AppTec360 Enterprise Mobile Manager & ContentBox

Administrasjonshåndbok | Versjon 5.0 (202110)

Innholdsfortegnelse

- Avstengningsenhet
- Start enheten på nytt
- Alarm og tapsmodus | Deaktiver tapsmodus
- Slett enhet
- Tørk av enheten
- Enterprise Wipe | Fjern MDM
- Send melding
- TeamViewer fjernkontroll
- Send innmeldingsforespørsel

Android

- Rediger enhet
- Tøm passord
- Lås enhet
- Slett enhet
- Tørk av enheten
- Fjern MDM
- Send melding
- Transformer til COPE-modus
- Send innmeldingsforespørsel
- Overfør eldre enheter

Vinduer

- Rediger enhet
- Slett enhet
- Enterprise Wipe | Fjern MDM
- TeamViewer fjernkontroll
- Send innmeldingsforespørsel

Innholdsstyring

- Gruppefiler
- Filutforsker
- Revisjonsspor
- Søppel
- Ekstern lagring

Revisjonslogg

iOS-konfigurasjon

- Begrensninger og innstillinger
  - Svartelistede / hvitelistede apper
  - SysApp-begrensninger
  - App-VPN
  - App-innstillinger
- App Store for bedrifter
  - iTunes-apper
  - Internt
- Kioskmodus
  - Søknadstype
    - Pakke
    - URL
  - Innstillinger for kioskmodus

Android Enterprise – fullstendig administrert enhetskonfigurasjon

Generelt

- Oversikt over gruppeprofiler (kun på gruppenivå)
- Enhetsoversikt (kun på enhetsnivå)
- Konfigureringsrevisjon (kun på enhetsnivå)
- Enhetslogg (kun på enhetsnivå)
  - Kommandologg
  - Mulige kommandostatuser
- Enhetsinnstillinger
  - Klientkonfigurasjon
  - Bakgrunn

Asset Management (kun på enhetsnivå)

- Enhetsinfo
  - Wi-Fi
- Cellular
- Bluetooth

Sikkerhetsstyring

- Tyverisikring (kun på enhetsnivå)
  - GPS-informasjon (kun på enhetsnivå)
  - Tørk og lås (kun på enhetsnivå)
  - Melding (kun på enhetsnivå)

- Sikkerhetskonfigurasjon
  - Enhetens passord
  - AntiVirus
- End of Life (kun på enhetsnivå)
  - Tørk (kun på enhetsnivå)
- Begrensningsinnstillinger
  - Begrensninger
- Sertifikatforvaltning

Administrasjon av tilkoblinger

- Wifi
  - Sikkerhetstype
    - WEP
    - WPA/WPA2
    - 802.1x EAP
- VPN
  - VPN-type
    - VPN
    - VPN per app
- Begrensninger

PIM-administrasjon

- Gmail Exchange

App-administrasjon

- Enterprise App Manager
  - Installerte apper (kun på enhetsnivå)
  - Systemapper (kun på enhetsnivå)
  - Obligatoriske apper
  - Svart- og hvitelisting
  - AE System-apper
- Begrensninger og innstillinger
  - Innstillinger for appadministrasjon
- App Store for bedrifter
  - Internt
- Enterprise Play Store
  - AE Play Store
- Kioskmodus og lanseringsprogram

- Melding (kun på enhetsnivå)
- Sikkerhetskonfigurasjon
  - Passord
  - Kryptering
  - AntiVirus
- End of Life (kun på enhetsnivå)
  - Tørk (kun på enhetsnivå)
- Begrensningsinnstillinger
  - Begrensninger
  - AE Enhetseier

BYOD-container

- Android Enterprise
  - Android Enterprise
  - Gmail Exchange
  - AE System-apper
  - Containerpassord
- Samsung KNOX
  - Aktivering
  - Knox Passcode
  - Knox Security
  - Knox Exchange
  - Knox e-post
  - Knox-apper

Administrasjon av tilkoblinger

- Wifi
  - Sikkerhetstype
    - WEP
    - WPA/WPA2
    - 802.1x EAP
- VPN
- Begrensninger
- APN
- Bluetooth

PIM-administrasjon

- Utveksling

Generell oversikt

Introduksjon til AppTec360

AppTecs Enterprise-Mobile-Management-løsning gir mulighet til å administrere og konfigurere alle mobile enheter med den intuitive administrasjonskonsollen. I dette scenariet kan EMM-serveren enten kjøre i dine egne omgivelser, eller du kan bruke vår skybaserte løsning.

Selv når det gjelder sentral installasjon av bedriftsapplikasjoner på smarttelefoner, har du kommet til rett sted. Med Enterprise Mobile Manager kan du distribuere bedriftsapplikasjoner og dokumenter til enheter i løpet av sekunder, eller blokkere uønskede applikasjoner med hvit-/svartelisting.

Bruken av private enheter i bedrifter utgjør en ny utfordring når det gjelder sikring av smarttelefoner og nettbrett. På grunn av at de ansatte ønsker å bruke smarttelefonene sine i stadig større grad, må IT-administratorer beskytte et stort antall ulike typer enheter. Vi hjelper deg med å sikre alle enheter og de sensitive dataene som er lagret på dem, og administrerer dem fra en intuitiv konsoll.

Operativsystemer for enheter som støttes

AppTec360 tilbyr støtte for iOS-, Android- og Windows-enheter. Vær oppmerksom på at funksjonskapasiteten til de nevnte plattformene kan variere fra operativsystem til operativsystem.

- Apple iOS 11.0 eller nyere*
- Apple macOS 10.11 eller nyere
- Google Android 4.4 eller nyere** på nettskyversjonen
- Google Android 4.1 eller nyere** på OnPrem-versjonen
- MS Windows 10 eller nyere*** (stasjonær datamaskin, bærbar PC og nettbrett)

**Vær oppmerksom på at enheter med iOS 10 eller tidligere ikke kan registreres på grunn av drastiske endringer som Apple har gjort i registreringsprosessen.*

***Enheter kan kobles til og konfigureres selv om de bruker en versjon som ikke lenger støttes av produsenten. Vær oppmerksom på at det kan finnes funksjoner som krever en bestemt Android-versjon. I supporttilfeller følger vi produsentens offisielle support. Ved problemer eller feil som skyldes en utdatert versjon som ikke lenger støttes av produsenten, forbeholder vi oss retten til å kun tilby begrenset support.*

****Home-versjonen av Windows støttes ikke på grunn av begrensninger i operativsystemet. Vi anbefaler på det sterkeste at du bruker en OS-versjon som fortsatt støttes av produsenten. Ikke bare av kompatibilitetshensyn, men også av sikkerhetsgrunner. Derfor anbefaler vi iOS 12 eller nyere og Android 9 eller nyere.*

LDAP-kataloger som støttes

- Microsoft Active Directory
- Åpne LDAP

Oppdatert informasjon om "Operativsystemer som støttes" og "LDAP-kataloger som støttes" finner du her:

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

Forklaring av «Supervised-Mode» på Apple-enheter

Supervised-Mode representerer et utvidet grensesnitt for iOS-enheter.

På den respektive konfigurerte enheten kan det legges til ytterligere begrensninger som gjelder funksjonaliteten til sluttbrukerenheten. Disse finnes også i administrasjonshåndboken og er merket med et banner.

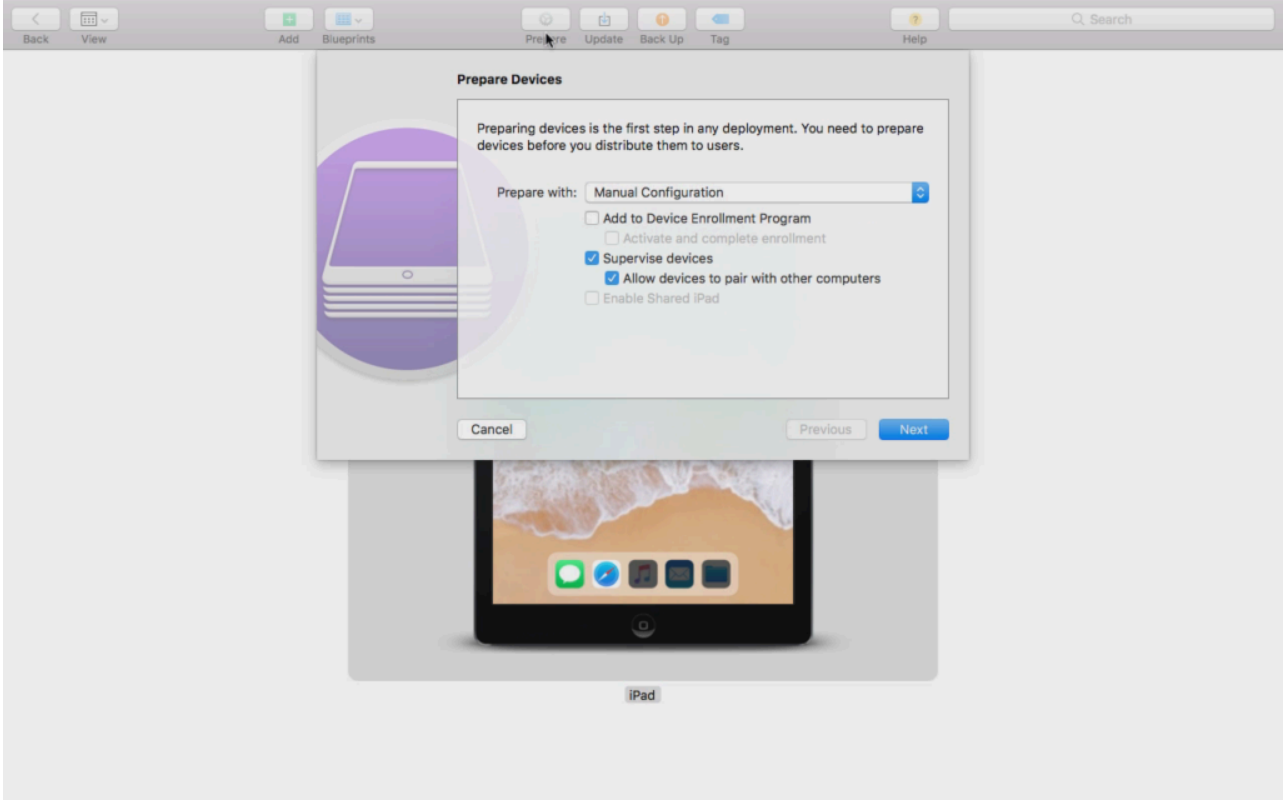
Tilgjengelig i overvåket modus

"Supervised-Mode" kan aktiveres med programmet "Apple Configurator". Apple Configurator kan angi standardinnstillingene på nye iOS-enheter som et konfigurasjonsverktøy (via USB-grensesnittet).

Verktøyet kan ikke bare installere konfigurasjonsprofiler, men også apper. Det er gratis, men krever en Mac-datamaskin.

Aktiver overvåket modus

1. Åpne Apple Configurator



2. Klikk på enheten og velg "Klargjør"
3. Velg "Manuell konfigurasjon" og "Overvåk enheter"
4. Klikk på "Neste"
5. (valgfritt) Nå kan du legge til en MDM-server der enheten skal registreres. Koblingen for dette finner du i "Generelle innstillinger - iOS-konfigurasjon - Konfigurator og URL" Velg din organisasjon eller opprett en ny
6. Velg din organisasjon eller opprett en ny
7. Velg hvilke trinn som skal hoppes over i det første oppsettet, og klikk på "Neste" (FORSIKTIG: Hvis du fortsetter, slettes enheten din!)

Nå settes enheten i overvåket modus. Dette kan ta noen minutter. Når det er gjort, starter enheten på nytt.

Nå er enheten din overvåket!

Legge til en enhet i DEP

Du kan også legge til enheter i DEP (Device Enrollment Program) ved hjelp av Apple Configurator, hvis enhetene dine bruker iOS 11 eller nyere.

Mer informasjon om DEP: https: //www.apple.com/business/dep/

Følg de samme trinnene som du ville gjort for å overvåke en enhet, og kryss i tillegg av for "Add to Device Enrollment Programm". Du vil bli bedt om å oppgi DEP-påloggingsdata hvis du aldri tidligere har logget deg på DEP med Apple Configurator.

Etter at prosessen er fullført, finner du enheten på DEP-serveren "Devices Added by Apple Configurator 2". Du kan nå bruke denne serveren og koble den til administrasjonskonsollen eller overføre enheten til en allerede eksisterende server.

Du har nå lagt til en enhet i DEP!

Forklaring av Android Enterprise

Hva er Android Enterprise?

Android Enterprise gir bedre kontroll over arbeidsenheter som administreres med MDM. Dette gjør at administratorer enten kan ha full kontroll over Android-enhetene sine eller skille bedriftsdata fra private data på containerenheter. I tillegg gjør Android Enterprise det enklere å registrere enheter og distribuere apper.

Hva er kravene for å bruke Android Enterprise?

Android Enterprise kan brukes gratis av alle. Du trenger bare å koble en Google-konto til MDM for å aktivere alle Android Enterprise-funksjonene. Mer om dette finner du i Android Enterprise-delen.

Android Enterprise kan brukes på enheter med Android 5.1 eller nyere, med unntak av Enhanced Work Profile (se nedenfor). Vi anbefaler minst Android 7 eller nyere for enklere registrering, eller Android 11 for å få tilgang til alle tilgjengelige funksjoner.

Hvilke moduser er tilgjengelige med Android Enterprise?

Det finnes tre ulike moduser som kan brukes når du bruker Android Enterprise.

AE Fullt administrert enhet (arbeidsadministrert): En fullstendig administrert enhet som kun brukes i jobbsammenheng. Dette gir administratoren full kontroll over enheten. Dette tillater ikke privat bruk av enheten. For å registrere enheter i denne modusen må enhetene tilbakestilles og registreres med en QR-kode (se AE Enrollment) eller registreres via Knox Enrollment eller Zero Touch.

AE BYOD-container: BYOD-containeren (bring your own device) gir brukerne tilgang til bedriftsdata på sin private telefon i en separat container. I denne modusen kan ikke private apper se bedriftsdata og -apper og omvendt. For å registrere enheter i denne modusen må AppTec-appen lastes ned, og en QR-kode kan skannes. Opprett en enhet i konsollen, og velg "AE Container (BYOD & Enahnced Work Profile)" som enhetstype. Klikk på QR-koden på den nyopprettede enheten for å hente QR-koden, og sett den første bryteren til "Legacy & BYOD".

AE Enhanced Work Profile: (krever Android 11 eller nyere) Mens den ovennevnte BYOD-containeren bringer bedriftsdata til en privat enhet, gjør Enhanced Work Profile det samme, men for en bedriftseid enhet. Den oppretter den samme containeren, men gir administratoren litt mer kontroll over enheten, slik at brukeren ikke bare kan fjerne MDM fra enheten. Opprett en enhet i konsollen, og velg "AE Container (BYOD & Enahnced Work Profile)" som enhetstype. Klikk på QR-koden på den nyopprettede enheten for å hente QR-koden, og sett den første bryteren til "Enhanced Work Profile". Denne QR-koden kan skannes etter at du har tilbakestilt enheten og trykket 6 ganger på skjermen som forklart i Metode 1 i AE-registrering.

Hvordan kan jeg tilordne apper til Android Enterprise-enheter?

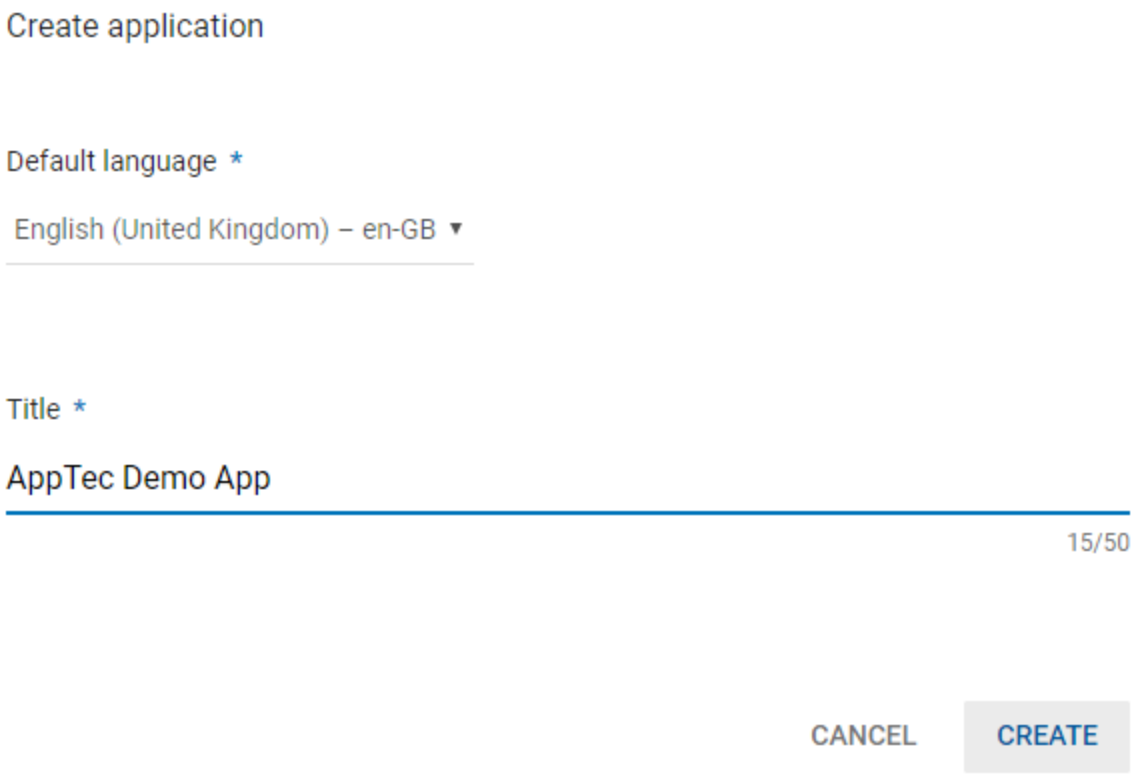
Først må du godkjenne appene du vil bruke i Generelle innstillinger → Appadministrasjon → AE Play Store → Play Store-apper. Når du har godkjent en app, kan du tilordne den til den obligatoriske applisten → i profilen din ved å klikke på "+" og velge appen fra "AE Play Store"-fanen. Appen lastes ned og installeres automatisk. Det kreves ingen Google-konto på enheten, og brukeren trenger ikke å bekrefte eller tillate dette.

Last opp dine egne apper til Google Play Store

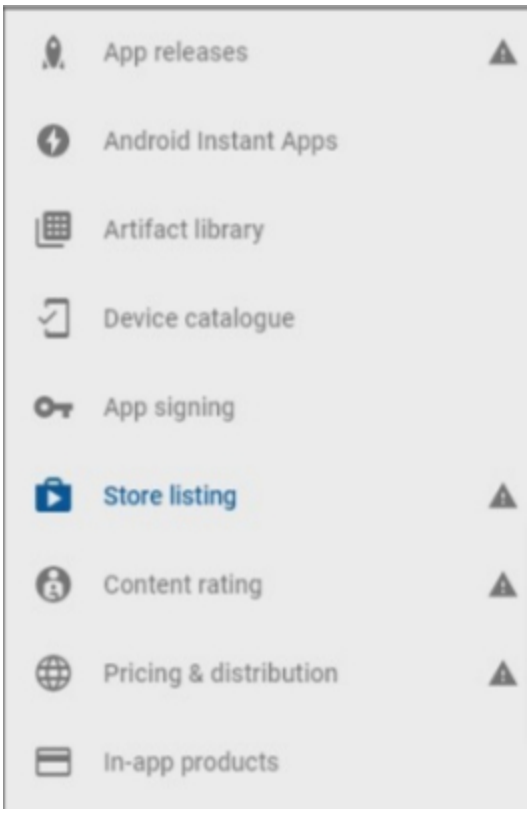
Det er mulig å laste opp egne apper til Google Play Store. På denne måten kan du dra nytte av forskjellige fordeler som oppdateringsmekanismen i Play Store.

For å gjøre dette trenger du en Google Developer-konto. Logg inn ved hjelp av Google Play Console(https://play.google.com/apps/publish)

Klikk på "Opprett applikasjon". Velg standardspråk og tittelen på appen.



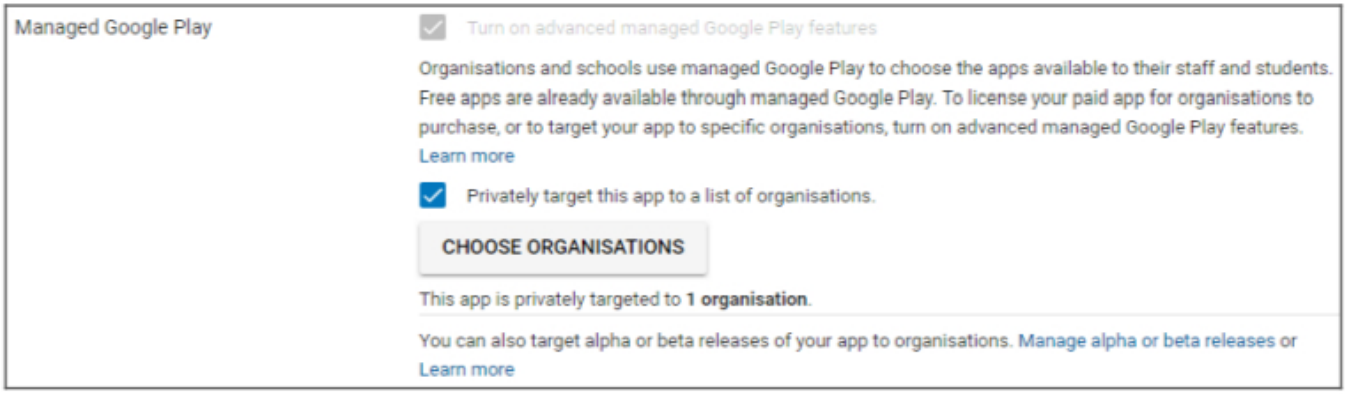
På den følgende siden blir du bedt om å oppgi forskjellige detaljer om appen din.



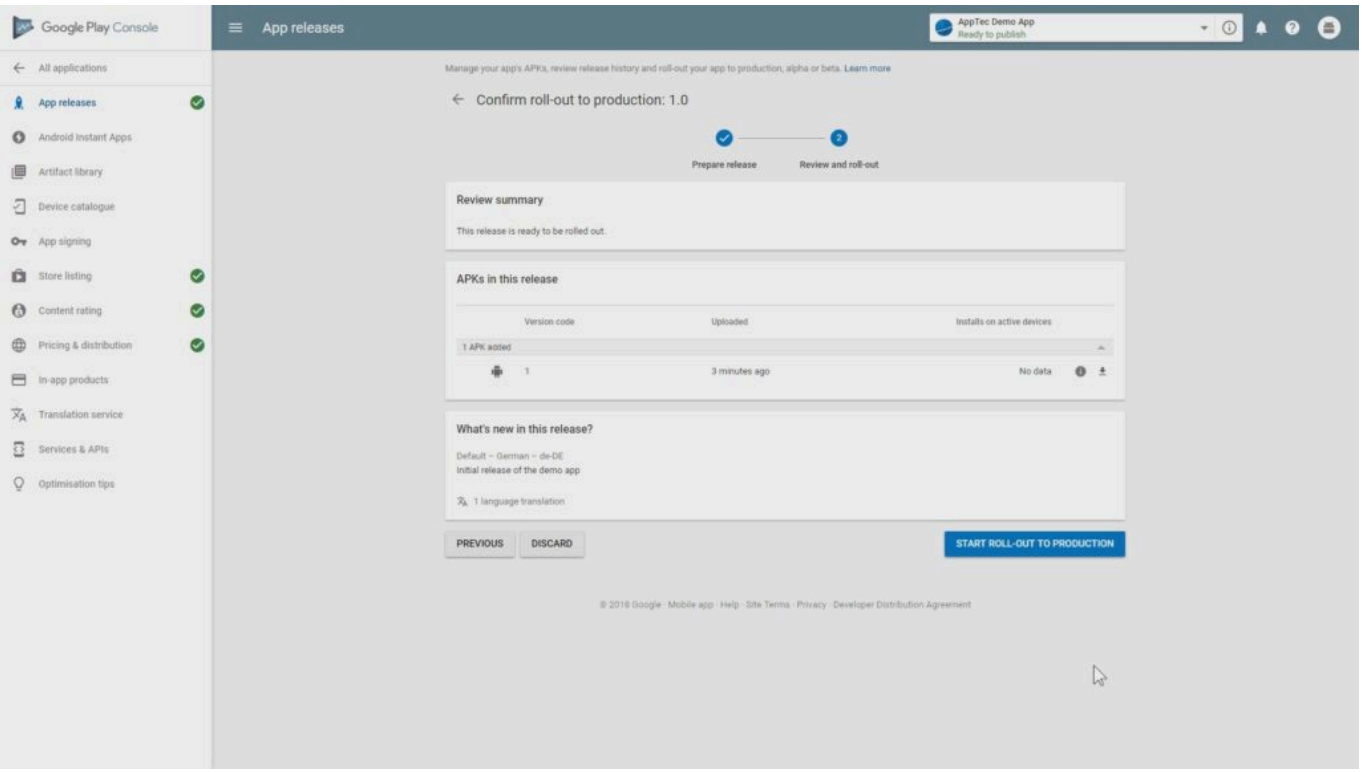
Etter at du har lagt inn alle opplysningene, vil du se forskjellige hint-symboler på venstre side.

Hold musepekeren over dem for å se hvilke trinn som er igjen, og følg disse i den rekkefølgen du ønsker.

Merk: Sørg for å merke av i de to avmerkingsboksene ved "Managed Google Play" under "Pricing & Distribution". Ellers vil appen være offentlig og tilgjengelig for alle. Sørg også for å velge land for distribusjon.



Når du har fullført alle trinnene, kan du gå til "Apputgivelser". Klikk på "Review" og "Start Roll-Out to Production" for å ferdigstille utkastet og publisere appen.



Det kan ta litt tid før appen er tilgjengelig i Play Store. Når prosessen er ferdig, kan du søke etter appen din i Play for Work-butikken og godkjenne den. Deretter kan du tilordne appen til enheter ved hjelp av EMM-konsollen, akkurat som du gjør med andre apper.

Krav og installasjon

Krav

Systemkrav

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

*Merk: Maskinen må opprettes med Generation 1 når du bruker Hyper-V.

Den virtuelle disken har en målstørrelse på 20 GB, og maskinen krever 4 GB RAM.

Apparatet er basert på Debian 9 64bit

Oppgrader den importerte maskinen til den nyeste kompatibiliteten (f.eks. i VMWare), og sørg for at maskinens OS-type er riktig innstilt i hypervisoren.

Lisensnøkkel

For å kunne aktivere og installere serveren, trenger du en gyldig lisensfil. Du kan få en slik fra AppTec360 direkte og/eller fra din respektive forhandler.

IP-adresse og DNS-oppløsning

AppTec360-apparatet må kunne nås av enheten ved hjelp av vertsnavnet som lisensen er utstedt for.

For å registrere Windows 10-enheter må du også sette opp et ekstra underdomene i form av "enterpriseenrollment.", som peker til apparatet.

SSL-sertifikat

Ettersom alle tilkoblinger til og fra enhetene må sikres ved hjelp av SSL, trenger du et gyldig sertifikat for vertsnavnet utstedt av en sertifikatmyndighet som enheten har tillit til. Den private nøkkelen for sertifikatet må lastes opp uten passordbeskyttelse. I de fleste tilfeller kreves det et mellomliggende sertifikat for sertifiseringsinstansen for at enhetene skal gjenkjenne serversertifikatet.

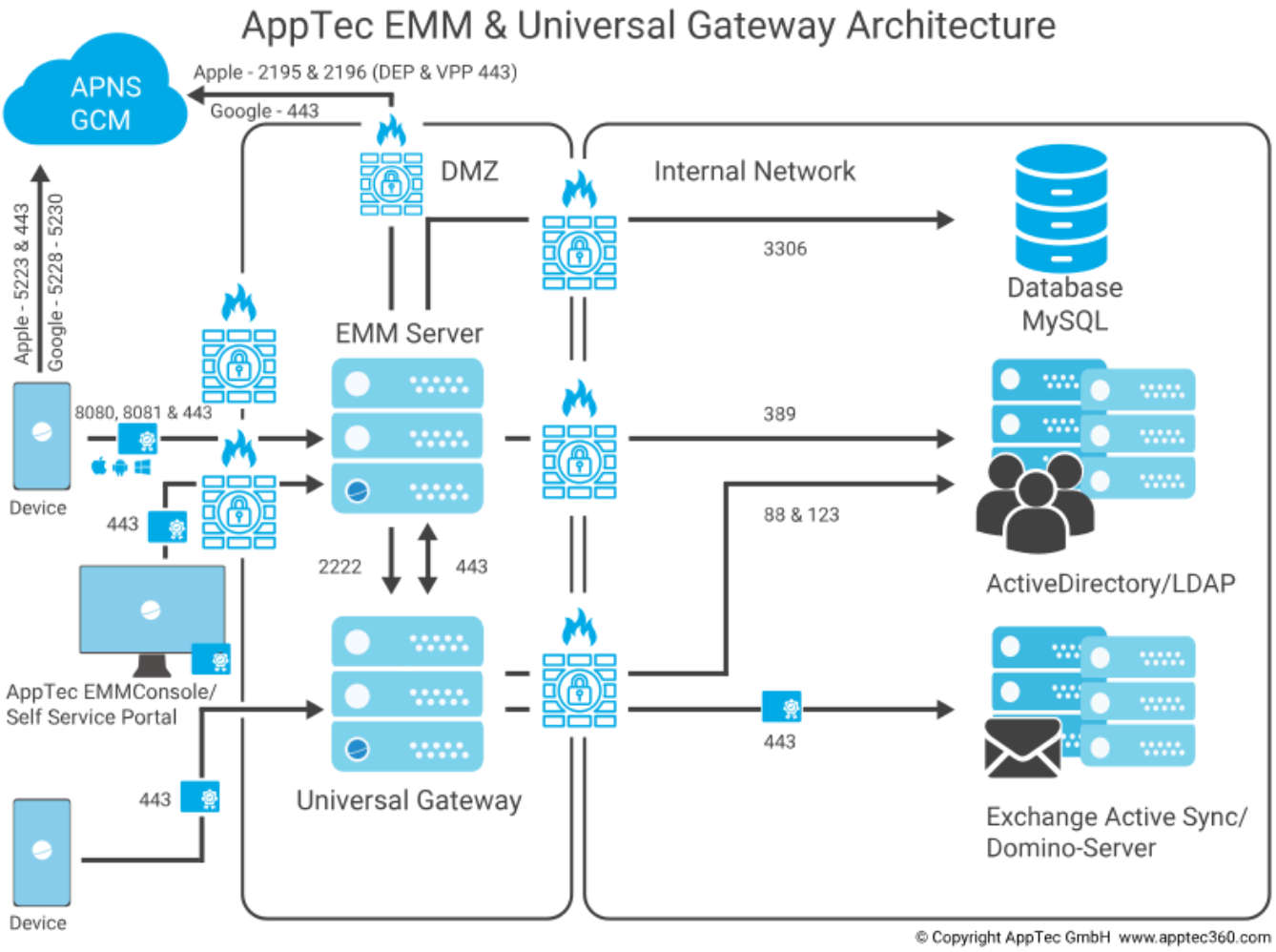
Windows 10-enheter vil kreve et spesifikt sertifikat for underdomenet enterpriseenrollment.

Fra og med apparatversjon 202104 kan du også bruke Let's Encrypt-sertifikater, som genereres automatisk (beskrevet i Trinn to - SSL-sertifikat).

SMTP-server

En e-postserver og/eller et e-postrelé er påkrevd for at AppTec360 EMM skal kunne sende e-post (f.eks. for enhetsregistrering og kontovalidering).

Brannmurregler



Dette diagrammet viser hvilken tilkobling som er nødvendig avhengig av hvilke tjenester du vil bruke.

For en mer detaljert beskrivelse, se tabellen på neste side.

Alle (eksterne/enheter)	→	**AppTec360 Appliance / emmconsole.com**
Porter	443	Administrasjon, Enterprise AppStore og Windows Phone-kommunikasjon
	8080	Android- og iOS-kommunikasjon
	80	Første gangs oppsett av Let´s Encrypt. Bruker 443 etterpå.
Alle (enheter)	→	**Alle (eksterne)**
Porter	5223, 443	Apple Push Service, må kunne nås uten proxy, 443 som fallback, se https://support.apple.com/en-us/HT203609
	5228-5230	Android Push Service (FCM), må kunne nås uten proxy
AppTec360 Apparat	→	**Domenekontroller**
Porter	389, (LDAPS 636)	Brukersynkronisering med LDAP
AppTec360 Apparat	→	**Alle**
Havn	443	Brukes for Android Push Service (GCM) Søk i AppStore / Play Store
AppTec360 Apparat	→	**emmconsole.com**
Porter	443	AppTec360 Appliance-oppdateringer, generering av APNS-sertifikater
AppTec360 Apparat	→	**Apple-nettverk (17.0.0.0.0/8)**
Porter	2195, 2196	Apples push-tjeneste og tilbakemeldingstjeneste
	443	DEP OG VPP

Sikkerhetsoppdateringer

Debian-operativsystemet bør oppdateres regelmessig for å få de nyeste sikkerhetsoppdateringene. Pass imidlertid på at du ikke oppgraderer til en nyere hovedversjon av Debian manuelt. Når AppTec360 EMM er kompatibel med en nyere hovedversjon, vil vi legge til en måte å oppgradere på i en appliance-oppdatering.

Standardpassord for den virtuelle enheten

Innloggingsbruker (rotinnlogging er deaktivert. Bruk "sudo" for administrasjonsoppgaver)

apptec

Innlogging Passord

apptec

MySQL Root-bruker

rot

MySQL Root-passord

apptec

MySQL Standardbruker

AppTec

MySQL Standard brukerpassord

AppTec

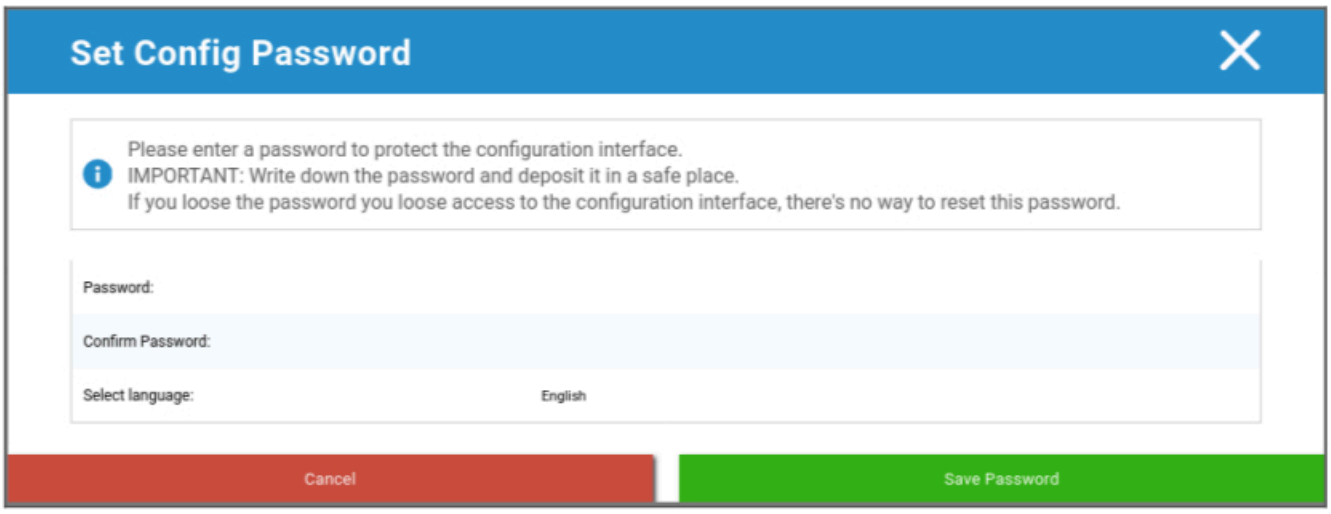
Konfigurasjon av det virtuelle apparatet

Viktig: Før du begynner å konfigurere Virtual Appliance, må skjermoppløsningen være satt til minst 1280 x 800 piksler.

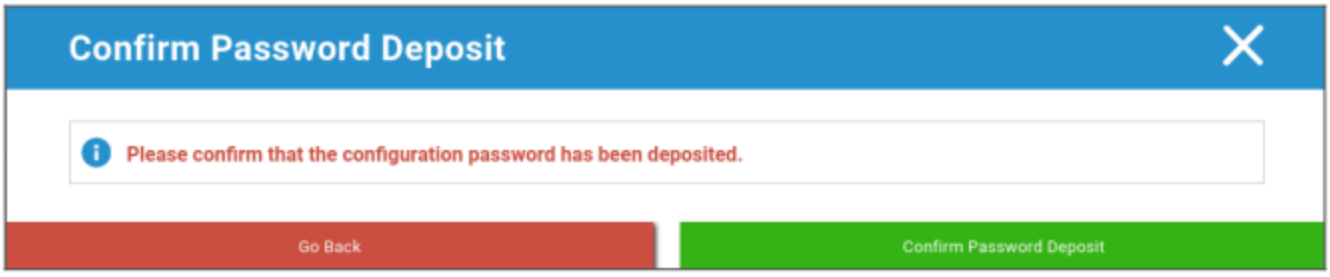
Etter at du har logget deg inn på apparatet, bør Firefox starte automatisk og vise konfigurasjonsgrensesnittet.

Forberedelse

Først må du oppgi et passord for konfigurasjonsgrensesnittet. Dette passordet brukes til å kryptere all informasjon og alle filer som legges inn i konfigurasjonsgrensesnittet. Her kan du også angi hvilket språk grensesnittet skal vises på (kan endres senere).

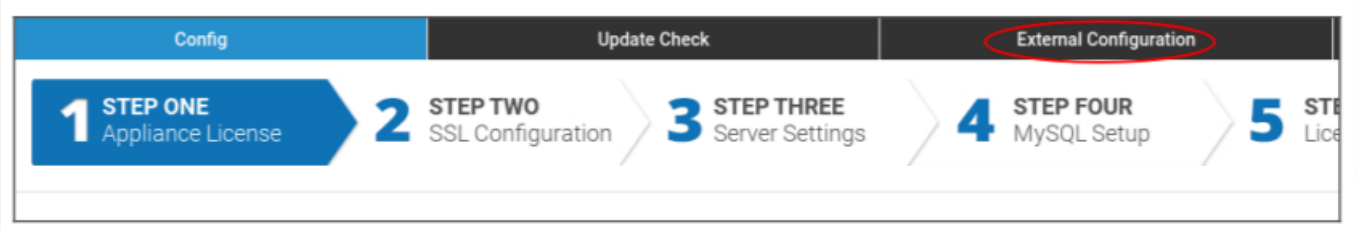


Passordet kan bare tilbakestilles av AppTec360 Support, så sørg for at du oppbevarer det på et trygt sted og bekrefter den kommende popupen.



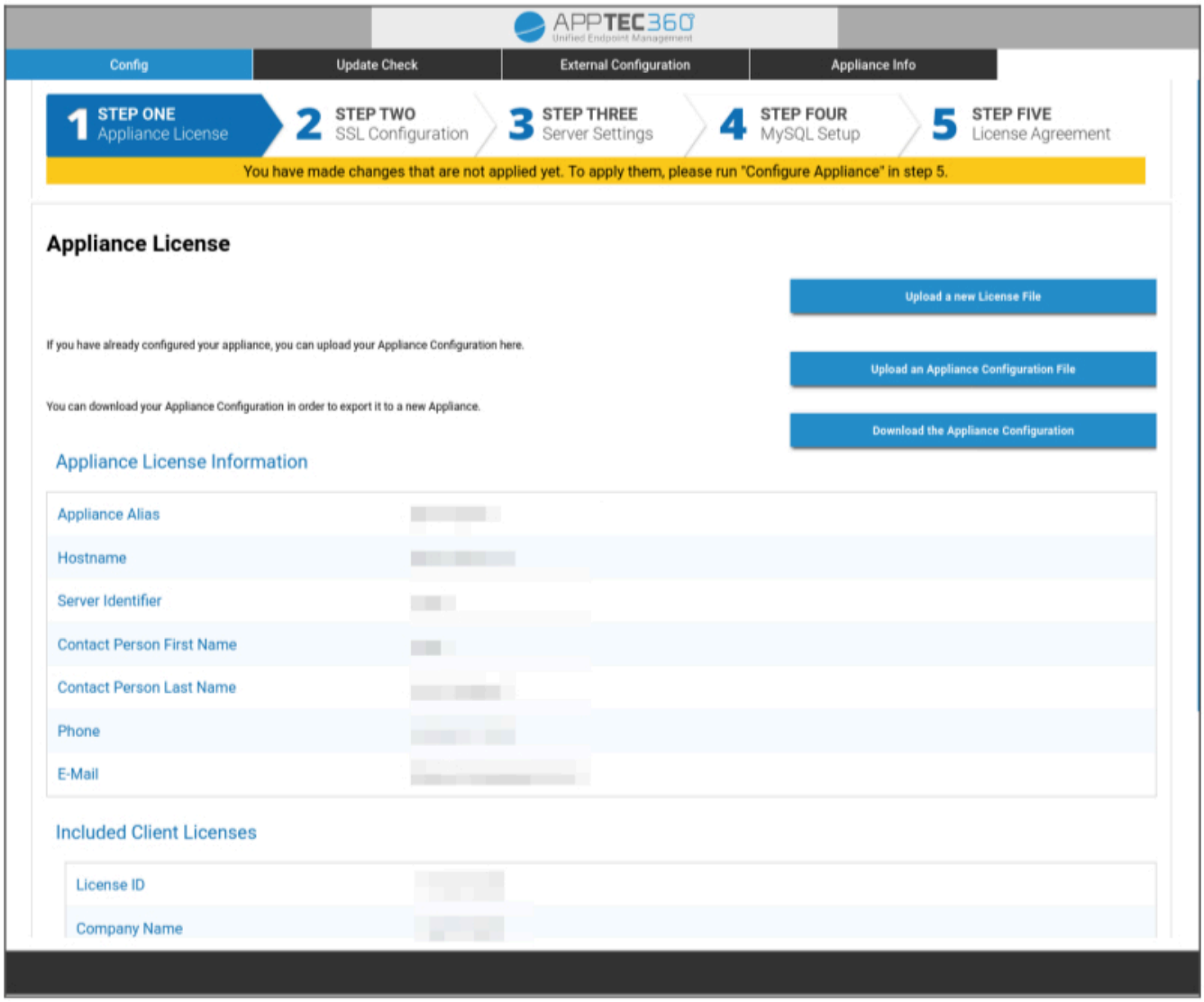
Konfigurer fra ekstern vert

For å forenkle installasjonsprosessen kan du gjøre konfigurasjonssiden tilgjengelig fra en ekstern vert. Dette gjør du ved å følge trinnene i "Konfigurer fra ekstern vert".



Trinn én – lisens for apparatet

1. Vennligst last opp lisensfilen som du har mottatt fra AppTec.
2. Hvis lisensfilen er lastet opp, kan du se lisensinformasjonen for apparatet som i skjermbildet nedenfor.



Trinn to – SSL-sertifikat

Du kan enten bruke den automatiske sertifikatoppsettet ved hjelp av Let's Encrypt, eller du kan levere sertifikatene selv (se SSL-sertifikat for mer informasjon).

Automatisk

Sertifikatet genereres automatisk ved hjelp av Let's Encrypt-tjenesten.

AppTec360 EMM bruker HTTP-01-utfordringen for validering av domenet, noe som betyr at HTTP-porten må være åpen fra Internett for den første forespørselen om et sertifikat. Etterfølgende fornyelsesforespørsler kan valideres via HTTPS.

Bytt alternativknappene til "Automatic (Let's Encrypt)" og trykk på "SAVE VALUES". Sertifikatet vil automatisk bli forespurt når du bruker konfigurasjonen i trinn fem - Lisensavtale. Sertifikatet fornyes automatisk om nødvendig, og du vil motta en e-post hvis sertifikatet er i ferd med å utløpe (noe som innebærer at fornyelsen kan ha mislyktes).

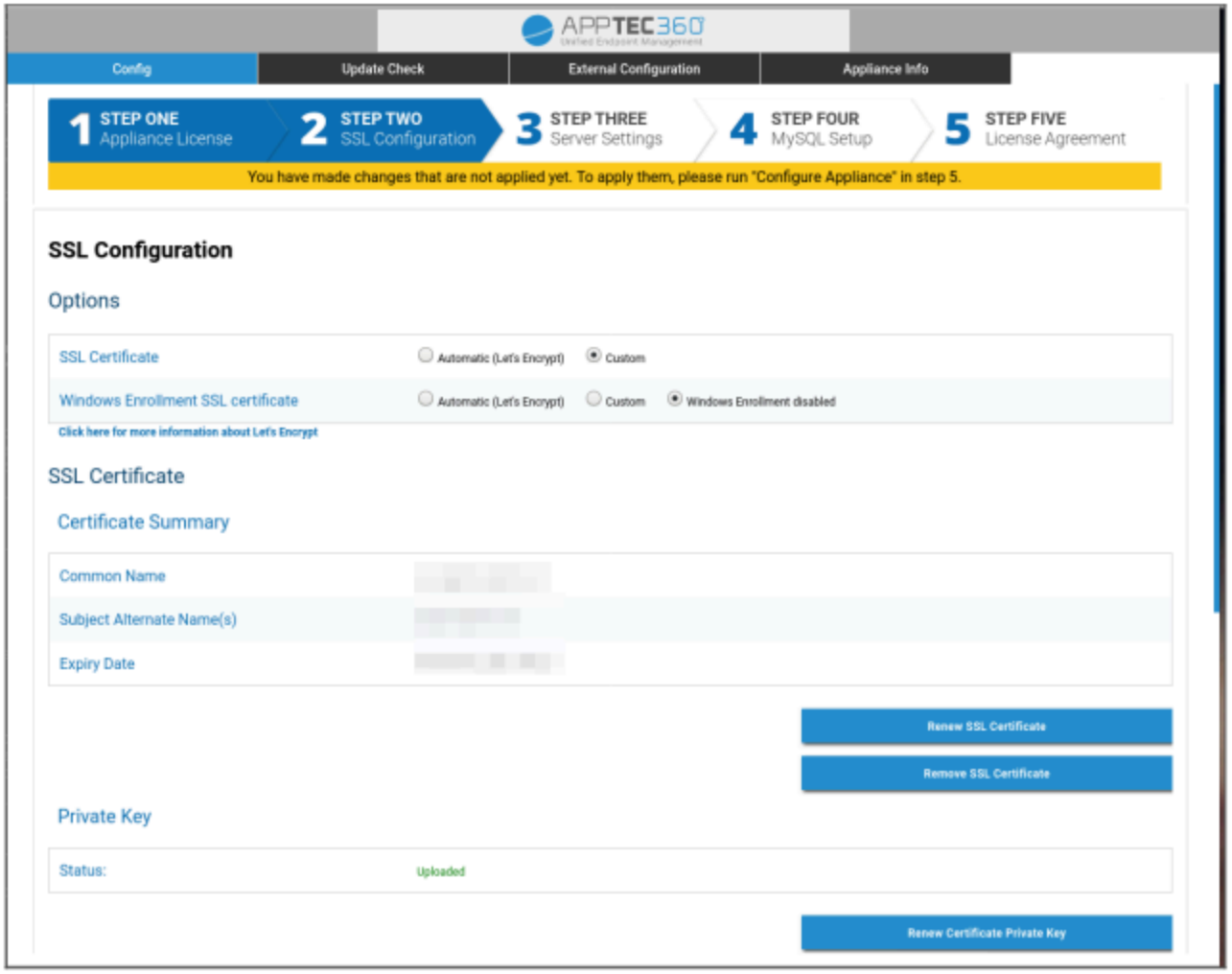
Tilpasset

1. Last opp SSL-sertifikatet for ditt lisensierte vertsnavn. Du kan se vertsnavnet i Trinn én - Lisens for apparatet.

2. Last også opp den private nøkkelen for sertifikatet og om nødvendig det mellomliggende sertifikatet.

Viktig: Nøkkelen må ikke være passordbeskyttet. Hvis den er det, må du fjerne passordet før du laster den opp.

Tips: Hvis du også vil bruke Windows 10-enheter, må du aktivere "Windows Enrollment SSL certificate" og laste opp sertifikatet, den private nøkkelen og det mellomliggende sertifikatet for underdomenet ditt (beskrevet i IP-adresse og DNS-oppløsning) nederst på siden.



Trinn tre – Serverinnstillinger

1. Vennligst skriv inn en global e-postadresse for kundestøtte. Denne adressen vil bli brukt i e-poster til brukerne dine, slik at de vet hvem de skal kontakte hvis det oppstår problemer med enheten deres.
2. Angi e-postinnstillinger som skal brukes av systemet til å sende e-post. Innstillingene vil bli brukt til å sende e-post til brukeren og også til å sende feilrapporter og funksjonsforespørsler til"support@apptec360.com".Etter at du har lagret e-postinnstillingene, må du bekrefte dem ved å klikke på "Test e-postkonfigurasjon" og følge instruksjonene.

Trinn fire – MySQL-oppsett

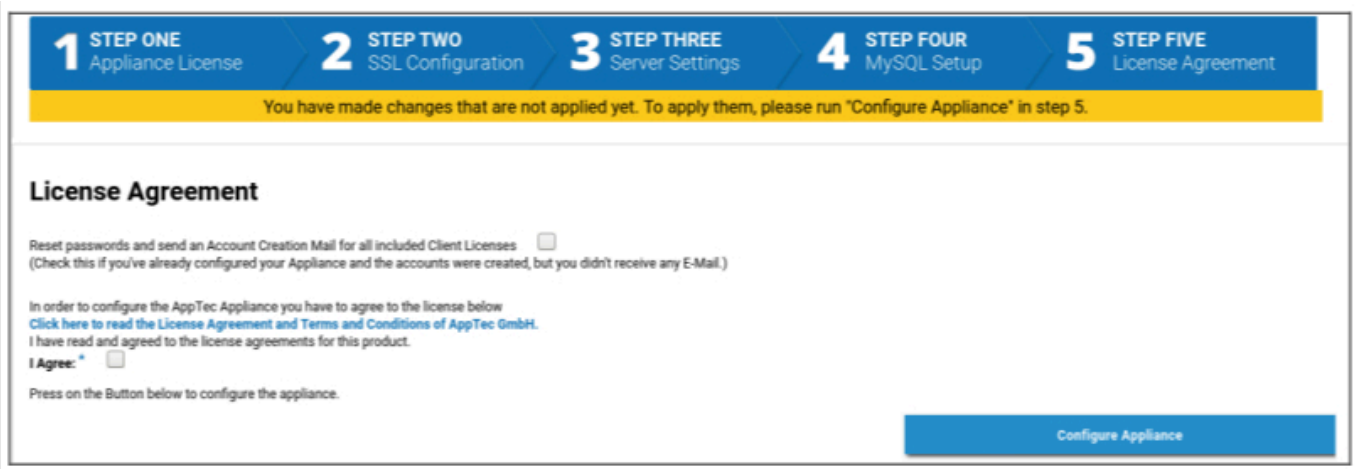
1. Hvis du vil bruke den interne databasen, kan du hoppe over dette trinnet. Hvis ikke kan du angi tilkoblingsinformasjonen for den eksterne databaseserveren.


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)

Trinn fem – Lisensavtale

1. Vennligst les lisensavtalen.
2. Kryss av for "I Agree" og trykk på "Configure Appliance"-knappen for å bruke innstillingene.

Tips: Du må kjøre "Configure Appliance" hver gang du endrer innstillingene i de fem trinnene for å bruke innstillingene.



Gratulerer!

Du er ferdig med konfigurasjonen av det virtuelle apparatet.

En e-post med passordet ditt ble sendt til adressen du har oppgitt for lisensen (synlig under "Inkluderte klientlisenser" i Trinn 1 - Lisens for apparatet).

Du kan nå logge inn på konsollen ved hjelp av dette passordet og e-postadressen du har mottatt det på.

For å logge inn på konsollen skriver du inn vertsnavnet til konsollen i adressefeltet i nettleseren din.

Du finner vertsnavnet til apparatet ditt i Trinn én - Lisens for apparatet.

Feilsøking

1. Du mottok ikke en e-post da du konfigurerte apparatet i trinn fem - Lisensavtale:

Kontroller at e-postinnstillingene i Trinn tre - Serverinnstillinger er riktige. Hvis du vil sende passordet på nytt, merker du av for "Tilbakestill passord og send en e-post om kontoopprettelse for alle inkluderte klientlisenser" i Trinn fem - Lisensavtale før du kjører "Konfigurer apparat" på nytt.

2. Du har fått en feil i forbindelse med Let's Encrypt under konfigurasjonen i trinn fem - Lisensavtale:

Kontroller at apparatet kan nås via domenenavnet på port 80. Let's encrypt skriver også en logg til "/var/log/letsencrypt", noe som kan hjelpe deg med videre feilsøking.

Sikkerhetsanbefalinger

Det anbefales å utføre følgende trinn for å sikre AppTec360-apparatet ditt.

Dette er ikke en fullstendig bruksanvisning, men bare en anbefaling for en grunnleggende konfigurasjon.

- Endre passordet for AppTec360-brukeren
- Endre passordet for MySQL-brukerne "root" og "AppTec", og oppdater Trinn fire - MySQL-oppsett tilsvarende
- Endre standard SSH-serverport
- Blokker port 80 i konsollen og ikke tillat innkommende HTTP-trafikk, bruk kun HTTPS. Når du har konfigurert, er det også mulig med ekstern konfigurasjon via HTTPS.
- Begrens tilgangen til administrasjonsgrensesnittet til kun visse IP-adresser nederst i Trinn tre - Serverinnstillinger
- Konfigurer brannmuren

Generelle innstillinger

Kontooversikt

Kontoinformasjon

Oversikt

Her kan du se en oversikt over AppTec360-kontoen din.

Selskapets navn	Ditt firmanavn
Opprettelsesdato	Dato for opprettelse av kontoen din
Lisens type	Betalt = betalt lisens Gratis = ubetalt lisens Merk: Kontoer på en OnPremise Appliance vil av tekniske årsaker alltid vises som betalt
Klientidentifikator	Identifikator for kontoen din (dette er IKKE kundenummeret ditt)
Lisensens utløpsdato	Utløpsdato for din AppTec360-lisens
ContentBox-lisens	Gratis = gratis lisens for 25 enheter Betalt = betalt lisens for x enheter
Launcher	Viser om du kan bruke den egendefinerte startprogrammet for Android eller ikke
Enheter	Antall lisenser i bruk / totalt antall lisenser
Kontaktperson	Oppgitt kontaktperson
Telefon	Oppgitt telefonnummer
E-post*	Oppgitt e-postadresse
Rotbruker	Root-brukere som kan logge inn
Programvareversjon	Nåværende programvareversjon

**Merk: E-postadressen som vises her, er den du oppga for å registrere kontoen. Basert på denne blir det opprettet en bruker i bruker-/enhetstreet som kan endres. Hvis du redigerer denne brukeren, endres e-postadressen du må bruke for å logge inn, men ikke informasjonen i kontooversikten.* .

Feilrapport

En feilrapport kan sendes direkte til kundestøtte for å rapportere problemer eller feil, og inneholder informasjon og logger om kontoen og oppsettet ditt.

Emne	Emnet for feilrapporten. Ta med et saksnummer hvis du vil legge til dette i en eksisterende supportsak.
Forventet atferd	Beskriv i detalj hva du gjorde og hva du forventet skulle skje
Faktisk atferd	Beskriv i detalj hva som skjer. Vennligst siter feilmeldinger NØYAKTIG. Det hjelper også hvis du legger til skjermbilder i vedlegget.
Når opplevde du problemet?	Vennligst oppgi et nøyaktig tidspunkt for når du fikk en spesifikk feilmelding/et spesifikt problem. I beste fall inkluderer du også sekunder, f.eks. 18:55:27
Kan problemet replikeres? Hvis ja, hvordan (i detalj)?	Beskriv i detalj hvordan du kan reprodusere problemet.
Har denne funksjonen tidligere fungert som forventet? Hvis ja, inntil når?	La det stå tomt hvis du ikke vet.
Ble det gjort noen spesifikke endringer i systemet før dette problemet oppstod? Hvis ja, hvilke endringer (i detalj)?	Nevn alltid hva den siste endringen eller handlingen din var før problemet dukket opp, selv om du mener det er irrelevant.
Hvis det er aktuelt: Hvilke enhetsmodeller og OS-versjoner er berørt?	Oppgi alltid den nøyaktige OS-versjonen (f.eks. iOS 14.7.1 eller Android 11)
Hvis det er aktuelt: Hva er den offentlige IP-adressen og/eller serienummeret til enheten?	Navngi minst én, selv om alle enhetene er berørt.
Inkluder loggfiler	Merk av for å sende loggfilen sammen med feilrapporten. Dette anbefales å gjøre.
Hent gjeldende VPP-status fra Apple og inkluder i feilrapporten	Inkluderer informasjon om VPP-lisenstildelinger. Aktiver denne bare hvis du blir bedt om det av kundestøtte eller hvis problemet ditt handler om VPP.
Vedlegg	Legg ved filer som kan være nyttige (f.eks. skjermbilder av en feilmelding)

Forespørsel om funksjonalitet

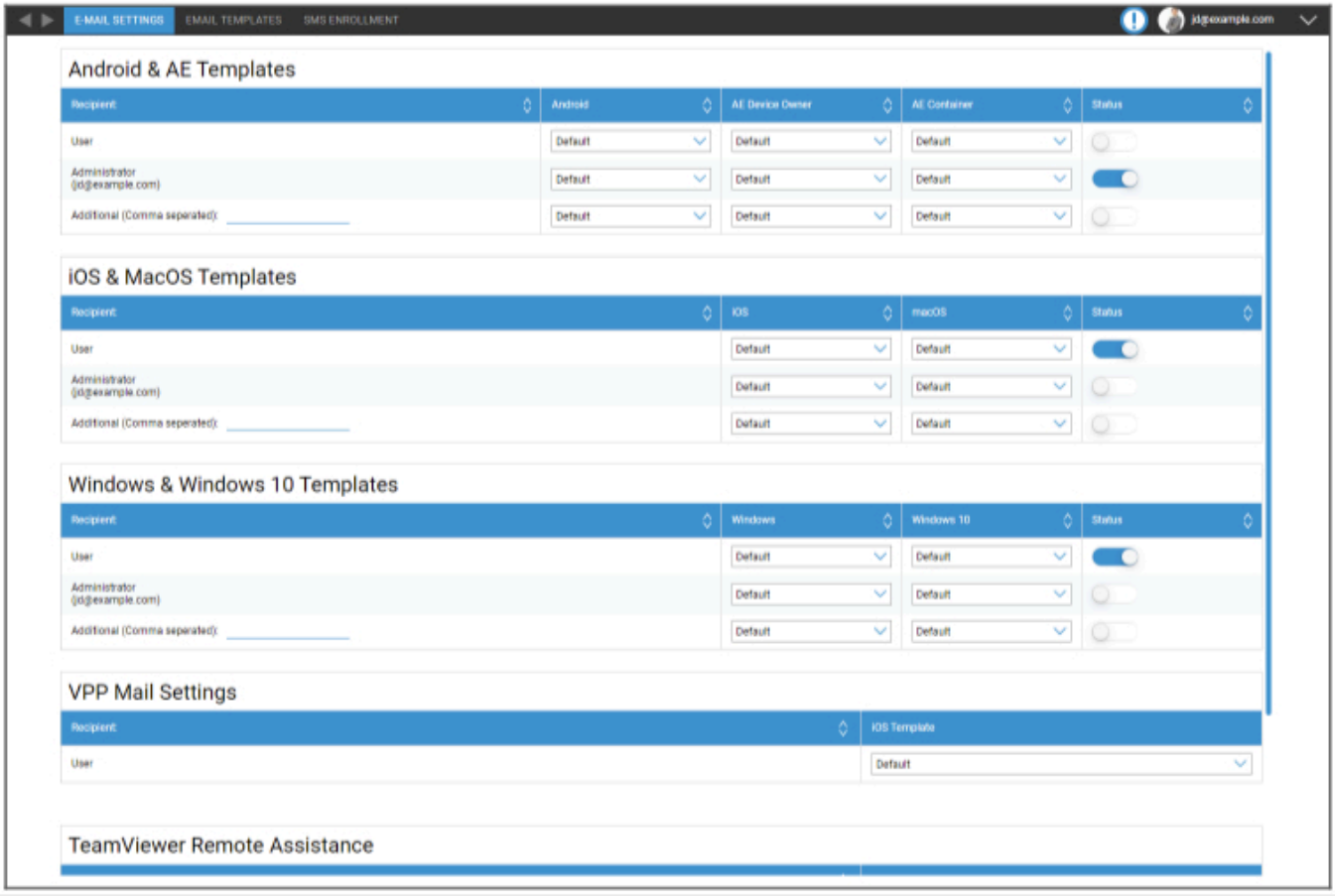
En funksjonsforespørsel kan sendes direkte til kundestøtte. Denne kan inneholde en forespørsel om en spesifikk funksjon eller en forbedring for

Sammendrag	Et kort sammendrag av problemet ditt
Beskrivelse	En detaljert beskrivelse av problemet ditt, vær så spesifikk som mulig
Vedlegg	Legg ved filer til feilrapporten

Global konfigurasjon

E-postinnstillinger

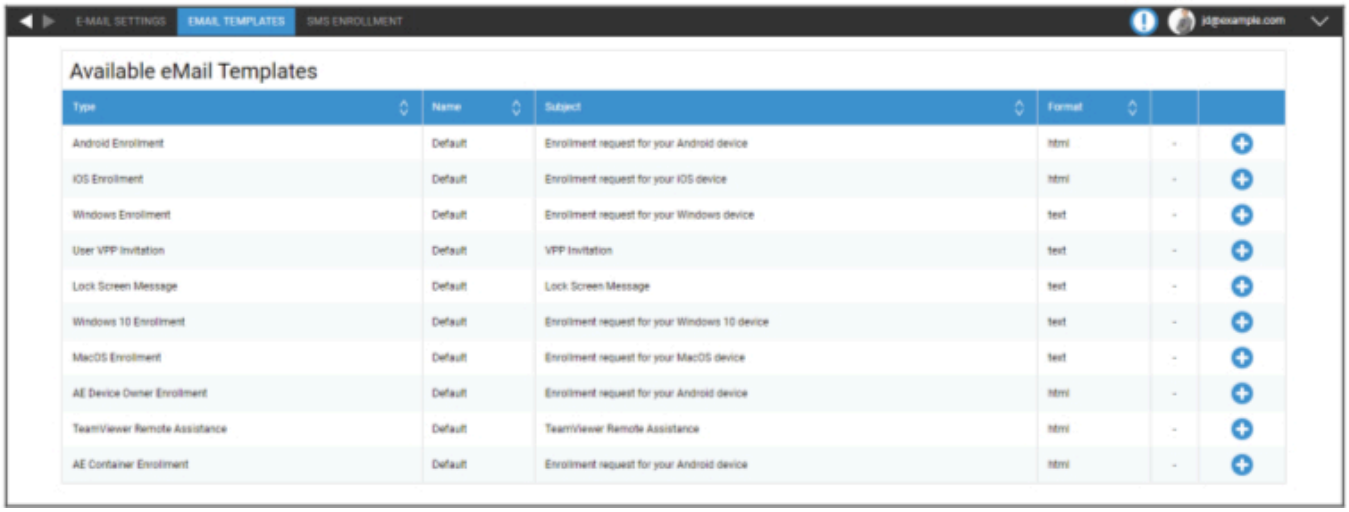
Her kan du definere hvem som får en e-post når det genereres en påmeldingsforespørsel, og hvilken tekstmal som skal brukes for denne e-posten.



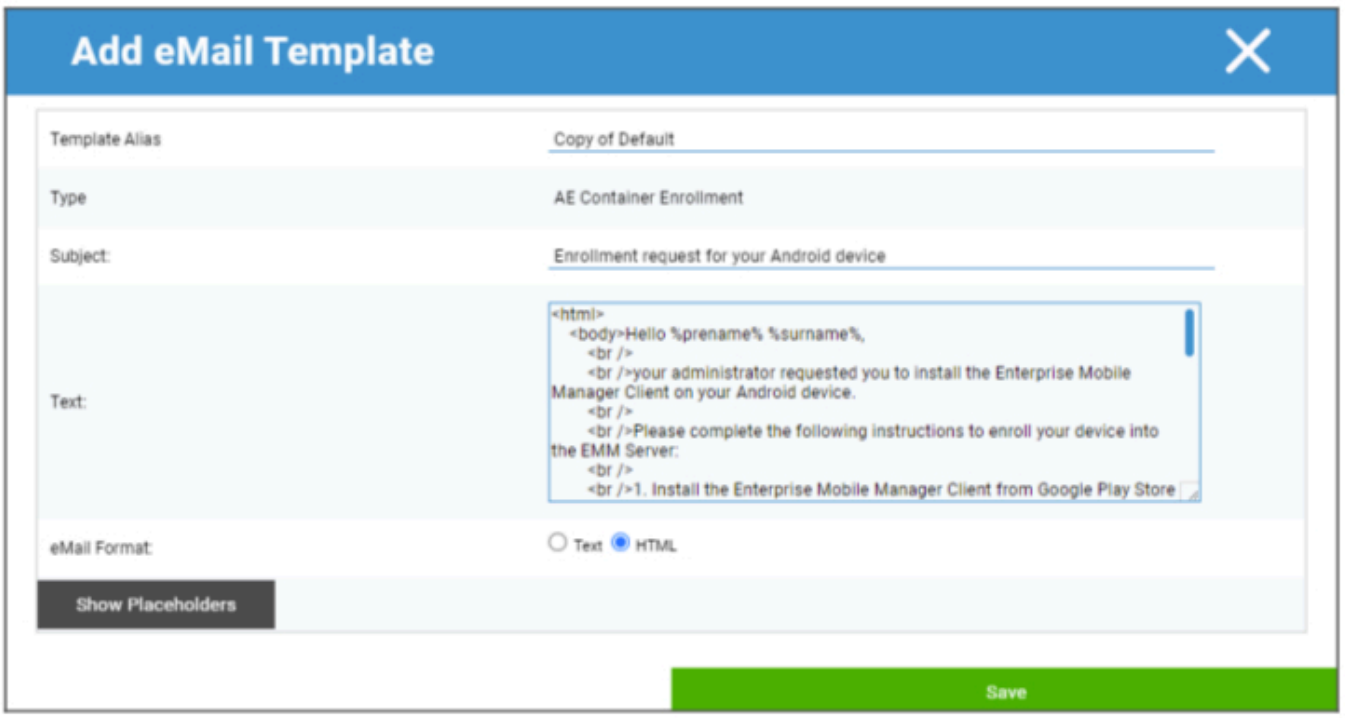
E-postmaler

Her kan du generere og redigere maler for ulike scenarier. Disse kan være i vanlig tekstform eller i HTML. Med HTML kan du bedre kontrollere formateringen av teksten.

Standardmalene kan ikke redigeres eller slettes.



Du kan også bruke plassholdere som variabler som automatisk blir erstattet. Klikk på "Vis plassholdere" mens du redigerer for å se tilgjengelige plassholdere. Forskjellige kategorier har forskjellige plassholdere.



SMS-registrering

Her kan du deaktivere/aktivere SMS-registreringsprosessen.

(Standard: deaktivert)

Du vil også se et display som angir hvor mange SMS-kreditter som fortsatt er tilgjengelige.

SMS-kreditter må kjøpes separat.

Personvern

GPS-tilgang

Her kan du beskytte GPS-visningen for hver enhet med 1 eller 2 passord (fire øyne-prinsippet). Du blir bedt om å oppgi passord hver gang du prøver å få tilgang til posisjonen til en enhet.

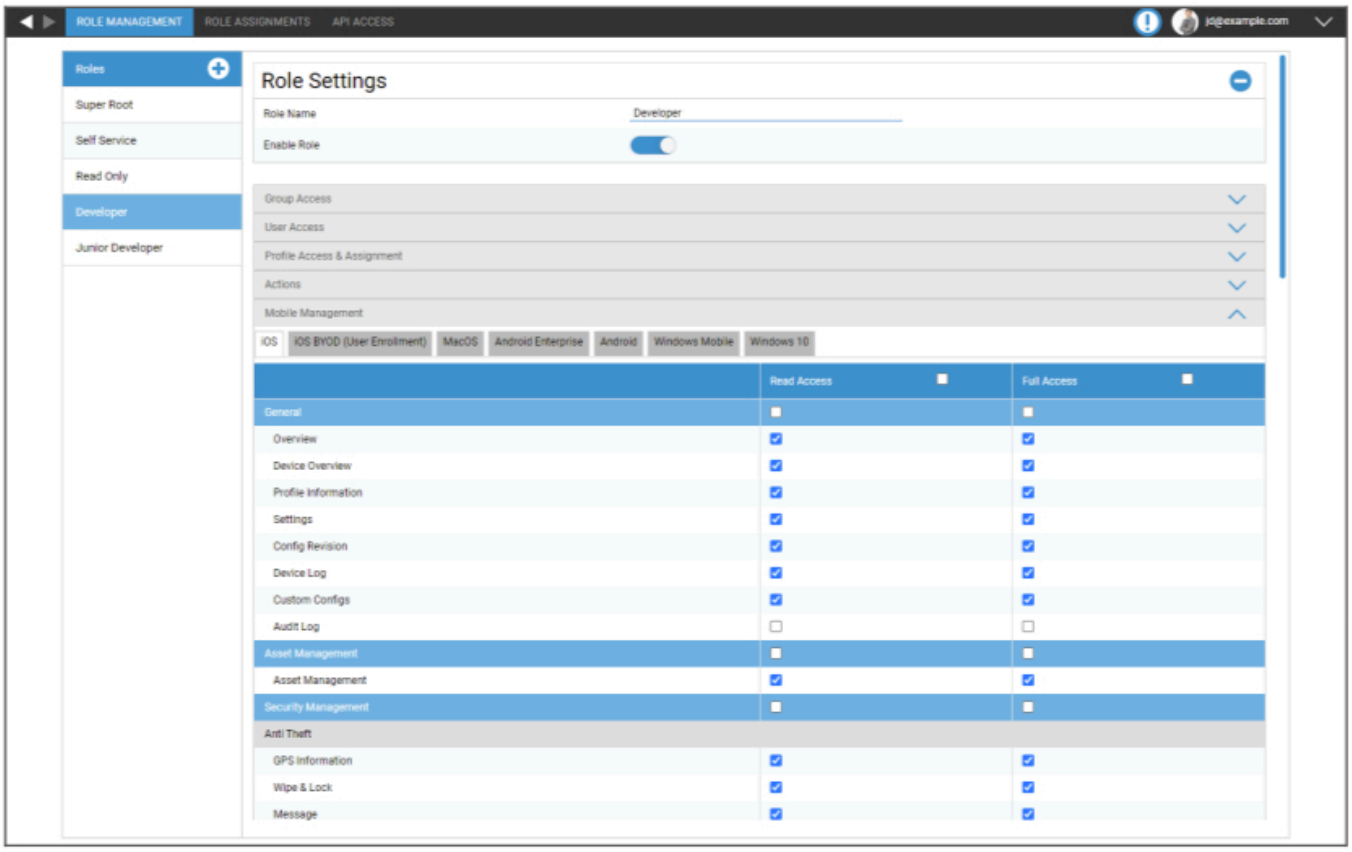
Begrens tilgang til GPS-innstillinger	Av = funksjonen er slått av, og det kreves ikke passord for lokalisering
	On = funksjonen er slått på, og det kreves passord for lokalisering
Beskyttelsesmetode	Bruk ett passord = bruk ett passord for lokalisering
	Bruk to passord = bruk to passord for lokalisering
Skriv inn passord (1)	Skriv inn valgt passord
Gjenta passord (1)	Skriv inn valgt passord på nytt
valgfritt: Skriv inn passord 2	Skriv inn det andre valgte passordet
valgfritt: Gjenta passord 2	Skriv inn det andre valgte passordet på nytt

Merk: Etter at du har angitt passordet/passordene, må du taste det/dem inn én gang til før det er helt aktivert.

Rollebasert tilgang

Rollehåndtering

Rollene definerer hva en bruker kan se og gjøre når han eller hun logger seg på administrasjonskonsollen. Dette gjør det mulig å opprette brukere som kan logge inn, men som har begrenset funksjonalitet.



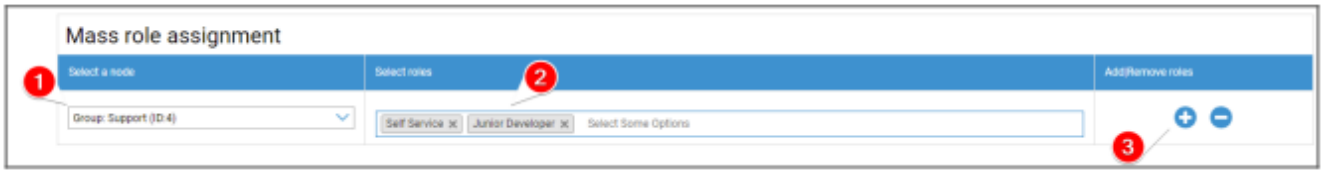
Superrotrollen er en standardrolle som alltid kan se og endre alt. Den kan ikke endres eller slettes. Selvbetjeningsrollen kan bare se sine egne brukere og enheter. Du kan kombinere Self Service og en egendefinert rolle for f.eks. å gi brukere mulighet til å logge inn og registrere enheter på egen hånd og bare for sin egen bruker.

Egendefinerte roller kan aktiveres eller deaktiveres manuelt. Nye roller er deaktivert som standard. Brukere med en deaktivert rolle fungerer som om de ikke har rollen. Dette gjør at du f.eks. midlertidig kan begrense en gitt rolle fra deres handlinger.

Alle tillatelser er delt mellom "Lesetilgang" og "Full tilgang". Ved å gi en rolle lesetilgang kan de se den spesifikke delen av konsollen. Ved å gi dem full tilgang kan rollen se og endre den spesifikke delen av konsollen.

Tildeling av roller

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

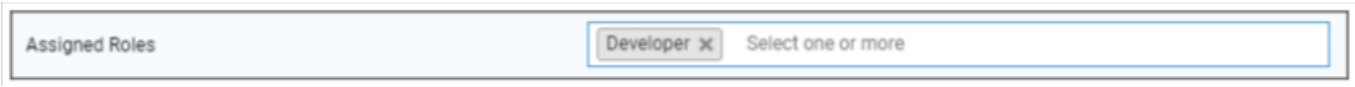


1. Velg hvilken gruppe eller bruker du vil legge til eller fjerne roller for. Du kan enten velge en enkelt bruker eller en gruppe. Når du velger en gruppe, vil endringen påvirke alle brukere i gruppen og alle brukere i undergruppene i den valgte gruppen.
2. Velg hvilken rolle du vil legge til eller fjerne. Du kan velge én 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. Lagre for å fullføre prosessen. Brukere som tidligere ikke hadde noen rolle og "Kan logge inn" deaktivert, vil automatisk motta en e-post med en lenke for å angi et passord.

Under Tildeling av masseroller finner du oversikten over de tildelte rollene. Du kan også endre roller manuelt for bestemte brukere.

Tildeling av en rolle

For å tildele en rolle til en bruker må du gå til Mobile Management, der du finner treet med grupper, brukere og enheter. Rediger brukeren for å tildele en rolle. Alternativt kan du også bruke metoden ovenfor for enkeltbrukere.



API-tilgang

Få tilgang til AppTec360 REST API

AppTec360 REST API krever et autentiseringstoken (API-nøkkel) og en privat nøkkel som må genereres i administrasjonskonsollen.

For å gjøre dette logger du inn i AppTec360 EMM og går til

Generelle innstillinger → Rollebasert tilgang → API-tilgang, og legg til en ny nøkkel.

Du må velge en bruker som skal ha rettigheter til API-nøkkelen.

Den private nøkkelen kan bare lastes ned én gang. Etter at nedlastingen har startet, slettes nøkkelen, og "Last ned"-knappen forsvinner.

Hvis du mister den private nøkkelen din, må du generere en ny API-nøkkel.

Generelle regler

- REST API er tilgjengelig under basis-URL-en:

/public/external/api

- Alle forespørsler må sendes via POST.
- REST API støtter bare forespørsler via HTTPS.
- Forespørsler må inneholde følgende overskrifter:

Navn på overskrift	Overskriftsverdi	Beskrivelse
Innholdstype	application/json	fast
autorisasjon	123...xyz	API-nøkkel fra fanen "API-tilgang"
underskrift	Base64-kodet signatur	Signaturen til nyttelasten generert med privat nøkkel fra fanen "API-tilgang"

- Forespørselen må være et json-kodet objekt som må inneholde følgende verdier:

Felt	Felt Eksempel Verdi	Beskrivelse
api	v2/enhet/listdeenheter	Navnet på API-et
tid	1529662725	Unix-tidsstempel (UTC) for klientmaskinen. Den maksimalt tillatte tidsforskjellen mellom klienten og serveren er 30 minutter.

- Hvis API-et lykkes, returnerer det de forespurte dataene (se spørringene nedenfor) og en HTTP-statuskode 200.
- Hvis det oppstår en feil, vil HTTP-statuskoden være mellom 4xx og 5xx, avhengig av feilen, og svarobjektet vil inneholde en matrise med nøkkelen "errors", som inneholder en liste over feilmeldinger som er lesbare for mennesker.
- Hvis det ikke finnes noen matchende data for en enhet, returneres en tom matrise.
- Hvis en enhets-ID ikke finnes, vil returdataene være null.

Eksempel på forespørsel

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]}}

Forespørsler

Liste over alle enheter

Funksjonalitet: Returnerer en liste over alle enheter som inneholder enhets-ID, IMEI og serie
API URI: v2/device/listdevices
Obligatoriske parametere: ingen
Valgfrie parametere: ingen

Eksempel på forespørsel

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

Eksempel på svartekst

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

Hent liste over (GPS-)posisjoner

Funksjonalitet: Returnerer en liste over alle lagrede posisjonsloggoppføringer for enhets-ID-er
API URI: v2/device/listposition
Obligatoriske parametere: "ids" - Array av enhets-ID-er
Valgfrie parametere: ingen

Eksempel på forespørsel


```
{
"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 ressursoversikt

Funksjonalitet:
Returnerer en liste over alle lagrede mulige ressurser som kan forespørres ved hjelp av Get any asset data.
Du kan enten bruke det lesbare skjemaet eller ressursetiketten til å be om dataene.
API URI: v2/device/getassetmap
Obligatoriske parametere: ingen
Valgfrie parametere: ingen

Eksempel på forespørsel

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

Eksempel på svartekst

Dette svaret ble forkortet av hensyn til lesbarheten.

{
"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 eiendelsdata

Funksjonalitet: Returnerer en liste over forespurte ressursdata for enhets-ID-er
API URI: v2/device/getassetdata
Obligatoriske parametere: "ids" - Array av enhets-ID-er
Valgfrie parametere:
"assetkeys" - Ressursdatanøkler som skal returneres. Hvis ikke spesifisert, returneres alle tilgjengelige aktivadata
. Du kan få en liste over ressursnøkler ved hjelp av Get asset map.

Eksempel på forespørsel

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

Eksempel på svartekst

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

Eksempelkode 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-konfigurasjon

APNS-sertifikat

Her kan du laste opp et APNS-sertifikat. Dette kreves for å administrere iOS- og MacOS-enheter.

Merk: APNS-sertifikatet er kun gyldig i ett år. Det må fornyes før det utløper. Fornyelsesprosessen er identisk med opprettelsen (se nedenfor) og tar bare noen få minutter.

Hvis du glemmer å fornye dette i tide, kan du ikke gjøre endringer på de allerede registrerte enhetene dine **og du må registrere alle enhetene på nytt**.

Trinn 1

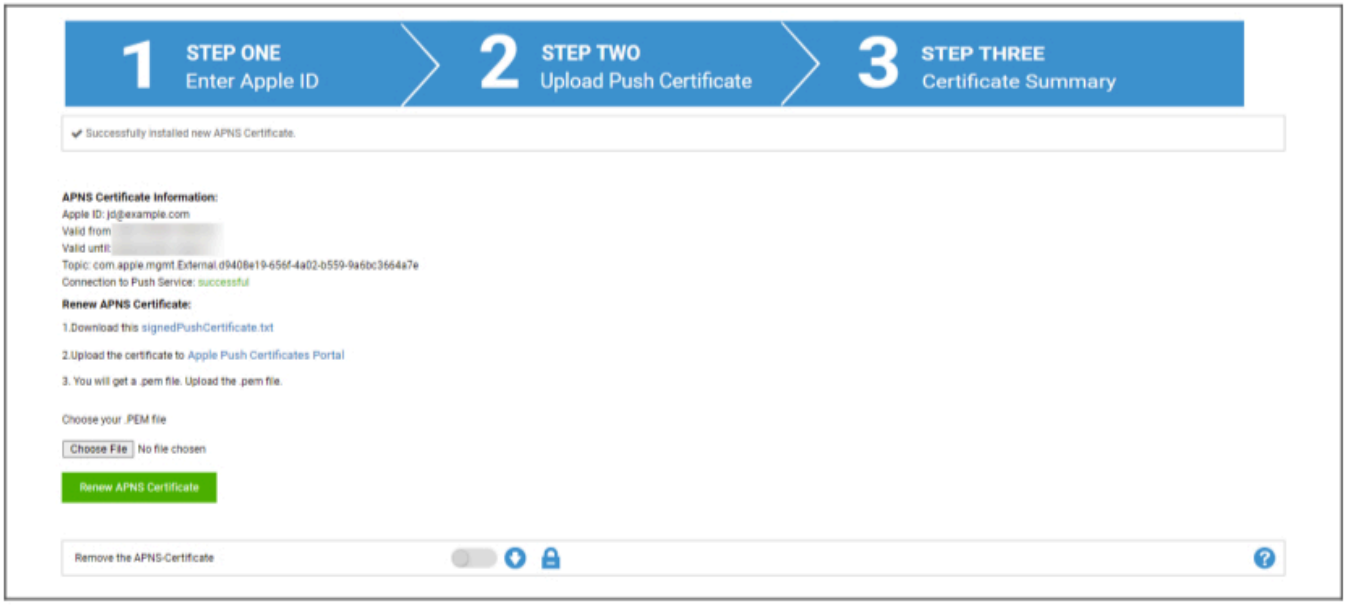
- Først skriver du inn Apple-ID-en du vil bruke til å opprette APNS-sertifikatet.

Merk: Denne Apple-ID-en brukes kun til å opprette APNS-sertifikater. Denne Apple-ID-en har ingenting med enhetene å gjøre, og enhetene vil ikke vite om denne Apple-ID-en. I tillegg trenger du også tilgang til denne Apple-ID-en for å fornye APNS-sertifikatet. Derfor anbefales det å bruke en generisk Apple-ID og dokumentere påloggingsdataene. En påminnelse sendes til den brukte e-postadressen til Apple-ID-en før APNS-sertifikatet utløper.

- Klikk på "Neste trinn" for å fortsette.
- (valgfritt) Du kan også gjenopprette det tidligere slettede APNS-sertifikatet hvis du slettet det ved et uhell

Trinn 2

- Last ned signedPushCertificate.txt
- Gå til https://identity.apple.com/pushcert/ og logg inn med Apple-ID-en fra trinn 1
- Klikk på "Opprett et sertifikat"
- (valgfritt) skriv inn en merknad. Dette kan være nyttig hvis du administrerer flere leietakere, slik at du enkelt kan identifisere dem.
- Klikk på "Choose File" for å velge den tidligere nedlastede signedPushCertificate.txt
- Klikk på "Last opp".
- Du vil nå se en bekreftelse på at du har opprettet et APNS-sertifikat.
- Klikk på "Last ned" og lagre den.
- Gå tilbake til administrasjonskonsollen.
- Klikk på "Choose File" og velg APNS-sertifikatet du vil laste opp.
- Klikk på "Last opp"



Trinn 3

Du har nå konfigurert APNS-sertifikatet og kan nå administrere iOS- og MacOS-enheter.

I trinn 3 ser du en oversikt over APNS-sertifikatene du bruker for øyeblikket.

Du har også muligheten til å fornye APNS-sertifikatet ved å følge trinnene som vises på skjermen. Husk å fornye dette før det utløper.

Når du fornyer APNS-sertifikatet, må du huske å logge inn med Apple-ID-en som vises i trinn 3, og også å fornye det tidligere brukte sertifikatet og IKKE opprette et nytt. Du vil se "emnet" for APNS-sertifikatet i trinn 3 og når du klikker på "i" i Apple Push Certificate Portal. Dette er den unike ID-en som identifiserer sertifikatet. Dette vil hjelpe deg med å identifisere det riktige og fornye det riktige.

Når du får "Feil: Push-sertifikatet har et annet emne!" under fornyelsen, betyr det at du har fornyet et annet sertifikat eller opprettet et nytt.

Hvis du vil laste opp et nytt sertifikat, f.eks. hvis du ikke lenger har tilgang til den tidligere brukte Apple-ID-en, må du først slette det opplastede sertifikatet.

Hvis du sletter APNS-sertifikatet, betyr det uansett at du ikke lenger kan gjøre endringer for de enhetene som er registrert, før du registrerer dem på nytt. Så sørg for at du er forberedt på dette, og fjern bare sertifikatet hvis det ikke finnes noen annen måte.

Administrert tilgang

Her kan du aktivere brukerregistrering for iOS-enheter og delt iPad for iOS-enheter.

Brukerregistrering

"User Enrollment" aktiverer en spesiell modus for BYOD-enheter.

For hver bruker må det opprettes en administrert Apple-ID i Apple Business Portal.

Under registreringsprosessen vil brukerne bli bedt om å oppgi Apple-ID-legitimasjonen sin.

"User Enrollment" garanterer maksimal sikkerhet for brukeren, ettersom det kun er et begrenset sett med innstillinger og begrensninger som kan konfigureres av MDM.

Administrert domene:

Domenet som brukes til å tilordne brukerens e-postadresse til deres administrerte Apple-ID (må være i formatet: "@appleid.company.com"), f.eks. john.doe@example.com vil bli tilordnet til john.doe@appleid.company.com

Sjekk Apple Business Manager for å se ditt administrerte domene

Delt iPad

En delt iPad er en DEP-enhet som er konfigurert med en spesiell DEP-profil.

Dette gjør det mulig for flere brukere å logge inn på enheten ved hjelp av sin administrerte Apple-ID.

Den administrerte Apple-ID-en må opprettes i Apple Business Portal eller Apple School Manager.

Brukere som logger seg på en delt iPad, blir bedt om å oppgi sin administrerte Apple-ID-legitimasjon.

Administrert domene:

Domenet som brukes til å tilordne brukerens e-postadresse til deres administrerte Apple-ID (må være i formatet: "@appleid.company.com"), f.eks. john.doe@example.com vil bli tilordnet til john.doe@appleid.company.com

Sjekk Apple Business Manager for å se ditt administrerte domene

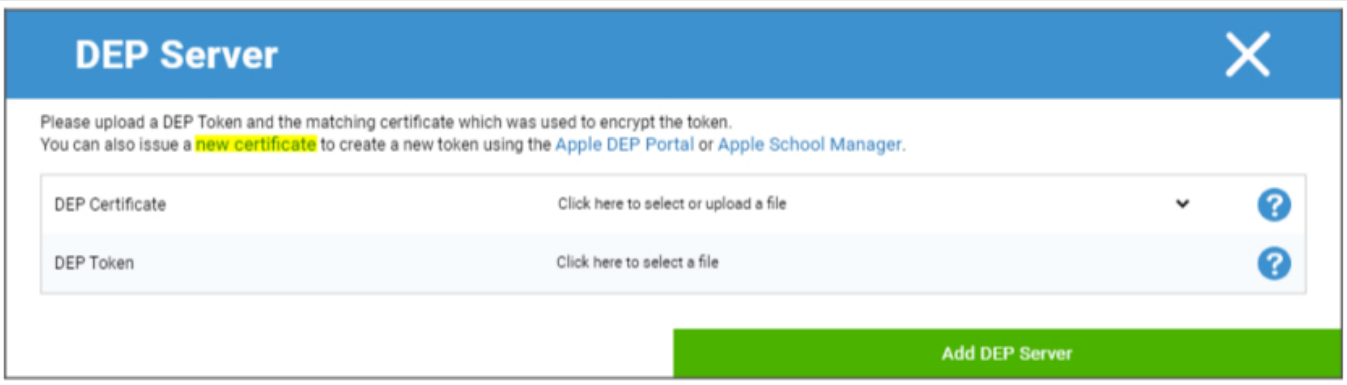
DEP

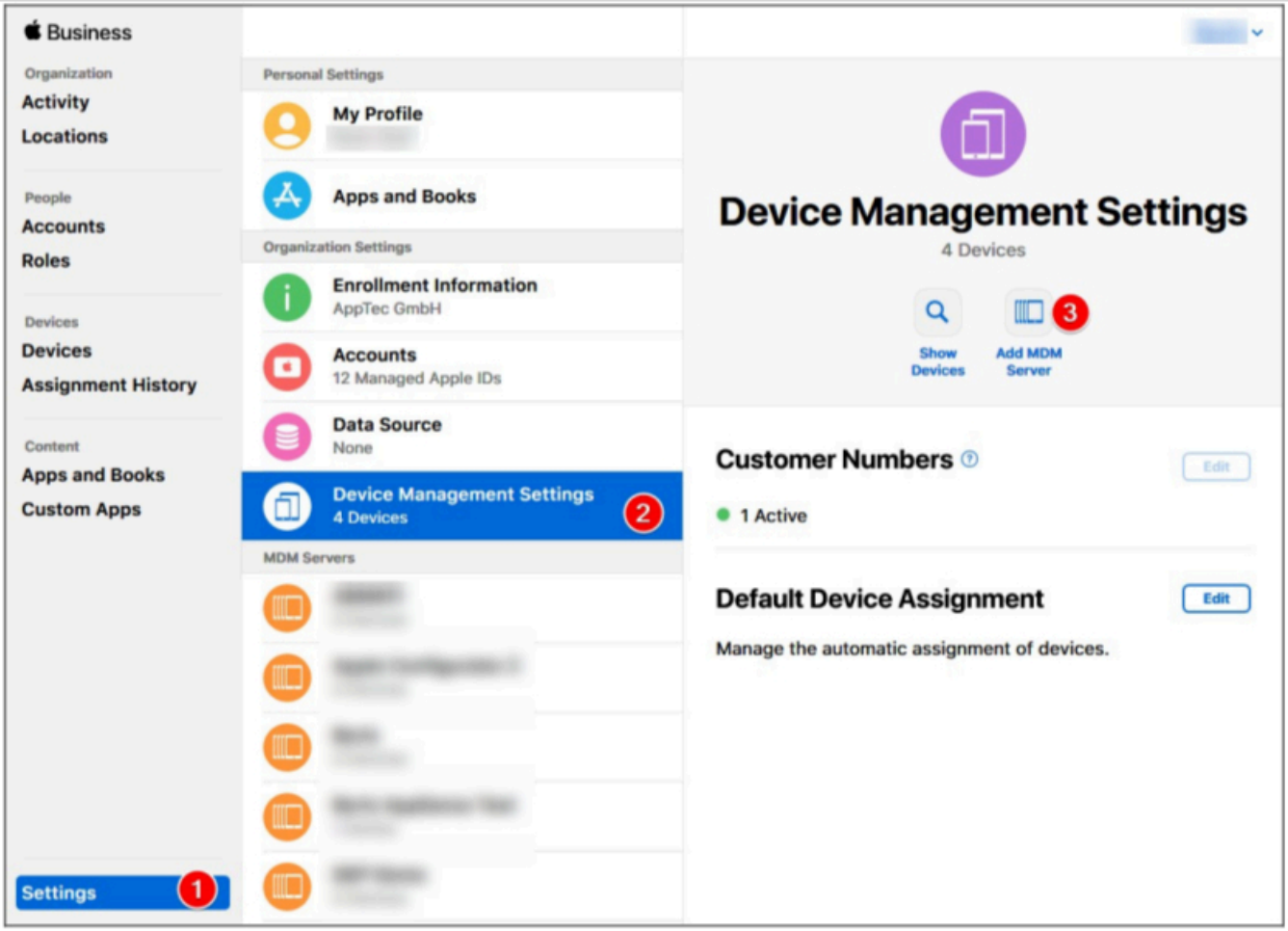
Med DEP (Device Enrollment Program) kan du enkelt registrere enheter i MDM. Når du bruker DEP, blir enhetene automatisk koblet til MDM når du konfigurerer enheten. Du kan også hoppe over nesten alle oppsettstrinnene som vanligvis er obligatoriske på iOS.

Husk at du må kjøpe enhetene fra en forhandler som støtter DEP. Kontakt forhandleren eller Apple for mer informasjon.

Mer informasjon om DEP: https: //www.apple.com/business/dep/

Klikk på "+" for å legge til et DEP Token. I popup-vinduet klikker du på "nytt sertifikat" i teksten (markert med gult i bildet nedenfor). Dette vil generere og laste ned et DEP-sertifikat. Gå deretter til Apple Business Manager(https://business.apple.com/) eller Apple School Manager(https://school.apple.com/).

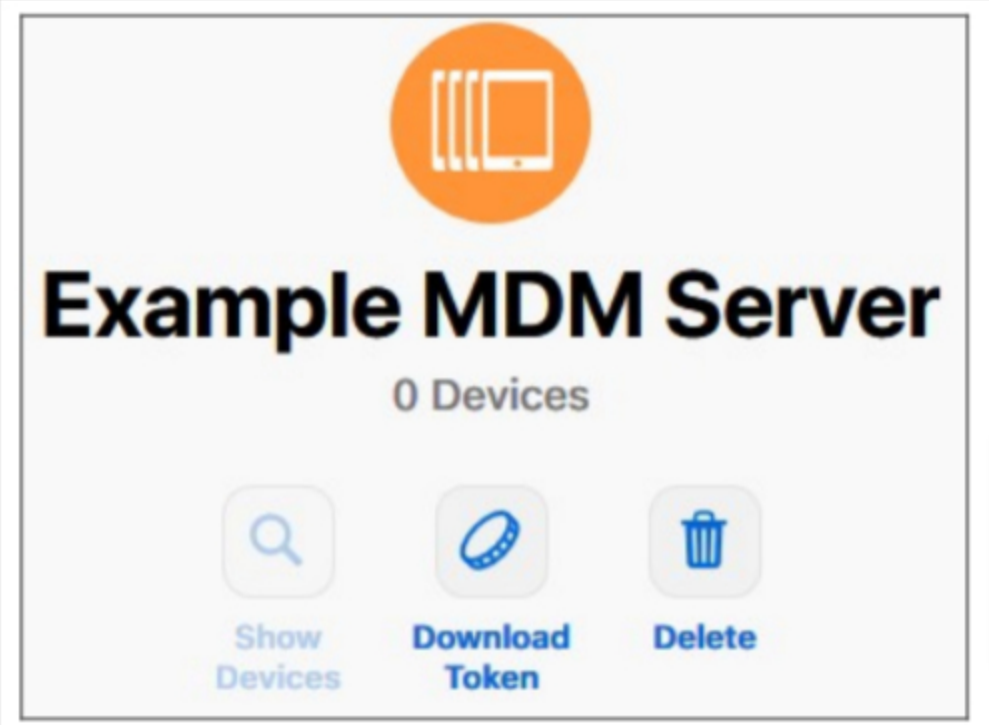




I Apple Business Manager følger du trinnene som vist i bildet ovenfor. Innstillinger → Innstillinger for enhetsadministrasjon → Legg til MDM-server.

Gi serveren det navnet du ønsker, og last opp det tidligere nedlastede DEP-sertifikatet under MDM-serverinnstillinger → Last opp offentlig nøkkel, og klikk på "Lagre".

Du vil nå få valget "Last ned token". Klikk på dette og lagre det. Tokenet er bare gyldig i ett år. Men ved å klikke på "Last ned token" igjen får du et nytt, noe som gjør det enkelt å fornye tokenet.



Du kan nå gå tilbake til MDM, der du tidligere lastet ned DEP-sertifikatet. Hvis du ikke lukket fanen, bør popup-vinduet for å legge til en DEP-server fortsatt være åpent, og DEP-sertifikatet bør allerede være valgt. Du kan nå laste opp Token i feltet "DEP Token" og klikke på DEP Server.

I kolonnen "**Enheter**" ser du hvor mange enheter som er tilordnet denne DEP-serveren. Enheter som legges til denne DEP-serveren, opprettes automatisk i DEP-poolen i Mobile Management.

Du kan klikke på dette nummeret for å få en oversikt over alle DEP-enhetene dine og statusen deres.

Merk: Avhengig av arbeidsflyten eller konfigurasjonen i Business Manager kan det være at du må tilordne disse enhetene til DEP-serveren manuelt. Du kan også angi en standard DEP-server i Apple Business Manager for nye enheter.

I kolonnen "**Profiler**" ser du hvor mange DEP-profiler du har. Du kan også klikke på dette tallet for å se detaljer om DEP-profilene dine, og du kan slette gamle/ubrukte profiler her. Det er for øyeblikket ikke mulig å endre disse. Hvis du vil gjøre en endring, må du opprette en ny.

I kolonnen "**Last Synchronization**" kan du synkronisere DEP-serveren manuelt (f.eks. hvis du nettopp har lagt til en ny enhet i DEP) og se datoen for den siste vellykkede synkroniseringen.

I kolonnen "**Auto Profile**" kan du angi en DEP-profil som automatisk standard. Denne profilen tilordnes automatisk til nye enheter. Hvis du ikke angir en automatisk profil, må du tilordne en profil

manuelt til nye enheter hver gang.

I kolonnen "**Legg**til profil" kan du legge til en ny DEP-profil. Enheten vil motta denne i begynnelsen av oppsettet av enheten. DEP-profilen definerer hvordan enheten skal konfigureres, og hvilke oppsettstrinn som skal hoppes over.

Merk: Etter at en enhet er registrert, kan disse innstillingene bare endres ved å utføre en tilbakestilling til fabrikkinnstillingene og registrere enheten med en ny profil. Dette gjelder spesielt for "**Flyttbar**" og "**Tillat**sammenkobling". Når det gjelder "**Tillat sammenkobling**", anbefales det å slå denne på, siden den kan deaktiveres via MDM-restriksjoner, men den kan ikke aktiveres igjen hvis den er deaktivert i DEP-profilen.

I kolonnen "**Rediger**" kan du laste opp et nytt token, f.eks. når du skal fornye tokenet.

Konfigurator og URL

URL-adresser for poolregistrering

Her kan du opprette en URL-adresse og en QR-kode for registrering som er gyldig for et bestemt antall registreringer og frem til en bestemt dato. Dette gjør at du kan registrere flere enheter med bare én lenke eller QR-kode.

Enheter som er registrert med denne URL-adressen eller QR-koden, vil ligge i Pool i Mobile Management, og du må tilordne dem manuelt til en gruppe eller bruker i etterkant.

Merk: Dette er kun for manuell registrering. Ikke bruk denne URL-en hvis du registrerer enhetene via Apple Configurator.

MDM-profil – Apple Configurator

Her kan du hente URL-en du trenger når du registrerer enheter via Apple Configurator. Når du klargjør enheter med Apple Configurator, kan du legge til enhetene i MDM i samme prosess. Apple Configurator krever denne URL-adressen for dette.

Enheter som legges til via Apple Configurator, vil ligge i Pool i Mobile Management, og du må tilordne dem manuelt til en gruppe eller bruker i etterkant.

Du finner også en .mobileconfig-fil her som kan brukes til å registrere enhetene via Apple Configurator. Det anbefales uansett å bruke URL-en.

Android-konfigurasjon

Android-konfigurasjon

Avinstaller beskyttelse	Hvis denne funksjonen er aktivert, kan ikke brukeren deaktivere enhetsadministratoren uten å oppgi passordet som er angitt av MDM-administratoren. Passordet angis under registreringen, så enheter må registreres på nytt for å oppdatere passordet. Det finnes to alternativer for å fjerne enhetsadministratorene: 1. Manuelt på enheten ◦ Åpne EMM-appen på enheten ◦ Gå til Status-fanen ◦ Trykk på "Avinstaller beskyttelse" ◦ Skriv inn passordet Du kan bruke Revisjon til å hente det riktige passordet fra "Passordhistorikk" i konsollen. ◦ Bla nedover og trykk på det nylig tilføyde punktet, "Trykk for å avinstallere AppTec360 MDM App" (du har 20 sekunder på å utføre denne oppgaven) ◦ Bekreft dialogen "Avinstaller AppTec360 MDM App" med "ok". Dette vil fjerne registreringen av enheten fra konsollen. ◦ For å fjerne appen fra enheten, bekreft dialogen "AppTec360 MDM vil bli avinstallert" med "UNINSTALL" 2. den automatiske (konsoll) ◦ Velg enheten i konsollen ◦ Klikk på det blå tannhjulikonet og velg "Enterprise Wipe" Merk: Kun tilgjengelig med Android 4.x og lavere versjoner eller på enheter med KNOX API (Samsung-enheter)
Avinstaller passord (revisjon x)	Det etablerte passordet, som brukeren kan fjerne enhetsadministratoren med

	Revisjon x = teller, hvor ofte passordet allerede har blitt endret Det er viktig hvilket passord brukeren trenger, fordi det er mulig at enheten ikke har kommunisert med AppTec360 Server og at det nyeste passordet derfor ikke har blitt overført ennå
Passordhistorikk	Når du klikker på den blå knappen ("Vis historikk"), kan du se de tidligere etablerte passordene
Utvidet beskyttelse mot avinstallasjon	Dette alternativet gir beskyttelse mot ikke-SAFE-enheter Så lenge denne innstillingen er aktivert, er det ikke mulig å deaktivere enhetsadministratoren på en enkel måte
Oppfordre brukeren til å avinstallere blokkerte apper?	Hvis det er mulig, vil blokkerte apper ikke bare bli blokkert, men også avinstallert automatisk. Brukeren vil bli bedt om å avinstallere blokkerte apper hvis det ikke er mulig å avinstallere dem automatisk.
Intelligent system for blokkering av apper	Hvis Whitelisting er aktivert, blokkerer Android MDM-klienten alle brukerinstallerte apper. Aktiver denne innstillingen for å blokkere alle systemapper som kan startes i hvitelistingsmodus.

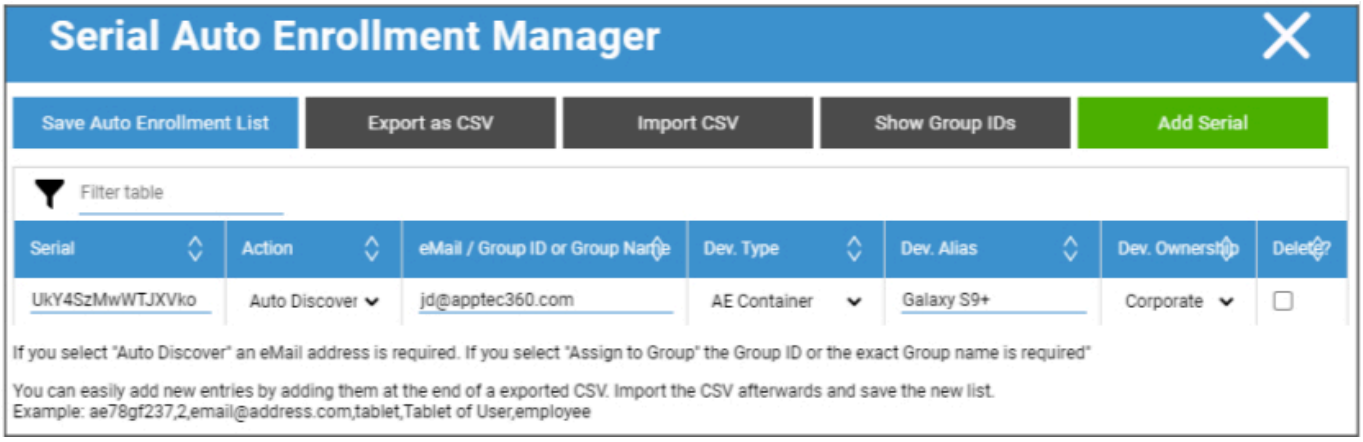
Automatisk innmelding

Her kan du aktivere funksjonen Auto Enrollment for å registrere enhetene dine automatisk når AppTec360 MDM Client åpnes på enheten.

Viktig: Denne registreringsmetoden er foreldet og fungerer ikke lenger på Android 10 eller nyere. Når du bruker Android 7 eller nyere, bør du uansett registrere enheter som Android Enterprise fullt ut administrert. Hvis du vil bruke Android Enterprise BYOD-containeren og du bruker Android 10 eller nyere, må du registrere enheten manuelt via legitimasjon, QR-kode eller SMS. Auto Enrollment List brukes uansett fortsatt til å automatisere registreringsprosessen for f.eks. AE Enrollment, Knox Enrollment osv.

Auto Enrollment List brukes uansett fortsatt til å automatisere registreringsprosessen for f.eks. AE Enrollment, Knox Enrollment osv.

Ved å klikke på "Serial Manager" eller "IMEI Manager" kan du legge til henholdsvis serienummeret eller IMEI-nummeret til enhetene dine. Det er ikke nødvendig å gjøre begge deler for enhetene dine, bare én er nok.



Handling definerer om enhetene skal registreres i utvalget, en bruker eller en gruppe.

Du kan også eksportere og importere en .csv-fil og filtrere oppføringene dine etter nøkkelord.

Android Enterprise

Her kan du konfigurere Android Enterprise. Dette er nødvendig for å kunne bruke alle Android Enterprise-funksjonene.

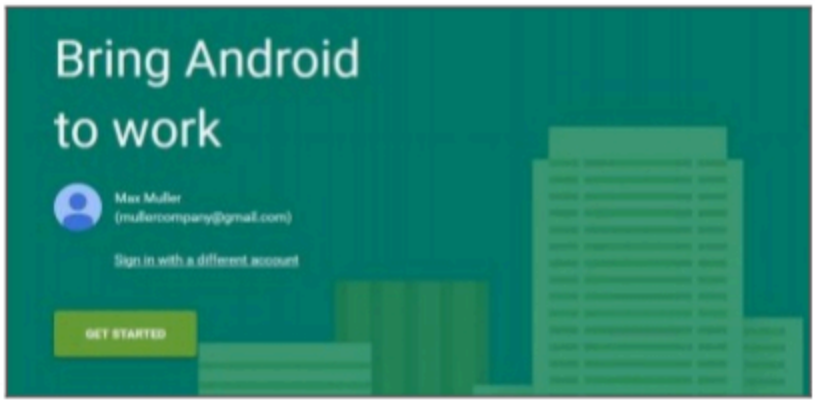
Første metode: Android Enterprise-konto (Google-konto)

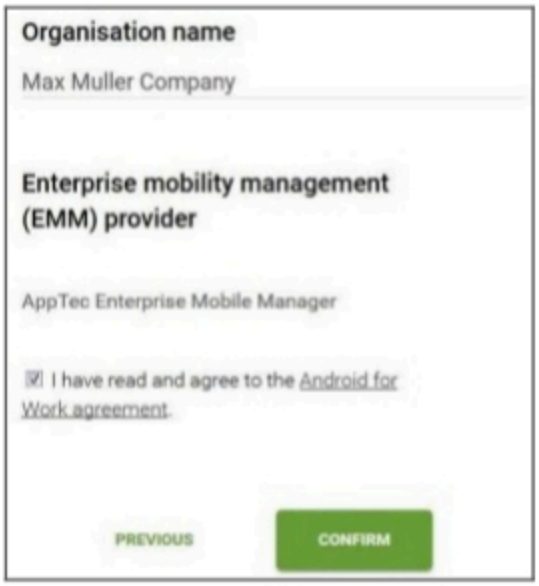
Trykk først på "Prepare Setup", og etter et kort øyeblikk skal knappen "Start Setup" vises.

Dette tar deg til Googles Android Enterprise Setup-side.

Logg inn med Google-kontoen du vil bruke, hvis du ikke allerede er logget inn, og trykk på "Kom i gang".

Nå kan du skrive inn navnet på selskapet ditt. Etter å ha gjort det, merker du av i avmerkingsboksen og trykker på "Bekreft"





I det siste trinnet kan du fullføre registreringen og bør gå tilbake til konsollen. Hvis alt fungerte, skal det se slik ut:

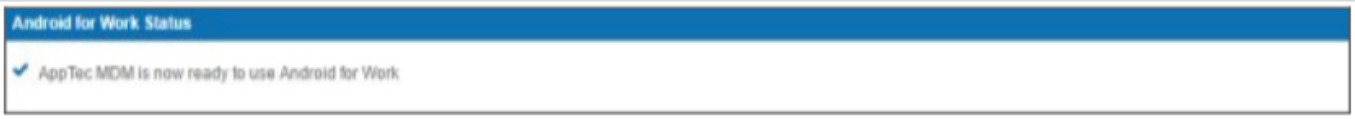
Nå kan du begynne å konfigurere Android Enterprise Container.

Andre metode: G-Suite-konto

Trykk på "Bruk G-Suite" og logg inn på Google Admin-kontoen din. Der går du til "Sikkerhet" -> "Vis mer" -> "Administrer EMM-leverandør for Android" og genererer et Token. Merk: Hvis du ikke ser Android Enterprise-innstillingene i G-Suite-kontoen din, må du gå til "Få flere apper og tjenester" og legge til Android-enhetsadministrasjon. Skriv nå inn Token og ditt primære domene i konsollen vår, og klikk på "Lagre endringer". Når du er ferdig, klikker du på "Bruk Android Enterprise-konto".

Nå bør du se knappen "Opprett tjenestekonto". Klikk på den. Denne prosessen kan ta noen øyeblikk.

Hvis alt fungerte, skulle det se slik ut:



Nå kan du begynne å konfigurere Android Enterprise Container.

Beskyttelse mot tilbakestilling til fabrikkinnstilling

Med Factory Reset Protection kan du binde enheten din til en Google-konto etter eget valg, noe som også overstyrer en eventuell eksisterende binding til en Google-konto. For å bruke Factory Reset Protection må du først konfigurere den her og aktivere den i profilene dine etterpå.

For å konfigurere fabrikktilbakestillingsbeskyttelsen klikker du på "FRP Setup" og følger instruksjonene på skjermen.

MERK: Les og utfør trinnene nøye. Vi anbefaler at du gjør dette i et nytt inkognitovindu i nettleseren for å unngå at du automatisk logger inn på feil Google-konto. Du kan sperre deg selv helt ute av enheten hvis du skulle angi feil ID eller miste tilgangen til den brukte Google-kontoen!

AE-innmelding

Her kan du aktivere Android Enterprise Ernollment. Ved å bruke denne metoden vil enhetene dine bli registrert i Android Enterprise Device Owner Mode. I denne modusen vil du ha full kontroll over enheten.

Aktiver AE-registrering	Aktiverer AE-registrering Forsiktig: Hvis du deaktiverer AE Enrollment, vil eksisterende QR-koder og allerede konfigurerte NFC-programmeringsenheter slutte å fungere. Hvis du aktiverer AE Enrollment igjen, må du sende NFC-pushkonfigurasjoner på nytt / generere nye QR-koder.
Aktiver automatisk oppdagelse	Når en enhet registrerer seg selv via "AE Enrollment", vil systemet forsøke å tilordne den til en bruker basert på informasjonen som er angitt i Serial / IMEI Whitelist ("General Settings" > "Android Configuration" > "Auto Enrollment").
Blokker ukjente enheter	Bare enheter som er hvitelistet i Serial / IMEI Whitelist ("Generelle innstillinger" > "Android-konfigurasjon" > "Automatisk registrering") har lov til å registrere seg.

Merknad om metode 1 og 2: "Velkomstskjermen" refererer til det første skjermbildet du ser etter tilbakestillingen til fabrikkinnstillingene. Dette kan se annerledes ut avhengig av hvilken Android-versjon og/eller enhetsmodell du bruker.

Metode 1: Registrering med QR-kode

(krever Android 7.0 eller nyere) Vi anbefaler at du alltid bruker denne metoden hvis du kjører Android 7 eller nyere.

1. Tilbakestill enheten til fabrikkinnstilling
2. Generer QR-koden for registreringen ved hjelp av en av de to følgende metodene:
    - Klikk på "Generer QR-kode" i "Generelle innstillinger -> Android-konfigurasjon -> AE-registrering". Velg om du vil hoppe over lagringskrypteringen og/eller om alle systemapper skal fjernes.
    - (alternativt) Velg en eksisterende enhet. I "Enhetsoversikt" klikker du på QR-koden som vises der. Velg om du ønsker å hoppe over lagringskrypteringen og/eller om alle systemapper skal fjernes.
3. Trykk nå 6 ganger på velkomstskjermen på enheten din. Dette bør starte QR-registreringsmodus.
4. Koble deg nå til et trådløst nettverk, og vent en kort stund til QR-kodeleseren er installert
5. Skann nå QR-koden
6. Nå er det klart. Enheten din er nå registrert i Android Enterprise Device Mode.
    - a. Hvis du brukte QR-koden i "Generelle innstillinger", kan du finne enheten din i "Pool -> AE Device Owner Devices". (Tips: Det er mulig at du må laste inn nettstedet på nytt for å

se enhetene). Hvis du har krysset av for "Aktiver automatisk oppdagelse", finner du den i din Auto Discover-bruker.

- Hvis du har brukt QR-koden til en eksisterende enhetsprofil, vil enheten bli registrert i denne profilen.

Metode 2: NFC-registrering

(krever NFC og Android 6.0 eller nyere)

Forberedelse: Skriv inn WiFi-informasjonen din i "Generelle innstillinger -> Android-konfigurasjon -> AE-registrering -> Data for NFC-klargjøring". Bruk nå "NFC Device" for å søke etter enheten som skal bli programmereren. Denne enheten vil bli brukt til å sende registreringsinformasjonen til de andre enhetene via NFC.

1. Tilbakestill enheten til fabrikkinnstilling
2. Åpne NFC-paringsappen fra AppTec360 på programmeringsenheten
3. Velg om du vil hoppe over lagringskrypteringen og/eller om alle systemappene skal fjernes.
4. Hold begge enhetene rygg mot rygg
5. Nå skal Android Enterprise Enrollment være sterk
6. Du finner nå enheten din i konsollen
    - a. Hvis du ikke har konfigurert Auto Discover i bassenget
    - b. I brukeren du har konfigurert for Auto Discover
    - c. Tips: Det er mulig at du må laste inn nettstedet på nytt for å se enhetene

Metode 3: Google-konto

(krever Android 5.1 eller nyere)

(Merk: Hvis du bruker denne metoden, blir ikke enheten automatisk registrert. I stedet må du registrere den manuelt eller automatisere prosessen ved å bruke Auto Enrollment).

1. Tilbakestill enheten til fabrikkinnstilling
2. Gå gjennom oppsettstrinnene til du kan logge inn med en Google-konto
3. Skriv inn "afw#apptec" som brukernavn/e-post
4. Trykk på "Neste"
5. Enheten din er nå en Android Enterprise-enhet

KNOX Innmelding

Her kan du aktivere KNOX Enrollment og finne informasjonen du trenger for å opprette en KNOX Enrollment-profil i KNOX Deployment Portal. Du trenger en konto på KNOX Deployment Portal for å konfigurere og bruke dette.

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

Aktiver KNOX-registrering	Aktiverer KNOX-registreringen. Advarsel! Hvis du deaktiverer KNOX Enrollment, vil eksisterende MDM-profiler slutte å fungere. Hvis du aktiverer KNOX Enrollment igjen, må du oppdatere feltet "Custom JSON Data" i MDM-profilen din.
Aktiver automatisk oppdagelse	Når en enhet registrerer seg selv via "KNOX Enrollment", vil systemet forsøke å tilordne den til en bruker basert på informasjonen som er angitt i Serial / IMEI Whitelist ("General Settings" > "Android Configuration" > "Auto Enrollment").

1. Logg inn på Samsung KNOX Mobile Enrollment Portal https://eukme.samsungknox.com/itadmin
2. Gå til "MDM-profiler"
3. Klikk på "Legg til"
4. Velg "Server URI not required for my MDM" og klikk på "Next"
5. Opprett nå en profil med informasjonen som vises i administrasjonskonsollen

Nå kan denne KNOX Enrollment Profile installeres direkte på enheten av Samsung hvis du kjøper enhetene direkte fra Samsung.

Alternativt kan du laste ned KNOX Deployment-appen, logge inn med KNOX Deployment-kontoen din og sende KNOX Enrollment Profile via NFC til andre enheter.

Hvis enheten har en KNOX Enrollment Profile installert, vil den laste ned appen vår og registrere enheten, forutsatt at den har en fungerende internettforbindelse.

Enhetsregistrering via KNOX Enrollment finner du i "Pool -> KNOX Enrollment", eller i den brukeren du har angitt i Auto Discover.

Null berøring

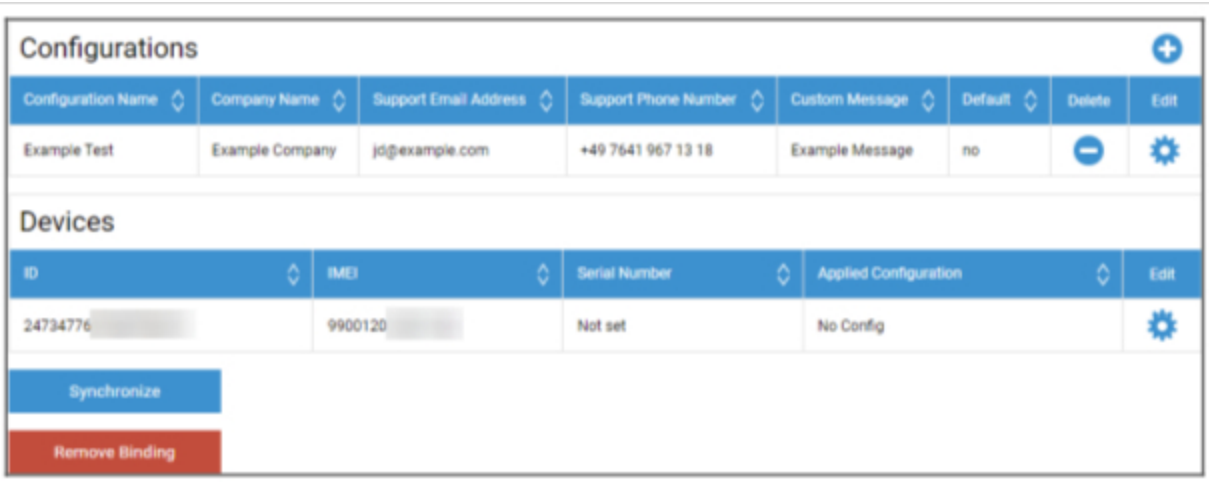
Med Zero-Touch kan du enkelt registrere enhetene dine uten å måtte berøre dem eller konfigurere noe på selve enheten. Du trenger bare å slå den på, gå gjennom konfigurasjonen som normalt, og enheten vil motta all informasjon om hvordan den skal konfigureres og kobles til MDM helt automatisk.

For å bruke Zero-Touch må du kjøpe enhetene dine fra en forhandler som støtter Zero-Touch. Den samme forhandleren oppretter også en konto for deg i Zero-Touch-portalen. Kontakt forhandleren din for å få mer informasjon om prosedyren eller hvis du har problemer med å få tilgang til Zero-Touch-portalen.

Klikk på "Start oppsett" for å starte oppsettet. Du vil bli omdirigert til en innloggingsside der du må velge Google-kontoen din som har tilgang til Zero-Touch Portal.

MERK: Det er mulig å velge en hvilken som helst konto. Sørg derfor for å velge riktig konto i dette trinnet. Hvis du ikke ser enhetene/konfigurasjonene dine, har du høyst sannsynlig brukt feil konto.

Etter at påloggingen er fullført, ser det slik ut:



Klikk på "+" for å legge til en konfigurasjon, og fyll ut feltene som vises på skjermen. Hvis du aktiverer konfigurasjonen som standardkonfigurasjon, tilordnes den automatisk til de nye enhetene. Hvis du oppretter eller angir en standardkonfigurasjon, tilordnes den ikke til allerede eksisterende enheter.

Hvis en enhet ikke har noen konfigurasjon tilordnet, vil den bli konfigurert som en vanlig enhet og ikke koble seg til MDM. Sørg derfor for at enhetene dine har en konfigurasjon tilordnet.

Når du har koblet til kontoen din, enhetene dine er synlige og du har tilordnet en konfigurasjon til dem, kan du begynne å konfigurere enhetene.

Du kan legge til enhetene i Auto Enrollment List, slik at de automatisk blir registrert i en spesifisert gruppe eller bruker. Hvis du ikke har konfigurert noe i Auto Enrollment-listen, vil enhetene bli registrert

i Pool.

Windows-konfigurasjon

Windows-konfigurasjon

Her har du muligheten til å aktivere følgende konfigurasjoner på Windows 10-PC-en din:

Øyeblikkelig DM-tilkobling	
Tid for første forsøk	Etablerer det første tilkoblingsforsøket til enheten, denne verdien øker eksponentielt
Nye tilkoblingsforsøk	Angir hvor mange tilkoblingsforsøk DM-klienten skal utføre ved en tilkoblingsfeil
Maksimal sovetid	Angir maksimal hviletid etter en tilkoblingsfeil
Første synkroniseringsforsøk	Intervaller som enheten skal kommunisere med serveren med etter den første tilkoblingen
Første gjentakelsesintervall	Relatert til "Første synkroniseringsforsøk" Her er tidene oppgitt i minutter Under "First Sync Retries" er for eksempel verdien "2" oppført, og under "First Retry Interval" er verdien "4 Minutes" oppført, slik at enheten kommuniserer to ganger hvert fjerde minutt etter den første tilkoblingen.
Andre synkroniseringsforsøk	Intervaller som enheten skal kommunisere med serveren med etter at "Første synkroniseringsforsøk" er fullført
Andre gjentakelsesintervall	Samme prinsipp som for "First Retry Interval" - bare at her gjelder det for "Second Sync Retries"
Regelmessige synkroniseringsforsøk	Intervaller for hvor ofte enheten skal kommunisere med serveren i fremtiden Standard: "Uendelig" Vi anbefaler at du ikke endrer denne verdien, for hvis du skriver inn "10", vil enheten kommunisere med serveren 10 ganger og deretter stoppe.
Regelmessig gjentakelsesintervall	Samme prinsipp som for "First/Second Retry Interval" - bare at her gjelder innstillingene for fremtiden
Regelmessig gjentakelsesintervall	Samme prinsipp som for "First/Second Retry Interval" - bare at her gjelder innstillingene for fremtiden

Innholdsboks

Konfigurasjon

Her kan du konfigurere ContentBox. Du kan plassere filer for grupper i ContentBox som du kan få tilgang til med ContentBox-appen på enheten.

Aktiver innholdsboks	Aktiver ContentBox. Hvis du deaktiverer dette hvis du ikke bruker ContentBox, kan du spare ressurser på OnPremise-maskiner.
Bruk ekstern ContentBox-installasjon	ContentBox kan også betjenes med din egen Nextcloud.
URL	Fullstendig URL til Nextcloud-enheten
Rotbruker	Rotbruker av Nextcloud-kontoen
Rotpassord	Root-passordet til Nextcloud-kontoen
Standard gruppemappetillatelser	Standard gruppemappetillatelser, kan endres individuelt for hver gruppe (i Mobile Management)
Del gruppemappe med undergrupper	Hvis den er aktiv, kan hver undergruppe lese alle mappene til hovedgruppen, og kan også konfigureres individuelt for hver gruppe (Mobile Management)
Tillatelser for undergrupper	Tillatelser for undergrupper kan konfigureres individuelt for hver gruppe (Mobile Management)
Tillat deling	Gjør det mulig for brukeren å dele innholdet via lenker, kan konfigureres individuelt for hver gruppe
Maksimal filopplastingsstørrelse i MB	Maksimal størrelse på en fil Standard: 512 MB Maksimal konfigurasjon: 2048
WebDAV-legitimasjon	
WebDAV-URL	Du kan også åpne ContentBox med WebDAV. Vennligst ikke slett følgende mapper under noen omstendigheter: /apptecgroups /apptecgroups/AppTecGroup-X
Rotbruker	Navn på rotbrukerne
Passord	Passord for rotbrukerne

Synkroniseringen med ContentBox skjer automatisk. Du kan imidlertid utføre en manuell synkronisering med "Synchronize ContentBox".

I tillegg kan du her aktivere/deaktivere ContentBox på hver enkelt enhet.

Dette er bare relevant hvis du ikke har lisensiert ContentBox i tillegg, da har du fortsatt tilgang til 25 enheter som du kan teste ContentBox med - her kan du aktivere dette for de respektive enhetene.

LDAP-konfigurasjon

Oversikt over LDAP

Her kan du opprette en forbindelse til Active Directory via LDAP for å masseimportere brukere og grupper. Synkroniseringen må utføres manuelt. Du kan konfigurere flere LDAP-tilkoblinger til forskjellige systemer eller med forskjellige konfigurasjoner/filter.

Servernavn	Visningsnavnet til serveren
Type	For øyeblikket er det bare Active Directories som støtter LDAP som støttes
LDAP-domene	Det primære LDAP-domenet (f.eks. example.com)
LDAP-vert	Bare nødvendig hvis LDAP-verten ikke kan nås under det angitte LDAP-domenet.
Havn	La stå tom for å bruke standardport (389 eller 636 for SSL)
Brukernavn	F.eks. CN=John,OU=Users,DC=EXAMPLE,DC=COM Merk: De fleste systemer krever brukernavnet i dette formatet og godtar ikke "John" som brukernavn.
Passord	
Bekreft passord	
Tilkoblingssikkerhet	Merk: Når du bruker SSL eller TLS, blir sertifikatet til Active Directory sjekket. Hvis dette er selvsignert, må du legge til rot-CA-en i tillitslageret på den lokale maskinen. Hvis du er i skyen, må Active Directory levere et klarert sertifikat, ellers vil tilkoblingen bare fungere uten kryptering.
Automatisk synkronisering.	Aktiverer automatisk synkronisering av LDAP-katalogen i det tidsintervallet som er angitt i de generelle LDAP-innstillingene.
Base DN	Hvis du ikke ønsker å synkronisere hele katalogen, kan du angi en OU her, for eksempel OU=AndroidUsers,OU=Users,DC=EXAMPLE,DC=COM
Medlem av	Alle importerte brukere blir lagt til i den valgte gruppen
Bare aktiverte brukere?	Når dette er aktivert, vil attributtet userAccountControl bli tatt i betraktning, og brukere uten dette attributtet vil ikke bli importert.
LDAP-filter	Du kan bruke LDAP Filter til å filtrere hvilke brukere som blir importert
Regex-filter	Du kan bruke Regex Filter til å filtrere hvilke brukere som blir importert
Testtilkobling	Tester tilkoblingen når konfigurasjonen lagres
Tilbakestille katalogstruktur ved	Hvis true, flyttes alle LDAP-oppføringer tilbake til sin opprinnelige plassering i LDAP-treet. Anbefales å være aktivert.

synkronisering?	
Importere slettede brukere og grupper på nytt?	Når denne funksjonen er aktivert, vil brukere og grupper som har blitt slettet, bli opprettet på nytt. Anbefales å være aktivert.
Synkronisere slettinger?	Når denne funksjonen er aktivert, slettes grupper og brukere når de slettes på LDAP-serveren. Også enheter til slettede brukere slettes.

Under listen over LDAP-konfigurasjoner kan du definere perioden systemet skal synkroniseres automatisk. Bruker bare LDAP-konfigurasjoner for automatisk synkronisering som har det tilhørende alternativet aktivert.

App-administrasjon

In-house App DB

Android

Her kan du laste opp Android-appene som bedriften din har utviklet, og distribuere dem senere i Mobile Management i enhets- eller gruppeprofiler.

Vær oppmerksom på at vi anbefaler å kun distribuere apper på denne måten, som ikke er tilgjengelige i Google Play Store.

Klikk på "+" for å laste opp APK-filen til en app du ønsker å laste opp. For øyeblikket er det kun APK-formatet som støttes.

Opplastingsgrensen på OnPremise-apparater kan økes i trinn 3 i apparatkonfigurasjonen. Hvis du ønsker å øke opplastingsgrensen på Cloud, kan du kontakte kundestøtte for mer informasjon.

Vær oppmerksom på at APK-er vanligvis er litt mindre enn innholdet. Det er mulig at en opplasting mislykkes på grunn av dette, siden APK-en pakkes ut i prosessen. Det er f.eks. mulig at en APK på 95 MB mislykkes med en opplastingsgrense på 100 MB. I så fall må du øke opplastingsgrensen som nevnt ovenfor.

Vi anbefaler også at du først flytter APK-en manuelt til en testenhet (f.eks. via USB) og prøver å installere den manuelt med Files-appen på enheten. Hvis dette ikke fungerer av en eller annen grunn, vil det også mislykkes via MDM.

Oppdater målet

Med funksjonen "Update Target" kan du velge hvilken versjon av en app som skal installeres, eller hvilken versjon en app skal oppdateres til hvis du har aktivert "Keep up to date" for en app.

Hvis du ikke har valgt et oppdateringsmål, vil den høyeste versjonen bli brukt.

Husk at Android ikke kan nedgradere apper. Vær også oppmerksom på at "Version Code" avgjør om en versjon er høyere, lavere eller den samme. Sørg derfor for å øke denne versjonen korrekt i appen din når du lager en oppdatering.

iOS

Her kan du laste opp iOS-appene du har utviklet, og distribuere dem senere i Mobile Management i enhets- eller gruppeprofilen din.

Klikk på "+" for å laste opp IPA-en til en app du ønsker å laste opp. Kun IPA-formatet støttes per nå.

Opplastingsgrensen på OnPremise-apparater kan økes i trinn 3 i apparatkonfigurasjonen. Hvis du ønsker å øke opplastingsgrensen på Cloud, kan du kontakte kundestøtte for mer informasjon.

Oppdater målet

Med funksjonen "Update Target" kan du velge hvilken versjon av en app som skal installeres, eller hvilken versjon en app skal oppdateres til hvis du har aktivert "Keep up to date" for en app.

Hvis du ikke har valgt et oppdateringsmål, vil den høyeste versjonen bli brukt.

MacOS

Her kan du laste opp MacOS-appene du har utviklet, og distribuere dem senere i Mobile Management i enhets- eller gruppeprofilen din.

Klikk på "+" for å laste opp PKG-en til en app du ønsker å laste opp. Kun PKG-formatet støttes per nå.

Opplastingsgrensen på OnPremise-apparater kan økes i trinn 3 i apparatkonfigurasjonen. Hvis du ønsker å øke opplastingsgrensen på Cloud, kan du kontakte kundestøtte for mer informasjon.

Oppdater målet

Med funksjonen "Update Target" kan du velge hvilken versjon av en app som skal installeres, eller hvilken versjon en app skal oppdateres til hvis du har aktivert "Keep up to date" for en app.

Hvis du ikke har valgt et oppdateringsmål, vil den høyeste versjonen bli brukt.

Windows 10

Her kan du laste opp Windows 10-apper og distribuere dem senere i Mobile Management i enhets- eller gruppeprofilen din.

Klikk på "+" for å laste opp APPX, APPXBUNDLE eller MSI for en app du ønsker å laste opp. Bare APPX-, APPXBUNDLE- eller MSI-formatet støttes per nå.

Du kan også laste opp og definere avhengigheter for en app, som automatisk distribueres og installeres før du installerer den ønskede appen.

Opplastingsgrensen på OnPremise-apparater kan økes i trinn 3 i apparatkonfigurasjonen. Hvis du ønsker å øke opplastingsgrensen på Cloud, kan du kontakte kundestøtte for mer informasjon.

Oppdater målet

Med funksjonen "Update Target" kan du velge hvilken versjon av en app som skal installeres, eller hvilken versjon en app skal oppdateres til hvis du har aktivert "Keep up to date" for en app.

Hvis du ikke har valgt et oppdateringsmål, vil den høyeste versjonen bli brukt.

Win32-pakke (.exe)

Du kan også distribuere .exe-filer/installasjonsprogrammer til enhetene dine.

Navn på pakken	Navnet som vil vises i MDM
Beskrivelse	Beskrivelse vist i MDM
Pakkefil	Bare .zip-filer er tillatt. Plasser filene du vil distribuere, i denne zip-filen.
Distribusjonskontekst	**System**: Installasjonskommandoen kjører med systemrettigheter, som er høyere enn "User". Når du bruker "System", har prosessen heller ikke noe brukergrensesnitt, så den vil være stille, og brukerprofilen, f.eks. miljøvariabler som %AppDat%, er ikke tilgjengelig. **User**: Installasjonskommandoen har tilgang til brukerprofilen og kan vise brukergrensesnittet hvis det er nødvendig. Merk: Noen prosesser fungerer kanskje bare i én kontekst. Hvis en programvare f.eks. installerer seg selv i AppData, vil den bare fungere når du velger "User".
Installer kommando	Kommandoen som brukes til å installere programmet. For eksempel vil installasjonskommandoen for en zip-fil som inneholder "setup.exe" i roten, og som støtter parameteren "/s" for en stille installasjon, være "setup.exe /s". Vær oppmerksom på at ulike programvarer kan ha ulike parametere.
Avinstaller kommandoen	Kommandoen som skal kjøres for å avinstallere programvaren via MDM. Vanligvis peker denne til avinstallasjonsprogrammet. For eksempel "C:\Program Files\ExampleSoftware\uninstall.exe".
Krav	
Merk: Alle de angitte kravene må være oppfylt for at programvaren skal kunne installeres. Ellers vil den ikke bli installert. Noen felt kan være obligatoriske. Hvis det ikke er angitt noen verdi for et krav, blir kravet ignorert.	
OS-arkitektur	OS-arkitektur
Min. OS-versjon	Min. OS-versjon
Min. ledig diskplass (MB)	Min. ledig diskplass (MB)
Min. fysisk minne (MB)	Min. fysisk minne (MB)
Min. antall logiske prosessorer	Min. antall logiske prosessorer
Min. CPU-hastighet (MHz)	Min. CPU-hastighet (MHz)

Ytterligere krav	Du kan også definere regler manuelt eller laste opp et skript her for å utføre ytterligere kravkontroller hvis du ønsker det.
Regler for deteksjon	
Deteksjonsmetode	Her kan du definere hvordan du skal oppdage om appen er installert på enheten. Install-kommandoer kjøres bare når disse reglene registrerer at appen IKKE er installert. Avinstaller-kommandoer kjøres bare når disse reglene oppdager at appen ikke er installert. **Definere regler manuelt**: Her kan du manuelt definere én eller flere regler for å sjekke om for eksempel en bestemt fil, mappe, MSI eller registernøkkel er til stede. Hvis alle de angitte deteksjonsreglene er sanne, vil appen bli ansett som tilstedeværende. **Bruk skript**: Last opp ditt eget skript med dine egne kontroller. Hvis skriptet returnerer "$TRUE", vil appen bli ansett som tilstedeværende.
Regler for deteksjon	

App-innstillinger

Innstillinger for iOS-appen

Her kan du definere standardinnstillingene for å legge til en app i den obligatoriske app- eller bedriftsappbutikken.

Merk: Dette angir bare det som er valgt som standard når du legger til apper. Dette endrer IKKE eksisterende innstillinger for apper som allerede er lagt til i de obligatoriske appene eller i Enterprise App Store.

Hold deg oppdatert	Holder appen automatisk oppdatert. Vær oppmerksom på at det kan ta opptil 7 dager etter at en oppdatering er utgitt før appen er oppdatert.
Forbikjøring når den ikke er administrert	Hvis en app allerede er installert som uadministrert (av brukeren), vil appen bli overtatt og administrert av MDM.
Fjern appen når MDM-profilen fjernes	Avinstallerer appen når MDM fjernes.
Forhindre sikkerhetskopiering av appdataene	Forhindrer sikkerhetskopiering av appdataene.

Innstillinger for Android-apper

Her kan du definere standardinnstillingene for å legge til en app i den obligatoriske app- eller bedriftsappbutikken.

Merk: Dette angir bare det som er valgt som standard når du legger til. Dette endrer IKKE innstillingene for apper som allerede er lagt til i de obligatoriske appene eller i Enterprise App Store.

Hold deg oppdatert	Holder appen automatisk oppdatert. Bare tilgjengelig for InHouse-apper.
Kontrollert oppdatering av AppTec360 EMM-klienten	Hvis aktivert, kan administratorer spesifisere oppdateringsmålet for AppTec360 EMM Client. En liste over alle tilgjengelige versjoner av AppTec360 EMM Client vil vises i "Generelle innstillinger" → "App Management" → "In-House App DB" → "Android".

Tredjepartsapper

Android

Her kan du angi aktiveringskoden for Ikarus.

Sett denne til "Bruk aktiveringskode", og skriv inn aktiveringskoden din her.

Merk: Etter at du har tastet inn koden og lagret den, er koden ennå ikke lagt til i profilen som sendes til enheten. Du må utføre en endring i profilen din for at koden skal legges til i profilen. Endre f.eks. en bryter i profilen fra av → på → av - Lagre → Tilordne nå.

iOS

Her kan du angi din SecurePIM-lisens. Når du har angitt lisensen, trykker du på "Lagre endringer", og du kan bruke SecurePIM-alternativene.

VPP / KNOX Premium

Apples volumkjøpsprogram (VPP) lar deg enkelt distribuere betalte og gratis apper til enhetene dine. Dette anbefales på det sterkeste siden du ikke trenger en Apple-ID på enhetene, brukerne trenger ikke å bekrefte installasjonen (overvåket), brukerne trenger ikke å oppgi passordet til Apple-ID-en, og du kan enkelt distribuere betalte apper uten å kjøpe dem på hver enhet på nytt.

For å bruke VPP må du registrere deg i Apple Business Manager.

VPP-lisenser

Her kan du få en oversikt over VPP-appene dine, hvor mange lisenser som er brukt og hvor mange som er tilgjengelige.

Ved å klikke på hjulet kan du se hvilke enheter som har en lisens tildelt, og hva statusen for denne tildelingen er.

Ved å klikke på oppdateres VPP-cachen, som sammenligner lisensene som er tilordnet i MDM med lisensene som er tilordnet på Apples side. Dette kan løse lisensproblemer i noen tilfeller.

VPP Token

Her kan du laste opp VPP-tokenet ditt, som du finner i Apple Business Manager i Innstillinger → Apper og bøker. Du kan laste opp flere VPP-tokens.

Du kan fornye en Token ved å laste ned en ny i Apple Business Manager, klikke på "Rediger"-hjulet og laste opp den nye.

"VPP-modus" bestemmer hvordan lisenstildelingen håndteres. Avhengig av scenarioet ditt, må du bruke forskjellige moduser:

"Enhetsbasert" må brukes når du registrerer enhetene via QR-kode, Link, Apple Configurator eller DEP.

"Brukerbasert" er påkrevd hvis enhetene er registrert med brukerregistrering eller som delt iPad.

Hvis du aktiverer "Automatisert lisenshåndtering", vil brukere som flyttes fra én gruppe til en annen, automatisk bli tildelt Apple VPP-lisenser basert på gruppeprofilen de flyttes til.

Eksisterende Apple VPP-lisenser fra gruppen de har flyttet fra, vil ikke bli tilbakekalt.

Nye brukere som legges til i en gruppe, vil automatisk bli tildelt Apple VPP-lisenser basert på den respektive gruppeprofilen.

KNOX Premium Key

Her kan du legge inn KNOX Premium-nøkkelen din for å bruke Samsung KNOX Container.

Vær oppmerksom på at dette ikke lenger støttes etter Android 10. Bruk Android Enterprise Container i stedet.

Innstillinger for App Store

Region og språk

Her kan du angi standard språk og region for App Search i App Management.

Vær oppmerksom på at innstillingen for iTunes også definerer hvordan systemet henter informasjon om bestemte apper. Hvis du støter på apper i listene dine som vises på en merkelig måte (f.eks. manglende ikon), kan det hende at du har angitt et område der den aktuelle appen ikke er tilgjengelig.

AE Play Store

Her finner du alle alternativene for Play Store for Android Enterprise-enheter for å godkjenne apper, laste opp egne apper til Play Store eller lage dine egne webapper.

Godkjente apper

Her kan du få en oversikt over alle appene du har godkjent.

Apper i Play Store

Dette vil laste inn en iFrame som viser Play Store. Søk etter en app du ønsker, klikk på den og godkjenn den. Når du godkjenner appen, kan du også angi at godkjenningen skal tilbakekalles hvis de nødvendige tillatelsene endres. Vi anbefaler at du lar disse innstillingene være standard når du godkjenner apper.

Når en app er godkjent, kan du legge den til i profilene dine.

Knappen "Godkjenn" endres til "Tilbakekall godkjenning" etter at du har godkjent den, slik at du alltid kan fjerne appene hvis du ikke trenger dem lenger.

Private apper

Her kan du laste opp din egen app som en privat app til Google Play Store. Dette gjør at du kan distribuere appen gjennom Googles tjenester og oppdatere den gjennom dem. Dette har også den fordelen at dine egne apper kan installeres uten brukerbekreftelse, noe som normalt er nødvendig.

Web-apper

Her kan du opprette Web Apps, som er lenker til bestemte websider som kan tilordnes som apper.

Du kan også gi dette et egendefinert ikon og definere hvordan det skal vises.

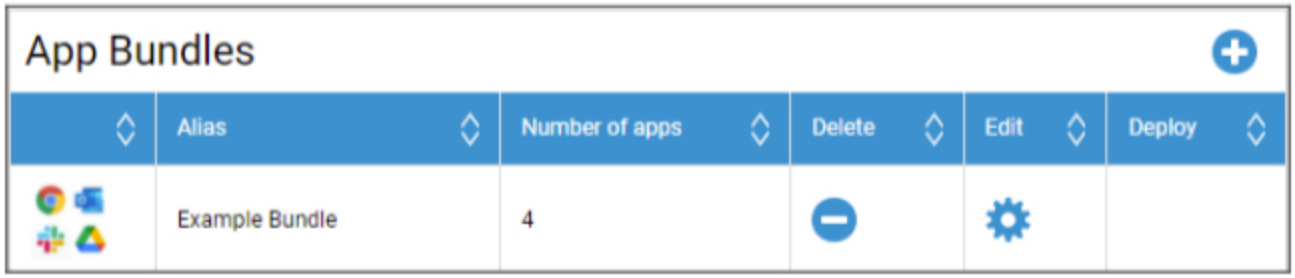
Butikkens layout

Butikkoppsettet definerer hvordan apper vises i Play-butikken, eller om de vises i det hele tatt.

Husk at hvis du vil vise apper i Play Store som brukeren kan installere manuelt, må disse legges til her i oppsettet **OG** i profilen til Enterprise Play Store. Hvis du bare legger til en app i én av dem, vil den ikke vises.

App-pakke

Med App Bundles kan du definere grupper av apper som kan tilordnes enhets- eller gruppeprofiler med ett klikk.



Klikk på "+" for å opprette en ny app-pakke. Når du har opprettet en app-pakke, kan du klikke på "Rediger" for å legge til apper fra ulike kilder i pakken.

En pakke kan legges til i profiler som alle andre apper. Når du legger til apper, får du en ekstra fane som heter "App Bundles", der du har dine Bundles.

Hvis du gjør endringer i en App Bundle, vises en knapp i kolonnen "Deploy". Da kan du pushe endringene til alle profiler som inneholder denne pakken. Husk derfor at du må gjøre dette manuelt etter at du har lagt til eller fjernet apper i en pakke.

Fjernkontroll

TeamViewer

TeamViewer Connector

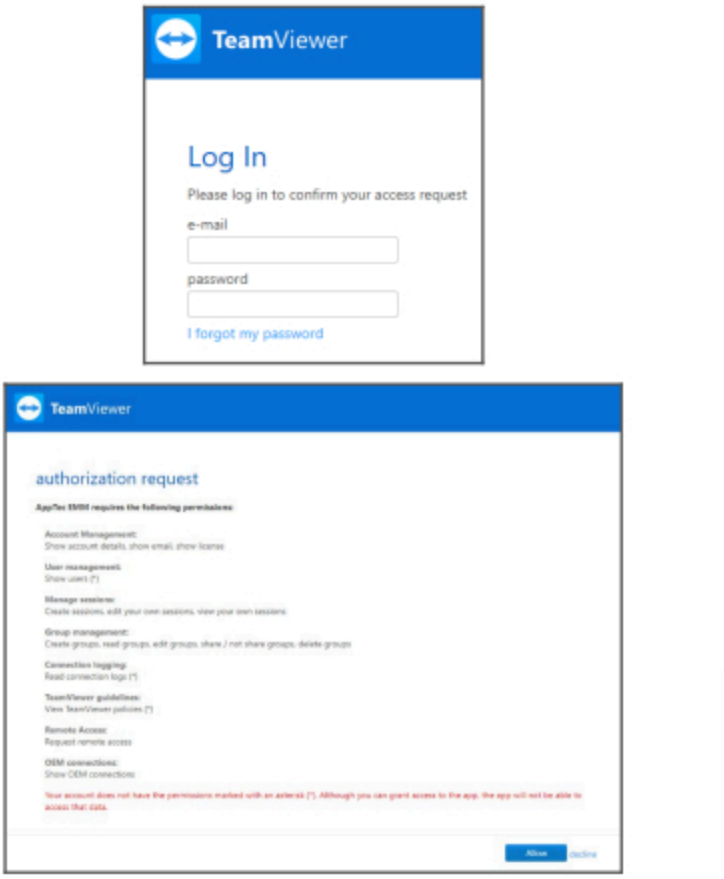
Merk: I den gratis prøveversjonen av skyversjonen vår kan du ikke koble til TeamViewer-kontoen din. Du får i stedet automatisk koblet til en gratis demokonto.

Gå til Generelle innstillinger -> Fjernkontroll -> TeamViewer. Her kan du koble TeamViewer-kontoen din til konsollen eller se informasjon om kontoen du har koblet til. Du kan også se alle aktive økter hvis du går til "Active Sessions".

Klikk på "Start oppsett" for å koble kontoen din.

Hvis du gjør det, kommer du til en ny side der du må logge inn med TeamViewer-kontoen din.

Etter at du har logget inn, må du autorisere AppTec360 MDM til å bruke denne kontoen. Etter at du har bekreftet dette, må du vente noen sekunder, og kontoen er tilkoblet.


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

Installer TeamViewer QuickSupport

Legg til appen "TeamViewer QuickSupport" i de obligatoriske appene i enhetsprofilen eller gruppeprofilen din, og klikk på "Assign Now". Vent til appen er installert på enheten.

Hvis du prøver å få tilgang til en enhet der appen ikke er installert, blir den installert, eller du blir bedt om å installere den, avhengig av enhetens konfigurasjon.

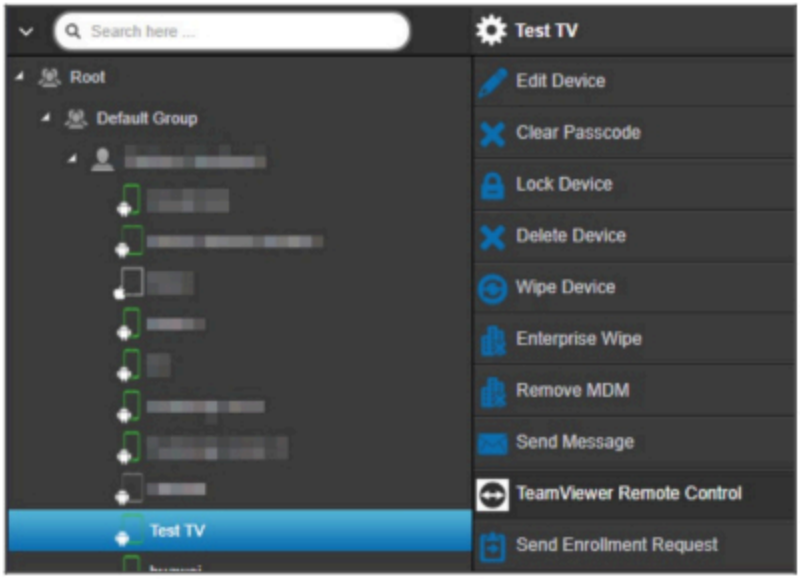
Fjernstyr enheten din

For å fjernstyre enheten velger du enheten, klikker på hjulet og velger "TeamViewer Remote Control"

Hvis det allerede finnes en aktiv økt, kan du enten bruke den gamle økten eller opprette en ny.

Bekreft at du vil opprette en ny TeamViewer-økt.

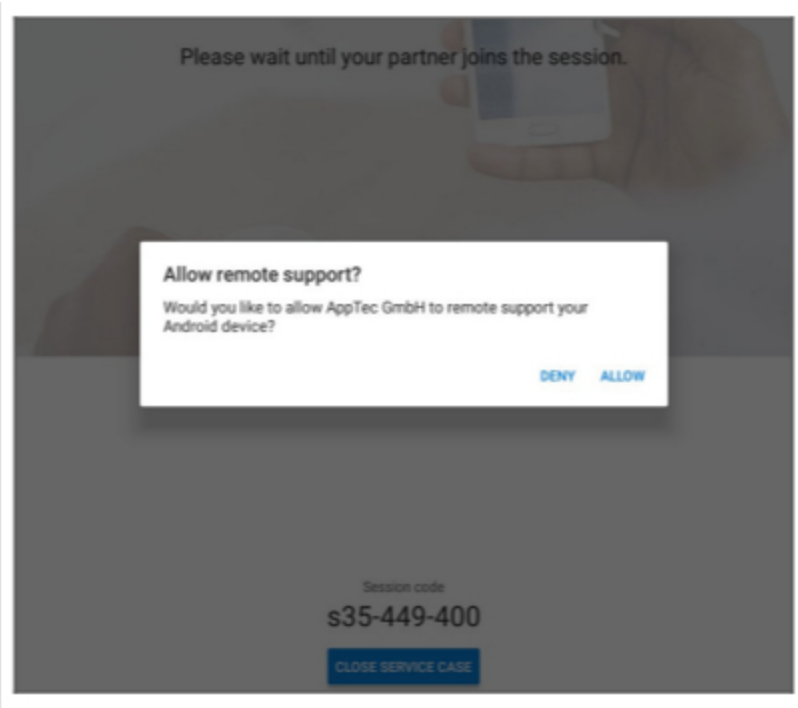
Etter noen sekunder får du opp en lenke til TeamViewer-økten din. Du kan klikke på "Start" for å åpne denne lenken i et nytt vindu.


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

Denne koblingen åpner den installerte TeamViewer-enheten og kobler deg til enheten din.

Nå må du bekrefte tilkoblingen på selve enheten for å fjernstyre den.

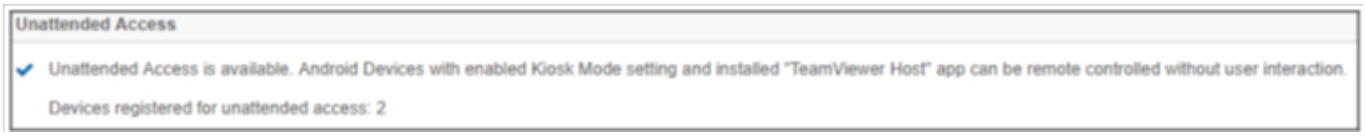


Hvis du bruker iOS, vil du få en melding i AppTec360 MDM Client. Med den koblingen vil enheten bli med i den eksterne økten. Avhengig av varslingsinnstillingene på enheten er det mulig at du ikke vil motta en melding og må åpne AppTec360 MDM Client manuelt.

På noen Android-enheter (f.eks. Samsung) er det nødvendig å installere en ekstra app som tillegg. TeamViewer-appen på enheten vil informere deg om dette, hvis det er nødvendig på din enhet.

Uovervåket tilgang

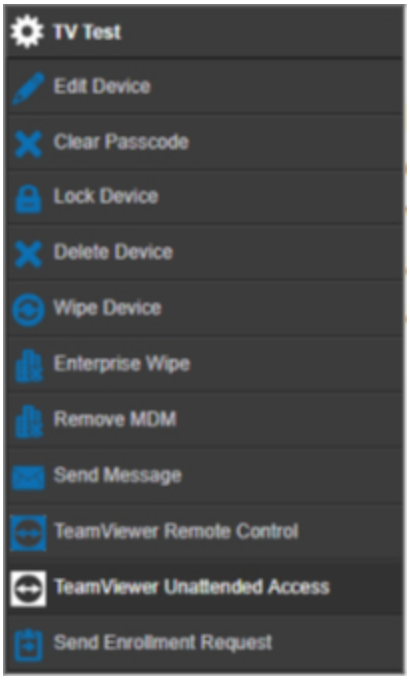
Merk: Uovervåket tilgang er bare mulig på Android-enheter.



Du kan bare koble til enhetene dine, uten å godta tilkoblingen på enheten, hvis TeamViewer-kontoen din bruker en "Tensor"- eller "Corporate"-lisens.

Du kan sjekke dette i "Generelle innstillinger" etter at du har koblet til kontoen din

For å bruke uovervåket tilgang må du installere appen "TeamViewer Host" og aktivere "Enable Unattended Access" under "Kiosk Mode & Launcher" i profilen din. Vær oppmerksom på at dette bare er mulig hvis du bruker kioskmodus.



Nå kan du velge uovervåket tilgang hvis du velger enheten din og klikker på hjulet. Dette vil koble deg til enheten din uten at du trenger å bekrefte det på selve enheten. Vær oppmerksom på at det kan ta noen øyeblikk før du får koblingen for å få tilgang til enheten din.

Splashtop

Hvis du aktiverer Splashtop-alternativet, vil du se konfigurasjonsalternativene for Splashtop i profilene dine.

For å bruke Splashtop må du angi Splashtop Streamer (com.splashtop.streamer.csrs) som obligatorisk app i profilen din. Deretter kan du aktivere Splashtop-konfigurasjonen i profilen din under "Fjernkontroll". Hvis du aktiverer dette, konfigureres Splashtop Streamer-appen. Hvis du bruker Splashtop Streamer, men ikke i kombinasjon med MDM, bør du la denne være av.

I profilen din under "Remote Control" må du også angi en distribusjonskode. Gå til https://my.splashtop.com og logg inn på Splashtop-kontoen din. Klikk på "Add Computer" og kopier den 12-sifrede distribusjonskoden fra den resulterende siden.

Uten Deploy Code er det IKKE mulig med fjernkontroll.

Deretter kan du høyreklikke på enheten og starte en ekstern økt ved å klikke på "Splashtop Remote Control"

Sim-kortadministrasjon

CSV-masseimport

Dette viser en oversikt over de tildelte simkortene dine og all informasjon om dem. Dette hjelper deg med å ha all informasjon, ikke bare om enhetene dine, men også om simkortene dine i ett og samme system.

MERK! Dette er en manuell håndtering/dokumentasjon. Det er ikke mulig å hente disse dataene automatisk fra enheter på grunn av personvern-/sikkerhetsmekanismer i operativsystemene.

Du kan også importere denne listen som CSV-fil.

Transportør og tariff

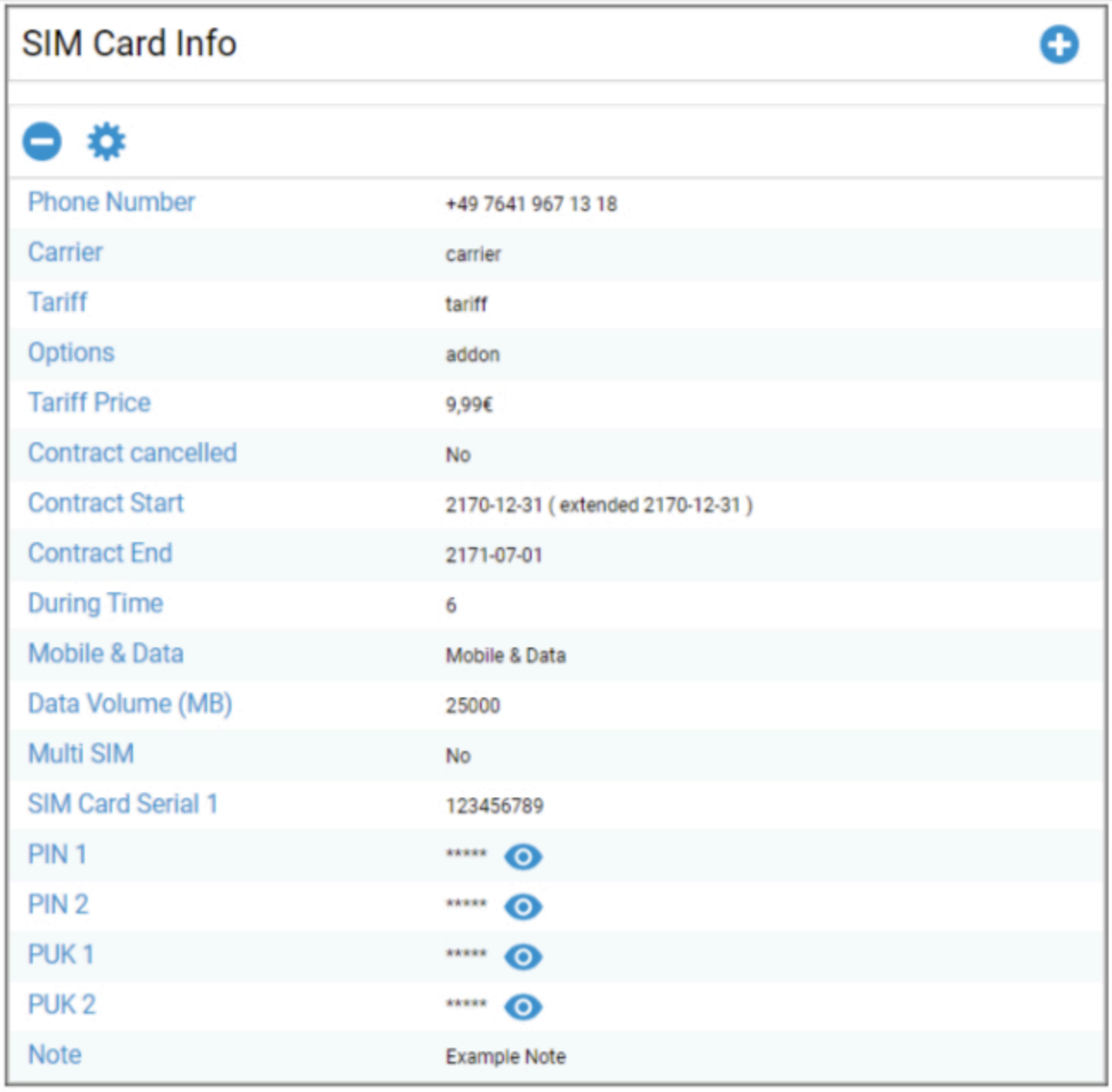
For å legge til et sim-kort klikker du først på knappen for å legge til én eller flere operatører.

Deretter klikker du på "+" på "Tariffinformasjon" for å legge til en tariff til en transportør.

Du kan eventuelt legge til valgfrie tillegg nedenfor hvis du har noe lignende.

Dette forbereder alt du trenger for å legge til et faktisk sim-kort. Sim-kort er for øyeblikket tilordnet en bruker. Gå derfor til Mobile Management, velg en bruker og gå til "Sim-kortoversikt".

Her ser du simkortene til denne brukeren. Hvis det finnes ett, kan du redigere eller fjerne det. Brukere kan ha flere sim-kort.

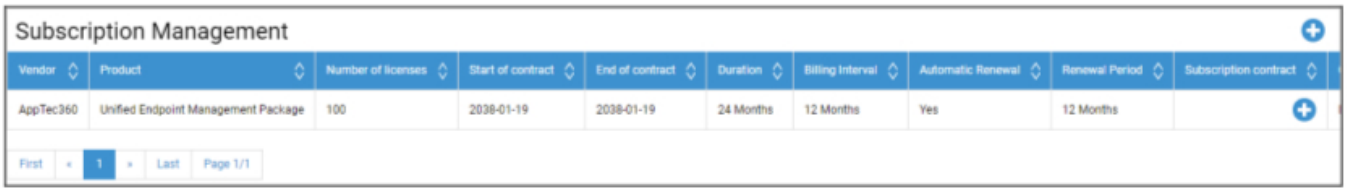


Klikk på "+" for å legge til et SIM-kort, og legg til all informasjonen du trenger. Disse simkortene vil også vises i listen over alle simkortene dine i Generelle innstillinger → Simkortadministrasjon.

Abonnementshåndtering

Abonnementshåndtering

Her kan du dokumentere løpende abonnementer, deres detaljer og også lagre ulike filer, f.eks. signert kontrakt, oppsigelsesbrev osv. Du kan også sette opp påminnelser som minner deg per e-post før abonnementet avsluttes og kanskje forlenges automatisk.



Klikk på "+" øverst for å legge til et abonnement. Du kan legge til så mange abonnementer du vil.

Klikk på "+" i de ulike feltene for å laste opp filer som gjelder dette abonnementet. Du kan laste opp alle filtyper, men vær oppmerksom på at ikke alle filtyper kan forhåndsvises i nettleseren.

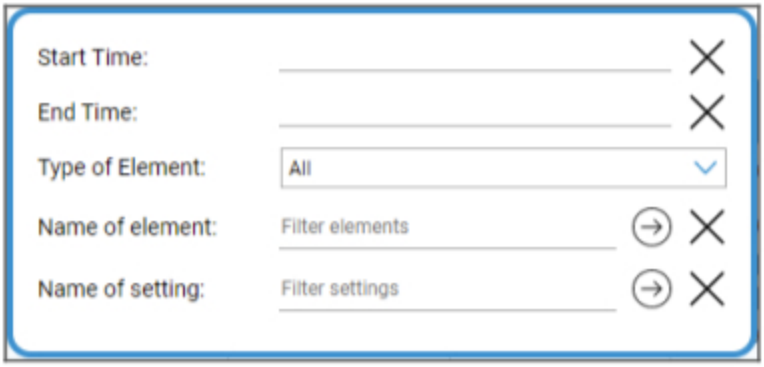
Generell revisjonslogg

Revisjonslogg

Her har du en generell revisjonslogg som viser alle endringer som er gjort. Mens revisjonsloggen for en bruker eller gruppe bare viser endringer som gjelder denne brukeren eller gruppen, viser denne ALLE endringer som er gjort hvor som helst i konsollen.

Du kan se hva som er endret, av hvem, når og hvor. I noen tilfeller kan du også utvide oppføringen for å se flere detaljer.

Det er mulig å klikke på brukeren eller på oppføringen i "Path / Type" for å komme til stedet der endringen er gjort.



Øverst til høyre kan du også definere et filter som kan hjelpe deg med å finne bestemte endringer i et miljø der det skjer mange endringer.

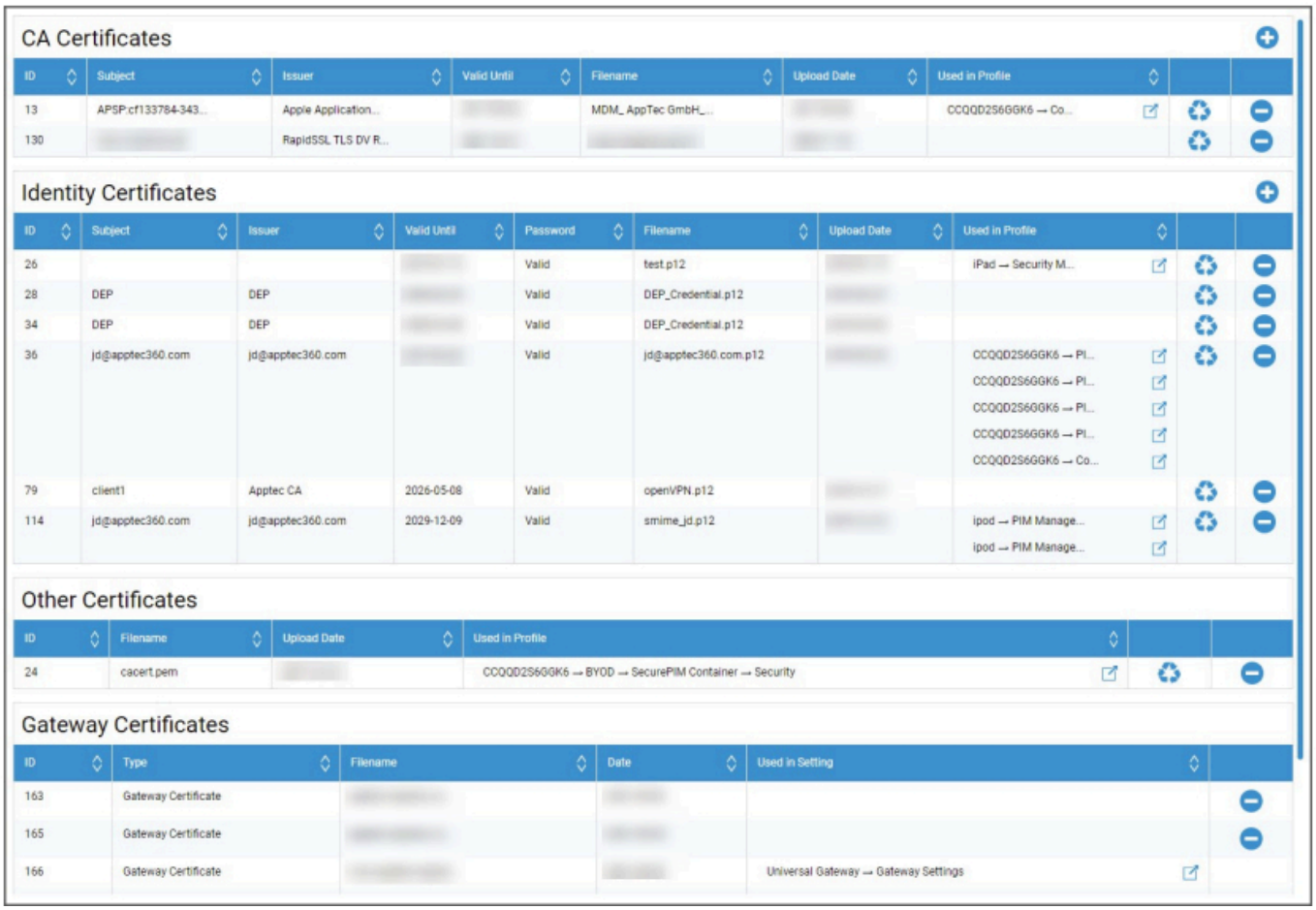
Innstillinger for revisjonslogg

"Oppbevaringsperiode for revisjonslogger" definerer hvor lenge revisjonsloggene skal oppbevares før de slettes.

Sertifikatforvaltning

Her får du en oversikt over alle sertifikater som er lastet opp og brukt i konsollen. Dette er bare en oversikt. Den faktiske konfigurasjonen for f.eks. Wi-Fi-sertifikater gjøres fortsatt i profilen på det tilsvarende stedet.

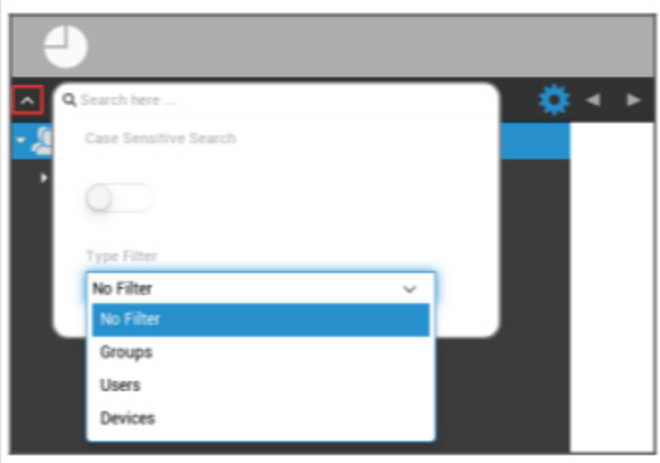
Her kan du også fjerne eller oppdatere sertifikater, noe som automatisk vil gjenspeiles i de berørte profilene. Klikk på informasjonen i "Brukes i profil" for å se nøyaktig hvor et sertifikat fortsatt er tilordnet.



Mobil administrasjon

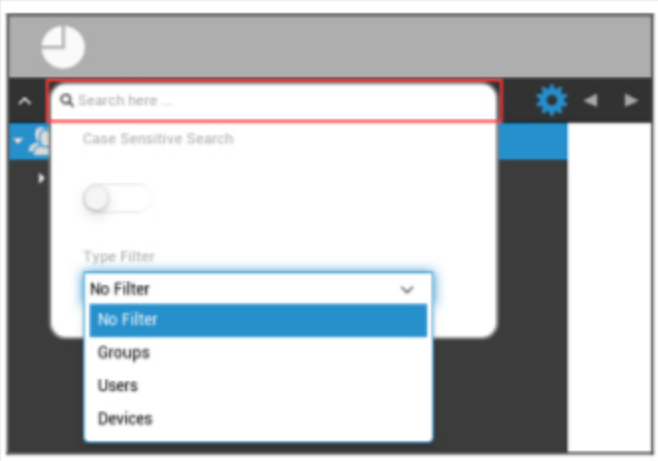
Skjermbilde for mobiladministrasjon

Enhetsfilter



Ved å klikke øverst i venstre hjørne av skjermen finner du en rekke filtre for visning av enheter.

Søkevindu



I søkevinduet kan du søke etter alle enheter og/eller brukere med et bestemt søkeord.

Alternativt utstyr

Når du har klikket på det aktuelle symbolet, vises en liste over tilgjengelige alternativer.

Disse endres for hvert gjeldende vindu og forklares i de respektive kapitlene.

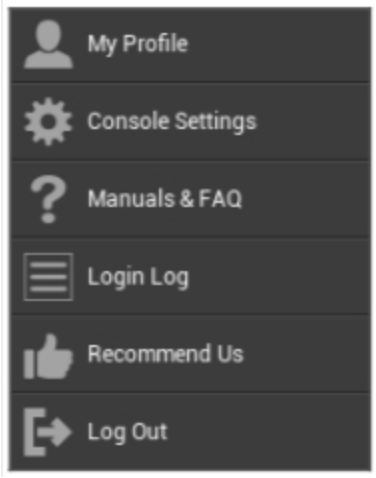
Navigasjonspiler

Ved å klikke på pilen til venstre kommer du til forrige side.

Etterpå, ved å klikke på høyre pil, kommer du tilbake til siden du nettopp forlot.

Administrasjon kontoinnstillinger

Hvis du klikker på e-postadressen som vist ovenfor, vises følgende meny:



Min profil	Rediger kontoopplysningene til administratorene
Konsollinnstillinger	Konfigurere konsollinnstillinger for Admins-kontoen
Håndbøker og vanlige spørsmål	Se siden "Manualer og vanlige spørsmål" i "Generelle innstillinger"
Innloggingslogg	Få tilgang til "Påloggingsloggen"
Anbefal oss	Se siden "Anbefal oss" under "Generelle innstillinger"
Logg ut	Logg ut av MDM-konsollen

Brukerinformasjon

Her kan du redigere kontoopplysningene til den påloggede administratoren.

Brukernavn	Brukernavn og/eller e-postadresse for kontoen
Navn	Administratorens fornavn
Etternavn	Administratorens etternavn
Innloggingsnavn	Innloggingsnavn for administratorer
E-postadresse	Administratorens e-postadresse
Alternativ e-postadresse	Administratorens alternative e-postadresse
Bilde	Profilbilde
Telefonnummer	Administratorens telefonnummer
Mobilnummer	Administratorens mobilnummer
Telefontilknytning	Telefontillegg
Beliggenhet	Beliggenhet
Stilling	Stilling i selskapet
Brukergruppe	Velg hvilken brukergruppe du vil tilordne administratorkontoen til
Kommentar	Skriv inn en kommentar
Skriv inn nytt passord	Skriv inn passordet for endring av passord
Gjenta nytt passord	Gjenta det nye passordet for å bekrefte

Vær oppmerksom på at administrasjonstilgangen også kan arkiveres som en lokal brukerkonto i hierarkistrukturen. Denne bør ikke slettes uten at det opprettes en ekstra administrator!

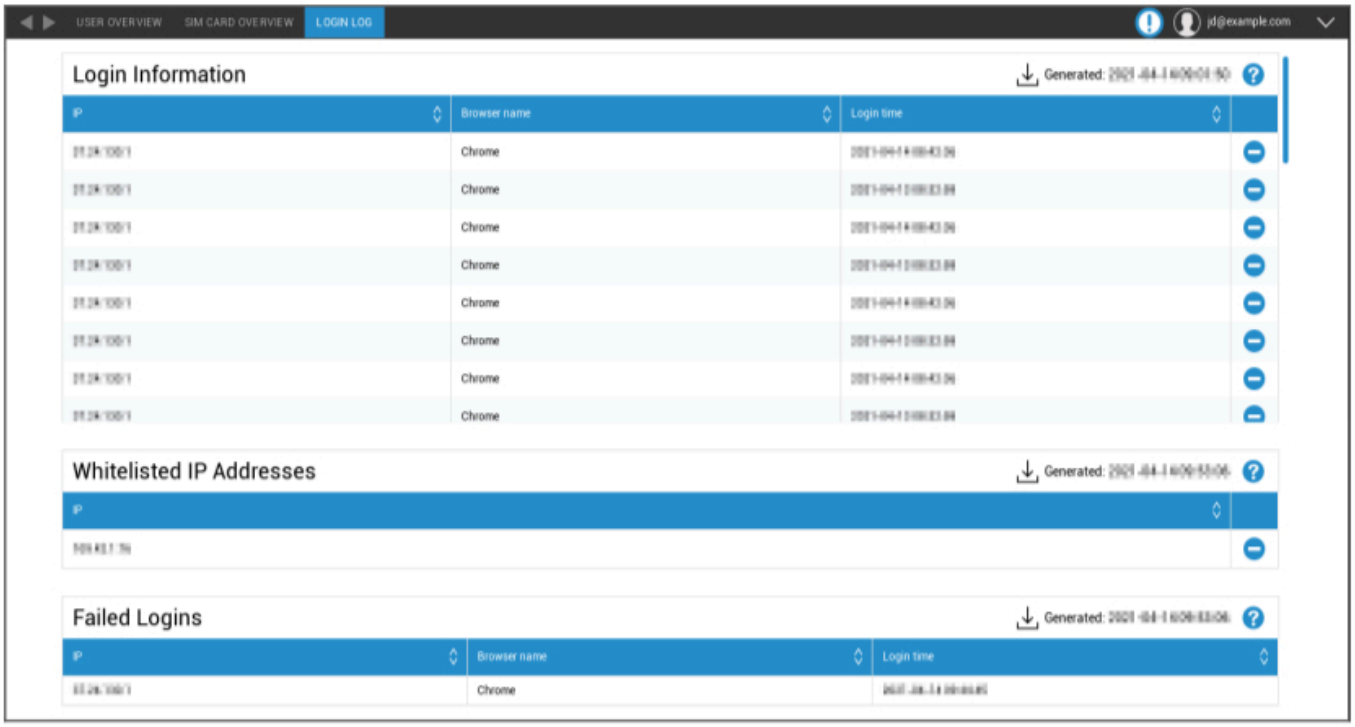
Konsollinnstillinger

Her kan du konfigurere følgende konsollinnstillinger for Admins-kontoen:

Alternativer for visning av katalogbruker	Definer hvordan brukere skal merkes i treet
Alternativer for visning av katalogenheter	Definer hvordan enheter skal merkes i treet
Tidsavbrudd for økten	Hvis brukeren ikke gjør noe i løpet av den angitte tiden, blir brukeren logget ut. Standardverdien er 60 minutter. Vennligst logg ut og logg på igjen etter at du har endret denne innstillingen.
Tidssone	Velg tidssonen som skal brukes
Tidsformat	Velg hvordan tidsstempler skal vises
Konsollspråk	Velg hvilket språk konsollen skal vises på. Engelsk og tysk er tilgjengelig.
Hovedfarge	Du kan angi en farge som skal brukes som base for konsollets fargeskjema. Du kan enten bruke fargevelgeren eller angi en farge i HTML HEX-notasjon. RGB-formatorer som 'rosa', 'gul' fungerer også.
Lagre kommando	Tastekombinasjonen for å utløse en lagring uten å trykke på "Lagre"-knappen.
Bruk tofaktorautentisering	Aktiver bruk av tofaktorautentisering ved pålogging. Du vil motta en e-post ved innlogging med en kode som du må oppgi for å logge inn.
Tidsavbrudd for tofaktorautentisering	Angi en tidsperiode hvor du ikke vil bli bedt om tofaktorautentisering etter en allerede vellykket autentisering.
Send bekreftelseskode via	Bekreftelseskoden sendes til de valgte alternativene. Enhetsmeldingen vises i AppTec360 MDM-appen på alle Android- og iOS-enheter som tilhører deg.
Send innloggingsmelding etter innlogging	Hvis denne funksjonen er aktivert, sendes det en e-post for hver pålogging fra en ip-adresse som ikke er hvitelistet. E-posten inneholder informasjon om påloggingen (f.eks. IP, nettleser).

Innloggingslogg

Her kan du se informasjon om innloggingene til den administratorkontoen som er logget på.



Innloggingsinformasjon	En liste som inneholder påloggingene til den innloggede administratorkontoen som ble registrert av konsollen. Denne listen viser alle vellykkede påloggingen de siste 30 dagene.
Hvitelistede IP-adresser	Dette er listen over alle IP-adressene du har hvitelistet. Hvis du logger inn fra en IP som er oppført her, vil du ikke få innloggingsmeldingen. Du kan legge til en IP-adresse i denne listen ved å klikke på knappen ved siden av en oppføring i listen "Påloggingsinformasjon" ovenfor. Du kan fjerne en IP-adresse fra denne listen ved å klikke på knappen ved siden av en oppføring i denne listen eller i listen "Påloggingsinformasjon" ovenfor.
Mislykkede påloggingen	Dette er en liste over alle mislykkede påloggingsforsøk de siste 30 dagene. Hvis du ikke har tastet inn riktig passord minst tre ganger i løpet av 20 minutter, vises en oppføring i denne listen. Du vil også bli informert om mislykkede påloggingsforsøk via e-post.

Bedriftsadministrasjon (Root-Node) i Mobile Management

Når du har kommet til Root-Node (første gruppe), kan du utføre en rekke innstillinger for bedriften din med hensyn til Mobile Management.

Opprett en undergruppe	Opprett en undergruppe
Gi nytt navn til rotnoden	Endre navn på rotnoden (f.eks. firmanavnet ditt)
Masseinnrullering	Registrer flere enheter/brukere samtidig
Masseoppdrag	Tilordne en profil for de respektive gruppene, med ett blikk
Rask appadministrasjon	Sende (av)installasjonsforespørsler for en applikasjon til de respektive gruppene av enheter
CSV-brukerimport	Importer brukere fra CSV til den respektive gruppen

Opprett en undergruppe

Med "Opprett en undergruppe" kan du opprette en ekstra undergruppe.

Du kan bestemme hvilken gruppe undergruppen skal tilordnes.

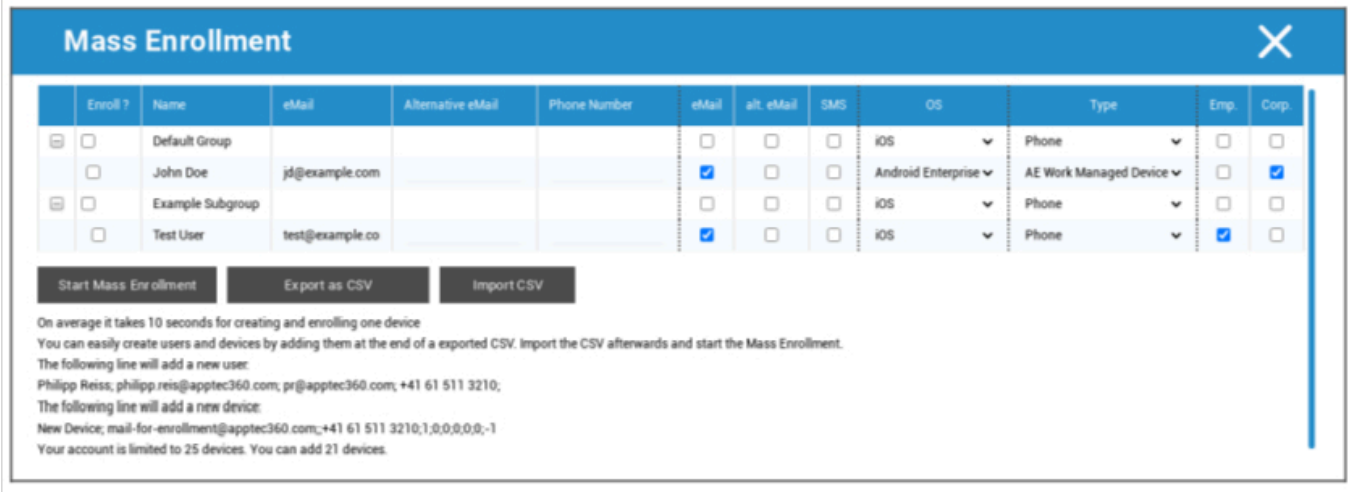
(Som standard opprettes en ny gruppe som tildeles som en undergruppe i rotnoden)

Gi nytt navn til rotnoden

Her kan du endre navn på rotnavnet ditt. Det er vanlig at firmanavnet brukes i dette tilfellet.

Masseinnrullering

Med "Mass Enrollment" kan du registrere flere enheter og brukere.



Du kan velge direkte på hvilken måte brukeren skal motta påmeldingen (e-post; alternativ e-post; SMS)

Avhengig av hvilken enhet brukeren skal motta (iOS, Android, Windows Phone), kan du markere det direkte her.

Her kan du også konfigurere om det er en smarttelefon eller et nettbrett, som du må velge riktig med en hake.

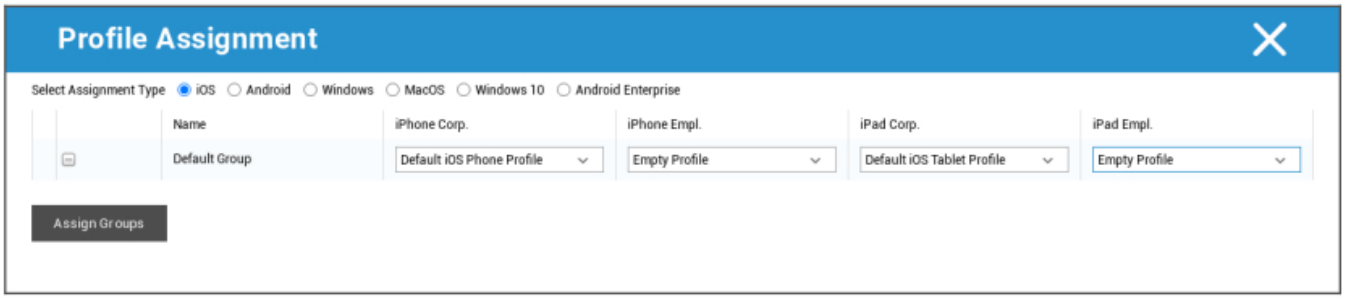
Som et siste trinn kan du fastslå om den aktuelle enheten er en bedriftsenhet eller en privat enhet (BYOD).

Med "Eksporter som CSV" kan du eksportere informasjonen som en CSV-datafil. Til gjengjeld kan du også importere CSV-datafilen med "Importer CSV", og filen skal se ut som i eksemplet nedenfor:

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

Masseoppdrag

Under Massetildeling kan du tilordne en profil til alle grupper, denne er delt inn i iOS - Android - Windows - MacOS - Windows 10 - Android Enterprise

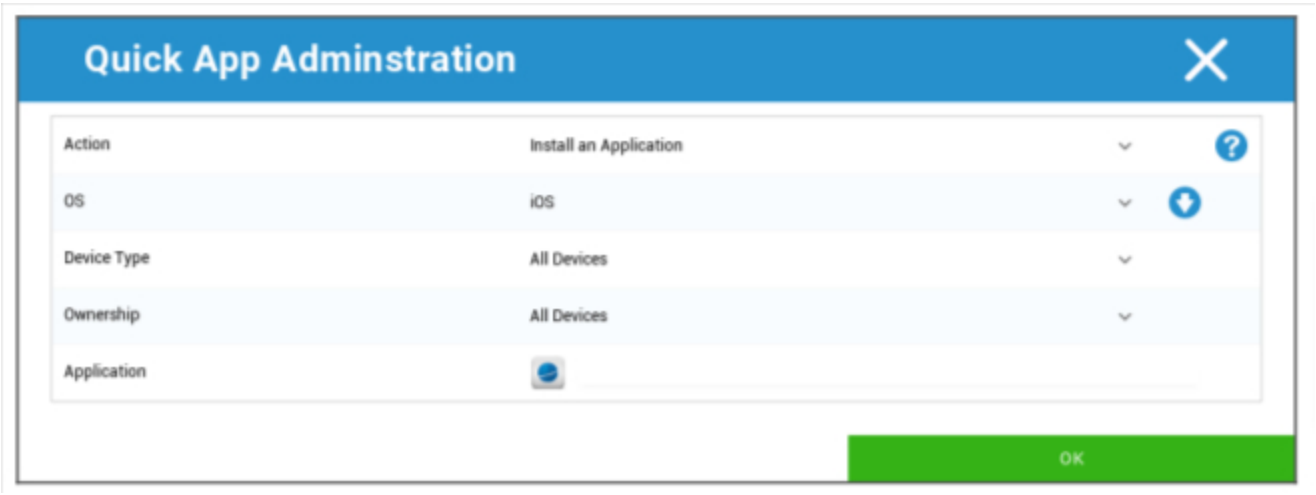


Windows - MacOS - Windows 10 - Android Enterprise

Rask appadministrasjon

Under Quick App Administration kan du sende forespørsler om installasjon eller avinstallasjon av en spesifisert applikasjon til et operativsystem etter eget valg.

Du kan også definere om forespørselen skal sendes til alle enhetstyper i det valgte operativsystemet eller bare til en bestemt enhetstype.



CSV-brukerimport

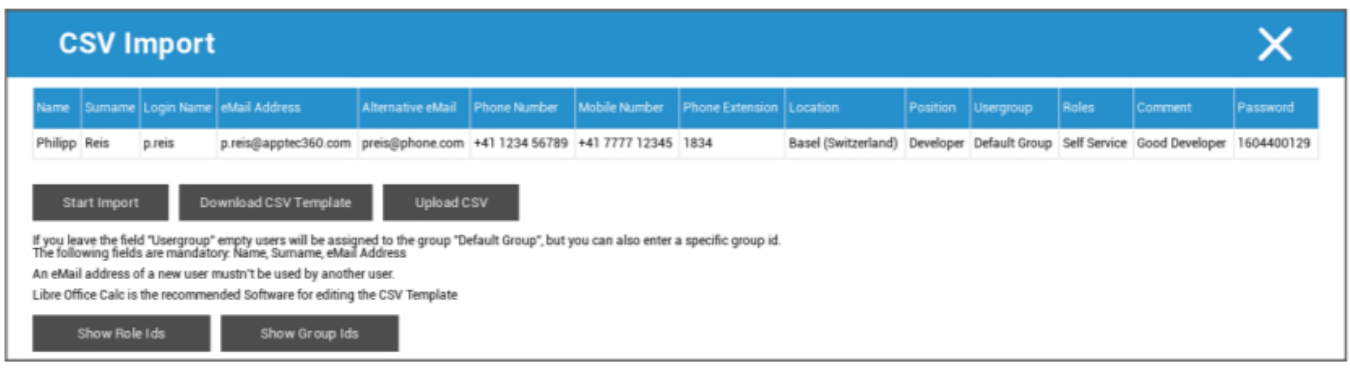
Importer brukere fra CSV til den respektive gruppen.

Med "Last ned CSV-mal" kan du eksportere en CSV-malfil som du kan fylle ut (eller bruke som referanse).

Du kan også bruke alternativene "Vis rolle-ID" og "Vis gruppe-ID" som referanse for å opprette din egen CSV-fil.

CSV-filen kan lastes opp til MDM med "Upload CSV".

Til slutt kan du starte importen ved å klikke på "Start import".



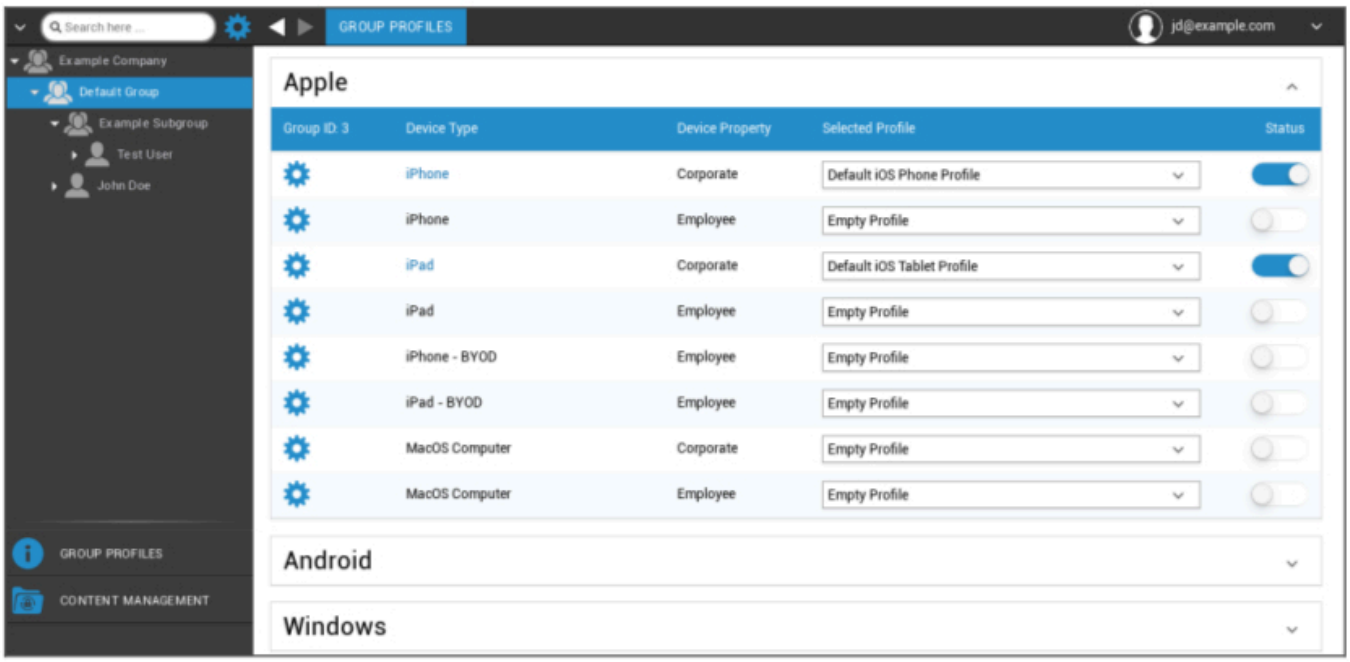
Gruppeledelse i Mobile Management

Ett klikk på oversikten viser de ulike konfigurasjonsprofilene for de respektive plattformene.

En profil inneholder alle innstillingsalternativer som kan etableres med AppTec360 på forhånd på sluttbrukerens enhet. På hver plattform kan du opprette profiler for bedriftsenheter (Corporate) eller Bring-Your-Own-Device-enheter (Employee).

For å kunne differensiere konfigurasjoner for enhetsgrupper, for eksempel basert på plassering eller funksjon, anbefales det at det opprettes flere undergrupper.

Vær oppmerksom på Profilhåndtering i Mobile Management



Med girmenyen kan du angi en rekke innstillinger for den respektive (under)gruppen.

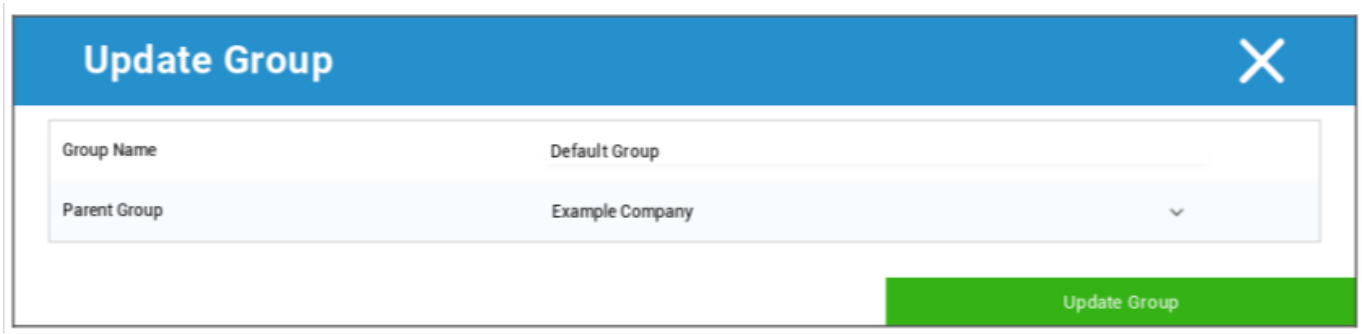
Opprett en undergruppe	Opprett undergruppe for den respektive (under)gruppen
Rediger valgt gruppe	Rediger valgt gruppe
Slett valgt gruppe	Slett valgt gruppe
Masseinnrullering	Registrer mange enheter/brukere samtidig for den valgte profilen
Masseoppdrag	Tilordne profiler til gruppen som er valgt for øyeblikket
Opprett en undergruppe	Opprett undergruppe for den respektive (under)gruppen
Opprett en bruker	Opprett en bruker for den respektive (under)gruppen

Opprett en undergruppe

Med "Opprett en undergruppe" kan du opprette en ekstra undergruppe.

Du kan angi hvilken gruppe undergruppen skal tilordnes (som standard tilordnes undergruppen til den gruppen som er valgt for øyeblikket).

Rediger valgt gruppe



Her kan du redigere profilen - følgende innstillinger er mulige:

- Gruppenavnet kan endres
- Foreldregruppen kan endres

Slett valgt gruppe

Under "Slett valgt gruppe" får du opp en liste over alle brukere og enheter som er i den aktuelle gruppen. Her har du muligheten til å slette dem.

For én bruker kan du utføre følgende slettekommandoer:

Slett bruker	Brukeren er slettet
Flytt bruker til gruppe:	Du kan flytte brukeren til en annen gruppe (følgende kolonne, f.eks. "Admins")

For én enhet kan du utføre følgende slettekommandoer:

Tørk og slett	Tørk og slett enheten
Slett fra System	Fjern kun enheten fra AppTec

Referanse: Masseinnrullering

Referanse: Masseoppdrag

Opprett en bruker

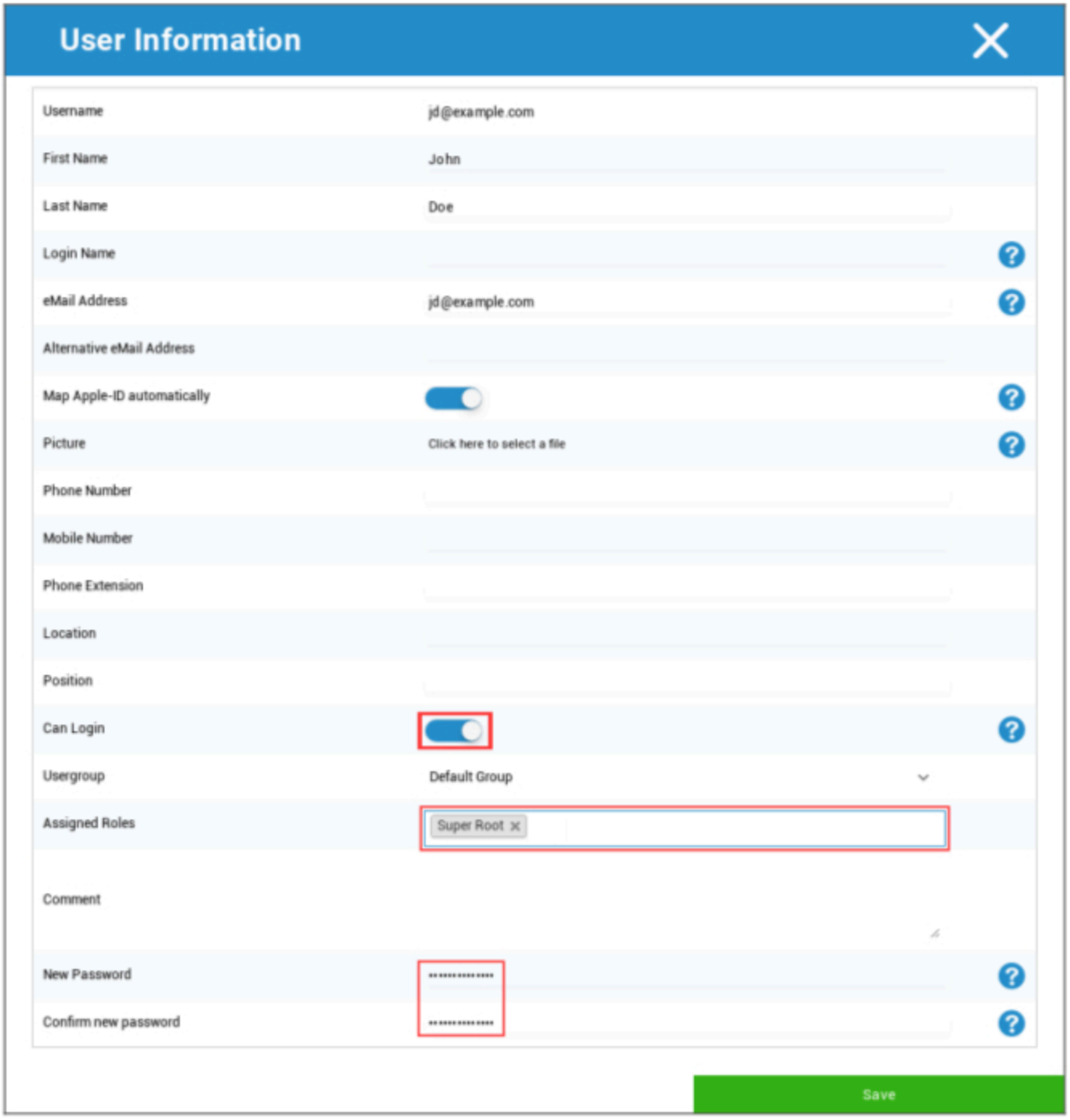
Med "Create a User" kan du legge til en ny bruker.

Opprett en ny administratorbruker

Du kan angi en bruker som Admin-bruker. Da får han/hun rettigheter til å logge inn på konsollen og endre brukere/grupper/enheter.

Opprett en vanlig bruker eller bruk en eksisterende bruker. Velg den brukeren du vil gi administratorrettigheter, klikk på hjulet og velg "Rediger bruker":

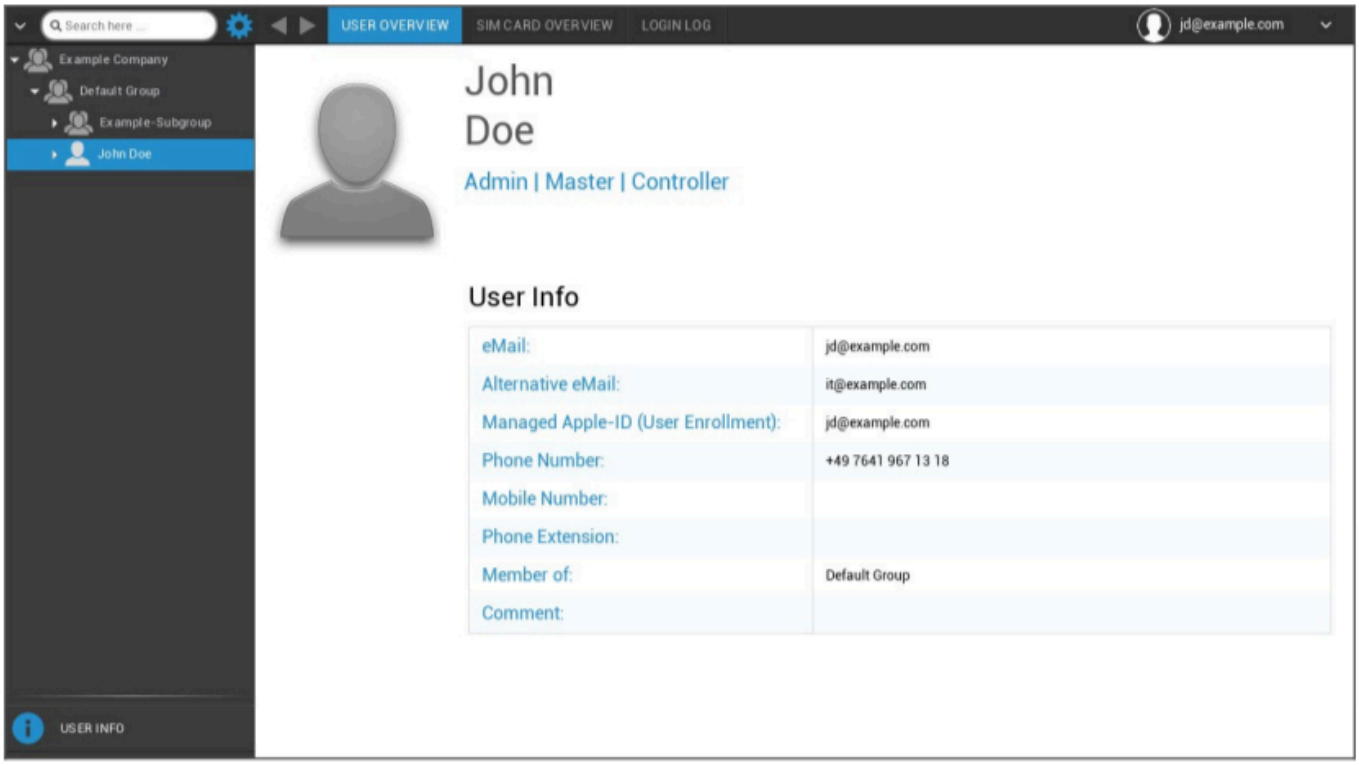
Aktiver bryteren for "Kan logge inn", tildel brukeren rollen "Super-Root" og angi et passord.



Lagre dette, og brukeren kan nå logge inn med brukernavn og passord.

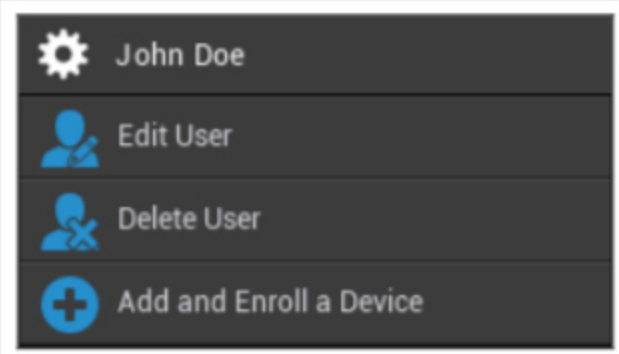
Brukeradministrasjon i Mobile Management

Når du velger en bestemt bruker, ser du følgende oversikt:



Du får en oversikt over all informasjonen du har lagt inn tidligere i "Opprett en bruker".

Med utstyret som er installert øverst, kan du utføre følgende konfigurasjoner:



Brukernavn	Brukernavn på valgt bruker
Rediger bruker	Rediger brukerinformasjon
Slett bruker	Slett bruker • Delete from System = Enheten vil bli fjernet fra AppTec

	• Wipe & Delete = Enheten gjenopprettes til fabrikkinnstillingene og fjernes fra AppTec
Legg til og registrer en enhet	Registrer en enhet for den valgte brukeren

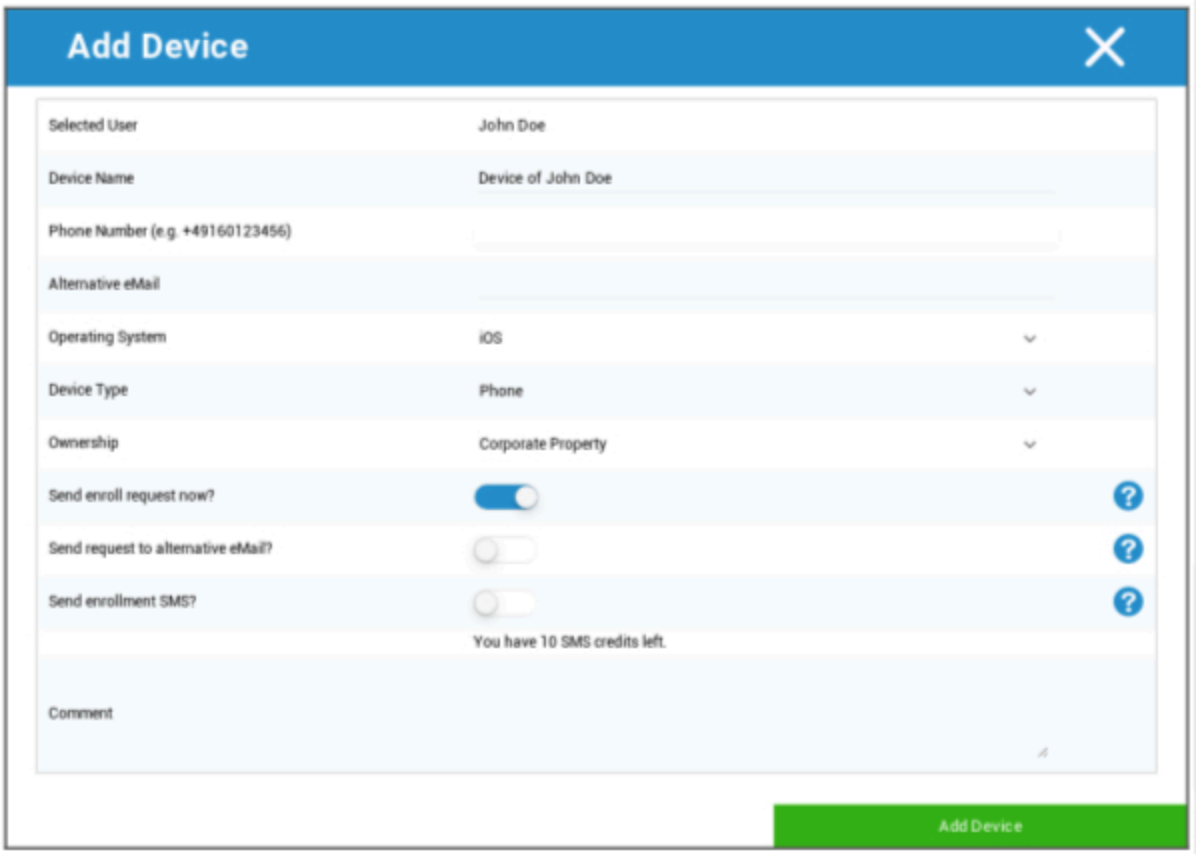
Vær oppmerksom på at administrasjonstilgangen også kan arkiveres som en lokal brukerkonto i hierarkistrukturen. Denne bør ikke slettes uten at det opprettes en ekstra administrator!

Legg til og registrer en enhet

Her kan du velge en enhet for den valgte bruken.

Alternativt kan du registrere enheter i en gruppe direkte. Dette gjør du ved å klikke på gruppen, klikke på hjulet og velge "Legg til og registrer en enhet".

Du bør se følgende oversikt:



Avhengig av hvilken type enhet du ønsker å registrere, må du utføre følgende konfigurasjoner:

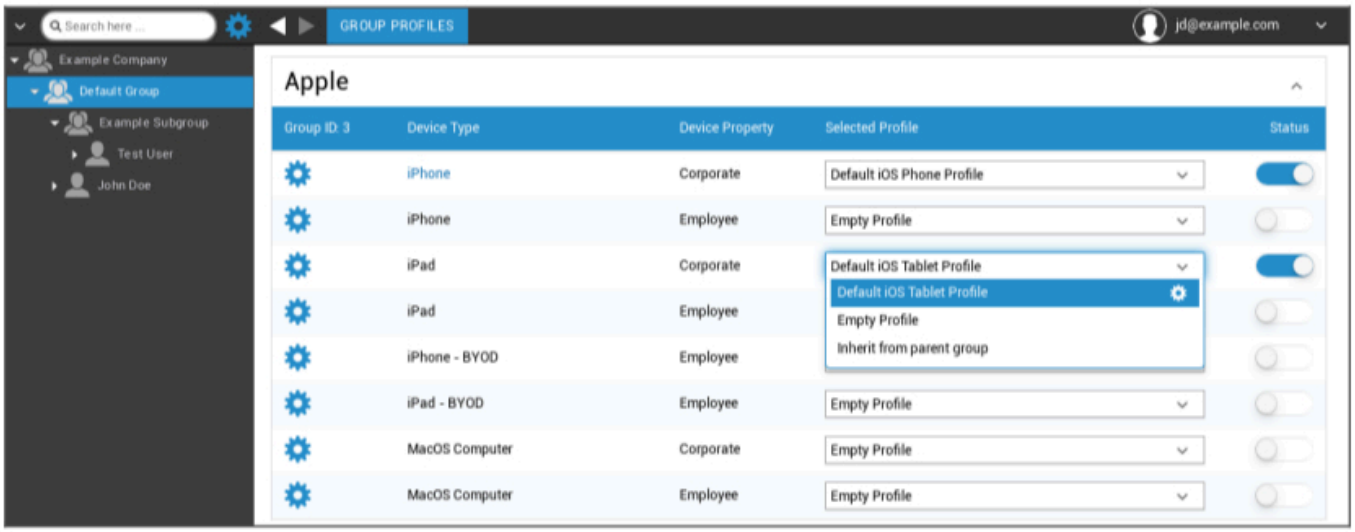
Utvalgt bruker	Valgt bruker (fylles ut automatisk)
Enhetens navn	Blir fylt ut automatisk (enhet for "brukerens navn") - kan imidlertid endres
Telefonnummer	Telefonnummer, fylles ut automatisk (så lenge det er oppgitt av brukeren) - her kan det imidlertid legges til eller endres
Alternativ e-post	Alternativ e-post, fylles ut automatisk (så lenge den er oppgitt av brukeren) - her kan den imidlertid legges til eller endres
Eier av enheten	Bedriftseiendom = bedriftsenhet Ansattes eiendom = BYOD-enhet
Velg driftssystem	Her kan du velge mellom følgende operativsystemer: • iOS • iOS BYOD (brukerregistrering) • MacOS • Android Enterprise • Android • Windows Mobile • Windows 10
Sende innmeldingsforespørsel?	E-posten sendes umiddelbart til hoved-e-postadressen, og brukeren blir bedt om å koble til enheten sin
Send forespørsel til alternativ e-post?	Send e-posten i tillegg eller utelukkende (i tilfelle "Send registreringsforespørsel?" ble deaktivert) til den alternative e-postadressen (e-posten er forskjellig fra den "normale" e-posten for registreringsforespørsel)
Sende innmeldings-SMS?	Send en innmeldingsforespørsel via SMS (telefonnummeret må oppgis)

Etter at registreringsforespørselen er sendt, vil enheten vises (merket med rødt) med en gang.

Så snart enheten har blitt koblet til, vil den kort tid etter bli merket med grønt og er dermed klar til å motta begrensninger, apper osv.

Profilhåndtering i Mobile Management

Når du har klikket på en gruppe, får du opp en oversikt over alle enhetsplattformene som skal konfigureres, og de respektive profilene som er tilordnet.



	Utfør konfigurasjonen for den valgte profilen
Enhetstype	Enhetstype og/eller modell
Enhetsegenskaper	Enhetens eier (Corporate = bedriftseiendom, Employee = privat ansatt-enhet)
Utvalgt profil	Valgt profil (tannhjulet åpner profilens konfigurasjonsdialog)
Status	På/Av (profilen aktiveres/deaktiveres)

Når du velger giret, får du følgende alternativer:

Opprett en profil

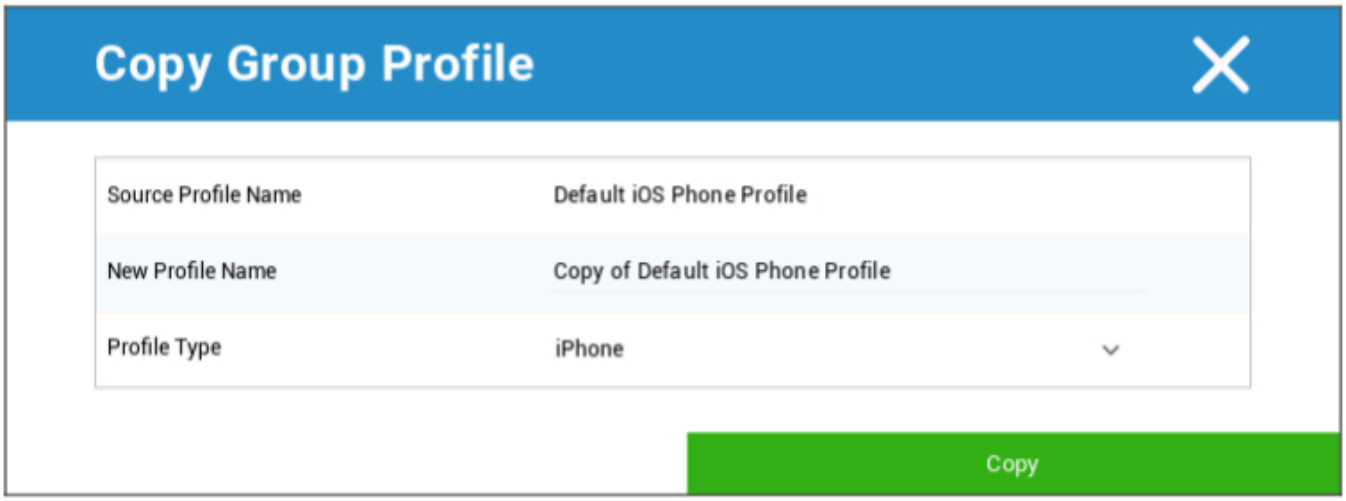
Du kan opprette og konfigurere en ny profil for hver oppføring og/eller plattform. Når du klikker på dette underpunktet, opprettes profilen umiddelbart, og du kan begynne å konfigurere iOS, Android og Windows Phone med en gang.

Rediger profil

Når du har klikket på "Rediger profil", kommer du til konfigurasjonsdisplayet for den aktuelle profilen, der du kan angi konfigurasjonene.

Kopier profil

Ved hjelp av funksjonen "Copy Profile" kan du kopiere oppsett/konfigurasjoner fra en allerede eksisterende profil og legge dem til i en ny profil.

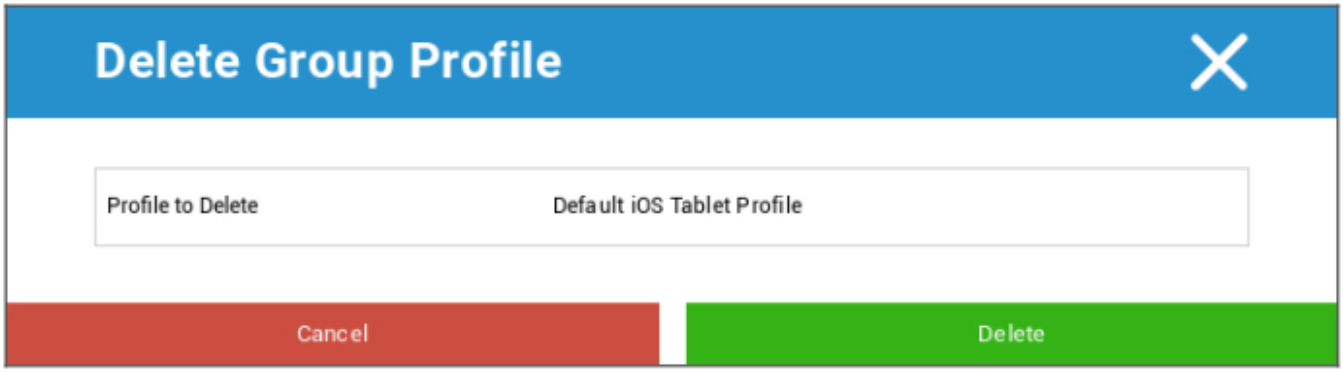


Navn på kildeprofil	Navnet på profilen som skal kopieres
Nytt profilnavn	Navnet på den nye profilen
Profiltype	Profiltype (telefon/nettbrett)

Når du klikker på "Kopier", blir profilen opprettet og kan nå tilordnes gruppen

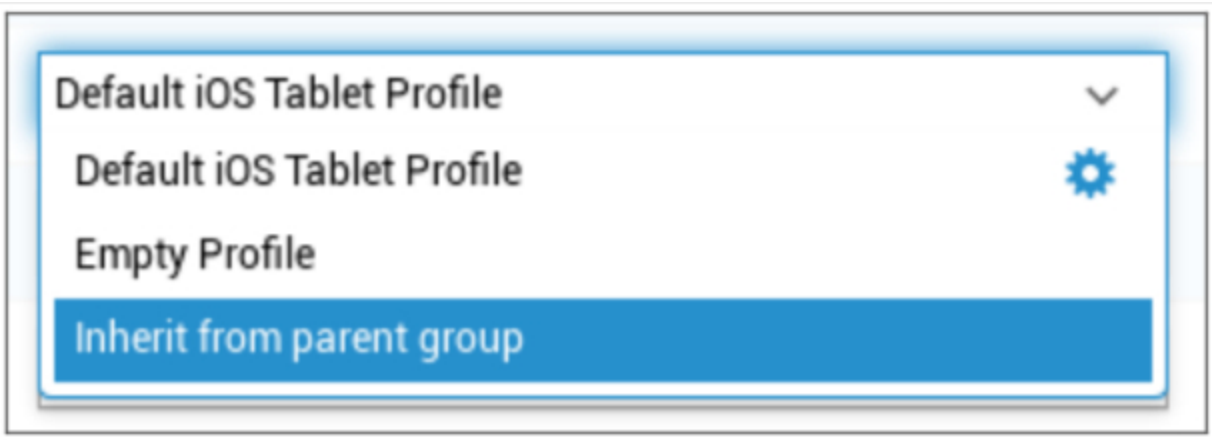
Slett profil

Her kan du slette en profil permanent. Vær oppmerksom på at under sletteprosessen og den påfølgende "Assign Now"-prosessen for profilen, vil konfigurasjonen forsvinne på de respektive enhetene i en berørt gruppe og kan ikke gjenopprettes!


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

Arving av profiler

Når du velger profiler, er alternativet "Arv fra overordnet gruppe" tilgjengelig.



Når profilen aktiveres, vil profilen til den overordnede gruppen brukes for den valgte enheten (og den respektive enhetstypen). Vær også oppmerksom på at endringer i denne profilen kan påvirke flere grupper.

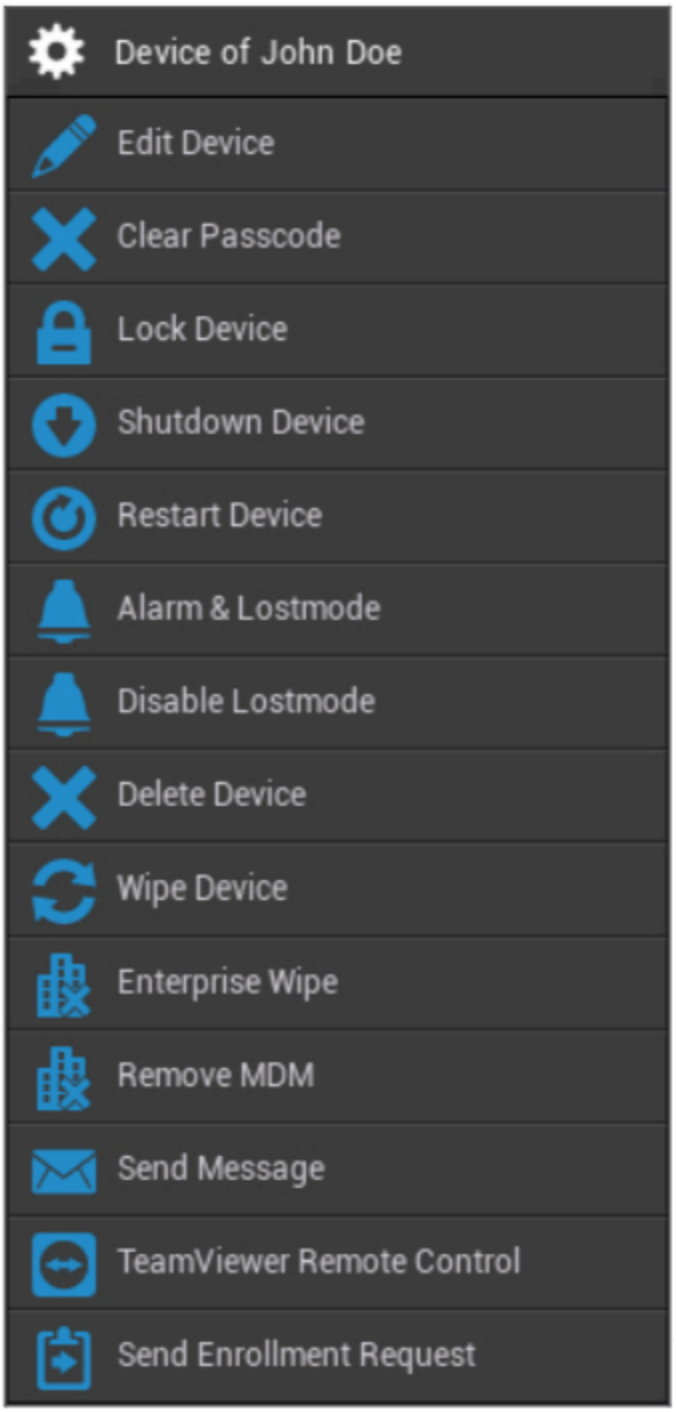
Denne konfigurasjonen settes som standardverdi når en ny undergruppe opprettes.

Konfigurasjonen "Empty Profile" er også tilgjengelig, som tilsvarer en tom profil, noe som betyr at det til slutt ikke vil bli utført noen nye konfigurasjoner på sluttbrukerens enhet.

Enhetsadministrasjon i Mobile Management

Når du velger en enhet, kan du utføre en rekke oppgaver via "tannhjulet". Disse er forskjellige, avhengig av OS-plattformene (iOS, Android Enterprise, Android, Windows Mobile, Windows 10).

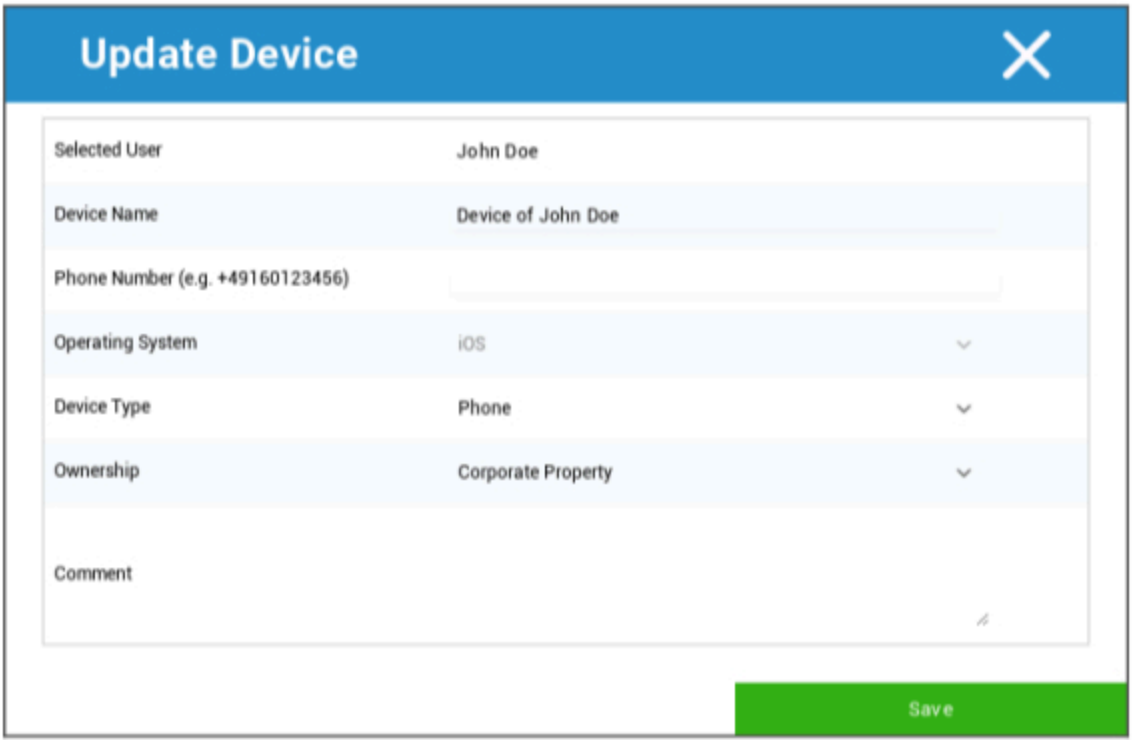
IOS



Rediger enhet	Rediger enhet
Tøm passord	Enhetens passord slettes
Lås enhet	Lås enheten (låseskjerm)
Avstengningsenhet	Avstengningsenhet

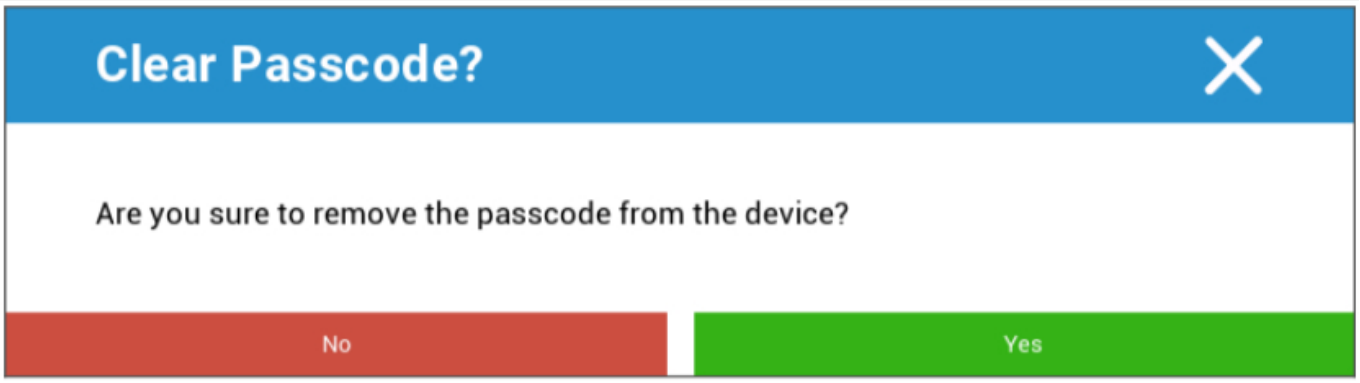
Start enheten på nytt	Start enheten på nytt
Alarm og Lostmode	Startalarm og Lostmode
Deaktiver Lostmode	Deaktiver Lostmode
Slett enhet	Fjern enheten fra AppTec
Tørk av enheten	Gjenopprett enheten til fabrikkinnstillingene
Enterprise Wipe	Informasjonen, appene og profilene som leveres av AppTec360 slettes (enheten skilles fra MDM)
Fjern MDM	
Send melding	Send push-varsler til enheten Meldingen vises i AppTec360-appen (fanen Melding)
TeamViewer fjernkontroll	Start en fjernkontrolløkt ved hjelp av TeamViewer
Send innmeldingsforespørsel	Send (gjentatt) innmeldingsforespørsel

Rediger enhet



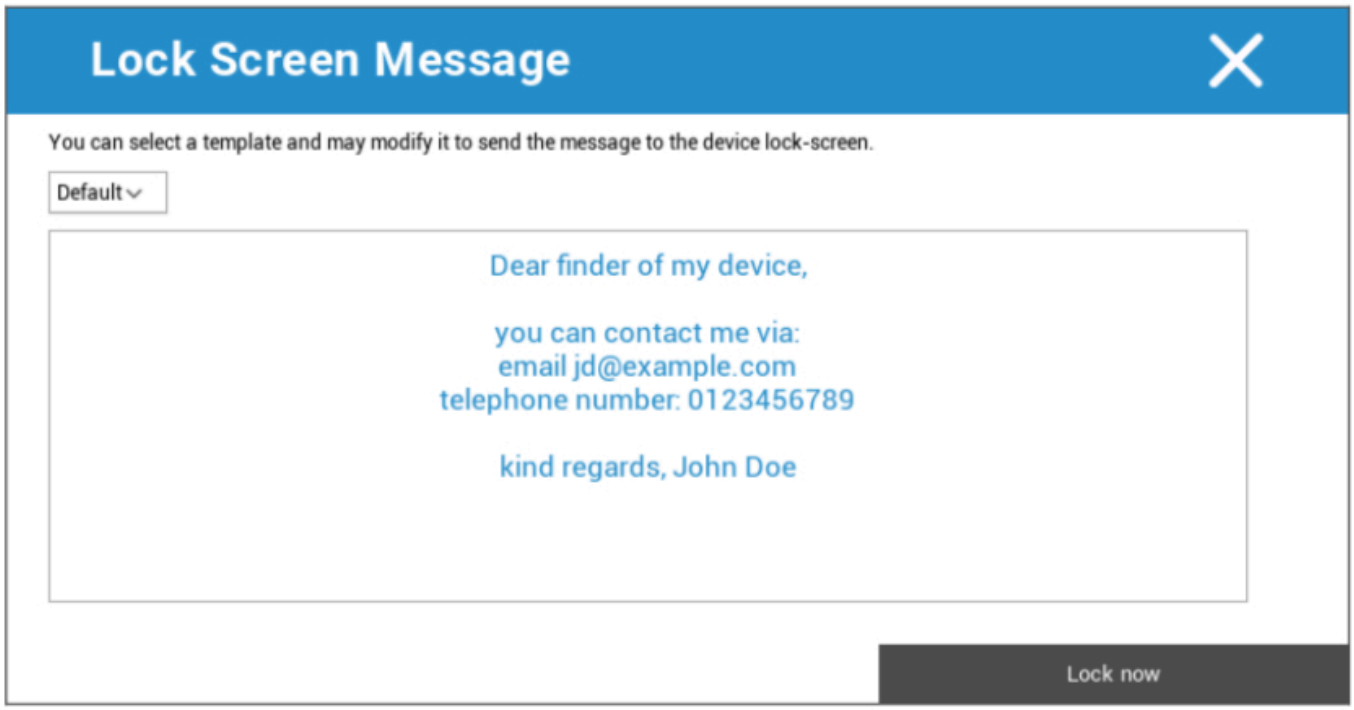
Her kan du oppdatere en rekke opplysninger om enheten.

Tøm passord



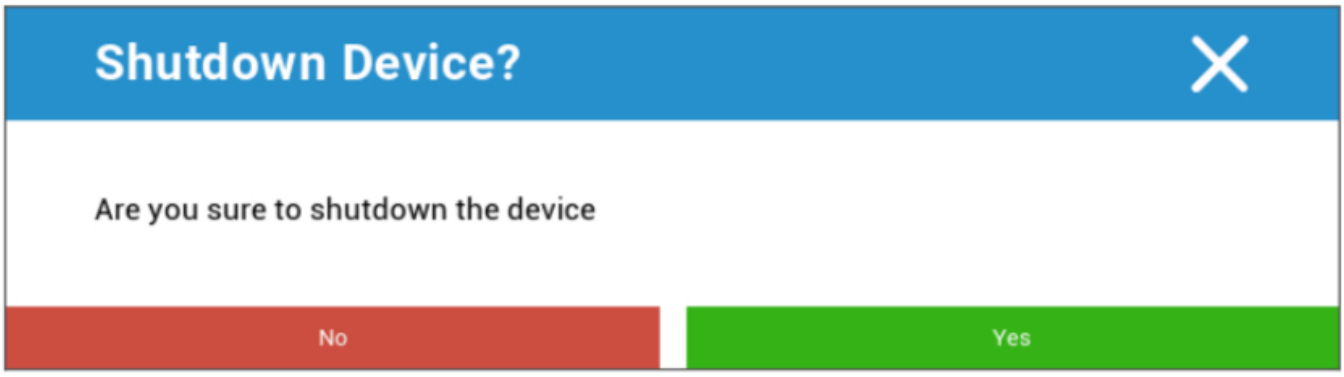
Under "Clear Passcode" kan du fjerne passordet fra enheten. Deretter vil brukeren bli bedt om å oppgi et nytt passord (avhengig av retningslinjene for passord).

Lås enhet



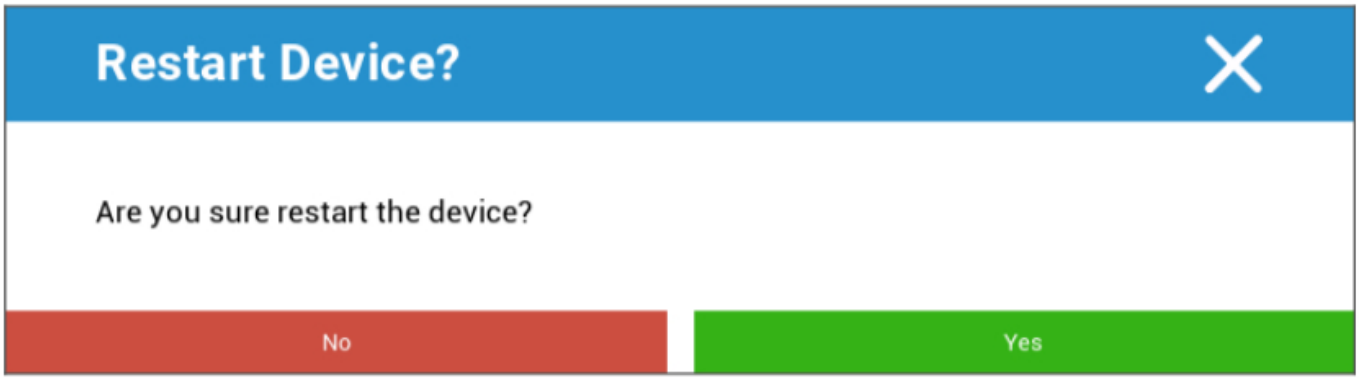
Her sendes en låskommando til sluttbrukerens enhet (låseskjerm).

Avstengningsenhet



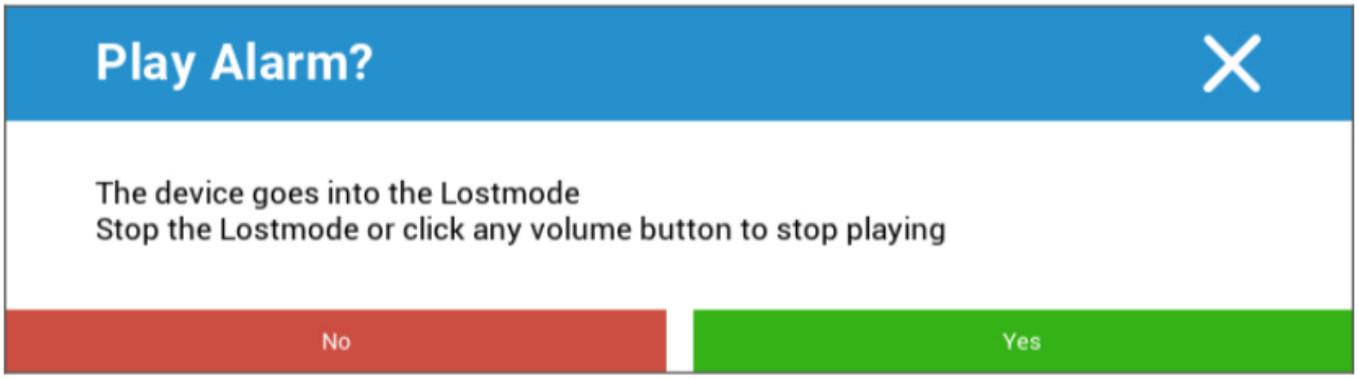
Her sendes en avslutningskommando til sluttbrukerenheten.

Start enheten på nytt

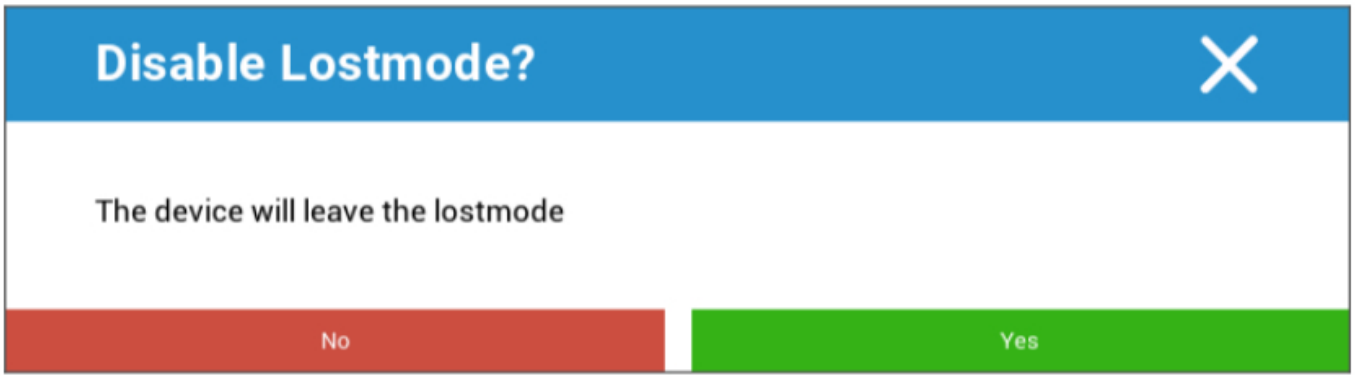


Her sendes en omstartkommando til sluttbrukerenheten.

Alarm og tapsmodus | Deaktiver tapsmodus



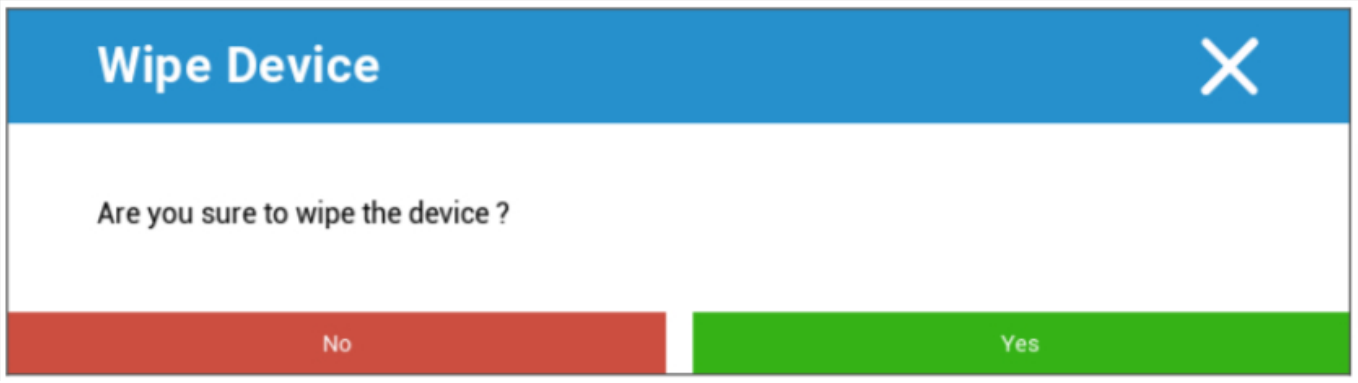
Her kan enheten stilles inn i Lostmode, som stiller inn enheten til å konstant spille av en alarmlyd. Lostmode kan stoppes ved å trykke på en hvilken som helst volumknapp på enheten eller eksternt ved å klikke på "Deaktiver Lostmode":



Slett enhet

Her kan slettekommandoen utføres. Du kan igjen velge om enheten bare skal fjernes fra AppTec360 ("Delete from System") eller om enheten skal fjernes fra AppTec360 og samtidig tilbakestilles til fabrikkinnstillingene ("Wipe & Delete").

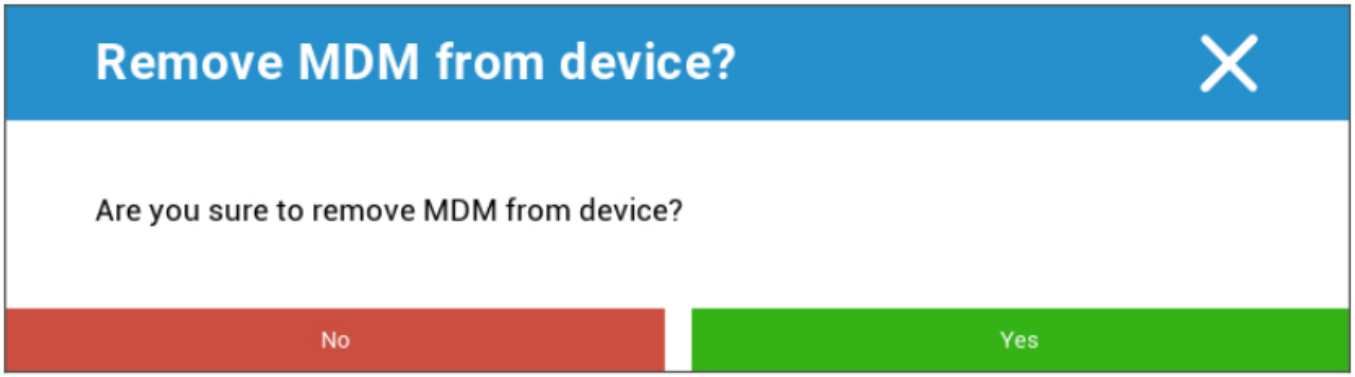
Tørk av enheten



Under "Wipe Device" kan du utføre en fullstendig sletting av enheten. Enheten gjenopprettes til fabrikkinnstillingene.

Enterprise Wipe | Fjern MDM

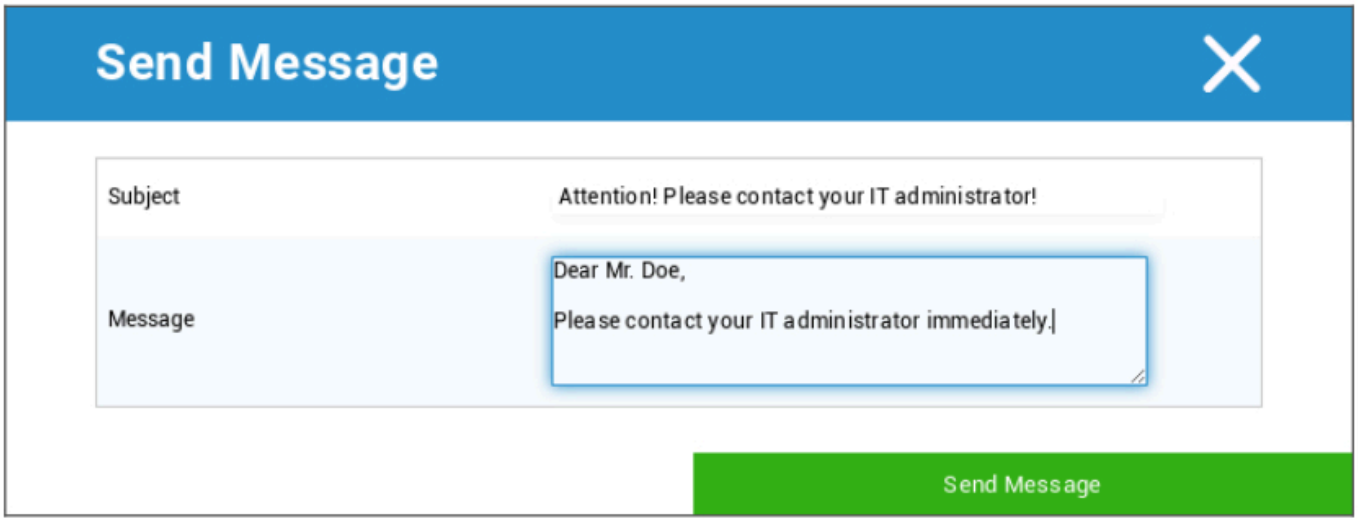
Kun informasjonen, appene og profilene som leveres av AppTec360 slettes. På denne måten vil bedriftsdataene ikke lenger være tilgjengelige på sluttbrukerens enhet. Det private området påvirkes ikke, og forblir fortsatt på sluttbrukerens enhet.



Med "Fjern MDM" kan du fjerne MDM-profilen på sluttbrukerens enhet og alle andre elementer som leveres av AppTec.

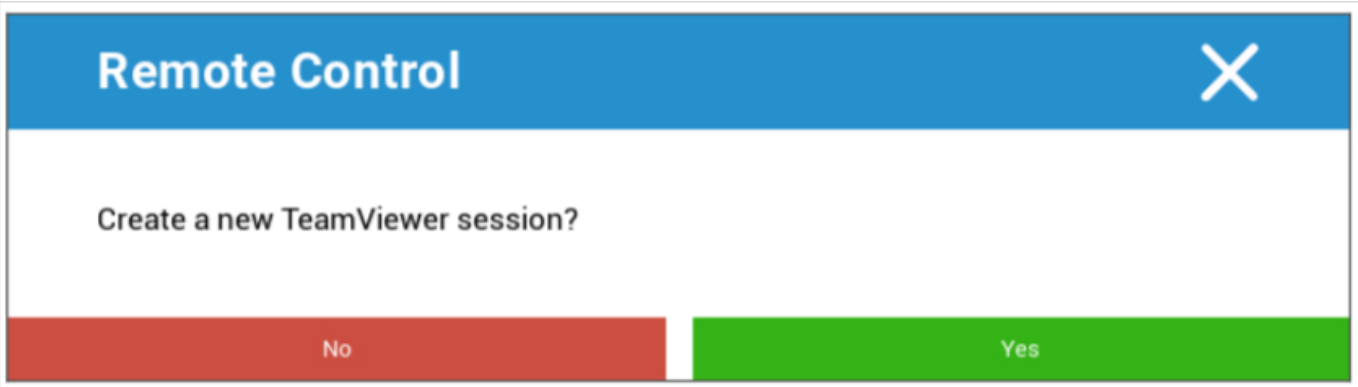
Denne kommandoen utfører samme handling som "Enterprise Wipe".

Send melding



Her kan du sende et push-varsel til den aktuelle enheten.

TeamViewer fjernkontroll



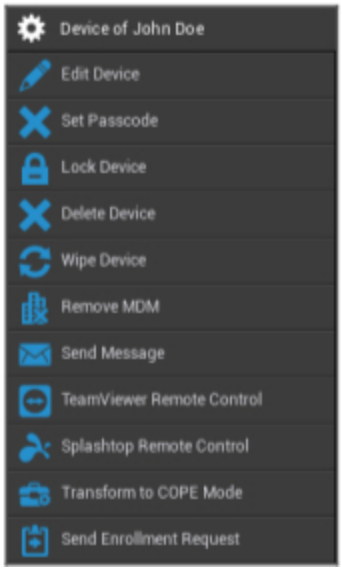
Her kan du starte en Teamviewer Remote Control-økt.

Send innmeldingsforespørsel

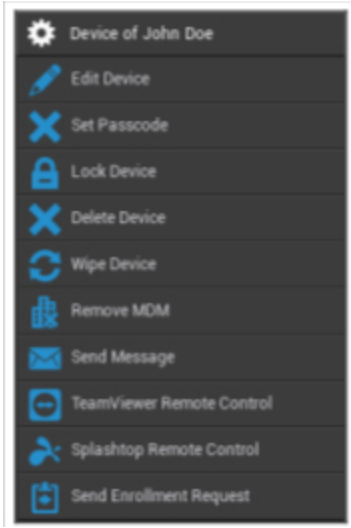
Med "Send registreringsforespørsel" kan du sende en registreringsforespørsel (på nytt) til den aktuelle brukeren.

Android

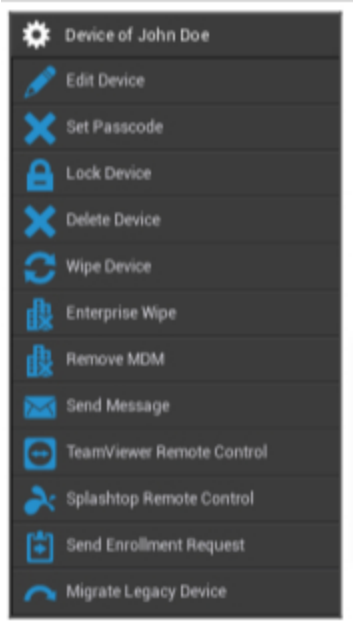
AE Fullt administrert enhet (arbeidsadministrert)



AE-arbeidsprofil (container)



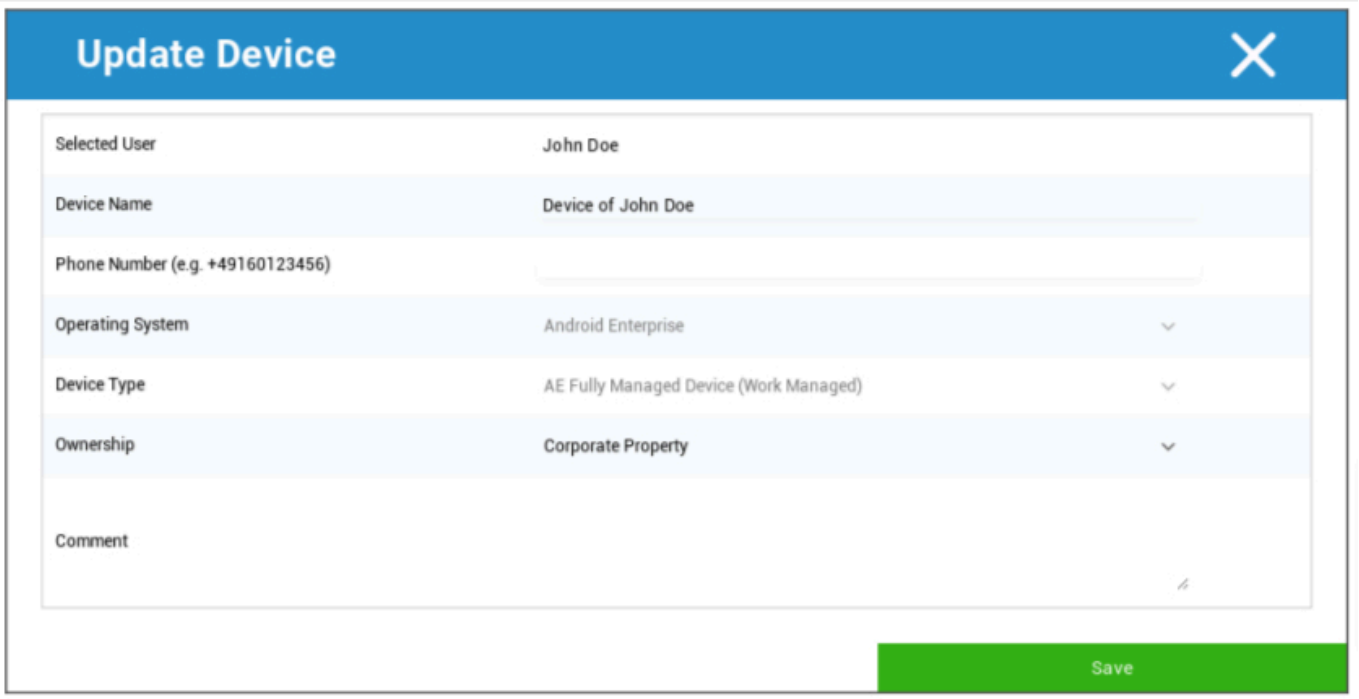
Android-telefon | Nettbrett



Rediger enhet	Rediger enhetsinformasjon
Angi passord	Angi enhetens passord
Lås enhet	Lås enheten (låseskjerm)
Slett enhet	Slett enheten fra AppTec
Tørk av enheten	Gjenopprett enheten til fabrikkinnstillingene
Enterprise Wipe	Informasjon, apper og profiler som leveres av AppTec360 slettes (enheten skilles fra MDM)
Fjern MDM	
Send melding	Send push-varsler til enheten Meldingen vises i AppTec360-appen (fanen Melding)
TeamViewer fjernkontroll	Start en fjernkontrolløkt for denne enheten ved hjelp av TeamViewer
Splashtop fjernkontroll	Start en fjernkontrolløkt for denne enheten ved hjelp av Splashtop
Overgang til COPE-modus (kun på AE Fullstendig administrert enhet (arbeidsadministrert))	Opprett en arbeidsprofil på denne AE Fullt administrert (arbeidsadministrert) enheten
Send innmeldingsforespørsel	Send (gjentatt) innmeldingsforespørsel
Migrere eldre enhet (kun på Android-telefoner/nettbrett når de er registrert med klargjøring i enhetseiermodus)	Overfør Android-telefon/nettbrett-profil til AE Fullt administrert enhet (arbeidsadministrert) - profil

Rediger enhet

Her kan du oppdatere en rekke enhetsopplysninger.



Utvalgt bruker	Bruker av enheten
Enhetens navn	Enhetens navn
Telefonnummer	Enhetens telefonnummer
Operativsystem	Android Enterprise Android
Enhetstype	Android Enterprise: • AE Fullt administrert enhet (arbeidsadministrert) • AE-arbeidsprofilmodus (kun container) • AE Fullt administrert enhet med arbeidsprofil (COPE) Android: • Telefon • Nettbrett
Eierskap	Corporate = bedriftens eiendom

	Ansatt = ansatt eiendom
Kommentar	Ytterligere beskrivelser for enheten

Tøm passord

Her kan du fjerne enhetens passord på den valgte enheten. Som standard på Android vil passordet være satt til "123456" - dette kan og bør endres av brukeren i etterkant.

Lås enhet

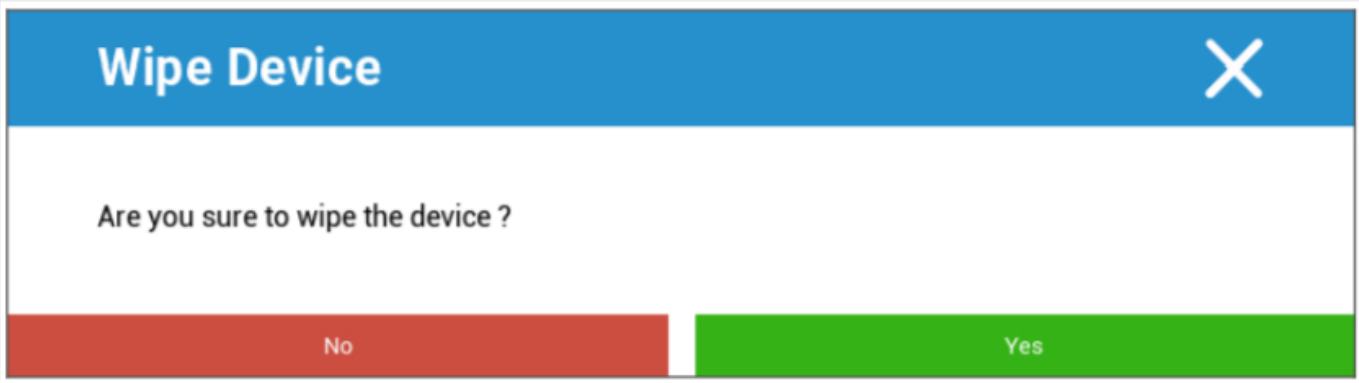
Her sendes en kommando for å låse enheten til enheten (låseskjerm).

Slett enhet

Her kan du utføre en slettekommando. Du kan igjen velge om enheten bare skal fjernes fra AppTec360 ("Delete from System") eller om enheten skal fjernes fra AppTec360 og i tillegg gjenopprettes til fabrikkinnstillingene ("Wipe & Delete").

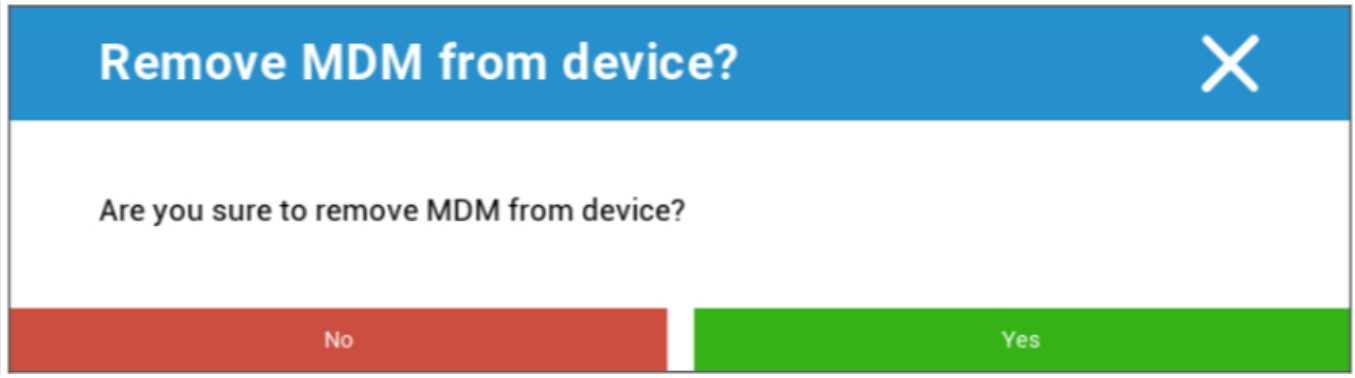
Tørk av enheten

Under "Wipe Device" kan du utføre en fullstendig sletting av enheten. Enheten vil da bli tilbakestilt til fabrikkinnstillingene.



Hvis enheten inneholder et SD-kort, kan du i tillegg slette SD-kortet. Du kan gjøre dette ved å sette "Wipe SD Card too? " til "På".

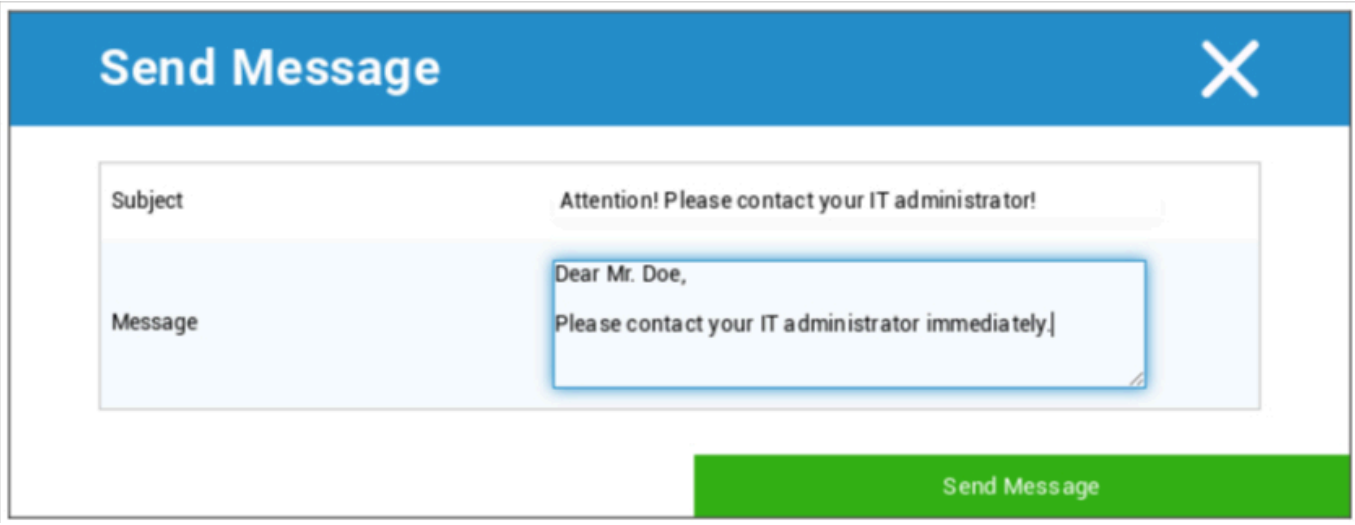
Fjern MDM



Dette er den anbefalte metoden for å skape et skille fra MDM.

Det er kun informasjonen, appene og profilene som leveres av AppTec360 som slettes, noe som betyr at alle bedriftsdata ikke lenger vil være tilgjengelige på sluttbrukerens enhet. Den private sfæren påvirkes imidlertid ikke, og forblir fortsatt på sluttbrukerens enhet.

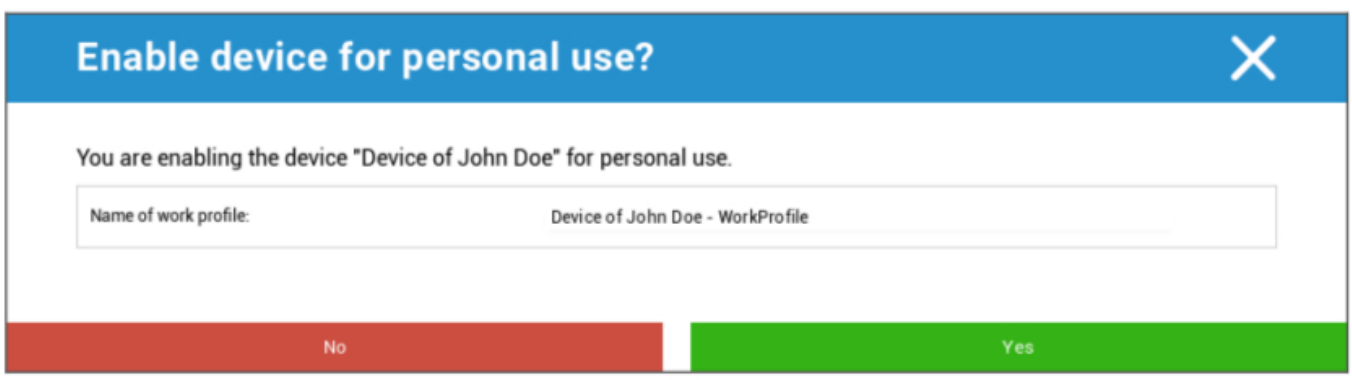
Send melding



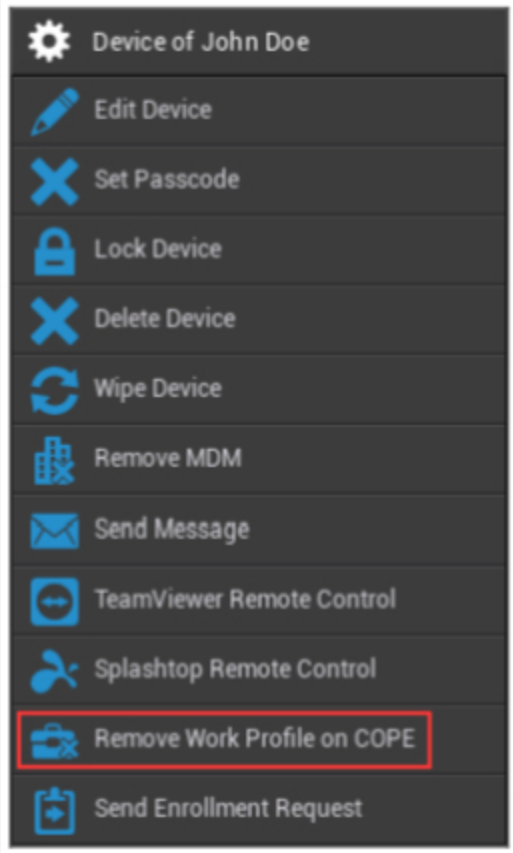
Her kan du sende et push-varsel til den aktuelle sluttbrukerens enhet.

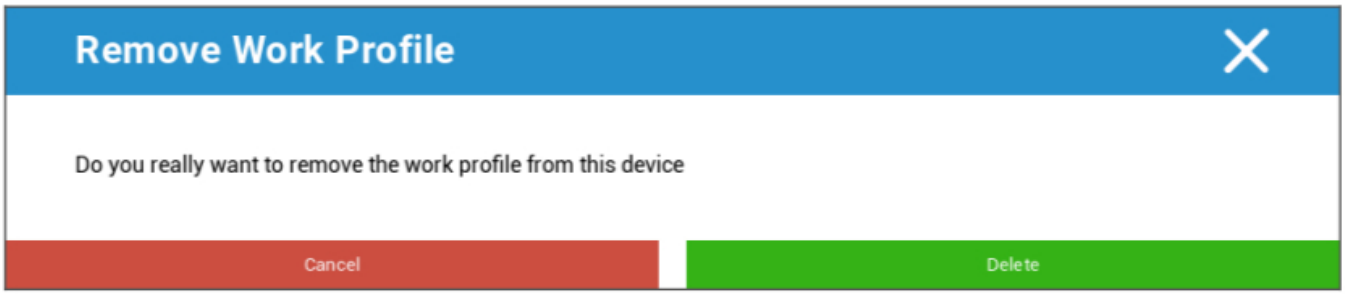
Transformer til COPE-modus

Opprett en arbeidsprofil på denne AE Fullt administrert (arbeidsadministrert) enheten



Etter at du har konvertert enheten til COPE-modus, kan du fjerne arbeidsprofilen ved å klikke på tannhjulet **Fjern arbeidsprofil på COPE**:




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

Send innmeldingsforespørsel

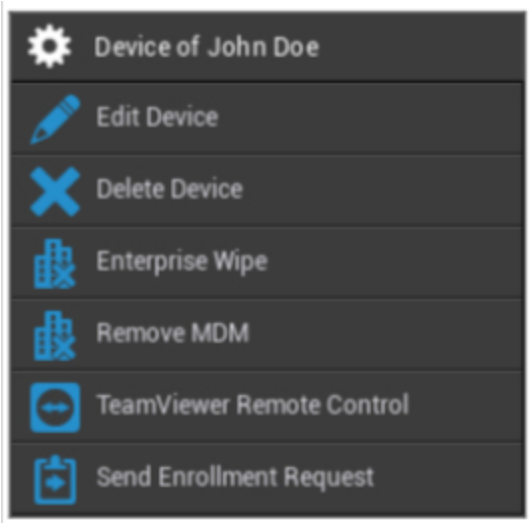
Med "Send registreringsforespørsel" kan du sende en registreringsforespørsel (på nytt) til den aktuelle brukeren.

Vær oppmerksom på at bare den nyeste registreringsforespørselen er gyldig.

Overfør eldre enheter

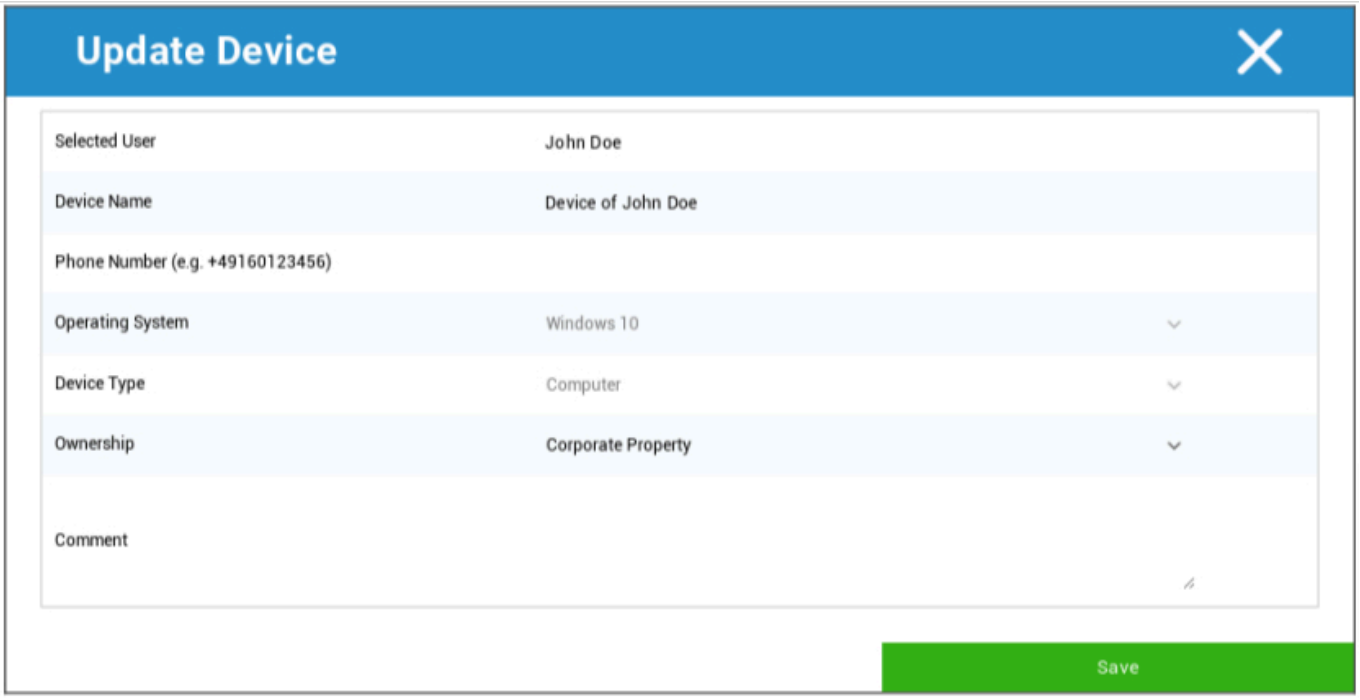
Overfør Android-telefon/nettbrett-profil til AE Fullt administrert enhet (arbeidsadministrert) -profil

Vinduer



Enhetens navn	**Navnet på den valgte enheten**
Rediger enhet	Rediger enhet
Slett enhet	Fjern enheten fra AppTec
Enterprise Wipe	Informasjon, apper og profil levert av AppTec360 slettes
Fjern MDM	
TeamViewer fjernkontroll	Fjernstyr enheten med TeamViewer
Send innmeldingsforespørsel	Send innmeldingsforespørsel (igjen)

Rediger enhet

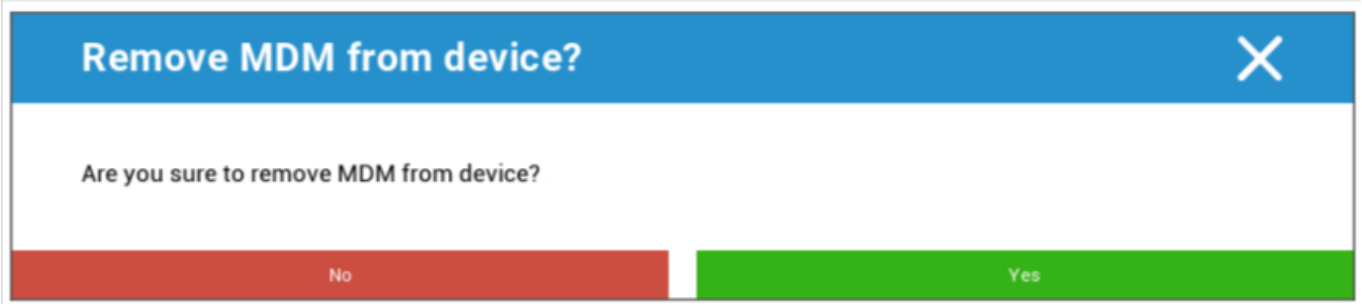


Her kan du oppdatere en rekke opplysninger om enheten.

Slett enhet

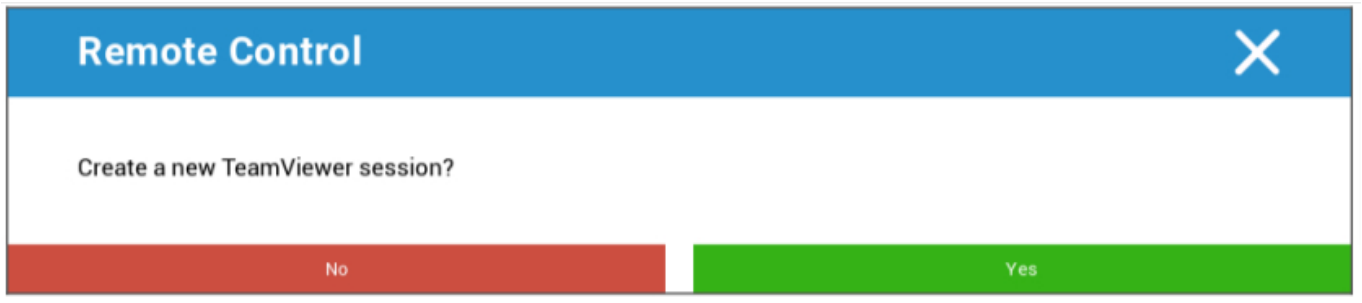
Her kan du utføre delete-kommandoen som bare fjerner enheten fra AppTec360.

Enterprise Wipe | Fjern MDM



Kun informasjonen, appene og profilene som leveres av AppTec360 slettes. På denne måten vil bedriftsdataene ikke lenger være tilgjengelige på sluttbrukerens enhet. Det private området påvirkes ikke, og forblir fortsatt på sluttbrukerens enhet.

TeamViewer fjernkontroll



Her kan du starte en TeamViewer Remote Control-økt for denne enheten.

Send innmeldingsforespørsel

Med "Send registreringsforespørsel" kan du sende en registreringsforespørsel (på nytt) til den aktuelle brukeren.

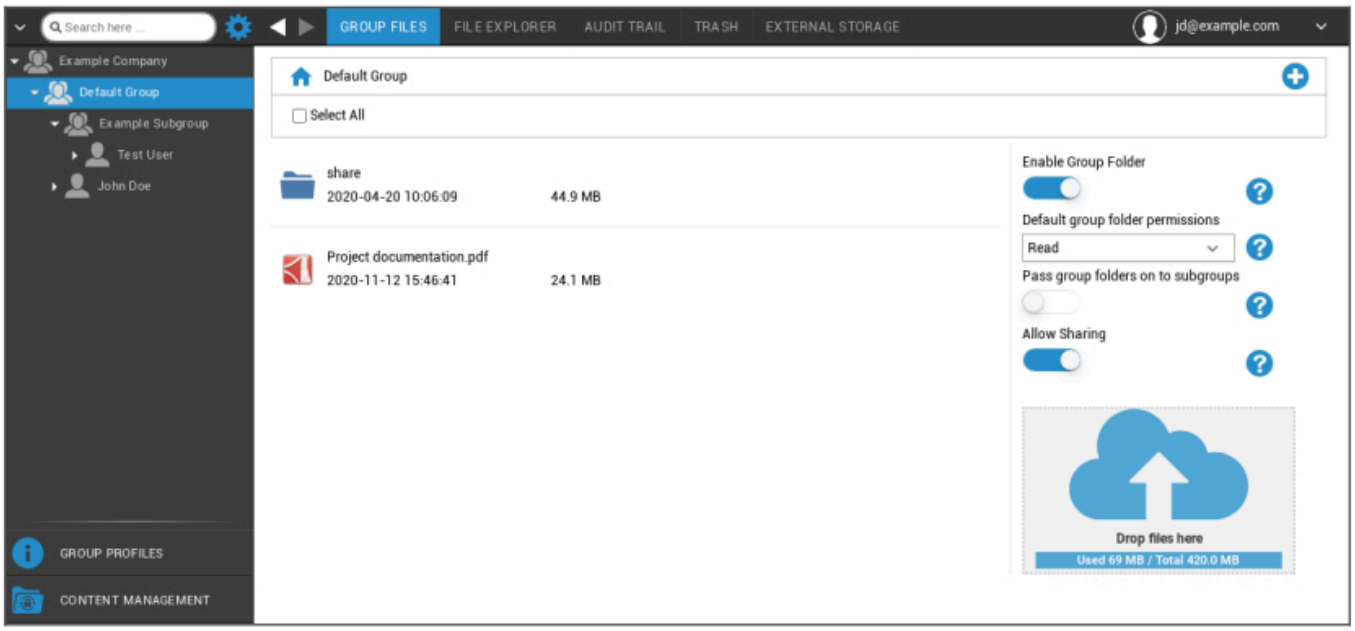
Innholdsstyring

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

Med Content Box kan du trygt distribuere dokumenter og andre bedriftsdata til sluttbrukernes enheter.

Gruppefiler

"Group Files" er en grunnleggende del av ContentBox. Her kan du angi innstillinger, laste opp dokumenter, opprette nye mapper osv.



Med symbolet i øvre høyre hjørne kan du opprette nye mapper som tilordnes den aktuelle gruppen med "Legg til mappe".

Med symbolet i øvre høyre hjørne kan du opprette en ny mappe via "Legg til mappe", som skal tilordnes den respektive gruppen.

Du kan gi mappen hvilket navn du vil.

Via "Last opp filer" kan du laste opp data. Her åpnes Standard-Explorer. Du kan selvfølgelig utføre disse to handlingene i alle (under)mapper.

Med symbolet i øvre venstre hjørne kan du gå tilbake til hovedmenyen.

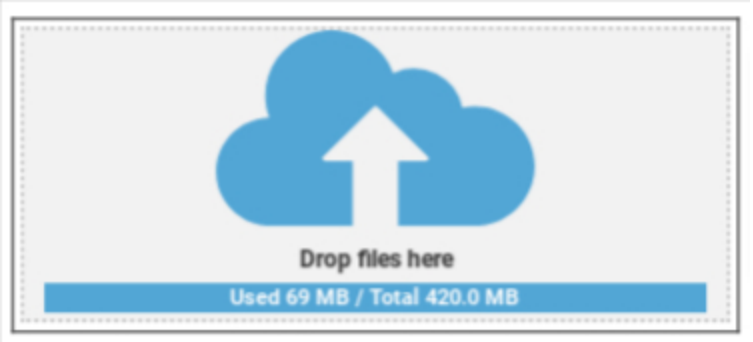
Du kan velge flere mapper og filer og laste dem ned med "Download", eller du kan slette dem ved å klikke på "Delete".

Du kan også velge alle filer og mapper med og utføre kommandoene "Last ned" og "Slett".

Når du beveger musepekeren over en mappe eller fil, ser du følgende oversikt:

- Med "Gi nytt navn" kan du gi nytt navn til mappen/filen
- Med "Last ned" kan du laste ned mappen/filen
- Med "Delete" kan du slette mappen/filen

Aktivere gruppemappe	Hvis den er aktivert, har alle medlemmer av gruppen tilgang til den aktuelle mappen
Standard gruppemappetillatelser	Tillatelser for brukerne i den valgte gruppen: Read = kun lesetillatelse Update = oppdateringstillatelse Create = opprette tillatelse Delete = slette tillatelse
Send gruppemapper videre til undergrupper	Hvis den er aktivert, kan de respektive undergruppene få tilgang til de overordnede datafilene
Tillatelser for undergrupper	Tillatelser for brukerne i den valgte undergruppen: Read = kun lesetillatelse Update = oppdateringstillatelse Create = opprette tillatelse Delete = slette tillatelse
Tillat deling	Hvis den er aktivert, kan brukeren dele filer via en lenke



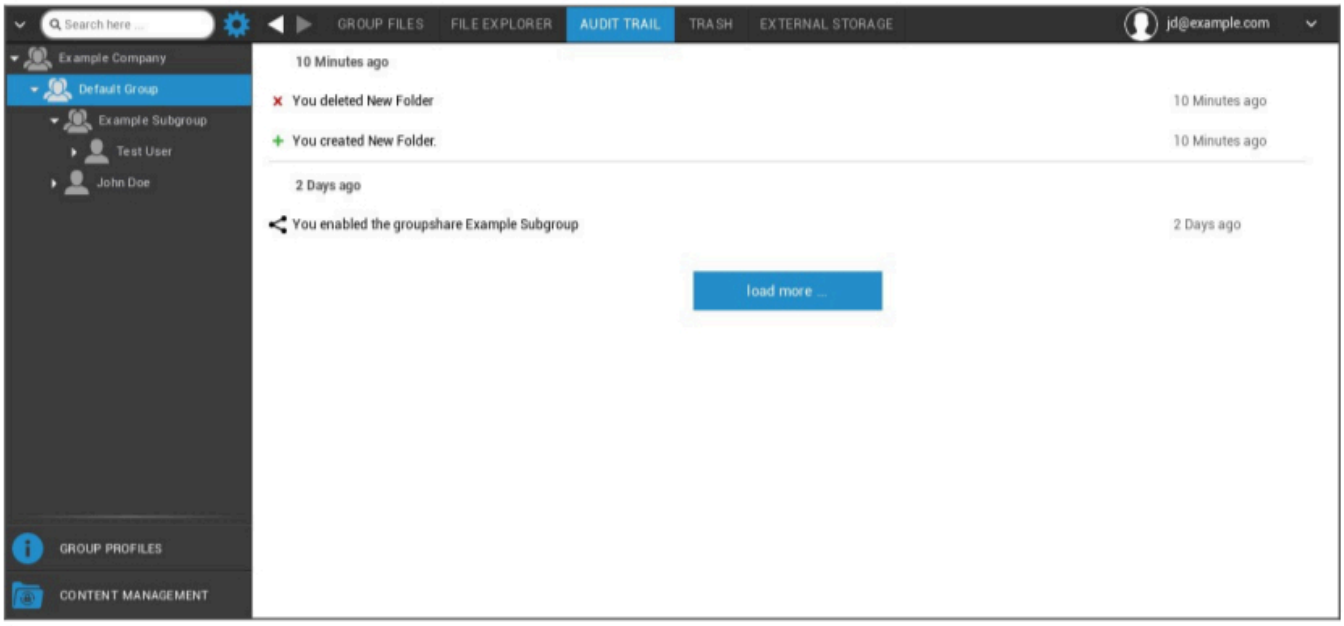
For å laste opp filer kan du bruke dette feltet ved å dra en fil til dette vinduet ved hjelp av Drag & Drop. Du kan også klikke på dette feltet for å velge og laste opp en fil ved hjelp av Internet Explorer.

Filutforsker

Med "File Explorer" kan du administrere alle mapper og filer - uavhengig av hvilken gruppe de er arkivert i.

Du finner også innstillingene og knappene som du lærte om i "Grupper filer".

Revisjonsspor



I "Audit Trail" kan du se i historikken hvilken bruker som har opprettet, slettet eller delt hva. På denne måten kan du når som helst fastslå hva som er gjort med bedriftens data.

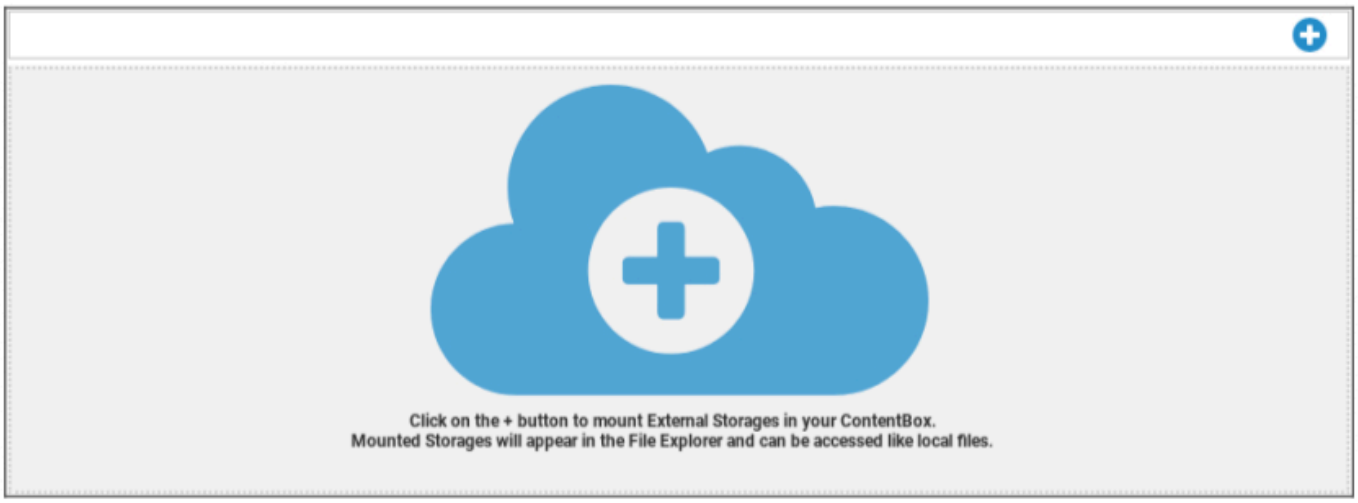
Søppel

Hvis du har slettet noe (ved et uhell), kan du se mappene og filene under "Papirkurv" og gjenopprette dem, alt etter hva du ønsker.

- Med "Undelete" kan du gjenopprette dataene/mappen.
- Med "Delete" kan du slette dataene/mappen permanent - du må bekrefte dele-kommandoen en gang til.

Vær oppmerksom på at lagringskapasiteten som brukes i søpla, reduserer den "totale plassen" som er tilgjengelig - dette er et krav fra ownCloud.

Ekstern lagring



Under overskriften "Ekstern lagring" kan du koble til ekstern lagring.

Med symbolet kan (ekstra) lagringsplass legges til.

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

Amazon S3	
Vis navn	Vis navn
Tilgangsnøkkel	Tilgangsnøkkel
Hemmelig nøkkel	Sikkerhetsnøkkel
Skuffe	Definere identiteten til undermappen som har blitt tildelt deg
Vertsnavn (valgfritt)	Vertsnavn (valgfritt)
Port (valgfritt)	Port (valgfritt)
Region	Region (valgfritt)
Aktiver SSL	Aktiver SSL
Aktiver banestil	Clear Path-adressen som er tildelt deg

FTP	
Vis navn	Vis navn
Vert	Vertsadresse
Brukernavn	Brukernavn
Passord	Passord
Rot	Hovedmeny
Sikker ftps://	

SFTP	
Vis navn	Vis navn
Vert	Vertsadresse
Brukernavn	Brukernavn
Passord	Passord
Rot	Hovedmeny

ownCloud	
Vis navn	Vis navn
URL	ownCloud URL
Brukernavn	Brukernavn
Passord	Passord
Ekstern undermappe	Standard mappe
Sikker https://	

WebDAV	
Vis navn	Vis navn
URL	WebDAV-URL
Brukernavn	Brukernavn
Passord	Passord
Rot	Hovedmeny
Sikker https://	
Windows Share	Støtte for Windows Share vil snart være tilgjengelig
SharePoint	Støtte for Microsoft SharePoint vil snart være tilgjengelig

Revisjonslogg

Her finner du en logg som registrerer informasjon om handlinger som utføres i MDM-konsollen.

Med filterikonet kan du bruke filtre på listen som vises.

Med rullegardinmenyen Elementer **per side**: Du kan velge hvor mange elementer som skal vises på én side i listen.

Tiltak iverksatt / Innstilling endret	Handlingen som ble utført / innstillingen som ble endret
Verdi	Verdien av den utførte handlingen/endrede innstillingen
Bruker	Navnet på brukeren som har utført handlingen/endret innstillingen
Dato	Tidsstempel for når denne handlingen ble utført/innstillingen ble endret
Sti / Type	Stien til der denne handlingen ble utført/innstillingen ble endret

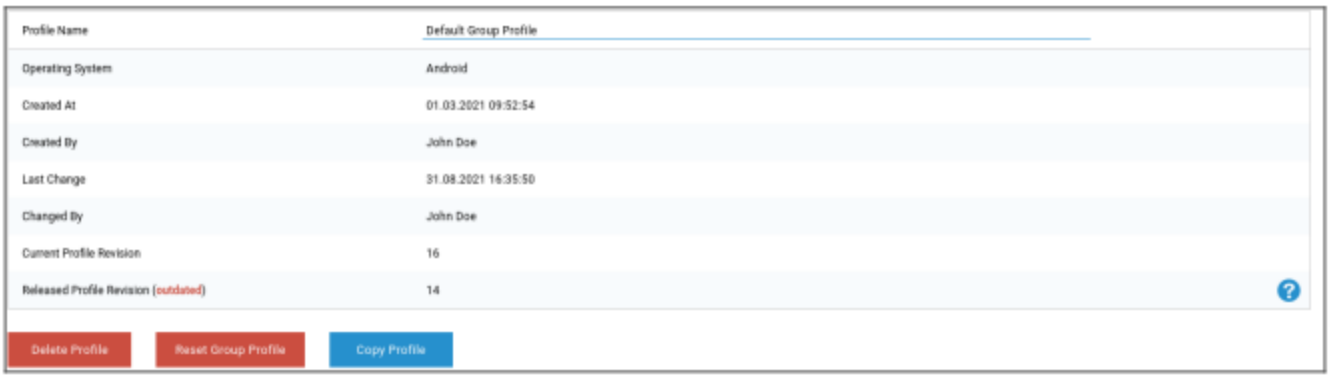
iOS-konfigurasjon

Generelt

Avhengig av om du har valgt en gruppe eller en enhet, er visningen og underpunktene forskjellige - vær oppmerksom på dette!

Oversikt over gruppeprofiler (kun på gruppenivå)

Når du åpner en gruppeprofil, får du en rask oversikt over profilen



Profilnavn	Navn på profilen (kan endres her)
Operativsystem	Operativsystemet profilen er beregnet på
Opprettet på	Tidspunktet for skapelsen
Opprettet av	Skaperen av profilen
Siste endring	Tidspunkt for siste endring av profilen
Endret av	Konto som gjorde de siste endringene
Nåværende profilrevisjon	Revisjon av lagret profilstatus
Utgitt profilrevisjon	Tilordnet profilrevisjon ("Tilordne nå"). Hvis etiketten viser "(utdatert)" bak teksten, betyr det at du har lagret profilen, men ikke tilordnet den ennå, slik at enhetene fortsatt vil få en eldre versjon.

Generell informasjon

Hvis du befinner deg direkte på enheten, får du en kort oversikt over den valgte enheten.

Enhetens navn	Enhetens navn
Telefonnummer	Enhetens telefonnummer
Modell	Modellnummer
Operativsystem	OS
Serienummer	Enhetens serienummer
Eierskap til enheten	Bedrifts- eller privat enhet Corporate = bedriftsenhet Ansatt = privat enhet
Enhetstype	Enhetstype (nettbrett eller telefon)
Jailbroken	Hvis det er en jailbreak på enheten
Overvåket	Angir om dette er en overvåket enhet
Overensstemmende	Hvis noen retningslinjer ble brutt
Sist sett	Status for når enheten sist kommuniserte med AppTec360 Server

Innstillinger

Disse innstillingene inneholder enhetens navn og en forhåndsdefinert bakgrunn.

Navngi enheten til systemnavn	Navnet som vil bli utstedt i AppTec360 Console (i venstre hierarkistruktur), vil være det samme som på den respektive sluttbrukerenheten (kan ses i enhetsinnstillingene)
Bruk egendefinert bakgrunnsbilde (kun overvåkede enheter)	Her kan du forhåndsdefinere bakgrunnen som skal vises på sluttbrukerens enhet (f.eks. for en type bedriftsmerkevare for enheten) Er kun tilgjengelig i overvåket modus!
Automatiske OS-oppdateringer	Fremtvinger OS-oppdateringer hvis tilgjengelig. Bare for DEP-enheter i overvåket modus.
Egendefinerte skrifter	Her kan du legge til egendefinerte skrifter.
Navn	Valgfritt. Det synlige navnet på skriften. Dette feltet erstattes av det faktiske navnet på skriften etter installasjon.
Skrifttype	Last opp skriftfilen (.otf eller .ttf).

Konfigureringsrevisjon

Her får du en oversikt over hvilken gruppeprofil som er tilordnet enheten.

Hvis du klikker på gruppeprofilen, får du direkte tilgang til profilen og kan utføre innstillinger.

Med symbolet kan du tilbakestille de tilordnede appene til gruppeprofilens innstillinger.

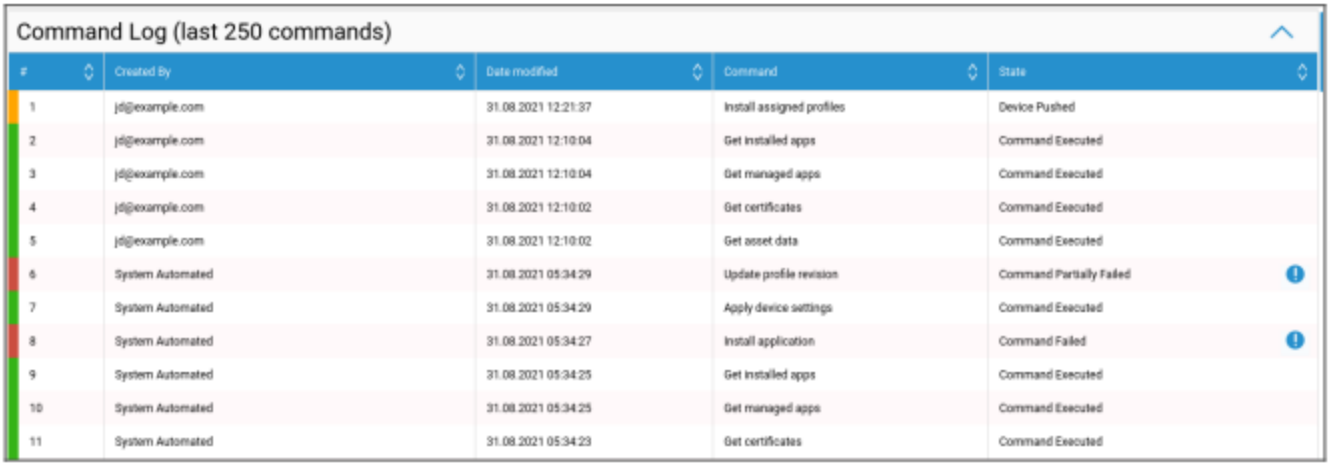
Med symbolet kan du tilbakestille enhetsprofilen slik at den ikke har noen innstillinger i det hele tatt.

"Nyere revisjon tilgjengelig" indikerer at gruppeprofilen har blitt endret og lagret, men ikke tilordnet. Gruppeprofilen må tilordnes med "Tilordne nå" på gruppenivå for at endringene skal gjelde for enhetene.

Enhetslogg (kun på enhetsnivå)

Kommandologg

Her kan du se hvilke kommandoer som er utstedt for enheten, og hvilken status de har.



Kommandoer som opprettes av "System Automated", opprettes automatisk av systemet.

Mulige kommandostatuser

Enhet skjøvet	En push-forespørsel har blitt sendt til push-tjenesten (f.eks. APNS) for å be enheten om å koble seg tilbake til EMM-serveren.
Kommando opprettet	Kommandoen ble opprettet i systemet.
Kommando sendt	Kommandoen ble sendt til enheten etter at den ble koblet til serveren.
Kommando utført	Kommandoen ble vellykket utført.
Kommando mislyktes	Kommandoen mislyktes. *
Kommandoen mislyktes delvis	Avhengig av enhetens operativsystem kan enkelte kommandoer bli gruppert sammen. I dette mislyktes noen deler av denne kommandogruppen. *
Kommando utført, men mislyktes til slutt	Kommandoen ble utført, men kanskje ikke.
Kommando Repushed	Kommandoen ble sendt på nytt av en bruker.
Kasseres	Kommandoen ble forkastet. For eksempel fordi den ble erstattet av en annen kommando, eller fordi enheten ble registrert på nytt og gamle kommandoer ble fjernet.

Hvis det er et utropstegn bak meldingen, kan du få mer informasjon ved å holde musepekeren over ikonet.

Asset Management (kun på enhetsnivå)

Asset Management (kun på enhetsnivå)

Enhetsinfo

Modell	Enhetens modellnummer
Operativsystem	OS
OS-versjon	OS-versjon
Serienummer	Serienummer
UDID	UDID for enhet
Enhetens navn	Enhetens navn
Overvåket	Viser om enheten er overvåket
Batteristatus	Batteristatus

Wi-Fi

IP-adresse	Enhetens IP-adresse
WiFi MAC	WiFi MAC-adresse

Cellular

Status	Status (SIM-kort til stede)
Telefonnummer	Telefonnummer
Roaming-status	Gjeldende roamingstatus
Roaming (tale/data)	Roamingstatus for tale/data
IP-adresse	IP-adresse
IMEI	IMEI-nummer
Operatør/transportør	Leverandør av mobiltjenester
SIM-operatørens nettverk	SIM-operatørens nettverk
Transportørversjon	Bærbar versjon
Fastvare for modem	Fastvare for modem
Nåværende MCC/MNC	Se "SIM MCC/MNC"
SIM MCC/MNC	Mobile Country Code er en etablert landidentifikasjon av ITU i henhold til E.212-standarden, som sammen med Mobile Network Code (MNC) brukes til å identifisere et mobilnettverk (= landskode). Når du går inn i et annet mobilnett, er "Current MCC/MNC" og "SIM MCC/MNC" derfor forskjellige.

Bluetooth

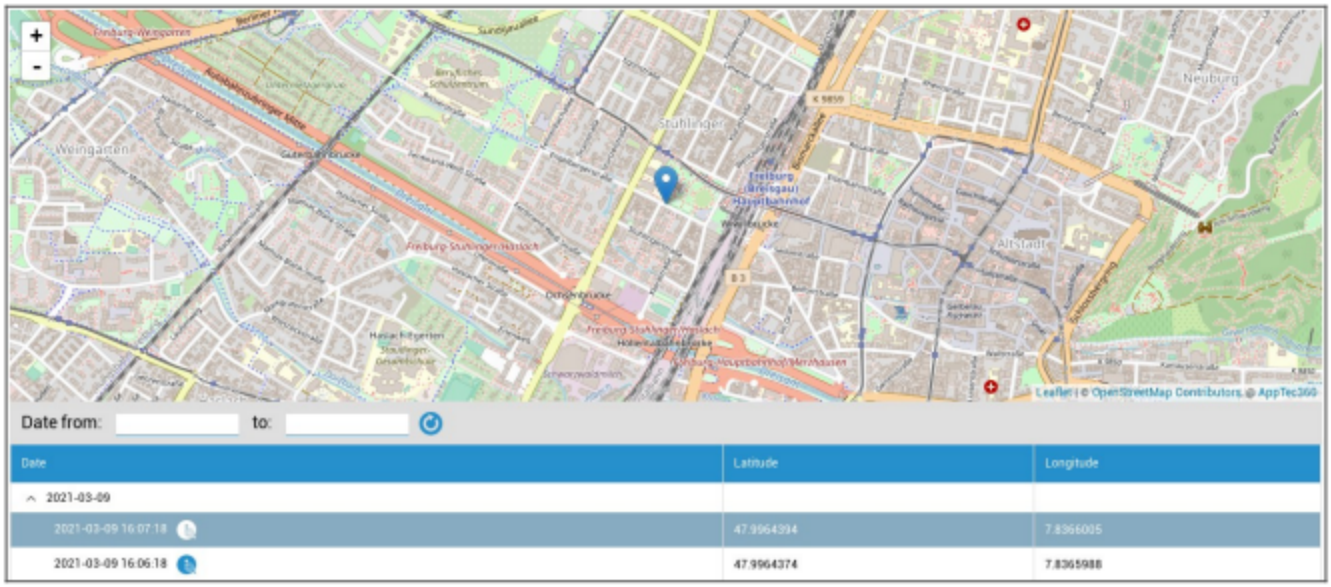
Bluetooth MAC	Bluetooth MAC-adresse

Sikkerhetsstyring

Tyverisikring (kun på enhetsnivå)

GPS-informasjon (kun på enhetsnivå)

Her kan du vurdere enhetens nåværende/seneste plassering. Lokaliseringen kan enten beskyttes med ett eller to passord - se: Generelle innstillinger - Personvern - GPS-tilgang



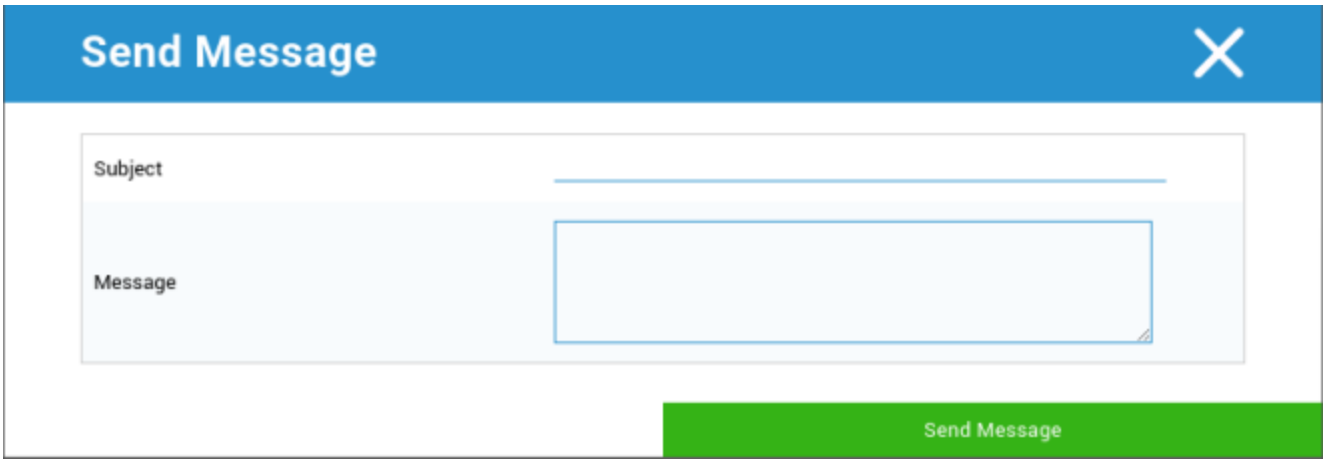
Tørk og lås (kun på enhetsnivå)

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

Full Wipe	Enheten tilbakestilles til fabrikkinnstillingene (både bedriftsdata og personlige data slettes)
Enterprise Wipe	Kun bedriftsdata fjernes fra sluttbrukerens enhet (alle apper, data osv. som ble levert av AppTec)
Låseskjerm	Skjermlåsen er aktivert, og det er tilstrekkelig å låse opp enheten med enhetens passord/PIN-kode
Kriminalteknisk nedlåsing (kun overvåkede enheter)	Hvis denne funksjonen aktiveres med symbolet  , låses enheten ved at det vises en melding som ikke kan lukkes. Den ansatte kan heller ikke låse opp enheten. Bare administratoren kan låse opp enheten i konsollen med opplåsingssymbolet  .
Tillat aktiveringslås (kun overvåkede enheter)	Hvis denne funksjonen er aktivert, blir enheten låst så snart "Finn min iPhone" er aktivert i iCloud-innstillingene.

Melding (kun på enhetsnivå)

I det følgende vinduet kan du fylle inn emne og en melding og sende den til en sluttbrukerenhet:



Sikkerhetskonfigurasjon

Passord

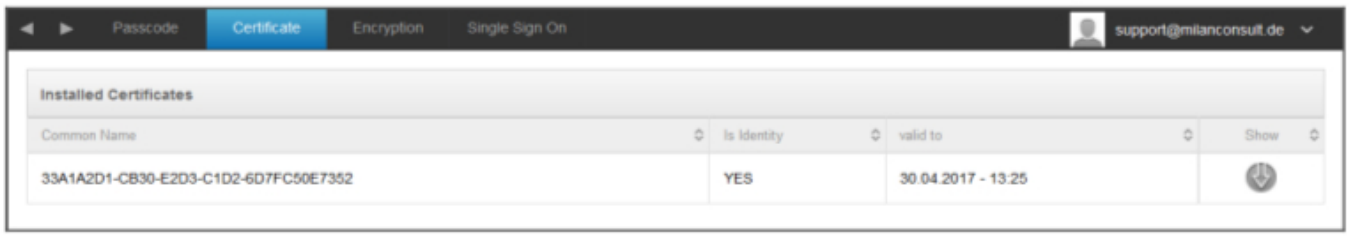
Her angir du innstillingene for enhetens passord

Deaktivering av kode tillatt	Når denne innstillingen er aktivert, blir du ikke bedt om å skrive inn passord Så snart et passord er opprettet, kan det ikke deaktiveres
Tillat enkel verdi	Tillat brukeren å bruke de samme, eskalerende og reduserende nummerstrengene (f.eks. 1234, 1111)
Krever alfanumerisk verdi	Passordene må inneholde minst én bokstav
Minimum lengde på passordet	Minimal passordlengde
Minimum antall komplekse tegn	Minimum antall alfanumeriske symboler i passordet
Maksimal alder på passordet	Antall dager etter at passordet må endres
Maksimal automatisk låsing	Maksimum tid etter hvilken enheten er låst
Maksimal frist for låsing av enheten	Tid, hvoretter enheten går inn i låst Standby-modus
Maksimalt antall mislykkede forsøk	Fastsetter hvor ofte et passord kan tastes inn feil før en fullstendig sletting av enheten vil bli utført
Maksimal alder på passordet (1-730 dager)	Maksimal passordalder
Passordhistorikk (1-50 passord)	Bruk av et gammelt passord er tillatt etter dette nummeret

Ved å klikke på papirkurven åpnes dialogboksen Password-Reset, som gjør det mulig å slette et glemt passord for enheten.

Sertifikat (kun på enhetsnivå)

Viser sertifikatene som er tilgjengelige på enheten



Kryptering

Krev kryptering av lagringsplass	Aktiver den installerte enhetens krypteringsfunksjon

Enkel pålogging

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

Her oppretter du tilgangslegitimasjonen og de respektive URL-adressene/appene som har tillatelse til å bruke Kerberos-tokens.

Tilgjengelig i overvåket modus	
Kontonavn	Kontonavn
Hovednavn	Unik identitet som Kerberos-billetter kan distribueres til
Riket	Kerberos Realm, som skal brukes (f.eks. ditt domene)

Med symbolet kan du opprette flere nettadresser.

URL-mønster som brukes til å begrense denne kontoen	URL-adresser som Kerberos-billetter kan distribueres til, skal fastsettes

Med symbolet kan du opprette flere apper.

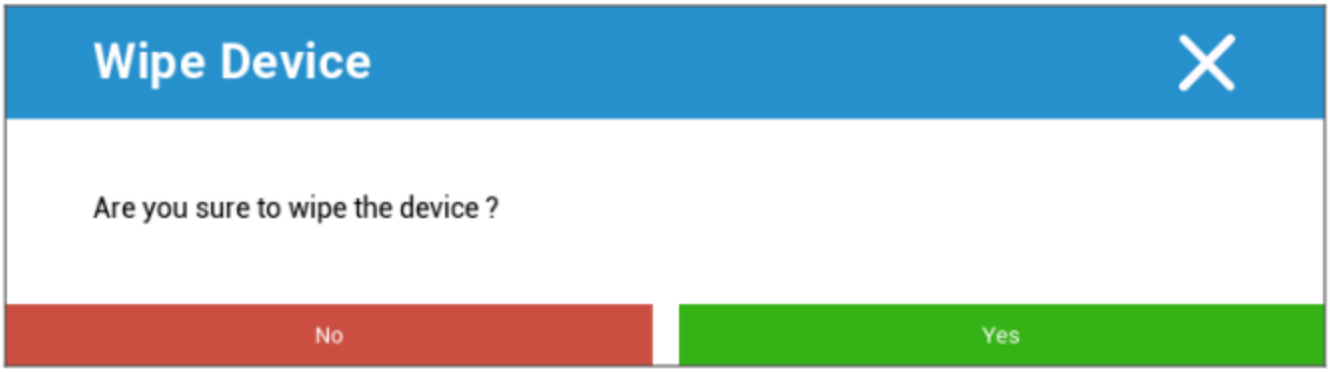
Apper for å begrense denne kontoen	Skal bestemmes Apper som Kerberos-billetter kan distribueres til

End of Life (kun på enhetsnivå)

Tørk (kun på enhetsnivå)

Under "Wipe" kan du gjenopprette enheten til fabrikkinnstillingene. Her slettes bedriftsdataene og de private dataene på sluttbrukerens enhet.

Når du klikker på "Minus-symbolet", bør du få følgende melding



Med "Yes" kan du utføre tørkingen.

Under "Wipe Report" kan følgende elementer vises

Tørket av	Historikk over hvem som utførte tørkingen
Dato	Dato
Status	Status (f.eks. om tørkingen ble vellykket)

Begrensningsinnstillinger

Enhetens funksjonalitet

Her kan du blokkere enkelte funksjoner på sluttbrukerens enhet

Tillat installasjon av apper	Tillat installasjon av apper
Tillat kamera	Tillat bruk av kameraet
Tillat FaceTime	Tillat FaceTime
Tillat skjermopptak	Tillat skjermopptak
Tillat automatisk synkronisering under roaming	Tillat automatisk synkronisering under roaming
Tillat Siri	Tillat Siri
Tillat taleoppringing	Tillat taleoppringing
Tillat kjøp i appen	Tillat kjøp i appen
Krev iTunes Store-passord for alle kjøp	Krev iTunes Store-passord for alle kjøp
Tillat flerspillerspill	Tillat flerspillerspill
Tillat å legge til Game Center-venner	Tillat å legge til Game Center-venner
Tillat åpning fra managed til unmanaged	Tillat åpning av innhold i administrerte apper i ikke-administrerte apper
Tillat åpning fra ikke-administrert til administrert	Tillat åpning av innhold i ikke-administrerte apper i administrerte apper
Tillat visning av i dag på låseskjermen	Når denne innstillingen er aktiv, vises "I dag"-visningen i varslingssenteret på låseskjermen
Tillat kontrollsenter på låseskjermen	Tillat Kontrollsenter på låseskjermen
Tillat TouchID	Tillat TouchID
Tillat over-the-air PKI-oppdateringer	Tillat over-the-air PKI-oppdateringer
Tillat passbook mens den er låst	Tillat passbook mens enheten er låst

Begrens sporing av annonser	Denne funksjonen deaktiverer annonsesporing (f.eks. annonsører kan ikke bruke annonsesporing for å distribuere personlig tilpassede annonser)
Tillat overlevering	Tillat overlevering
Tillat internettresultater i søkelyset	Tillat internettresultater i søkelyset (f.eks. Bing eller Wikipedia)
Krev passord ved første AirPlay-kobling	Krev passord ved første AirPlay-kobling
Force Watch Håndleddsbeskyttelse	Hvis den er aktivert, tvinges Apple Watch til å bruke "Wrist Protection" (håndleddsgjenkjenning)
Tillat iCloud Photo Library	Tillater iCloud Photo Library. Hvis det ikke tillates, vil alle bilder som ikke ble fullstendig lastet ned fra iCloud, slettes på den lokale lagringsplassen.
Tilgjengelig i overvåket modus	
Tillat endring av konto	Tillat endring av "e-post, kontakter, kalender"
Tillat AirDrop	Tillat AirDrop
Tillat endring av appens mobilnummer	Denne innstillingen blokkerer innstillingen for hvilke apper som har lov til å bruke mobildata Denne innstillingen kan for eksempel stilles inn manuelt på sluttbrukerens enhet, og deretter kan denne begrensningen aktiveres
Tillat Siri å søke etter brukergenerert innhold fra nettet	Nettsøk på visse nettsteder er blokkert, f.eks. Wikipedia, fordi alle kan gjøre endringer som de vil
Aktiver Siri-banneordfilter	Skjellsord som er rettet mot Siri, blir sensurert
Tillat iBook Store	Tillat iBook Store
Tillat iBook Store Erotikk	Tillat iBook Store Erotikk
Tillat endring av Finn mine venner-innstillinger	Tillat endring av Finn mine venner-innstillinger
Tillat Game Center	Tillat Game Center
Tillat sammenkobling av verter	Sammenkobling av kontrolldatamaskin
Tillat installasjon av konfigurasjonsprofiler	Tillat installasjon av konfigurasjonsprofiler
Tillat fjerning av app	Fjerning av kontrollapper

Tillat iMessage	Tillat iMessage
Tillat sletting av alt innhold og alle innstillinger	Tillat sletting av alt innhold og alle innstillinger
Tillat konfigurering av begrensninger	Tillat konfigurering av begrensninger
Tillat podcast	Tillat podcast
Tillat definisjonsoppslag	Tillat definisjonsoppslag
Tillat prediktivt tastatur	Tillat prediktivt tastatur
Tillat automatisk korrigering	Tillat automatisk korrigering
Tillat installasjon av UI-app	Hvis den er deaktivert, kan ingen apper installeres fra den offentlige AppStore (ikonet vises ikke lenger). Apper kan imidlertid fortsatt installeres via iTunes og konfiguratoren
Tillat tastatursnarveier	Tillat hurtigtaster, hvis enheten er koblet til et fysisk tastatur
Tillat sammenkobling av Apple Watch	Forhindrer sammenkobling mellom enheten og Apple Watch, eksisterende tilkoblinger vil bli avsluttet
Tillat endring av passord	Hvis dette ikke er tillatt, kan ingen enhetspassord legges til, endres eller fjernes
Tillat endring av devicenavn	Retningslinje for å avgjøre om enhetsnavnet kan endres
Tillat endring av bakgrunn	Retningslinje for å avgjøre om tapetet kan endres
Tillat automatisk nedlasting av apper	Hvis den deaktiveres, vil en kjøpt app ikke installeres automatisk på andre enheter. Gjelder ikke oppdateringer for eksisterende apper
Tillat nyheter	Tillat nyheter på iOS-enheten
Tillat tillit til Enterprise-apper	Hvis den er satt til false, forhindrer den tillit til bedriftsapper

iCloud

Blokker visse funksjoner under iCloud-paring

Tillat sikkerhetskopiering	Tillat sikkerhetskopiering
Tillat synkronisering av dokumenter	Tillat synkronisering av dokumenter
Tillat bildestrøm	Tillat bildestrøm
Tillat delt bildestrøm	Tillat delt bildestrøm
Tillat synkronisering av nøkkelring i skyen	Tillat synkronisering av nøkkelring i skyen
Tillat administrerte apper å lagre data	Tillat administrerte apper å lagre data
Tillat synkronisering av notater og høydepunkter for bedriftsbøker	Tillat synkronisering av notater og høydepunkter for bedriftsbøker
Tillat sikkerhetskopiering av virksomhetens bøker	Tillat sikkerhetskopiering av virksomhetens bøker

Sikkerhet og personvern

Blokker disse funksjonene knyttet til diagnostiske data

Tillat at diagnostiske data sendes til Apple	Tillat at diagnostiske data sendes til Apple
Tillat brukeren å godta ikke-klarerte TLS-sertifikater	Tillat brukeren å godta ikke-klarerte TLS-sertifikater
Tving frem krypterte sikkerhetskopier	Tving frem krypterte sikkerhetskopier

BYOD

Innebygd iOS-sikkerhet (container)

iOS har alltid kunnet skille mellom administrert (business) og uadministrert (privat). Alt som kommer fra MDM-systemet, behandles som administrert. Hvis du for eksempel installerer en app via MDM eller konfigurerer en Exchange-konto, vil dette bli behandlet som administrert av iOS.

Alt annet som konfigureres/installeres manuelt på enheten, vil bli behandlet som uadministrert. For eksempel hvis brukeren installerer WhatsApp på egen hånd, eller hvis brukeren legger til en Exchange-konto. Denne separasjonen har imidlertid aldri påvirket kontaktene. Men siden iOS 11.3 (og nyere) ble dette også lagt til for kontaktene.

Siden dette er en grunnleggende funksjonalitet i operativsystemet, trenger du ikke å installere noe eller sette opp en spesiell container.

Aktiver den innebygde funksjonen for å skille mellom private og forretningsmessige apper/informasjon/filer. Denne innstillingen vil også deaktivere noen andre funksjoner, som ellers kan slå av deler av dette skillet ved en feiltakelse.

Aktivering

Aktiver Container-løsningene som støttes av AppTec360

Aktiver Google Divide Container	Aktiver Google Divide Container
Aktiver SecurePIM Container	Aktiver SecurePIM Container

Hvis du har aktivert SecurePIM Container, finner du også følgende punkt under "Aktivering". I tillegg åpnes fire andre faner med en gang, som er beskrevet nedenfor.

E-postadresse for kundestøtte	E-postadresse for brukerstøtte hvor en bruker kan henvende seg med problemer

SecurePIM Passord

Under "SecurePIM Password" kan du angi retningslinjer for passordets sikkerhetsstyrke.

Tidsavbrudd for økten	Her kan du angi etter hvor mange minutter et nytt passord må skrives inn igjen, når SecurePIM kjører i bakgrunnen
Passordets lengde	Passordlengde for tilgang til SecurePIM Container
Store og små bokstaver	Minimum store bokstaver
Små bokstaver	Minimum små bokstaver
Spesielle tegn	Minimum spesialtegn
Siffer	Minimumssiffer
Tørkeapplikasjon	Antall ganger et passord kan tastes inn feil før SecurePIM-innholdet slettes (Appen forblir imidlertid fortsatt på sluttbrukerens enhet)

SecurePIM Sikkerhet

Under "SecurePIM-sikkerhet" kan du angi en rekke sikkerhetsinnstillinger.

Oppdage jailbreakede enheter	Hvis denne innstillingen er aktivert, vil tilgangen til SecurePIM Container bli blokkert så snart enheten blir oppdaget som jailbreaket
Sikre tekstfelt	Innholdet i innsendingsfeltene blir kryptert, slik at ingen informasjon når operativsystemet (iOS) Merk: Så lenge denne innstillingen er aktiv, er automatisk korrigering ikke lenger tilgjengelig
Eksporter kontaktdata til enheten	Hvis denne innstillingen er aktivert, kan brukeren eksportere Exchange-kontakter til sin lokale enhet. Merk: Bare navn og telefonnummer eksporteres
Vis sted for arrangementet	Hvis denne innstillingen er aktivert, vil plasseringen av de kommende hendelsene vises i varslingslinjen
Vis hendelsestittel	Hvis denne innstillingen er aktivert, vil plasseringen av tittelen på den kommende hendelsen vises i varslingslinjen

SecurePIM-nettleser

Her kan du konfigurere nettleseren til SecurePIM.

Med symbolet kan du definere en ny URL-adresse.

Med symbolet kan du fjerne en definert URL-adresse igjen.

"Hvitelistede URL-er" er URL-er som kan lastes inn.

"Svartelistede nettadresser" er nettadresser som ikke kan lastes inn og dermed er blokkert.

Vær oppmerksom på at oppføringene på hvitelisten har høyere prioritet enn oppføringene på svartelisten. Under "Bokmerketittel" kan du angi en tittel. Med "Bokmerke-URL" kan du knytte URL-adressen til bokmerketittelen - på denne måten kan du distribuere individualiserte bokmerker til de respektive brukerne.

Utveksling

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

ActiveSync-e-postadresse	Exchange-e-postadresse (legg merke til "Placeholders")
ActiveSync Exchange-pålogging	Utveksle brukernavn (legg merke til "Placeholders")
ActiveSync Exchange Server	Exchange Server-adresse (FQDN)
ActiveSync Exchange-domene	Exchange-domenets adresse
Brukersertifikat	Brukersertifikat
Sertifikatbasert autentisering	Brukeren autentiserer seg med et sertifikat
Tillat S/MIME-kryptering	Gjør det mulig for brukeren å kryptere e-posten sin
Tillat S/MIME-signering	Gjør det mulig for brukeren å signere e-posten sin
CRL-sjekk	Hvis det private sertifikatet er aktivt, vil det bli sammenlignet med CRL (Certificate Revocation List)

Administrasjon av tilkoblinger

Wi-Fi

Services Set Identifier (SSID)	SSID for nettverket som skal kobles til
Auto Join	Aktiver automatisk tilkobling når du blir med i et nettverk
Skjult nettverk	Aktiver, i tilfelle AP-et ikke kringkaster SSID

Proxy-oppsett

Konfigurering av en proxy for hvert aksesspunkt

Ingen		Opprett ingen fullmakt
Manuell		Opprett en manuell proxy
	URL til proxy-server	Adresse for tilgang til proxy-innstillinger
	Havn	Opprett porten for proxyen
	Autentisering	Brukernavn for autentisering på proxyen
	Passord	Passord for autentisering på proxyen
Automatisk		Opprett en proxy automatisk
URL til proxy-server		URL for tilgang til proxy-innstillingene

Sikkerhetstype

Opprett sikkerhetstype for AP-et

WEP	
Passord	Passord for AP

WPA/WPA2	
Passord	Passord for AP

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	
	Bruk PAC		Bruk av PAC (Protected Access Controll)
	Avsetning PAC	Konfigurasjon av Provision PAC	
	Lever PAC anonymt	Anonym levering av PAC	
	Indre autentiseringer	Autentiseringsprotokoll som skal brukes: PAP, CHAP, MSCHAP, MSCHAPv2	
	Brukernavn	Brukernavn for autentisering	
	Ikke bruk passord per tilkobling	Ikke bruk passord per tilkobling	
	Identitetssertifikat	Last opp/velg autentiseringssertifikat	
	Ytre identitet	Identitet som kan ses utenfra	
	Tillit		
	Pålitelig sertifikat 1	Last opp det første klarerte sertifikatet	
	Pålitelig sertifikat 2	Last opp et annet klarert sertifikat	
	Pålitelig sertifikat 3	Last opp et tredje klarert sertifikat	
	Navn på klarerte serversertifikater	Navnene på de forventede serversertifikatene (i en kommaseparert liste)	

Ingen	Etablerer ingen sikkerhet

VPN

Navn på tilkobling	Navn på VPN-profilen

VPN-type

VPN

All nettverkstrafikk på enheten blir rutet via en VPN-forbindelse.

Type tilkobling	Etablere VPN-tilkoblingstype
IPsec (Cisco)	IPsec-protokoll fra Cisco
PPTP	PPTP-protokoll
L2TP	L2TP-protokollen
Cisco AnyConnect	AnyConnect-protokollen
Juniper SSL	Juniper SSL-protokoll
F5 SSL	F5 SSL-protokoll
SonicWall mConnect	SonicWall mobil tilkobling
Aruba VIA	Aruba VIA-protokoll
Tilpasset SSL	Tilkobling via egendefinert SSL
OpenVPN	OpenVPN-protokollen

VPN per app

Når du åpner en bestemt app, opprettes en VPN-forbindelse

Start automatisk VPN-tilkobling per app		Start automatisk VPN-tilkobling per app
Type tilkobling		Etablere VPN-tilkoblingstype
	Cisco AnyConnect	AnyConnect-protokollen
	Juniper SSL	Juniper SSL-protokoll
	F5 SSL	F5 SSL-protokoll
	SonicWall mConnect	SonicWall mobil tilkobling
	Aruba VIA	Aruba VIA-protokoll
	Tilpasset SSL	Tilkobling via egendefinert SSL
	OpenVPN	OpenVPN-protokollen

Proxy-oppsett

Konfigurering av en proxy for VPN-tilkoblingen

Ingen	Opprett ingen fullmakt
Manuell	Opprett en proxy manuelt
URL til proxy-server	Adresse for tilgang til proxy-innstillinger
Havn	Opprett porten for proxyen
Autentisering	Brukernavn for autentisering hos proxyen
Passord	Passord for autentisering på proxyen
Automatisk	Opprett en proxy automatisk
URL til proxy-server	URL for tilgang til proxy-innstillingene

Vis plassholdere	Viser alle tilgjengelige brukervariabler som AppTec360 kan bruke

APN

Navn på tilgangspunkt	Navn på tilgangspunkt
Brukernavn for tilgangspunkt	Tilgangspunktets brukernavn
Passord for tilgangspunkt	Passord for tilgangspunkt
Proxy-server	Adresse til proxy-server
Havn	Den respektive proxy-porten

Cellular

Aktivere dataroaming	Aktivere dataroaming
Aktiver roaming for tale	Aktiver roaming for tale
Aktiver Hotspot	Aktiver Hotspot

HTTP-proxy

Proxy Type	
Manuell	Opprett en proxy manuelt
URL til proxy-server	Adresse for tilgang til proxy-innstillingene
Havn	Etablere proxy-port
Autentisering	Brukernavn for autentisering hos proxyen
Passord	Passord for autentisering på proxyen
Automatisk	Opprett en proxy automatisk
Proxy PAC URL	Proxy PAC URL
Tillat direkte tilkobling hvis PAC ikke kan nås	Tillat direkte tilkobling (uten VPN) hvis PAC ikke kan nås
Tillat omgåelse av proxy for å få tilgang til lukkede nettverk	Tillat omgåelse av proxy for å få tilgang til interne nettverk

AirPrint

IP-adresse	Skriverens IP-adresse
Ressurssti	Definert vei til AirPrint-enheten

AirPlay

Enhetens navn	Enhetens navn
Passord	Passord for sammenkobling
Hviteliste	Definer en liste over enheter som enheten utelukkende kan pare seg med

PIM-administrasjon

Exchange Active Sync

Kontonavn	Navn på e-postkonto
Exchange ActiveSync-vert	Serverens adresse/FQDN
Tillat flytting	Tillat flytting av e-post
Brukes kun i post	Interaksjoner kan bare forekomme i den opprinnelige Mail-appen
Bruk SSL	Bruk SSL-kryptering
Domene	Serverens domene
Bruker	Brukernavn
E-postadresse	e-postadresse (kun på enhetsnivå)
Passord (kun på enhetsnivå)	Brukerpassord
Identitetssertifikat	Velg det aktuelle sertifikatet for autentisering på serveren
Tidligere dager med Mail to Sync	Antall dager frem til e-postene skal synkroniseres tilbake. Ingen grense = ubegrenset
Aktiver S/MIME	Aktiver S/MIME-kryptering
Signering av sertifikat	Last opp det respektive signeringssertifikatet
Krypteringssertifikat	Last opp det respektive krypteringssertifikatet

E-post

Oppsett av POP3-/IMAP-kontoer på sluttbrukerens enhet

Kontobeskrivelse	Navn des E-postkontoer		
Kontotype	IMAP	Stiprefiks	Stiprefikset for spesielle mapper
	POP		
Brukerens visningsnavn	Brukerens visningsnavn		
E-postadresse	Brukerens e-postadresse		
Tillat flytting	Tillat flytting av e-post		
Aktiver S/MIME	Aktiver S/MIME-kryptering		
Signering av sertifikat	Last opp det respektive signeringssertifikatet		
Krypteringssertifikat	Last opp det respektive krypteringssertifikatet		

Innkommende post

Innkommende serverinnstillinger

E-postserveradresse	Adresse til e-postserver
Port for e-postserver	Port for e-postserver
Brukernavn	Respektive brukernavn
Autentiseringstype	Autentiseringstype
Ingen	Ingen autentiseringstype
Passord (kun på enhetsnivå)	Melding om passord
MDM-utfordring-svar	
NTLM	NTLM-autentisering
HTTP MD5-digest	
Bruk SSL	Bruk SSL, om nødvendig

Utgående post

Innstillinger for utgående server

E-postserveradresse	E-postserveradresse
Port for e-postserver	Port for e-postserver
Brukernavn	Respektive brukernavn
Autentiseringstype	
Ingen	Ingen autentiseringsmetode
Passord (kun på enhetsnivå)	Melding om passord
MDM-utfordring-svar	
NTLM	NTLM-autentisering
HTTP MD5-digest	
Bruk SSL	Bruk SSL, om nødvendig
Utgående passord er det samme som innkommende	Utgående passord er det samme som innkommende
Brukes kun i post	Aktiver, hvis alle utgående e-poster skal sendes via Mail-appen

CalDav

Konfigurere oppsett og distribusjon av en CalDav-konto

Kontobeskrivelse	Visningsnavn på kontoen
Vertsnavn	Vertsnavn og/eller IP-adresse
Havn	Port til CalDav-kontoen
Hoved-URL	Kontoens hoved-URL
Brukernavn	Respektive CalDav-brukernavn
Passord (kun på enhetsnivå)	Respektive CalDav-passord
Bruk SSL	Bruk SSL, om nødvendig

Kalendere du abonnerer på

Oppsett og distribusjon av abonnerte kalendere

Beskrivelse	Visningsnavn på kontoen
URL	URL-adressen til kalenderdatabasen
Brukernavn	Brukernavn for kalenderabonnementet
Passord (kun på enhetsnivå)	Passord for kalenderabonnementet
Bruk SSL	Bruk SSL, om nødvendig

LDAP

I dette området setter du opp en LDAP-tilkobling for å muliggjøre en dynamisk sertifikatutveksling mellom sluttbrukerenheten og Active Directory.

Vær oppmerksom på at den valgte brukeren må ha lesetillatelse.

Kontobeskrivelse	Kontobeskrivelse
Brukernavn på konto	Bruker for LDAP-tilgang
Passord for konto	Passord for LDAP-tilgang
Kontoens vertsnavn	LDAP-server Vertsnavn/IP-adresse
Bruk SSL	Bruk SSL, om nødvendig

I den andre delen kan du definere individuelle filtre for søk i LDAP-registeret.

Beskrivelse	Omfang	Søkebase
Filterbeskrivelse	Søkenivå i LDAP-registeret	Definer det enkelte filteret

Webadministrasjon

Nettklipp

Her kan du definere bokmerker med lenker til nettsider, intranettportaler osv. som vil være synlige som en applikasjon på sluttbrukerens enhet.

Etikett	Navn på tilkoblingen på sluttbrukerens enhet
URL	Lenke til de respektive nettsidene
Avtakbar	Hvis den er aktivert, kan brukeren fjerne webklippet
Ikon	Last opp en logo for tilkoblingen via denne dialogen: Dimensjoner 180x180, png-format
Prekomponert ikon	Hvis den er aktivert, vil ingen tilleggseffekter (skygge, refleksjon) vises på ikonet
Full skjerm	Når du åpner webklipp, åpnes nettleseren i fullskjermmodus

Filter for webinnhold

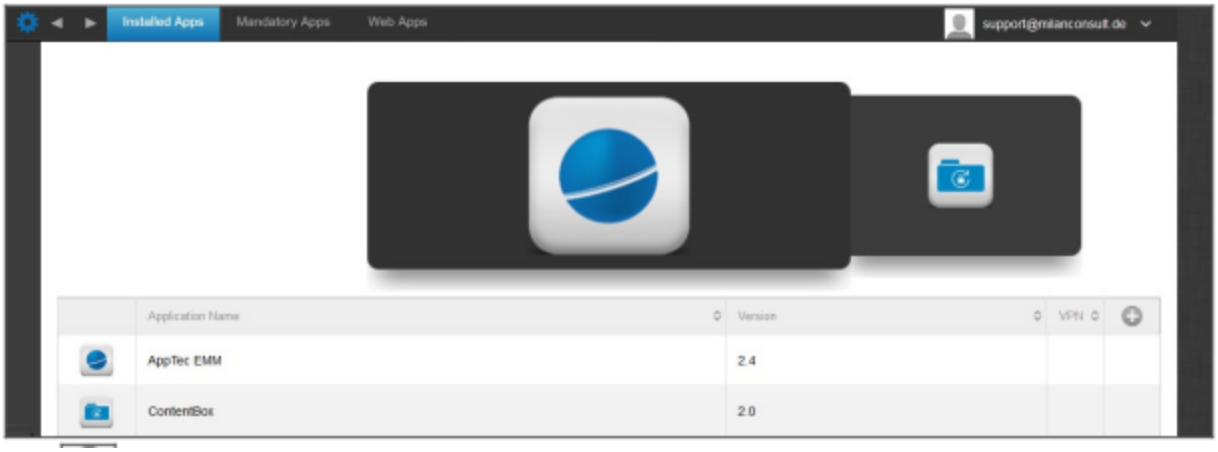
Web Content Filter gjør det mulig å begrense tilgangen til bestemte nettsider.

Tillatte nettsteder	
Begrens voksent innhold	Webfilter brukes automatisk for innhold for voksne
Tillatte nettadresser	Med +-symbolet legger du til tillatte sider
Svartelistede nettadresser	Med +-symbolet legger du til blokkerte sider
Kun spesifikke nettsteder	Bare spesifikt innhold kan vises, og dette kan du legge til med +-symbolet.

App-administrasjon

Enterprise App Manager

Installerte apper (kun på enhetsnivå)



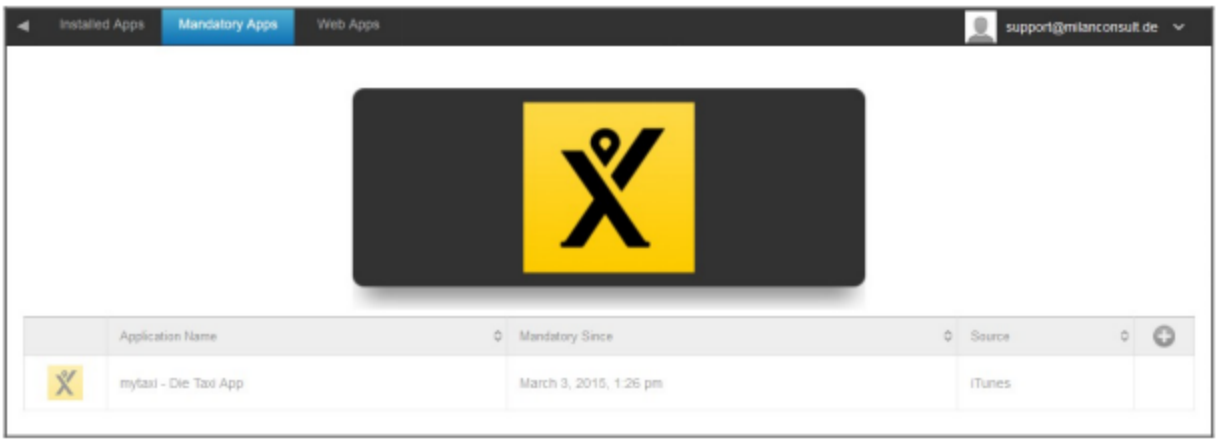
Her kan du se appene som for øyeblikket er installert på enheten.

Obligatoriske apper

Under Obligatoriske apper kan du aktivere nødvendige apper.

Brukeren vil kontinuerlig bli påminnet om å installere denne nevnte appen.

Via kan den obligatoriske appen defineres.



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

Hvis det dreier seg om en overvåket enhet, installeres appen automatisk.

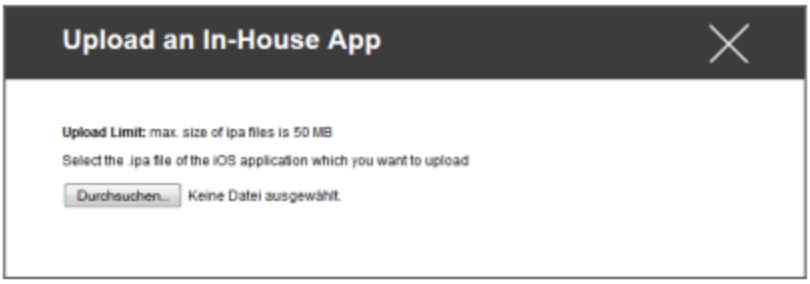
Du kan pushe en "Apple AppStore"-app fra den offentlige AppStore til enheten, i tillegg til en internt utviklet egenutviklet app.

Eller du kan velge fra kategorien "iOS In-House Apps" og velge en In-House App som du har lastet opp under Generelle innstillinger.

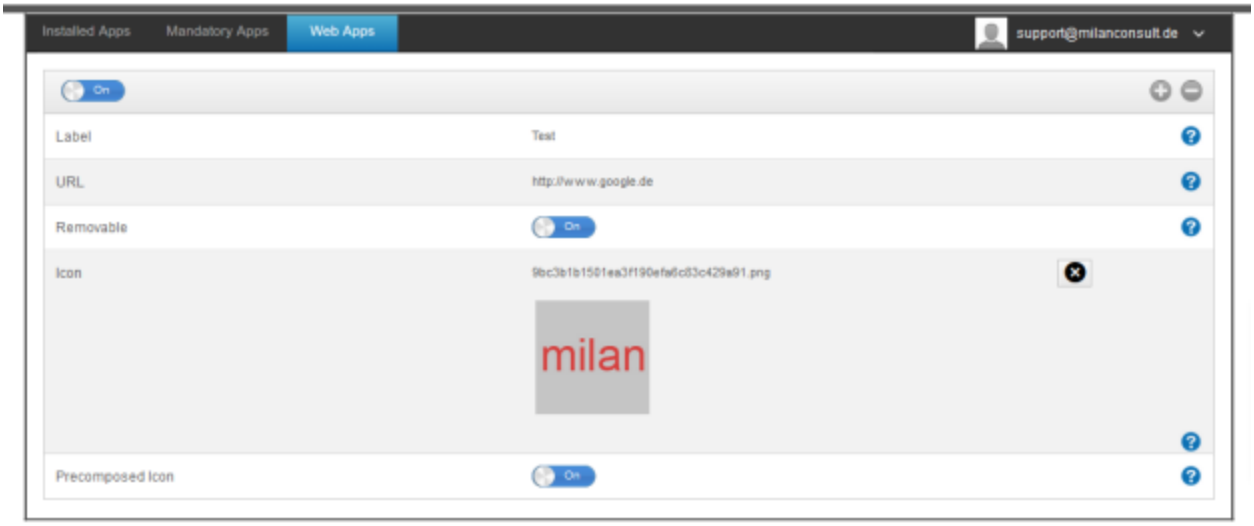
Installasjonsalternativer

Hold deg oppdatert (støttes kun for VPP per enhet)	En gang i uken vil det bli bestemt om det er en oppdatering for appen. Hvis ja, vil denne oppdateringen bli installert For interne apper vil oppdateringsmålet du har konfigurert i Generelle innstillinger, brukes til oppdateringsprosessen.
Forbikjøring når den ikke er administrert	Hvis appen allerede er installert, vil MDM ta over appen og administrere den
Fjern appen når MDM-profilen fjernes	Ved fjerning av enhetsadministrasjon vil appen bli avinstallert
Forhindre sikkerhetskopiering av appdata	Det vil ikke bli opprettet en sikkerhetskopi av app-spesifikke data
App-innstillinger	Under "App Settings" kan du tilordne appen visse verdier i forgrunnen (så lenge appen støtter det, spør om nødvendig appens utvikler).

Du kan også velge og laste opp en ipa-fil direkte via "Upload In-House App".



Web-apper



Under punktet "Web Apps" kan du, på samme måte som med "Web Clips", skyve internettsider eller intranettportaler som en applikasjon til sluttbrukerens enhet, i området Web Management. Som standard vises Web Apps i fullskjermmodus, men dette kan konfigureres under Webclips.

Etikett	Navn på tilkoblingen på sluttbrukerens enhet
URL	Lenke til det respektive nettstedet
Avtakbar	Hvis den er aktivert, kan brukeren fjerne webklippet
Ikon	Last opp en logo for tilkoblingen via denne dialogen: Dimensjoner 180x180, png-format
Prekomponert ikon	Hvis den er aktivert, vil ingen tilleggseffekter (skygge, refleksjon) vises på ikonet

Begrensninger og innstillinger

Svartelistede / hvitelistede apper

Her kan du angi hvilke apper som skal blokkeres (eller tillates), avhengig av innstillingene dine i "Generelle innstillinger". Ved å klikke på får du opp det kjente app-søket. Der kan du søke etter appene du ønsker å legge til.

Merk at en overvåket enhet er nødvendig for denne funksjonen

SysApp-begrensninger

Blokker bestemte apper eller funksjoner på enheten din

Tillat bruk av YouTube	Tillat bruk av YouTube
Tillat bruk av iTunes Store	Tillat bruk av iTunes Store
Tillat bruk av Safari	Tillat bruk av Safari
Aktiver autofyll	Tillater automatisk utfylling
Advarsel om maktmisbruk	Fremtvinger svindelvarselet
Aktiver JavScript	Gjør det mulig å bruke JavaScript
Blokker popup-vinduer	Blokkerer alle typer pup-ups
Tillat informasjonskapsler	Velg når Safari skal godta informasjonskapsler

App-VPN

Via symbolet kan du definere programmer som automatisk skal starte den valgte VPN-tilkoblingen ved oppstart.

App-innstillinger

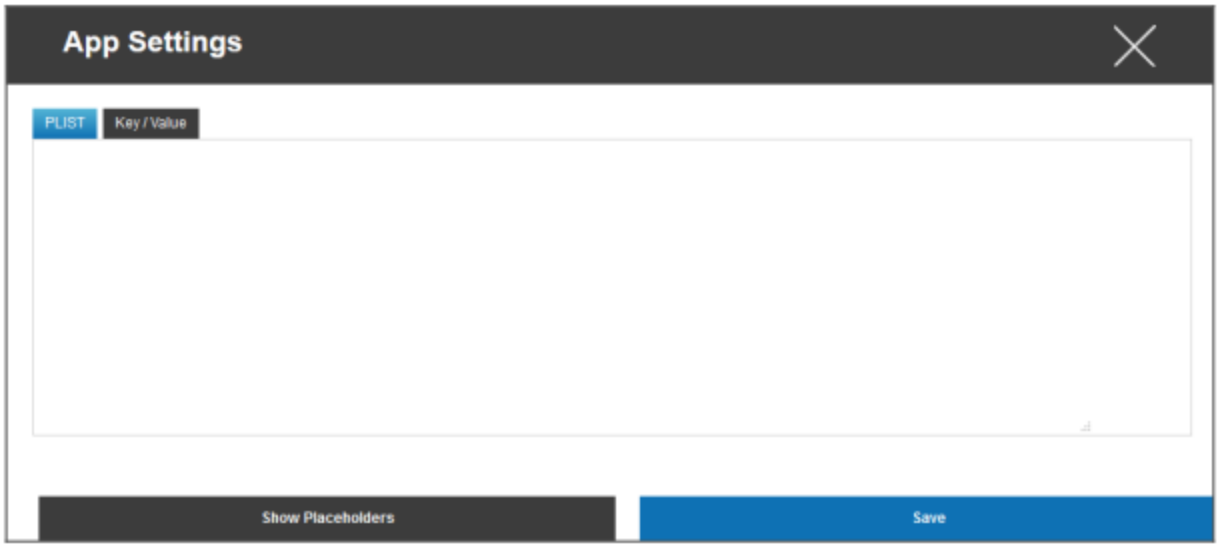
Under "App Settings" kan du tilordne appen visse verdier i forgrunnen (så lenge appen støtter det, spør om nødvendig appens utvikler).

Via symbolet legger du til en (ekstra) app. Du finner igjen den velkjente AppTec360-representasjonen av en App-Import.

Søk her etter appen du ønsker å konfigurere, og velg den. Innstillingene gjelder bare for apper som administreres.

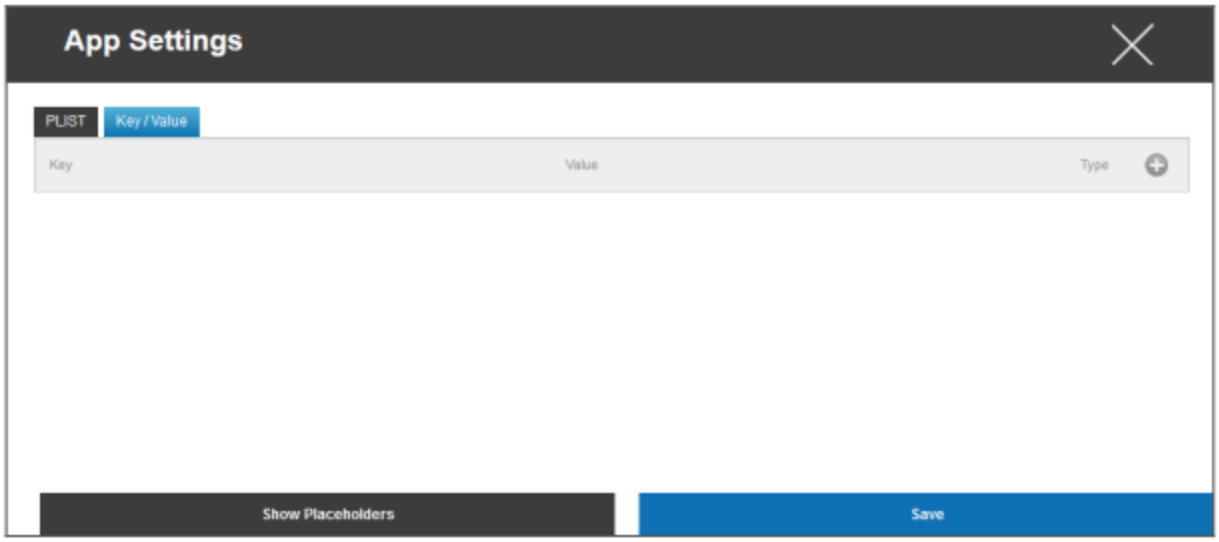
Hvis importen er vellykket, ser du følgende skjermbilde:

Nå kan du utføre en rekke konfigurasjoner med et klikk på . Du vil da få følgende oversikt:

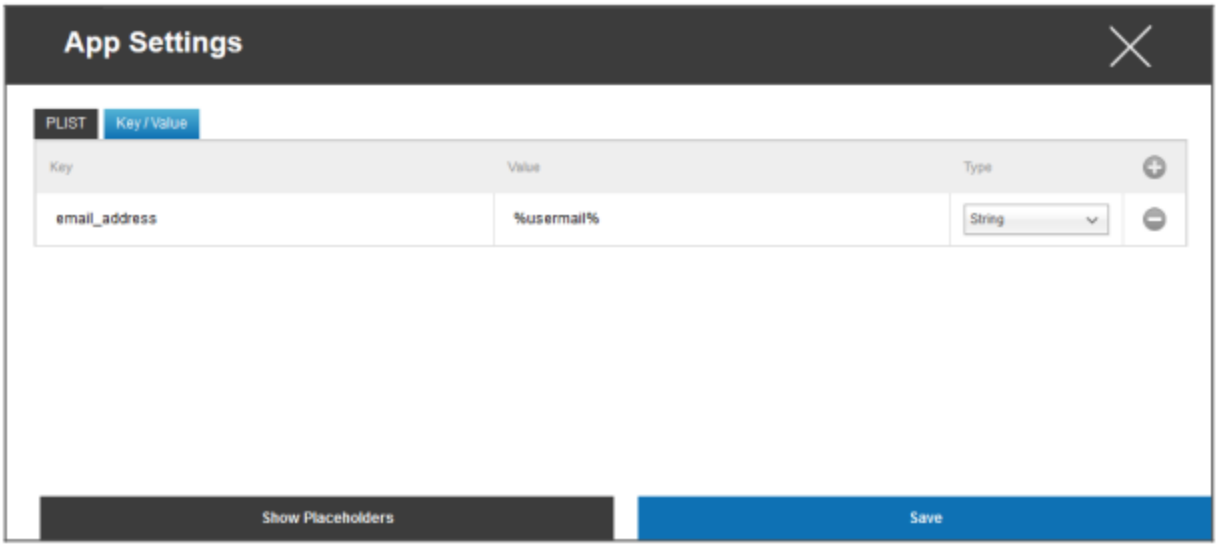


Hvis du allerede har en PLIST (kildetekst for konfigurasjon), kan du legge den til her og lagre det hele med "Save".

Under "Nøkkel/verdi" kan du knytte spesifikke konfigurasjoner til appen



Her kan du opprette en ny nøkkel og dens verdi med symbolet.



Alle AppTecs plassholdere står selvfølgelig til din disposisjon

"Type"-forklaring:

Streng	Tekst
Boolsk	Sant/usant
Antall	Antall

Med symbolet kan du fjerne en app igjen.

App Store for bedrifter

iTunes-apper

Under dette punktet kan du distribuere valgfrie apper til brukeren din.

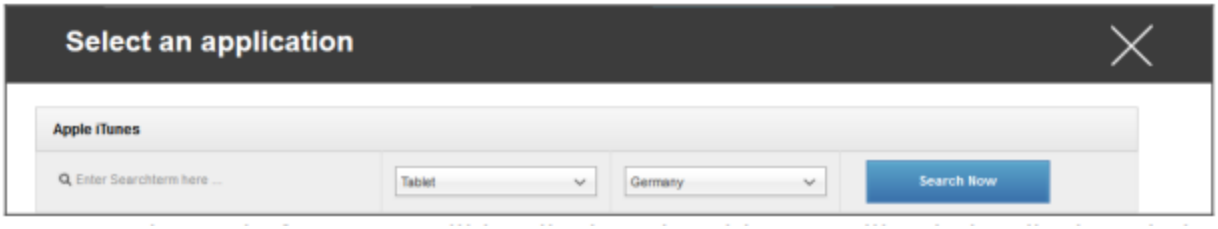
Hvis det finnes en app her, blir den automatisk installert på AppTec360 Store-enheten til sluttbrukeren.

Dette er ganske enkelt lenker til den offisielle Apple App Store. Av denne grunn må hver sluttbrukerenhet være utstyrt med en Apple-ID.

På dette tidspunktet anbefaler vi at hver bruker har sin egen Apple-ID.

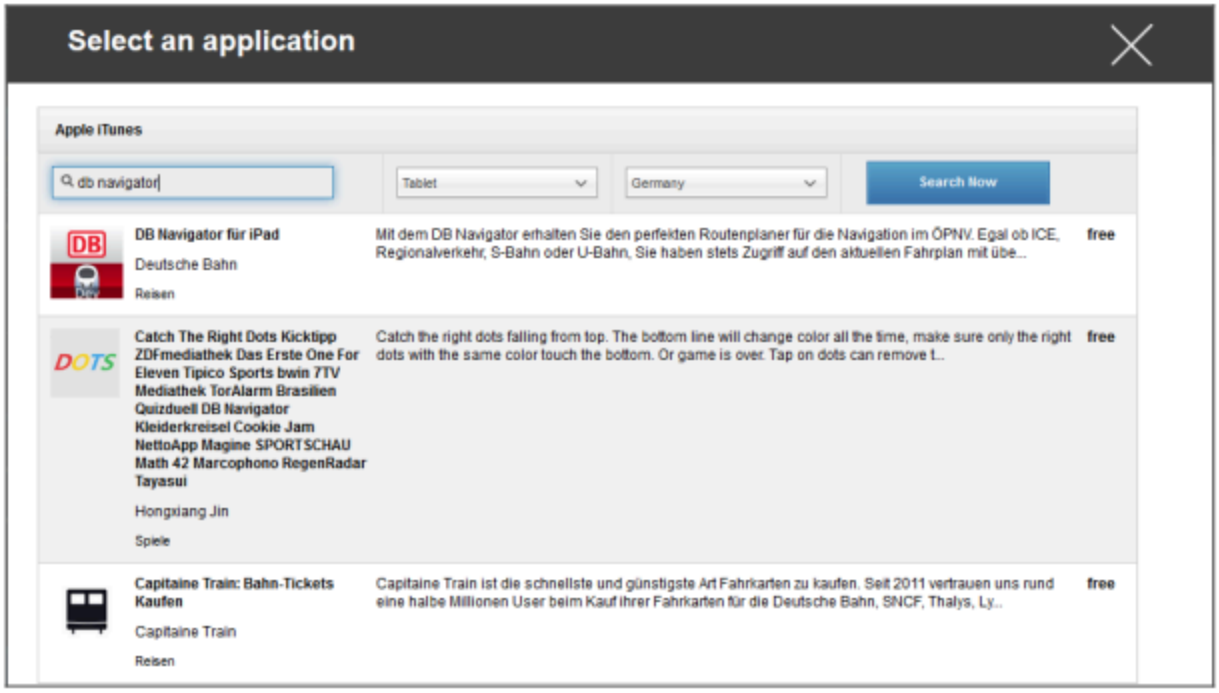
Med symbolet kan du legge til flere apper.

Deretter åpnes et vindu med følgende oversikt.



Vær oppmerksom på at bare gratisapper vises, mens betalte apper bare vises via VPN.

Under "Enter Search Term here ..." kan du søke etter en app som finnes i Apple App Store.



Når du klikker på ikonet eller på appens navn, blir du bedt om å utføre ytterligere konfigurasjoner.

Hold deg oppdatert	En gang i uken vil det bli bestemt om det er en oppdatering for appen. Hvis ja, vil denne oppdateringen bli installert
Fjern appen når MDM-profilen fjernes	Ved fjerning av enhetsadministrasjon vil appen bli avinstallert
Forhindre sikkerhetskopiering av appdata	Det vil ikke bli opprettet en sikkerhetskopi av app-spesifikke data
App-VPN	Velg en VPN-tilkobling, som vil starte når du åpner appen

Etter et klikk på "Install" legges appen til i Enterprise App Store og kan deretter installeres på sluttbrukerens enhet via AppTec360 AppStore.

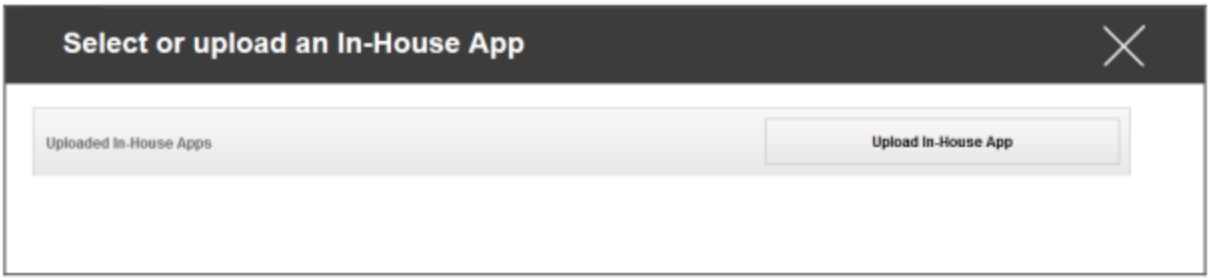
Hvis App-Store-importen er vellykket, får du følgende oversikt:

Internt

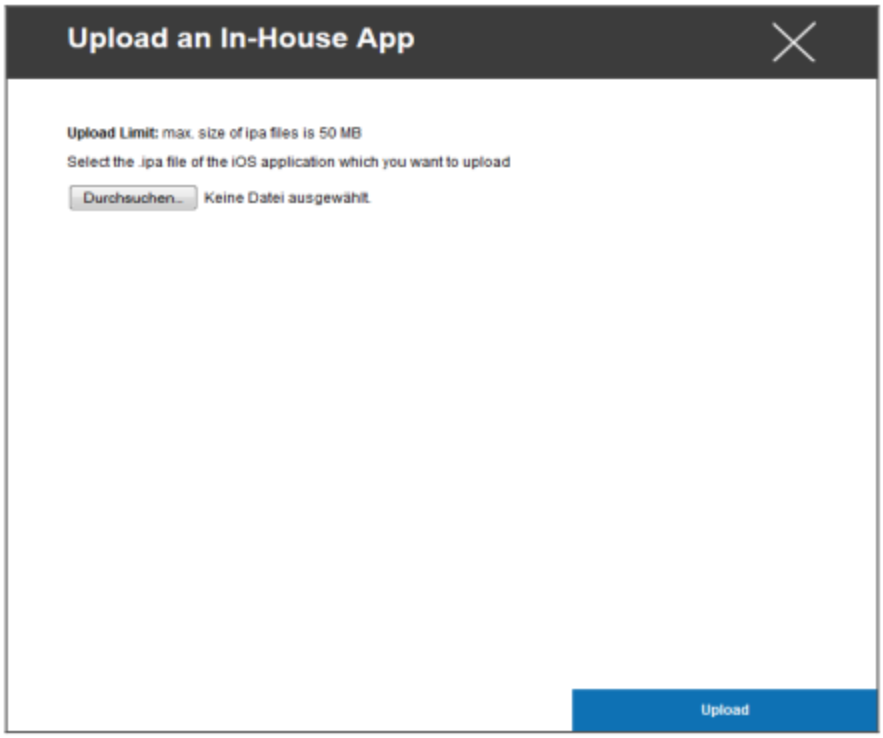
Under punktet "In-House" kan du laste opp internt utviklede apper og distribuere dem.

Med symbolet kan du distribuere flere In-House-apper.

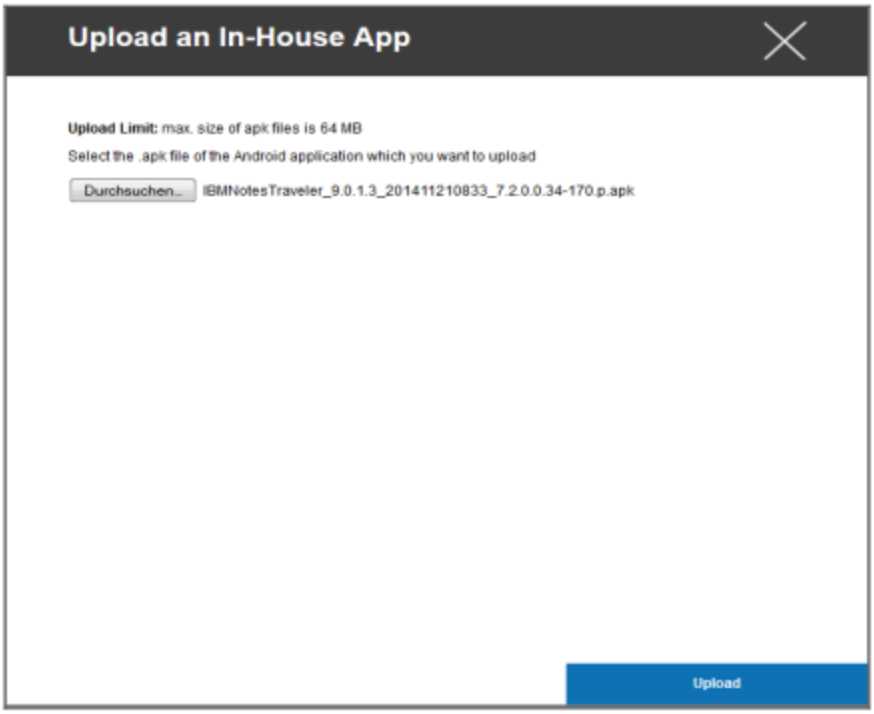
Hvis du aldri har distribuert In-House App før, vil du få følgende oversikt:



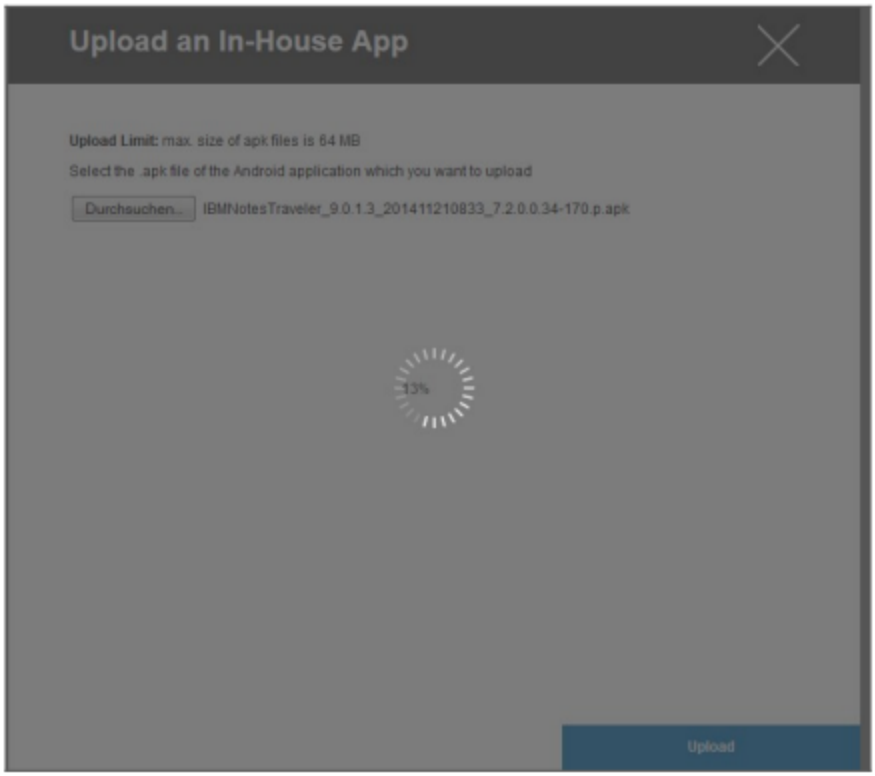
Klikk på "Last opp egen app", og du får opp følgende oversikt:



Nå velger du en .ipa-fil med "Søk ..." og klikker deretter på "Last opp"



Appen din vil nå bli lastet opp. I midten av sirkelen kan du se prosentandelen av hvor mye av appen din som allerede er lastet opp.



Hvis opplastingen av den interne appen er vellykket, vil du se den nylig opplastede appen i appkatalogen din.

Brukeren har nå muligheten til å se og installere denne appen i AppTec360 Store på sluttbrukerens enhet, under kategorien "In-House".

Siden dette ikke involverer en offentlig Apple AppStore-app, trenger ikke brukeren en lagret Apple-ID på sluttbrukerens enhet.

Kioskmodus

iOS Kiosk-modus er kun tilgjengelig i overvåket modus

Kioskmodus gjør det mulig å forhåndsdefinere en app eller URL, slik at det kun er mulig å kjøre/besøke denne appen/URL-en.

I tillegg kan du deaktivere ulike maskinvareknapper i kioskmodus.

Søknadstype

Pakke

Hvis du vil starte appen i kioskmodus, velger du "Pakke" under "Applikasjonstype"

Kiosk-applikasjon	Klikk her for å velge en app som skal starte i kioskmodus Her finner du den nåværende oversikten over App Management Du kan velge mellom "Apple iTunes Apps" og "iOS In-House Apps"

URL

Hvis du vil starte en URL i kioskmodus, velger du "URL" under "Applikasjonstype"

URL	Nå definerer du ønsket URL-adresse
Retningslinjer for samme opprinnelse	Hvis denne funksjonen er aktiv, kan brukeren bare surfe på undersidene til den forhåndsdefinerte URL-en Hvis du for eksempel har definert følgende URL: www.mypage.com, så kan brukeren surfe på www.mypage.com/subpage
Hvitelistede nettadresser	Her kan du vedlikeholde en hviteliste, og alle disse nettadressene er tillatt Maksimalt 1 URL per linje En URL må begynne med http:/ eller https://
Svartelistede nettadresser	Her kan du vedlikeholde en svarteliste, og alle disse nettadressene er ikke tillatt Maksimalt 1 URL per linje En URL må begynne med http:/ eller https://
Tøm nettleseren etter inaktivitet	Etter inaktivitet vil nettleserens hurtigbuffer tømmes
Avslutt passord aktivert	Hvis du aktiverer denne funksjonen, har brukeren mulighet til å avslutte Kioskmodus med et passord som du har forhåndsdefinert
Avslutt passord	Dette er passordet som er forhåndsdefinert av deg

Innstillinger for kioskmodus

Planlagt kioskmodus	Basert på tidspunktet på dagen kan du stille inn Kioskmodus, slik at modusen startes og avsluttes automatisk på et tidspunkt som er forhåndsbestemt.
Starttidspunkt	Starttidspunkt
Tid i minutter	Tid i minutter, etter hvilken Kioskmodus skal avsluttes igjen
Deaktiver berøring	Hvis aktivert, er berøringsskjermen deaktivert
Deaktiver enhetsrotasjon	Hvis den automatiske skjermtilpasningen er aktivert, deaktiveres den
Deaktiver ringetone-bryter	Hvis den er aktivert, vil ringeknappen bli deaktivert. Fra da av er atferden avhengig av den tidligere innstilte funksjonen
Deaktiver volumknappene	Hvis den er aktivert, vil volumknappene deaktiveres
Deaktiver Sleep Wake-knappen	Hvis den er aktivert, vil av/på-bryteren deaktiveres
Deaktiver automatisk låsing	Hvis den er aktivert, vil enheten ikke bli satt i standby-modus
Aktiver Voice Over	Hvis den er aktivert, aktiveres Voice Over Assistant
Aktiver zoom	Hvis den er aktivert, vil zoomen aktiveres
Aktivere inverterte farger	Hvis den er aktivert, aktiveres den inverterte visningsmodusen
Aktiver berøringshjelpemidler	Hvis den er aktivert, aktiveres AssistiveTouch
Aktivere talevalg	Hvis den er aktivert, aktiveres talevalget
Aktiver Mono Audio	Hvis den er aktivert, aktiveres Mono Audio
VoiceOver	Hvis den er aktivert, kan brukeren aktivere VoiceOver
Zoom	Hvis den er aktivert, kan brukeren aktivere Zoom
Inverter farger	Hvis den er aktivert, kan brukeren aktivere inverterte farger
Assistive Touch	Hvis den er aktivert, kan brukeren aktivere berøringshjelpemidler

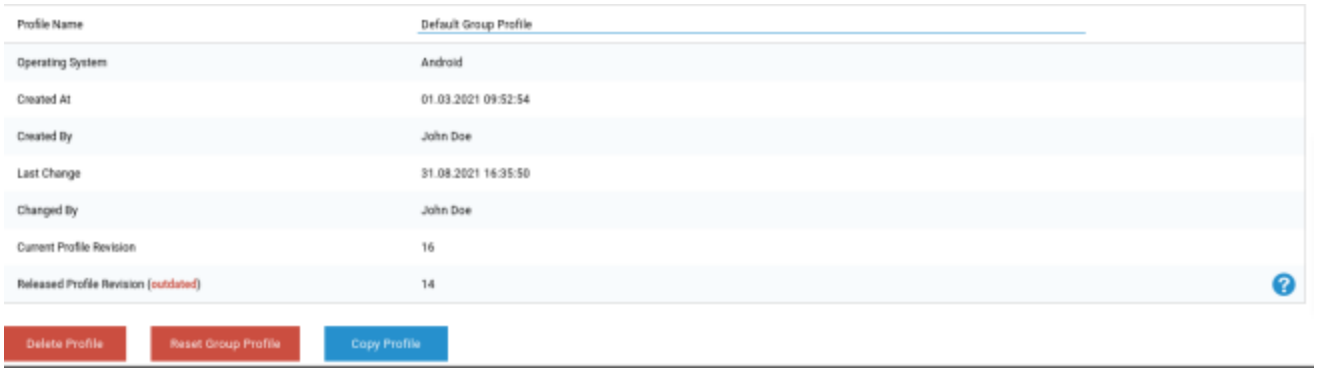
Android Enterprise – fullstendig administrert enhetskonfigurasjon

Avhengig av om du har valgt en gruppeprofil eller en enhet, vil oversikten og underpunktene være forskjellige - vær nøye med dette!

Generelt

Oversikt over gruppeprofiler (kun på gruppenivå)

Når du åpner en gruppeprofil, får du en rask oversikt over profilen.



Profilnavn	Navn på profilen (kan endres her)
Operativsystem	Operativsystemet profilen er beregnet på
Opprettet på	Tidspunktet for skapelsen
Opprettet av	Skaperen av profilen
Siste endring	Tidspunkt for siste endring av profilen
Endret av	Konto som gjorde de siste endringene
Nåværende profilrevisjon	Revisjon av lagret profilstatus
Utgitt profilrevisjon	Tilordnet profilrevisjon ("Tilordne nå"). Hvis etiketten viser "(utdatert)" bak teksten, betyr det at du har lagret profilen, men ikke tilordnet den ennå, slik at enhetene fortsatt vil få en eldre versjon.

Enhetsoversikt (kun på enhetsnivå)

Hvis du befinner deg på en enhet, vil du få en oversikt over den valgte enheten, og her finner du følgende:

Enhetens navn	Enhetens navn
Beliggenhet	Koordinater for plassering
Telefonnummer	Telefonnummer
Tildelte obligatoriske apper	Antall tildelte obligatoriske apper
OS-versjon	OS-versjon av enheten
Operativsystem	Operativsystem (Android Enterprise)
Serienummer	Enhetens serienummer
Eierskap til enheten	Bedrifts- eller privat enhet
Enhetstype	AE Arbeidsstyrt enhet
Rotfestet	Status, som angir om enheten har blitt rotfestet
Overensstemmende	I samsvar med retningslinjene
IP-adresse	IP-adressen til enheten
Sist sett	Tidspunkt for når enheten sist ble koblet til AppTec
Siste fremstøt	Tidspunkt for når siste push ble sendt til enheten
AE Device Owner-modus	Ja
Tildeling av bruker	Brukeren eller gruppen denne enheten er tilordnet til

Konfigureringsrevisjon (kun på enhetsnivå)

Her får du en oversikt over hvilken gruppeprofil som er tilordnet enheten.

Hvis du klikker på gruppeprofilen, får du direkte tilgang til denne profilen, og du kan utføre innstillinger.

Med dette symbolet kan du tilbakestille de distribuerte appene til gruppeprofilens innstillinger.

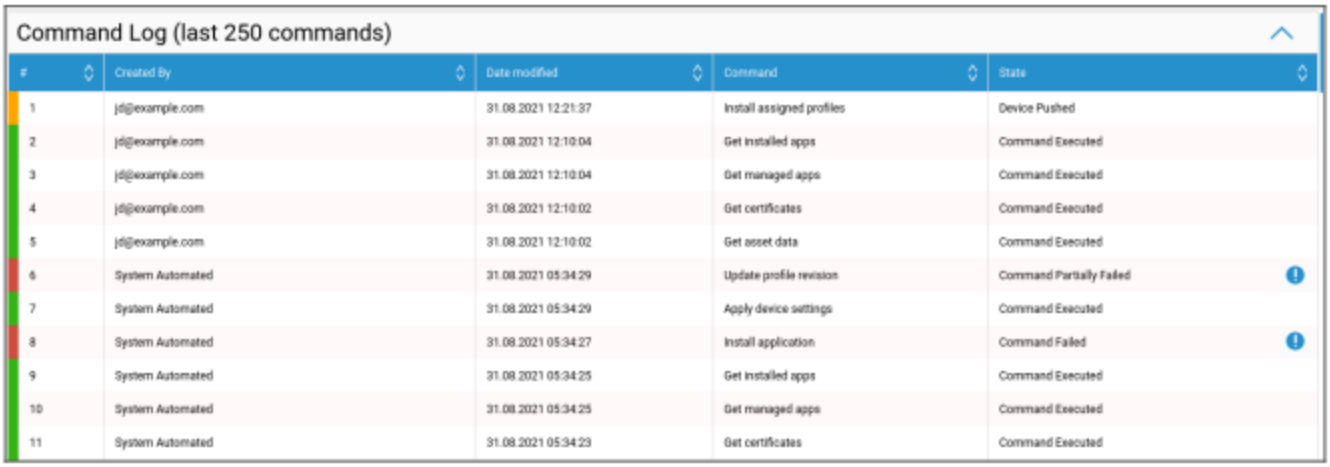
Med dette symbolet kan du tilbakestille alle appene som brukes, til gruppeprofilens innstillinger.

"Nyere revisjon tilgjengelig" indikerer at gruppeprofilen har blitt endret og lagret, men ikke tilordnet. Gruppeprofilen må tilordnes med "Tilordne nå" på gruppenivå for at endringene skal gjelde for enhetene.

Enhetslogg (kun på enhetsnivå)

Kommandologg

Her kan du se hvilke kommandoer som er utstedt for enheten, og hvilken status de har.



Kommandoer som opprettes av "System Automated", opprettes automatisk av systemet.

Mulige kommandostatuser

Enhet skjøvet	En push-forespørsel har blitt sendt til push-tjenesten (f.eks. APNS) for å be enheten om å koble seg tilbake til EMM-serveren.
Kommando opprettet	Kommandoen ble opprettet i systemet.
Kommando sendt	Kommandoen ble sendt til enheten etter at den ble koblet til serveren.
Kommando utført	Kommandoen ble vellykket utført.
Kommando mislyktes	Kommandoen mislyktes. *
Kommandoen mislyktes delvis	Avhengig av enhetens operativsystem kan enkelte kommandoer bli gruppert sammen. I dette mislyktes noen deler av denne kommandogruppen. *
Kommando utført, men mislyktes til slutt	Kommandoen ble utført, men kanskje ikke.
Kommando Repushed	Kommandoen ble sendt på nytt av en bruker.
Kasseres	Kommandoen ble forkastet. For eksempel fordi den ble erstattet av en annen kommando, eller fordi enheten ble registrert på nytt og gamle kommandoer ble fjernet.

Hvis det er et utropstegn bak meldingen, kan du få mer informasjon ved å holde musepekeren over ikonet.

Enhetsinnstillinger

Klientkonfigurasjon

Her kan du utføre følgende konfigurasjoner på Android-enheten din:

Tid utenfor samsvar	Tidsgrensen for brukersvar etter hvilken håndhevelseshandlingen iverksettes.
Håndhevingstiltak etter tidsavbrudd	Håndhevingstiltak når en bruker ikke utfører handlinger som fører til en kompatibel enhetsstatus
Datainnsamlingsfrekvens	Hyppighet for innsamling av enhets-/GPS-informasjon
Enhetens hjerteslagsfrekvens	Intervall som enheten skal kontakte AppTec360 Server med Min. 1 minutt Maks. 24 timer
Aktiver posisjonsoppdateringer	Hvis den er aktivert, sender enheten posisjonsoppdateringer til AppTec360 Server
Sted Oppdateringstidspunkt	Bestemmer i hvilke tidsintervaller enheten sender posisjonsoppdateringer til AppTec360
Bruk Google Location Accuracy for stedsoppdatering	Hvis den er aktivert, vil nettverksposisjonen brukes for posisjonsoppdateringer (hvis den er deaktivert under "Begrensninger", vil denne innstillingen ikke påvirke noe)
Bruk GPS-posisjon for posisjonsoppdatering	Hvis den er aktivert, vil GPS-enheten brukes til posisjonsoppdateringer
Tillat fiktive (falske) lokasjoner	Gjør det mulig å forfalske posisjonsinformasjon via tredjepartsapper
Tapt forbindelse Handling	Hvis denne funksjonen er aktivert, kan du angi en handling for det tilfellet at en enhet ikke får forbindelse til MDM-serveren i løpet av hjerteslagintervallet. Hvis enheten for eksempel har en hjerteslagstid på 5 minutter, kobler den seg til serveren kl. 10:35. Deretter forlater enheten Wi-Fi-området. Neste hjerteslag kl. 10:40 vil mislykkes, og den angitte handlingen vil bli utført.
Handling	Hvilke tiltak som skal iverksettes så snart en enhet ikke lenger er i samsvar med kravene. • Lock Device = låseenhet • Wipe Device = enheten gjenopprettes til fabrikkinnstillingene

	• Wipe Device & SD Card = enheten gjenopprettes til fabrikkinnstillingene, og SD-kortet slettes
Terskelverdi	Du kan angi en terskelverdi for antall mislykkede hjerteslag som er nødvendig for å utløse den angitte handlingen.

Policyhåndhevelsesmodus	Standard:	Brukerne vil med jevne mellomrom bli bedt om å utføre utestående handlinger
	Lazy Policy Enforcement:	Brukerne vil aldri bli bedt om å utføre utestående handlinger. Alle åpne handlinger vil vises i AppTec360 Client
	Aggressiv håndheving av retningslinjer:	Brukerne blir kontinuerlig bedt om å utføre utestående handlinger
AppTec360 Versjonslås	Hvis aktivert, kan en versjonskode for AppTec360 MDM-klienten spesifiseres. AppTec360-klienten vil kun oppdatere til den angitte versjonen. Nyere versjoner vil bli ignorert. En nedgradering er IKKE mulig.	
Versjonskode	Versjonskode for AppTec360 MDM-klienten som skal låses til.	
Deaktiver AppTec360-varsling	Hvis den er deaktivert, vil AppTec360-klienten ikke vise en varsling i varslingslinjen. Dermed kan brukere lukke AppTec360-klienten via oppgavebehandling. Hvis AppTec360-klienten er lukket, vil flere funksjoner, inkludert Kioskmodus og App Black/Whitelisting, ikke fungere som de skal. Samsung-enheter tilbyr en beskyttelsesmekanisme for AppTec360 Client. Varslingen er deaktivert som standard på Samsung-enheter som støtter KNOX API-er. Varselet skal ikke være deaktivert på enheter med Android 8.0 eller nyere.	

Bakgrunn

Angi egendefinert bakgrunnsbilde	Aktivere/deaktivere den egendefinerte bakgrunnen
Bakgrunn	Still inn bakgrunnsmodus til å bruke en fargekode eller et bilde
Angi en farge	Angi en bakgrunnsfarge som heks-verdi, f.eks. #000000 for svart eller #ffffff som hvit
Angi bilde som bakgrunnsbilde	Last opp bildefilen du vil bruke som bakgrunnsbilde

Asset Management (kun på enhetsnivå)

Enhetsinfo

Modell	Modellbetegnelse for enheten
Operativsystem	OS
OS-versjon	OS-versjon
Serienummer	Serienummer
Enhetens navn	Enhetens navn
Batteristatus	Batteristatus
Ledig / totalt minne	Ledig / totalt minne
Samsung Safe	Samsung SAFE-grensesnitt, nødvendig for en rekke innstillingsalternativer
SD-kort tilgjengelig	SD-kort tilgjengelig
SD-kort emulert	SD-kort emulert
SD-kortet kan tas ut	SD-kortet kan tas ut
SD ledig / totalt minne	SD ledig / totalt SD-kortminne

Wi-Fi

IP-adresse	Enhetens IP-adresse
WiFi MAC	WiFi MAC-adresse

Cellular

Status	Status (SIM-kort installert)
Telefonnummer	Telefonnummer
Roaming (tale/data)	Roaming for tale/data
Roaming-status	Gjeldende roamingstatus
IP-adresse	IP-adresse
Operatør/transportør	Operatør/transportør
Cellular Technology	Cellular Technology
IMEI	IMEI-nummer
ICCID	Dette er ID-en for SIM-kortet, ofte også et smartkort eller Integrated Circuit Card (ICC)
IMSI	International Mobile Subscriber Identity (IMSI) gir i GSM- og UMTS-mobilnett en sikker identifikasjon av nettverksbrukerne IMSI består av maksimalt 15 sifre og konfigureres på følgende måte: • Mobil landskode (MCC), 3 siffer • Mobilnettverkskode (MNC), 2 eller 3 siffer • Identifikasjonsnummer for mobilabonnent (MSIN), 1-10 siffer
Nåværende MCC/MNC	Se "SIM MCC/MNC"
SIM MCC/MNC	Mobile Country Code er en etablert landidentifikator som er fastsatt av ITU i henhold til E.212-standarden. Denne fungerer sammen med Mobile Network Code (MNC) for identifikasjon av mobilnettverket. Betyr SIM-kortets lands-/mobilnettverkskode. Hvis du roamer til et annet mobilnett, vil "Current MCC/MNC" og "SIM MCC/MNC" logisk sett være forskjellige.

Bluetooth

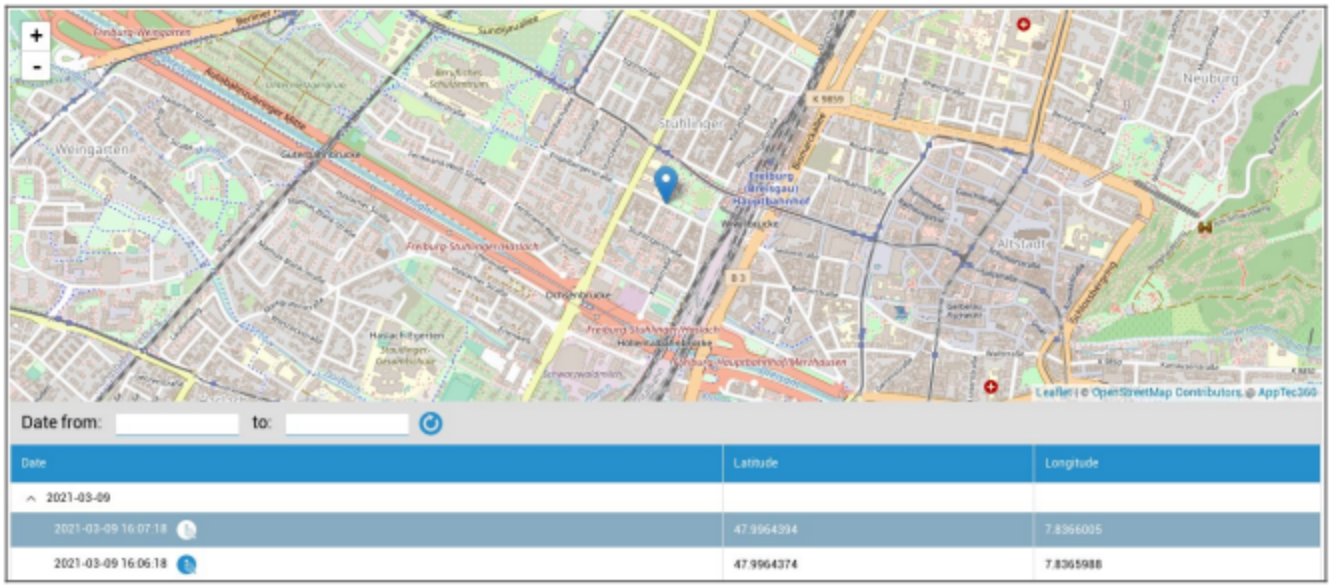
Bluetooth MAC	Bluetooth MAC-adresse

Sikkerhetsstyring

Tyverisikring (kun på enhetsnivå)

GPS-informasjon (kun på enhetsnivå)

Her kan du angi enhetens nåværende/seneste plassering. Lokaliseringen kan beskyttes med ett eller til og med to passord - se: Generelle innstillinger - Personvern - GPS-tilgang



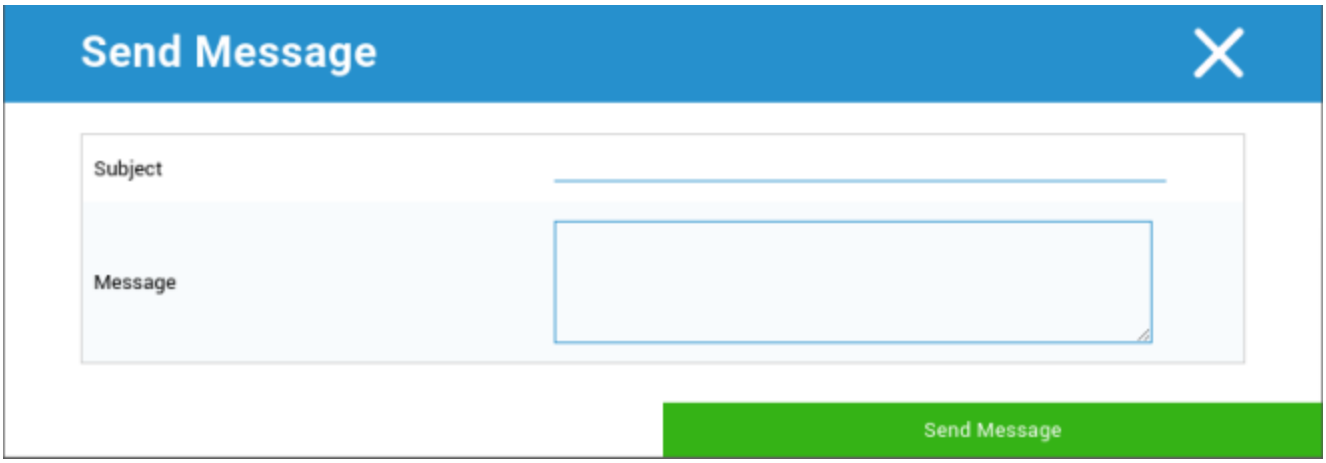
Tørk og lås (kun på enhetsnivå)

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

Full Wipe	Enheten tilbakestilles til fabrikkinnstillingene (både bedriftsdata og personlige data slettes)
Enterprise Wipe	Kun bedriftsdata fjernes fra sluttbrukerens enhet (alle apper, data osv. som ble levert av AppTec360)
Låseskjerm	Skjermlåsen er aktivert, og det er tilstrekkelig å låse opp enheten med enhetens passord/PIN-kode

Melding (kun på enhetsnivå)

Her kan du fylle inn emne og en melding og sende den til en sluttbrukerenhet.



Sikkerhetskonfigurasjon

Enhetens passord

Under "Passord" kan du angi et passord for enheten, og følgende innstillingsalternativer er tilgjengelige

Minimum passordlengde	Fastsetter det minste antallet symboler et passord må inneholde	
Passordkvalitet	Uspesifisert	Denne policyen stiller ingen krav til passordet.
	Biometrisk svakhet	Denne policyen åpner for biometrisk gjenkjenningsteknologi med lav sikkerhet. Dette innebærer teknologi som kan gjenkjenne identiteten til en person til omtrent en tresifret PIN-kode (falsk gjenkjenning er mindre enn 1 av 1 000).
	Noe	Denne policyen krever at det angis et passord eller et mønster, men den håndhever ingen spesifikke regler.
	Alfabetisk	Brukeren må ha angitt et passord som inneholder minst alfabetiske tegn (eller andre symboler).
	Alfanumerisk	Brukeren må ha angitt et passord som inneholder minst både numeriske og alfabetiske tegn (eller andre symboler).
	Kompleks	Som standard må brukeren ha angitt et passord som inneholder minst en bokstav, et tall og et spesialsymbol. Med denne passordkvaliteten kan passordene begrenses til å inneholde ulike sett med tegn, for eksempel minst en stor bokstav osv.
Minimum passordlengde	Angi antall tegn som kreves for passordet. Du kan for eksempel kreve at PIN-koden eller passordet skal inneholde minst seks tegn.	
Minimum antall siffer som kreves i passordet	Minimum antall siffer som kreves i passordet	
Minimum små bokstaver kreves i passordet	Minimum små bokstaver kreves i passordet	
Minimum store bokstaver kreves i passordet	Minimum store bokstaver kreves i passordet	
Minimum antall tegn som ikke er bokstaver	Minimum antall tegn som ikke er bokstaver som kreves i passordet	

som kreves i passordet	
Minimum symboler som kreves i passordet	Minimum symboler som kreves i passordet

Lås for maksimal inaktivitetstid	Maksimal brukerinaktivitet frem til tidslås
Tidsavbrudd for utløp av passord	Etableres, etter hvilket tidsintervall passordet utløper og et nytt passord må utstedes
Begrensning av passordhistorikk	Antall tidligere brukte passord som ikke er tillatt
Maksimalt antall mislykkede passordforsøk	Fastsetter hvor ofte et passord kan tastes inn feil før en fullstendig sletting av enheten vil bli utført
Tillat biometrisk autentisering	Muliggjør autentisering via fingeravtrykk eller irisskanning. Kun for Samsung KNOX 2.1 og nyere

AntiVirus

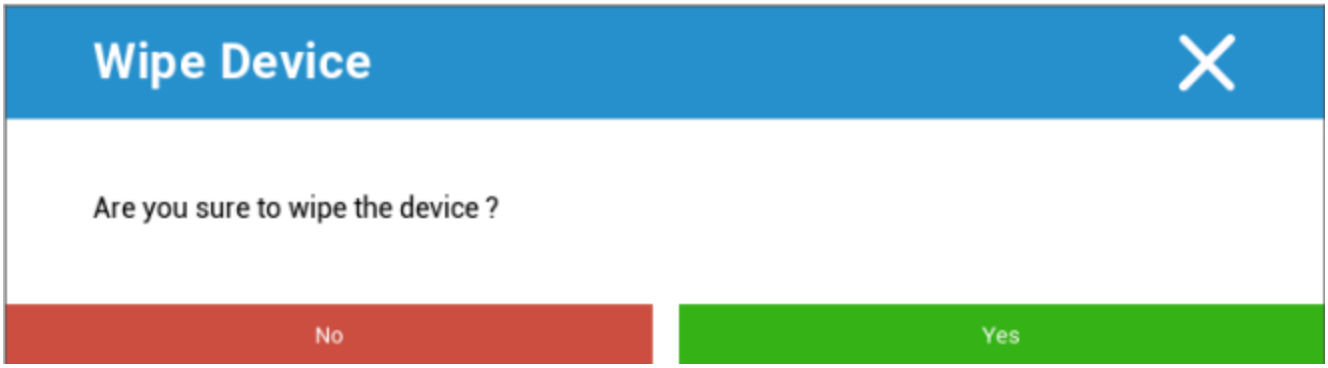
Automatisk skanning	Aktiver periodiske automatiske skanninger
Skanneintervall	Intervall for undersøkelse (Quick / Full)
Full automatisk skanning	Aktiver helautomatiske skanninger
Automatiske oppdateringer	Aktiver automatiske oppdateringer
Intervall for oppdateringssjekk	Hvor ofte appen og databasen bør oppdateres (virus/skadet kode)
App-beskyttelse	Aktiver automatisk appskanning
Beskyttelse av SD-kort	Aktiver automatisk skanning av SD-kort
Kun Wi-Fi-oppdatering	Når denne funksjonen er aktivert, vil oppdateringer bare bli brukt når enheten er koblet til et Wi-Fi-nettverk

End of Life (kun på enhetsnivå)

Tørk (kun på enhetsnivå)

Under "Wipe" kan du gjenopprette enheten til fabrikkinnstillingene. Her slettes bedriftsdataene og de private dataene på sluttbrukerens enhet.

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



Med "Yes" kan du utføre tørkingen.

Under "Wipe Report" kan følgende elementer vises

Tørket av	Historikk over hvem som utførte tørkingen
Dato	Dato
Status	Status (f.eks. om tørkingen ble vellykket)

Begrensningsinnstillinger

Begrensninger

Her kan en rekke ting begrenses og blokkeres.

Aktiver kamera	Tillat bruk av kamera	
Tving automatisk synkronisering	På	Synkronisering er permanent aktivert
	Av	Synkroniseringen er permanent deaktivert
	Brukerens valg	Valgt av brukeren
Force Bluetooth	På	Bluetooth er permanent aktivert
	Av	Bluetooth er permanent deaktivert
	Brukerens valg	Valgt av brukeren
Force GPS	På	GPS er permanent aktivert
	Av	GPS er permanent deaktivert
	Brukerens valg	Valgt av brukeren
Styrkenettverkets plassering	På	Permanent lokalisering på internett
	Av	Permanent deaktivering av internettlokalisering
	Brukerens valg	Valgt av brukeren

Sikkerhet		
Ikke tillat delingsplassering	Angir om en bruker ikke kan slå på stedsdeling.	
Ikke tillat sikker oppstart	Angir om brukeren ikke har lov til å starte enheten på nytt i sikker oppstartsmodus.	
Tillat ikke tilbakestilling av nettverk	Angir om en bruker ikke kan tilbakestille nettverksinnstillinger fra Innstillinger.	
Tillat ikke tilbakestilling til fabrikkinnstilling	Angir om en bruker ikke har lov til å tilbakestille enheten.	
Aktiver ADB	Gjør det mulig å koble til en PC via ADB	
Deaktiver Keyguard	Deaktiverer Keyguard	
Info om enhetsinnehaverens låseskjerm	Angir hvilken informasjon om enhetens eier som skal vises på låseskjermen.	
Håndhevelse av samsvar	Modus Prompt Bruker	Brukeren blir bedt om å utføre de nødvendige handlingene.
	Mode Lock-Down Container	Skjul alle apper til alle krav er oppfylt

App-administrasjon	
Tillat kobling av apper på tvers av profiler	Tillater at apper i den overordnede profilen kan håndtere nettlenker fra den administrerte profilen.
Ikke tillat appkontroll	Angir om en bruker ikke kan endre programmer i Innstillinger eller startprogrammer.
Ikke tillat appinstallasjon	Angir om en bruker ikke har tillatelse til å installere programmer.
Ikke tillat avinstallering av apper	Angir om en bruker ikke har lov til å avinstallere programmer.
Retningslinjer for kjøretidstillatelser	Angir hvordan nye tillatelsesforespørsler fra apper skal håndteres.
Tillat ukjente kilder	Hvis denne funksjonen er aktivert, kan brukerne laste ned apper ved å installere en .apk-fil.

Tilkoblingsmuligheter	
Ikke tillat mobilnettverkskonfigurasjon	Angir om en bruker ikke har lov til å konfigurere mobilnettverk.
Ikke tillat tethering-konfigurasjon	Angir om en bruker ikke har lov til å konfigurere nettdeling og bærbare hotspots.
Ikke tillat VPN-konfigurasjon	Angir om en bruker ikke skal tillates å konfigurere et VPN.
Ikke tillat Wifi-konfigurasjon	Angir om en bruker ikke har lov til å endre WiFi-tilgangspunkt.
Ikke tillat utgående NFC-stråle	Angir om brukeren ikke har lov til å bruke NFC til å sende ut data fra apper.
Lås WiFi-konfigurasjon	Denne innstillingen kontrollerer om WiFi-konfigurasjoner som opprettes av en enhetseier-app, skal være låst (det vil si at de bare skal kunne redigeres eller fjernes av enhetseier-appen, ikke engang av Innstillinger-appen).
Aktivere dataroaming	Aktiverer dataroaming

Bluetooth	
Ikke tillat Bluetooth	Angir om Bluetooth ikke er tillatt på enheten. Krever Android 8.0
Ikke tillat Bluetooth-deling	Angir om utgående Bluetooth-deling ikke er tillatt på enheten. Krever Android 8.0
Ikke tillat Bluetooth-konfigurasjon	Angir om en bruker ikke har lov til å konfigurere Bluetooth.

Kontoadministrasjon	
Ikke tillat å legge til administrert profil	Angir om en bruker ikke kan legge til administrerte profiler. Krever Android 8.0
Ikke tillat å legge til brukere	Angir om en bruker ikke kan legge til nye brukere.
Ikke tillat Fjern administrert profil	Angir om administrerte profiler for denne brukeren kan fjernes av andre enn profileieren. Krever Android 8.0
Ikke tillat endring av konto	Angir om en bruker ikke kan legge til og fjerne kontoer, med mindre de er lagt til programmatisk av Authenticator.

Telefoni	
Forby utgående anrop	Angir at brukeren ikke har lov til å foreta utgående telefonsamtaler.
Ikke tillat SMS	Angir at brukeren ikke har lov til å sende eller motta SMS-meldinger.

System	
Ikke tillat oppretting av vindu	Angir at det ikke skal opprettes andre vinduer enn appvinduer.
Ikke tillat å angi brukerikon	Angir om en bruker ikke har lov til å endre ikonet sitt.
Ikke tillat Set Wallpaper	Brukerbegrensning for å ikke tillate innstilling av bakgrunnsbilde.
Deaktiver statuslinjen	Deaktivering av statuslinjen blokkerer varsler, hurtiginnstillinger og andre skjermoverlegg som gjør det mulig å flykte fra en enhet som bare brukes én gang.
Aktiver automatisk tid	Stiller inn klokkeslettet automatisk.
Aktiver automatisk tidssone	Stiller inn tidssonen automatisk.
Holdes på mens du er koblet til	Enheten forblir aktiv mens den er koblet til en strømkilde.

Lagring	
Ikke tillat deaktivering av appverifisering	Angir om en bruker ikke har lov til å deaktivere programverifisering.
Ikke tillat montering av fysiske medier	Angir om en bruker ikke har lov til å montere fysiske eksterne medier.
Aktiver sikkerhetskopieringstjeneste	Backup-tjenesten administrerer alle mekanismer for sikkerhetskopiering og gjenoppretting på enheten. Hvis du setter denne til false, forhindres data fra å bli sikkerhetskopiert eller gjenopprettet. Sikkerhetskopieringstjenesten er av som standard. Krever Android 8.0
Aktiver USB-masselagring	Aktiverer bruk av USB-masselagring.

Tastatur	
Ikke tillat autofyll	Angir om en bruker ikke har lov til å bruke Autofyll-tjenester. Krever Android 8.0
Ikke tillat kopiering og liming mellom profiler	Angir om det som kopieres til utklippstavlen i denne profilen, kan limes inn i relaterte profiler.

Lyd	
Ikke tillat volumjustering	Angir om en bruker ikke kan justere hovedvolumet.
Ikke tillat Slå av mikrofonen	Angir om en bruker ikke kan justere mikrofonvolumet.
Mute-enhet	Mute-enhet.

Sertifikatforvaltning

Her kan du distribuere betrodde sertifikater og identitetssertifikater til enhetene dine.

Android 8 eller nyere er nødvendig for å distribuere betrodde sertifikater, og Android 9 eller nyere er nødvendig for å distribuere identitetssertifikater.

Med "+" kan du legge til flere sertifikater.

Klarerte sertifikater må være i PEM-format.

Identitetssertifikater må være i PKCS12-format

Administrasjon av tilkoblinger

Wifi

For denne innstillingen må du utføre forhåndskonfigurasjon av sluttbrukerens enheter for tilgang til interne Access
-punkter

Services Set Identifier (SSID)	SSID for nettverket som skal kobles til
Skjult nettverk	Aktiver, i tilfelle AP-et ikke kringkaster SSID

Sikkerhetstype

Fastsette AP-ets sikkerhetstype

WEP

Passord	Passord for AP

WPA/WPA2

Passord	Passord for AP

802.1x EAP

EAP-metode

PWD	Identitet	Identitet
	Passord	Passord

PEAP	Fase 2 autentiseringsprotokoll	ingen	Ingen tilleggsprotokoll
		MSCHAPV2	MSCHAPV2-protokollen
		GTC	GTC-protokoll
	CA-sertifikat	CA-sertifikat	
	Identitet	Identitet	
	Anonym identitet	Anonym identitet	
	Passord	Passord	

TTLS	Fase 2 autentiseringsprotokoll	ingen	Ingen tilleggsprotokoll
		PAP	PAP-protokoll
		MSCHAP	MSCHAP-protokollen
		MSCHAPV2	MSCHAPV2-protokollen
		GTC	GTC-protokoll
	CA-sertifikat	CA-sertifikat	
	Identitet	Identitet	
	Anonym identitet	Anonym identitet	
	Passord	Passord	

TLS	CA-sertifikat	CA-sertifikat
	Identitet	Identitet
	Passord	Passord

VPN

Navn på tilkobling	Navn på VPN-tilkoblingen

VPN-type

VPN

VPN-klient

AppTec360 VPN-klient	
Gateway-konfigurasjon	Velg Gateway VPN-konfigurasjon (se **Generelle innstillinger > Universal Gateway > VPN-innstillinger**)
Alltid på VPN	Aktiver Native Lockdown
Aktiver AppTec360 Lockdown	Aktiver AppTec360 Lockdown

Innebygd (kun tilgjengelig på Samsung-enheter)			
Type tilkobling	PPTP	Server	Server
		Aktiver PPTP-kryptering	Aktiver PPTP-kryptering
	L2TP / IPSec PSK	Server	Server
		IPSec forhåndsdelt nøkkel	IPSec forhåndsdelt nøkkel
		Aktiver L2TP-hemmelighet	Aktiver L2TP-hemmelighet
		L2TP-hemmelighet	L2TP-hemmelighet
	IPSec XAuth PSK	Server	Server
		IPSec-identifikator	IPSec-identifikator
		IPSec forhåndsdelt nøkkel	IPSec forhåndsdelt nøkkel
DNS-søkedomener	DNS-søkedomener		
Ekspertinnstillinger	DNS-servere	DNS-servere	
	Videresendingsruter	Videresendingsruter	

Åpen VPN		
Server	Server	
OpenVPN-profil	OpenVPN-profil	
OpenVPN-app	OpenVPN for Android (anbefalt)	
	OpenVPN Connect	
Ekspertinnstillinger	DNS-servere	DNS-servere
	Videresendingsruter	Videresendingsruter

Samsung / Strong Swan			
Type tilkobling	PPTP	Server	Server
		Brukernavn	Brukernavn
		Passord	Passord
		Aktiver PPTP-kryptering	Aktiver PPTP-kryptering
	L2TP / IPSec PSK	Server	Server
		IPSec forhåndsdelt nøkkel	IPSec forhåndsdelt nøkkel
		Brukernavn	Brukernavn
		Passord	Passord
		Aktiver L2TP-hemmelighet	L2TP-hemmelighet
	IPSec XAuth PSK	Server	Server
		IPSec-identifikator	IPSec-identifikator
		IPSec forhåndsdelt nøkkel	IPSec forhåndsdelt nøkkel
		Brukernavn	Brukernavn
		Passord	Passord
Ekspertinnstillinger	DNS-servere	DNS-servere	
	Videresendingsruter	Videresendingsruter	

Cisco Any Connect		
Server	Server	
Sertifikatmodus	Deaktivert	Deaktivert
	Automatisk	Automatisk
Ekspertinnstillinger	DNS-servere	DNS-servere
	Videresendingsruter	Videresendingsruter

VPN per app

VPN-klient

AppTec360 VPN-klient		
Gateway-konfigurasjon	Velg Gateway VPN-konfigurasjon (se **Generelle innstillinger > Universal Gateway > VPN-innstillinger**)	
VPN-apper	VPN-apper	
Alltid på VPN	Aktiver Native Lockdown	Alltid på VPN
Aktiver AppTec360 Lockdown	Aktiver AppTec360 Lockdown	

Samsung / Strong Swan			
Type tilkobling	PPTP	Server	Server
		VPN-apper	VPN-apper
		Brukernavn	Brukernavn
		Passord	Passord
		Aktiver PPTP-kryptering	Aktiver PPTP-kryptering
	L2TP / IPSec PSK	Server	Server
		VPN-apper	VPN-apper
		IPSec forhåndsdelt nøkkel	IPSec forhåndsdelt nøkkel
		Brukernavn	Brukernavn
		Passord	Passord
		Aktiver L2TP-hemmelighet	L2TP-hemmelighet
	IPSec XAuth PSK	Server	Server
		VPN-apper	VPN-apper
		IPSec-identifikator	IPSec-identifikator
		IPSec forhåndsdelt nøkkel	IPSec forhåndsdelt nøkkel
		Brukernavn	Brukernavn
		Passord	Passord
Ekspertinnstillinger	DNS-servere	DNS-servere	
	Videresendingsruter	Videresendingsruter	

Begrensninger

Her kan du angi begrensninger i forbindelse med tilkoblingshåndteringen.

Tillat dataroaming	Tillat mobildata under roaming
Tving frem dataroaming	Hvis den er aktivert, er roaming for mobildata permanent aktivert (anbefales ikke!) Denne innstillingen overskriver innstillingen "Tillat dataroaming"!
Følgende innstillinger er bare tilgjengelige på SAFE 2.x eller nyere	
Tillat bare nødanrop	Tillat bare nødanrop
Tillat WiFi	Tillat WiFi
Minimum sikkerhetsnivå for WiFi-nettverk	Minimum sikkerhetsnivå for WiFi-nettverk Åpen = alle typer WiFi er tillatt
Forby brukeren å legge til WiFi-nettverk	Brukeren kan ikke selv legge til et WiFi-nettverk Denne innstillingen er bare mulig hvis en WiFi-profil er definert under "Connection Management".
Tillat SMS og MMS	All = All SMS- og MMS-trafikk er tillatt Kun innkommende SMS = Kun innkommende SMS-meldinger er tillatt Outgoing SMS Only = Kun utgående SMS-meldinger er tillatt Ingen = Ingen SMS/MMS-trafikk er tillatt
Tillat synkronisering under roaming	Tillat synkronisering under roaming På = aktivert Av = deaktivert Brukervalg = brukerens valg
Tillat roaming av tale	Tillat roaming av tale På = aktivert Av = deaktivert User Choice = brukerens valg
Bruk System http Proxy Server	Bruken av en HTTP-proxy-server, som er gitt av systemets innstillinger i innstillinger, er avhengig av det tilkoblede nettverket (WiFi eller APN)

PIM-administrasjon

Gmail Exchange

Info: Denne konfigurasjonen vil bli brukt på Gmail-appen. Du må derfor godkjenne og installere Gmail.

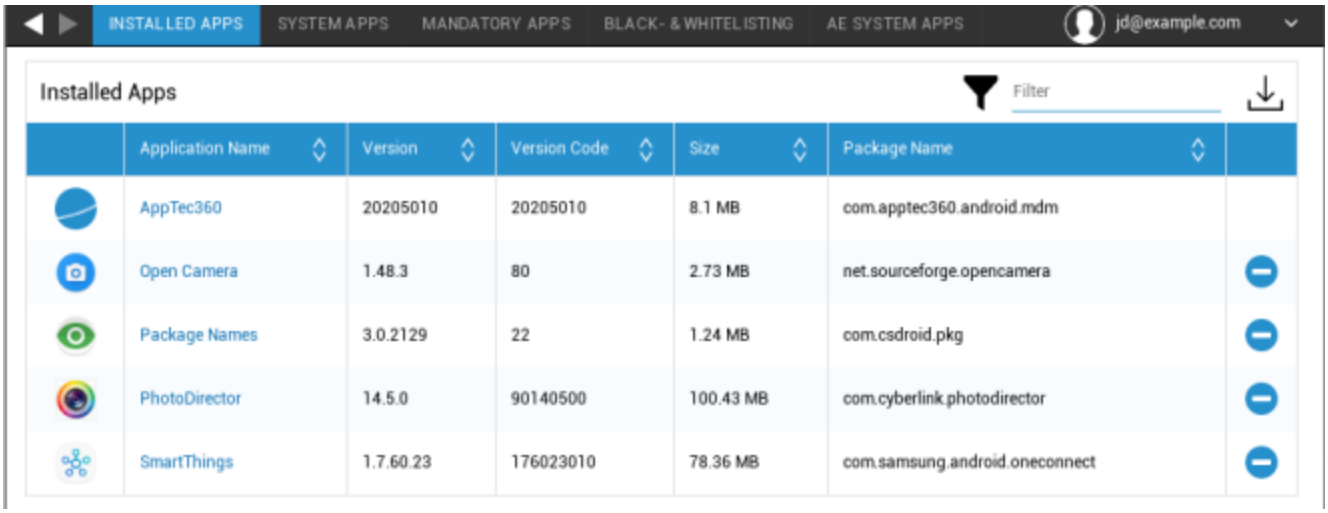
E-postadresse	Den oppgitte e-postadressen til brukeren Vær oppmerksom på "plassholderne", som du kan bruke til å arbeide med legitimasjon og ikke utføre endringer manuelt på alle enheter Med et klikk på kan du vise dem for deg selv
Serverens vertsnavn	Serveradressen til Exchange-serverne dine
Innloggingsnavn	Innloggingsnavnet for den respektive sluttbrukerenheten, legg også merke til "Placeholders here".
Signatur	En signatur kan legges ved (Tips: Noen enheter krever HTML-formatering for signaturen)
Antall foregående dager som skal synkroniseres	Antall dager som avgjør når e-poster synkroniseres tilbake
Enhetsidentifikator	En streng som inneholder EAS DeviceID. Dette er en del av EAS-protokollen og er nødvendig i noen områder
Bruk Secure Sockets Layer (SSL)	Bruk en SSL-tilkobling
Godta alle sertifikater	Alle sertifikater godtas. Velg dette alternativet hvis Exchange-serveren bruker et selvsignert sertifikat

App-administrasjon

Enterprise App Manager

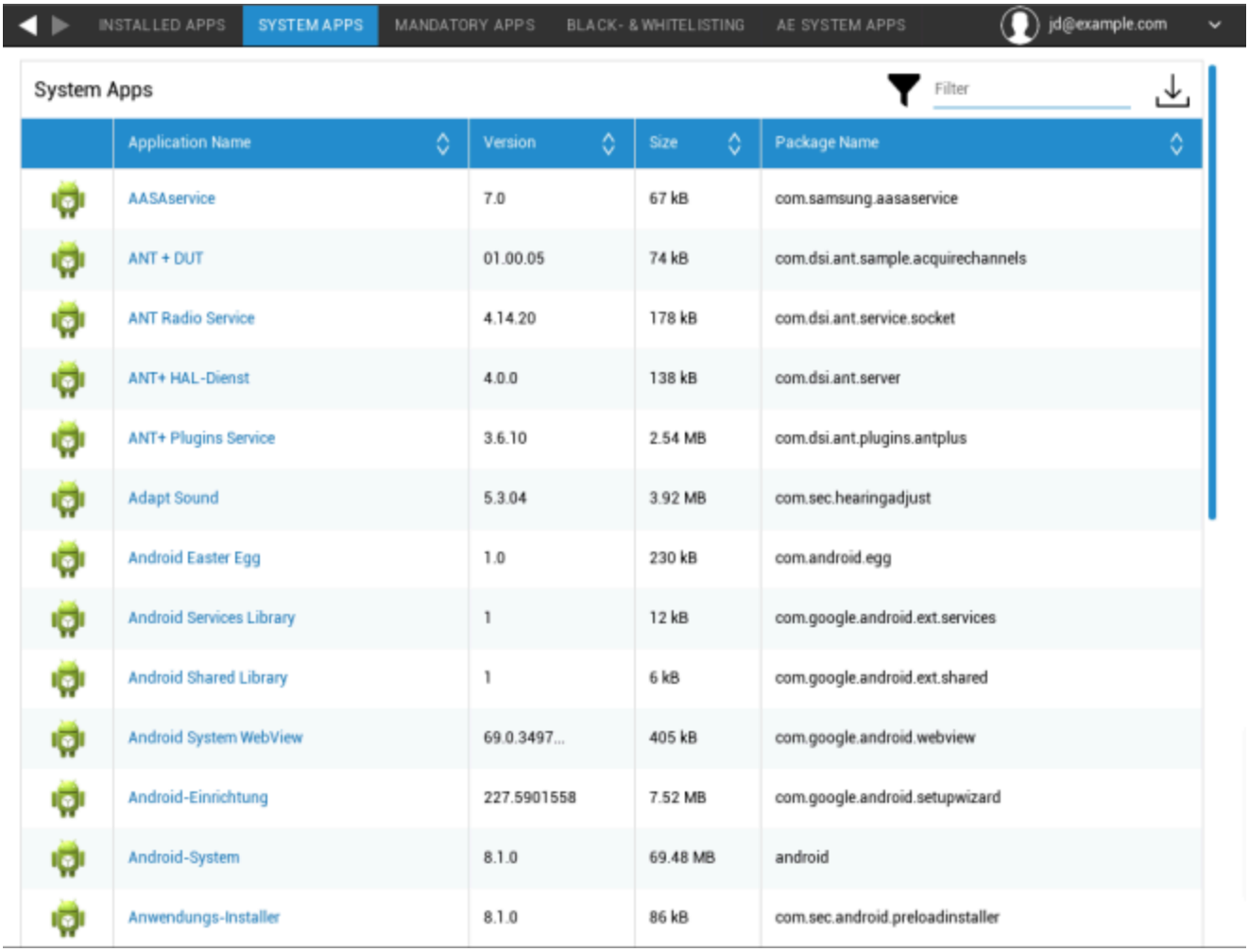
Installerte apper (kun på enhetsnivå)

Her vises alle apper som for øyeblikket er installert på sluttbrukerens enhet.



Systemapper (kun på enhetsnivå)

Under "System Apps" finner du en liste over alle apper og tjenester som allerede er installert på sluttbrukerenheten av produsenten av enheten.

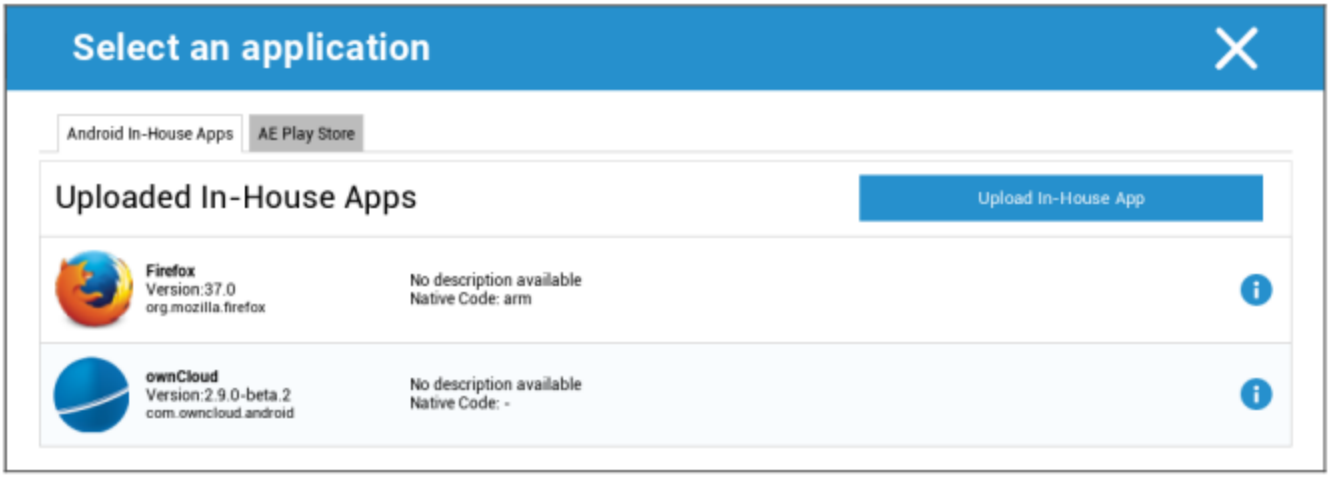


Obligatoriske apper

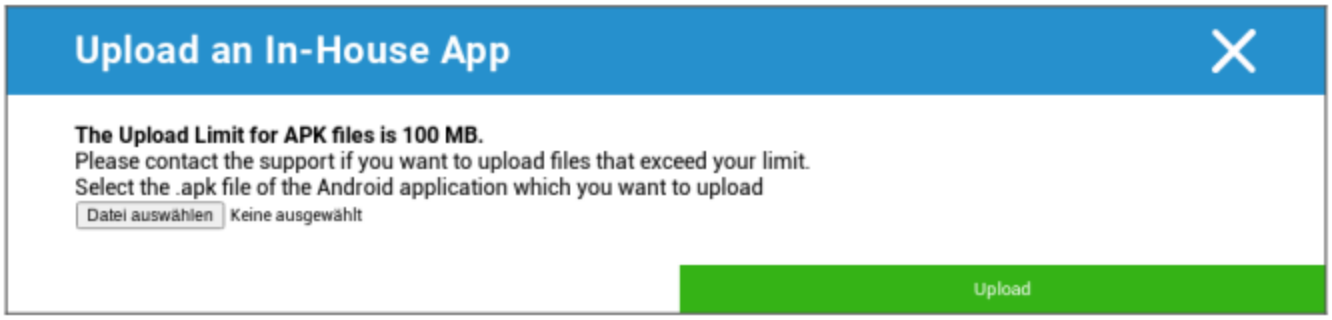
Under Obligatoriske apper kan du opprette de obligatoriske appene som kreves. Brukeren vil kontinuerlig bli bedt om å installere denne utpekte appen.

Via kan den obligatoriske nødvendige appen defineres.

Dette kan være en egen app fra "Android In-House Apps", som du har lastet opp i Generelle innstillinger.

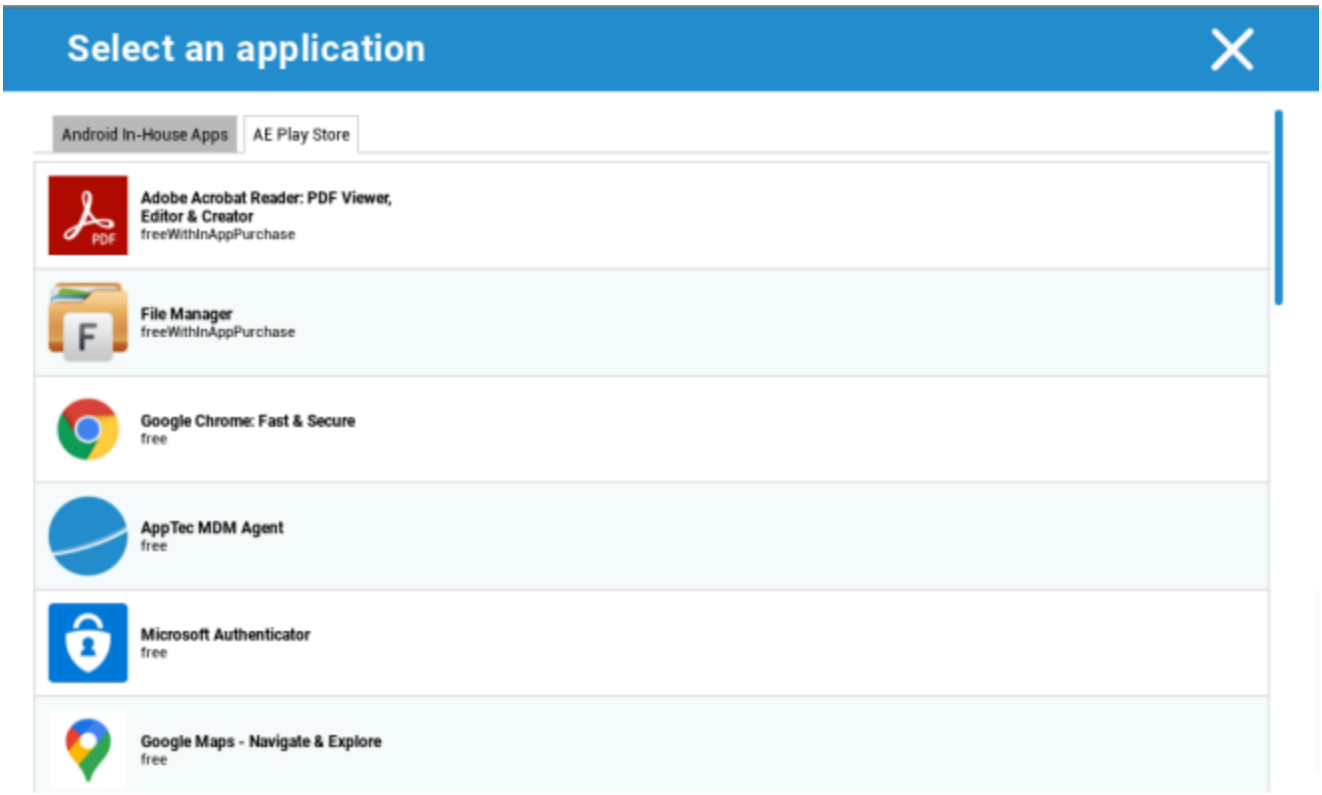


Du kan også velge og laste opp en apk-fil direkte med "Upload In-House App".



Hvis du installerer en In-House-app, har du mulighet til å aktivere "Hold deg oppdatert". Hvis dette er aktivert og du har definert en nyere versjon i In-House App DB, vil appen bli oppdatert på enheten.

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



Bare godkjente "AE Play Store-apper" vises i denne kategorien.

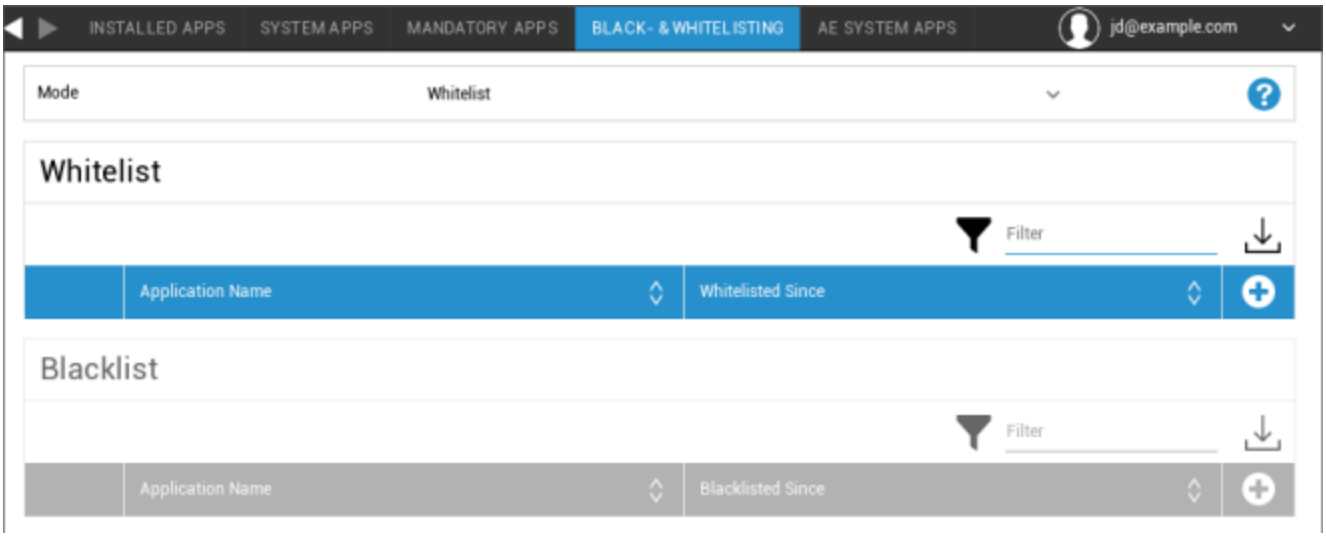
For å godkjenne en "AE Play Store-app", gå til "Generelle innstillinger" > "Appadministrasjon" > "AE Play

Store" og legge til en app via knappen som videresender deg til "Play Store Apps"-fanen (eller du kan gå direkte til "Play Store Apps"-fanen).

Under fanen "Play Store Apps" kan du søke etter apper. Når du klikker på en app, åpnes app-siden , og her kan du godkjenne appen ved å klikke på "Approve".

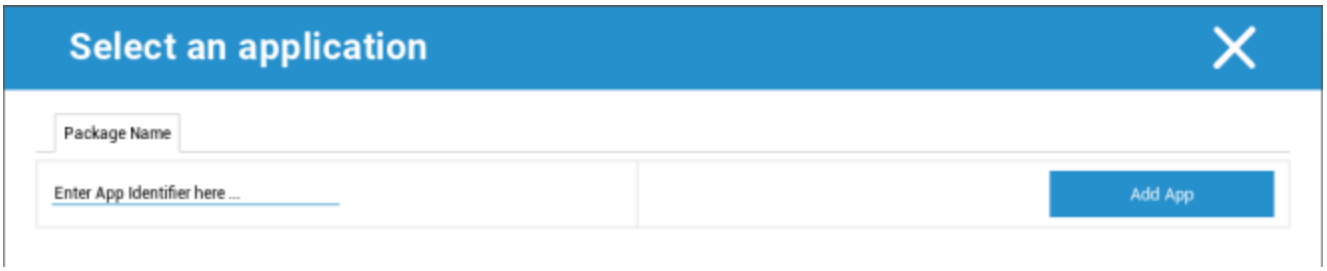
Svart- og hvitelisting

Under "Svart- og hvitelisting" kan du velge mellom modusene "Whitelist" og "Blacklist".



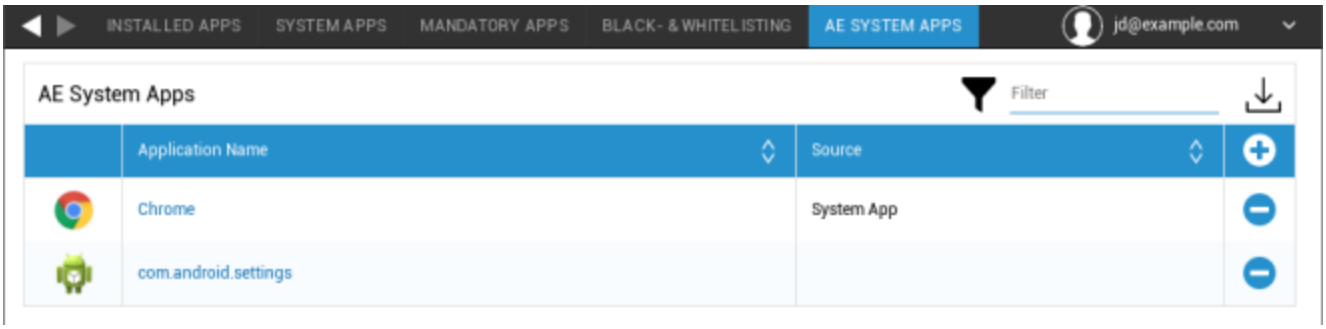
Hviteliste	Bare apper og tjenester som er lagt til i listen, kan installeres på sluttbrukerens enhet. Hvis disse allerede er forhåndsinstallert på sluttbrukerens enhet, vil de bli aktivert og stilt inn slik at brukeren kan kjøre dem.
	Alle andre apper som ikke er lagt til i listen, kan ikke installeres på sluttbrukerens enhet. Hvis disse allerede er forhåndsinstallert på sluttbrukerens enhet, blir de deaktivert og innstilt slik at brukeren ikke kan kjøre dem.
Svarteliste	Apper og tjenester som legges til i listen, kan ikke installeres på sluttbrukerens enhet. Hvis disse allerede er forhåndsinstallert på sluttbrukerens enhet, blir de deaktivert og innstilt slik at brukeren ikke kan kjøre dem.
	Alle andre apper som ikke er lagt til i listen, kan installeres på sluttbrukerens enhet. Hvis disse allerede er forhåndsinstallert på sluttbrukerens enhet, vil de bli aktivert og stilt inn slik at brukeren kan kjøre dem.

Via , legger du til flere apper eller tjenester i listen som brukes for øyeblikket.
Via , legger du til flere apper eller tjenester i listen som er inaktive for øyeblikket.
Du kan definere et "pakkenavn":

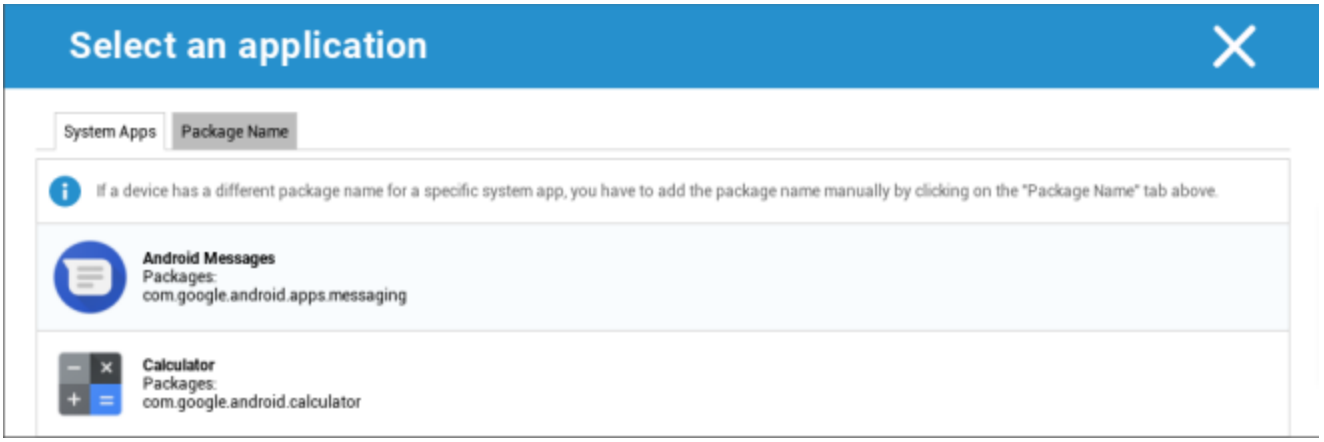

Select an application
Package Name
Enter App Identifier here ...
Add App

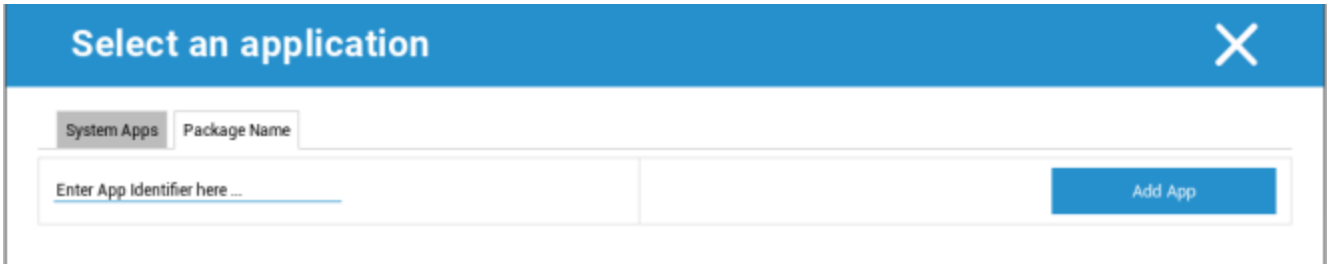
AE System-apper

Her kan du definere en liste som inneholder spesifikke systemapper som skal aktiveres på enhetene.



Hvis du klikker på knappen, kan du velge fra en liste over mulige systemapper fra Google eller skrive direkte inn pakkenavnet til en systemapp som skal aktiveres.





Vær oppmerksom på at systemappene i listen fra Google kun er apper som kan være systemapper, men at de ikke nødvendigvis må være systemapper på enhetene dine.

Denne listen påvirker imidlertid bare apper som allerede er forhåndsinstallert.

Apper som ikke er forhåndsinstallert på enhetene dine, vil ikke påvirke enhetene dine, uansett om appen er fra listen fra Google eller om appens pakkenavn legges inn direkte.

Begrensninger og innstillinger

Innstillinger for appadministrasjon

Her kan du konfigurere hvordan enheten skal oppføre seg når det gjelder appoppdateringer.

Hyppighet for oppdateringssjekk	Angi i hvilket intervall AppTec360 Client skal søke etter appoppdateringer. Standardverdien er 24 timer.
Wi-Fi-terskelverdi	Apper som er større enn den angitte størrelsen, lastes ned via Wi-Fi. Hvis "Kun Wi-Fi" er valgt, lastes alle apper ned via Wi-Fi.

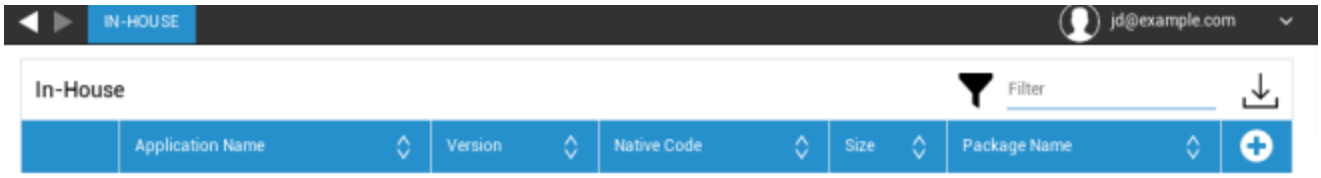
App Store for bedrifter

Internt

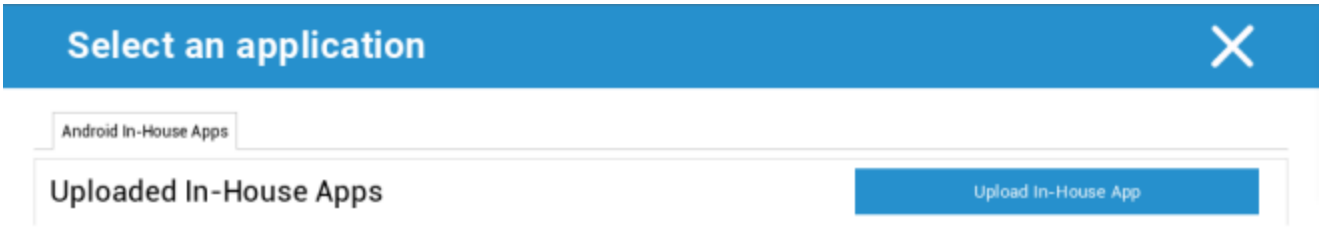
Under punktet "In-House" kan du laste opp og distribuere internt utviklede apper.

Med symbolet kan du distribuere flere In-House-apper.

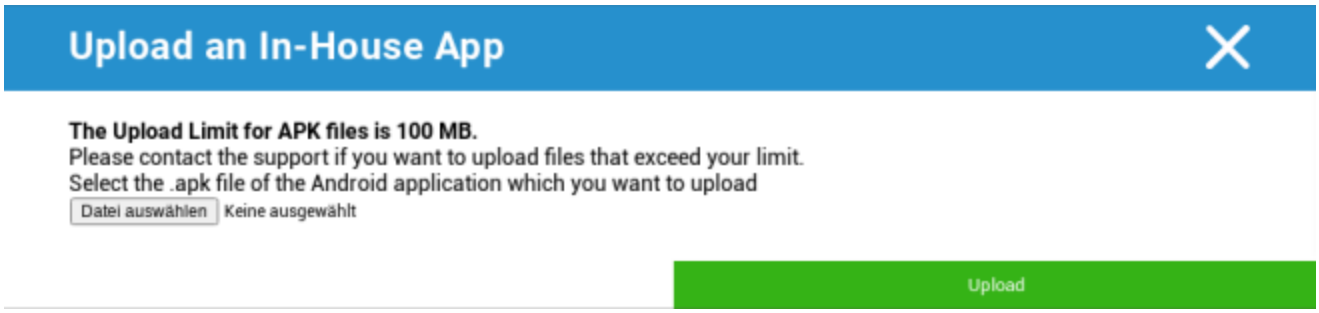
Hvis du installerer en In-House App, har du mulighet til å aktivere "Keep up to date". Hvis er aktivert og du har definert en nyere versjon i In-House App DB, vil appen bli oppdatert på på enheten.



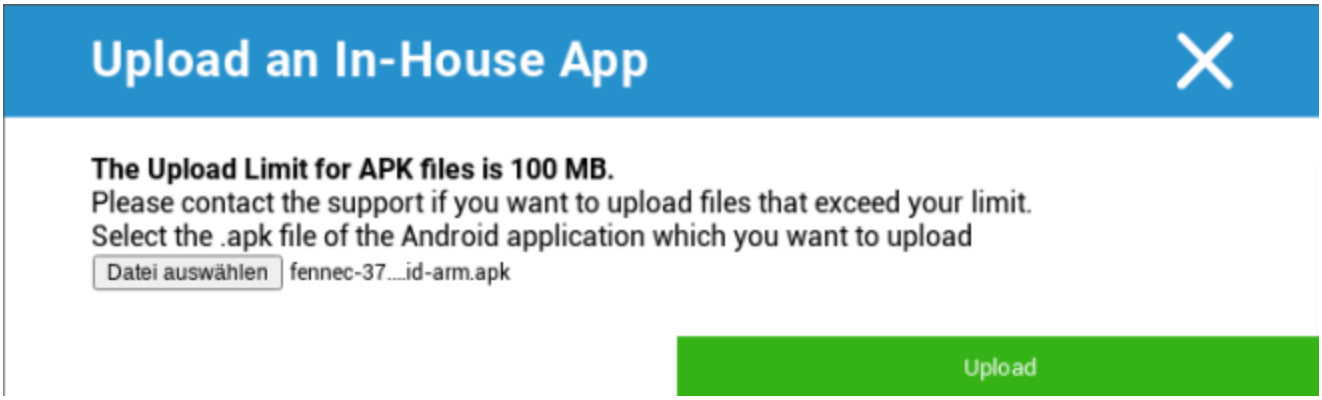
Hvis du ikke har distribuert In-House Apps, vil du motta følgende oversikt:



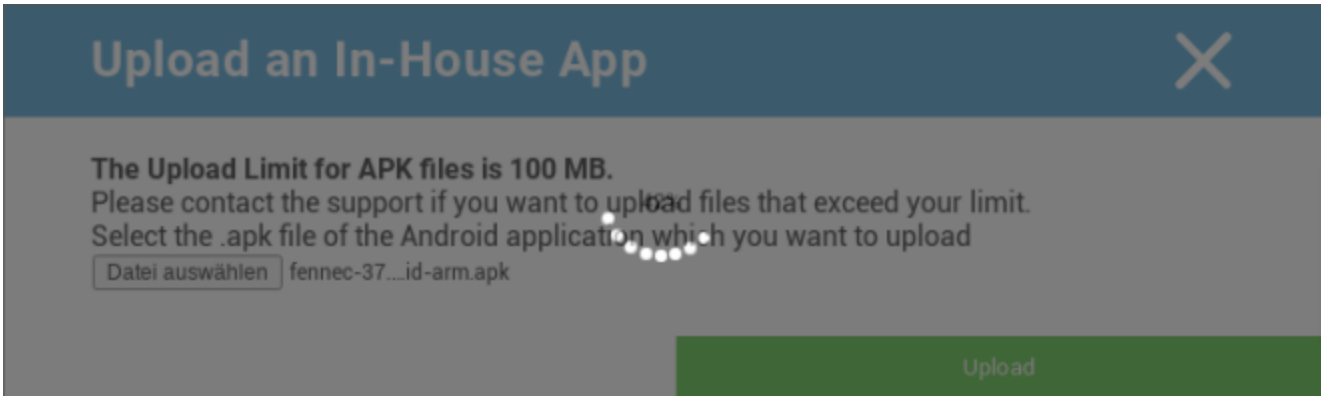
Klikk på "Last opp egen app", og du vil da få opp følgende oversikt:



Nå velger du med "Søk ..." en .apk-fil og klikker deretter på "Last opp".



Appen din vil nå lastes opp, og i midten av sirkelen vil du se en prosentindikator,
, som viser hvor mye av appen din som allerede er lastet opp.



Hvis opplastingen av din In-House-app har vært vellykket, kan du finne den opplastede appen i App Catalog.

Brukeren har nå muligheten til å se og installere denne appen i AppTec360 Store på sluttbrukerens -enhet, under kategorien "In-House".

Siden dette ikke involverer en Google PlayStore-app, trenger ikke brukeren en lagret Google ID på sin respektive sluttbrukerenhet.

Enterprise Play Store

AE Play Store

Her kan du legge til apper i Android Enterprise Playstore. Vær oppmerksom på at du må godkjenne Apper med din AE-administratorkonto før du kan legge dem til.

For godkjenning av en app, se instruksjonene i Obligatoriske apper.

Kioskmodus og lanseringsprogram

Kioskmodus

Kioskmodus lar deg forhåndsdefinere en app eller en URL. Da vil det kun være mulig å kjøre/besøke denne appen og/eller URL-en på

.

På samme måte kan ulike maskinvareknapper deaktiveres i Kiosk Mode diverse.

Automatisk start	Starter automatisk kioskmodus så snart profilen når sluttbrukerens enhet
Planlagt kioskmodus?	Du kan planlegge et tidspunkt for kioskmodus, som deretter starter og slutter automatisk på et tidspunkt du selv har angitt.
Starttidspunkt	Starttidspunkt
Tid i minutter	Tid i minutter, etter hvilken Kioskmodus skal avsluttes igjen

Søknadstype

Enkelt app	Hvis du vil starte appen i kioskmodus, velger du "Pakke" under "Applikasjonstype"
Kiosk-applikasjon	Klikk her for å velge en app som skal startes i kioskmodus Du finner den vanlige oversikten over App Management Du kan velge mellom "Google Play Store", "Android In-House Apps" og "Packagename"

Søknadstype

URL	Hvis du vil starte en URL i kioskmodus, velger du "URL" under "Applikasjonstype" Deretter definerer du ønsket URL-adresse
Tøm nettleseren etter inaktivitet	Her kan du definere et tidsintervall i minutter, etter hvilket Kioskmodus skal startes på nytt
Tøm nettbuffer og informasjonskapsler	Hvis du aktiverer denne funksjonen, vil nettbufferen (informasjonskapsler og hurtigbufrede bilder) slettes etter en omstart av kioskmodus
Retningslinjer for samme opprinnelse	Hvis denne funksjonen er aktiv, kan brukeren bare surfe på undersidene til en definert URL Du har for eksempel definert følgende URL:www.mypage.com Da kan brukeren surfe på: www.mypage.com/subpage
Hvitelistede nettadresser	Her kan du vedlikeholde en hviteliste, alle disse nettadressene er tillatt Maksimalt 1 URL per linje En URL må begynne med http:/ eller https://
Svartelistede nettadresser	Her kan du vedlikeholde en svarteliste, alle disse nettadressene er ikke tillatt Maksimalt 1 URL per linje En URL må begynne med http:/ eller https://
Skjermorientering	Denne innstillingen gjelder skjermjusteringene Automatisk = automatisk Stående = vertikalt format Landscape = liggende modus

Multi-app	Hvis du velger "Multi App"-kioskmodus, vil bruk av AppTec360 Launcher være obligatorisk.
Apper	Applikasjon: Velg en Playstore eller en egen app som kioskapplikasjon. Det er også mulig å angi et pakkenavn. Den valgte kioskapplikasjonen må være installert på enheten. Husk å angi Kiosk-applikasjonen som obligatorisk. Snarvei på startskjermen: Hvis den er satt til "På", opprettes det en snarvei på startskjermen. Hvis den er satt til "Av", vil appen fortsatt vises i applisten.

Avslutt passord aktivert	Hvis du aktiverer denne funksjonen, er det mulig for brukeren å avslutte Kioskmodus med et passord som er forhåndsdefinert av deg.
Avslutt passord	Dette er passordet som ble forhåndsdefinert av deg
Skjul statuslinjen automatisk	Hvis dette alternativet er aktivert, vil statuslinjen automatisk bli uthevet. Med dette alternativet kan brukerne se informasjonen på statuslinjen, men ikke få tilgang til dens funksjoner.
Deaktiver statuslinjen	Statuslinjen inneholder varsler, snarveier og informasjon. Kun tilgjengelig for Samsung-enheter med SAFE 4.0 eller nyere.
Deaktiver volumtastene	Deaktiver volumtaster (kun tilgjengelig på Samsung-enheter med SAFE 3.0 eller nyere)
Deaktiver av/på-bryter	Deaktiver av/på-bryter (kun tilgjengelig på Samsung-enheter med SAFE 3.0 eller nyere)
Deaktiver Hjem-knappen	Deaktiver Hjem-knapp. Hvis denne funksjonen er aktivert, kan Kioskmodus bare avsluttes i AppTec360-konsollen. (kun tilgjengelig på Samsung-enheter med SAFE 3.0 eller nyere)
Deaktiver navigasjonslinjen	Med denne kan du deaktivere navigasjonslinjen (Tilbake/Meny) Hvis denne funksjonen er aktivert, kan Kioskmodus bare avsluttes i AppTec360-konsollen (kun tilgjengelig på Samsung-enheter med SAFE 3.0 eller nyere)

AppTec360 Launcher

Aktiver AppTec360 Launcher	På: Aktiverer AppTec360 Launcher. Brukeren må angi den som standard Launcher én gang. Merk: Hvis kioskmodus er aktivert, og kioskmodus er satt til "Multi App", vil bruk av AppTec360-startprogrammet være påtvunget.
Store ikoner	På: Viser en større versjon av appikonene i startprogrammet
Skjul AppTec360-appikonet	På: Skjuler AppTec360-appen fullstendig
Skjul AppTec360 Store-ikonet	På: Skjuler AppTec360 Enterprise AppStore fullstendig

AppTec360-innstillinger

Aktiver AppTec360 Settings App	AppTec360 Settings-appen gir kontroll over WiFi- og Bluetooth-tilkoblinger
Aktiver innstillinger i Multi App Kioskmodus	Hvis dette er aktivert, kan brukerne få tilgang til AppTec360 Settings-appen mens Multi App Kiosk Mode er aktiv

Fjernkontroll

Splashtop

For å starte en fjernstyringsøkt for enheten din, må appen "Splashtop Streamer" installeres på enheten ved å legge den til i App **Management** → **Enterprise App Manager** → **Obligatoriske app**er.

Deretter konfigurerer du følgende innstillinger for Splashtop:

Aktiver Splashtop	Hvis dette er aktivert, vil AppTec360 konfigurere Splashtop-appen til å tillate fjernkontroll
Distribuere kode	Gå til https://my.splashtop.com og logg inn på Splashtop-kontoen din. Klikk på "Add Computer" og kopier den 12-sifrede distribusjonskoden fra siden du får opp.
Angi egendefinert distribusjonsportal?	Distribuere gateway
Distribuere Gateway Domain / Host	Distribuere gateway
Sertifikatverifisering	Sertifikatverifisering

Deretter kan du bruke alternativet Splashtop Remote Control i kontekstmenyen (tannhjulet ved siden av søkefeltet når enheten er valgt, eller høyreklikk på enheten i treet) for å starte fjernkontrolløkten.

TeamViewer

For å starte en fjernstyringsøkt for enheten din, må appen "TeamViewer QuickSupport" installeres på enheten ved å legge til appen i App **Management** → **Enterprise App Manager** → **Obligatoriske app**er.

Deretter kan du bruke alternativet **TeamViewer Remote Control** i kontekstmenyen (tannhjulet ved siden av søkefeltet når enheten er valgt, eller høyreklikk på enheten i treet) for å starte fjernkontrolløkten.

Innholdsstyring

Innholdsboks

Her kan du aktivere ContentBox.

Så snart du setter "Aktiver ContentBox" til "På", installeres en egen ContentBox-app automatisk på sluttbrukerens enhet.

Sikker nettleser

Her kan du konfigurere innstillinger for AppTec360 Secure Browser.

Så snart du setter "Sikker nettleser" til "På", installeres det automatisk en egen nettleser-app på på sluttbrukerens enhet.

Krever passord	Krev at brukeren oppretter og bruker et passord for å få tilgang til nettleseren.
Minste nødvendige passordlengde	Angi antall tegn som kreves for passordet
Nødvendig passordkvalitet	Angi ønsket passordkvalitet
Begrens nedlastinger / Åpne i	
Begrens opplastinger	
Last opp hviteliste	En liste over URL-adresser som det alltid vil være tillatt å laste opp.
Tillat kopiering	Tillat kopiering, klipping eller deling av tekst inne på nettsidene.
Tillat skjermopptak	Tillat å ta skjermbilder.
Hyppighet for opprydding av data	Velg med hvilken frekvens ALLE brukerdata (historikk, hurtigbuffer osv.) skal fjernes automatisk.
Selskapets bokmerker	Bokmerkene vises i mappen "Company bookmarks" i nettleserens bokmerker. De kan ikke redigeres av brukeren.
Skjul adresselinjen	
Hvitelisting i nettleseren (uten Universal Gateway)	Aktiverer hvitelisting av URL-er på klientsiden. • Selskapets bokmerker er alltid hvitelistet • Støttes kun for 100 nettadresser • Bruk Universal Gateway for ubegrenset svart- og hvitelisting
Hvitelistede nettadresser	En liste over tillatte nettadresser.
Gateway-basert svart- og hvitelisting	Svartelisting har følgende krav: • En fungerende AppTec360 Universal Gateway ("Generelle innstillinger" → "Universal Gateway")

	• En fungerende VPN-konfigurasjon med en spesifisert DNS-server ("Generelle innstillinger" → "Universal Gateway" → "VPN-innstillinger") • En svartelistekonfigurasjon ("Generelle innstillinger" → "Universal Gateway" → "Domain Blacklist") • En gyldig VPN-tilkobling i profilen ("Tilkoblingsadministrasjon" → "VPN")

Ytterligere API

Samsung KNOX

Begrensninger

Tillat SD-kort	
Tillat skriving på SD-kort	
Tillat skjermopptak	
Tillat utklippstavle	
Sikkerhetskopier innstillinger og appdata i Google Cloud	
Gjenopprett innstillinger fra Google Cloud når du installerer en app på nytt	
Tillat USB-feilsøking	
Tillat Google Crash Report	
Tillat tilbakestilling til fabrikkinnstilling	
Tillat OTA-oppgradering	
Tillat USB-vertslagring	Hvis denne funksjonen er aktivert, kan brukeren koble til en hvilken som helst pennstasjon (bærbar USB-lagring), ekstern HD eller Secure Digital (SD)-kortleser, og den blir montert som en lagringsstasjon på enheten.
Tillat USB Media Player (MTP, PTP)	
Tillat mikrofon	Deaktiverer mikrofonen for tredjepartsapplikasjoner
Tillat NFC (Near Field Communication)	
Tillat ukjente kilder (APK Sideloading)	Hvis dette er aktivert, er sidelasting av apper (APK-filer) tillatt. Når denne innstillingen er deaktivert, må brukeren aktivere den manuelt når du tillater installasjon av APK-er fra ukjente kilder på nytt.
Tillat brukeroppretting	Hvis denne funksjonen er aktivert, kan brukeren opprette flere kontoer på enheten, f.eks. gjestekontoer.

E-post

E-postadresse	
Protokoll for innkommende server	
Innkommende serveradresse	
Innkommende serverport	
Pålogging/brukernavn for innkommende server	
Passord for innkommende server	
Innkommende server bruker SSL	
Innkommende server bruker TLS	
Innkommende server godtar alle sertifikater	
Protokoll for utgående server	
Adresse til utgående server	
Utgående serverport	
Utgående server bruker ekstra legitimasjon	Hvis den er deaktivert, bruker systemet innkommende legitimasjon også for den utgående serveren.
Pålogging/brukernavn for utgående server	
Passord for utgående server	
Utgående server bruker SSL	
Utgående server bruker TLS	
Utgående server godtar alle sertifikater	
Sett signatur	
Signatur	Merk: For noen enheter må signaturen angis i HTML-format.
Varsle brukeren om mottak av ny e-post	

Utveksling

E-postadresse	
Serverens vertsnavn	Vertsnavnet til Exchange-serveren
Innloggingsnavn	Brukernavnet som brukes til å logge inn på Exchange Server
Domene	Hvis en ACL Gateway-konfigurasjon er aktivert og feltet Domain ikke er tomt, vil AppTec360 Universal Gateway autentisere enheten med følgende navn "Domain\Login Name
Passord	
Antall foregående dager som skal synkroniseres	
Frekvens for synkronisering av e-post	
Synkronisering under roaming	
Sett signatur	
Signatur	Merk: For noen enheter må signaturen angis i HTML-format.
Standard konto	
Bruk Secure Sockets Layer (SSL)	
Bruk Transport Layer Security (TLS)	
Godta alle sertifikater	

APN

APN Visningsnavn	
Navn på tilgangspunkt	Navn på APN
Protokoll for utgående server	
MCC - Mobil landskode	La stå tom for å bruke mmc for installert SIM-kort
MNC - Mobilnettverkskode	La stå tom for å bruke mnc fra installert SIM-kort
Serveradresse	
Serverens portnummer	
Serverens proxy-adresse	
Adresse til MMS-server	La stå tom som standard
MMS-portnummer	La stå tom som standard
MMS-proxy-adresse	La stå tom som standard
Brukernavn	
Passord	
Type tilgangspunkt	Aksepterte typer er "default", "mms", "supl".
	Hvis null eller tomt oppgis, brukes "default,supl,mms" som standard.
	La den være tom som standard.
Foretrukket APN	

Bluetooth

Tillat enhetsoppdagelse via Bluetooth	
Tillat Bluetooth-paring	
Tillat Bluetooth-headset-enheter	
Tillat håndfrie Bluetooth-enheter	
Tillat Bluetooth A2DP-enheter	A2DP, Advanced Audio Distribution Profile, gjør det mulig å strømme lyd mellom enheter
Tillat utgående anrop	
Tillat dataoverføring via Bluetooth	
Tillat Bluetooth-tilknytning	
Tillat tilkobling til datamaskin via Bluetooth	

Tilkobling

Tillat bare nødanropTillat Wi-Fi	
Minimum sikkerhetsnivå for Wi-Fi-nettverk	
Forby brukeren å legge til Wi-Fi-nettverk	Denne begrensningen kan bare aktiveres hvis minst én aktiv Wi-Fi-profil er definert under Connection Management
Tillat SMS og MMS	
Tillat synkronisering under roaming	
Tillat roaming av tale	

Android Enterprise – Fullt administrert enhet med arbeidsprofil (COPE)

Generell forklaring av COPE

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

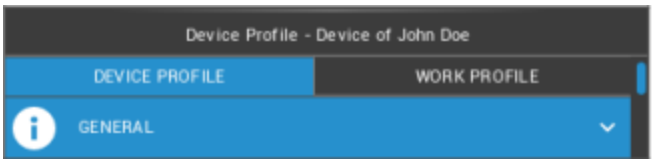
COPE-modus gjør det mulig å registrere en Android-enhet som en **Android Enterprise - Fullt administrert enhet** med integrert **Android Enterprise - Container-profil**.

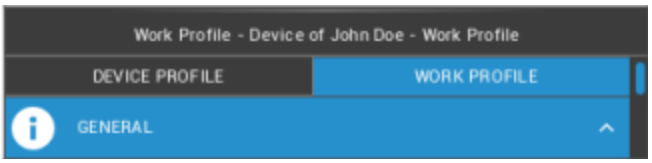
Dette kan enten være en Android-enhet som allerede er registrert som en **Android Enterprise - Fullt administ** rert enhet og som Android **Enterprise - Container** i tillegg er satt opp på, eller en nyregistrert Android-enhet som er direkte registrert som en Android **Enterprise - Fullt administrert** enhet sammen med Android **Enterprise - Container** på toppen av den.

COPE-modus er kun tilgjengelig for enheter med Android 8, 9 og 10

Konfigurasjon av profiler for COPE-enheter

Siden det ikke finnes noen konfigurasjonsprofil for COPE-modus i seg selv, er konfigurasjonen av **Android Enterprise - Fullt administrert enhet** og **Android Enterprise - Container** delt inn i to profiler i COPE-profilen. Det er mulig å bytte mellom de to profilene for konfigurasjonen av hver profil ved å klikke på den respektive knappen på venstre side av konsollen:





Begge profilene kan konfigureres som beskrevet for hver enkelt profil:

Android Enterprise - Fullt administrert enhet

Android Enterprise - Container

Gå tilbake til AE Fullt administrert enhet

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

Ved å fjerne Container-profilen vil COPE-profilen bli omgjort til en **Android Enterprise - Fullt administrert enhetsprofil**.

Android Enterprise – konfigurasjon av containere

Avhengig av om du har valgt en gruppeprofil eller en enhet, vil oversikten og underpunktene være forskjellige - vær nøye med dette!

Generelt

Profiloversikt (kun på profilnivå)

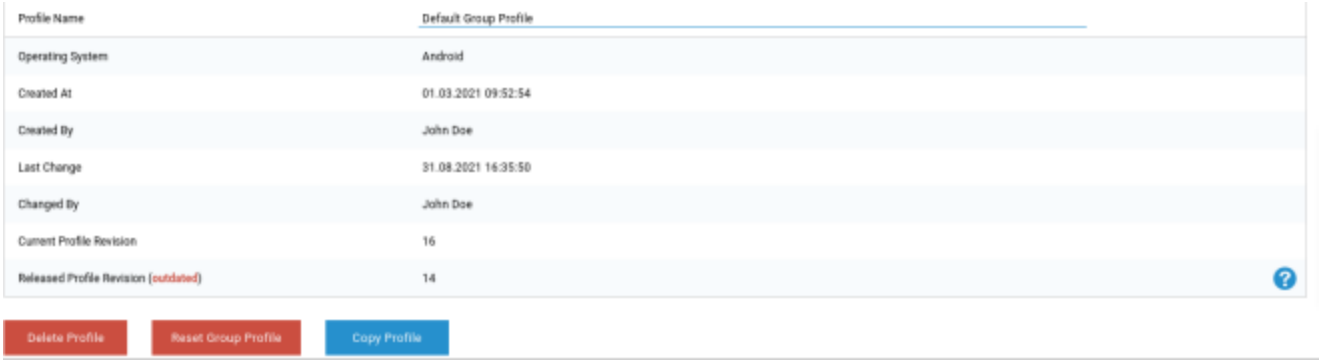
Hvis du befinner deg i en profil, vil du få en kort oversikt over profilen, med hensyn til navn, operativsystem, opprettelsesdato, forfatter osv.

Profilnavn	Profilnavn - kan omdøpes direkte her
Operativsystem	Gyldig operativsystem for profilen
Opprettet på	Dato for opprettelse
Opprettet av	Opprettet av
Siste endring	Siste endringsdato
Endret av	Brukeren som utførte de siste endringene i denne profilen
Nåværende profilrevisjon	Antall ganger profilen allerede har blitt oppdatert
Utgitt profilrevisjon	Antall ganger profilen allerede er oppdatert og har blitt tildelt enheter

Slett profil	Slett profil
Tilbakestill gruppeprofil	Tilbakestill gruppeprofil
Kopier profil	Kopier profil

Oversikt over gruppeprofiler (kun på gruppenivå)

Når du åpner en gruppeprofil, får du en rask oversikt over profilen.



Profilnavn	Navn på profilen (kan endres her)
Operativsystem	Operativsystemet profilen er beregnet på
Opprettet på	Tidspunktet for skapelsen
Opprettet av	Skaperen av profilen
Siste endring	Tidspunkt for siste endring av profilen
Endret av	Konto som gjorde de siste endringene
Nåværende profilrevisjon	Revisjon av lagret profilstatus
Utgitt profilrevisjon	Tilordnet profilrevisjon ("Tilordne nå"). Hvis etiketten viser "(utdatert)" bak teksten, betyr det at du har lagret profilen, men ikke tilordnet den ennå, slik at enhetene fortsatt vil få en eldre versjon.

Enhetsoversikt (kun på enhetsnivå)

Hvis du befinner deg på en enhet, vil du få en oversikt over den valgte enheten, og her finner du følgende:

Enhetens navn	Enhetens navn
Beliggenhet	Koordinater for plassering
Telefonnummer	Telefonnummer
Tildelte obligatoriske apper	Antall tildelte obligatoriske apper
OS-versjon	OS-versjon av enheten
Operativsystem	Operativsystem (Android Enterprise)
Serienummer	Enhetens serienummer
Eierskap til enheten	Bedrifts- eller privat enhet
Enhetstype	AE Arbeidsstyrt enhet
Rotfestet	Status, som angir om enheten har blitt rotfestet
Overensstemmende	I samsvar med retningslinjene
IP-adresse	IP-adressen til enheten
Sist sett	Tidspunkt for når enheten sist ble koblet til AppTec
Siste fremstøt	Tidspunkt for når siste push ble sendt til enheten
Tildeling av bruker	Brukeren eller gruppen denne enheten er tilordnet til

Konfigureringsrevisjon

Her får du en oversikt over hvilken gruppeprofil som er tilordnet enheten.

Hvis du klikker på gruppeprofilen, får du direkte tilgang til denne profilen, og du kan utføre innstillinger.

Med dette symbolet kan du tilbakestille de distribuerte appene til gruppeprofilens innstillinger.

Med dette symbolet kan du tilbakestille alle appene som brukes, til gruppeprofilens innstillinger.

"Nyere revisjon tilgjengelig" indikerer at gruppeprofilen har blitt endret og lagret, men ikke tilordnet. Gruppeprofilen må tilordnes med "Tilordne nå" på gruppenivå for at endringene skal gjelde for

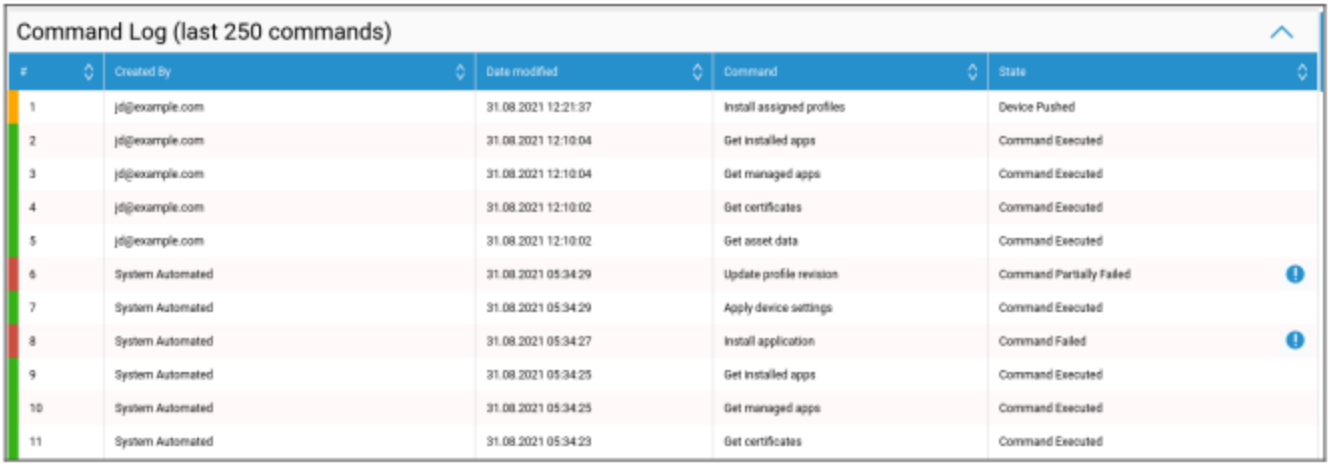
enhetene.

Enhetslogg (kun på enhetsnivå)

Her vil du motta ulike enhetslogger. Ved behov kan du finne årsaken til en feil direkte her.

Kommandologg

Her kan du se hvilke kommandoer som er utstedt for enheten, og hvilken status de har.



Mulige kommandostatuser

Enhet skjøvet	En push-forespørsel har blitt sendt til push-tjenesten (f.eks. APNS) for å be enheten om å koble seg tilbake til EMM-serveren.
Kommando opprettet	Kommandoen ble opprettet i systemet.
Kommando sendt	Kommandoen ble sendt til enheten etter at den ble koblet til serveren.
Kommando utført	Kommandoen ble vellykket utført.
Kommando mislyktes	Kommandoen mislyktes. *
Kommandoen mislyktes delvis	Avhengig av enhetens operativsystem kan enkelte kommandoer bli gruppert sammen. I dette mislyktes noen deler av denne kommandogruppen. *
Kommando utført, men mislyktes til slutt	Kommandoen ble utført, men kanskje ikke.
Kommando Repushed	Kommandoen ble sendt på nytt av en bruker.
Kasseres	Kommandoen ble forkastet. For eksempel fordi den ble erstattet av en annen kommando, eller fordi enheten ble registrert på nytt og gamle kommandoer ble fjernet.

*Hvis det er et utropstegn bak meldingen, kan du få mer informasjon ved å holde musepekeren over ikonet.

Enhetsinnstillinger

Klientkonfigurasjon

Her kan du utføre følgende konfigurasjoner på Android-enheten din:

Tid utenfor samsvar	Tidsgrensen for brukersvar etter hvilken håndhevelseshandlingen iverksettes.
Håndhevingstiltak etter tidsavbrudd	Håndhevingstiltak når en bruker ikke utfører handlinger som fører til en kompatibel enhetsstatus
Datainnsamlingsfrekvens	Hyppighet for innsamling av enhets-/GPS-informasjon
Enhetens hjerteslagsfrekvens	Intervall som enheten skal kontakte AppTec Server med Min. 1 minutt Maks. 24 timer
Aktiver posisjonsoppdateringer	Hvis den er aktivert, sender enheten posisjonsoppdateringer til AppTec Server
Sted Oppdateringstidspunkt	Bestemmer i hvilke tidsintervaller enheten sender posisjonsoppdateringer til AppTec
Bruk Google Location Accuracy for stedsoppdatering	Hvis den er aktivert, vil nettverksposisjonen brukes for posisjonsoppdateringer (hvis den er deaktivert under "Begrensninger", vil denne innstillingen ikke påvirke noe)
Bruk GPS-posisjon for posisjonsoppdatering	Hvis den er aktivert, vil GPS-enheten brukes til posisjonsoppdateringer
Tillat fiktive (falske) lokasjoner	Gjør det mulig å forfalske posisjonsinformasjon via tredjepartsapper
Tapt forbindelse Handling	Hvis denne funksjonen er aktivert, kan du angi en handling for det tilfellet at en enhet ikke får forbindelse til MDM-serveren i løpet av hjerteslagintervallet. Hvis enheten for eksempel har en hjerteslagstid på 5 minutter, kobler den seg til serveren kl. 10:35. Deretter forlater enheten Wi-Fi-området. Neste hjerteslag kl. 10:40 vil mislykkes, og den angitte handlingen vil bli utført.

Handling	Hvilke tiltak som skal iverksettes så snart en enhet ikke lenger er i samsvar med kravene. • Lock Device = låsenhet • Wipe Device = enheten gjenopprettes til fabrikkinnstillingene • Wipe Device & SD Card = enheten gjenopprettes til fabrikkinnstillingene, og SD-kortet slettes
Terskelverdi	Du kan angi en terskelverdi for antall mislykkede hjerteslag som er nødvendig for å utløse den angitte handlingen.

Policyhåndhevelsesmodus	Standard:	Brukerne vil med jevne mellomrom bli bedt om å utføre utestående handlinger
	Lazy Policy Enforcement:	Brukerne vil aldri bli bedt om å utføre utestående handlinger. Alle åpne handlinger vil vises i AppTec Client
	Aggressiv håndheving av retningslinjer:	Brukerne blir kontinuerlig bedt om å utføre utestående handlinger
AppTec Versjonslås	Hvis aktivert, kan en versjonskode for AppTec-appen spesifiseres. AppTec-klienten vil kun oppdatere til den angitte versjonen. Nyere versjoner vil bli ignorert. En nedgradering er IKKE mulig.	
Versjonskode	Versjonskode for AppTec-appen som skal låses til.	
Deaktiver AppTec Notification	Hvis den er deaktivert, vil AppTec Client ikke vise en varsling i varslingslinjen. Dermed kan brukerne lukke AppTec-klienten via oppgavebehandling. Hvis AppTec-klienten er lukket, vil flere funksjoner, inkludert Kiosk Mode og App Black/Whitelisting, ikke fungere som de skal. Samsung-enheter tilbyr en beskyttelsesmekanisme for AppTec Client. Varslingen er deaktivert som standard på Samsung-enheter som støtter KNOX API-er. Varselet skal ikke være deaktivert på enheter med Android 8.0 eller nyere.	

Bakgrunn

Angi egendefinert bakgrunnsbilde	Aktivere/deaktivere den egendefinerte bakgrunnen
Bakgrunn	Still inn bakgrunnsmodus til å bruke en fargekode eller et bilde
Angi en farge	Angi en bakgrunnsfarge som heks-verdi, f.eks. #000000 for svart eller #ffffff som hvit
Angi bilde som bakgrunnsbilde	Last opp bildefilen du vil bruke som bakgrunnsbilde

Asset Management (kun på enhetsnivå)

Enhetsinfo

Modell	Modellbetegnelse for enheten
Operativsystem	OS
OS-versjon	OS-versjon
Serienummer	Serienummer
Enhetens navn	Enhetens navn
Batteristatus	Batteristatus
Ledig / totalt minne	Ledig / totalt minne
Samsung Safe	Samsung SAFE-grensesnitt, nødvendig for en rekke innstillingsalternativer
SD-kort tilgjengelig	SD-kort tilgjengelig
SD-kort emulert	SD-kort emulert
SD-kortet kan tas ut	SD-kortet kan tas ut
SD ledig / totalt minne	SD ledig / totalt SD-kortminne

Wi-Fi

IP-adresse	Enhetens IP-adresse
WiFi MAC	WiFi MAC-adresse

Cellular

Status	Status (SIM-kort installert)
Telefonnummer	Telefonnummer
Roaming (tale/data)	Roaming for tale/data
Roaming-status	Gjeldende roamingstatus
IP-adresse	IP-adresse
Operatør/transportør	Operatør/transportør
Cellular Technology	Cellular Technology
IMEI	IMEI-nummer
ICCID	Dette er ID-en for SIM-kortet, ofte også et smartkort eller Integrated Circuit Card (ICC)
IMSI	International Mobile Subscriber Identity (IMSI) gir i GSM- og UMTS-mobilnett en sikker identifikasjon av nettverksbrukerne IMSI består av maksimalt 15 sifre og konfigureres på følgende måte: • Mobil landskode (MCC), 3 siffer • Mobilnettverkskode (MNC), 2 eller 3 siffer • Identifikasjonsnummer for mobilabonnent (MSIN), 1-10 siffer
Nåværende MCC/MNC	Se "SIM MCC/MNC"
SIM MCC/MNC	Mobile Country Code er en etablert landidentifikator som er fastsatt av ITU i henhold til E.212-standarden. Denne fungerer sammen med Mobile Network Code (MNC) for identifikasjon av mobilnettverket. Betyr SIM-kortets lands-/mobilnettverkskode. Hvis du roamer til et annet mobilnett, vil "Current MCC/MNC" og "SIM MCC/MNC" logisk sett være forskjellige.

Bluetooth

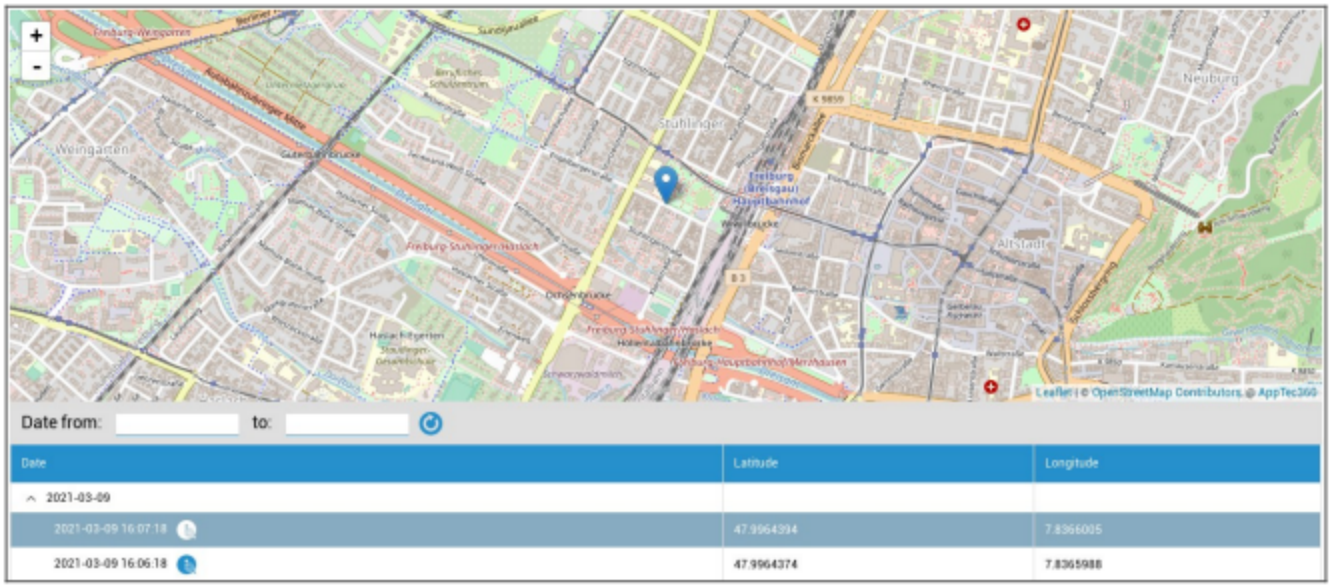
Bluetooth MAC	Bluetooth MAC-adresse

Sikkerhetsstyring

Tyverisikring (kun på enhetsnivå)

GPS-informasjon (kun på enhetsnivå)

Her kan du angi enhetens nåværende/seneste plassering. Lokaliseringen kan beskyttes med ett eller til og med to passord - se: Generelle innstillinger - Personvern - GPS-tilgang



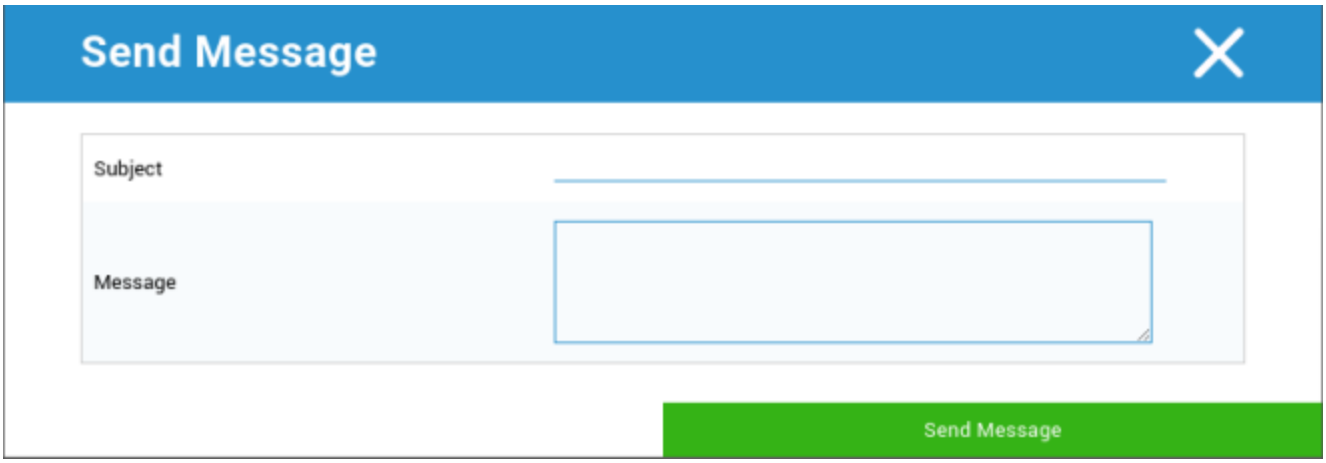
Tørk og lås (kun på enhetsnivå)

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

Full Wipe	Enheten gjenopprettes til fabrikkinnstillingene (både bedriftsdata og personlige data slettes). Fungerer bare for Enhanced Work Profile
Enterprise Wipe	Kun bedriftsdata fjernes fra sluttbrukerens enhet (alle apper, data osv. som ble levert av AppTec)
Låseskjerm	Skjermlåsen er aktivert, og det er tilstrekkelig å låse opp enheten med enhetens passord/PIN-kode

Melding (kun på enhetsnivå)

Her kan du fylle inn emne og en melding og sende den til en sluttbrukerenhet



Sikkerhetskonfigurasjon

Enhetens passord

Under "Passord" kan du angi et passord for enheten, og følgende innstillingsalternativer er tilgjengelige

Minimum passordlengde	Fastsetter det minste antallet symboler et passord må inneholde	
Passordkvalitet	Uspesifisert	Denne policyen stiller ingen krav til passordet.
	Biometrisk svakhet	Denne policyen åpner for biometrisk gjenkjenningsteknologi med lav sikkerhet. Dette innebærer teknologi som kan gjenkjenne identiteten til en person til omtrent en tresifret PIN-kode (falsk gjenkjenning er mindre enn 1 av 1 000).
	Noe	Denne policyen krever at det angis et passord eller et mønster, men den håndhever ingen spesifikke regler.
	Alfabetisk	Brukeren må ha angitt et passord som inneholder minst alfabetiske tegn (eller andre symboler).
	Alfanumerisk	Brukeren må ha angitt et passord som inneholder minst både numeriske og alfabetiske tegn (eller andre symboler).
	Kompleks	Som standard må brukeren ha angitt et passord som inneholder minst en bokstav, et tall og et spesialsymbol. Med denne passordkvaliteten kan passordene begrenses til å inneholde ulike sett med tegn, for eksempel minst en stor bokstav osv.
Minimum passordlengde	Angi antall tegn som kreves for passordet. Du kan for eksempel kreve at PIN-koden eller passordet skal inneholde minst seks tegn.	
Minimum antall siffer som kreves i passordet	Minimum antall siffer som kreves i passordet	
Minimum små bokstaver kreves i passordet	Minimum små bokstaver kreves i passordet	
Minimum store bokstaver kreves i passordet	Minimum store bokstaver kreves i passordet	
Minimum antall tegn som ikke er bokstaver	Minimum antall tegn som ikke er bokstaver som kreves i passordet	

som kreves i passordet	
Minimum symboler som kreves i passordet	Minimum symboler som kreves i passordet

Lås for maksimal inaktivitetstid	Maksimal brukerinaktivitet frem til tidslås
Tidsavbrudd for utløp av passord	Etableres, etter hvilket tidsintervall passordet utløper og et nytt passord må utstedes
Begrensning av passordhistorikk	Antall tidligere brukte passord som ikke er tillatt
Maksimalt antall mislykkede passordforsøk	Fastsetter hvor ofte et passord kan tastes inn feil før en fullstendig sletting av enheten vil bli utført
Tillat biometrisk autentisering	Muliggjør autentisering via fingeravtrykk eller irisskanning. Kun for Samsung KNOX 2.1 og nyere

Containerpassord

Under "Passcode" kan du angi et containerpassord, og følgende innstillingsalternativer er tilgjengelige for deg

Minimum passordlengde	Fastsetter det minste antallet symboler et passord må inneholde	
Passordkvalitet	Uspesifisert	Denne policyen stiller ingen krav til passordet.
	Biometrisk svakhet	Denne policyen åpner for biometrisk gjenkjenningsteknologi med lav sikkerhet. Dette innebærer teknologi som kan gjenkjenne identiteten til en person til omtrent en tresifret PIN-kode (falsk gjenkjenning er mindre enn 1 av 1 000).
	Noe	Denne policyen krever at det angis et passord eller et mønster, men den håndhever ingen spesifikke regler.
	Alfabetisk	Brukeren må ha angitt et passord som inneholder minst alfabetiske tegn (eller andre symboler).
	Alfanumerisk	Brukeren må ha angitt et passord som inneholder minst både numeriske og alfabetiske tegn (eller andre symboler).
	Kompleks	Som standard må brukeren ha angitt et passord som inneholder minst en bokstav, et tall og et spesialsymbol. Med denne passordkvaliteten kan passordene begrenses til å inneholde ulike sett med tegn, for eksempel minst en stor bokstav osv.
Minimum passordlengde	Angi antall tegn som kreves for passordet. Du kan for eksempel kreve at PIN-koden eller passordet skal inneholde minst seks tegn.	
Minimum antall siffer som kreves i passordet	Minimum antall siffer som kreves i passordet	
Minimum små bokstaver kreves i passordet	Minimum små bokstaver kreves i passordet	
Minimum store bokstaver kreves i passordet	Minimum store bokstaver kreves i passordet	
Minimum antall tegn som ikke er bokstaver som kreves i passordet	Minimum antall tegn som ikke er bokstaver som kreves i passordet	

Minimum symboler som kreves i passordet	Minimum symboler som kreves i passordet

Lås for maksimal inaktivitetstid	Maksimal brukerinaktivitet frem til tidslås
Tidsavbrudd for utløp av passord	Etableres, etter hvilket tidsintervall passordet utløper og et nytt passord må utstedes
Begrensning av passordhistorikk	Antall tidligere brukte passord som ikke er tillatt
Maksimalt antall mislykkede passordforsøk	Fastsetter hvor ofte et passord kan tastes inn feil før en fullstendig sletting av enheten vil bli utført

AntiVirus

Automatisk skanning	Aktiver periodiske automatiske skanninger
Skanneintervall	Intervall for undersøkelse (Quick / Full)
Full automatisk skanning	Aktiver helautomatiske skanninger
Automatiske oppdateringer	Aktiver automatiske oppdateringer
Intervall for oppdateringssjekk	Hvor ofte appen og databasen bør oppdateres (virus/skadet kode)
App-beskyttelse	Aktiver automatisk appskanning
Beskyttelse av SD-kort	Aktiver automatisk skanning av SD-kort
Kun Wi-Fi-oppdatering	Når denne funksjonen er aktivert, vil oppdateringer bare bli brukt når enheten er koblet til et Wi-Fi-nettverk

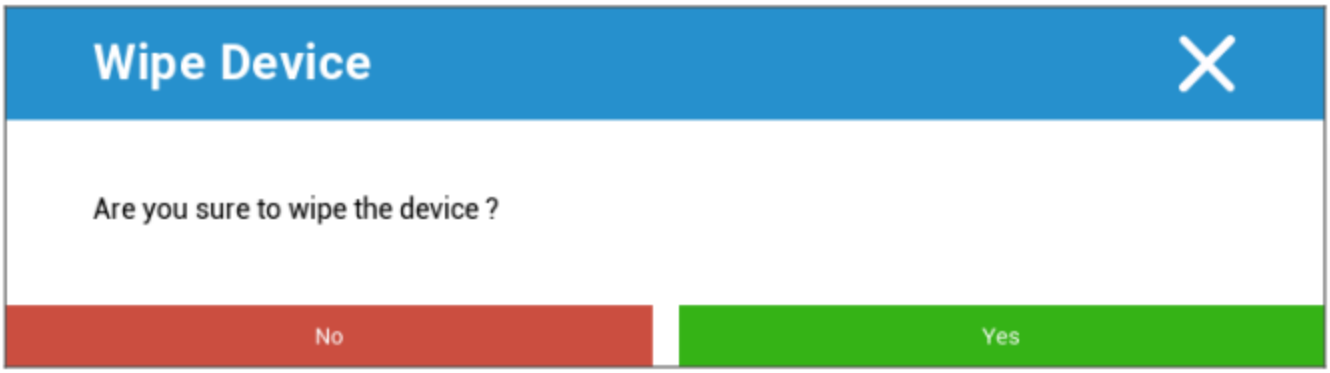
End of Life (kun på enhetsnivå)

Tørk (kun på enhetsnivå)

Under "Wipe" kan du gjenopprette enheten til fabrikkinnstillingene (kun på Enhanced Work Profile).

Her slettes både bedriftsdata og private data på sluttbrukerens enhet.

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



Med "Yes" kan du utføre tørkingen.

Under "Wipe Report" kan følgende elementer vises

Tørket av	Historikk over hvem som utførte tørkingen
Dato	Dato
Status	Status (f.eks. om tørkingen ble vellykket)

Begrensningsinnstillinger

Begrensninger

Her kan en rekke ting begrenses og blokkeres.

Håndhevelse av samsvar	Mode Prompt User - Brukeren blir bedt om å utføre de nødvendige handlingene. Mode Lock-Down Container - Skjul alle apper til alle krav er oppfylt
Retningslinjer for kjøretidstillatelser	Spør brukeren om nye forespørsler om tillatelse Alltid innvilge nye forespørsler om nye tillatelser Alltid avslå nye forespørsler om tillatelse Advarsel: Noen apper har problemer med å gjenkjenne tillatelsene hvis disse er angitt automatisk. Hvis du alltid gir tillatelser og støter på problemer med apper som sier at tillatelser mangler, kan du sette dette til "spør brukeren" og installere appen på nytt.
Tillat utgående utklippstavle	Tillater kopiering og liming fra innsiden av beholderen til utsiden
Tillat oppløsning av anroper-ID	Viser navnet på en innkommende samtale basert på kontaktene i containeren
Tillat oppløsning av kontaktsøk	Gjør det mulig å søke etter navn i containerens kontakter når du ringer
Tillat deling av Bluetooth-kontakter	Gir tilgang til beholderkontakt i en bil
Ikke tillat utgående NFC-stråle	Deaktiverer NFC for beholderen
Tillat ukjente kilder	Hvis denne funksjonen er aktivert, kan brukerne laste ned apper ved å installere en .apk-fil.
Tillat USB-feilsøking	Hvis den er aktivert, kan brukerne aktivere USB-feilsøking.
Ikke tillat endring av konto	Tillater ikke oppretting, sletting og endring av kontoer i beholderen Vær oppmerksom på at noen apper må opprette eller endre kontoer for å fungere som forventet

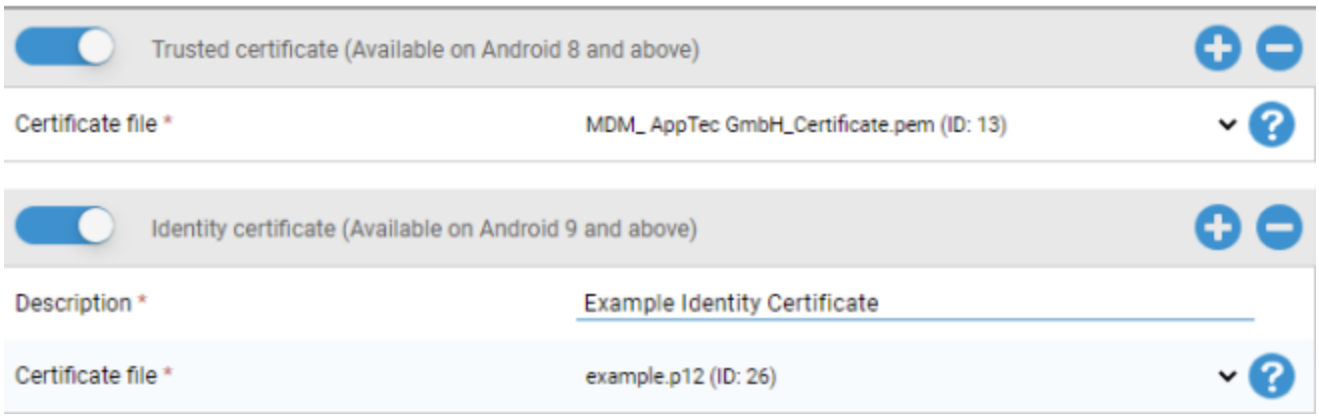
Begrensninger i arbeidsprofilen. Kun tilgjengelig på Android 11-enheter og nyere, med Enhanced Work Profile	
Ikke tillat kamera	Angir om kameraet ikke er tillatt i arbeidsprofilen.

Ikke tillat Bluetooth	Angir om Bluetooth ikke er tillatt i arbeidsprofilen.
Aktiver beskyttelse mot tilbakestilling til fabrikkinnstilling	Aktiver dette for å overstyre beskyttelsen mot tilbakestilling til fabrikkinnstillingene i Android til Google-kontoen du har definert i "Generelle innstillinger" → "Android-konfigurasjon" → "Android Enterprise" → "Beskyttelse mot tilbakestilling til fabrikkinnstillingene" Hvis dette er aktivert og du tilbakestiller enheten, må du oppgi den konfigurerte Google-kontoen for å konfigurere enheten på nytt.
Kontroll av OS-oppdatering	Aktiver denne for å angi at oppdateringen skal skje automatisk, i et vindu eller utsatt.
Oppdater retningslinjer	Automatisk: Installeres automatisk så snart en oppdatering er tilgjengelig. Vindubasert: Installer automatisk innenfor et daglig vedlikeholdsvindu. Dette konfigurerer også Play-apper til å bli oppdatert i vinduet. Dette anbefales på det sterkeste for kioskenheter, fordi dette er den eneste måten apper som er festet til forgrunnen, kan oppdateres av Play. Utsett: Utsett automatisk installasjon i opptil 30 dager.

Begrensninger for personlig profil. Kun tilgjengelig på Android 11-enheter og nyere, med Enhanced Work Profile	
Ikke tillat kamera	Angir om kameraet ikke er tillatt i den personlige profilen.
Ikke tillat Bluetooth	Angir om Bluetooth ikke er tillatt i den personlige profilen.
Tillat ukjente kilder	Hvis denne funksjonen er aktivert, kan brukere av arbeidsprofilen laste ned apper ved å installere en .apk-fil.

Sertifikatforvaltning

Her kan du distribuere betrodde sertifikater og identitetssertifikater til enhetene dine. Android 8 eller nyere kreves for å distribuere betrodde sertifikater, og Android 9 eller nyere kreves for å distribuere identitetssertifikater.



Med "+" kan du legge til flere sertifikater.

Klarerte sertifikater må være i PEM-format.

Identitetssertifikater må være i PKCS12-format.

Administrasjon av tilkoblinger

Wifi

For denne innstillingen må du utføre forhåndskonfigurasjon av sluttbrukerens enheter for tilgang til interne Access
-punkter

Services Set Identifier (SSID)	SSID for nettverket som skal kobles til
Skjult nettverk	Aktiver, i tilfelle AP-et ikke kringkaster SSID

Sikkerhetstype

Fastsette AP-ets sikkerhetstype

WEP

Passord	Passord for AP

WPA/WPA2

Passord	Passord for AP

802.1x EAP

EAP-metode

PWD	Identitet	Identitet
	Passord	Passord

PEAP	Fase 2 autentiseringsprotokoll	ingen	Ingen tilleggsprotokoll
		MSCHAPV2	MSCHAPV2-protokollen
		GTC	GTC-protokoll
	CA-sertifikat	CA-sertifikat	
	Identitet	Identitet	
	Anonym identitet	Anonym identitet	
	Passord	Passord	

TTLS	Fase 2 autentiseringsprotokoll	ingen	Ingen tilleggsprotokoll
		PAP	PAP-protokoll
		MSCHAP	MSCHAP-protokollen
		MSCHAPV2	MSCHAPV2-protokollen
		GTC	GTC-protokoll
	CA-sertifikat	CA-sertifikat	
	Identitet	Identitet	
	Anonym identitet	Anonym identitet	
	Passord	Passord	

TLS	CA-sertifikat	CA-sertifikat
	Identitet	Identitet
	Passord	Passord

VPN

Navn på tilkobling	Navn på VPN-tilkoblingen

VPN-type

VPN

VPN-klient

AppTec VPN-klient	
Gateway-konfigurasjon	Velg Gateway VPN-konfigurasjon (se **Generelle innstillinger > Universal Gateway > VPN-innstillinger**)
Alltid på VPN	Aktiver Native Lockdown
Aktiver AppTec Lockdown	Aktiver AppTec Lockdown

Innebygd (kun tilgjengelig på Samsung-enheter)			
Type tilkobling	PPTP	Server	Server
		Aktiver PPTP-kryptering	Aktiver PPTP-kryptering
	L2TP / IPSec PSK	Server	Server
		IPSec forhåndsdelt nøkkel	IPSec forhåndsdelt nøkkel
		Aktiver L2TP-hemmelighet	Aktiver L2TP-hemmelighet
		L2TP-hemmelighet	L2TP-hemmelighet
	IPSec XAuth PSK	Server	Server
		IPSec-identifikator	IPSec-identifikator
		IPSec forhåndsdelt nøkkel	IPSec forhåndsdelt nøkkel
DNS-søkedomener	DNS-søkedomener		
Ekspertinnstillinger	DNS-servere	DNS-servere	
	Videresendingsruter	Videresendingsruter	

Åpen VPN		
Server	Server	
OpenVPN-profil	OpenVPN-profil	
OpenVPN-app	OpenVPN for Android (anbefalt)	
	OpenVPN Connect	
Ekspertinnstillinger	DNS-servere	DNS-servere
	Videresendingsruter	Videresendingsruter

Samsung / Strong Swan			
Type tilkobling	PPTP	Server	Server
		Brukernavn	Brukernavn
		Passord	Passord
		Aktiver PPTP-kryptering	Aktiver PPTP-kryptering
	L2TP / IPSec PSK	Server	Server
		IPSec forhåndsdelt nøkkel	IPSec forhåndsdelt nøkkel
		Brukernavn	Brukernavn
		Passord	Passord
		Aktiver L2TP-hemmelighet	L2TP-hemmelighet
	IPSec XAuth PSK	Server	Server
		IPSec-identifikator	IPSec-identifikator
		IPSec forhåndsdelt nøkkel	IPSec forhåndsdelt nøkkel
		Brukernavn	Brukernavn
		Passord	Passord
Ekspertinnstillinger	DNS-servere	DNS-servere	
	Videresendingsruter	Videresendingsruter	

Cisco Any Connect		
Server	Server	
Sertifikatmodus	Deaktivert	Deaktivert
	Automatisk	Automatisk
Ekspertinnstillinger	DNS-servere	DNS-servere
	Videresendingsruter	Videresendingsruter

VPN per app

VPN-klient

AppTec VPN-klient		
Gateway-konfigurasjon	Velg Gateway VPN-konfigurasjon (se **Generelle innstillinger > Universal Gateway > VPN-innstillinger**)	
VPN-apper	VPN-apper	
Alltid på VPN	Aktiver Native Lockdown	Alltid på VPN
Aktiver AppTec Lockdown	Aktiver AppTec Lockdown	

Samsung / Strong Swan			
Type tilkobling	PPTP	Server	Server
		VPN-apper	VPN-apper
		Brukernavn	Brukernavn
		Passord	Passord
		Aktiver PPTP-kryptering	Aktiver PPTP-kryptering
	L2TP / IPSec PSK	Server	Server
		VPN-apper	VPN-apper
		IPSec forhåndsdelt nøkkel	IPSec forhåndsdelt nøkkel
		Brukernavn	Brukernavn
		Passord	Passord
		Aktiver L2TP-hemmelighet	L2TP-hemmelighet
	IPSec XAuth PSK	Server	Server
		VPN-apper	VPN-apper
		IPSec-identifikator	IPSec-identifikator
		IPSec forhåndsdelt nøkkel	IPSec forhåndsdelt nøkkel
		Brukernavn	Brukernavn
		Passord	Passord
Ekspertinnstillinger	DNS-servere	DNS-servere	
	Videresendingsruter	Videresendingsruter	

Begrensninger

Her kan du angi restriksjoner i forhold til tilkoblingsadministrasjon

Tillat dataroaming	Tillat mobildata under roaming
Tving frem dataroaming	Hvis den er aktivert, er roaming for mobildata permanent aktivert (anbefales ikke!) Denne innstillingen overskriver innstillingen "Tillat dataroaming"!
Bruk System http Proxy Server	Bruken av en HTTP-proxy-server, som er gitt av systemets innstillinger i innstillinger, er avhengig av det tilkoblede nettverket (WiFi eller APN)

PIM-administrasjon

Gmail Exchange

Info: Denne konfigurasjonen vil bli brukt på Gmail-appen. Du må derfor godkjenne og installere Gmail.

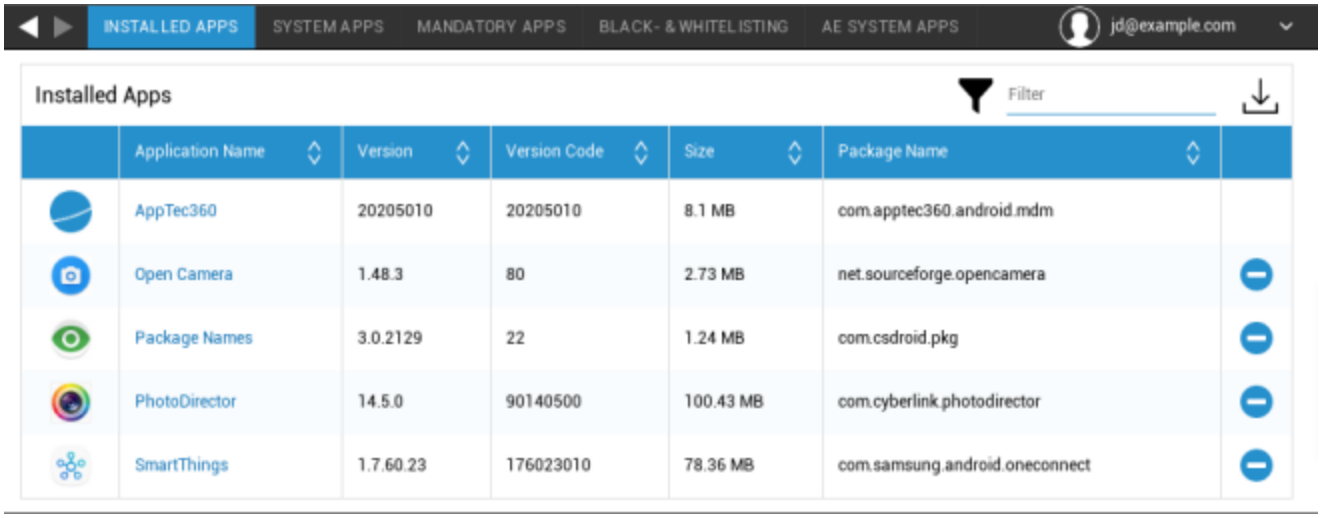
E-postadresse	Den oppgitte e-postadressen til brukeren Vær oppmerksom på "plassholderne", som du kan bruke til å arbeide med legitimasjon og ikke utføre endringer manuelt på alle enheter Med et klikk på kan du vise dem for deg selv
Serverens vertsnavn	Serveradressen til Exchange-serverne dine
Innloggingsnavn	Innloggingsnavnet for den respektive sluttbrukerenheten, legg også merke til "Placeholders here".
Signatur	En signatur kan legges ved (Tips: Noen enheter krever HTML-formatering for signaturen)
Antall foregående dager som skal synkroniseres	Antall dager som avgjør når e-poster synkroniseres tilbake
Enhetsidentifikator	En streng som inneholder EAS DeviceID. Dette er en del av EAS-protokollen og er nødvendig i noen områder
Bruk Secure Sockets Layer (SSL)	Bruk en SSL-tilkobling
Godta alle sertifikater	Alle sertifikater godtas. Velg dette alternativet hvis Exchange-serveren bruker et selvsignert sertifikat
Tillat ikke-administrerte kontoer	Tillat brukere å legge til eller fjerne andre Exchange-kontoer enn den kontoen som er angitt i denne administrerte konfigurasjonen. Hvis denne innstillingen er aktivert, kan du ikke hindre brukere i å legge til andre Exchange-kontoer i Gmail. Du kan heller ikke kontrollere datadeling mellom andre apper og Exchange-kontoer som er lagt til av brukere. Denne innstillingen bør bare aktiveres hvis brukerne dine har behov for å ha mer enn én Exchange-konto i Gmail.
Kundesertifikat	Klientsertifikat. Kun påkrevd hvis e-postserveren forventer at dette sertifikatet skal være til stede.

App-administrasjon

Enterprise App Manager

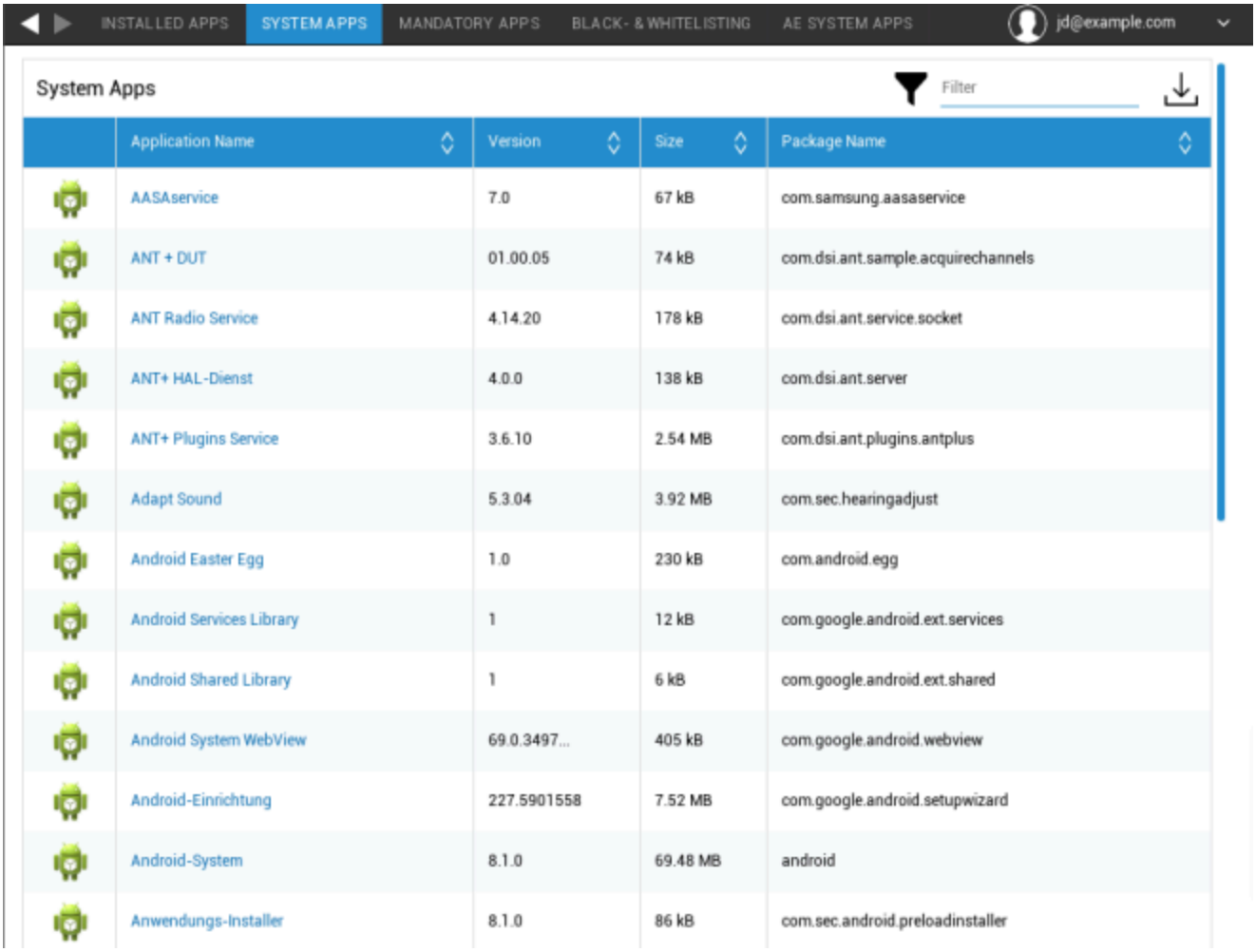
Installerte apper (kun på enhetsnivå)

Her vises alle apper som for øyeblikket er installert i beholderen.



Systemapper (kun på enhetsnivå)

Under "System Apps" finner du en liste over alle apper og tjenester som allerede er installert på sluttbrukerenheten av produsenten av enheten.

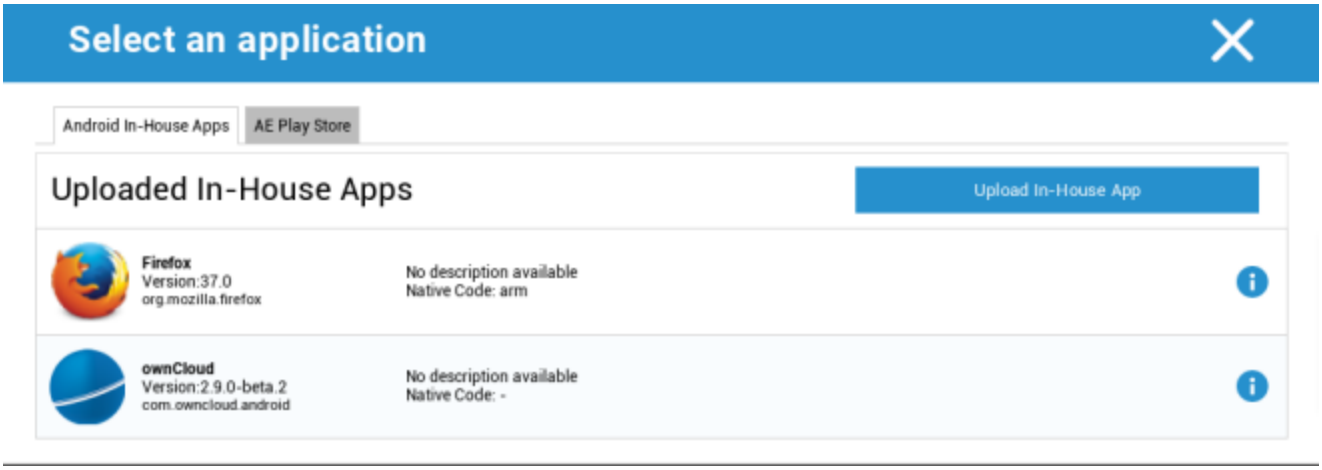


Obligatoriske apper

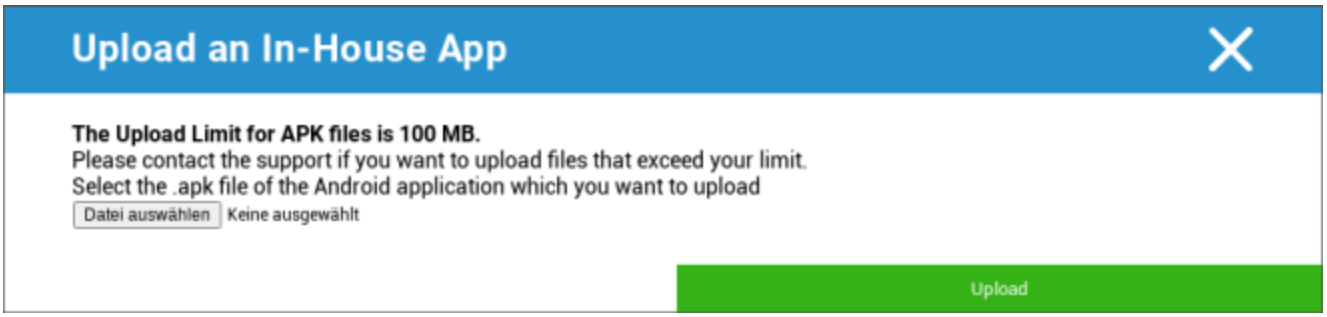
Under Obligatoriske apper kan du opprette de obligatoriske appene som kreves. Brukeren vil kontinuerlig bli bedt om å installere denne utpekte appen, hvis det er en InHouse-app. Apper fra Play Store installeres automatisk.

Via kan den obligatoriske nødvendige appen defineres.

Dette kan være en egen app fra "Android In-House Apps", som du har lastet opp i Generelle innstillinger.

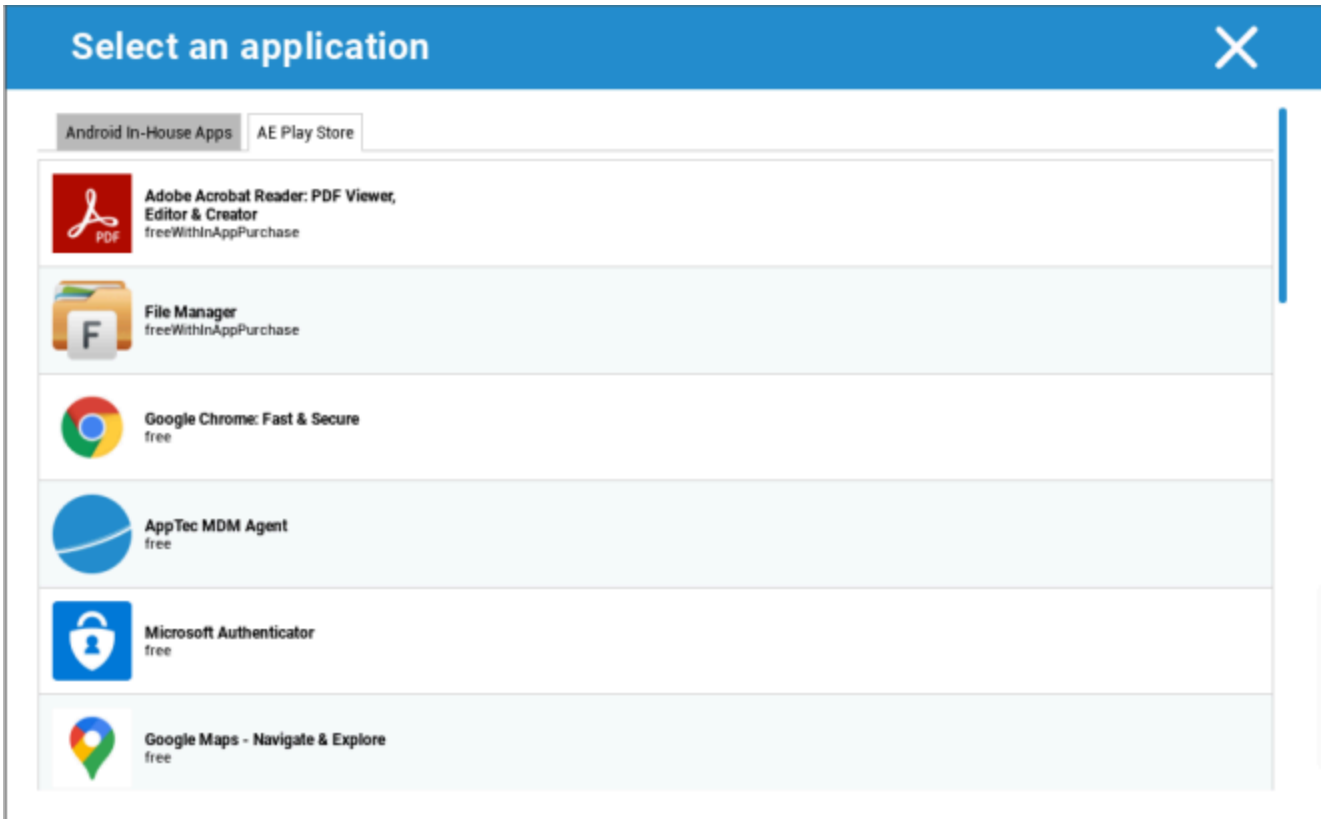


Du kan også velge og laste opp en apk-fil direkte med "Upload In-House App".



Hvis du installerer en In-House-app, har du mulighet til å aktivere "Hold deg oppdatert". Hvis dette er aktivert og du har definert en nyere versjon i In-House App DB, vil appen bli oppdatert på enheten.

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



Bare godkjente "AE Play Store-apper" vises i denne kategorien.

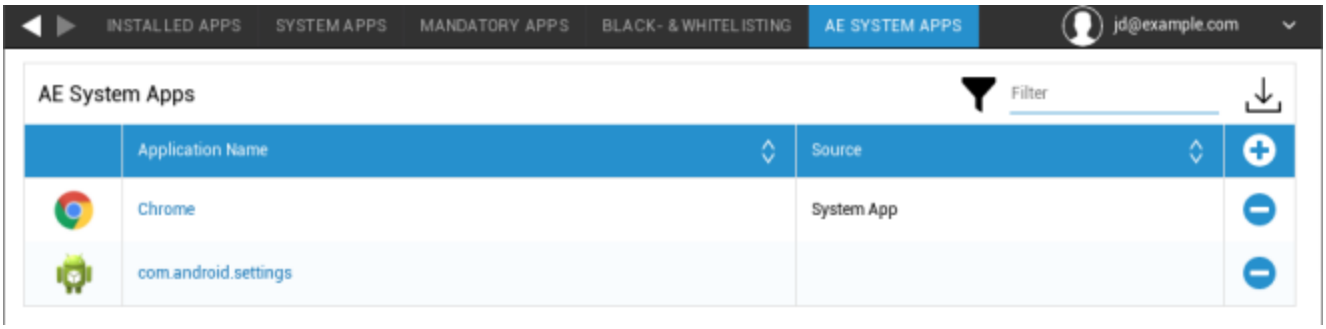
For å godkjenne en "AE Play Store-app", gå til "Generelle innstillinger" > "Appadministrasjon" > "AE Play

Store" og legge til en app via knappen som videresender deg til "Play Store Apps"-fanen (eller du kan gå direkte til "Play Store Apps"-fanen).

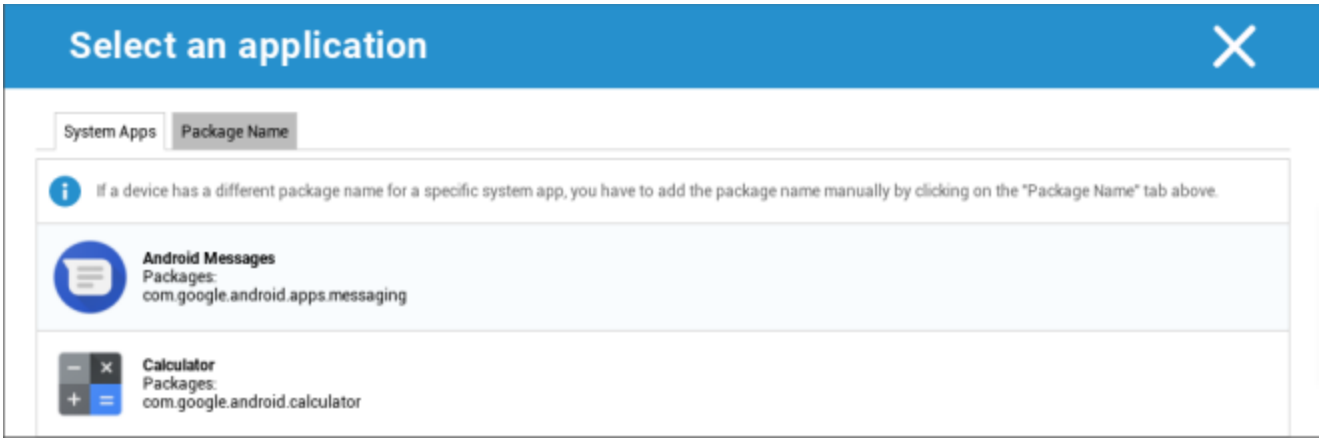
Under fanen "Play Store Apps" kan du søke etter apper. Når du klikker på en app, åpnes app-siden, og her kan du godkjenne appen ved å klikke på "Approve".

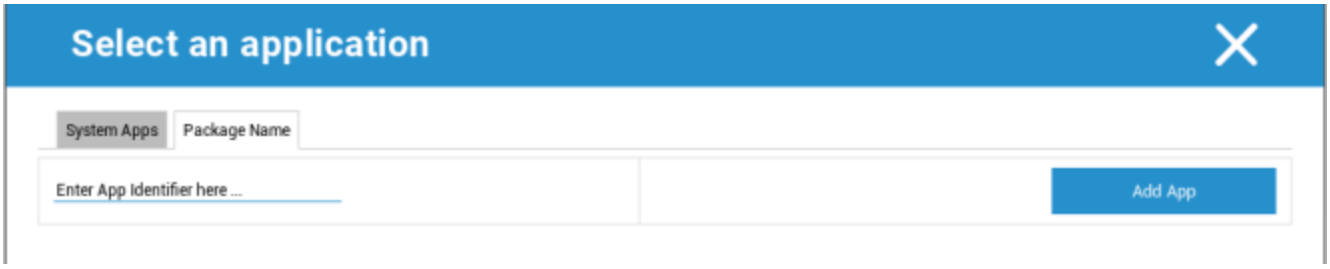
AE System-apper

Her kan du definere en liste som inneholder spesifikke systemapper som skal aktiveres på enhetene.



Hvis du klikker på knappen, kan du velge fra en liste over mulige systemapper fra Google eller skrive direkte inn pakkenavnet til en systemapp som skal aktiveres.





Vær oppmerksom på at systemappene i listen fra Google kun er apper som kan være systemapper, men at de ikke nødvendigvis må være systemapper på enhetene dine.

Denne listen påvirker imidlertid bare apper som allerede er forhåndsinstallert.

Apper som ikke er forhåndsinstallert på enhetene dine, vil ikke påvirke enhetene dine, uansett om appen er fra listen fra Google eller om appens pakkenavn legges inn direkte.

Begrensninger og innstillinger

Innstillinger for appadministrasjon

Her kan du konfigurere hvordan enheten skal oppføre seg når det gjelder appoppdateringer.

Hyppighet for oppdateringssjekk	Angi i hvilket intervall AppTec Client skal søke etter appoppdateringer. Standardverdien er 24 timer.
Wi-Fi-terskelverdi	Apper som er større enn den angitte størrelsen, lastes ned via Wi-Fi. Hvis "Kun Wi-Fi" er valgt, lastes alle apper ned via Wi-Fi.

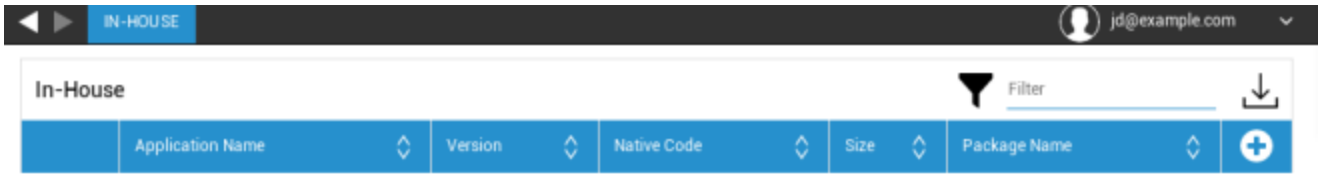
App Store for bedrifter

Internt

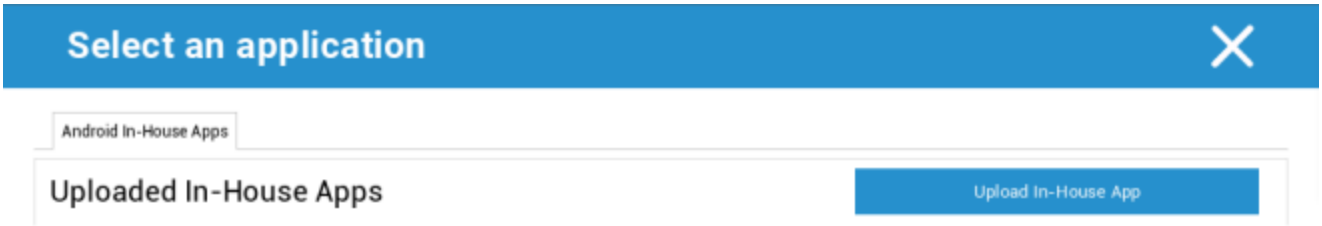
Under punktet "In-House" kan du laste opp og distribuere internt utviklede apper.

Med symbolet kan du distribuere flere In-House-apper.

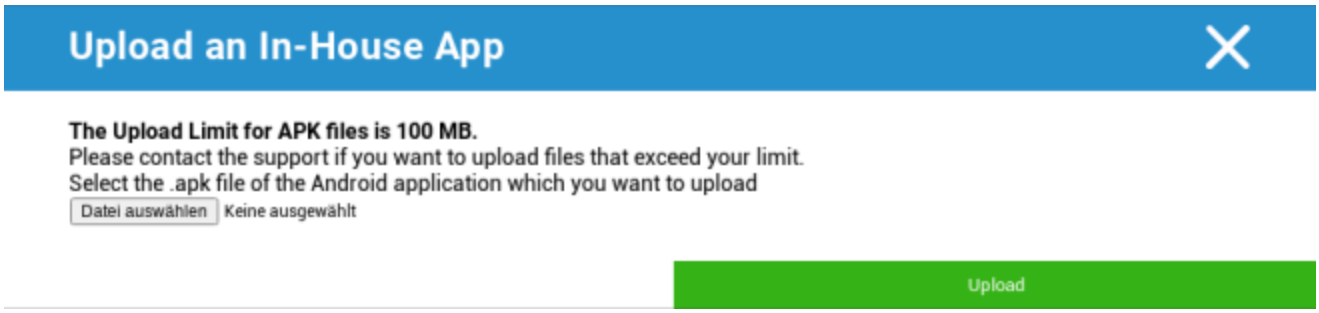
Hvis du installerer en In-House-app, har du mulighet til å aktivere "Hold deg oppdatert". Hvis dette er aktivert og du har definert en nyere versjon i In-House App DB, vil appen bli oppdatert på enheten.



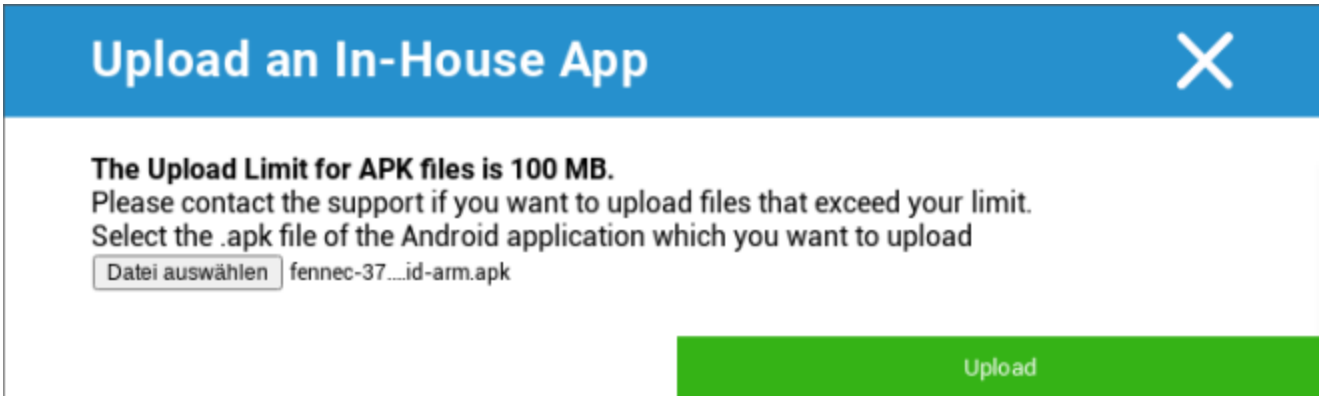
Hvis du ikke har distribuert In-House Apps, vil du motta følgende oversikt:



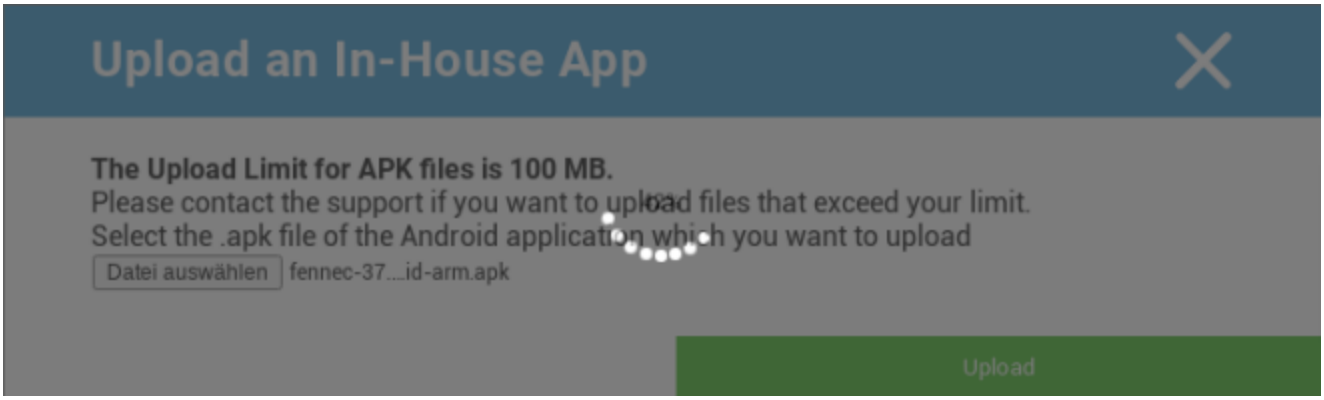
Klikk på "Last opp egen app", og du vil da få opp følgende oversikt:



Nå velger du med "Søk ..." en .apk-fil og klikker deretter på "Last opp".



Appen din blir nå lastet opp, og i midten av sirkelen ser du en prosentindikator som viser hvor mye av appen din som allerede er lastet opp.



Hvis opplastingen av din In-House-app har vært vellykket, kan du finne den opplastede appen i App Catalog.

Brukeren har nå muligheten til å se og installere denne appen i AppTec Store på sluttbrukerens enhet, under kategorien "In-House".

Siden dette ikke involverer en Google PlayStore-app, trenger ikke brukeren en lagret Google-ID på sin respektive sluttbrukerenhet.

Enterprise Play Store

AE Play Store

Her kan du legge til apper i Android Enterprise Playstore. Vær oppmerksom på at du må godkjenne apper med AE-administratorkontoen din før du kan legge dem til.

For godkjenning av en app, se instruksjonene i Obligatoriske apper.

Innholdsstyring

Innholdsboks

Her kan du aktivere ContentBox.

Så snart du setter "Aktiver ContentBox" til "På", installeres det automatisk en egen ContentBox-app på sluttbrukerens enhet.

Sikker nettleser

Her kan du konfigurere innstillinger for AppTec Secure Browser.

Så snart du setter "Sikker nettleser" til "På", installeres det automatisk en egen nettleser-app på sluttbrukerens enhet.

Krever passord	Krev at brukeren oppretter og bruker et passord for å få tilgang til nettleseren.
Minste nødvendige passordlengde	Angi antall tegn som kreves for passordet
Nødvendig passordkvalitet	Angi ønsket passordkvalitet
Begrens nedlastinger / Åpne i	
Begrens opplastinger	
Last opp hviteliste	En liste over URL-adresser som det alltid vil være tillatt å laste opp.
Tillat kopiering	Tillat kopiering, klipping eller deling av tekst inne på nettsidene.
Tillat skjermopptak	Tillat å ta skjermbilder.
Hyppighet for opprydding av data	Velg med hvilken frekvens ALLE brukerdata (historikk, hurtigbuffer osv.) skal fjernes automatisk.
Selskapets bokmerker	Bokmerkene vises i mappen "Company bookmarks" i nettleserens bokmerker. De kan ikke redigeres av brukeren.
Skjul adresselinjen	
Hvitelisting i nettleseren (uten Universal Gateway)	Aktiverer hvitelisting av URL-er på klientsiden. • Selskapets bokmerker er alltid hvitelistet • Støttes kun for 100 nettadresser • Bruk Universal Gateway for ubegrenset svart- og hvitelisting
Hvitelistede nettadresser	En liste over tillatte nettadresser.
Gateway-basert svart- og hvitelisting	Svartelisting har følgende krav: • En fungerende AppTec Universal Gateway ("Generelle innstillinger" → "Universal Gateway")

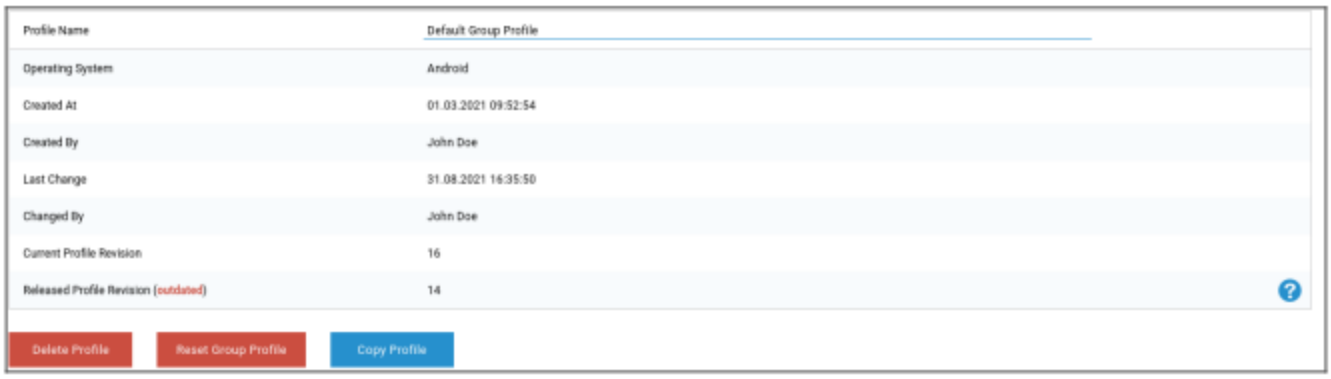
	• En fungerende VPN-konfigurasjon med en spesifisert DNS-server ("Generelle innstillinger" → "Universal Gateway" → "VPN-innstillinger") • En svartelistekonfigurasjon ("Generelle innstillinger" → "Universal Gateway" → "Domain Blacklist") • En gyldig VPN-tilkobling i profilen ("Tilkoblingsadministrasjon" → "VPN")

Android-konfigurasjon

Generelt

Oversikt over gruppeprofiler (kun på gruppenivå)

Når du åpner en gruppeprofil, får du en rask oversikt over profilen.



Profilnavn	Navn på profilen (kan endres her)
Operativsystem	Operativsystemet profilen er beregnet på
Opprettet på	Tidspunktet for skapelsen
Opprettet av	Skaperen av profilen
Siste endring	Tidspunkt for siste endring av profilen
Endret av	Konto som gjorde de siste endringene
Nåværende profilrevisjon	Revisjon av lagret profilstatus
Utgitt profilrevisjon	Tilordnet profilrevisjon ("Tilordne nå"). Hvis etiketten viser "(utdatert)" bak teksten, betyr det at du har lagret profilen, men ikke tilordnet den ennå, slik at enhetene fortsatt vil få en eldre versjon.

Enhetsoversikt (kun på enhetsnivå)

Hvis du befinner deg på en enhet, vil du få en oversikt over den valgte enheten, og her finner du følgende:

Enhetens navn	Enhetens navn
Sist kjente posisjon	De siste kjente GPS-koordinatene
Telefonnummer	Telefonnummer
Tildelte obligatoriske apper	Antall tildelte obligatoriske apper
OS-versjon	OS-versjon av enheten
Operativsystem	Operativsystem (Android / iOS / Windows Phone)
Serienummer	Enhetens serienummer
Eierskap til enheten	Bedrifts- eller privat enhet
Enhetstype	Telefon eller nettbrett
Rotfestet	Status, som angir om enheten har blitt rotfestet
Overensstemmende	I samsvar med retningslinjene
IP-adresse	IP-adresse
Sist sett	Tidspunkt for når enheten sist ble koblet til AppTec
Siste fremstøt	Tidspunkt for når serveren sendte en push til enheten
Tildeling av bruker	En rullegardinmeny for å tilordne enheten til en annen bruker

Konfigureringsrevisjon (kun på enhetsnivå)

Her får du en oversikt over hvilken gruppeprofil som er tilordnet enheten.

Hvis du klikker på gruppeprofilen, får du direkte tilgang til profilen og kan utføre innstillinger.

Med symbolet kan du tilbakestille de tilordnede appene til gruppeprofilens innstillinger.

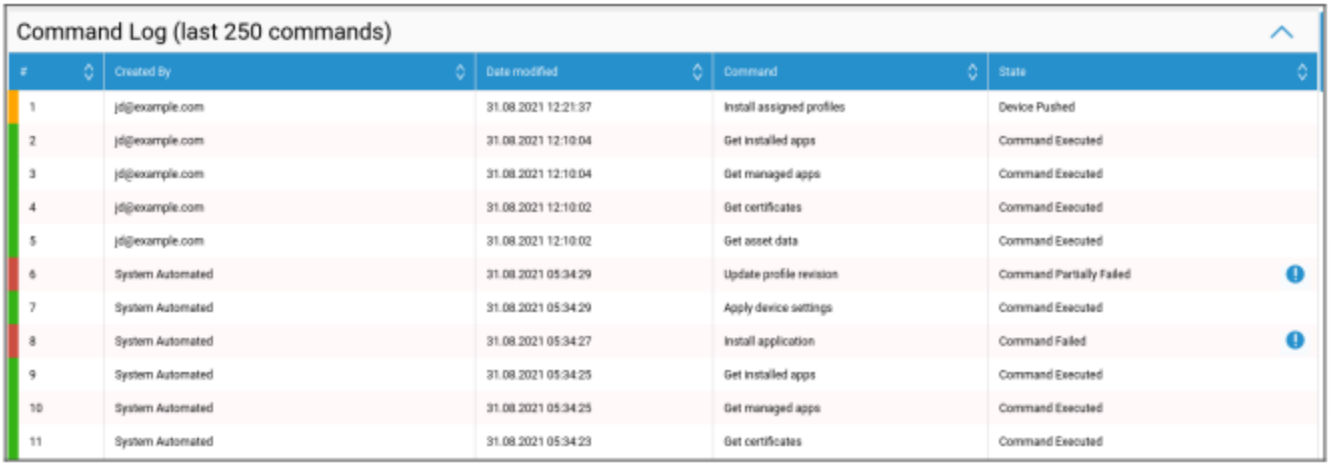
Med symbolet kan du tilbakestille enhetsprofilen slik at den ikke har noen innstillinger i det hele tatt.

"Nyere revisjon tilgjengelig" indikerer at gruppeprofilen har blitt endret og lagret, men ikke tilordnet. Gruppeprofilen må tilordnes med "Tilordne nå" på gruppenivå for at endringene skal gjelde for enhetene.

Enhetslogg (kun på enhetsnivå)

Kommandologg

Her kan du se hvilke kommandoer som er utstedt for enheten, og hvilken status de har.



Kommandoer som opprettes av "System Automated", opprettes automatisk av systemet.

Mulige kommandostatuser

Enhet skjøvet	En push-forespørsel har blitt sendt til push-tjenesten (f.eks. APNS) for å be enheten om å koble seg tilbake til EMM-serveren.
Kommando opprettet	Kommandoen ble opprettet i systemet.
Kommando sendt	Kommandoen ble sendt til enheten etter at den ble koblet til serveren.
Kommando utført	Kommandoen ble vellykket utført.
Kommando mislyktes	Kommandoen mislyktes. *
Kommandoen mislyktes delvis	Avhengig av enhetens operativsystem kan enkelte kommandoer bli gruppert sammen. I dette mislyktes noen deler av denne kommandogruppen. *
Kommando utført, men mislyktes til slutt	Kommandoen ble utført, men kanskje ikke.
Kommando Repushed	Kommandoen ble sendt på nytt av en bruker.
Kasseres	Kommandoen ble forkastet. For eksempel fordi den ble erstattet av en annen kommando, eller fordi enheten ble registrert på nytt og gamle kommandoer ble fjernet.

*Hvis det er et utropstegn bak meldingen, kan du få mer informasjon ved å holde musepekeren over ikonet.

Enhetsinnstillinger

Klientkonfigurasjon

Her kan du utføre følgende konfigurasjoner på Android-enheten din:

Advarselsmelding etter deaktivering av Device Management	Etablert advarsel etter deaktivering av Device Management
Tid utenfor samsvar	Tidsgrense for når "Håndhevingstiltak etter samsvar" skal utføres hvis enheten ikke er i samsvar med kravene. Min. 1 minutt Maks. 24 timer
Håndhevingstiltak etter tidsavbrudd	Hvilke tiltak som skal iverksettes så snart en enhet ikke lenger er i samsvar med kravene. • ikke gjøre noe = ingen handling • Lock Device = låseenhet • Wipe Device = enheten gjenopprettes til fabrikkinnstillingene
Datainnsamlingsfrekvens	Hyppighet for innsamling av enhets-/GPS-informasjon
Enhetens hjerteslagsfrekvens	Intervall som enheten skal kontakte AppTec360 Server med Min. 1 minutt Maks. 24 timer
Aktiver posisjonsoppdateringer	Hvis den er aktivert, sender enheten posisjonsoppdateringer til AppTec360 Server
Sted Oppdateringstidspunkt	Bestemmer i hvilke tidsintervaller enheten sender posisjonsoppdateringer til AppTec
Bruk Google Location Accuracy for stedsoppdatering	Hvis den er aktivert, vil Google Location Accuracy (tidligere kjent som nettverksposisjon) brukes for posisjonsoppdateringer (hvis dette ble deaktivert under "Begrensninger", vil denne innstillingen ikke påvirke noe)
Bruk GPS-posisjon for posisjonsoppdatering	Hvis den er aktivert, vil GPS-enheten brukes til posisjonsoppdateringer

Tillat fiktive (falske) lokasjoner	Gjør det mulig å forfalske posisjonsinformasjon via tredjepartsapper
Tapt forbindelse Handling	Gjør det mulig å angi en bestemt handling som skal utføres etter et visst antall mislykkede hjerteslag
Policyhåndhevelsesmodus	Definerer hvor aggressivt AppTec360 Client ber brukeren om å utføre visse handlinger som krever brukerinput. Interval (standard) = spør i intervaller, slik at brukeren kan sette dette i bakgrunnen en stund. Ingen varsling = ingen popup-vindu for nødvendig interaksjon. Du må åpne AppTec360 Client manuelt for å sjekke om det er en nødvendig handling Konstant varsel = Brukeren kan bare utføre den nødvendige handlingen. AppTec360 Client vil tvinge seg selv i forgrunnen hvis brukeren prøver å unngå det
AppTec360 Versjonslås	Lar deg definere en versjon av AppTec360 Client som er den maksimale versjonen klienten oppdaterer seg selv til.

Bakgrunn

Her kan du definere en egendefinert bakgrunn.

Med "Angi en farge" kan du definere en farge i hex-format (f.eks. #000000). Bare hex-verdier er tillatt.

Med "Angi bilde som bakgrunn" kan du laste opp et bilde. Vær oppmerksom på at ulike enheter med ulike startprogrammer og OS-versjoner fungerer forskjellig. Det finnes ingen generell veiledning for størrelse og forhold, siden dette avhenger av enheten.

Bruk JPG (eller JPEG) eller PNG som filformat.

Asset Management (kun på enhetsnivå)

Kapitalforvaltning

Enhetsinfo

Modell	**Modellbetegnelse for enheten**
Operativsystem	OS
OS-versjon	OS-versjon
AE-støtte	Støtte for Android Enterprise (container og fullstendig administrert)
Serienummer	Serienummer
Enhetens navn	Enhetens navn
Batteristatus	Batteristatus
Ledig / totalt minne	Ledig / totalt minne
Samsung KNOX	Samsung KNOX API-nivå
SD-kort tilgjengelig	SD-kort tilgjengelig
SD-kort emulert	SD-kort emulert
SD-kortet kan tas ut	SD-kortet kan tas ut
SD ledig / totalt minne	SD ledig / totalt SD-kortminne

Wi-Fi

IP-adresse	Enhetens IP-adresse
WiFi MAC	WiFi MAC-adresse

Cellular

Status	Status (SIM-kort installert)
Telefonnummer	Telefonnummer
Roaming (tale/data)	Roaming for tale/data
Roaming-status	Gjeldende roamingstatus
IP-adresse	IP-adresse
Operatør/transportør	Operatør/transportør
Cellular Technology	Cellular Technology
IMEI	IMEI-nummer
ICCID	Dette er ID-en for SIM-kortet, ofte også et smartkort eller Integrated Circuit Card (ICC)
IMSI	International Mobile Subscriber Identity (IMSI) gir i GSM- og UMTS-mobilnett en sikker identifikasjon av nettverksbrukerne IMSI består av maksimalt 15 sifre og konfigureres på følgende måte: • Mobil landskode (MCC), 3 siffer • Mobilnettverkskode (MNC), 2 eller 3 siffer • Identifikasjonsnummer for mobilabonnent (MSIN), 1-10 siffer
Nåværende MCC/MNC	Se "SIM MCC/MNC"
SIM MCC/MNC	Mobile Country Code er en etablert landidentifikator som er fastsatt av ITU i henhold til E.212-standarden. Denne fungerer sammen med Mobile Network Code (MNC) for identifikasjon av mobilnettverket. Betyr SIM-kortets lands-/mobilnettverkskode. Hvis du roamer til et annet mobilnett, vil "Current MCC/MNC" og "SIM MCC/MNC" logisk sett være forskjellige.

Bluetooth

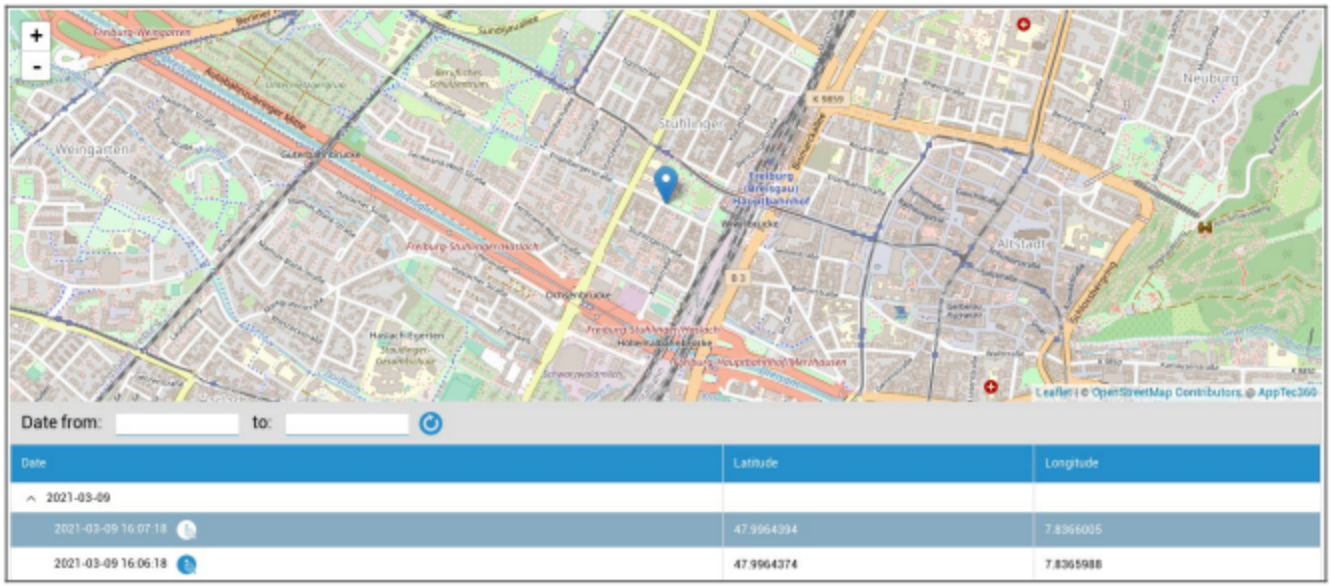
Bluetooth MAC	Bluetooth MAC-adresse

Sikkerhetsstyring

Tyverisikring (kun på enhetsnivå)

GPS-informasjon (kun på enhetsnivå)

Her kan du angi enhetens nåværende/seneste plassering. Lokaliseringen kan beskyttes med ett eller til og med to passord - se: Generelle innstillinger - Personvern - GPS-tilgang



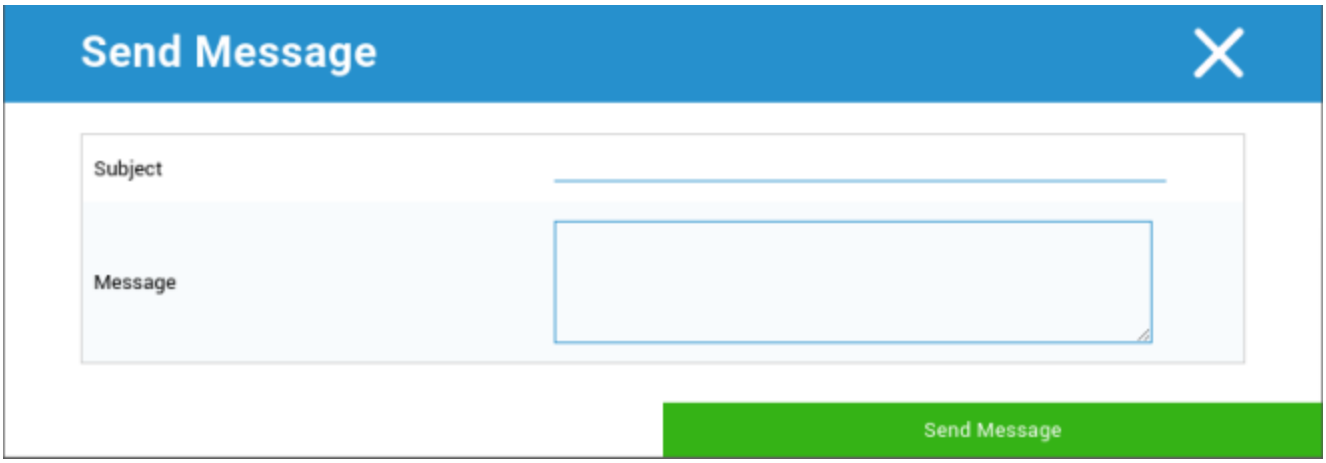
Tørk og lås (kun på enhetsnivå)

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

Full Wipe	Enheten tilbakestilles til fabrikkinnstillingene (både bedriftsdata og personlige data slettes)
Enterprise Wipe	Kun bedriftsdata fjernes fra sluttbrukerens enhet (alle apper, data osv. som ble levert av AppTec360)
Låseskjerm	Skjermlåsen er aktivert, og det er tilstrekkelig å låse opp enheten med enhetens passord/PIN-kode

Melding (kun på enhetsnivå)

Du kan fylle inn emne og en melding og sende den til en sluttbrukerenhet. Denne meldingen vil vises i AppTec360 Client.



Sikkerhetskonfigurasjon

Passord

Under "Passord" kan du angi et passord for enheten, og følgende innstillingsalternativer er tilgjengelige

Minimum passordlengde	Fastsetter det minste antallet symboler et passord må inneholde
Passordkvalitet	Passordstyrke Uspesifisert = ikke spesifisert Alle passord er ok = alle passord er akseptable minst numeriske tegn = må inneholde minst numeriske tegn minst komplekse tegn = må inneholde minst spesialtegn minst alfanumeriske tegn = må inneholde minst alfanumeriske tegn minst alfabetiske tegn = må inneholde minst alfabetiske tegn
Lås for maksimal inaktivitetstid	Maksimal tidsavbrudd på skjermen. Dette konfigurerer bare den maksimale verdien som kan velges av brukeren.
Minimum små bokstaver kreves i passordet	Minimum små bokstaver kreves i passordet
Minimum store bokstaver kreves i passordet	Minimum store bokstaver kreves i passordet
Minimum antall tegn som ikke er bokstaver som kreves i passordet	Minimum antall tegn som ikke er bokstaver som kreves i passordet
Minimum antall siffer som kreves i passordet	Minimum antall siffer som kreves i passordet
Minimum symboler som kreves i passordet	Minimum symboler som kreves i passordet
Tidsavbrudd for utløp av passord	Etableres, etter hvilket tidsintervall passordet utløper og et nytt passord må utstedes
Begrensning av passordhistorikk	Antall tidligere brukte passord som ikke er tillatt
Maksimalt antall mislykkede passordforsøk	Fastsetter hvor ofte et passord kan tastes inn feil før en fullstendig sletting av enheten vil bli utført

Kryptering

Under dette punktet kan du kryptere det interne enhetsminnet, så vel som SD-kortminnet.

Krev lagringskryptering	Hvis denne innstillingen er aktivert, krypteres enhetens minne så lenge enheten støtter denne funksjonen. Når enhetens minne er kryptert for første gang, er det ikke lenger mulig å dekryptere det. På samme måte vil passordpolicyen automatisk bli endret til 6 alfanumeriske symboler
Krev SD-kortkryptering	Denne innstillingen gjelder bare for Samsung-enheter! Hvis denne innstillingen er aktivert, kan det eksterne SD-kortet krypteres og kan bare dekrypteres manuelt på sluttbrukerens enhet. På samme måte vil passordpolicyen automatisk bli endret til 6 alfanumeriske symboler

AntiVirus

Hvis du aktiverer AntiVirus, installeres Ikarus på enhetene. Vær oppmerksom på at dette krever en separat lisens som kan angis i Generelle innstillinger → Appadministrasjon → Tredjepartsapper.

Automatisk skanning	Definerer om Ikarus skal skanne automatisk eller ikke, og hvor ofte skanningen skal utføres Hvis du aktiverer "Full automatisk skanning", utføres en fullstendig skanning. Ellers vil en hurtigskanning bli utført
Automatiske oppdateringer	Aktiverer automatisk oppdatering av virusdatabasen og angir hvor ofte dette skal skje
App-beskyttelse	Aktiverer skanning av apper i tillegg til den vanlige skanningen som bare skanner filer
Beskyttelse av SD-kort	Aktiverer SD-kortbeskyttelse. Uten denne funksjonen er skanningen begrenset til det lokale lagringsområdet
Kun Wi-Fi-oppdatering	Begrenser oppdatering til Wi-Fi

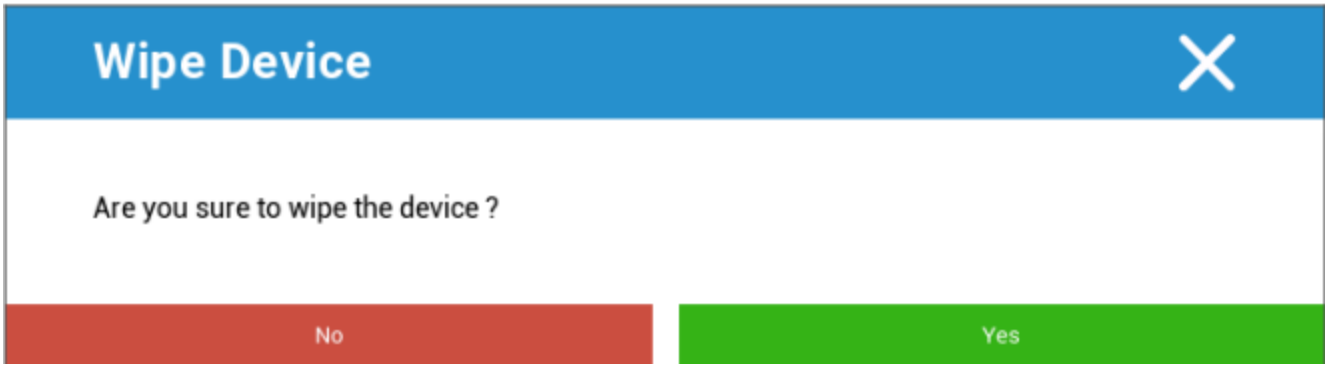
End of Life (kun på enhetsnivå)

Tørk (kun på enhetsnivå)

Under "Wipe" kan du gjenopprette enheten til fabrikkinnstillingene. Her slettes bedriftsdataene og de private dataene på sluttbrukerens enhet.

Når du klikker på "Minus-symbolet", bør du få følgende melding

Slette SD-kortet også?	SD-kortets minne vil også bli slettet



Med "Yes" kan du utføre tørkingen.

Under "Wipe Report" kan følgende elementer vises

Tørket av	Historikk over hvem som utførte tørkingen
Dato	Dato
Status	Status (f.eks. om tørkingen ble vellykket)

Begrensningsinnstillinger

Begrensninger

Her kan en rekke ting begrenses og blokkeres.

Aktiver kamera	Tillat bruk av kamera
Tving automatisk synkronisering	Relatert til "Synkroniser"-grensesnittet På = synkronisering er permanent aktivert Av = synkronisering er permanent deaktivert Brukervalg = valgt av brukeren
Force Bluetooth	På = Bluetooth er permanent aktivert Av = Bluetooth er permanent deaktivert Brukervalg = valgt av brukeren
Force GPS	På = GPS er permanent aktivert Av = GPS er permanent deaktivert Brukervalg = valgt av brukeren
Tving frem Googles posisjonsnøyaktighet	På = Permanent internettlokalisering Av = Permanent deaktivering av internettlokalisering Brukervalg = valgt av brukeren

For Samsung-enheter med KNOX 1.0-grensesnitt eller høyere er følgende innstillingsalternativer tilgjengelige.

Tillat SD-kort	Tillat SD-kort
Tillat skriving på SD-kort	Tillat "skriving" på SD-kortet
Tillat skjermopptak	Tillat skjermopptak
Tillat utklippstavle	Tillat utklippstavle
Sikkerhetskopier innstillinger og appdata i Google Cloud	Av = deaktiver Google Backup On = aktiver Google Backup Brukervalg = valgt av brukeren
Tillat USB-feilsøking	Tillat USB-feilsøking (brukes for eksempel til å opprette enhetslogger (ADB))
Tillat Google Crash Report	Tillat at Google Crash Report sendes fra appene
Tillat tilbakestilling til fabrikkinnstilling	Gjør det mulig for brukeren å gjenopprette enheten til fabrikkinnstillingene
Tillat OTA-oppgradering	Tillat oppdateringer "over luften"
Tillat USB-vertslagring	Hvis aktivert, kan USB-minne, i form av en HD eller en SD-kortleser, kobles til
Tillat USB Media Player (MTP, PTP)	Tillat USB Media Player (MTP,PTP)
Tillat mikrofon	På = Tillat mikrofon for tredjepartsapper Av = blokkerer mikrofonen for tredjepartsapper Brukervalg = brukerne kan velge, hvis tredjepartsappen har tilgang til mikrofonen
Tillat NFC (Near Field Communication)	Tillat NFC
Tillat ukjente kilder (APK Sideloading)	Hvis dette er aktivert, er sidelasting av apper (APK-filer) tillatt. Når denne innstillingen er deaktivert, må brukeren aktivere den manuelt når du tillater installasjon av APK-er fra ukjente kilder på nytt.
Tillat brukeroppretting	Tillater opprettelse av flere brukere

AE Enhetseier

(Enheten må være i Android Enterprise Device Owner Mode) Det anbefales å opprette enhetene som "Android Enterprise"-enhet og ikke som "Android"-enhet.

Sikkerhet	
Ikke tillat delingsplassering	Angir om en bruker ikke kan slå på stedsdeling.
Ikke tillat sikker oppstart	Angir om brukeren ikke har lov til å starte enheten på nytt i sikker oppstartsmodus.
Tillat ikke tilbakestilling av nettverk	Angir om en bruker ikke kan tilbakestille nettverksinnstillinger fra Innstillinger.
Tillat ikke tilbakestilling til fabrikkinnstilling	Angir om en bruker ikke har lov til å tilbakestille enheten.
Aktiver ADB	Gjør det mulig å koble til en PC via ADB
Deaktiver Keyguard	Deaktiverer Keyguard
Info om enhetsinnehaverens låseskjerm	Angir hvilken informasjon om enhetens eier som skal vises på låseskjermen.
Håndhevelse av samsvar	Mode Prompt User - Brukeren blir bedt om å utføre de nødvendige handlingene. Mode Lock-Down Container - Skjul alle apper til alle krav er oppfylt

App-administrasjon	
Tillat kobling av apper på tvers av profiler	Tillater at apper i den overordnede profilen kan håndtere nettlenker fra den administrerte profilen.
Ikke tillat appkontroll	Angir om en bruker ikke kan endre programmer i Innstillinger eller startprogrammer.
Ikke tillat appinstallasjon	Angir om en bruker ikke har tillatelse til å installere programmer.
Ikke tillat avinstallering av apper	Angir om en bruker ikke har lov til å avinstallere programmer.
Retningslinjer for kjøretidstillatelser	Angir hvordan nye tillatelsesforespørsler fra apper skal håndteres.
Tillat ukjente kilder	Hvis denne funksjonen er aktivert, kan brukerne laste ned apper ved å installere en .apk-fil.

Tilkoblingsmuligheter	
Ikke tillat mobilnettverkskonfigurasjon	Angir om en bruker ikke har lov til å konfigurere mobilnettverk.
Ikke tillat tethering-konfigurasjon	Angir om en bruker ikke har lov til å konfigurere nettdeling og bærbare hotspots.
Ikke tillat VPN-konfigurasjon	Angir om en bruker ikke skal tillates å konfigurere et VPN.
Ikke tillat Wifi-konfigurasjon	Angir om en bruker ikke har lov til å endre WiFi-tilgangspunkt.
Ikke tillat utgående NFC-stråle	Angir om brukeren ikke har lov til å bruke NFC til å sende ut data fra apper.
Lås WiFi-konfigurasjon	Denne innstillingen kontrollerer om WiFi-konfigurasjoner som opprettes av en enhetseier-app, skal være låst (det vil si at de bare skal kunne redigeres eller fjernes av enhetseier-appen, ikke engang av Innstillinger-appen).
Aktivere dataroaming	Aktiverer dataroaming

Bluetooth	
Ikke tillat Bluetooth	Angir om Bluetooth ikke er tillatt på enheten. Krever Android 8.0
Ikke tillat Bluetooth-deling	Angir om utgående Bluetooth-deling ikke er tillatt på enheten. Krever Android 8.0
Ikke tillat Bluetooth-konfigurasjon	Angir om en bruker ikke har lov til å konfigurere Bluetooth.

Kontoadministrasjon	
Ikke tillat å legge til administrert profil	Angir om en bruker ikke kan legge til administrerte profiler. Krever Android 8.0
Ikke tillat å legge til brukere	Angir om en bruker ikke kan legge til nye brukere.
Ikke tillat Fjern administrert profil	Angir om administrerte profiler for denne brukeren kan fjernes av andre enn profileieren. Krever Android 8.0
Ikke tillat endring av konto	Angir om en bruker ikke kan legge til og fjerne kontoer, med mindre de er lagt til programmatisk av Authenticator.

Telefoni	
Forby utgående anrop	Angir at brukeren ikke har lov til å foreta utgående telefonsamtaler.
Ikke tillat SMS	Angir at brukeren ikke har lov til å sende eller motta SMS-meldinger.

System	
Ikke tillat oppretting av vindu	Angir at det ikke skal opprettes andre vinduer enn appvinduer.
Ikke tillat å angi brukerikon	Angir om en bruker ikke har lov til å endre ikonet sitt.
Ikke tillat Set Wallpaper	Brukerbegrensning for å ikke tillate innstilling av bakgrunnsbilde.
Deaktiver statuslinjen	Deaktivering av statuslinjen blokkerer varsler, hurtiginnstillinger og andre skjermoverlegg som gjør det mulig å flykte fra en enhet som bare brukes én gang.
Aktiver automatisk tid	Stiller inn klokkeslettet automatisk.
Aktiver automatisk tidssone	Stiller inn tidssonen automatisk.
Holdes på mens du er koblet til	Enheten forblir aktiv mens den er koblet til en strømkilde.

Lagring	
Ikke tillat deaktivering av appverifisering	Angir om en bruker ikke har lov til å deaktivere programverifisering.

Ikke tillat montering av fysiske medier	Angir om en bruker ikke har lov til å montere fysiske eksterne medier.
Aktiver sikkerhetskopieringstjeneste	Backup-tjenesten administrerer alle mekanismer for sikkerhetskopiering og gjenoppretting på enheten. Hvis du setter denne til false, forhindres data fra å bli sikkerhetskopiert eller gjenopprettet. Sikkerhetskopieringstjenesten er av som standard. Krever Android 8.0
Aktiver USB-masselagring	Aktiverer bruk av USB-masselagring.

Tastatur	
Ikke tillat autofyll	Angir om en bruker ikke har lov til å bruke Autofyll-tjenester. Krever Android 8.0
Ikke tillat kopiering og liming mellom profiler	Angir om det som kopieres til utklippstavlen i denne profilen, kan limes inn i relaterte profiler.

Lyd	
Ikke tillat volumjustering	Angir om en bruker ikke kan justere hovedvolumet.
Ikke tillat Slå av mikrofonen	Angir om en bruker ikke kan justere mikrofonvolumet.
Mute-enhet	Mute-enhet.

Retningslinjer for systemoppdatering	
Kontroller OS-oppdateringer	Aktiver denne for å angi at oppdateringen skal skje automatisk, i et vindu eller utsatt.

BYOD-container

Android Enterprise

Android Enterprise

Aktiver Android Enterprise	Aktiver Android Enterprise (AE). AE støttes fra og med Android 5.1 og nyere.
Håndhevelse av samsvar	Mode Prompt User - Brukeren blir bedt om å utføre de nødvendige handlingene. Mode Lock-Down Container - Skjul alle apper til alle krav er oppfylt
Retningslinjer for kjøretidstillatelser	Spør brukeren om nye forespørsler om tillatelse Alltid innvilge nye forespørsler om nye tillatelser Alltid avslå nye forespørsler om tillatelse Advarsel: Noen apper har problemer med å gjenkjenne tillatelsene hvis disse er angitt automatisk. Hvis du alltid gir tillatelser og støter på problemer med apper som sier at tillatelser mangler, kan du sette dette til "spør brukeren" og installere appen på nytt.
Tillat utgående utklippstavle	Tillater kopiering og liming fra innsiden av beholderen til utsiden
Tillat oppløsning av anroper-ID	Viser navnet på en innkommende samtale basert på kontaktene i containeren
Tillat oppløsning av kontaktsøk	Gjør det mulig å søke etter navn i containerens kontakter når du ringer
Tillat deling av Bluetooth-kontakter	Gir tilgang til beholderkontakt i en bil
Ikke tillat utgående NFC-stråle	Deaktiverer NFC for beholderen
Tillat ukjente kilder	Hvis denne funksjonen er aktivert, kan brukerne laste ned apper ved å installere en .apk-fil.
Tillat USB-feilsøking	Hvis den er aktivert, kan brukerne aktivere USB-feilsøking.
Ikke tillat endring av konto	Tillater ikke oppretting, sletting og endring av kontoer i beholderen Vær oppmerksom på at noen apper må opprette eller endre kontoer for å fungere som forventet

Gmail Exchange

Lar deg konfigurere Gmail i containeren. Vær oppmerksom på at aktivering av denne konfigurasjonen ikke automatisk installerer appen. Du må fortsatt legge til denne appen som obligatorisk app.

E-postadresse	E-postadresse
Serverens vertsnavn	Serverens vertsnavn
Innloggingsnavn	Innloggingsnavn
Signatur	Signatur
Antall foregående dager som skal synkroniseres	Antall foregående dager som skal synkroniseres.
Enhetsidentifikator	EAS-identifikator. Hold denne tom hvis miljøet ditt ikke krever dette
Bruk Secure Sockets Layer (SSL)	Aktiverer bruk av SSL. Deaktivering av dette kan redusere sikkerheten
Godta alle sertifikater	Godtar alle sertifikater. Aktivering av dette kan redusere sikkerheten
Tillat ikke-administrerte kontoer	Gjør det mulig for brukeren å legge til flere kontoer
Kundesertifikat	Last opp klientsertifikat hvis Exchange-serveren din krever dette

AE System-apper

Her kan du aktivere systemapper for Android Enterprise Container. Vær oppmerksom på at den angitte appen må finnes i systemlageret, ellers skjer det ingenting.

Containerpassord

Bare for Android 7.0 eller nyere

Gjør det mulig å angi et spesifikt passordkrav for beholderen.

Minimum passordlengde	Fastsetter det minste antallet symboler et passord må inneholde
Passordkvalitet	Passordstyrke Uspesifisert = ikke spesifisert Alle passord er ok = alle passord er akseptable minst numeriske tegn = må inneholde minst numeriske tegn minst komplekse tegn = må inneholde minst spesialtegn minst alfanumeriske tegn = må inneholde minst alfanumeriske tegn minst alfabetiske tegn = må inneholde minst alfabetiske tegn
Lås for maksimal inaktivitetstid	Maksimal tid til beholderen blir låst. Dette konfigurerer bare den maksimale verdien som kan velges av brukeren
Minimum små bokstaver kreves i passordet	Minimum små bokstaver kreves i passordet
Minimum store bokstaver kreves i passordet	Minimum store bokstaver kreves i passordet
Minimum antall tegn som ikke er bokstaver som kreves i passordet	Minimum antall tegn som ikke er bokstaver som kreves i passordet
Minimum antall siffer som kreves i passordet	Minimum antall siffer som kreves i passordet
Minimum symboler som kreves i passordet	Minimum symboler som kreves i passordet
Tidsavbrudd for utløp av passord	Etableres, etter hvilket tidsintervall passordet utløper og et nytt passord må utstedes
Begrensning av passordhistorikk	Antall tidligere brukte passord som ikke er tillatt
Maksimalt antall mislykkede passordforsøk	Fastsetter hvor ofte et passord kan tastes inn feil før containeren slettes

Samsung KNOX

Aktivering

Her kan du aktivere Samsung KNOX Container. Vær oppmerksom på at denne ikke lenger støttes av Samsung på Android 10 eller nyere. Bruk Android Enterprise Container på Android 10 eller nyere

Knox Passcode

Fastsett retningslinjene som gjelder innstillingene for enhetens passord

Minimum passordlengde	Fastsetter hvor mange symboler passordet må ha
Passordkvalitet	Passordstyrke Alle passord er ok = Alle passord er ok Minst numeriske tegn = Minst numeriske tegn må være til stede Minst komplekse tegn = Minimum spesialtegn må være til stede Minst alfanumeriske tegn = Minst alfanumeriske tegn må være til stede Minst alfabetiske tegn = Minst alfabetiske tegn må være til stede
Minimum komplekse tegn kreves	Minimum komplekse tegn må være til stede
Maksimal tidsavbrudd for inaktivitet	Maksimal tidsavbrudd for inaktivitet før tastaturlåsing
Tillat fingeravtrykksautentisering	Tillat autentisering med fingeravtrykk
Tillat irisautentisering	Tillat autentisering med irisgjenkjenning
Maks alder på passord	Fastsetter etter hvilken tid passordet utløper og et nytt passord må utstedes
Lagret passordhistorikk	Antall tidligere passord som ikke er tillatt
Maksimalt antall mislykkede passordforsøk	Fastsetter hvor ofte passordet kan sendes inn feil før en fullstendig sletting av enheten vil finne sted

Knox Security

Begrens spesifikke enhetsfunksjoner

Aktiver kamera	Tillat bruk av kameraet
Tillat Samsung KNOX App Store	Tillat bruk av Samsung KNOX App Store
Tillat Google Play-tjenester	Tillat Google Play-tjenester
Tillat nettleser	Tillat bruk av den opprinnelige nettleseren
Tillat skjermbilder	Tillat oppretting av skjermbilder
Tillat import av kontakter	Hvis den er aktivert, er det mulig å få tilgang til enhetskontakter fra KNOX Container

Tillat eksport av kontakter	Hvis den er aktivert, er det mulig å få tilgang til KNOX-kontaktene fra enheten
Tillat kalenderimport	Hvis den er aktivert, er det mulig å få tilgang til enhetskalenderen fra KNOX Container
Tillat kalendereksport	Hvis den er aktivert, er det mulig å få tilgang til KNOX-kalenderen fra enheten
Tillat ikke-sikkert tastatur	Tillat bruk av et ikke-sikkert tastatur
Aktiver filimport	Aktiver filimport til KNOX-containeren
Aktiver fileksport	Aktiver fileksport fra KNOX-containeren

Knox Exchange

Her kan du konfigurere Exchange-profilen for KNOX-containeren

E-postadresse	Den oppgitte e-postadressen til brukeren Vær oppmerksom på "plassholderne", som du kan bruke til å arbeide med legitimasjon og ikke utføre endringer manuelt på alle enheter Med et klikk på **Vis plassholdere** kan du vise dem for deg selv
Serverens vertsnavn	Serveradressen til Exchange-serverne dine
Innloggingsnavn	Innloggingsnavnet for den respektive sluttbrukerenheten, vær også oppmerksom på "plassholderne" her
Domene	Domeneadresse
Passord (kun på enhetsnivå)	Eventuelt kan en individuell enhet gis et passord, og hvis dette forblir tomt, vil brukeren bli bedt om å oppgi Exchange-passordet sitt.
Antall foregående dager som skal synkroniseres	Antall dager som avgjør når e-poster synkroniseres tilbake
Signatur	En signatur kan legges ved
Standard konto	Fastsetter at denne e-postkontoen er standardkontoen
Bruk Secure Sockets Layer (SSL)	Bruk en SSL-tilkobling
Bruk Transport Layer Security (TLS)	Bruk en TLS-tilkobling
Godta alle sertifikater	Alle sertifikater godtas. Velg dette alternativet hvis Exchange-serveren bruker et selvsignert sertifikat

Knox e-post

E-postadresse	Den oppgitte e-postadressen til brukeren Vær oppmerksom på "plassholderne", som du kan bruke til å arbeide med legitimasjon og ikke utføre endringer manuelt på alle enheter Med et klikk på **Vis plassholdere** kan du vise dem for deg selv
Protokoll for innkommende server	Protokoll for innkommende server IMAP eller POP
Innkommende serveradresse	Innkommende serveradresse
Innkommende serverport	Innkommende serverport
Pålogging/brukernavn for innkommende server	Pålogging/brukernavn for innkommende server
Passord for innkommende server	Passord for innkommende server
Innkommende server bruker SSL	Innkommende server bruker SSL
Innkommende server bruker TLS	Innkommende server bruker TLS
Innkommende server godtar alle sertifikater	Innkommende server godtar alle typer sertifikater
Protokoll for utgående server	Protokoll for utgående server SMTP
Utgående serverport	Utgående serverport
Utgående server bruker ekstra legitimasjon	Ytterligere legitimasjon for den utgående serveren. Hvis denne er satt til "av", brukes innstillingene for innkommende server
Pålogging/brukernavn for utgående server	Pålogging/brukernavn for utgående server
Passord for utgående server	Passord for utgående server
Utgående server bruker SSL	Utgående server bruker SSL
Utgående server bruker TLS	Utgående server bruker TLS
Utgående server godtar alle sertifikater	Utgående server godtar alle typer sertifikater
Signatur	Her kan en signatur legges ved

Varsle brukeren om mottak av ny e-post	Varsle brukeren om mottak av ny e-post

Knox-apper

Her kan du opprette apper som du ønsker å distribuere til sluttbrukernes enheter. Disse vil da være tilgjengelige i KNOX-Containeren. For å legge til en app, gjør du som i menyen Obligatoriske apper

Navn på applikasjon	Navn på applikasjon
Obligatorisk siden	Tidspunkt for når appen ble lagt til
Kilde	Appens kilde (Play Store | Internt)

Ved å klikke på symbolet kan den aktuelle appen fjernes igjen

Administrasjon av tilkoblinger

Wifi

For denne innstillingen må du utføre forhåndskonfigurasjonen av sluttbrukerens enheter for tilgang til interne aksesspunkter

Services Set Identifier (SSID)	SSID for nettverket som skal kobles til
Skjult nettverk	Aktiver, i tilfelle AP-et ikke kringkaster SSID
Sikkerhetstype	Fastsette AP-ets sikkerhetstype

Sikkerhetstype

WEP

Passord	Passord for AP

WPA/WPA2

Passord	Passord for AP

802.1x EAP

EAP-metode	

PWD	Identitet	Identitet
	Passord	Passord

PEAP	Fase 2 autentiseringsprotokoll	ingen	Ingen tilleggsprotokoll
		MSCHAPV2	MSCHAPV2-protokollen
		GTC	GTC-protokoll
	CA-sertifikat	CA-sertifikat	
	Identitet	Identitet	
	Anonym identitet	Anonym identitet	
	Passord	Passord	

EAP-metode	

TTLS	Fase 2 autentiseringsprotokoll	ingen	Ingen tilleggsprotokoll
		PAP	PAP-protokoll
		MSCHAP	MSCHAP-protokollen
		MSCHAPV2	MSCHAPV2-protokollen
		GTC	GTC-protokoll
	CA-sertifikat	CA-sertifikat	
	Identitet	Identitet	
	Anonym identitet	Anonym identitet	
	Passord	Passord	

TLS	CA-sertifikat	CA-sertifikat
	Identitet	Identitet
	Passord	Passord

VPN

Type tilkobling	**Etablere VPN-tilkoblingstype**

Hvis du velger "Per-App VPN" som VPN-type, vil de tilgjengelige VPN-klientene endres. Per-App VPN begrenser VPN til bestemte apper og starter VPN-tilkoblingen automatisk hvis en bestemt app startes.

AppTec360 VPN-klient	Bruker AppTec360 VPN Client i kombinasjon med Universal Gateway
Navn på tilkobling	Navn på VPN-tilkobling
Gateway-konfigurasjon	Velg VPN-konfigurasjonen til Universal Gateway
Alltid på VPN	Tvinger VPN til alltid å være aktivt, slik at all trafikk går gjennom VPN.
Aktiver Native Lockdown	Blokkerer all nettverkstilkobling når enheten ikke er koblet til VPN-et. Bruk dette med forsiktighet, siden det kan føre til at hele tilkoblingen går tapt hvis det ikke er riktig konfigurert. Kun for Android Enterprise på Android 7 eller nyere
Aktiver AppTec360 Lockdown	Blokkerer bruken av alle apper inntil VPN-tilkoblingen er startet

Cisco AnyConnect	
Navn på tilkobling	Navn på VPN-tilkobling
Server	Serveradresse
Sertifikatmodus	Deaktivert = deaktivert Automatisk = automatisk

L2TP (kun KNOX)	Kun tilgjengelig på Samsung-enheter
Navn på tilkobling	Navn på tilkobling
Server	Serveradresse
Aktiver L2TP-hemmelighet	
DNS-søkedomener	DNS-søkedomener

Type tilkobling	**Etablere VPN-tilkoblingstype**

PPTP (kun KNOX)	Kun tilgjengelig på Samsung-enheter
Navn på tilkobling	Navn på VPN-tilkobling
Server	Serveradresse
Aktiver kryptering	Aktiver kryptering
DNS-søkedomener	DNS-søkedomener

L2TP/IPSec PSK (kun KNOX)	Kun tilgjengelig på Samsung-enheter
Navn på tilkobling	Navn på VPN-tilkobling
Server	Serveradresse
IPSec forhåndsdelt nøkkel	Forhåndsdelt nøkkel for autentisering
Aktiver L2TP-hemmelighet	
L2TP-hemmelighet	
DNS-søkedomener	DNS-søkedomener

IPSec XAuth PSK (kun KNOX)	Kun tilgjengelig på Samsung-enheter
Navn på tilkobling	Navn på VPN-tilkobling
Server	Serveradresse
IPSec-identifikator	Brukernavn for tilkoblingen
IPSec forhåndsdelt nøkkel	Passord for tilkoblingen
DNS-søkedomener	DNS-søkedomener

OpenVPN	

Navn på tilkobling	Navn på tilkobling
OpenVPN-profil	Her kopieres innholdet i .ovpn-filen
OpenVPN-app	Det finnes to forskjellige apper for bruk av OpenVPN Vi anbefaler appen "OpenVPN for Android". Men alternativt kan appen "OpenVPN Connect" brukes

Begrensninger

Her kan du angi begrensninger i forbindelse med tilkoblingshåndteringen.

Tillat dataroaming	Tillat mobildata under roaming
Tving frem dataroaming	Hvis den er aktivert, er roaming for mobildata permanent aktivert (anbefales ikke!) Denne innstillingen overskriver innstillingen "Tillat dataroaming"!
Følgende innstillinger er kun tilgjengelige på Samsung KNOX 2.0 eller nyere	
Tillat bare nødanrop	Tillat bare nødanrop
Tillat WiFi	Tillat WiFi
Minimum sikkerhetsnivå for WiFi-nettverk	Minimum sikkerhetsnivå for WiFi-nettverk Åpen = alle typer WiFi er tillatt
Forby brukeren å legge til WiFi-nettverk	Brukeren kan ikke selv legge til et WiFi-nettverk Denne innstillingen er bare mulig hvis en WiFi-profil er definert under "Connection Management".
Tillat SMS og MMS	All = All SMS- og MMS-trafikk er tillatt Kun innkommende SMS = Kun innkommende SMS-meldinger er tillatt Outgoing SMS Only = Kun utgående SMS-meldinger er tillatt Ingen = Ingen SMS/MMS-trafikk er tillatt
Tillat synkronisering under roaming	Tillat synkronisering under roaming På = aktivert Av = deaktivert Brukervalg = brukerens valg
Tillat roaming av tale	Tillat roaming av tale På = aktivert Av = deaktivert User Choice = brukerens valg
Bruk System http Proxy Server	Bruken av en HTTP-proxy-server, som er gitt av systemets innstillinger i innstillinger, er avhengig av det tilkoblede nettverket (WiFi eller APN)

APN

Følgende innstillinger er bare tilgjengelige på Samsung SAFE 2.0 eller nyere!

APN Visningsnavn	APN Visningsnavn	
Navn på tilgangspunkt	APNs navn	
Protokoll for utgående server	Ikke angitt	
	Ingen	
	PAP	PAP-protokoll
	CHAP	CHAP-protokollen
	PAP eller CHAP	Enten PAP- eller CHAP-protokollen
MCC - Mobil landskode	MCC angis her, la dette feltet stå tomt hvis MCC-en til det innsatte SIM-kortet skal brukes	
MNC - Mobilnettverkskode	MNC angis her, la dette feltet stå tomt hvis MCC-en til det innsatte SIM-kortet skal brukes	
Serveradresse	Serveradresse	
Serverens portnummer	Serverens portnummer	
Serverens proxy-adresse	Serverens proxy-adresse	
Adresse til MMS-server	MMS-serveradresse, for Standard, vennligst la den stå tom	
MMS-portnummer	MMS-portnummer	
MMS-proxy-adresse	MMS-proxy-adresse	
Brukernavn	Brukernavn	
Passord	Passord	
Type tilgangspunkt	Tillatte typer er: "standard", "mms", "supl" Hvis dette feltet ikke fylles ut, vil "default,supl,mms" bli brukt	
Foretrukket APN	APN er å foretrekke	

Bluetooth

Her kan du utføre en rekke Bluetooth-innstillinger.

Følgende innstillinger er kun tilgjengelige på Samsung KNOX 1.0 eller nyere!

Tillat enhetsoppdagelse via Bluetooth	Tillat enhetsoppdagelse via Bluetooth
Tillat Bluetooth-paring	Tillat sammenkobling via Bluetooth
Tillat Bluetooth-headset-enheter	Tillat Bluetooth-headset-enheter
Tillat håndfrie Bluetooth-enheter	Tillat håndfrie Bluetooth-enheter
Tillat Bluetooth A2DP-enheter	Tillat Bluetooth A2DP lydstrømming mellom enheter
Tillat utgående anrop	Tillat utgående anrop viaBT
Tillat dataoverføring via Bluetooth	Tillat dataoverføring via Bluetooth
Tillat Bluetooth-tilknytning	Gjør det mulig å bruke enheten som et modem (Bluetooth-internettforbindelse)
Tillat tilkobling til datamaskin via Bluetooth	Tillat tilkobling til datamaskin via Bluetooth

PIM-administrasjon

Utveksling

Kun tilgjengelig for Samsung KNOX 1.0 eller nyere!

E-postadresse	Den oppgitte e-postadressen til brukeren Vær oppmerksom på "plassholderne", som du kan bruke til å arbeide med legitimasjon og ikke utføre endringer manuelt på alle enheter Med et klikk på **Vis plassholdere** kan du vise dem for deg selv
Serverens vertsnavn	Serveradressen til Exchange-serverne dine
Innloggingsnavn	Innloggingsnavnet for den respektive sluttbrukerenheten, legg også merke til "Placeholders here".
Domene	Domeneadresse
Passord (kun på enhetsnivå)	Eventuelt kan en individuell enhet gis et passord, og hvis dette er tomt, vil brukeren bli bedt om å oppgi Exchange-passordet sitt.
Antall foregående dager som skal synkroniseres	Antall dager som avgjør når e-poster synkroniseres tilbake
Signatur	En signatur kan legges ved (Tips: Noen enheter krever HTML-formatering for signaturen)
Standard konto	Fastsetter at denne e-postkontoen er standardkontoen
Bruk Secure Sockets Layer (SSL)	Bruk en SSL-tilkobling
Bruk Transport Layer Security (TLS)	Bruk en TLS-tilkobling
Godta alle sertifikater	Alle sertifikater godtas. Velg dette alternativet hvis Exchange-serveren bruker et selvsignert sertifikat

E-post

Her kan du distribuere IMAP- og POP-kontoer til de respektive sluttbrukernes enheter.

Følgende innstillinger er kun tilgjengelige på Samsung KNOX 1.0 eller nyere!		
E-postadresse	Den oppgitte e-postadressen til brukeren Vær oppmerksom på "plassholderne", som du kan bruke til å arbeide med legitimasjon og ikke utføre endringer manuelt på alle enheter Med et klikk på **Vis plassholdere** kan du vise dem for deg selv	
Protokoll for innkommende server	Protokoll for innkommende server	IMAP eller POP
Innkommende serveradresse	Innkommende serveradresse	
Innkommende serverport	Innkommende serverport	
Pålogging/brukernavn for innkommende server	Pålogging/brukernavn for innkommende server	
Passord for innkommende server (kun på enhetsnivå)	Passord for innkommende server (kun på enhetsnivå)	
Innkommende server bruker SSL	Innkommende server bruker SSL	
Innkommende server bruker TLS	Innkommende server bruker TLS	
Innkommende server godtar alle sertifikater	Innkommende server godtar alle typer sertifikater	
Protokoll for utgående server	Protokoll for utgående server	SMTP
Utgående serverport	Utgående serverport	
Utgående server bruker ekstra legitimasjon	Ytterligere legitimasjon for den utgående serveren. Hvis denne er satt til "av", brukes innstillingene for innkommende server	
Pålogging/brukernavn for utgående server	Pålogging/brukernavn for utgående server	
Passord for utgående server (kun på enhetsnivå)	Passord for utgående server	
Utgående server bruker SSL	Utgående server bruker SSL	
Utgående server bruker TLS	Utgående server bruker TLS	
Utgående server godtar alle sertifikater	Utgående server godtar alle typer sertifikater	

Signatur	En signatur kan legges ved her (Tips: Noen enheter krever HTML-formatering for signaturen)
Varsle brukeren om mottak av ny e-post	Varsler brukeren om mottak av ny e-post

AE Gmail Exchange

Info: Denne konfigurasjonen vil bli brukt på Gmail-appen. Du må derfor godkjenne og installere Gmail.

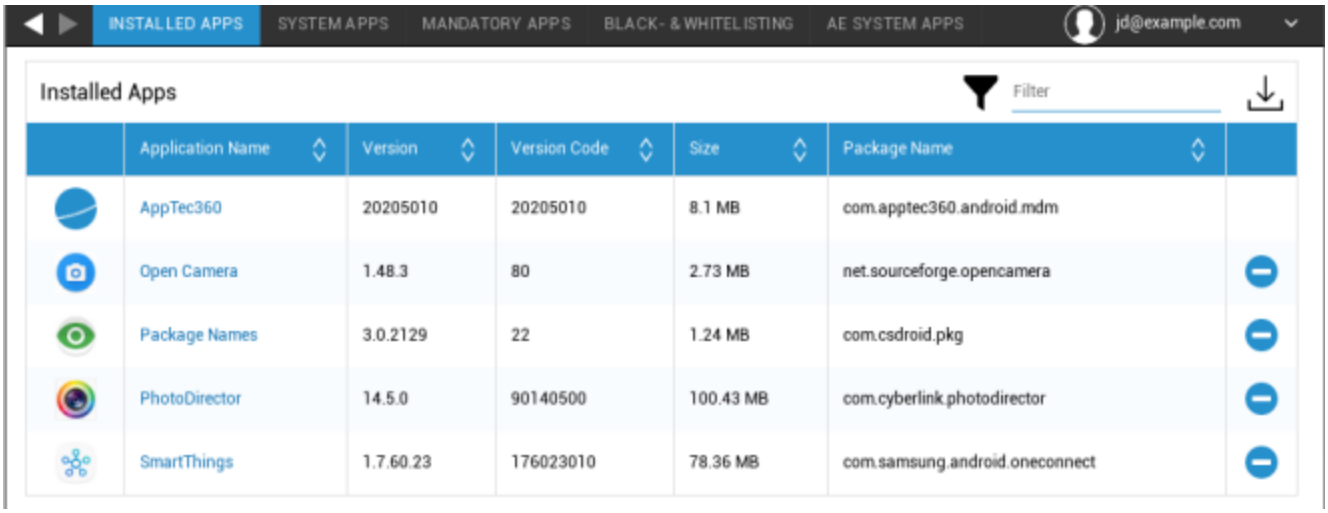
E-postadresse	Den oppgitte e-postadressen til brukeren Vær oppmerksom på "plassholderne", som du kan bruke til å arbeide med legitimasjon og ikke utføre endringer manuelt på alle enheter Med et klikk på Vis plassholdere kan du vise dem for deg selv
Serverens vertsnavn	Serveradressen til Exchange-serverne dine
Innloggingsnavn	Innloggingsnavnet for den respektive sluttbrukerenheten, legg også merke til "Placeholders here".
Signatur	En signatur kan legges ved (Tips: Noen enheter krever HTML-formatering for signaturen)
Antall foregående dager som skal synkroniseres	Antall dager som avgjør når e-poster synkroniseres tilbake
Enhetsidentifikator	EAS-identifikator. Hold denne tom hvis miljøet ditt ikke krever dette
Bruk Secure Sockets Layer (SSL)	Bruk en SSL-tilkobling
Godta alle sertifikater	Alle sertifikater godtas. Velg dette alternativet hvis Exchange-serveren bruker et selvsignert sertifikat
Tillat ikke-administrerte kontoer	Gjør det mulig for brukeren å legge til flere kontoer
Kundesertifikat	Last opp klientsertifikat hvis Exchange-serveren din krever dette

App-administrasjon

Enterprise App Manager

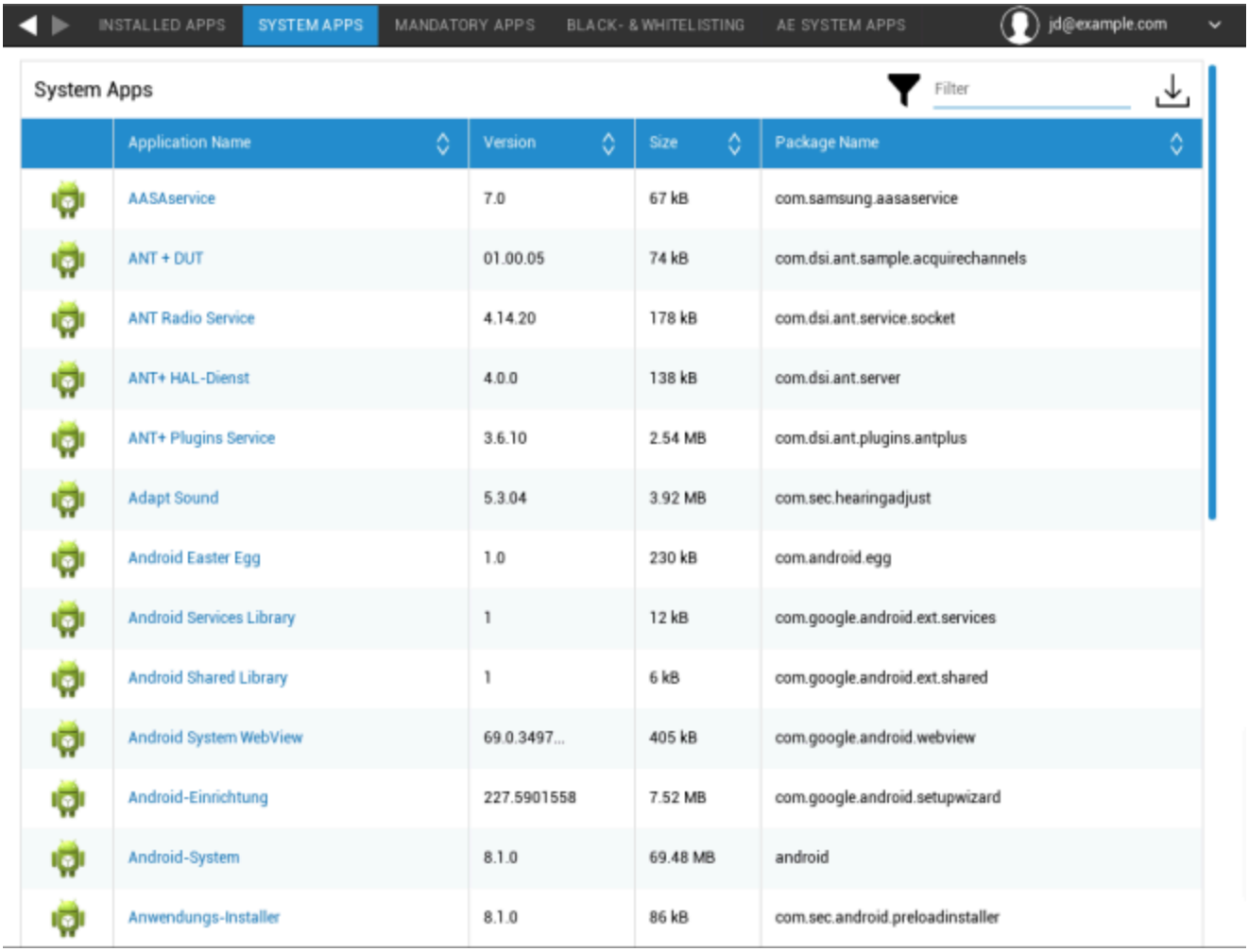
Installerte apper (kun på enhetsnivå)

Her vises alle apper som for øyeblikket er installert på sluttbrukerens enhet.


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

Systemapper (kun på enhetsnivå)

Under "System Apps" vil alle de forhåndsinstallerte systemene bli listet opp med pakkenavn og versjon.



Obligatoriske apper

I Obligatoriske apper kan du definere hvilke apper som må installeres på enheten. Avhengig av konfigurasjon og enhet vil appen installeres automatisk, eller brukeren vil bli bedt om å installere den.

Vær oppmerksom på at det anbefales å bruke Android Enterprise for enkel appadministrasjon.

Scenariene er listet opp nedenfor:

Vanlige Play Store-apper

Installasjoner av Playstore-apper krever alltid en brukerinteraksjon. I tillegg må en Google-konto konfigureres på enheten.

Installasjon av egen app

På Samsung-enheter installeres disse appene lydløst. Det eneste unntaket er containeren, der brukeren må bekrefte installasjonen.

I alle andre tilfeller må brukeren bekrefte installasjonen av appen.

Android Enterprise Play Store-apper

Disse appene installeres alltid i det stille, uten at brukeren trenger å gjøre noe.

For å legge til en obligatorisk app klikker du på "+" og velger ønsket app fra listen. Vær oppmerksom på at du ikke kan installere apper fra "Google Play Store"-fanen hvis enheten er konfigurert med Android Enterprise, enten som fullstendig administrert eller som container.

Hvis du bruker Android Enterprise, velger du appene fra "AE Play Store"-delen. For å gjøre apper tilgjengelige her må du bekrefte dem i Google Enterprise Play-butikken ved å gå til Generelle innstillinger → AE Play Store → Play Store-apper.

Når du fjerner en obligatorisk app, blir den også avinstallert fra enheten.

Du kan klikke på navnet på en app i den obligatoriske applisten og gå til "konfigurasjon"-fanen for å konfigurere en app. Dette krever bruk av Android Enterprise, og appen må støtte dette. Derfor avhenger de tilgjengelige alternativene av den valgte appen.

AE System-apper

Her kan du aktivere systemapper for Android Enterprise-enheter. Vær oppmerksom på at den angitte appen må finnes i systemets lagringsplass, ellers skjer det ingenting. 296

Begrensninger og innstillinger

Svart- og hvitelisting

Her kan du definere en svart- eller hviteliste. Alle apper på svartelisten vil bli blokkert. Alle apper som ikke er på hvitelisten, vil bli blokkert. En tom svarteliste blokkerer ingenting, mens en tom hviteliste blokkerer alt*.

**Alle obligatoriske apper og apper fra Enterprise App Store blir automatisk hvitelistet. Du trenger ikke å legge dem til manuelt.*

Når du klikker på "+", kan du enten søke etter en app du vil legge til i svart- eller hvitelisten, eller du kan skrive inn et pakkenavn manuelt.

Sys App Restriksjoner

Under "Sys App Restrictions" kan du blant annet blokkere forhåndsinstallerte apper og tjenester etter eget ønske.

Deaktiver nettleser	Deaktiver standard nettleser
Deaktiver kalender	Deaktiver innebygd kalender
Deaktiver kalkulator	Deaktiver kalkulator
Deaktiver Chrome-nettleseren	Deaktiver Chrome-nettleseren
Deaktiver klokke	Deaktiver klokken
Deaktiver kontakter	Deaktiver kontakter
Deaktiver oppringing	Deaktiver innfødt oppringing
Deaktiver e-post	Deaktiver e-post
Deaktiver Exchange	Deaktiver Exchange-kontoer
Deaktiver Facebook	Deaktiver Facebook-appen
Deaktiver Galleri	Deaktiver den innebygde galleri-appen
Deaktiver Gmail	Deaktiver Gmail
Deaktiver Google Bøker	Deaktiver Google Bøker
Deaktiver Google Play Kiosk	Deaktiver Google Play Kiosk
Deaktiver Google Maps	Deaktiver Google Maps
Deaktiver Google Music	Deaktiver Google Music
Deaktiver Google Filmer	Deaktiver Google Filmer
Deaktiver Google Play Store	Deaktiver Google Play Store (offentlig App Store)
Deaktiver Google Plus	Deaktiver Google Plus
Deaktiver Google Søk	Deaktiver Google Søk
Deaktiver Google Talk / Google Hangouts	Deaktiver Google Talk / Google Hangouts
Deaktiver musikkspiller	Deaktiver den innebygde musikkspiller-appen
Deaktiver innstillinger	Deaktiver enhetsinnstillinger
Deaktiver Sim Toolkit	Deaktiver Sim Toolkit-tjenester
Deaktiver SMS / MMS	Deaktiver SMS / MMS
Deaktiver Street View	Deaktiver Street View-tjenester
Deaktiver Youtube	Deaktiver Youtube

Samsung-apper

Under "Samsung Apps" kan du definere ytterligere innstillinger og/eller begrensninger for Samsung-enheter.

Deaktiver AllShare Play / Samsung Link	Deaktiver AllShare Play / Samsung Link
Deaktiver ChatON	Deaktiver ChatON
Deaktiver Game Hub	Deaktiver Game Hub
Deaktiver gruppespill	Deaktiver gruppespill
Deaktiver hjelp	Deaktiver Samsung Help
Deaktiver KNOX	Deaktiver Samsung KNOX Container
Deaktiver Memo	Deaktiver talememo
Deaktiver Mine filer	Deaktiver Mine filer
Deaktiver optisk leser	Deaktiver optisk leser
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-assistenten
Deaktiver Samsung-apper	Deaktiver Samsung App Store
Deaktiver Samsung Hub	Deaktiver Samsung Entertainment Stores
Deaktiver videospiller	Deaktiver videospiller
Deaktiver stemmeopptaker	Deaktiver stemmeopptaker
Deaktiver WatchON	Deaktiver WatchON (simulerer en fjernkontroll)

Huawei-apper

Under "Huawei Apps" kan du definere ytterligere innstillinger og/eller begrensninger på Huawei-enheten.

Deaktiver DLNA	Deaktiver DLNA
Deaktiver App Installer	Deaktiver App Installer
Deaktiver File Manager	Deaktiver File Manager
Deaktiver Backup Manager	Deaktiver Backup Manager
Deaktiver systemoppdatering	Deaktiver systemoppdatering
Deaktiver verktøykasse	Deaktiver verktøykasse
Deaktiver Vær	Deaktiver Vær
Deaktiver FM-radio	Deaktiver FM-radio

Innstillinger for appadministrasjon

Her kan du definere oppdateringsatferden til InHouse Apps.

Oppdateringssjekkfrekvens definerer hvor ofte AppTec360-appen ser etter oppdateringer for InHouse-apper. Når en ny versjon har blitt oppdaget, lastes den ned og installeres.

Wi-Fi-terskelverdi definerer om nedlastingen skal begrenses til Wi-Fi-tilkoblinger hvis appen er større enn den konfigurerte terskelverdien. Hvis den er mindre eller du ikke definerer en terskel, vil appen lastes ned via Wi-Fi og mobilnettverk.

App Store for bedrifter

Vær oppmerksom på at apper som legges til her (Enterprise App Store), IKKE blir installert automatisk på enheten(e). Brukeren må åpne Enterprise App Store på enheten og installere appen manuelt.

Hvis du vil installere apper automatisk på enheten, kan du gå til "App Management" → "Enterprise App Manager" → "Obligatoriske apper" og legge til de ønskede appene der.

Under dette punktet kan du distribuere valgfrie apper til brukerne dine.

Playstore

Klikk på "+" for å legge til en Play Store-app i butikken. Hvis du bruker Android Enterprise, går du til "App Management Enterprise Play Store". Vær også oppmerksom på at en Google-konto må være konfigurert på → enheten for å installere appene som er definert her.

Internt

Under punktet "In-House" kan du laste opp og distribuere internt utviklede apper.

Klikk på "+" for å legge til en InHouse-app i Enterprise App Store, som deretter kan installeres av brukeren. I denne dialogen kan du også laste opp en ny InHouse-app.

Enterprise Play Store

Vær oppmerksom på at apper som legges til her (Enterprise Play Store), IKKE blir installert automatisk på enheten(e). Brukeren må åpne Play Store på enheten og installere appen manuelt.

Hvis du vil installere apper automatisk på enheten, kan du gå til "App Management" → "Enterprise App Manager" → "Obligatoriske apper" og legge til de ønskede appene der.

Under dette punktet kan du distribuere valgfrie apper til brukerne dine.

Her kan du legge til apper i Android Enterprise Playstore. Vær oppmerksom på at du må godkjenne apper i Generelle innstillinger → AE Play Store → Play Store-apper. Disse appene legges til i den vanlige Google Play-butikken.

Vær også oppmerksom på at du først må definere et oppsett med apper i Generelle innstillinger → Appadministrasjon → AE Play Store → Butikkoppsett.

Apper må være i et oppsett før du kan legge dem til i butikken.

Kioskmodus og lanseringsprogram

Kioskmodus

Kioskmodus lar deg forhåndsdefinere en app eller en URL. Da vil det bare være mulig å kjøre/besøke denne appen og/eller URL-en.

På samme måte kan ulike maskinvareknapper deaktiveres i Kiosk Mode diverse.

Automatisk start	Starter automatisk kioskmodus så snart profilen når sluttbrukerens enhet
Planlagt kioskmodus?	Du kan planlegge et tidspunkt for kioskmodus, som deretter starter og slutter automatisk på et tidspunkt du selv har angitt.
Starttidspunkt	Starttidspunkt
Tid i minutter	Tid i minutter, etter hvilken Kioskmodus skal avsluttes igjen

Søknadstype

Enkelt app	Hvis du vil starte appen i kioskmodus, velger du "Pakke" under "Applikasjonstype"
Kiosk-applikasjon	Klikk her for å velge en app som skal startes i kioskmodus Du finner den vanlige oversikten over App Management Du kan velge mellom "Google Play Store", "Android In-House Apps" og "Packagename"

Søknadstype

URL	Hvis du vil starte en URL i kioskmodus, velger du "URL" under "Applikasjonstype" Deretter definerer du ønsket URL-adresse
Tøm nettleseren etter inaktivitet	Her kan du definere et tidsintervall i minutter, etter hvilket Kioskmodus skal startes på nytt
Tøm nettbuffer og informasjonskapsler	Hvis du aktiverer denne funksjonen, vil nettbufferen (informasjonskapsler og hurtigbufrede bilder) slettes etter en omstart av kioskmodus
Retningslinjer for samme opprinnelse	Hvis denne funksjonen er aktiv, kan brukeren bare surfe på undersidene til en definert URL Du har for eksempel definert følgende URL:www.mypage.com Da kan brukeren surfe på: www.mypage.com/subpage
Hvitelistede nettadresser	Her kan du vedlikeholde en hviteliste, alle disse nettadressene er tillatt Maksimalt 1 URL per linje En URL må begynne med http:/ eller https://
Svartelistede nettadresser	Her kan du vedlikeholde en svarteliste, alle disse nettadressene er ikke tillatt Maksimalt 1 URL per linje En URL må begynne med http:/ eller https://
Skjermorientering	Denne innstillingen gjelder skjermjusteringene Automatisk = automatisk Stående = vertikalt format Landscape = liggende modus

Multi-app	Hvis du velger "Multi App"-kioskmodus, vil bruk av AppTec360 Launcher være obligatorisk.
Apper	Applikasjon: Velg en Playstore eller en egen app som kioskapplikasjon. Det er også mulig å angi et pakkenavn. Den valgte kioskapplikasjonen må være installert på enheten. Husk å angi Kiosk-applikasjonen som obligatorisk. Snarvei på startskjermen: Hvis den er satt til "På", opprettes det en snarvei på startskjermen. Hvis den er satt til "Av", vil appen fortsatt vises i applisten.

Avslutt passord aktivert	Hvis du aktiverer denne funksjonen, er det mulig for brukeren å avslutte Kioskmodus med et passord som er forhåndsdefinert av deg.
Avslutt passord	Dette er passordet som ble forhåndsdefinert av deg
Skjul statuslinjen automatisk	Hvis dette alternativet er aktivert, vil statuslinjen automatisk bli uthevet. Med dette alternativet kan brukerne se informasjonen på statuslinjen, men ikke få tilgang til dens funksjoner.
Deaktiver statuslinjen	Statuslinjen inneholder varsler, snarveier og informasjon. Kun tilgjengelig for Samsung-enheter med KNOX 1.0 eller nyere.
Deaktiver volumtastene	Deaktiver volumtaster (kun tilgjengelig på Samsung-enheter med KNOX 1.0 eller nyere)
Deaktiver av/på-bryter	Deaktiver av/på-bryteren (kun tilgjengelig på Samsung-enheter med KNOX 1.0 eller høyere)
Deaktiver Hjem-knappen	Deaktiver Hjem-knapp. Hvis denne funksjonen er aktivert, kan Kioskmodus bare avsluttes i AppTec360-konsollen. (kun tilgjengelig på Samsung-enheter med KNOX 1.0 eller nyere)
Deaktiver navigasjonslinjen	Med denne kan du deaktivere navigasjonslinjen (Tilbake/Meny) Hvis denne funksjonen er aktivert, kan Kioskmodus bare avsluttes i AppTec360-konsollen (kun tilgjengelig på Samsung-enheter med KNOX 1.0 eller nyere)

Innstillinger for appoppdatering	
Tillat appoppdateringer	Brukerne vil bli bedt om å utføre appoppdateringer selv når Kiosk Mode er aktiv. På enheter med Samsung KNOX oppdateres apper i stillhet.
Oppdateringsvindu	Angi et intervall der brukerne blir bedt om å installere appoppdateringer.

TeamViewer	
Aktiver uovervåket tilgang	Hvis denne funksjonen er aktivert, kan administratorer fjernstyre enheten uten brukerinteraksjon. Appen TeamViewer Host må være installert på enheten.

AppTec360 Launcher

Aktiver AppTec360 Launcher	På: Aktiverer AppTec360 Launcher. Brukeren må angi den som standard Launcher én gang. Merk: Hvis kioskmodus er aktivert, og kioskmodus er satt til "Multi App", vil bruk av AppTec360-startprogrammet være påtvunget.
Store ikoner	På: Viser en større versjon av appikonene i startprogrammet
Skjul AppTec360-appikonet	På: Skjuler AppTec360-appen fullstendig
Skjul AppTec360 Store-ikonet	På: Skjuler AppTec360 Enterprise AppStore fullstendig

AppTec360-innstillinger

Aktiver AppTec360 Settings App	AppTec360 Settings-appen gir kontroll over WiFi- og Bluetooth-tilkoblinger
Aktiver innstillinger i Multi App Kioskmodus	Hvis dette er aktivert, kan brukerne få tilgang til AppTec360 Settings-appen mens Multi App Kiosk Mode er aktiv

Fjernkontroll

Splashtop

Viser gjeldende status for Splashtop-oppsettet. Her ser du trinnene du må utføre for å få ekstern tilgang til enheten via Splashtop. Her må du også skrive inn distribusjonskoden som du kan få fra Splashtop-nettstedet. Distribusjonskoden er nødvendig for å koble til enheten.

Teamviewer

Viser gjeldende status for Teamviewer-oppsettet. Her ser du trinnene du må utføre for å få ekstern tilgang til enheten via Teamviewer.

Innholdsstyring

Innholdsboks

Her kan du aktivere Contentbox for denne enheten. Når den er aktivert, blir Contentbox-appen installert på enheten.

Sikker nettleser

Her kan du aktivere Secure Browser for denne enheten. Når den er aktivert, blir Secure Browser-appen installert på enheten. Denne nettleseren kan konfigureres til å tilby en nettleser på enheten som er begrenset til dine behov.

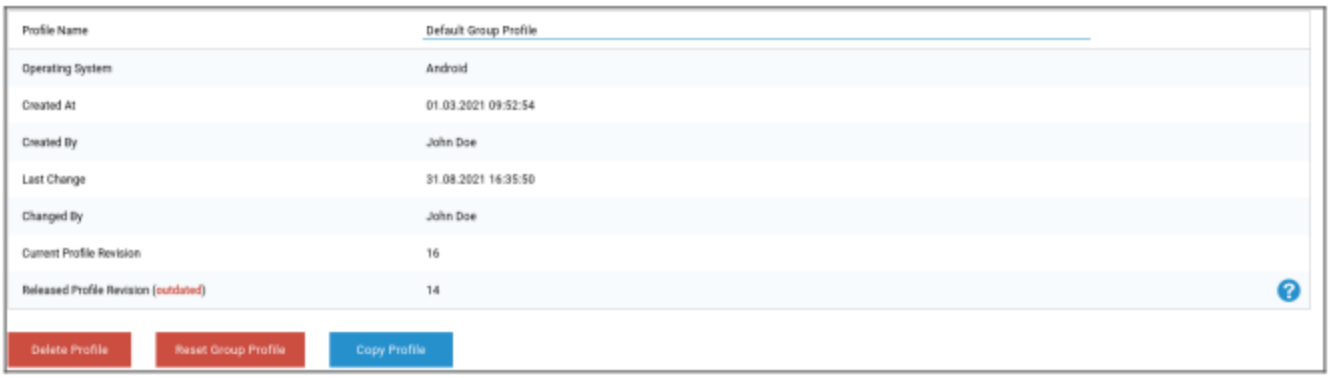
Krever passord	Krev at brukeren oppretter og bruker et passord for å få tilgang til nettleseren.
Begrens nedlastinger / Åpne i	Blokkerer nedlastinger fra nettsteder
Begrens opplastinger	Begrenser opplastinger til bestemte URL-adresser. Oppgi ingen URL for å blokkere opplastingen helt
Tillat kopiering	Tillat kopiering, klipping eller deling av tekst inne på nettsidene.
Tillat skjermopptak	Tillat å ta skjermbilder.
Hyppighet for opprydding av data	Velg med hvilken frekvens ALLE brukerdata (historikk, hurtigbuffer osv.) skal fjernes automatisk.
Selskapets bokmerker	Bokmerkene vises i mappen "Company bookmarks" i nettleserens bokmerker. De kan ikke redigeres av brukeren.
Skjul adresselinjen	Skjuler adresselinjen slik at brukeren ikke ser URL-en han besøker
Hvitelisting i nettleseren (uten Universal Gateway)	Aktiverer hvitlisting av nettadresser på klientsiden. - Bedriftsbokmerker er alltid hvitelistet - Støttes kun for 100 nettadresser - Bruk Universal Gateway for ubegrenset svart- og hvitelisting
Gateway-basert svart- og hvitelisting	Svartelisting har følgende krav: - En fungerende AppTec360 Universal Gateway ("Generelle innstillinger" → "Universal Gateway") - En fungerende VPN-konfigurasjon med en spesifisert DNS-server ("Generelle innstillinger" → "Universal Gateway" → "VPN-innstillinger") - En svartelistekonfigurasjon ("Generelle innstillinger" → "Universal Gateway" → "Domain Blacklist") - En gyldig VPN-tilkobling i profilen ("Connection Management" → "VPN")

Konfigurasjon Windows 10 PC

Generelt

Oversikt over gruppeprofiler (kun på gruppenivå)

Når du åpner en gruppeprofil, får du en rask oversikt over profilen.



Profilnavn	Navn på profilen (kan endres her)
Operativsystem	Operativsystemet profilen er beregnet på
Opprettet på	Tidspunktet for skapelsen
Opprettet av	Skaperen av profilen
Siste endring	Tidspunkt for siste endring av profilen
Endret av	Konto som gjorde de siste endringene
Nåværende profilrevisjon	Revisjon av lagret profilstatus
Utgitt profilrevisjon	Tilordnet profilrevisjon ("Tilordne nå"). Hvis etiketten viser "(utdatert)" bak teksten, betyr det at du har lagret profilen, men ikke tilordnet den ennå, slik at enhetene fortsatt vil få en eldre versjon.

Enhetsoversikt (kun på enhetsnivå)

Enhetens oppsummerte oversikt, som inneholder følgende:

PC-navn	Navnet på PC-en
Kunde	Enhetene av Windows-typen
Sist kjente posisjon	Breddegrad og lengdegrad for enhetens siste kjente posisjon
Tildelte obligatoriske apper	Antall obligatoriske apper som er tilordnet enheten
PC UID	UID for PC-en
OS-utgave	Viser Windows-utgaven din
OS-versjon	Gjeldende installert Windows-versjon
OS Build	Nåværende Windows-versjon
Operativsystem	Operativsystem som er installert for øyeblikket
Serienummer	Enhetens serienummer
Eierskap til enheten	Den konfigurerte eierskapstypen
Enhetstype	Type enhet
Rotfestet	Viser om enheten er rotfestet
Overensstemmende	Viser om enheten er kompatibel
Sist sett	Dato og klokkeslett for når endringene ble gjort på profilen
Tildeling av bruker	Viser brukeren eller gruppen denne enheten er tilordnet for øyeblikket. Du kan flytte enheten ved å velge en annen bruker eller gruppe fra nedtrekkslisten.

Innstillinger

Tillat automatisk oppdatering	Tillat eller ikke tillat automatiske systemoppdateringer.

Konfigureringsrevisjon (kun på enhetsnivå)

Her får du en oversikt over hvilken gruppeprofil som er tilordnet enheten.

Hvis du klikker på gruppeprofilen, får du direkte tilgang til profilen og kan utføre innstillinger.

Med symbolet kan du tilbakestille de tilordnede appene til gruppeprofilens innstillinger.

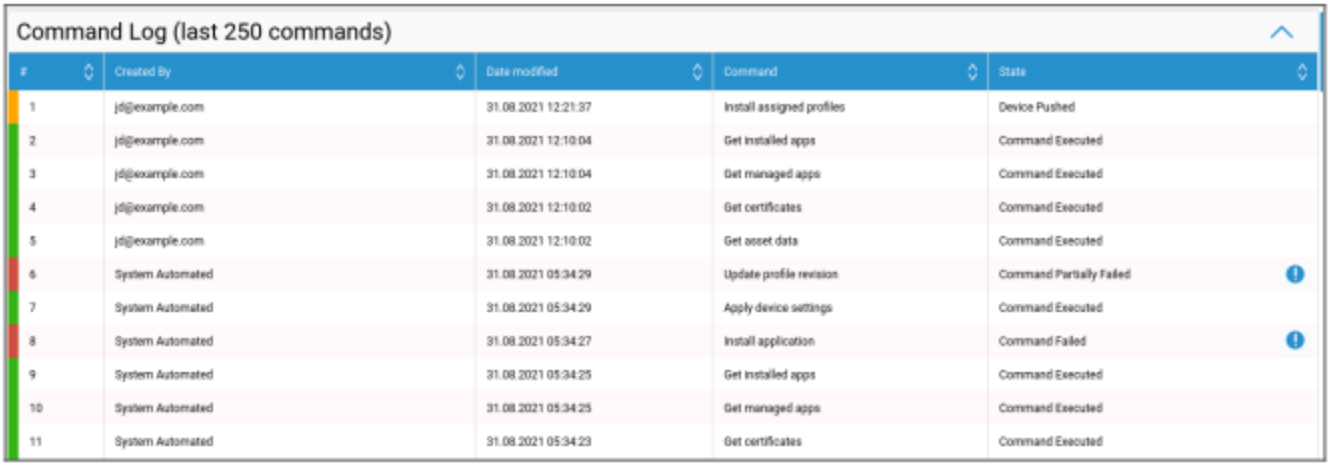
Med symbolet kan du tilbakestille enhetsprofilen slik at den ikke har noen innstillinger i det hele tatt.

"Nyere revisjon tilgjengelig" indikerer at gruppeprofilen har blitt endret og lagret, men ikke tilordnet. Gruppeprofilen må tilordnes med "Tilordne nå" på gruppenivå for at endringene skal gjelde for enhetene.

Enhetslogg (kun på enhetsnivå)

Kommandologg

Her kan du se hvilke kommandoer som er utstedt for enheten, og hvilken status de har.



Kommandoer som opprettes av "System Automated", opprettes automatisk av systemet.

Mulige kommandostatuser

Enhet skjøvet	En push-forespørsel har blitt sendt til push-tjenesten (f.eks. APNS) for å be enheten om å koble seg tilbake til EMM-serveren.
Kommando opprettet	Kommandoen ble opprettet i systemet.
Kommando sendt	Kommandoen ble sendt til enheten etter at den ble koblet til serveren.
Kommando utført	Kommandoen ble vellykket utført.
Kommando mislyktes	Kommandoen mislyktes. *
Kommandoen mislyktes delvis	Avhengig av enhetens operativsystem kan enkelte kommandoer bli gruppert sammen. I dette mislyktes noen deler av denne kommandogruppen. *
Kommando utført, men mislyktes til slutt	Kommandoen ble utført, men kanskje ikke.
Kommando Repushed	Kommandoen ble sendt på nytt av en bruker.
Kasseres	Kommandoen ble forkastet. For eksempel fordi den ble erstattet av en annen kommando, eller fordi enheten ble registrert på nytt og gamle kommandoer ble fjernet.

*Hvis det er et utropstegn bak meldingen, kan du få mer informasjon ved å holde musepekeren over ikonet.

Asset Management (kun på enhetsnivå)

Enhetsinfo

Produsent	Produsent av enheten
Modell	Enhetsmodell
Modellnummer	Modellnummer
Operativsystem	Operativsystem
OS-versjon	OS-versjon
Serienummer	Serienummer
ExchangeID	ExchangeID
Totalt RAM	Totalt RAM
Skjermoppløsning	Skjermoppløsning
Telefon Språk	Enhetens språk
Fastvareversjon	Fastvareversjon
DM-klientversjon	Versjon av Device Management Client
Maskinvareversjon	Maskinvareversjon av enheten
CPU-arkitektur	CPU-arkitektur (prosessortype)

Cellular

SIM-operatørens nettverk	Bærernettverk
Telefonnummer	Telefonnummer
Roaming-status	Roaming-status
IMEI	IMEI
IMSI	IMSI
Fastvare for modem	Fastvare for modem

Synkroniseringsinfo

Øyeblikkelig DM-tilkobling	Enheten skal umiddelbart opprette en forbindelse til AppTec
Tid for første forsøk	Første forsøk for denne første tilkoblingen
Nye tilkoblingsforsøk	Antall nye tilkoblingsforsøk etter en frakobling fra Connection Manager eller en feil på WinInet-nivå
Maksimal sovetid	Maksimal hviletid etter feil ved pakkesending
Første synkroniseringsforsøk	Tid for første etappe etter innskrivningen
Første gjentakelsesintervall	Tid for første etappe etter innskrivningen
Andre synkroniseringsforsøk	Tid for andre fase etter innskrivningen
Andre gjentakelsesintervall	Tid for andre fase etter innskrivningen
Regelmessige synkroniseringsforsøk	Tid for de ytterligere trinnene etter innskrivningen
Regelmessig gjentakelsesintervall	Tid for de ytterligere trinnene etter innskrivningen

Sikkerhetsstyring

Tyverisikring (kun på enhetsnivå)

GPS-informasjon (kun på enhetsnivå)

Her kan du angi enhetens nåværende/seneste plassering. Lokaliseringen kan beskyttes med ett eller til og med to passord - se: "Generelle innstillinger" > "Personvern" > "GPS-tilgang"

GPS-innstillinger

Aktiver GPS-sporing	Aktiver regelmessig synkronisering av GPS-informasjon.
Sporingsintervall	Still inn intervallet for synkronisering av GPS-informasjon.

Sikkerhetskonfigurasjon

Passord

Minimum passordlengde	Minimum passordlengde	
Sammensetning av passord	Angir hvor mange spesifikke tegn passordet må inneholde Disse består av store bokstaver, små bokstaver, tall og spesialsymboler	
Passordkvalitet	Her kan du angi passordkvalitet	
	Alfanumerisk	Bare tall og bokstaver
	Numerisk	Bare tall
	Numerisk eller alfanumerisk	Tall eller tall og bokstaver
Maksimal inaktivitetstid Lås	Antall minutter brukeren har vært inaktiv på enheten, og deretter låses enheten. Brukeren må låse opp enheten etter denne tiden ved å taste inn enhetens passord.	
Passordets utløpsdato	Still inn hvor lang tid det skal gå før et nytt passord må angis	
Begrensning av passordhistorikk	Antall tidligere brukte passord som ikke er tillatt	
Maksimalt antall mislykkede passordforsøk	Antall ganger passordet kan tastes inn feil før enheten blir fullstendig slettet	

Antivirus

Antivirusinnstillinger - Angi skannekonfigurasjon	
Type skanning	Velger om du vil utføre en rask eller fullstendig skanning
Angi skannestart	Velger tidspunktet på dagen som Windows Defender skal starte skanningen på
Skannefrekvens	Velger hvilken dag Windows Defender-skanningen skal kjøres
Oppdateringsfrekvens for signaturer	Angir intervallet i timer som skal brukes til å sjekke for signaturer

Konfigurer filtype for skanning	
Tillat skanning av arkivfiler	Tillat eller ikke tillat skanning av arkiver (f.eks. .zip) når de åpnes.
Tillat skanning av skript	Tillater eller avviser Windows Defender Script Scanning-funksjonalitet.
Tillat skanning av e-post	Tillat eller forbyr skanning av e-post.
Tillat skanning av nettverksfiler	Tillat eller forbyr skanning av nettverksfiler.
Tillat full skanning av tilordnede nettverksstasjoner	Tillat eller ikke tillat skanning av tilordnede nettverksstasjoner (bare aktivert når full skanning er aktivert).
Kontroller toveis skanning	Kontrollerer hvilke sett med filer som skal overvåkes.
Tillat full skanning av flyttbare stasjoner	Tillat eller ikke tillat full skanning av flyttbare stasjoner. Bare når full skanning er igangsatt.

Type filer som skal utelukkes fra skanningen	
Ignorer filtyper for skanning	Definer et sett med filtyper. Hver filtype for hvert felt.
Ignorer katalogstier	Definer et sett med katalogstier for å unngå å skanne dem. Én bane per felt. Eksempler: "C:\Example", "C:\Windows" eller "C:\Users".
Utelukke prosesser fra skanning	Utelukk filer som har blitt åpnet av bestemte prosesser fra Microsoft Defender Antivirus-skanninger. . Én bane per felt. Eksempler: "C:\myFile.exe", "C:\Windows\myProcess.exe", "C:\myScript.bat

Ekstra innstillinger	
Tillat overvåking i sanntid	Tillat eller ikke tillat Windows Defender Realtime Monitoring-funksjonalitet
Tillat atferdsovervåking	Tillat eller ikke tillat Windows Behavior Monitoring-funksjonalitet
Tillat beskyttelse i skyen	Tillat eller ikke tillat at Windows Defender sender informasjon til Microsoft om eventuelle problemer som oppdages. Microsoft vil analysere denne informasjonen, lære mer om problemet som påvirker enheten, og tilby forbedrede løsninger
	Adferd for sending av prøver
Tillat Windows Defender IOAV-beskyttelse	Tillat eller ikke tillat Windows Defender IOAV-beskyttelse
Tillat tilgang til Defenders "On Access Protection"-grensesnitt	
Gjennomsnittlig CPU-belastningsfaktor	Representerer den gjennomsnittlige CPU-belastningsfaktoren for Windows Defender-skanningen (i prosent)

Håndtering av skadelig programvare	
Lav alvorlighetsgrad	Du kan definere hvordan enheten skal håndtere skadelig programvare for hvert alvorlighetsgradnivå. Tilgjengelige alternativer er: • Ren • Karantene • Fjern • Tillat • Brukerdefinert • Blokk
Moderat alvorlighetsgrad	
Høy alvorlighetsgrad	
Alvorlig alvorlighetsgrad	
Dager for å beholde renset skadelig programvare	Tidsperiode i dager som filer/elementer i karantene skal lagres på systemet. Standardverdien er 0, noe som betyr at elementer forblir i karantene og ikke fjernes automatisk. Maksverdien er 90.

Sikkerhetssenter

Windows sikkerhetssenter - Innstillinger for Windows-sikkerhet	
Deaktiver virus- og trusselbeskyttelse UI	
Hide Ransomware Data Recovery UI	
Deaktiver brukergrensesnittet for kontobeskyttelse	
Deaktiver brannmur og nettverksbeskyttelse UI	
Deaktiver brukergrensesnittet for app- og nettleserkontroll	
Ikke tillat endringer i Exploit-beskyttelsen	Ikke tillat brukeren å gjøre endringer i innstillingene for Exploit-beskyttelse
Deaktiver enhetssikkerhet UI	
Skjul feilsøking av TPM	Skjul innstillinger for feilsøking av TPM
Deaktiver Clear TPM-knappen	
Deaktiver brukergrensesnittet for enhetens ytelse og helse	
Deaktiver familiealternativer UI	

Tilpass skåler	
Aktiver tilpasset supportinformasjon	Aktiver for å vise tilpasset kontaktinformasjon for bedriften din nederst til høyre i Sikkerhetssenter-appen.
E-postadresse	Angi selskapets e-postadresse
Selskapets navn	Angi selskapets navn
Firmaets telefon	Still inn selskapets telefon
Hjelp URL	Angi selskapets hjelpe-URL

Ekstra innstillinger	
Deaktiver varslinger	Deaktiver visning av Windows Defender Security Center-varsler.
Anbefalinger for oppdatering av TPM-fastvare	Skjul anbefalingen om å oppdatere TPM-fastvare når en sårbar fastvare oppdages.
Vis firmanavn og kontaktalternativer	Vis firmanavnet og kontaktalternativene dine på et kontaktkort i Windows Defender Security Center.
Skjul Secure Boot	Skjul området Security Boot.
Skjul kontroll av sikkerhetsvarslingsområdet	Skjul kontrollen for Windows Security-varslingsområdet.

Konfigurasjon av brannmur

Brannmurkonfigurasjon - Globale innstillinger	
Ignorer innstilt autentisering	Ignorer hele autentiseringssettet hvis de ikke støtter alle autentiseringspakkene som er angitt i settet
Type pakkekø	Angir hvordan skalering for programvaren på mottakssiden skal aktiveres for både kryptert mottak og klarering av videresendingsbanen for IPsec-tunnelgatewayscenarioet.
Deaktiver utføre tilstandsbasert FTP-filtrering	Hvis den er deaktivert, vil den ikke utføre stateful File Transfer Protocol (FTP)-filtrering for å tillate sekundære tilkoblinger
Inaktivitetstid for sikkerhetstilknytning	Dette feltet konfigurerer inaktivitetstiden for sikkerhetstilknytninger i sekunder. Sikkerhetstilknytninger slettes når det ikke har vært nettverkstrafikk i den angitte tidsperioden.
Koding av forhåndsdelt nøkkel	Angi kodingen av den forhåndsdelte nøkkelen
Unntak fra IPSec	Konfigurere unntak for Internett-protokollen
Kontroll av sertifikatopphevelseslisten	

Brannmurprofiler (domeneprofil / privat profil / offentlig profil)	
Aktiver brannmur for denne profilen	
Deaktiver varslinger	Deaktiver visning av varsel til brukeren når et program er blokkert fra å lytte på en port.
Blokkerer unicast-svar på multicast-sendinger	
Håndhev regler for brannmur for autoriserte applikasjoner	Hvis den ikke håndheves, blir autoriserte applikasjonsbrannmurregler i det lokale lageret ignorert og ikke håndhevet
Håndhev globale regler for portbrannmur	Hvis den ikke håndheves, ignoreres globale portbrannmurregler i det lokale lageret og håndheves ikke. Innstillingen har bare betydning hvis den er angitt eller opplistet i gruppepolicylageret eller hvis den er opplistet fra GroupPolicyRSoPStore
Håndhev brannmurregler	Hvis den ikke er valgt, blir brannmurreglene fra det lokale lageret ignorert og ikke håndhevet.
Håndhev sikkerhetsregler for tilkobling	Hvis den ikke håndheves, ignoreres sikkerhetsreglene for tilkobling fra det lokale lageret og håndheves ikke.
Standard utgående handling	Handlingen som brannmuren utfører som standard på utgående tilkoblinger
Standard innkommende handling	Handlingen som brannmuren utfører som standard på innkommende tilkoblinger
Deaktiver Stealth-modus	Stealth-modus er en mekanisme i Windows-brannmuren som bidrar til å forhindre at ondsinnede brukere får tilgang til informasjon om nettverksdatamaskiner og tjenestene de kjører.
Deaktiverer forhindring av å svare på uønsket trafikk	Hvis den er deaktivert, skal brannmurens regler for skjult modus ikke hindre vertsdatamaskinen i å svare på uoppfordret nettverkstrafikk hvis trafikken er sikret med IPsec

Brannmurregler

Brannmurregler	
Navn	Navn på regelen
Beskrivelse	Beskrivelse av regelen
Handling	Angi om denne regelen skal blokkere trafikken eller tillate den. Vær oppmerksom på at alternativet Blokker også kan blokkere trafikken (avhengig av resten av konfigurasjonen) mellom MDM-serveren og enheten.
Retning	
Aktiver kantkryssing (kun tilgjengelig når **Retning** er satt til **innkommende trafikk**)	Angir at spesifikk innkommende trafikk er tillatt å tunnellere gjennom NAT-er og andre edge-enheter ved hjelp av Teredo-tunneleringsteknologien.

Programmer og tjenester	
Definer applikasjoner, alt annet	Hvis den ikke er aktivert, vil den vurdere alle søknader
Navn på pakkefamilie	Navnet på pakkefamilien som regelen skal gjelde for.
Filbanen til applikasjonen	Det fullstendige programmet, for eksempel C:\Windows\System\Notepad.exe, som regelen skal gjelde for
Fullt kvalifisert binært navn	Det fullt kvalifiserte binære navnet som regelen skal gjelde for. Et FQBN er en streng i følgende form: {Publisher\Product\Filename,Version}.
Tjenestens navn	Skriv inn navnet på en tjeneste (f.eks. "EventLog"). Du kan få en liste over tjenestenavn i Powershell ved å kjøre kommandoen "Get-Service".

Protokoller og porter				
Protokoll	Protokollen som brukes av regelen.			
	Tilgjengelige verdier: - Alle - Tilpasset - HOPORT - ICMPv4 - IGMP - TCP - UDP - IPv6 - IPv6-rute - IPv6-Frag - GRE - ICMPv6 - IPv6-NoNxt - IPv6-Opts - VRRP - PGM - L2TP	Når den er satt til Egendefinert	Skriv inn et protokollnummer mellom 0 og 255	Protokollnummeret
		Når den er satt til TCP eller UDP	Angi lokale porter, ellers vil alle bli brukt	Lokale porter som regelen skal bruke, områdeporter er også tillatt
			Lokal havn	En enkelt port eller en rekke porter. F.eks. 100-120,200,300-320.
			Angi eksterne porter, ellers vil alle bli brukt	Eksterne porter som regelen skal bruke, områdeporter er også tillatt
			Ekstern port	En enkelt port eller en rekke porter. F.eks. 100-120,200,300-320.

Omfang	
Angi lokale IP-er, ellers hvilken som helst IP	Sett med lokale IP-er, det kan også være en rekke IP-er atskilt med -.
Lokal IP-adresse	Sett med enkelt-IP-er eller en rekke IP-er atskilt med -.
Angi eksterne IP-adresser, ellers hvilken som helst ekstern IP	Angi et sett med eksterne IP-adresser, det kan også være en rekke IP-adresser atskilt med "-".
Ekstern IP-adresse	Angi enkelt-IP-er eller en rekke IP-er
Tokens	Tokens som kan angis sammen med eksterne adresser. Tokens Intranet, RmtIntranet og Ply2Renders støttes i Windows 10, versjon 1809 og nyere.

Avanserte innstillinger	
Angi profiler, ellers vil alle bli brukt	Hvis deaktivert, vil alle profiler bli brukt

Domene	Domeneprofil
Privat	Privat profil
Offentlig	Offentlig profil
Angi grensesnitt, ellers vil alle bli brukt	Hvis deaktivert, vil alle grensesnitt bli brukt
Lokalt nettverk	Grensesnitt for lokalt nettverk
Ekstern tilgang	Grensesnitt for ekstern tilgang
Trådløs	Trådløst grensesnitt

Lokale rektorer	
Legg til autoriserte lokale brukere	Tillat å legge til en liste over lokale brukere som skal bruke denne regelen
Autoriserte brukere	Liste over autoriserte lokale brukere for denne regelen. Brukeren må være i SDDL-format (Security Description Definition Language), f.eks. PC_NAME\USERNAME. Dette feltet må ikke fylles ut hvis et tjenestenavn er angitt for å bruke denne regelen.

Begrensningsinnstillinger

Enhetens funksjonalitet

Tillat SD-kort	Tillat bruk av SD-kort
Tillat kamera	Tillat bruk av kameraet
Tillat lokasjonstjeneste	Tillat enhetsplasseringstjeneste
Tillat sidelading av apper	Tillat installasjon av apper fra ukjente kilder
Tillat utviklermodus	Tillater utviklermodus
Tillat roaming av mobildata	Tillat roaming av mobildata
Tillat Cortana	Tillat stemmeassistenten Cortana
Tillat søk å bruke plassering	Tillat søk å bruke posisjon
Tillat å legge til andre e-postkontoer enn Microsoft	Angi om brukeren har tillatelse til å legge til e-postkontoer som ikke er MSA-kontoer.
Tillat tilkobling av Microsoft-konto	Angi om du vil tillate bruk av MSA-kontoer for autentisering og tjenester som ikke er e-postrelaterte.
Tillat synkronisering av mine innstillinger	Gjør det mulig å synkronisere innstillinger på tvers av hele enheten
Bedriftsbeskyttede domenenavn	Angir virksomhetens domenenavn atskilt med ";".
Tillat brukeren å deaktivere systemgjenoppretting	Gjør det mulig for brukeren å deaktivere Systemgjenoppretting. **ADVARSEL!** Denne funksjonen bør bare brukes på enheter som eies eller leveres av bedriften eller organisasjonen, eller på en brukereid enhet der brukeren tillater at enheten administreres fullt ut av bedriften. Hvis du deaktiverer denne policyinnstillingen, blir Systemgjenoppretting slått av, og veiviseren for systemgjenoppretting er ikke tilgjengelig. Muligheten til å konfigurere Systemgjenoppretting eller opprette et gjenopprettingspunkt via Systembeskyttelse er også deaktivert.
Tillat utmelding av brukere	Gjør det mulig for brukeren å fjerne bedriftsdelen fra enheten og dermed koble seg fra AppTec360-serverne. Hvis dette skjer, vil det ikke lenger være mulig å administrere enheten.

	ADVARSEL! Denne funksjonen skal bare brukes på enheter som eies eller leveres av bedriften eller organisasjonen, eller på en brukereid enhet der brukeren tillater at enheten administreres fullt ut av bedriften. Hvis du deaktiverer denne policyinnstillingen, vil ikke brukerne kunne fjerne MDM-registreringer. Angi om brukeren har lov til å slette arbeidsplasskontoen via kontrollpanelet på arbeidsplassen. MDM-serveren kan alltid slette kontoen eksternt.

BitLocker

BitLocker-konfigurasjon

Generelle innstillinger	
Krev kryptering av enheten	Avhengig av Windows-utgaven og systemkonfigurasjonen kan brukerne bli bedt om å aktivere enhetskryptering: - For å bekrefte at kryptering fra en annen leverandør ikke er aktivert. - Slik slår du av BitLocker Drive Encryption og deretter på BitLocker igjen.
Krypteringsmetoder	
Krypteringsmetode for operativsystemstasjoner	
Krypteringsmetode for faste datastasjoner	
Krypteringsmetode for flyttbare dataenheter	
Deaktiver advarsel om tredjeparts diskkryptering	Deaktiver advarselen om at en tredjeparts diskkrypteringstjeneste brukes på enheten. Fra og med Windows 10, versjon 1803, støttes denne innstillingen bare for enheter som er koblet til Azure Active Directory.
Tillat kjøring av kryptering mens en ikke-administratorbruker er logget inn	Støttes kun for enheter som er tilknyttet Azure Active Directory

AppTec360-utvidelser	
Lydløs kryptering	Hvis dette velges sammen med "Krev enhetskryptering", vil AppTec360 Management Service kjøre automatisk lydløs kryptering av enhetens stasjoner.
Automatisk generering av brukerlegitimasjon	Den krypterte OS-stasjonen blir beskyttet med automatisk generert brukerlegitimasjon. Enten en TPM-PIN-kode, når en TPM er tilgjengelig, eller et sekssifret tekstpassord. Den genererte legitimasjonen sendes til e-postadressen som er registrert for den gitte enheten. Hvis dette alternativet er slått av, er den eneste mulige beskyttelsen for stille kryptering å bruke TPM. I så fall vil stille kryptering mislykkes for enheter uten TPM.
Krypter faste stasjoner	Alle tilgjengelige faste datastasjoner blir også kryptert og beskyttet med "Automatic Unlock" ved hjelp av en nøkkel som er lagret på OS-stasjonen.

Innstillinger for OS-stasjon	
Krev ekstra autentisering ved oppstart	Med denne innstillingen kan du konfigurere om BitLocker skal kreve autentisering hver gang datamaskinen starter. Denne innstillingen brukes under oppsettet av BitLocker. Hvis du aktiverer denne innstillingen, kan brukerne konfigurere avanserte oppstartsalternativer i konfigurasjonsveiviseren for BitLocker.
Blokker BitLocker uten en kompatibel TPM	
Kun TPM	
TPM og PIN-kode	
TPM og nøkkel	
TPM, nøkkel og PIN-kode	Hvis du ønsker å kreve bruk av en PIN-kode og en USB-minnepinne (nøkkel), må brukeren konfigurere BitLocker ved hjelp av kommandolinjeverktøyet "manage-bde" i stedet for installasjonsveiviseren for BitLocker Drive Encryption.

Krev minimum PIN-lengde	
	Minimum tegn

Konfigurer melding og URL for gjenoppretting før oppstart	Konfigurer hele gjenopprettingsmeldingen eller erstatt den eksisterende URL-adressen som vises på gjenopprettingsskjermen før oppstart når OS-stasjonen er låst. Merk: Ikke alle tegn og språk støttes i pre-boot. Det anbefales på det sterkeste at du tester at tegnene du bruker, vises riktig på gjenopprettingsskjermen før oppstart.
	Alternativ for gjenopprettingsmelding før oppstart
	Tilpasset gjenopprettingsmelding
	Tilpasset URL for gjenoppretting

Alternativer for gjenoppretting av OS-stasjoner		Med denne innstillingen kan du kontrollere hvordan BitLocker-beskyttede operativsystemstasjoner gjenopprettes hvis du ikke har den nødvendige legitimasjonen. Denne innstillingen brukes under oppsettet av BitLocker. Som standard er en sertifikatbasert datagjenopprettingsagent tillatt, gjenopprettingsalternativene kan spesifiseres av brukeren, inkludert gjenopprettingspassord og gjenopprettingsnøkkel, og gjenopprettingsinformasjon sikkerhetskopieres ikke til AD DS.
	Block Certificate-basert datagjenopprettingsagent	Angi om et datagjenopprettingsverktøy kan brukes med BitLocker-beskyttede operativsystemstasjoner. Før en datagjenopprettingsagent kan brukes, må den legges til fra elementet Offentlige nøkkelpolicyer i enten konsollen for gruppepolicybehandling eller i redigeringsprogrammet for lokal gruppepolicy. Se BitLocker Drive Encryption Deployment Guide på Microsoft TechNet for mer informasjon om hvordan du legger til datagjenopprettingsagenter.
	Innstillinger for BitLocker-gjenopprettingspassord	
	Innstillinger for BitLocker-gjenopprettingsnøkkel	
	Lagre informasjon om BitLocker-gjenoppretting i Active Directory Domain Services	
	AD DS BitLocker-konfigurasjon for gjenopprettingslagring	Lagring av nøkkelpakken støtter gjenoppretting av data fra en stasjon som har blitt fysisk ødelagt.
	Krev lagring av gjenopprettingsdata i AD DS	Hindre brukere i å aktivere BitLocker med mindre datamaskinen er koblet til domenet og

Faste stasjonsinnstillinger	
Alternativer for gjenoppretting av faste stasjoner	Med denne innstillingen kan du kontrollere hvordan BitLocker-beskyttede faste stasjoner gjenopprettes hvis du ikke har den nødvendige legitimasjonen. Denne innstillingen brukes under oppsettet av BitLocker. Som standard er en sertifikatbasert datagjenopprettingsagent tillatt, gjenopprettingsalternativene kan spesifiseres av brukeren, inkludert gjenopprettingspassord og gjenopprettingsnøkkel, og gjenopprettingsinformasjon sikkerhetskopieres ikke til AD DS.
Block Certificate-basert datagjenopprettingsagent	
Innstillinger for BitLocker-gjenopprettingspassord	
Innstillinger for BitLocker-gjenopprettingsnøkkel	
Lagre informasjon om BitLocker-gjenoppretting i Active Directory Domain Services	
AD DS BitLocker-konfigurasjon for gjenopprettingslagring	Lagring av nøkkelpakken støtter gjenoppretting av data fra en stasjon som har blitt fysisk ødelagt.
Krev lagring av gjenopprettingsdata i AD DS	Hindre brukere i å aktivere BitLocker med mindre datamaskinen er koblet til domenet og sikkerhetskopieringen av BitLocker-gjenopprettingsinformasjon til AD DS er vellykket. Merk: Gjenopprettingspassordet genereres automatisk.
Nekter skrivetilgang til ubeskyttede faste stasjoner	

Innstillinger for flyttbare stasjoner	
Nekter skrivetilgang til ubeskyttede flyttbare stasjoner	Nekter skrivetilgang til flyttbare datastasjoner som ikke er beskyttet av Bitlocker. Merk: Hvis "Flyttbare disker: Nekt skrivetilgang" er aktivert i gruppepolicyen, vil denne policyinnstillingen bli ignorert.
Nekte skrivetilgang til enheter som er konfigurert i en annen organisasjon	Bare stasjoner med identifikasjonsfelt som samsvarer med datamaskinens identifikasjonsfelt, vil få skrivetilgang. Disse feltene er definert av gruppepolicyinnstillingen "Oppgi unike identifikatorer for organisasjonen din".

BitLocker-tilstand

Her kan du se den nåværende statusen for BitLocker-krypterte stasjoner

C [OS Drive]
Krypteringsstatus
Kryptert (%)
Beskyttelsesstatus
Krypteringsmetode
Nøkkelbeskyttere
Gjenoppretting av passord

Ved å klikke på knappen "Roter gjenopprettingspassord" kan du rotere BitLocker-gjenopprettingspassordet.

Sertifikatforvaltning

Sertifikatliste

Her er en liste over sertifikater som er installert på enheten som vises.

Sertifikatkonfigurasjon

Her kan du konfigurere sertifikater og hvordan de skal installeres på enheten.

Pålitelig sertifikat	
Beskrivelse	Beskrivelse av sertifikat
Omfang	Omfanget av sertifikatdistribusjon: Nåværende bruker vs. enhet
Sertifikatlager	"Untrusted Certificates" er bare tilgjengelig fra og med Windows 10, versjon 1803
Sertifikatfil	Last opp en PKCS#1-fil

Identitetssertifikat			
Beskrivelse	Beskrivelse av sertifikat		
Omfang	Omfanget av sertifikatdistribusjon: Nåværende bruker vs. enhet		
Nøkkelplassering	Tilbyderen av nøkkellagring som den private nøkkelen skal installeres på.		
		TPM. Mislykkes hvis ingen TPM er til stede	
	TPM. Hvis det ikke finnes noen TPM, går du tilbake til Software KSP		
	Leverandør av programvare for lagring av nøkler		Merk privat nøkkel som eksporterbar
	Windows Hello for bedrifter	Beholderens navn	Angir navnet på Windows Hello for Business (tidligere kjent som Microsoft Passport for Work).
		PIN-meldingstekst	Angir den egendefinerte teksten som skal vises på PIN-meldingen i Windows Hello for Business under sertifikatregistrering.
Legitimasjon	Last opp en PKCS#12-fil		

SCEP

Beskrivelse	Beskrivelse av SCEP Server		
Omfang av distribusjon	Omfang av sertifikatdistribusjon: Aktuell enhet vs. bruker		
URL-adresser til SCEP-servere	En eller flere servere som utsteder sertifikater via SCEP		
Emne	Representasjon av et X.500-navn. F.eks. "C=USA, O=Microsoft Corporation, CN=foo, 1.2.5.3=bar"		
Alternative navn på emnet	Type	E-postadresse	
		DNS	
		URI	
		Brukerens hovednavn (UPN)	
CA Fingeravtrykk	SHA1-fingeravtrykket til sertifikatutstederens sertifikat. E.g. 31:8F:1E:78:5C:D5:12:9F:7E:3B:AD:F3:1C:C0:19:03:96:43:A9:E5		
Gyldighetsperiode enheter	Dager, måneder eller år		
Gyldighetsperiode			
Utfordring	Brukes som forhåndsdelt hemmelighet for automatisk registrering		
Nye forsøk	Antall ganger enheten skal prøve på nytt hvis serveren sender et PENDING-svar. Standardverdien er 5. Maksimumsverdien er 30.		
Forsinkelse på nytt forsøk	Antall minutter å vente før du prøver på nytt. Standardverdien er 5. Minimumsverdien er 1.		
Nøkkelstørrelse	Nøkkelstørrelse i bits		
Hash-algoritme	Familie av hashalgoritmer		
Nøkkelbruk	Utvidelsen for nøkkelbruk definerer formålet (f.eks. kryptering, signatur) med nøkkelen i sertifikatet. Minst ett av alternativene "Digital signatur" eller "Nøkkelkryptering" må være valgt.		
Utvidet bruk av nøkler	Angir bruk av utvidede nøkler, avhengig av SCEP-serverens konfigurasjon. Angi listen over tilsvarende OID-er, f.eks. 1.3.6.1.5.5.7.3.2 (Klientautentisering)		
Nøkkelplassering	Tilbyderen av nøkkellagring som den private nøkkelen skal installeres på.		
		TPM. Mislykkes hvis ingen TPM er til stede	
	TPM. Hvis det ikke finnes noen TPM, går du tilbake til Software KSP		

	Leverandør av programvare for lagring av nøkler			
	Windows Hello for bedrifter	Beholderens navn	Angir navnet på Windows Hello for Business (tidligere kjent som Microsoft Passport for Work).	
		PIN-meldingstekst	Angir den egendefinerte teksten som skal vises på PIN-meldingen i Windows Hello for Business under sertifikatregistrering.	

Administrasjon av tilkoblinger

Wifi

Med denne innstillingen kan du utføre forhåndskonfigurasjonen av sluttbrukernes enheter for tilgang til interne aksesspunkter

Identifikator for tjenestesett (SSID)	SSID til nettverket som tilkoblingen skal opprettes til
Auto Join	Aktiver automatisk tilkobling til nettverket
Skjult nettverk	Aktiver, i tilfelle AP-et ikke kringkaster SSID

Sikkerhetstype

Etablere AP-sikkerhetstype

WEP Open System	
Passord	Passord for AP

WPA PSK	
Passord	Passord for AP

WPA EAP	
Autentiseringstype	Autentiseringstype, kun mulig med "PEAP-MSCAHPv2"
Rask tilkobling	Enheter kan bytte mellom aksesspunkter uten å måtte autentisere seg på nytt
Tilgang for gjester	Brukeren har ingen konto og bør derfor registrere seg som gjest
Karantenekontroller	Klienten må utføre NAP-kontroller (Network Access Protection) og dele resultatene med systemet, som deretter avgjør om klienten kan koble seg til
Krever kryptobinding	Autentisering er bare mulig via Crypto Binding
Servervalidering	Klienten sjekker om serversertifikatet er gyldig. Hvis dette er tilfelle, vil en tilkobling bli opprettet
Spør etter sertifikater	Tillater brukeren å godta sertifikater som ikke er klarerte
Servernavn	Gir mulighet til å vise navnet på RADIUS-serveren som tilbyr nettverksautentisering og autorisasjon

WPA2-PSK	
Passord	AP-passord

WPA2 EAP	
Autentiseringstype	Autentiseringstype, kun mulig med "PEAP-MSCAHPv2"
Rask tilkobling	
Tilgang for gjester	
Karantenekontroller	Aktiverer nettverkstilgangsbeskyttelsen NAP
Krever kryptobinding	Autentisering er bare mulig via Crypto Binding
Servervalidering	
Spør etter sertifikater	Ber om et validert serversertifikat, navn eller en rotsertifikatgodkjenning (CA)
Servernavn	Liste over servere som skal være klarert av enhetene
Ingen	Ingen etablert sikkerhet
Bruk proxy-server	Bruk av en proxy-server
Serveradresse	Adresse til proxy-server
Serverport	Proxy-serverens serverport

Bruk proxy-server

Aktiver bruk av proxy-server.

Serveradresse	Proxy-serveradresse som brukes av dette nettverket.
Serverport	Proxy-serverport som brukes av dette nettverket.

Begrensninger for wifi

Her kan du definere ulike Wifi-begrensninger.

Tillat WiFi	Tillat/nekt WiFi
Tillat deling på Internett	Tillat bruk av et hotspot
Tillat automatisk tilkobling til WiFi Sense Hot Spots	Tillat automatisk tilkobling til WiFi Sense Hot Spots
Tillat manuell WiFi-konfigurasjon	Tillat brukeren å koble seg til WiFi-nettverk som ikke er definert av AppTec
WLAN-skannefrekvens	Fastsetter intervallet for WLAN-skanning. En høyere verdi øker evnen til å gjenkjenne WIFI-nettverk.

VPN

Utfør de riktige innstillingene her for å konfigurere VPN-tilkoblinger

Navn på tilkobling	Angitt navn på tilkoblingen		
VPN-type	En VPN-tilkobling per app brukes til å sikre trafikken til visse apper.		
	VPN	Alltid på	Dette vil automatisk koble til VPN-et ved pålogging og forbli tilkoblet til brukeren kobler fra manuelt.
	VPN per app	VPN-apper	Definer apper som bruker denne VPN-tilkoblingen
		Låsing per app	Per-App Lockdown gjør at de valgte appene kun har tilkobling via denne VPN-tilkoblingen. Denne funksjonen er avhengig av Windows Defender-brannmuren.
	WIP-profil	WIP-domene for denne tilkoblingen	Enterprise ID, som er nødvendig for å koble denne VPN-profilen til en Windows Information Protection (WIP)-policy

Type tilkobling

AppTec360 VPN	
For "AppTec360 VPN" er det nødvendig at app-sideloading er tillatt. Aktiver "Tillat sidelasting av apper" i "Security Management" → "Restriksjonsinnstillinger" → "Enhetsfunksjonalitet".	
Gateway-konfigurasjon	Hvis du vil konfigurere en VPN-tilkobling med svartelisting, må du velge en VPN-konfigurasjon med en spesifisert DNS-server. Du kan konfigurere en VPN-konfigurasjon i "Generelle innstillinger" → "Universal Gateway" → "VPN-innstillinger".

IKEv2		
Tjenere	Liste over VPN-servere	
Enhetstunnel	Aktiver tilkobling før pålogging av bruker.	
Autentiseringsmetode	EAP	EAP XML
	Maskinsertifikater	
Krypteringsalgoritme		
Algoritme for integritetskontroll		
Diffie-Hellman-gruppe		
Algoritme for krypteringstransformasjon		
Algoritme for autentiseringstransformasjon		
Perfekt forward secrecy-gruppe (PFS)		

PPTP		
Tjenere	Liste over VPN-servere	
Autentiseringsmetode	EAP	EAP XML

L2TP		
Tjenere	Liste over VPN-servere	
Autentiseringsmetode	EAP	EAP XML
Krypteringsalgoritme		
Algoritme for integritetskontroll		
Diffie-Hellman-gruppe		
Algoritme for krypteringstransformasjon		
Algoritme for autentiseringstransformasjon		
Perfekt forward secrecy-gruppe (PFS)		

Automatisk		
Tjenere	Liste over VPN-servere	
Autentiseringsmetode	EAP	EAP XML

Generiske VPN-konfigurasjoner

Husk legitimasjon ved hver pålogging	
Registrer IP-adresser med intern DNS	
Regler for filtrering av nettverkstrafikk	Begrens VPN-tilkoblingen til det definerte settet med regler.
Liste over DNS-suffikser	DNS-suffikser som skal legges til i DNS-søkelisten for ruting av korte navn.
Regler for navneløsningsregler (NRPT)	NRPT-regler (Name Resolution Policy Table) definerer hvordan DNS løser opp navn når den er koblet til VPN-et.
Pålitelig nettverksdeteksjon	Liste over DNS-suffikser for identifisering av klarerte nettverk.
Delt tunnelering	Delt tunnelering betyr at trafikken kan gå over et hvilket som helst grensesnitt som bestemmes av nettverksstakken.
Delte tunneleringsruter	Liste over ruter som skal legges til i rutingstabellen for VPN-grensesnittet.
Proxy-oppsett	Konfigurerer proxyen som brukes med dette nettverket
Fullmaktsadresse	Proxy-serveradresse som et fullt kvalifisert vertsnavn eller en IP-adresse.
Havn	Proxy-serverport.
URL for automatisk proxy-konfigurasjon	URL for å hente proxy-innstillingene automatisk.

VPN-begrensninger

Her kan du definere ulike VPN-begrensninger.

Tillat VPN-innstillinger	Denne retningslinjen tillater/forbyr brukeren å deaktivere og endre VPN-innstillingene
Tillat VPN over mobilnettet	Tillater/forbyr enheten å opprette en VPN-tilkobling hvis enheten bruker mobildata
Tillat VPN-roaming over mobilnettet	Tillater/forbyr enheten å opprette en VPN-tilkobling, hvis enheten roamer

Bluetooth

Her kan du bestemme om Bluetooth skal være tillatt/forbudt.

Tillat Bluetooth	Aktiver/deaktiver Bluetooth

PIM-administrasjon

Exchange Active Sync

Oppsett av ActiveSync-kontoen på sluttbrukerens enhet

Kontonavn	Navn på e-postkonto
Serverens vertsnavn	Serveradresse/FQDN
Domenenavn	Serverens domene
E-postadresse	E-postadresse
Brukernavn	Brukernavn
Brukerpassord	Eventuelt kan du allerede knytte et passord til brukeren her
Bruk SSL	Bruk SSL-tilkobling
Synkroniseringsintervall	Her kan synkroniseringsintervallet fastsettes Manuell synkronisering = Brukeren må laste ned e-postene sine og utføre en manuell synkronisering
Aldersfilter for e-post	Hvor lang tid det tar før e-postene skal synkroniseres Ingen filter = ubegrenset
Loggnivå	Fastsettelse av loggnivåer for ActiveSync-trafikken
Synkroniser e-post	Aktivert = e-poster synkroniseres
Synkroniser kontakter	Aktivert = kontaktene er synkronisert
Synkroniser kalenderen	Aktivert = kalenderen er synkronisert
Synkroniser oppgaver	Aktivert = oppgavene er synkronisert

E-post

Etablering av POP3/IMAP4-kontoer på sluttbrukerens enhet.

Kontobeskrivelse	Navn på e-postkonto
Avsendernavn	Vises avsendernavn
Domenenavn	Domenenavn for e-postkontoen
E-postadresse	Brukerens e-postadresse
Brukernavn	Brukernavn
Brukerpassord	Eventuelt kan du allerede knytte et passord til brukeren her
Alternativ legitimasjon for utgående server	Her kan det defineres om det kreves andre legitimasjonsopplysninger for den utgående serveren
Utgående domenenavn	Utgående domenenavn
Brukernavn for utgående server	Brukernavn på utgående server
Passord for utgående server	Passord for utgående server
E-postprotokoll	POP3 eller IMAP4, kan brukes som protokoll
Vertsnavn for innkommende e-postserver	Vertsnavn for innkommende e-postserver
Bruk SSL for innkommende e-post	Bruk SSL for innkommende e-post
Vertsnavn for utgående e-postserver	Vertsnavn for utgående e-postserver
Bruk SSL for utgående e-post	Bruk SSL for utgående e-post
Autentisering av utgående server	En utgående serverautentisering er påkrevd
Synkroniseringsintervall	Her kan synkroniseringsintervallet fastsettes Manuell synkronisering = Brukeren må laste ned e-postene sine og utføre en manuell synkronisering
Aldersfilter for e-post	Hvor lang tid det tar før e-postene skal synkroniseres Ingen filter = ubegrenset

App-administrasjon

Enterprise App Manager

Installerte apper

Her er en liste over appene som for øyeblikket er installert på enheten som vises.

Obligatoriske apper

Her kan du konfigurere en liste over apper som er obligatoriske på enheten.

Denne listen sjekkes hver gang enheten kobles til MDM, og alle apper på listen som ikke er installert på enheten, installeres, uavhengig av om appen er avinstallert eller aldri har vært installert før.

Du kan laste opp Windows 10 In-House-apper og deretter legge dem til i denne listen, eller du kan legge til Microsoft Office-konfigurasjoner som må konfigureres på forhånd i "Generelle innstillinger" > "Appadministrasjon" > "Microsoft Office".

Sys App Restriksjoner

Innboks-apper
Tillat alarmer og klokke
Tillat kalkulator
Tillat kamera
Tillat kontaktstøtte
Tillat Cortana
Tillat filutforsker
Tillat å komme i gang
Tillat Groove Music
Tillat kart
Tillat meldinger
Tillat Microsoft Edge
Tillat filmer og TV
Tillat penger
Tillat nyheter
Tillat OneDrive
Tillat OneNote
Tillat Outlook-kalender og e-post
Tillat folk
Tillat telefon
Tillat bilder
Tillat Powerpoint
Tillat innstillinger
Tillat Skype
Tillat sport
Tillat butikk
Tillat stemmeopptaker
Tillat lommebok
Tillat vær

Tillat Windows Feedback Hub
Tillat Word
Tillat Xbox

Innstilling av sider
Tillat kontoer på arbeidsplassen
Tillat avansert informasjon
Tillat apper-hjørnet
Tillat blokkering og filtrering
Tillat fargeprofil
Tillat kjøremodus
Tillat e-post og kontoer
Tillat Equalizer
Tillat tastatur
Tillat navigasjonslinje
Tillat flymodus for nettverk
Tillat nettverksdeling på Internett
Tillat nettverkstjenester
Tillat Wi-Fi-nettverk
Tillat PC-system Bluetooth
Tillat vurdering av enheten din
Tillat gjenoppretting av oppdatering
Tillat deling
Tillat start
Tillat tid Språk
Tillat tid Region
Tillat Windows standard låseskjerm
Tillat jobb- eller skolekonto

Svart- og hvitelisting

Under "Svart- og hvitelisting" kan du velge mellom modusene "Whitelist" og "Blacklist".

Hviteliste	Bare apper og tjenester som er lagt til i listen, kan installeres på sluttbrukerens enhet. Hvis disse allerede er forhåndsinstallert på sluttbrukerens enhet, vil de bli aktivert og stilt inn slik at brukeren kan kjøre dem.
	Alle andre apper som ikke er lagt til i listen, kan ikke installeres på sluttbrukerens enhet. Hvis disse allerede er forhåndsinstallert på sluttbrukerens enhet, blir de deaktivert og innstilt slik at brukeren ikke kan kjøre dem.
Svarteliste	Apper og tjenester som legges til i listen, kan ikke installeres på sluttbrukerens enhet. Hvis disse allerede er forhåndsinstallert på sluttbrukerens enhet, blir de deaktivert og innstilt slik at brukeren ikke kan kjøre dem.
	Alle andre apper som ikke er lagt til i listen, kan installeres på sluttbrukerens enhet. Hvis disse allerede er forhåndsinstallert på sluttbrukerens enhet, vil de bli aktivert og stilt inn slik at brukeren kan kjøre dem.

Via kan du legge til flere apper eller tjenester i listen over brukte apper.

Via kan du legge til flere apper eller tjenester i den inaktive listen.

Du kan enten legge til en app fra "Windows App Store" eller angi en "App Identifier" direkte for å legge den til i svart- eller hvitelisten.

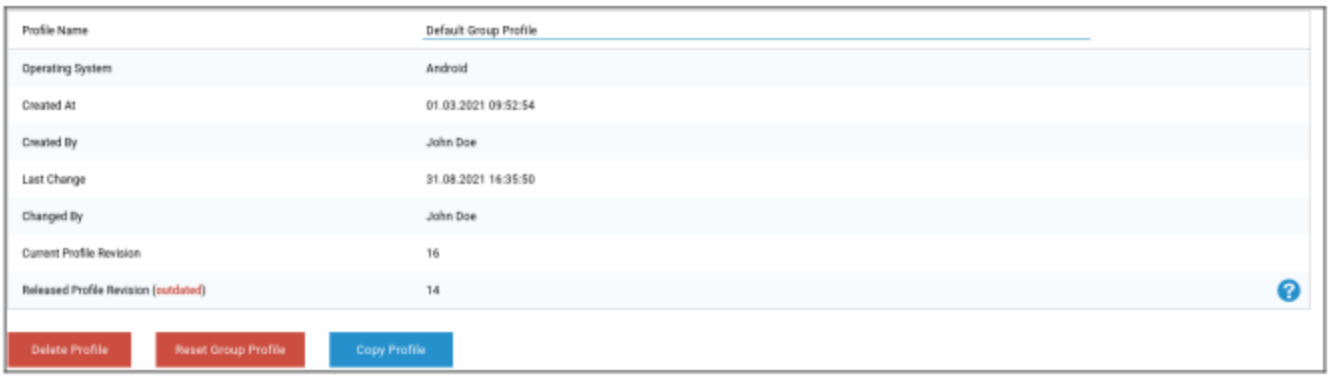
MacOS-konfigurasjon

Avhengig av om du har valgt en profil eller en enhet, er visningen og underpunktene forskjellige - vær oppmerksom på dette!

Generelt

Oversikt over gruppeprofiler (kun på gruppenivå)

Når du åpner en gruppeprofil, får du en rask oversikt over profilen.



Profilnavn	Navn på profilen (kan endres her)
Operativsystem	Operativsystemet profilen er beregnet på
Opprettet på	Tidspunktet for skapelsen
Opprettet av	Skaperen av profilen
Siste endring	Tidspunkt for siste endring av profilen
Endret av	Konto som gjorde de siste endringene
Nåværende profilrevisjon	Revisjon av lagret profilstatus
Utgitt profilrevisjon	Tilordnet profilrevisjon ("Tilordne nå"). Hvis etiketten viser "(utdatert)" bak teksten, betyr det at du har lagret profilen, men ikke tilordnet den ennå, slik at enhetene fortsatt vil få en eldre versjon.

Enhetsoversikt (kun på enhetsnivå)

En kortfattet oversikt over enheten.

Enhetens navn	Enhetens navn
Modell	Modell
Operativsystem	Operativsystem
Serienummer	Serienummeret til enheten
Eierskap til enheten	Den konfigurerte eierskapstypen
Enhetstype	Type enhet
Overensstemmende	Viser om enheten er kompatibel
IP-adresse	IP-adressen enheten er koblet til serveren fra
Sist sett	Tidspunkt for siste tilkobling fra enheten
Siste fremstøt	Tidspunkt for siste push sendt til enheten
Oppdrag	Her kan du flytte enheten til en annen bruker eller gruppe

Konfigureringsrevisjon (kun på enhetsnivå)

Her får du en oversikt over hvilken gruppeprofil som er tilordnet enheten.

Hvis du klikker på gruppeprofilen, får du direkte tilgang til profilen og kan utføre innstillinger.

Med symbolet kan du tilbakestille de tilordnede appene til gruppeprofilens innstillinger.

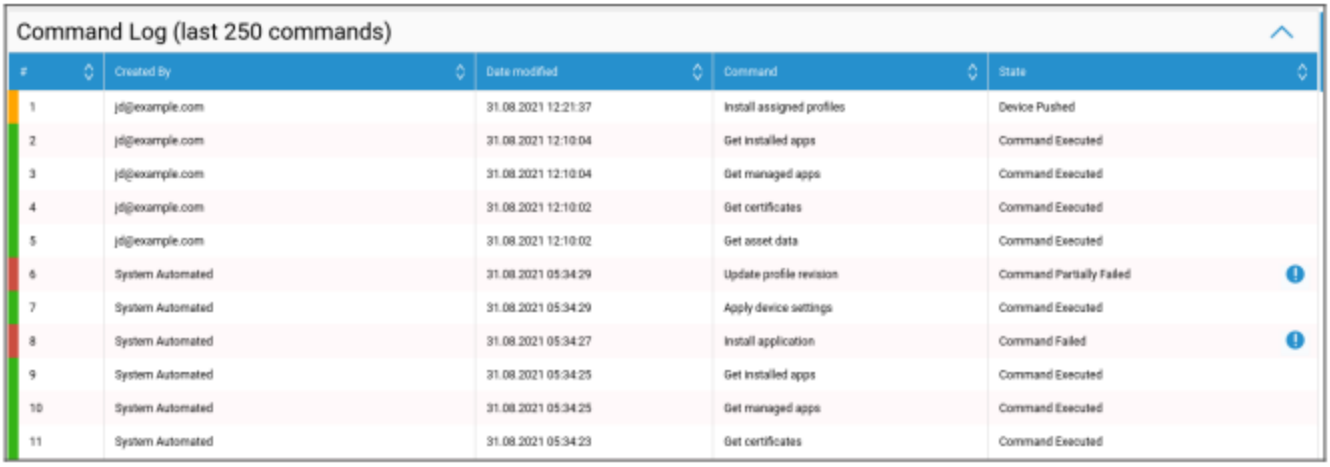
Med symbolet kan du tilbakestille enhetsprofilen slik at den ikke har noen innstillinger i det hele tatt.

"Nyere revisjon tilgjengelig" indikerer at gruppeprofilen har blitt endret og lagret, men ikke tilordnet. Gruppeprofilen må tilordnes med "Tilordne nå" på gruppenivå for at endringene skal gjelde for enhetene.

Enhetslogg (kun på enhetsnivå)

Kommandologg

Her kan du se hvilke kommandoer som er utstedt for enheten, og hvilken status de har.



Kommandoer som opprettes av "System Automated", opprettes automatisk av systemet.

Mulige kommandostatuser

Enhet skjøvet	En push-forespørsel har blitt sendt til push-tjenesten (f.eks. APNS) for å be enheten om å koble seg tilbake til EMM-serveren.
Kommando opprettet	Kommandoen ble opprettet i systemet.
Kommando sendt	Kommandoen ble sendt til enheten etter at den ble koblet til serveren.
Kommando utført	Kommandoen ble vellykket utført.
Kommando mislyktes	Kommandoen mislyktes. *
Kommandoen mislyktes delvis	Avhengig av enhetens operativsystem kan enkelte kommandoer bli gruppert sammen. I dette mislyktes noen deler av denne kommandogruppen. *
Kommando utført, men mislyktes til slutt	Kommandoen ble utført, men kanskje ikke.
Kommando Repushed	Kommandoen ble sendt på nytt av en bruker.
Kasseres	Kommandoen ble forkastet. For eksempel fordi den ble erstattet av en annen kommando, eller fordi enheten ble registrert på nytt og gamle kommandoer ble fjernet.

*Hvis det er et utropstegn bak meldingen, kan du få mer informasjon ved å holde musepekeren over ikonet.

Asset Management (kun på enhetsnivå)

Enhetsinfo

Modellnummer	Modellnummer
Vertsnavn	Vertsnavn
Lokalt vertsnavn	Lokalt vertsnavn
Operativsystem	Operativsystem
OS-versjon	OS-versjon
UDID	UDID
Ledig / totalt minne	Ledig / totalt minne

WiFi

IP-adresse	IP-adresse
WiFi MAC	WiFi MAC

Cellular

Telefonnummer	Telefonnummer
Roaming-status	Roaming-status
Roaming (tale/data)	Roaming (tale/data)
IP-adresse	IP-adresse
Operatør/transportør	Operatør/transportør
SIM-operatørens nettverk	Bærernettverk
Transportørversjon	Transportørversjon
ICCID	ICCID
Nåværende MCC/MNC	Nåværende MCC/MNC
SIM MCC/MNC	SIM MCC/MNC

Bluetooth

Bluetooth MAC	Bluetooth MAC

Oppdateringsadministrasjon (kun på enhetsnivå)

Oppdater informasjon

Denne fanen viser informasjon om systemoppdateringsinnstillingene på enheten.

Autocheck aktivert	Hvis systemet automatisk søker etter oppdateringer.
Automatisk app-oppdatering aktivert	Hvis systemet skal installere appoppdateringer automatisk.
Automatiske OS-oppdateringer aktivert	Hvis systemet vil installere systemoppdateringer automatisk.
Automatiske sikkerhetsoppdateringer aktivert	Hvis systemet skal installere sikkerhetsoppdateringer automatisk.
App-oppdatering av bakgrunnsnedlasting aktivert	Hvis systemet laster ned appoppdateringer i bakgrunnen.
Katalog-URL	URL-adressen til programvareoppdateringskatalogen som klienten bruker.
Er standard katalog	Hvis "ja", er Catalog standardkatalogen.
Utfør periodisk kontroll	Hvis "ja", start en ny skanning.
Forrige skannedato	Datoen for den siste skanningen av programvareoppdateringen.
Tidligere skanneresultat	Resultatkoden for siste skanning av programvareoppdatering.

Sikkerhetsstyring

Tyverisikring

Tørk og lås

Full Wipe	Send en kommando for å tilbakestille enheten til fabrikkinnstillingene
Enterprise Wipe	Fjern MDM fra enheten og fjern alle MDM-data (f.eks. kontoer, apper)
Låseskjerm	Få enheten til å gå tilbake til låseskjermen

Sikkerhetskonfigurasjon

Passord

Deaktivering av kode tillatt	Bestemmer om brukeren skal tvinges til å angi en PIN-kode. Ved å angi denne verdien (og ikke andre) tvinges brukeren til å angi en passordkode, uten at det stilles krav til lengde eller kvalitet.
Tillat enkel verdi	Tillat brukeren å bruke de samme, eskalerende og reduserende nummerstrengene (f.eks. 1234, 1111)
Krever alfanumerisk verdi	Passordene må inneholde minst én bokstav
Minimum lengde på passordet	Minimal passordlengde
Minimum antall komplekse tegn	Minimum antall alfanumeriske symboler i passordet
Maksimal alder på passordet	Antall dager etter at passordet må endres
Maksimal automatisk låsing	Maksimum tid etter hvilken enheten er låst
Maksimal frist for låsing av enheten	Hvor lenge enheten kan være låst uten å bli bedt om passord ved opplåsing
Maksimal alder på passordet (1-730 dager, eller ingen)	Dager etter hvilke passordet må endres
Passordhistorikk (1-50 passord, eller ingen)	Antall unike passord før gjenbruk

Sertifikat

PKCS#1	
Beskrivelse	Skriv inn en beskrivelse for sertifikatet
Legitimasjon	Last opp en pkcs1-fil

PKCS#12	
Beskrivelse	Skriv inn en beskrivelse for sertifikatet
Legitimasjon	Last opp en pkcs12-fil

Begrensningsinnstillinger

Enhetens funksjonalitet

Tillat kamera	Tillat bruk av kameraet
Tillat Game Center	Hvis den er falsk, deaktiveres Game Center, og ikonet fjernes fra startskjermen.
Tillat flerspillerspill	Når den er falsk, forbyr den flerspillerspill.
Tillat å legge til Game Center-venner	Når false, forbyr det å legge til venner i Game Center.
Tillat iCloud Photo Library	Hvis satt til false, deaktiveres iCloud Photo Library. Alle bilder som ikke er fullstendig lastet ned fra iCloud Photo Library til enheten, vil bli fjernet fra lokal lagring.
Tillat Touch ID	Hvis false, forhindrer Touch ID fra å låse opp en enhet.

iCloud

Blokker visse funksjoner under iCloud-paring

Tillat synkronisering av dokumenter	Tillat synkronisering av dokumenter
Tillat synkronisering av iCloud-nøkkelring	Tillat synkronisering av iCloud-nøkkelring
Tillat iCloud-notater	Når false, avviser MacOS iCloud Notes-tjenester
Tillat iCloud BTMM	Når false, deaktiveres MacOS Tilbake til min Mac iCloud-tjenesten.
Tillat iCloud FMM	Når false, deaktiveres MacOS Find My Mac iCloud-tjenesten.
Tillat iCloud-bokmerker	Når false, deaktiveres MacOS iCloud Bookmark-synkronisering.
Tillat iCloud Mail	Når false, avviser MacOS Mail iCloud-tjenester.
Tillat iCloud-kalender	Når false, avviser MacOS Cloud iCloud-tjenester.
Tillat iCloud-påminnelser	Når false, deaktiveres iCloud-påminnelsestjenester.
Tillat iCloud Addressbook	Når false, avviser MacOS iCloud Address Book-tjenester.

Mediehåndtering

Løs ut ved utlogging	Mata ut alle flyttbare medier ved utlogging
Tillat nettverk	Tillat tilgang for nettverksmedier
Tillat intern disk	Tillat tilgang for intern disk.
Krev autentisering	Krev autentisering for bruk av dette mediet
Kun lesing	Brukeren kan bare lese data fra mediet
Tillat ekstern disk	Tillat tilgang for ekstern disk.
Krev autentisering	Krev autentisering for bruk av dette mediet
Kun lesing	Brukeren kan bare lese data fra mediet
Tillat bruk av diskbilder	Tillat tilgang for bilder.
Krev autentisering	Krev autentisering for bruk av dette mediet
Kun lesing	Brukeren kan bare lese data fra mediet
Tillat bruk av DVD-RAM-skiver	Tillat tilgang for DVD-RAM-disk.
Krev autentisering	Krev autentisering for bruk av dette mediet
Kun lesing	Brukeren kan bare lese data fra mediet
Tillat bruk av DVD-er	Tillat tilgang for DVD-disk.
Krev autentisering	Krev autentisering for bruk av dette mediet
Tillat bruk av CD-er	Tillat tilgang for CD-disk.
Krev autentisering	Krev autentisering for bruk av dette mediet

Administrasjon av tilkoblinger

Wi-Fi

Her kan du legge til og konfigurere Wi-Fi-tilkoblinger

Identifikator for tjenestesett (SSID)	SSID for nettverket som tilkoblingen skal opprettes til
Auto Join	Aktiver automatisk tilkobling for nettverket
Skjult nettverk	Aktiver, i tilfelle AP-et ikke kringkaster SSID
Proxy-oppsett	Konfigurering av en proxy for hvert aksesspunkt
Ingen	Ikke bruk en proxy-server
Manuell	Opprett en manuell proxy
URL til proxy-server	Adresse for tilgang til proxy-innstillinger
Havn	Opprett porten for proxyen
Autentisering	Brukernavn for autentisering på proxyen
Passord	Passord for autentisering på proxyen
Automatisk	Opprett en proxy automatisk
URL til proxy-server	URL for proxy-innstillingsfilen
Sikkerhetstype	Opprett sikkerhetstype for AP-et
WEP	
Passord	Passord for AP
WPA/WPA2	
Passord	Passord for AP
WEP Enterprise - WPA / WPA WPA2 Enterprise / Enhver bedrift	Se tabell Feil: Referansekilden ble ikke funnet nedenfor
Ingen	Etablerer ingen sikkerhet
Deaktiver randomisering av MAC-adresse	Deaktiverer randomisering av MAC-adresser for det aktuelle Wi-Fi-nettverket mens det er tilknyttet nettverket. Dette viser også en personvernadvarsel i Innstillinger som indikerer at nettverket har redusert personvernbeskyttelse.

Wi-Fi-konfigurasjon for bedrifter

Merk: Bare tilgjengelig når "Security Type" er satt til en Enterprise Type.

Protokoller	Autentiseringsprotokoll som støttes på målnettverket
TLS	Aktivere/deaktivere bruk
TTLS	Aktivere/deaktivere bruk
Indre autentiseringer	Autentiseringsprotokoll som skal brukes: PAP, CHAP, MSCHAP, MSCHAPv2
LEAP	Aktivere/deaktivere bruk
PEAP	Aktivere/deaktivere bruk
EAP-FAST	Aktivere/deaktivere bruk
EAP-SIM	Aktivere/deaktivere bruk
Bruk PAC	Bruk av PAC (Protected Access Control)
Avsetning PAC	Konfigurasjon av Provision PAC
Lever PAC anonymt	Anonym levering av PAC
Autentisering	
Brukernavn	Brukernavn for autentisering
Ikke bruk Per tilkobling Passord	Ikke bruk passord per tilkobling
Passord	Passordet som skal brukes
Identitetssertifikat	Last opp/velg autentiseringssertifikat
Ytre identitet	Identitet som kan ses utenfra
Tillit	
Pålitelig sertifikat 1	Last opp det første klarerte sertifikatet
Pålitelig sertifikat 2	Last opp et annet klarert sertifikat
Pålitelig sertifikat 3	Last opp et tredje klarert sertifikat
Betrodd server Navn på sertifikater	Navnene på de forventede serversertifikatene (i en kommaseparert liste)

VPN

Avhengig av hvilken tilkoblingstype som er valgt, kan ulike felt være synlige.

Navn på tilkobling	Navn på VPN-profilen
VPN-type	
VPN	All nettverkstrafikk på enheten blir rutet via en VPN-forbindelse.
Type tilkobling	Etablere VPN-tilkoblingstype
IPsec (Cisco)	IPsec-protokoll fra Cisco
L2TP	L2TP-protokollen
Tilpasset SSL	Tilkobling via egendefinert SSL
IKEv2	IKEv2-protokollen
Proxy-oppsett	Konfigurering av en proxy for VPN-tilkoblingen
Ingen	Opprett ingen fullmakt
Manuell	Opprett en proxy manuelt
URL til proxy-server	Adresse for tilgang til proxy-innstillinger
Havn	Opprett porten for proxyen
Autentisering	Brukernavn for autentisering hos proxyen
Passord	Passord for autentisering på proxyen
Automatisk	Opprett en proxy automatisk
URL til proxy-server	URL for tilgang til proxy-innstillingene

HTTP-proxy

Proxy Type	
Manuell	Opprett en proxy manuelt
URL til proxy-server	Adresse for tilgang til proxy-innstillingene
Havn	Etablere proxy-port
Autentisering	Brukernavn for autentisering hos proxyen
Passord	Passord for autentisering på proxyen
Automatisk	Opprett en proxy automatisk
Proxy PAC URL	Proxy PAC URL
Tillat direkte tilkobling hvis PAC ikke kan nås	Tillat direkte tilkobling (uten VPN) hvis PAC ikke kan nås
Tillat omgåelse av proxy for å få tilgang til lukkede nettverk	Tillat omgåelse av proxy for å få tilgang til interne nettverk

AirPrint

IP-adresse	Skriverens IP-adresse
Ressurssti	Definert vei til AirPrint-enheten

AirPlay

Enhetens navn	Enhetens navn
Passord	Passord for sammenkobling
Hviteliste	Definer en liste over enheter som enheten utelukkende kan pare seg med

PIM-administrasjon

Exchange Active Sync

Kontonavn	Navn på kontoen.
E-postadresse	Adressen til kontoen (f.eks. max@company.com)
Serverens vertsnavn	Internt vertsnavn
Innloggingsnavn	"Domain" og "Login Name" må være tomme for at enheten skal spørre etter bruker.
Domene	"Domain" og "Login Name" må være tomme for at enheten skal spørre etter bruker. Hvis en ACL Gateway-konfigurasjon er aktivert og feltet Domain ikke er tomt, vil AppTec360 Universal Gateway autentisere enheten med følgende navn "Domain\Login Name"
Passord	Passordet for kontoen (f.eks. secretUserPassword)
Tidligere dager med Mail to Sync	Antall siste dager med e-post som skal synkroniseres
Bruk SSL	Bruk SSL for intern Exchange-vert
Avansert alternativ	Vis avanserte alternativer
Serverport	Intern port
Serverbane	Intern sti
Eksternt vertsnavn	Ekstern vert
Ekstern port	Ekstern port
Ekstern sti	Ekstern sti
Bruk SSL for eksterne Utvekslingsvert	Bruk SSL for ekstern Exchange-vert

E-post

Oppsett av POP3-/IMAP-kontoer på sluttbrukerens enhet

Kontobeskrivelse	Navn des E-postkontoer
Kontotype	
IMAP	
Stiprefiks	Stiprefikset for spesielle mapper
POP	
Brukerens visningsnavn	Brukerens visningsnavn
E-postadresse	Brukerens e-postadresse

Innkommende post	Innkommende serverinnstillinger
E-postserveradresse	Adresse til e-postserver
Port for e-postserver	Port for e-postserver
Brukernavn	Respektive brukernavn
Autentiseringstype	Autentiseringstype
Ingen	Ingen autentiseringstype
Passord (kun på enhetsnivå)	Melding om passord
MDM-utfordring-svar	
NTLM	NTLM-autentisering
HTTP MD5-digest	
Bruk SSL	Bruk SSL, om nødvendig

Utgående post	Innstillinger for utgående server
E-postserveradresse	E-postserveradresse
Port for e-postserver	Port for e-postserver
Brukernavn	Respektive brukernavn
Autentiseringstype	
Ingen	Ingen autentiseringsmetode
Passord (kun på enhetsnivå)	Melding om passord
MDM Utfordring-Svar	
NTLM	NTLM-autentisering
HTTP MD5-digest	
Bruk SSL	Bruk SSL, om nødvendig
Utgående passord er det samme som innkommende	Utgående passord er det samme som innkommende
Brukes kun i post	Aktiver, hvis alle utgående e-poster skal sendes via Mail-appen

CalDav

Konfigurere oppsett og distribusjon av en CalDav-konto

Kontobeskrivelse	Visningsnavn på kontoen
Vertsnavn	Vertsnavn og/eller IP-adresse
Havn	Port til CalDav-kontoen
Hoved-URL	Kontoens hoved-URL
Brukernavn	Respektive CalDav-brukernavn
Passord (kun på enhetsnivå)	Respektive CalDav-passord
Bruk SSL	Bruk SSL, om nødvendig

CardDav

Konfigurere oppsett og distribusjon av en CardDav-konto

Kontobeskrivelse	Visningsnavn på kontoen
Vertsnavn	Vertsnavn og/eller IP-adresse
Havn	Porten til CardDav-kontoen
Hoved-URL	Kontoens hoved-URL
Brukernavn	Respektive CardDav-brukernavn
Passord (kun på enhetsnivå)	Respektivt CardDav-passord
Bruk SSL	Bruk SSL, om nødvendig

LDAP

I dette området setter du opp en LDAP-tilkobling for å muliggjøre en dynamisk sertifikatutveksling mellom sluttbrukerenheten og Active Directory.

Vær oppmerksom på at den valgte brukeren må ha lesetillatelse.

Kontobeskrivelse	Kontobeskrivelse
Brukernavn på konto	Bruker for LDAP-tilgang
Passord for konto	Passord for LDAP-tilgang
Kontoens vertsnavn	LDAP-server Vertsnavn/IP-adresse
Bruk SSL	Bruk SSL, om nødvendig

I den andre delen kan du definere individuelle filtre for søk i LDAP-registeret.

Beskrivelse	Omfang	Søkebase
Filterbeskrivelse	Søkenivå i LDAP-registeret	Definer det enkelte filteret

Dashbord og rapportering

Dashbord-innstillinger

Her kan du se hvilke dashbord som finnes, redigere dem eller opprette nye. Hvert dashbord har sitt eget sett med data som skal vises, og sin egen grafkonfigurasjon.

Kontroll av dashbordinnstillinger

Offentlig	Gjør instrumentbordet offentlig, slik at andre brukere kan se instrumentbordet. Brukerne må selvfølgelig kunne logge inn og se instrumentpaneler. Hvis "Public" ikke er aktivert, er det bare oppretteren som kan se det.
Standard	Angir dashbordet som standard, slik at det åpnes automatisk neste gang du åpner dashbordvisningen.
	Vis dashbordet og dets grafer
	Slett dashbordet
	Rediger navn og innstillinger for dashbordet
	Lag en kopi av dashbordet
	Legg til et helt nytt dashbord

Dashbordvisning

Her vises data og grafer for det valgte instrumentbordet, og du kan også endre disse.

Dashbordkontroll

	Lar deg definere hvilke data som skal vises i dashbordet, hvor mye data som skal vises og i hvilken størrelse disse dataene skal vises
	Tar deg tilbake til oversikten over dashbordet
	Tilbakestiller det åpne instrumentbordet til standardinnstillingene
	Lagrer alle endringer du har gjort i det åpne dashbordet (f.eks. hvilke data som skal vises)
	Endre diagramtype til søylediagram
	Endre diagramtype til kakediagram
	Endre diagramtype til smultringdiagram
	Endre karttype til polart arealkart
	Endre sorteringsrekkefølgen

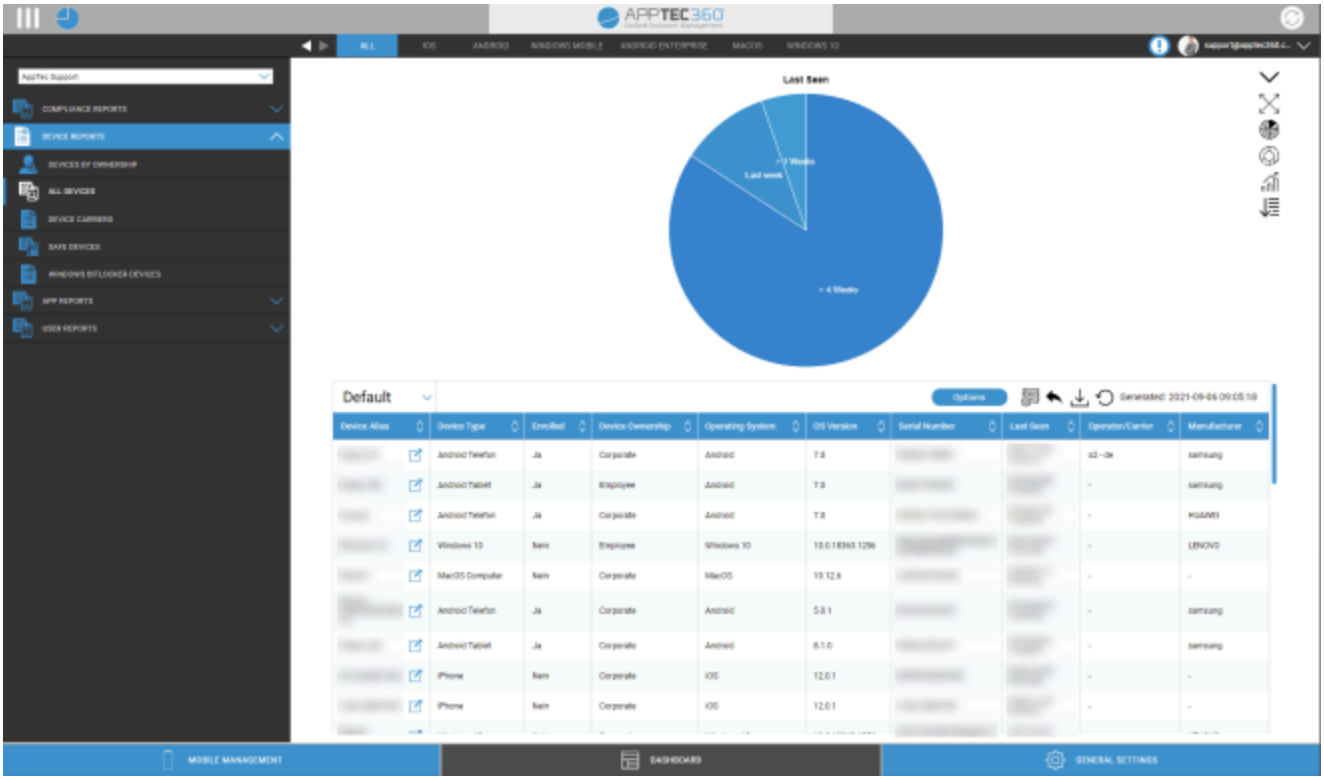
Utvidet rapportering

"Utvidet rapportering" gir detaljerte oversikter og grafer over enhets- og brukerinformasjon.

Det finnes noen få standardrapporter, men alle kan endres manuelt for å legge til eller fjerne data som skal vises.

Vær oppmerksom på at du bare kan endre hvilke data som vises manuelt. Den valgte rapportkategorien definerer hvilke data dette er basert på. Du vil f.eks. aldri kunne se Android-enheter i iOS-rapporten i Enhetsrapporter Alle enheter iOS

Øverst til venstre kan du begrense dataene i rapporteringen til en bestemt gruppe (og alle dens undergrupper). Som standard er dette satt til rotnoden, slik at ALLE enheter og brukere tas med i beregningen.



Utvidet rapporteringskontroll

I hver oversikt kan du bruke følgende funksjoner for å endre rapporten slik du ønsker:

	Skjul diagrammet (hvis diagrammet vises)
	Vis diagram (hvis diagrammet er skjult)
	Utvid diagrammet (hvis diagrammet er sammenfoldet)
	Skjul diagrammet (hvis diagrammet er utvidet)
	Endre diagramtype til søylediagram
	Endre diagramtype til kakediagram
	Endre diagramtype til smultringdiagram
	Endre karttype til polart arealkart
	Endre sorteringsrekkefølgen
	Endre følgende deler av oversikten som vises: • Legg til/fjern kolonner • Angi rekkefølgen kolonnene skal vises i • Vis/skjul diagrammet over tabellen • Velg kolonnen som skal brukes til diagrammet • Filtrer dataene i tabellen din
	Åpne Setup Manager for å lagre og laste inn ulike rapporter
	Tilbakestiller den åpne rapporten til standardinnstillingen
	Eksporter den aktuelle rapporten som en .csv-fil
	Regenerere data og laste inn gjeldende rapport på nytt

Du finner en liste over alle standardrapporter på de neste sidene.

Rapporter om samsvar

Forankrede enheter

Oversikt over enheter som har blitt rootet/jailbreaket.

Standardkolonner for denne rapporten:

Enhetsalias
Eier av enheten
E-post
Operativsystem
Telefonnummer
Sist sett
Produsent

Roaming-enheter

Oversikt over alle enhetene som roamer

Standardkolonner for denne rapporten:

Enhetsalias
Eier av enheten
E-post
Enhetstype
Operativsystem
Telefonnummer
Sist sett

Roaming-aktiverte enheter

Oversikt over alle enheter som har aktivert roaming, men som ikke nødvendigvis roamer for øyeblikket.

Standardkolonner for denne rapporten:

Enhetsalias
Eier av enheten
E-post
Enhetstype
Operativsystem
Telefonnummer
Sist sett

Overvåkede enheter

Oversikt over alle enheter som er overvåket i overvåket modus (kun iOS)

Standardkolonner for denne rapporten:

Enhetsalias
Eier av enheten
E-post
Enhetstype
Sist sett

Inaktive enheter

Oversikt over alle enheter som ikke har koblet seg til serveren i løpet av de siste 7 dagene

Standardkolonner for denne rapporten:

Enhetsalias
Eier av enheten
E-post
Enhetstype
Operativsystem
Sist sett

Enhetsrapporter

Enheter etter eierskap

Her kan du se hvor mange enheter som for øyeblikket er utplassert som bedriftsenheter (bedriftsenheter) og ansattes enheter (private enheter).

Standardkolonner for denne rapporten:

Enhetsalias
Eier av enheten
Enhetstype
Eierskap til enheten
Operativsystem

Alle enheter

Her kan du se en oversikt over alle enheter med den viktigste informasjonen.

Standardkolonner for denne rapporten:

Enhetsalias
Enhetstype
Innmeldt
Eierskap til enheten
Operativsystem
OS-versjon
Serienummer
Sist sett
Operatør/transportør
Produsent

Bærere av enheter

Her kan du se en oversikt over operatøren (mobilleverandøren).

Standardkolonner for denne rapporten:

Enhetsalias
Eier av enheten
E-post
Operativsystem
OS-versjon
Operatør/transportør

SAFE-enheter

Her kan du se en oversikt over hvilke enheter som bruker SAFE Version.

Fordi oversikten og/eller SAFE kun er tilgjengelig for Samsung-enheter, vil du ikke se de vanlige fanene under dette punktet.

Standardkolonner for denne rapporten:

Enhetsalias
Eier av enheten
E-post
Enhetstype
Sist sett
SAFE-versjon

Windows BitLocker-enheter

Her kan du se en oversikt over Windows-enheter som bruker BitLocker.

Standardkolonner for denne rapporten:

Enhetsalias
Eier av enheten
E-post

BitLocker-tilstand

App-rapporter

Her får du en rekke oversikter over apper. I alle disse rapportene kan du klikke på en oppføring for å se hvilke versjoner som er installert på enhetene, og hvor ofte. I denne visningen kan du klikke på en spesifikk versjon igjen for å se hvilke enheter som har denne spesifikke versjonen installert.

Merk: Det kan ta litt tid før systemet får oppdatert informasjon fra enheten. I tillegg oppdateres ikke rapportene hvert minutt. Du må kanskje være tålmodig for å se den gjeldende statusen hvis du nettopp har tildelt en ny app eller versjon. Hvis du laster inn rapporten på nytt manuelt, vil rapporten vise de mest oppdaterte dataene som er tilgjengelige.

Installerte apper

Her får du en oversikt over alle installerte apper.

Standardkolonner for denne rapporten:

Navn	Navnet på den aktuelle appen og/eller tjenesten
Identifikator	Definert app/tjeneste-ID
Totalt antall	Hvor ofte denne appen/tjenesten har blitt installert på sluttbrukernes enheter

Mest installerte apper

Her får du en oversikt over de appene som har blitt installert mest.

Standardkolonner for denne rapporten:

Navn	Navnet på den aktuelle appen og/eller tjenesten
Identifikator	Definert app/tjeneste-ID
Totalt antall	Hvor ofte denne appen/tjenesten har blitt installert på sluttbrukernes enheter

Obligatoriske apper

Her får du en oversikt over obligatoriske (påbudte) apper.

Standardkolonner for denne rapporten:

Navn	Navnet på den aktuelle appen og/eller tjenesten
Identifikator	Definert app/tjeneste-ID
App-kilde	Hvilken AppStore er involvert: • Google PlayStore (Android) • iTunes AppStore (iOS)
OS	Operativsystem

Svartelistede apper

Her får du en oversikt over alle definerte svartelistede apper.

Standardkolonner for denne rapporten:

Navn	Navnet på den respektive appen og/eller tjenesten
Identifikator	Definert app/tjeneste-ID
App-kilde	Hvilken AppStore er involvert: • Google PlayStore (Android) • iTunes AppStore (iOS)
OS	Operativsystem

Brukerrapporter

Tariff

Her får du en oversikt over brukernes telefontariffer og SIM-kort.

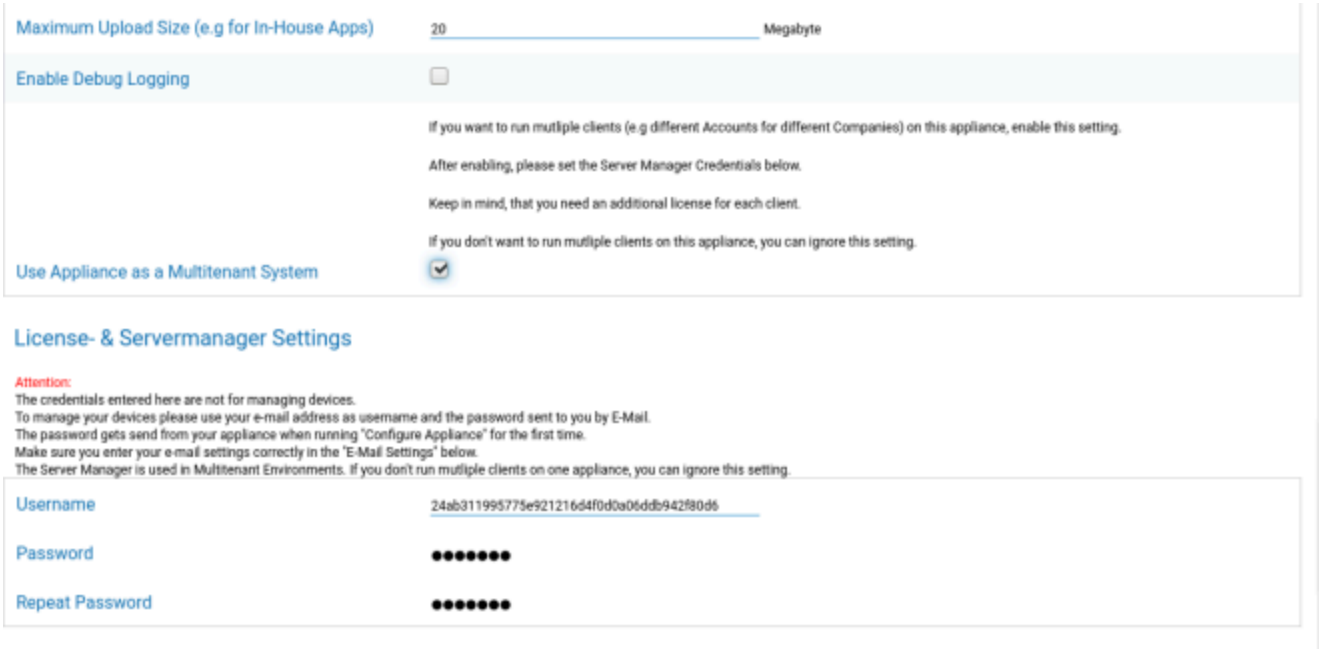
Standardkolonner for denne rapporten:

E-post
Navn
phoneNumber
transportør
tariff
mulighet
pris
kontraktAvbrutt
kontraktStart
underTid
mobileAndData
dataVolume
multiSIM
type
simCardSerial1
simCardSerial2
simCardSerial3
pin1
pin2
puk1
puk2
Merk

Forvaltning av flere leietakere

AppTec360 EMM kan være vertskap for flere separate leietakere, hver med sine egne brukere og grupper, tillatelser og globale innstillinger.

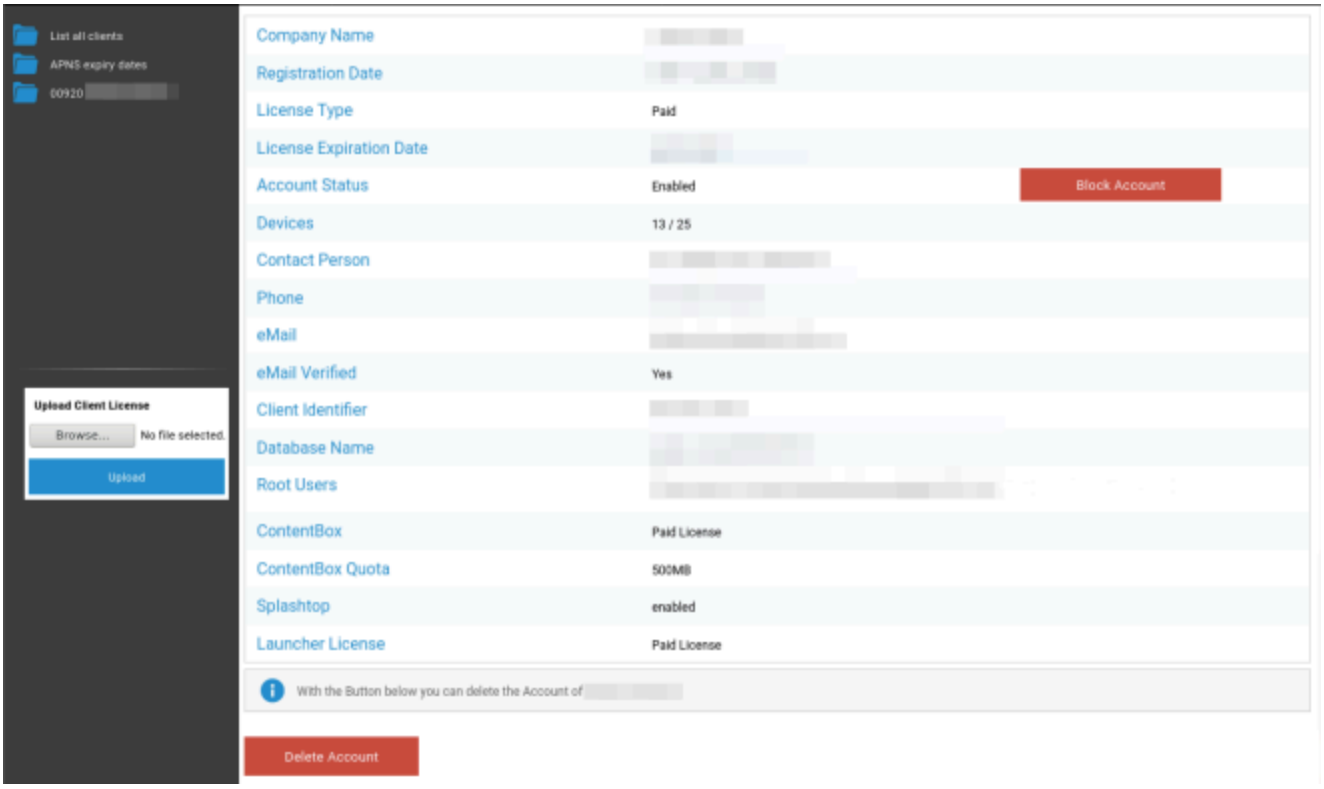
For å aktivere Multitenant-funksjoner må du aktivere det i konfigurasjonsgrensesnittet til apparatet i "Trinn tre - Serverinnstillinger".



I den nye menyen angir du et brukernavn og et passord for Servermanager. Lagre innstillingene, og kjør "Configure Appliance" i "Trinn fem - Lisensavtale" for å ta i bruk innstillingen.

Når konfigurasjonen er fullført, kan du nå logge inn med den angitte påloggingsinformasjonen via det vanlige Mobile Management-grensesnittet.

Etter innlogging kan du se følgende visning.



Til venstre ser du alle leietakere (i dette tilfellet bare én med id 920), og til høyre ser du informasjon om denne klienten. Du har også mulighet til å blokkere tilgangen til kontoen og slette klienten (FORSIKTIG: Dette vil fjerne alle data knyttet til klienten).

Til venstre kan du laste opp en ny klientlisens, som enten kan være en lisensoppdatering for en eksisterende klient eller en ny lisens som automatisk oppretter en ny klient. Når en ny klient opprettes, sendes det automatisk en e-post med innloggingspassordet til e-postadressen som lisensen ble utstedt til.

For å få en ny eller oppdatert klientlisens (f.eks. ved behov for flere enhetslisenser), kontakt din salgsrepresentant.

Flere visninger

Liste over alle kunder

Viser en oversikt over alle klienter i systemet.

Klient-ID	Klient-ID
Identifikator	Klientidentifikator
Database	Database
Selskapets navn	Selskapets navn
E-post	Kontaktperson e-post
Verifisert	Om kontaktpersonens e-post er verifisert eller ikke
Land	Land
Enheter	Antall registrerte enheter
Registreringsdato	Tidspunkt for tildeling av lisens
Siste innlogging	Siste innlogging på administratorkonto
Lisens	Visning av lisenstype (gratis|betalt)
CB-lisens	ContentBox-lisens (gratis|betalt)
Status	Gjeldende status for AppTec-Client
Utløpt	Viser om lisensen har utløpt
iOS	Antall iOS-enheter
Android	Antall Android-enheter
Windows Mobile	Antall Windows Mobile-enheter
MacOS	Antall MacOS-enheter
Windows 10	Antall Windows 10-enheter
Android Enterprise	Antall Android Enterprise-enheter
IOS BYOD (brukerregistrering)	Antall IOS BYOD-enheter (brukerregistrering)
IoT	Antall IoT-enheter

APNS utløpsdatoer

Viser en oversikt over utløpsdatoer for alle APNS-sertifikater for alle klienter.

Klient-ID	Klient-ID
Selskapets navn	Selskapets navn
Utløpsdato	Utløpsdato for Apple APNS-sertifikatet
Info	Informasjon om utløpsdatoen

Kontakt

Har du flere spørsmål? Bare kontakt oss under:

For generelle tekniske spørsmål

support@apptec360.com

+41 61 511 3210

For spørsmål knyttet til installasjon av en virtuell appliance

consulting@apptec360.com

+41 61 511 3214

Ansvarsfraskrivelse