler i det lokale lager og håndhæves ikke.
Gennemfør globale regler for port-firewall	Hvis den ikke håndhæves, ignoreres globale portfirewallregler i det lokale lager og håndhæves ikke. Indstillingen har kun betydning, hvis den er indstillet eller opregnet i gruppepolitiklageret, eller hvis den er opregnet fra GroupPolicyRSoPStore.
Håndhæv firewall-regler	Hvis den ikke håndhæves, ignoreres firewall-regler fra det lokale lager og håndhæves ikke.
Håndhæv regler for forbindelsessikkerhed	Hvis den ikke håndhæves, ignoreres og håndhæves reglerne for forbindelsessikkerhed fra den lokale butik ikke.
Standard udgående handling	Den handling, som firewallen som standard udfører på udgående forbindelser
Standard indgående handling	Den handling, som firewallen som standard udfører på indgående forbindelser
Deaktiver Stealth-tilstand	Stealth mode er en mekanisme i Windows Firewall, der hjælper med at forhindre ondsindede brugere i at finde oplysninger om netværkscomputere og de tjenester, de kører.
Deaktiver forhindring af at svare på uopfordret trafik	Hvis den er deaktiveret, må firewallens regler for skjult tilstand ikke forhindre værtscomputeren i at svare på uopfordret netværkstrafik, hvis denne trafik er sikret med IPsec.

Firewall-regler

Firewall-regler	
Navn	Navn på reglen
Beskrivelse	Beskrivelse af reglen
Handling	Angiv, om denne regel vil blokere trafikken eller tillade den. Vær opmærksom på, at indstillingen Bloker også kan blokere trafikken (afhængigt af resten af konfigurationen) mellem MDM-serveren og enheden.
Retning	
Aktivér Edge Traversal (kun tilgængelig, når **Retning** er **indstillet til indgående trafik**)	Angiver, at specifik indgående trafik er tilladt at tunnelere gennem NAT'er og andre edge-enheder ved hjælp af Teredo-tunneleringsteknologien.

Programmer og tjenester	
Definer applikationer, alt andet	Hvis den ikke er aktiveret, vil den overveje alle ansøgninger
Pakkens familienavn	Navnet på den pakkefamilie, som reglen skal gælde for.
Filsti til applikationen	Det fulde program, såsom C:\Windows\System\Notepad.exe, som reglen vil gælde for
Fuldt kvalificeret binært navn	Det fuldt kvalificerede binære navn, som reglen skal gælde for. Et FQBN er en streng i følgende form: {Udgiver\Produkt\Filnavn,Version}.
Navn på tjeneste	Indtast navnet på en tjeneste (f.eks. "EventLog"). Du kan få en liste over servicenavne i Powershell ved at køre kommandoen "Get-Service".

Protokoller og porte				
Protokol	Den protokol, der bruges af reglen.			
	Tilgængelige værdier: - Enhver - Brugerdefineret - HOPORT - ICMPv4 - IGMP - TCP - UDP - IPv6 - IPv6-rute - IPv6-Frag - GRE - ICMPv6 - IPv6-NoNxt - IPv6-Opts - VRRP - PGM - L2TP	Når den er indstillet til Brugerdefineret	Indsæt et protokolnummer mellem 0 og 255	Protokollens nummer
		Når den er indstillet til TCP eller UDP	Angiv lokale porte, ellers vil alle blive brugt	Lokale porte, som reglen vil bruge, områdeporte er også tilladt
			Lokal havn	En enkelt port eller en række porte. F.eks. 100-120,200,300-320.
			Angiv fjernporte, ellers vil alle blive brugt	Fjernporte, som reglen vil bruge, intervalporte er også tilladt
			Ekstern port	En enkelt port eller en række porte. F.eks. 100-120,200,300-320.

Omfang	
Angiv lokale IP'er, ellers enhver IP	Sæt af lokale IP'er, det kan også være en række IP'er adskilt af -.
Lokal IP-adresse	Sæt af enkelte IP'er eller en række IP'er adskilt af -.
Angiv fjern-IP'er, ellers enhver fjern-IP	Angiv et sæt fjern-IP'er, det kan også være en række IP'er adskilt af "-".
Ekstern IP-adresse	Angiv enkelte IP'er eller en række IP'er
Mønter	Tokens, der kan indstilles sammen med fjernadresser. Tokens Intranet, RmtIntranet og Ply2Renders understøttes i Windows 10, version 1809 og senere.

Avancerede indstillinger	
Angiv profiler, ellers vil alle blive brugt	Hvis deaktiveret, vil alle profiler blive brugt
Domæne	Domæneprofil

Privat	Privat profil
Offentlig	Offentlig profil
Angiv grænseflader, ellers vil alle blive brugt	Hvis deaktiveret, vil alle grænseflader blive brugt
Lokalt netværk	Grænseflade til lokalt netværk
Fjernadgang	Interface til fjernadgang
Trådløs	Trådløs grænseflade

Lokale rektorer	
Tilføj autoriserede lokale brugere	Tillad at tilføje en liste over lokale brugere, der skal bruge denne regel
Autoriserede brugere	Liste over autoriserede lokale brugere til denne regel. Brugeren skal være i SDDL-format (Security Description Definition Language), f.eks. pc_NAME\USERNAME. Dette felt skal ikke udfyldes, hvis et tjenestenavn er indstillet til at bruge denne regel.

Begrænsningsindstillinger

Enhedens funktionalitet

Tillad SD-kort	Tillad brug af et SD-kort
Tillad kamera	Tillad brug af kameraet
Tillad placeringstjeneste	Tillad enhedens placeringstjeneste
Tillad Sideloading af app	Tillad installation af apps fra ukendte kilder
Tillad udviklertilstand	Tillader udviklertilstand
Tillad roaming af mobildata	Tillad roaming af mobildata
Tillad Cortana	Tillad stemmeassistent Cortana
Tillad søgning at bruge placering	Lad søgning bruge placering
Tillad tilføjelse af ikke-Microsoft e-mail-konto	Angiv, om brugeren har lov til at tilføje e-mailkonti, der ikke er MSA.
Tillad forbindelse til Microsoft-konto	Angiv, om du vil tillade brug af MSA-konto til ikke-emailrelateret forbindelsesgodkendelse og -tjenester.
Tillad synkronisering af mine indstillinger	Giver mulighed for at synkronisere indstillinger på tværs af hele enheden
Virksomhedsbeskyttede domænenavne	Angiver virksomhedens domænenavne adskilt af ";".
Tillad brugeren at deaktivere systemgendannelse	Giver brugeren mulighed for at deaktivere Systemgendannelse. **ADVARSEL!** Denne funktion bør kun bruges på enheder, der ejes eller stilles til rådighed af virksomheden eller organisationen, eller på en brugerejet enhed, hvor brugeren tillader, at enheden administreres fuldt ud af virksomheden. Hvis du deaktiverer denne politikindstilling, slås Systemgendannelse fra, og der er ikke adgang til guiden Systemgendannelse. Muligheden for at konfigurere Systemgendannelse eller oprette et gendannelsespunkt via Systembeskyttelse er også deaktiveret.
Tillad afmelding af brugere	Giver brugeren mulighed for at fjerne virksomhedsdelen fra enheden og dermed afbryde forbindelsen til AppTec360-serverne. Hvis dette sker, vil det ikke længere være muligt at administrere enheden. **ADVARSEL!**

	Denne funktion bør kun bruges på enheder, der ejes eller stilles til rådighed af virksomheden eller organisationen, eller på en brugerejet enhed, hvor brugeren tillader, at enheden administreres fuldt ud af virksomheden. Hvis du deaktiverer denne politikindstilling, vil brugerne ikke kunne fjerne MDM-tilmeldinger. Angiv, om brugeren har lov til at slette arbejdspladskontoen via arbejdspladsens kontrolpanel. MDM-serveren kan altid fjernslette kontoen.

BitLocker

BitLocker-konfiguration

Generelle indstillinger	
Kræv kryptering af enheder	Spørg brugerne, om de vil aktivere enhedskryptering Afhængigt af Windows-udgaven og systemkonfigurationen kan brugerne blive spurgt: - For at bekræfte, at kryptering fra en anden udbyder ikke er aktiveret. - For at slå BitLocker Drive Encryption fra og derefter slå BitLocker til igen.
Krypteringsmetoder	
Krypteringsmetode til operativsystemdrev	
Krypteringsmetode til faste datadrev	
Krypteringsmetode til flytbare datadrev	
Slå advarsel om tredjeparts diskkryptering fra	Deaktiver advarslen om en tredjeparts diskkrypteringstjeneste, der bruges på enheden. Fra og med Windows 10, version 1803, understøttes denne indstilling kun for Azure Active Directory-tilsluttede enheder.
Tillad at køre kryptering, mens en ikke-administratorbruger er logget ind	Understøttes kun for Azure Active Directory-tilsluttede enheder

AppTec360-udvidelser	
Lydløs kryptering	Hvis det vælges sammen med "Kræv enhedskryptering", vil AppTec360 Management Service køre automatisk lydløs kryptering af enhedens drev.
Generer automatisk brugeroplysninger	Det krypterede OS-drev bliver beskyttet med automatisk genererede brugeroplysninger. Enten en TPM-pinkode, når en TPM er tilgængelig, eller en 6-cifret tekstadgangskode. De genererede legitimationsoplysninger sendes til den e-mailadresse, der er registreret for den givne enhed. Hvis denne indstilling er slået fra, er den eneste mulige beskyttelse af lydløs kryptering at bruge TPM. I så fald vil lydløs kryptering mislykkes for enheder uden TPM.
Krypter faste drev	Alle tilgængelige faste datadrev bliver også krypteret og beskyttet med "automatisk oplåsning" ved hjælp af en nøgle, der er gemt på OS-drevet.

Indstillinger for OS-drev

Kræv yderligere godkendelse ved opstart	Denne indstilling giver dig mulighed for at konfigurere, om BitLocker kræver en godkendelse, hver gang computeren starter. Denne indstilling anvendes under opsætningen af BitLocker. Hvis du aktiverer denne indstilling, kan brugerne konfigurere avancerede opstartsindstillinger i BitLocker-opsætningsguiden.
Bloker BitLocker uden en kompatibel TPM	
Kun TPM	
TPM og PIN-kode	
TPM og nøgle	
TPM, nøgle og PIN-kode	Hvis du vil kræve brug af en pinkode og et USB-flashdrev (nøgle), skal brugeren konfigurere BitLocker ved hjælp af kommandolinjeværktøjet "manage-bde" i stedet for installationsguiden til BitLocker Drive Encryption.

Kræver minimum PIN-længde	
	Minimum tegn

Konfigurer pre-boot recovery-meddelelse og URL	Konfigurer hele gendannelsesmeddelelsen, eller erstat den eksisterende URL, der vises på gendannelsesskærmen før startnøglen, når OS-drevet er låst. Bemærk: Ikke alle tegn og sprog understøttes i pre-boot. Det anbefales på det kraftigste, at du tester, at de tegn, du bruger, vises korrekt på pre-boot recovery-skærmen.
	Mulighed for besked før opstart af gendannelse
	Brugerdefineret genoprettelsesmeddelelse
	Brugerdefineret URL til gendannelse

Muligheder for gendannelse af OS-drev		Denne indstilling giver dig mulighed for at styre, hvordan BitLocker-beskyttede operativsystemdrev gendannes, hvis du ikke har de nødvendige legitimationsoplysninger. Denne indstilling anvendes under opsætningen af BitLocker. Som standard er en certifikatbaseret datagendannelsesagent tilladt, gendannelsesmulighederne kan specificeres af brugeren, herunder gendannelsesadgangskode og gendannelsesnøgle, og gendannelsesoplysningerne sikkerhedskopieres ikke til AD DS.
	Blokcertifikat-baseret datagendannelsesagent	Angiv, om en datagendannelsesagent kan bruges med BitLocker-beskyttede operativsystemdrev. Før en datagendannelsesagent kan bruges, skal den tilføjes fra Public Key Policies-elementet i enten Group Policy Management Console eller Local Group Policy Editor. Se BitLocker Drive Encryption Deployment Guide på Microsoft TechNet for at få flere oplysninger om tilføjelse af datagendannelsesagenter.
	Indstillinger for BitLocker-genoprettelsesadgangskode	
	Indstillinger for BitLocker-genoprettelsesnøgle	
	Gem oplysninger om BitLocker-gendannelse i Active Directory Domain Services	
	Konfiguration af AD DS BitLocker-gendannelseslager	Opbevaring af nøglepakken understøtter gendannelse af data fra et drev, der er blevet fysisk beskadiget.
	Kræv lagring af gendannelsesdata i AD DS	Forhindrer brugere i at aktivere BitLocker, medmindre computeren er forbundet til domænet og

Faste drevindstillinger	
Muligheder for gendannelse af faste drev	Denne indstilling giver dig mulighed for at styre, hvordan BitLocker-beskyttede faste drev gendannes, hvis du ikke har de nødvendige legitimationsoplysninger. Denne indstilling anvendes under opsætningen af BitLocker. Som standard er en certifikatbaseret datagendannelsesagent tilladt, gendannelsesmulighederne kan specificeres af brugeren, herunder gendannelsesadgangskode og gendannelsesnøgle, og gendannelsesoplysningerne sikkerhedskopieres ikke til AD DS.
Blokcertifikat-baseret datagendannelsesagent	
Indstillinger for BitLocker-genoprettelsesadgangskode	
Indstillinger for BitLocker-genoprettelsesnøgle	
Gem oplysninger om BitLocker-gendannelse i Active Directory Domain Services	
Konfiguration af AD DS BitLocker-gendannelseslager	Opbevaring af nøglepakken understøtter gendannelse af data fra et drev, der er blevet fysisk beskadiget.
Kræv lagring af gendannelsesdata i AD DS	Forhindr brugere i at aktivere BitLocker, medmindre computeren er forbundet til domænet, og sikkerhedskopieringen af BitLocker-gendannelsesoplysninger til AD DS lykkes. Bemærk: Adgangskoden til gendannelse genereres automatisk.
Nægt skriveadgang til ubeskyttede faste drev	

Indstillinger for flytbare drev	
Nægt skriveadgang til ubeskyttede flytbare drev	Nægt skriveadgang til flytbare datadrev, som ikke er beskyttet af Bitlocker. Bemærk: Hvis "Flytbare diske: Nægt skriveadgang" er aktiveret i gruppepolitikken, vil denne politikindstilling blive ignoreret.
Nægt skriveadgang til enheder, der er konfigureret i en anden organisation	Kun drev med identifikationsfelter, der matcher computerens identifikationsfelter, får skriveadgang. Disse felter er defineret af gruppepolitikindstillingen "Angiv de unikke identifikatorer for din organisation".

BitLocker-status

Her kan du se den aktuelle status for BitLocker-krypterede drev

C [OS Drive]
Krypteringsstatus
Krypteret (%)
Status for beskyttelse
Krypteringsmetode
Nøglebeskyttere
Adgangskode til gendannelse

Med et klik på knappen "Rotate recovery password" kan du rotere BitLocker-genoprettelsesadgangskoden.

Administration af certifikater

Liste over certifikater

Her er en liste over de certifikater, der er installeret på den enhed, der vises.

Konfiguration af certifikat

Her kan du konfigurere certifikater, og hvordan de skal installeres på enheden.

Betroet certifikat	
Beskrivelse	Beskrivelse af certifikat
Omfang	Anvendelsesområde for certifikater: Nuværende bruger vs. enhed
Lager for certifikater	"Untrusted Certificates" er kun tilgængelig fra og med Windows 10, version 1803
Certifikat-fil	Upload en PKCS#1-fil

Identitetscertifikat			
Beskrivelse	Beskrivelse af certifikat		
Omfang	Anvendelsesområde for certifikater: Nuværende bruger vs. enhed		
Vigtig placering	Den Key Storage Provider, som den private nøgle skal installeres på.		
		TPM. Fejl hvis ingen TPM til stede	
	TPM. Hvis der ikke er nogen TPM til stede, går man tilbage til Software KSP.		
	Software Key Storage Provider		Marker den private nøgle som eksporterbar
	Windows Hello til virksomheder	Beholderens navn	Angiver navnet på Windows Hello for Business (tidligere kendt som Microsoft Passport for Work).
		PIN-prompt-tekst	Angiver den brugerdefinerede tekst, der skal vises på Windows Hello for Business PIN-prompten under certifikattilmelding.
Legitimation	Upload en PKCS#12-fil		

SCEP

Beskrivelse	Beskrivelse af SCEP-server		
Implementeringens omfang	Anvendelsesområde for certifikater: Nuværende enhed vs. bruger		
URL'er til SCEP-servere	En eller flere servere, der udsteder certifikater via SCEP		
Emne	Repræsentation af et X.500-navn. F.eks. "C=US, O=Microsoft Corporation, CN=foo, 1.2.5.3=bar"		
Alternative navne til emnet	Type	E-mail-adresse	
		DNS	
		URI	
		Brugerens hovednavn (UPN)	
CA Fingeraftryk	SHA1-fingeraftrykket for certifikatet fra certifikatudstederen. E.g. 31:8F:1E:78:5C:D5:12:9F:7E:3B:AD:F3:1C:C0:19:03:96:43:A9:E5		
Enheder for gyldighedsperiode	Dage, måneder eller år		
Gyldighedsperiode			
Udfordring	Bruges som den forhåndsdelte hemmelighed til automatisk tilmelding		
Forsøg igen	Det antal gange, enheden skal prøve igen, hvis serveren sender et PENDING-svar. Standardværdien er 5. Den maksimale værdi er 30.		
Forsøgsforsinkelse	Antal minutter, der skal ventes, før man prøver igen. Standardværdien er 5. Minimumsværdien er 1.		
Nøgle størrelse	Nøglestørrelse i bits		
Hash-algoritme	Familie af hashalgoritmer		
Brug af nøgler	Udvidelsen til nøglebrug definerer formålet (f.eks. kryptering, signatur) med den nøgle, der er indeholdt i certifikatet. Mindst én af "Digital signatur" eller "Kryptering af nøgle" skal vælges.		
Udvidet brug af nøgler	Angiver udvidet brug af nøgler, afhængig af SCEP-serverens konfiguration. Angiv listen over tilsvarende OID'er, f.eks. 1.3.6.1.5.5.7.3.2 (klientgodkendelse).		
Vigtig placering	Den Key Storage Provider, som den private nøgle skal installeres på.		
		TPM. Fejl hvis ingen TPM til stede	
	TPM. Hvis der ikke er nogen TPM til stede, går man tilbage til Software KSP.		

	Software Key Storage Provider			
	Windows Hello til virksomheder	Beholderens navn	Angiver navnet på Windows Hello for Business (tidligere kendt som Microsoft Passport for Work).	
		PIN-prompt-tekst	Angiver den brugerdefinerede tekst, der skal vises på Windows Hello for Business PIN-prompten under certifikattilmelding.	

Håndtering af forbindelser

Wifi

Med denne indstilling kan du udføre forudgående konfiguration af slutbrugernes enheder for adgang til interne adgangspunkter

Identifikator for servicesæt (SSID)	SSID til det netværk, som forbindelsen skal oprettes til
Automatisk tilslutning	Aktivér automatisk tilslutning til netværket
Skjult netværk	Aktivér, hvis AP'et ikke udsender SSID'et

Sikkerhedstype

Etablering af AP-sikkerhedstype

WEP åbent system	
Adgangskode	Adgangskode til AP'et

WPA PSK	
Adgangskode	Adgangskode til AP'et

WPA EAP	
Autentificeringstype	Godkendelsestype, kun mulig med "PEAP-MSCAHPv2"
Hurtig genforbindelse	Enheder kan skifte mellem Access Points uden at skulle godkende sig selv igen
Gæsteadgang	Brugeren har ikke en konto og skal derfor registrere sig som gæst.
Kontrol af karantæne	Klienten skal udføre NAP-tjek (Network Access Protection) og dele resultaterne med systemet, som derefter beslutter, om klienten kan oprette forbindelse.
Kræver kryptobinding	Autentificering er kun mulig via Crypto Binding
Server-validering	Klienten tjekker, om servercertifikatet er gyldigt. Hvis det er tilfældet, vil der blive etableret en forbindelse.
Spørg efter certifikater	Giver brugeren mulighed for at acceptere ikke-betroede certifikater
Server-navne	Giver mulighed for at vise navnet på den RADIUS-server, der tilbyder netværksgodkendelse og -autorisation.

WPA2-PSK	
Adgangskode	AP-adgangskode

WPA2 EAP	
Autentificeringstype	Godkendelsestype, kun mulig med "PEAP-MSCAHPv2"
Hurtig genforbindelse	
Gæsteadgang	
Kontrol af karantæne	Aktiverer netværksadgangsbeskyttelsen NAP
Kræver kryptobinding	Autentificering er kun mulig via Crypto Binding
Server-validering	
Spørg efter certifikater	Spørger efter et valideret servercertifikat, navn eller en rodcertifikatgodkendelse (CA)
Server-navne	Liste over de servere, som enhederne skal have tillid til
Ingen	Ingen etableret sikkerhed
Brug proxyserver	Brug af en proxyserver
Serveradresse	Adresse på proxyserver
Serverport	Proxyserverens serverport

Brug proxyserver

Aktivér brug af proxyserver.

Serveradresse	Proxyserveradresse, der bruges af dette netværk.
Serverport	Proxyserverport, der bruges af dette netværk.

Begrænsninger for wifi

Her kan du definere forskellige Wifi-begrænsninger.

Tillad WiFi	Tillad/afvis WiFi
Tillad internetdeling	Tillad brug af et hotspot
Tillad automatisk tilslutning til WiFi Sense Hot Spots	Tillad automatisk tilslutning til WiFi Sense Hot Spots
Tillad manuel WiFi-konfiguration	Tillad brugeren at oprette forbindelse til WiFi-netværk, der ikke er defineret af AppTec
WLAN-scanningsfrekvens	Fastsætter WLAN-scanningsintervallet. Her øger en højere værdi evnen til at genkende WIFI-netværk.

VPN

Udfør de relevante indstillinger her for at konfigurere VPN-forbindelser

Navn på forbindelse	Angivne forbindelsesnavn		
VPN-type	En VPN-forbindelse pr. app bruges til at sikre trafikken i visse apps.		
	VPN	Altid tændt	Dette vil automatisk forbinde VPN'en ved login og forblive forbundet, indtil brugeren manuelt afbryder forbindelsen.
	VPN pr. app	VPN-apps	Definer apps, der bruger denne VPN-forbindelse
		Låsning pr. app	Per-App Lockdown gør, at de valgte apps kun har forbindelse via denne VPN-forbindelse. Denne funktion afhænger af Windows Defender Firewall.
	WIP-profil	WIP-domæne for denne forbindelse	Enterprise ID, som kræves for at forbinde denne VPN-profil med en Windows Information Protection (WIP)-politik

Tilslutningstype

AppTec360 VPN	
For "AppTec360 VPN" kræves det, at app-sideloading er tilladt. Aktiver venligst "Tillad app-sideloading" i "Sikkerhedsstyring" → "Begrænsningsindstillinger" → "Enhedsfunktionalitet".	
Gateway-konfiguration	Hvis du vil konfigurere en VPN-forbindelse med sortlistning, skal du vælge en VPN-konfiguration med en specificeret DNS-server. Du kan opsætte en VPN-konfiguration i "Generelle indstillinger" → "Universal Gateway" → "VPN-indstillinger".

IKEv2		
Servere	Liste over VPN-servere	
Enhedstunnel	Aktivér forbindelse før brugerlogon.	
Godkendelsesmetode	EAP	EAP XML
	Maskincertifikater	
Krypteringsalgoritme		
Algoritme til integritetskontrol		
Diffie-Hellman-gruppe		
Ciffer-transformationsalgoritme		
Transformationsalgoritme til autentificering		
Perfekt fremadrettet hemmeligholdelse (PFS) gruppe		

PPTP		
Servere	Liste over VPN-servere	
Godkendelsesmetode	EAP	EAP XML

L2TP		
Servere	Liste over VPN-servere	
Godkendelsesmetode	EAP	EAP XML
Krypteringsalgoritme		
Algoritme til integritetskontrol		
Diffie-Hellman-gruppe		
Ciffer-transformationsalgoritme		
Transformationsalgoritme til autentificering		
Perfekt fremadrettet hemmeligholdelse (PFS) gruppe		

Automatisk		
Servere	Liste over VPN-servere	
Godkendelsesmetode	EAP	EAP XML

Generiske VPN-konfigurationer

Husk legitimationsoplysninger ved hvert logon	
Registrer IP-adresser med intern DNS	
Regler for filtrering af netværkstrafik	Begræns VPN-forbindelsen til det definerede regelsæt.
DNS-suffix-søgeliste	DNS-suffikser, der skal føjes til DNS-søgelisten til routing af korte navne.
NRPT-regler (Name Resolution Policy Table)	NRPT-regler (Name Resolution Policy Table) definerer, hvordan DNS opløser navne, når der er forbindelse til VPN'en.
Registrering af pålidelige netværk	Liste over DNS-suffikser til identifikation af betroede netværk.
Delt tunnelering	Split tunneling betyder, at trafikken kan gå over enhver grænseflade, som bestemmes af netværksstakken.
Opdelte tunnelruter	Liste over ruter, der skal føjes til routingtabellen for VPN-grænsefladen.
Proxy-opsætning	Konfigurerer den proxy, der bruges med dette netværk
Proxy-adresse	Proxyserveradresse som et fuldt kvalificeret værtsnavn eller en IP-adresse.
Havn	Proxyserverens port.
URL til automatisk proxy-konfiguration	URL for automatisk at hente proxyindstillingerne.

VPN-begrænsninger

Her kan du definere forskellige VPN-begrænsninger.

Tillad VPN-indstillinger	Denne retningslinje tillader/forbyder brugeren at deaktivere og ændre VPN-indstillingerne
Tillad VPN over mobilnettet	Tillader/forbyder enheden at oprette en VPN-forbindelse, hvis enheden bruger mobildata
Tillad VPN-roaming over mobilnettet	Tillader/forbyder enheden at oprette en VPN-forbindelse, hvis enheden roamer

Bluetooth

Her kan du bestemme, om Bluetooth skal være tilladt/forbudt.

Tillad Bluetooth	Aktiver/deaktiver Bluetooth

PIM-styring

Aktiv synkronisering af Exchange

Opsætning af ActiveSync-kontoen på slutbrugerens enhed

Kontonavn	Navn på e-mailkonto
Serverens værtsnavn	Serveradresse/FQDN
Domænenavn	Server-domæne
E-mail-adresse	E-mail-adresse
Brugernavn	Brugernavn
Brugeradgangskode	Eventuelt kan du allerede knytte en adgangskode til brugeren her
Brug SSL	Brug SSL-forbindelse
Synkroniseringsinterval	Her kan synkroniseringsintervallet fastlægges Manuel synkronisering = Brugeren skal downloade sine e-mails og udføre en manuel synkronisering
Aldersfilter for mails	Tidsrum, indtil e-mails skal synkroniseres Intet filter = ubegrænset
Log-niveau	Etablering af logningsniveauer for ActiveSync-trafikken
Synkroniser e-mail	Aktiveret = e-mails er synkroniseret
Synkroniser kontakter	Aktiveret = kontakter er synkroniseret
Synkroniser kalender	Aktiveret = kalenderen er synkroniseret
Synkroniser opgaver	Aktiveret = opgaverne er synkroniseret

E-mail

Oprettelse af POP3/IMAP4-konti på slutbrugerens enhed.

Beskrivelse af konto	Navn på e-mailkonto
Afsenderens navn	Visning af afsendernavn
Domænenavn	Domænenavn for e-mailkontoen
E-mail-adresse	Brugerens e-mailadresse
Brugernavn	Brugernavn
Brugeradgangskode	Eventuelt kan du allerede knytte en adgangskode til brugeren her
Alternative legitimationsoplysninger til udgående servere	Her kan det defineres, hvis der kræves andre legitimationsoplysninger til den udgående server
Udgående domænenavn	Udgående domænenavn
Brugernavn på udgående server	Brugernavn på udgående server
Adgangskode til udgående server	Adgangskode til udgående server
E-mail-protokol	POP3 eller IMAP4 kan bruges som protokol
Værtsnavn for indgående mailserver	Værtsnavn for indgående mailserver
Brug SSL til indgående mails	Brug SSL til indgående e-mails
Værtsnavn for udgående mailserver	Værtsnavn for udgående mailserver
Brug SSL til udgående mails	Brug SSL til udgående e-mails
Godkendelse af udgående server	En udgående servergodkendelse er påkrævet
Synkroniseringsinterval	Her kan synkroniseringsintervallet fastlægges Manuel synkronisering = Brugeren skal downloade sine e-mails og udføre en manuel synkronisering
Aldersfilter for mails	Tidsrum, indtil e-mails skal synkroniseres Intet filter = ubegrænset

App-administration

Enterprise App Manager

Installerede apps

Her er en liste over de apps, der i øjeblikket er installeret på den enhed, der vises.

Obligatoriske apps

Her kan du konfigurere en liste over apps, der er obligatoriske på enheden.

Denne liste tjekkes, hver gang enheden opretter forbindelse til MDM, og alle apps på listen, som ikke er installeret på enheden, installeres, uanset om appen er afinstalleret eller aldrig har været installeret før.

Du kan uploade Windows 10 In-House Apps og derefter tilføje dem til denne liste, eller du kan tilføje Microsoft Office-konfigurationer, som skal konfigureres på forhånd i "Generelle indstillinger" > "App Management" > "Microsoft Office".

Begrænsninger for systemapper

Indbakke-apps
Tillad alarmer og ur
Tillad lommeregner
Tillad kamera
Tillad kontakt med support
Tillad Cortana
Tillad filudforsker
Tillad at komme i gang
Tillad Groove-musik
Tillad kort
Tillad beskeder
Tillad Microsoft Edge
Tillad film og tv
Tillad penge
Tillad nyheder
Tillad OneDrive
Tillad OneNote
Tillad Outlook-kalender og -mail
Tillad mennesker
Tillad telefon
Tillad billeder
Tillad Powerpoint
Tillad indstillinger
Tillad Skype
Tillad sport
Tillad butik
Tillad stemmeoptager
Tillad tegnebog
Tillad vejret

Tillad Windows Feedback Hub
Tillad ord
Tillad Xbox

Indstilling af sider
Tillad konti på arbejdspladsen
Tillad avanceret info
Tillad apps-hjørnet
Tillad blokering og filtrering
Tillad farveprofil
Tillad køretilstand
Tillad e-mail og konti
Tillad Equalizer
Tillad tastatur
Tillad navigationslinje
Tillad flytilstand for netværk
Tillad deling af netværk og internet
Tillad netværkstjenester
Tillad netværk Wi-Fi
Tillad pc-systemets Bluetooth
Tillad bedømmelse af din enhed
Tillad gendannelse af opdatering
Tillad deling
Tillad start
Tillad tid Sprog
Tillad tid Region
Tillad Windows' standardlåseskærm
Tillad arbejds- eller skolekonto

Sort- og hvidlistning

Under "Black- & Whitelisting" kan du vælge mellem tilstanden "Whitelist" og tilstanden "Blacklist".

Hvidliste	Kun apps og tjenester, der er føjet til listen, kan installeres på slutbrugerens enhed. Hvis de allerede er forudinstalleret på slutbrugerens enhed, vil de blive aktiveret og indstillet, så brugeren kan køre dem.
	Alle andre apps, der ikke er føjet til listen, kan ikke installeres på slutbrugerens enhed. Hvis de allerede er forudinstalleret på slutbrugerens enhed, vil de blive deaktiveret og indstillet, så brugeren ikke kan køre dem.
Sortliste	Apps og tjenester, der føjes til listen, kan ikke installeres på slutbrugerens enhed. Hvis de allerede er forudinstalleret på slutbrugerens enhed, vil de blive deaktiveret og indstillet, så brugeren ikke kan køre dem.
	Alle andre apps, der ikke er føjet til listen, kan installeres på slutbrugerens enhed. Hvis de allerede er forudinstalleret på slutbrugerens enhed, vil de blive aktiveret og indstillet, så brugeren kan køre dem.

Med kan du tilføje yderligere apps eller tjenester til den aktuelt anvendte liste.

Med kan du tilføje yderligere apps eller tjenester til den aktuelt inaktive liste.

Du kan enten tilføje en app fra "Windows App Store" eller direkte indtaste en "app-identifikator" for at tilføje den til sort- eller hvidlisten.

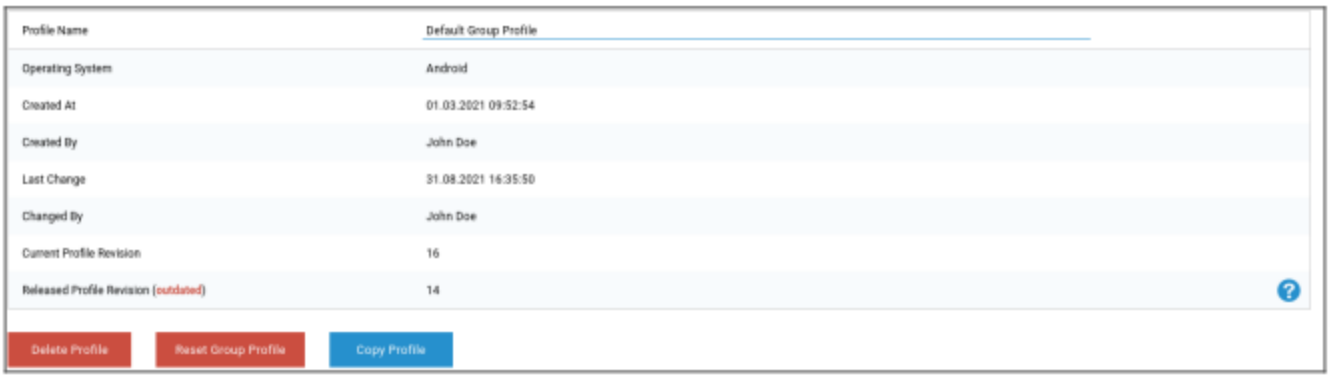
MacOS-konfiguration

Afhængigt af om du har valgt en profil eller en enhed, er displayet og dets underpunkter forskellige - vær meget opmærksom på dette!

Generelt

Oversigt over gruppeprofiler (kun på gruppeniveau)

Når du åbner en gruppeprofil, får du et hurtigt overblik over profilen.



Navn på profil	Navn på profilen (kan ændres her)
Operativsystem	Operativsystem, som profilen er til
Oprettet på	Tidspunkt for skabelse
Oprettet af	Profilens skaber
Sidste ændring	Tidspunkt for sidste ændring af profilen
Ændret af	Konto, der foretog de sidste ændringer
Nuværende profilrevision	Revision af gemt profiltilstand
Udgivet profilrevision	Tildelt profilrevision ("Tildel nu"). Hvis etiketten viser "(forældet)" bag teksten, betyder det, at du har gemt profilen, men ikke tildelt den endnu, så enhederne vil stadig få en ældre version.

Enhedsoversigt (kun på enhedsniveau)

Enhedens sammenfattede oversigt.

Enhedens navn	Enhedens navn
Model	Model
Operativsystem	Operativsystem
Serienummer	Enhedens serienummer
Ejerskab af enhed	Den konfigurerede ejerskabstype
Enhedstype	Enhedens type
Overensstemmende	Viser, om enheden er kompatibel
IP-adresse	IP-adressen, som enheden er forbundet til serveren fra
Sidst set	Tidspunkt for sidste forbindelse fra enheden
Sidste skub	Tidspunkt for sidste push sendt til enheden
Opgave	Her kan du flytte enheden til en anden bruger eller gruppe

Config Revision (kun på enhedsniveau)

Her får du en oversigt over, hvilken gruppeprofil der er tildelt enheden.

Hvis du klikker på gruppeprofilen, får du direkte adgang til profilen, og du kan foretage indstillinger.

Med symbolet kan du gendanne de tildelte apps til gruppeprofilens indstillinger.

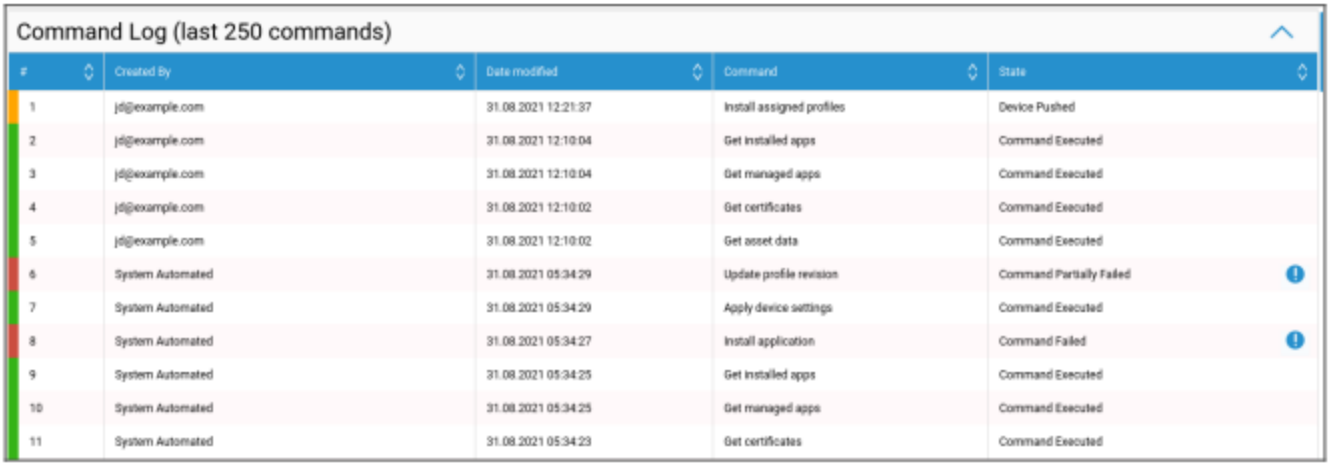
Med symbolet kan du nulstille enhedens profil, så den slet ikke har nogen indstillinger.

"Nyere revision tilgængelig" angiver, at gruppeprofilen er blevet ændret og gemt, men ikke tildelt. Gruppeprofilen skal tildeles med "Tildel nu" på gruppeniveau for at anvende ændringerne på enhederne.

Enhedslog (kun på enhedsniveau)

Kommando-log

Her kan du se, hvilke kommandoer der er udstedt til enheden, og hvad deres status er.



Kommandoer, der er oprettet af "System Automated", oprettes automatisk af systemet.

Mulige kommandostatusser

Enhed skubbet	Der er sendt en push-anmodning til push-tjenesten (f.eks. APNS) for at fortælle enheden, at den skal oprette forbindelse tilbage til EMM-serveren.
Kommando oprettet	Kommandoen blev oprettet i systemet.
Kommando sendt	Kommandoen blev sendt til enheden, efter at den havde oprettet forbindelse til serveren.
Kommando udført	Kommandoen blev udført med succes.
Kommando mislykkedes	Kommandoen mislykkedes. *
Kommando delvist mislykket	Afhængigt af enhedens operativsystem kan nogle kommandoer blive grupperet sammen. Nogle dele af denne kommandogruppe mislykkedes. *
Kommandoen blev udført, men mislykkedes til sidst	Kommandoen blev udført, men måske blev den ikke.
Kommando genindført	Kommandoen blev repushed af en bruger.
Kasseret	Kommandoen blev kasseret. For eksempel fordi den blev erstattet af en anden kommando, eller fordi enheden blev genindskrevet, og gamle kommandoer blev fjernet.

*Hvis der er et udråbstegn bag beskeden, kan du få flere oplysninger ved at holde markøren over ikonet.

Asset Management (kun på enhedsniveau)

Enhedsinfo

Modelnummer	Modelnummer
Værtsnavn	Værtsnavn
Lokalt værtsnavn	Lokalt værtsnavn
Operativsystem	Operativsystem
OS-version	OS-version
UDID	UDID
Fri / samlet hukommelse	Fri / samlet hukommelse

WiFi

IP-adresse	IP-adresse
WiFi MAC	WiFi MAC

Cellulær

Telefonnummer	Telefonnummer
Roaming-status	Roaming-status
Roaming (tale/data)	Roaming (tale/data)
IP-adresse	IP-adresse
Operatør/transportør	Operatør/transportør
SIM-bærerens netværk	Bærende netværk
Transportør-version	Transportør-version
ICCID	ICCID
Nuværende MCC/MNC	Nuværende MCC/MNC
SIM MCC/MNC	SIM MCC/MNC

Bluetooth

Bluetooth MAC	Bluetooth MAC

Opdateringsstyring (kun på enhedsniveau)

Opdatering af info

Denne fane viser oplysninger om systemopdateringsindstillingerne på enheden.

Autocheck aktiveret	Hvis systemet automatisk tjekker for opdateringer.
Automatisk app-opdatering aktiveret	Hvis systemet vil installere app-opdateringer automatisk.
Automatiske OS-opdateringer aktiveret	Hvis systemet vil installere systemopdateringer automatisk.
Automatiske sikkerhedsopdateringer aktiveret	Hvis systemet vil installere sikkerhedsopdateringer automatisk.
App-opdatering af baggrundsdownload aktiveret	Hvis systemet vil downloade app-opdateringer i baggrunden.
Katalog-URL	URL'en til det softwareopdateringskatalog, som klienten bruger.
Er standardkatalog	Hvis "ja", er Catalog standardkataloget.
Udfør periodisk kontrol	Hvis "ja", start en ny scanning.
Tidligere scanningsdato	Datoen for den sidste softwareopdateringsscanning.
Tidligere scanningsresultat	Resultatkoden for den sidste softwareopdateringsscanning.

Sikkerhedsstyring

Anti-tyveri

Tør og lås

Fuld aftørring	Send en kommando til fabriksnulstilling af enheden
Enterprise Wipe	Fjern MDM fra enheden, og fjern alle MDM-data (f.eks. konti, apps).
Låseskærm	Få enheden til at vende tilbage til låseskærmen

Sikkerhedskonfiguration

Adgangskode

Deaktivering af kode tilladt	Bestemmer, om brugeren skal tvinges til at angive en pinkode. Ved at indstille denne værdi (og ikke andre) tvinges brugeren til at indtaste en adgangskode, uden at der stilles krav til længde eller kvalitet.
Tillad simpel værdi	Tillad brugeren at bruge de samme, eskalerende og reducerende talstrenge (f.eks. 1234, 1111)
Kræver alfanumerisk værdi	Adgangskoder skal indeholde mindst ét bogstav
Minimumslængde på adgangskoden	Minimal længde på adgangskode
Minimum antal komplekse tegn	Minimalt antal alfanumeriske symboler i adgangskoden
Maksimal alder på adgangskoden	Antal dage, hvorefter adgangskoden skal ændres
Maksimal autolås	Maksimal tid, hvorefter enheden er låst
Maksimal afdragsfri periode for enhedslås	Hvor lang tid enheden kan være låst uden at blive bedt om at indtaste adgangskoden ved oplåsning
Maksimal alder på adgangskoden (1-730 dage eller ingen)	Dage, efter hvilke adgangskoden skal ændres
Adgangskodehistorik (1-50 adgangskoder eller ingen)	Antal unikke adgangskoder før genbrug

Certifikat

PKCS#1	
Beskrivelse	Indtast en beskrivelse af certifikatet
Legitimation	Upload en pkcs1-fil

PKCS#12	
Beskrivelse	Indtast en beskrivelse af certifikatet
Legitimation	Upload en pkcs12-fil

Begrænsningsindstillinger

Enhedens funktionalitet

Tillad kamera	Tillad brug af kameraet
Tillad Game Center	Hvis den er falsk, er Game Center deaktiveret, og ikonet er fjernet fra startskærmen.
Tillad multiplayer-spil	Når den er falsk, forbyder den multiplayer-spil.
Tillad tilføjelse af Game Center-venner	Når den er falsk, forbydes det at tilføje venner til Game Center.
Tillad iCloud Photo Library	Hvis den er sat til false, deaktiveres iCloud Photo Library. Alle fotos, der ikke er fuldt downloadet fra iCloud Photo Library til enheden, fjernes fra det lokale lager.
Tillad Touch ID	Hvis den er falsk, forhindrer den Touch ID i at låse en enhed op.

iCloud

Bloker visse funktioner under iCloud-parring

Tillad synkronisering af dokumenter	Tillad synkronisering af dokumenter
Tillad synkronisering af iCloud-nøglering	Tillad synkronisering af iCloud-nøglering
Tillad iCloud-noter	Når den er falsk, afviser den MacOS iCloud Notes-tjenester.
Tillad iCloud BTMM	Når den er falsk, afviser den MacOS Back to My Mac iCloud-tjenesten.
Tillad iCloud FMM	Når den er falsk, afviser den MacOS Find My Mac iCloud-tjenesten.
Tillad iCloud-bogmærker	Når den er falsk, afviser den MacOS iCloud Bookmark-synkronisering.
Tillad iCloud Mail	Når den er falsk, tillader den ikke MacOS Mail iCloud-tjenester.
Tillad iCloud-kalender	Når den er falsk, afviser den MacOS Cloud iCloud-tjenester.
Tillad iCloud-påmindelser	Når den er falsk, afviser den iCloud Reminder-tjenester.
Tillad iCloud-adressebog	Når den er falsk, afviser den MacOS iCloud Address Book-tjenester.

Ledelse af medier

Skub ud ved logout	Skub alle flytbare medier ud ved logout
Tillad netværk	Tillad adgang for netværksmedier
Tillad intern disk	Tillad adgang for intern disk.
Kræver godkendelse	Kræv godkendelse for brug af dette medie
Kun læsning	Brugeren er kun i stand til at læse data fra mediet
Tillad ekstern disk	Tillad adgang for ekstern disk.
Kræver godkendelse	Kræv godkendelse for brug af dette medie
Kun læsning	Brugeren er kun i stand til at læse data fra mediet
Tillad brug af diskbilleder	Tillad adgang for billeder.
Kræver godkendelse	Kræv godkendelse for brug af dette medie
Kun læsning	Brugeren er kun i stand til at læse data fra mediet
Tillad brug af DVD-RAM'er	Tillad adgang for DVD-RAM-disk.
Kræver godkendelse	Kræv godkendelse for brug af dette medie
Kun læsning	Brugeren er kun i stand til at læse data fra mediet
Tillad brug af dvd'er	Tillad adgang for dvd-disk.
Kræver godkendelse	Kræv godkendelse for brug af dette medie
Tillad brug af cd'er	Tillad adgang for cd-disk.
Kræver godkendelse	Kræv godkendelse for brug af dette medie

Håndtering af forbindelser

Wi-Fi

Her kan du tilføje og konfigurere Wi-Fi-forbindelser

Identifikator for servicesæt (SSID)	SSID for det netværk, som forbindelsen skal oprettes til
Automatisk tilslutning	Aktivér automatisk tilslutning til netværket
Skjult netværk	Aktiver, hvis AP'et ikke udsender SSID'et
Proxy-opsætning	Konfiguration af en proxy for hvert adgangspunkt
Ingen	Brug ikke en proxyserver
Manuel	Opret en manuel proxy
URL til proxyserver	Adresse for adgang til proxyindstillinger
Havn	Fastlæg porten til proxyen
Autentificering	Brugernavn til godkendelse på proxyen
Adgangskode	Adgangskode til godkendelse på proxyen
Automatisk	Opret automatisk en proxy
URL til proxyserver	URL til filen med proxyindstillinger
Sikkerhedstype	Etablering af sikkerhedstype for AP'et
WEP	
Adgangskode	Adgangskode til AP'et
WPA/WPA2	
Adgangskode	Adgangskode til AP'et
WEP Enterprise - WPA /. WPA2 Virksomhed /. Enhver virksomhed	Se tabel Fejl: Henvisningskilde ikke fundet nedenfor
Ingen	Etablerer ingen sikkerhed
Deaktiver randomisering af MAC-adresse	Deaktiverer randomisering af MAC-adresser for det pågældende Wi-Fi-netværk, mens det er tilknyttet netværket. Dette viser også en advarsel om beskyttelse af personlige oplysninger i Indstillinger, der indikerer, at netværket har reduceret beskyttelse af personlige oplysninger.

Konfiguration af Enterprise Wi-Fi

Bemærk: Kun tilgængelig, når "Sikkerhedstype" er indstillet til en virksomhedstype.

Protokoller	Godkendelsesprotokol understøttet på målnetværket
TLS	Aktiver / deaktiver brug
TTLS	Aktiver / deaktiver brug
Indre godkendelser	Den godkendelsesprotokol, der skal bruges: PAP, CHAP, MSCHAP, MSCHAPv2
LEAP	Aktiver / deaktiver brug
PEAP	Aktiver / deaktiver brug
EAP-FAST	Aktiver / deaktiver brug
EAP-SIM	Aktiver / deaktiver brug
Brug PAC	Brug af PAC (beskyttet adgangskontrol)
Tilvejebringelse af PAC	Konfiguration af Provision PAC
Tilvejebringelse af PAC anonymt	Anonym levering af PAC
Autentificering	
Brugernavn	Brugernavn til autentificering
Brug ikke Per forbindelse Adgangskode	Brug ikke adgangskode pr. forbindelse
Adgangskode	Den adgangskode, der skal bruges
Identitetscertifikat	Upload/vælg godkendelsescertifikat
Ydre identitet	Identitet, der kan ses udefra
Tillid	
Betroet certifikat 1	Upload det første betroede certifikat
Betroet certifikat 2	Upload det andet betroede certifikat
Betroet certifikat 3	Upload et tredje betroet certifikat
Betroet server Navne på certifikater	Navnene på de forventede servercertifikater (i en kommasepareret liste)

VPN

Afhængigt af den valgte forbindelsestype kan forskellige felter være synlige.

Navn på forbindelse	Navn på VPN-profilen
VPN-type	
VPN	Al enhedens netværkstrafik vil blive dirigeret via en VPN-forbindelse.
Tilslutningstype	Etablering af VPN-forbindelsestype
IPsec (cisco)	IPsec-protokol fra Cisco
L2TP	L2TP-protokol
Brugerdefineret SSL	Forbindelse via brugerdefineret SSL
IKEv2	IKEv2-protokol
Proxy-opsætning	Konfiguration af en proxy til VPN-forbindelsen
Ingen	Opret ingen fuldmagt
Manuel	Opret en proxy manuelt
URL til proxyserver	Adresse for adgang til proxyindstillinger
Havn	Fastlæg porten til proxyen
Autentificering	Brugernavn til autentificering på proxyen
Adgangskode	Adgangskode til autentificering på proxyen
Automatisk	Opret automatisk en proxy
URL til proxyserver	URL til adgang til proxyindstillingerne

HTTP-proxy

Proxy-type	
Manuel	Opret en proxy manuelt
URL til proxyserver	Adresse for adgang til proxyindstillingerne
Havn	Etablering af proxy-port
Autentificering	Brugernavn til autentificering på proxyen
Adgangskode	Adgangskode til autentificering på proxyen
Automatisk	Opret automatisk en proxy
Proxy PAC-URL	Proxy PAC-URL
Tillad direkte forbindelse, hvis PAC ikke kan nås	Tillad direkte forbindelse (uden VPN), hvis PAC ikke kan nås
Tillad omgåelse af proxy for at få adgang til lukkede netværk	Tillad omgåelse af proxy for at få adgang til lukkede interne netværk

AirPrint

IP-adresse	Printerens IP-adresse
Ressource-sti	En klar vej til AirPrint-enheden

AirPlay

Enhedens navn	Enhedens navn
Adgangskode	Adgangskode til parring
Hvidliste	Definer en liste over enheder, som enheden udelukkende kan parre sig med

PIM-styring

Aktiv synkronisering af Exchange

Kontonavn	Navn på kontoen.
E-mail-adresse	Adressen til kontoen (f.eks. max@company.com)
Serverens værtsnavn	Internt værtsnavn
Login-navn	"Domain" og "Login Name" skal være tomme, for at enheden kan spørge efter brugeren.
Domæne	"Domain" og "Login Name" skal være tomme, for at enheden kan spørge efter brugeren. Hvis en ACL Gateway-konfiguration er aktiveret, og feltet Domæne ikke er tomt, vil AppTec360 Universal Gateway godkende enheden med følgende navn "Domæne\Login-navn"
Adgangskode	Adgangskoden til kontoen (f.eks. secretUserPassword)
Tidligere dage med Mail to Sync	Antallet af tidligere dages post, der skal synkroniseres
Brug SSL	Brug SSL til intern Exchange-vært
Avanceret mulighed	Vis avancerede indstillinger
Serverport	Intern port
Server-sti	Intern sti
Eksternt værtsnavn	Ekstern vært
Ekstern port	Ekstern port
Ekstern sti	Ekstern sti
Brug SSL til eksterne Udvekslingsvært	Brug SSL til ekstern Exchange-vært

E-mail

Opsætning af POP3/IMAP-konti på slutbrugerens enhed

Beskrivelse af konto	Navn på e-mail-konti
Kontotype	
IMAP	
Stipræfiks	Stipræfikset for særlige mapper
POP	
Brugerens visningsnavn	Brugerens visningsnavn
E-mail-adresse	Brugerens e-mailadresse

Indgående post	Indstillinger for indgående server
Mailserver-adresse	Mailserver-adresse
Port til mailserver	Mailserver-port
Brugernavn	Respektive brugernavn
Autentificeringstype	Autentificeringstype
Ingen	Ingen godkendelsestype
Adgangskode (kun på enhedsniveau)	Adgangskode-prompt
MDM-udfordring-svar	
NTLM	NTLM-autentificering
HTTP MD5-digest	
Brug SSL	Brug SSL, hvis det er nødvendigt

Udgående post	Indstillinger for udgående server
Mailserver-adresse	Mailserver-adresse
Port til mailserver	Port til mailserver
Brugernavn	Respektive brugernavn
Autentificeringstype	
Ingen	Ingen godkendelsesmetode
Adgangskode (kun på enhedsniveau)	Adgangskode-prompt
MDM-udfordring-svar	
NTLM	NTLM-autentificering
HTTP MD5-digest	
Brug SSL	Brug SSL, hvis det er nødvendigt
Udgående adgangskode samme som indgående	Udgående adgangskode samme som indgående
Brug kun i mail	Aktivér, hvis alle udgående e-mails skal sendes via Mail-appen

CalDav

Konfigurer opsætning og distribution af en CalDav-konto

Beskrivelse af konto	Visningsnavn på kontoen
Værtsnavn	Værtsnavn og/eller IP-adresse
Havn	Port til CalDav-kontoen
Hoved-URL	Kontoens primære URL
Brugernavn	Respektive CalDav-brugernavn
Adgangskode (kun på enhedsniveau)	Respektive CalDav-adgangskode
Brug SSL	Brug SSL, hvis det er nødvendigt

CardDav

Konfigurer opsætning og distribution af en CardDav-konto

Beskrivelse af konto	Visningsnavn på kontoen
Værtsnavn	Værtsnavn og/eller IP-adresse
Havn	Port til CardDav-kontoen
Hoved-URL	Kontoens primære URL
Brugernavn	Respektive CardDav-brugernavn
Adgangskode (kun på enhedsniveau)	Respektive CardDav-adgangskode
Brug SSL	Brug SSL, hvis det er nødvendigt

LDAP

I dette område skal du oprette en LDAP-forbindelse for at muliggøre en dynamisk certifikatudveksling mellem slutbrugerenheden og Active Directory.

Vær opmærksom på, at den valgte bruger skal have læserettigheder.

Beskrivelse af konto	Beskrivelse af konto
Brugernavn til konto	Bruger til LDAP-adgang
Adgangskode til konto	Adgangskode til LDAP-adgang
Kontoens værtsnavn	LDAP-serverens værtsnavn/IP-adresse
Brug SSL	Brug SSL, hvis det er nødvendigt

I den anden del kan du definere individuelle filtre til søgning i LDAP-registret.

Beskrivelse	Omfang	Søg i basen
Beskrivelse af filter	Søgeniveau i LDAP-registret	Definer det enkelte filter

Dashboard og rapportering

Dashboard-indstillinger

Her kan du se, hvilke dashboards der findes, redigere dem eller oprette nye. Hvert dashboard har sit eget sæt data, der skal vises, og sin egen grafkonfiguration.

Kontrol af dashboard-indstillinger

Offentlig	Indstiller dashboardet til at være offentligt, så andre brugere kan se det. Brugerne skal selvfølgelig kunne logge ind og se Dashboards. Hvis "Public" ikke er aktiveret, er det kun skaberen, der kan se det.
Standard	Indstiller Dashboard som standard, så det automatisk åbnes, næste gang du åbner Dashboard View.
	Vis instrumentbrættet og dets grafer
	Slet instrumentbrættet
	Rediger dashboardets navn og indstillinger
	Lav en kopi af dashboardet
	Tilføj et helt nyt dashboard

Dashboard-visning

Her vises data og grafer for det valgte dashboard, og du kan også ændre dem.

Kontrol af instrumentbrættet

	Giver dig mulighed for at definere, hvilke data der skal vises i dashboardet, mængden af data, der skal vises, og i hvilken størrelse disse data skal vises.
	Bringer dig tilbage til Dashboard-oversigten
	Nulstiller det aktuelt åbnede dashboard til standardindstillingen
	Gemmer alle de ændringer, du har foretaget i det aktuelt åbnede dashboard (f.eks. hvilke data, der skal vises).
	Skift diagramtype til søjlediagram
	Skift diagramtype til cirkeldiagram
	Skift diagramtype til doughnut-diagram
	Skift diagramtype til polarområdediagram
	Skift sorteringsrækkefølge

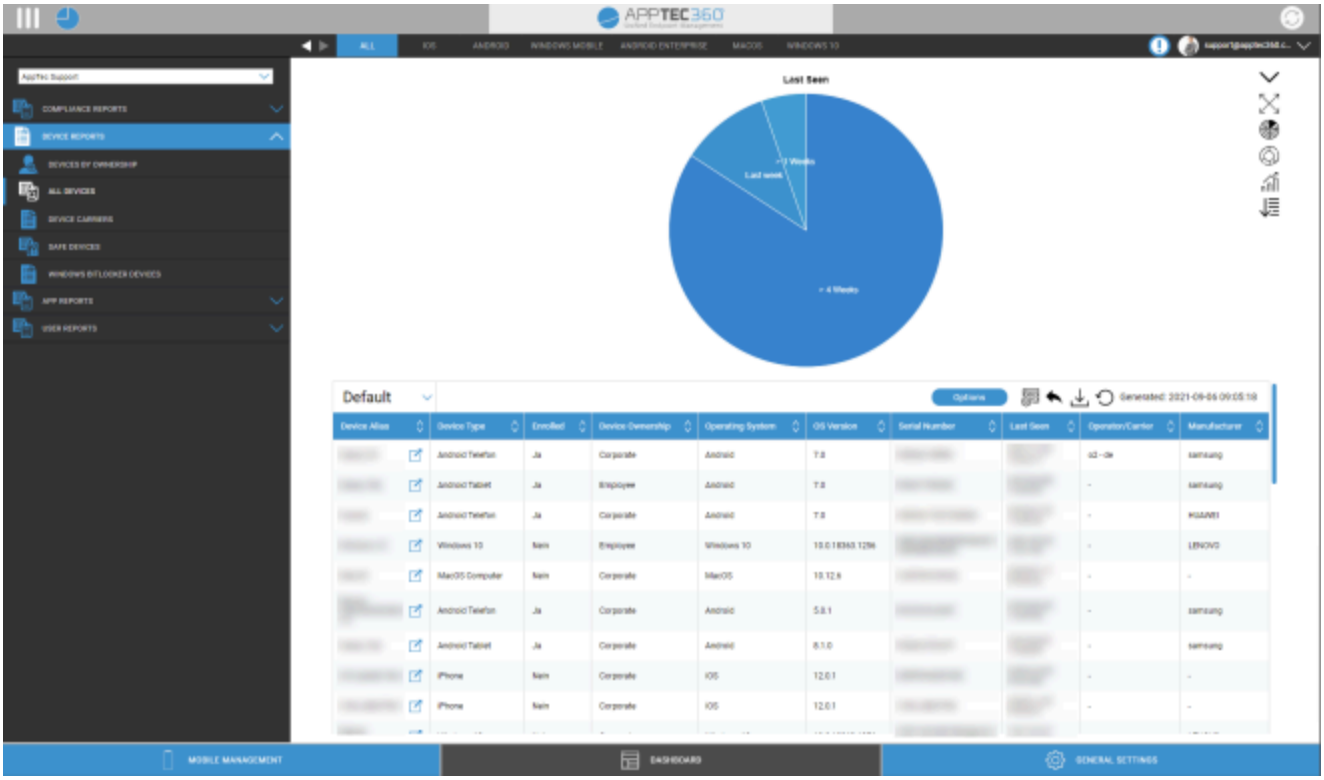
Udvidet rapportering

"Udvidet rapportering" giver detaljerede oversigter og grafer over oplysninger om enheder og brugere.

Der er nogle få standardrapporter, men de kan alle ændres manuelt for at tilføje eller fjerne data, der skal vises.

Bemærk, at du kun kan ændre manuelt, hvilke data der vises. Den valgte rapportkategori definerer de data, den er baseret på. Du vil f.eks. aldrig kunne se Android-enheder i iOS-rapporten i Device Reports All Devices iOS.

Øverst til venstre kan du begrænse rapporteringsdataene til en bestemt gruppe (og alle dens undergrupper). Som standard er dette indstillet til din rodknude, så den tager ALLE enheder og brugere i betragtning.



Udvidet rapporteringskontrol

I hver oversigt kan du bruge følgende funktioner til at ændre rapporten på den måde, du ønsker:

	Skjul diagram (hvis diagram vises)
	Vis diagram (hvis diagram er skjult)
	Udvid diagrammet (hvis diagrammet er foldet sammen)
	Skjul diagrammet (hvis diagrammet er udvidet)
	Skift diagramtype til søjlediagram
	Skift diagramtype til cirkeldiagram
	Skift diagramtype til doughnut-diagram
	Skift diagramtype til polarområdediagram
	Skift sorteringsrækkefølge
	Rediger følgende dele af den viste oversigt: • Tilføj/fjern kolonner • Angiv den rækkefølge, som kolonnerne skal vises i • Vis/skjul diagrammet over tabellen • Vælg den kolonne, der skal bruges til diagrammet • Filtrer dataene i din tabel
	Åbn opsætningshåndteringen for at gemme og indlæse forskellige rapporter
	Nulstiller den aktuelt åbnede rapport til standard
	Eksporter den aktuelle rapport som en .csv-fil
	Generer data og genindlæs den aktuelle rapport

Du kan finde en liste over alle standardrapporter på de næste sider.

Rapporter om overholdelse

Forankrede enheder

Oversigt over de enheder, der er blevet rooted/jailbreaket.

Standardkolonner i denne rapport:

Enhedsalias
Enhedens ejer
E-mail
Operativsystem
Telefonnummer
Sidst set
Producent

Roaming-enheder

Oversigt over alle de enheder, der roamer

Standardkolonner i denne rapport:

Enhedsalias
Enhedens ejer
E-mail
Enhedstype
Operativsystem
Telefonnummer
Sidst set

Roaming-aktiverede enheder

Oversigt over alle enheder, der har aktiveret roaming, men som ikke nødvendigvis roamer i øjeblikket.

Standardkolonner i denne rapport:

Enhedsalias
Enhedens ejer
E-mail
Enhedstype
Operativsystem
Telefonnummer
Sidst set

Overvågede enheder

Oversigt over alle enheder, der er overvåget i overvåget tilstand (kun iOS)

Standardkolonner i denne rapport:

Enhedsalias
Enhedens ejer
E-mail
Enhedstype
Sidst set

Inaktive enheder

Oversigt over alle enheder, der ikke har oprettet forbindelse til serveren i de sidste 7 dage

Standardkolonner i denne rapport:

Enhedsalias
Enhedens ejer
E-mail
Enhedstype
Operativsystem
Sidst set

Enhedsrapporter

Enheder efter ejerskab

Her kan du se, hvor mange enheder der i øjeblikket er implementeret som virksomhedsenheder (corporate devices) og medarbejderenheder (private devices).

Standardkolonner i denne rapport:

Enhedsalias
Enhedens ejer
Enhedstype
Ejerskab af enhed
Operativsystem

Alle enheder

Her kan du se en oversigt over alle enheder med de vigtigste oplysninger.

Standardkolonner i denne rapport:

Enhedsalias
Enhedstype
Indskrevet
Ejerskab af enhed
Operativsystem
OS-version
Serienummer
Sidst set
Operatør/transportør
Producent

Bærere af enheder

Her kan du se en oversigt over operatøren (mobiludbyderen).

Standardkolonner i denne rapport:

Enhedsalias
Enhedens ejer
E-mail
Operativsystem
OS-version
Operatør/transportør

SAFE-enheder

Her kan du se en oversigt over, hvilke enheder der bruger SAFE Version.

Fordi oversigten og/eller SAFE kun er tilgængelig for Samsung-enheder, vil du ikke se de sædvanlige faner under dette punkt.

Standardkolonner i denne rapport:

Enhedsalias
Enhedens ejer
E-mail
Enhedstype
Sidst set
SAFE-version

Windows BitLocker-enheder

Her kan du se en oversigt over de Windows-enheder, der bruger BitLocker.

Standardkolonner i denne rapport:

Enhedsalias
Enhedens ejer
E-mail

BitLocker-status

App-rapporter

Her får du en række forskellige oversigter over apps. I alle disse rapporter kan du klikke på en post for at se, hvilke versioner der er installeret på enhederne, og hvor ofte. I denne visning kan du klikke på en specifik version igen for at se, hvilke enheder der har denne specifikke version installeret.

Bemærk: Det kan tage lidt tid, før systemet får opdaterede oplysninger fra enheden. Desuden opdateres rapporterne ikke hvert minut. Du skal måske være tålmodig for at se den aktuelle status, hvis du lige har tildelt en ny app eller version. Manuel genindlæsning af rapporten vil tvinge rapporten til at vise de mest opdaterede data, der er tilgængelige.

Installerede apps

Her får du en oversigt over alle installerede apps.

Standardkolonner i denne rapport:

Navn	Navnet på den pågældende app og/eller tjeneste
Identifikator	Bestemt app/service-id
Samlet antal	Hvor ofte denne app/tjeneste er blevet installeret på slutbrugernes enheder

Mest installerede apps

Her får du et overblik over de apps, der er blevet installeret mest.

Standardkolonner i denne rapport:

Navn	Navnet på den pågældende app og/eller tjeneste
Identifikator	Bestemt app/service-id
Samlet antal	Hvor ofte denne app/tjeneste er blevet installeret på slutbrugernes enheder

Obligatoriske apps

Her får du en oversigt over obligatoriske (påbudte) apps.

Standardkolonner i denne rapport:

Navn	Navnet på den pågældende app og/eller tjeneste
Identifikator	Bestemt app/service-id
App-kilde	Hvilken AppStore er involveret: • Google PlayStore (Android) • iTunes AppStore (iOS)
OS	Operativsystem

Sortlistede apps

Her får du en oversigt over alle definerede sortlistede apps.

Standardkolonner i denne rapport:

Navn	Navnet på den pågældende app og/eller tjeneste
Identifikator	Bestemt app/service-id
App-kilde	Hvilken AppStore er involveret: • Google PlayStore (Android) • iTunes AppStore (iOS)
OS	Operativsystem

Brugerrapporter

Takst

Her får du et overblik over dine brugeres telefontakster og SIM-kort.

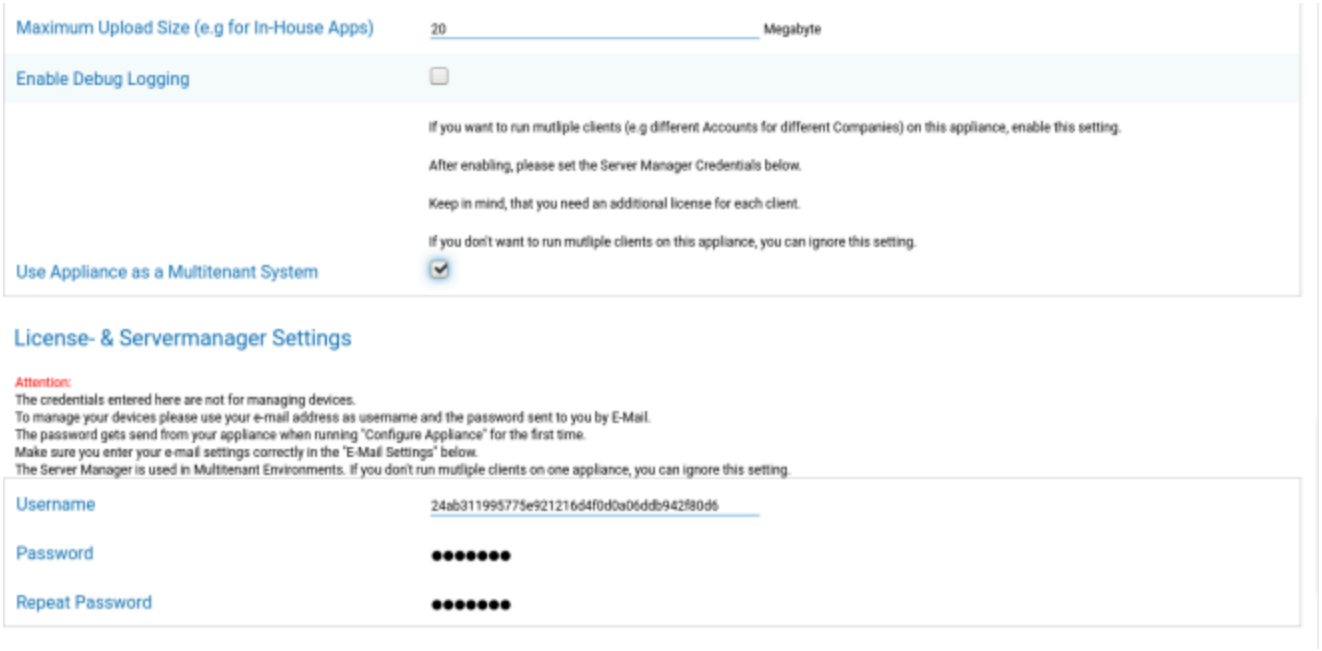
Standardkolonner i denne rapport:

E-mail
Navn
telefonNummer
transportør
Tarif
mulighed
Pris
kontraktAnnulleret
kontraktStart
underTid
mobileAndData
dataVolume
multiSIM
type
simCardSerial1
simCardSerial2
simCardSerial3
pin1
pin2
puk1
puk2
Bemærk

Administration af flere lejere

AppTec360 EMM er i stand til at hoste flere separate lejere, hver med deres egne brugere og grupper, tilladelser og globale indstillinger.

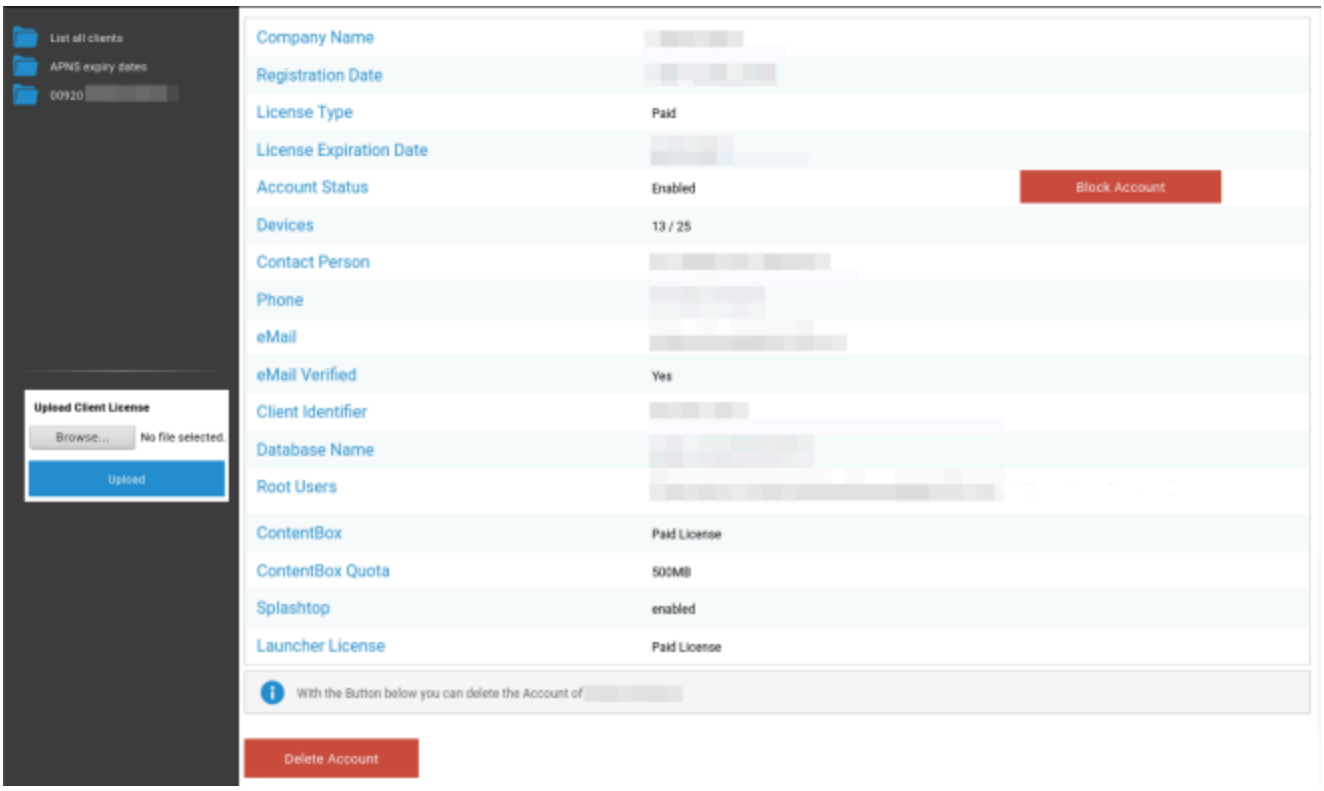
For at aktivere multitenant-funktioner skal du aktivere det i apparatets konfigurationsgrænseflade i "Trin tre - Serverindstillinger".



I den nye menu skal du angive et brugernavn og en adgangskode til Servermanager. Gem indstillingerne, og kør "Configure Appliance" i "Trin fem - Licensaftale" for at anvende indstillingen.

Når konfigurationen er færdig, kan du nu logge ind med de indstillede legitimationsoplysninger via den normale Mobile Management-grænseflade.

Efter login kan du se følgende visning.



Til venstre kan du se alle lejere (i dette tilfælde kun én med id 920), og til højre kan du se oplysninger om denne klient. Du har også mulighed for at blokere adgangen til kontoen samt at slette klienten (FORSIGTIG: Dette vil fjerne alle data relateret til den pågældende klient).

Til venstre kan du uploade en ny klientlicens, som enten kan være en licensopdatering til en eksisterende klient eller en ny licens, som automatisk opretter en ny klient. Når en ny klient oprettes, sendes der automatisk en e-mail med login-adgangskoden til den e-mailadresse, som licensen er udstedt til.

Kontakt din salgsrepræsentant for at få en ny eller opdateret klientlicens (f.eks. hvis du har brug for flere enhedslicenser).

Yderligere visninger

Liste over alle kunder

Viser en oversigt over alle klienter i systemet.

Klient-ID	Klient-ID
Identifikator	Klient-identifikator
Database	Database
Virksomhedens navn	Virksomhedens navn
E-mail	Kontaktperson eMail
Bekræftet	Om kontaktpersonens e-mail er verificeret eller ej
Land	Land
Enheder	Antal registrerede enheder
Registreringsdato	Tidspunkt for licenstildeling
Sidste login	Sidste login til administratorkonto
Licens	Visning af licenstype (gratis|betalt)
CB-licens	ContentBox-licenstype (gratis|betalt)
Status	Aktuel status for AppTec-klienten
Udløbet	Viser, om licensen er udløbet
iOS	Antal iOS-enheder
Android	Antal Android-enheder
Windows Mobile	Antal Windows Mobile-enheder
MacOS	Antal MacOS-enheder
Windows 10	Antal Windows 10-enheder
Android Enterprise	Antal Android Enterprise-enheder
IOS BYOD (brugertilmelding)	Antal IOS BYOD-enheder (brugertilmelding)
IoT	Antal IoT-enheder

APNS udløbsdatoer

Viser en oversigt over alle udløbsdatoer for APNS-certifikater for alle klienter.

Klient-ID	Klient-ID
Virksomhedens navn	Virksomhedens navn
Udløbsdato	Udløbsdato for Apple APNS-certifikatet
Info	Information om udløb

Kontakt

Yderligere spørgsmål? Du skal blot kontakte os under:

For generelle tekniske spørgsmål

support@apptec360.com

+41 61 511 3210

For spørgsmål relateret til installation af en virtuel appliance

consulting@apptec360.com

+41 61 511 3214

Ansvarsfraskrivelse