# AppTec360 Enterprise Mobile Manager & ContentBox

## Administrationshandbok | Version 5.0 (202110)

# Innehållsförteckning

- Meddelande (endast på enhetsnivå)
- Säkerhetskonfiguration
  - Lösenord
  - Kryptering
  - AntiVirus
- End of Life (endast på enhetsnivå)
  - Torka (endast på enhetsnivå)
- Inställningar för begränsning
  - Begränsningar
  - Ägare av AE-enhet

## BYOD Container

- Android Företag
  - Android Företag
  - Gmail Exchange
  - Appar för AE-system
  - Container lösenord
- Samsung KNOX
  - Aktivering
  - Knox-lösenord
  - Knox Säkerhet
  - Knox Exchange
  - Knox eMail
  - Knox Appar

## Hantering av anslutningar

- Wifi
  - Typ av säkerhet
    - WEP
    - WPA/WPA2
    - 802.1x EAP
- VPN
- Begränsningar
- APN
- Bluetooth

## PIM-hantering

- Utbyte

- E-post
- AE Gmail Exchange

### App-hantering

- Enterprise App Manager
  - Installerade appar (endast på enhetsnivå)
  - Systemappar (endast på enhetsnivå)
  - Obligatoriska appar
  - Appar för AE-system
- Begränsningar och inställningar
  - Svart- och vitlistning
  - Sys App Begränsningar
    - Samsung-appar
    - Appar från Huawei
  - Inställningar för apphantering
- App Store för företag
  - Playstore
  - Internt
- Play Store för företag
- Kioskläge och startprogram
  - Kiosk-läge
  - AppTec360 Launcher
  - AppTec360 Inställningar

### Fjärrkontroll

- Splashtop
- Teamviewer

### Innehållshantering

- Innehållsbox
- Säker webbläsare

## Konfiguration Windows 10 PC

### Allmänt

- Översikt över grupprofiler (endast på gruppnivå)
- Enhetsöversikt (endast på enhetsnivå)
- Inställningar
- Config Revision (endast på enhetsnivå)

# Allmän översikt

## Introduktion till AppTec360

AppTecs Enterprise-Mobile-Management-Solution erbjuder möjligheten att hantera och konfigurera alla mobila enheter med sin intuitiva hanteringskonsol. I det här scenariot kan EMM-servern antingen köras i din egen miljö eller så kan du använda vår molnbaserade lösning.

Även när det gäller en central installation av företagsapplikationer på smartphones har du kommit till rätt ställe. Med Enterprise Mobile Manager kan du distribuera företagsapplikationer och dokument till enheter inom några sekunder eller blockera oönskade applikationer med vit-/blacklisting.

Användningen av privata enheter på företag innebär en ny utmaning när det gäller att säkra smartphones och surfplattor. Eftersom medarbetarna vill använda sina smartphones i allt större utsträckning måste IT-administratörerna skydda ett stort antal olika typer av enheter. Vi hjälper dig att säkra alla enheter och de känsliga data som lagras på dem och hanterar dem från en intuitiv konsol.

## Operativsystem för enheter som stöds

AppTec360 erbjuder stöd för iOS-, Android- och Windows-enheter. Observera att funktionskapaciteten hos de nämnda plattformarna kan skilja sig från ett operativsystem till ett annat.

- Apple iOS 11.0 eller högre*
- Apple macOS 10.11 eller högre
- Google Android 4.4 eller senare** på molnversionen
- Google Android 4.1 eller högre** på OnPrem-versionen
- MS Windows 10 eller högre*** (stationär dator, bärbar dator och surfplatta)

**Observera att enheter med iOS 10 eller tidigare inte kan registreras på grund av drastiska förändringar som Apple har gjort i registreringsprocessen.*

***Enheter kan anslutas och konfigureras även om de använder en version som inte längre stöds av tillverkaren. Observera att det kan finnas funktioner som kräver en viss Android-version. I supportärenden följer vi tillverkarens officiella support. Vid problem eller buggar som orsakas av en föråldrad version som inte längre stöds av tillverkaren förbehåller vi oss rätten att endast erbjuda begränsad support.*

****Home-versionen av Windows stöds inte på grund av begränsningar i operativsystemet. Vi rekommenderar starkt att du använder en OS-version som fortfarande stöds av tillverkaren. Inte bara av kompatibilitetsskäl utan också av säkerhetsskäl. Därför rekommenderar vi iOS 12 eller högre och Android 9 eller högre.*

## LDAP-kataloger som stöds

- Microsoft Active Directory
- Öppna LDAP

Uppdaterad information om "Operativsystem för enheter som stöds" och "LDAP-kataloger som stöds" finns här:

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

# Förklaring av ”Supervised-Mode” på Apple-enheter

Supervised-Mode innebär ett utökat gränssnitt för iOS-enheter.

På respektive konfigurerad enhet kan ytterligare begränsningar tillämpas, eftersom de avser funktionaliteten hos slutanvändarens enhet. Dessa finns också i administrationshandboken och är därför markerade med en banderoll.

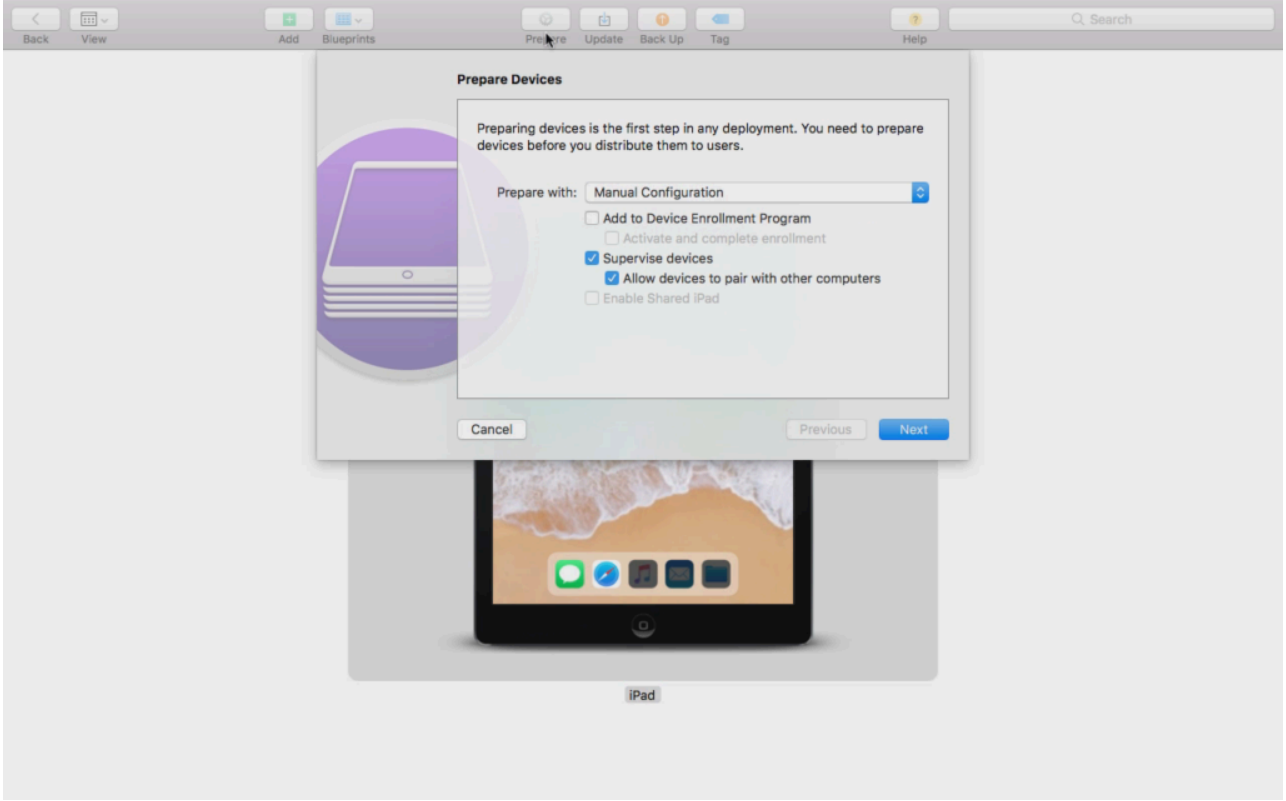
## Tillgänglig i Supervised-mode

"Supervised-Mode" kan aktiveras med hjälp av programmet "Apple Configurator". Apple Configurator kan ställa in standardinställningarna på nya iOS-enheter som ett konfigurationsverktyg (via USB-gränssnittet).

Verktyget kan inte bara installera konfigurationsprofiler utan även appar. Det är kostnadsfritt, men kräver en Mac-dator.

## Aktivera det övervakade läget

1. Öppna Apple Configurator




2. Klicka på enheten och välj "Förbered"
3. Välj "Manuell konfiguration" och "Övervaka enheter"
4. Klicka på "Nästa"
5. (Valfritt) Nu kan du lägga till en MDM-server där enheten ska registreras. Länken för detta finns i "Allmänna inställningar - iOS-konfiguration - Konfigurator och URL" Välj din organisation eller skapa en ny
6. Välj din organisation eller skapa en ny
7. Välj vilka steg som ska hoppas över i den inledande installationen och klicka på "Nästa" (OBSERVERA: Om du fortsätter raderas din enhet!)

Nu kommer din enhet att sättas i övervakat läge. Detta kan ta några minuter. När det är gjort kommer enheten att starta om.

Nu är din enhet övervakad!

## Lägga till en enhet i DEP

Du kan också lägga till enheter i DEP (Device Enrollment Programm) med hjälp av Apple Configurator, om dina enheter har iOS 11 eller senare.

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

Följ samma steg som när du övervakar en enhet och markera dessutom "Add to Device Enrollment Program". Du kommer att bli ombedd att ange dina inloggningsuppgifter för DEP om du aldrig tidigare har loggat in i DEP med Apple Configurator.

När processen har slutförts finns enheten i DEP-servern "Devices Added by Apple Configurator 2". Du kan nu använda den här servern och ansluta den till managementkonsolen eller överföra enheten till en redan befintlig server.

Du har nu framgångsrikt lagt till en enhet i DEP!

# Förklaring av Android Enterprise

## Vad är Android Enterprise?

Android Enterprise ger bättre kontroll över arbetsenheter som hanteras med en MDM. Detta gör att administratörer antingen kan ha full kontroll över sina Android-enheter eller separera företagsdata från privata data på containerenheter. Dessutom möjliggör Android Enterprise en enklare registrering av enheterna och en enkel appdistribution.

## Vilka är kraven för att använda Android Enterprise?

Android Enterprise kan användas kostnadsfritt av alla. Du behöver bara ansluta ett Google-konto till MDM för att aktivera alla Android Enterprise-funktioner. Mer om detta finns i avsnittet Android Enterprise.

Android Enterprise kan användas på enheter med Android 5.1 eller senare, med undantag för Enhanced Work Profile (se nedan). Vi rekommenderar minst Android 7 eller högre för en enklare registrering eller Android 11 för att kunna använda alla tillgängliga funktioner.

## Vilka är de tillgängliga lägena med Android Enterprise?

Det finns 3 olika lägen att använda när du använder Android Enterprise.

AE Fullt hanterad enhet (arbetshanterad): En helt hanterad enhet som endast används i arbetet. Detta ger administratören full kontroll över enheten. Detta tillåter inte privat användning av enheten. För att registrera enheter i detta läge måste enheterna återställas och registreras med en QR-kod (se AE-registrering) eller registreras via Knox Enrollment eller Zero Touch.

AE BYOD-behållare: BYOD-containern (bring your own device) gör det möjligt för användare att komma åt företagsdata på sin privata telefon i en separat container. I det här läget kan privata appar inte se företagets data och appar och vice versa. För att registrera enheter i det här läget måste AppTec-appen laddas ner och en QR-kod kan skannas. Skapa en enhet i konsolen och välj "AE Container (BYOD & Enahnced Work Profile)" som enhetstyp. Klicka på QR-koden på den nyligen skapade enheten för att hämta QR-koden och ställ in den första växeln till "Legacy & BYOD".

AE Enhanced Work Profile: (kräver Android 11 eller senare) Medan den ovan nämnda BYOD-containern för över företagsdata till en privat enhet, gör Enhanced Work Profile samma sak men för en företagsägd enhet. Den skapar samma container, men ger administratören lite mer kontroll över enheten, så att användaren inte bara kan ta bort MDM från enheten. Skapa en enhet i konsolen och välj "AE Container (BYOD & Enahnced Work Profile)" som enhetstyp. Klicka på QR-koden på den nyligen skapade enheten för att hämta QR-koden och ställ in den första brytaren på "Enhanced Work

Profile". Denna QR-kod kan skannas efter att du har återställt enheten och tryckt 6 gånger på skärmen enligt förklaringen i Metod 1 i AE-registrering.

### Hur kan jag tilldela appar till Android Enterprise-enheter?

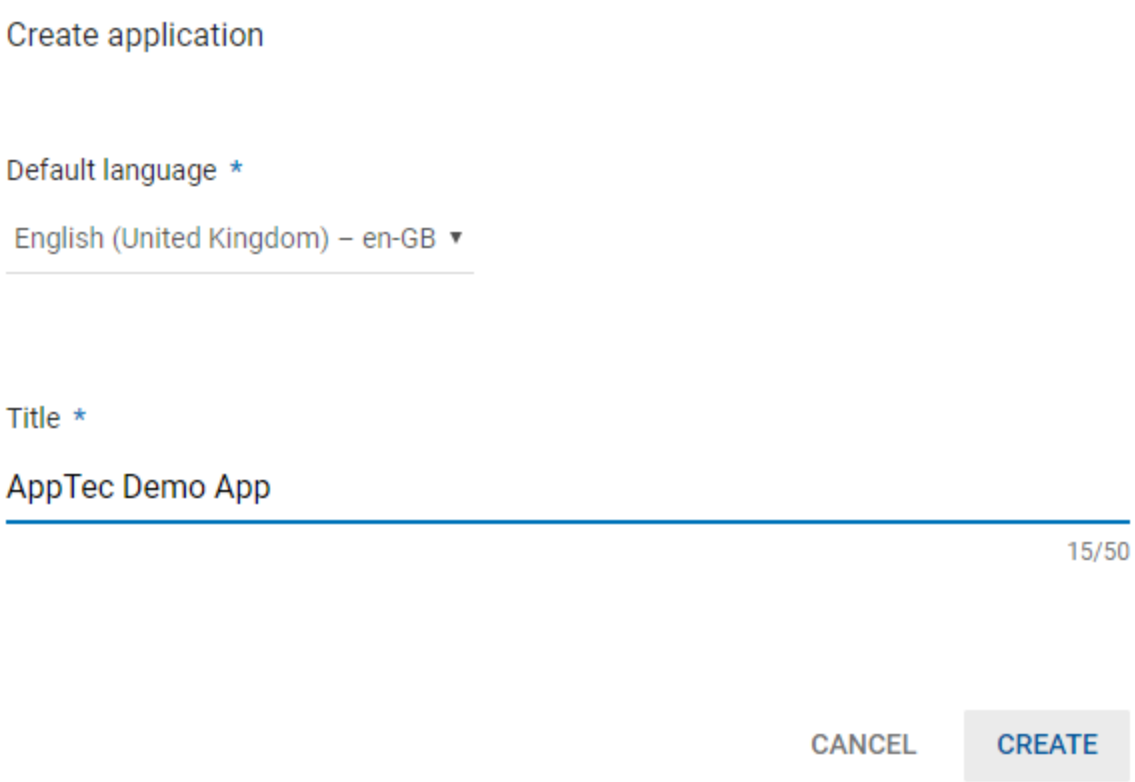
Först måste du godkänna de appar som du vill använda i Allmänna inställningar → Apphantering → AE Play Store → Play Store-appar. När du har godkänt en app kan du lägga till den i den obligatoriska applistan → i din profil genom att klicka på "+" och välja appen på fliken "AE Play Store". Appen laddas ner och installeras automatiskt. Det krävs inget Google-konto på enheten och användaren behöver inte bekräfta eller tillåta detta.

## Ladda upp dina egna appar till Google Play Store

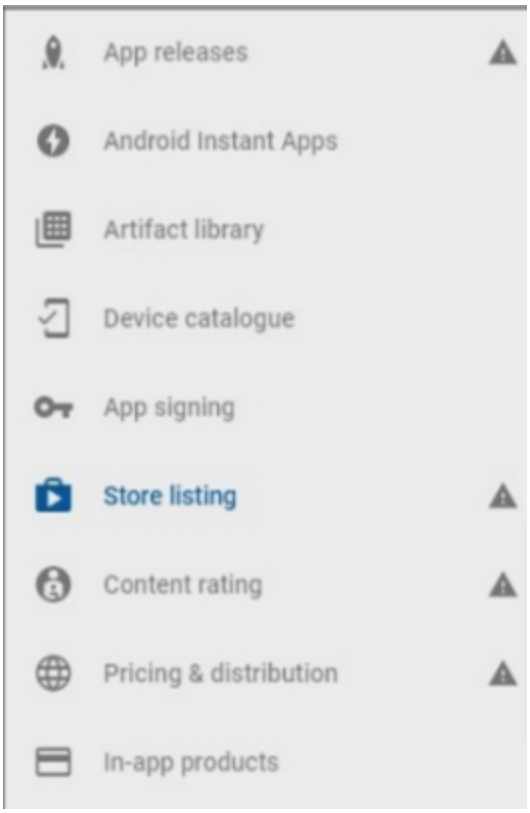
Det är möjligt att ladda upp dina Inhouse Apps till Google Play Store. På så sätt kan du dra nytta av olika fördelar, t.ex. Play Stores uppdateringsmekanism.

För att göra det behöver du ett Google Developer-konto. Logga in med hjälp av Google Play Console(https://play.google.com/apps/publish)

Klicka på "Skapa applikation". Välj ditt standardspråk och titeln på appen.



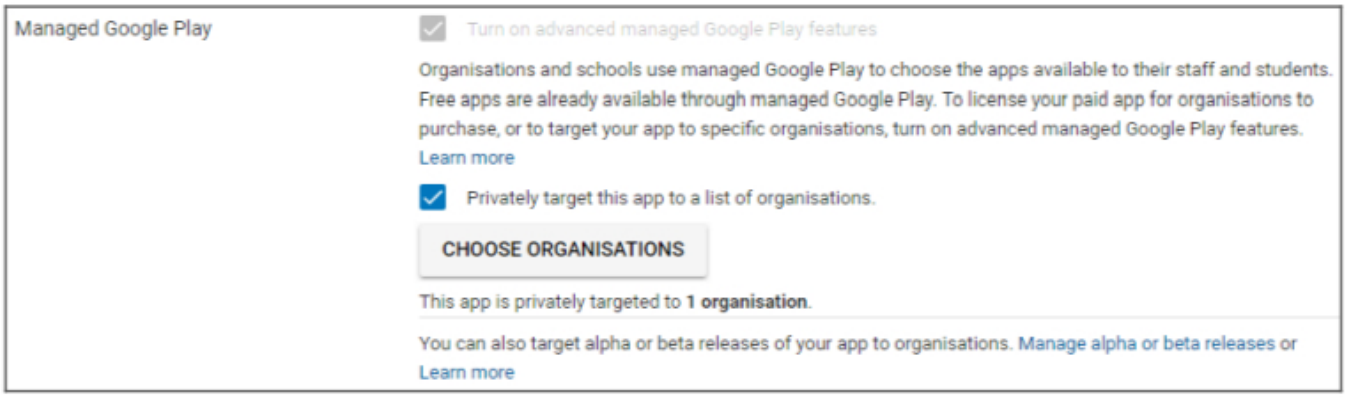
På följande sida kommer du att bli ombedd att ange olika uppgifter om din app.



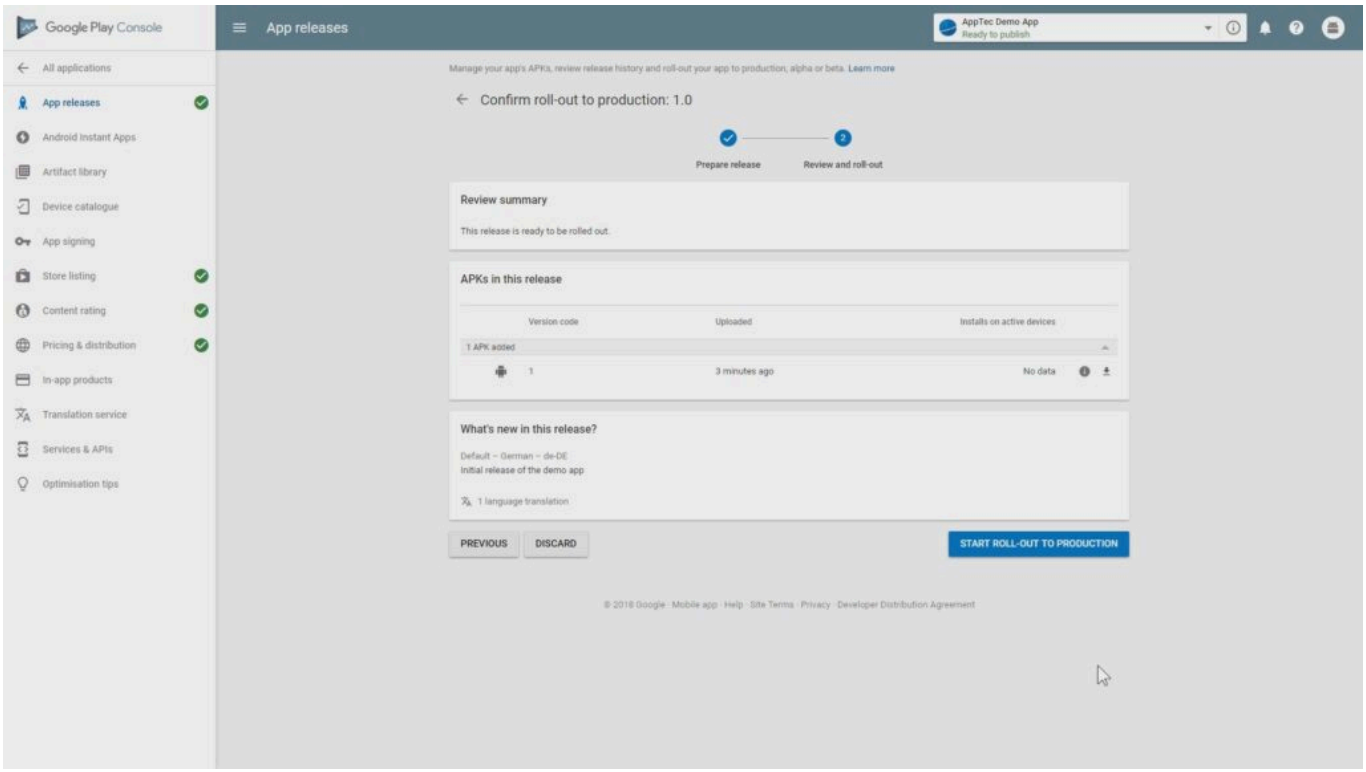

När du har angett alla detaljer ser du olika tipssymboler på vänster sida.

Håll muspekaren över dem för att se vilka steg som återstår och följ dem i valfri ordning.

Obs: Se till att markera de två kryssrutorna vid "Managed Google Play" under "Pricing & Distribution". Annars kommer appen att vara offentlig och kan nås av alla. Se också till att välja land för distribution.



När du har slutfört alla steg kan du gå till "App releases". Klicka på "Review" och "Start Roll-Out to Production" för att slutföra ditt utkast och publicera appen.




Det kan ta lite tid innan appen är tillgänglig i Play Store. När processen är klar kan du söka efter din app i Play for Work-butiken och godkänna den. Därefter kan du helt enkelt tilldela appen till enheter med hjälp av EMM-konsolen precis som du gör med andra appar.

# Krav och installation

## Krav och önskemål

### Systemkrav

Den virtuella apparaten finns tillgänglig i Open Virtualization Format (VMWare, VirtualBox, Citrix Xen Server) och som komprimerad .vhdx-fil (Hyper-V)*.

*Anm: Maskinen måste skapas med Generation 1 när Hyper-V används.

Den virtuella disken har en målstorlek på 20 GB och maskinen kräver 4 GB RAM.

Apparaten är baserad på Debian 9 64bit

Uppgradera den importerade maskinen till den senaste kompatibiliteten (t.ex. i VMWare) och se till att maskinens OS-typ är korrekt inställd i din hypervisor.

### Licensnyckel

För att framgångsrikt kunna aktivera och installera servern behöver du en giltig licensfil. Du kan få en sådan från AppTec360 direkt och/eller från din respektive återförsäljare.

### IP-adress och DNS-resolution

AppTec360-apparaten måste kunna nås av den enhet som använder det värdnamn som licensen är utfärdad för.

För att registrera Windows 10-enheter måste du också ställa in en ytterligare underdomän i form av "enterpriseenrollment.", som pekar på apparaten.

## SSL-certifikat

Eftersom alla anslutningar till och från enheterna måste säkras med SSL behöver du ett giltigt certifikat för värdnamnet som utfärdats av en certifikatutfärdare som enheten litar på. Den privata nyckeln för certifikatet måste laddas upp utan lösenordsskydd. I de flesta fall krävs ett mellanliggande certifikat för certifikatutfärdaren för att enheterna ska känna igen servercertifikatet.

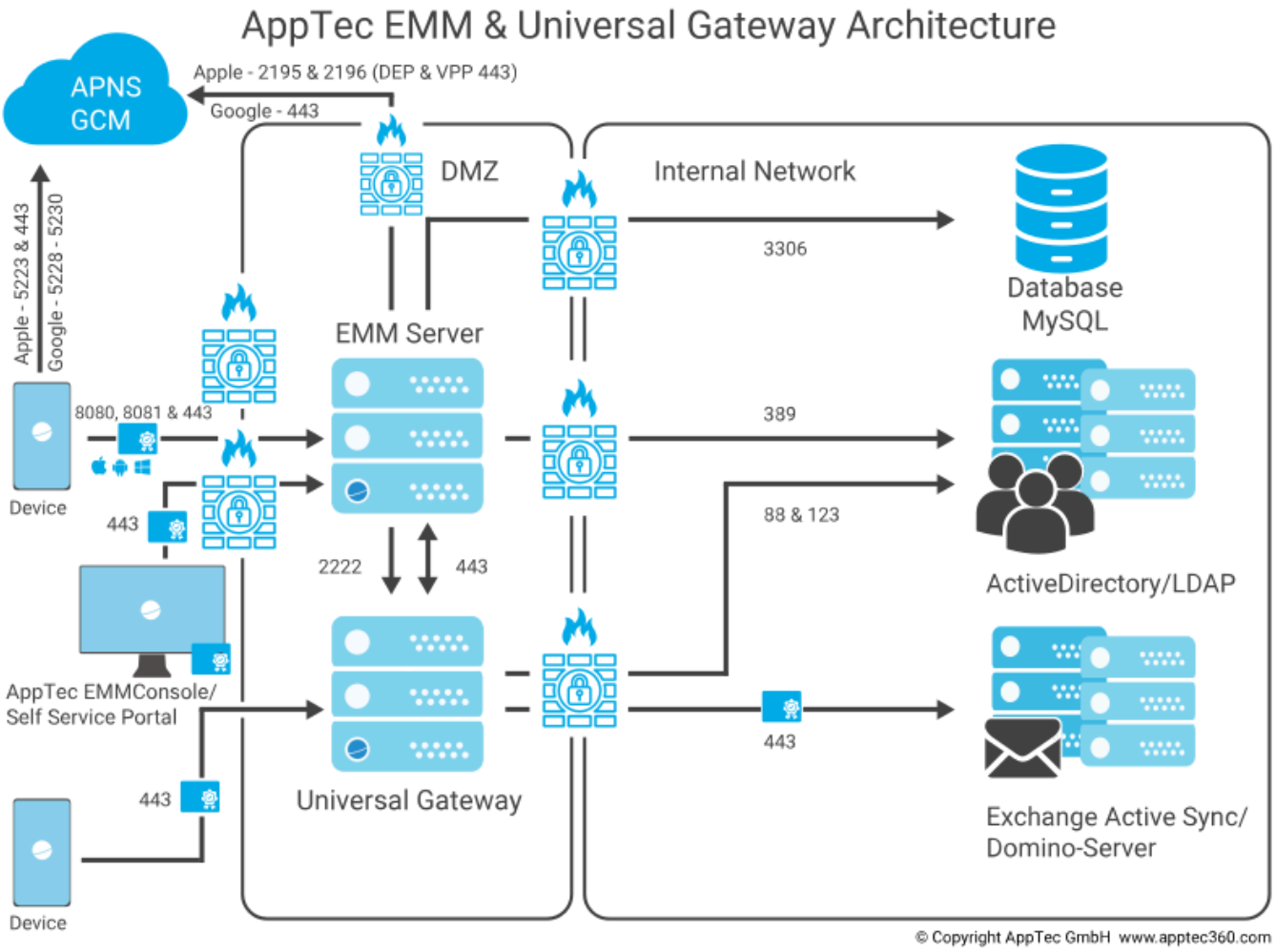
Windows 10-enheter kommer att kräva ett specifikt certifikat för din enterpriseenrollment-underdomän.

Från och med applianceversion 202104 kan du också använda Let's Encrypt-certifikat, som genereras automatiskt (beskrivs i Steg två - SSL-certifikat).

## SMTP-server

En e-postserver och/eller ett e-postrelä krävs för att AppTec360 EMM ska kunna skicka e-postmeddelanden (t.ex. för enhetsregistrering och kontovalidering).

## Brandväggsregler




Detta diagram visar vilken anslutning som behövs beroende på vilka tjänster du vill använda.

För en mer detaljerad beskrivning, se tabellen på nästa sida.

| | | |
|---|---|---|
| **Alla (externa/enheter)** | → | **AppTec360 Apparat / emmconsole.com** |
| Portar | 443 | Hantering, Enterprise AppStore och Windows Phone-kommunikation |
| | 8080 | Android & iOS Kommunikation |
| | 80 | Första gången installation av Let´s Encrypt. Använder 443 efteråt. |
| **Alla (enheter)** | → | **Valfri (extern)** |
| Portar | 5223, 443 | Apple Push Service, måste vara nåbar utan proxy, 443 som fallback, se https://support.apple.com/en-us/HT203609 |
| | 5228-5230 | Android Push Service (FCM), måste vara nåbar utan proxy |
| **AppTec360 Apparat** | → | **Domänkontrollant** |
| Portar | 389, (LDAPS 636) | Synkronisering av användare med LDAP |
| **AppTec360 Apparat** | → | **Alla** |
| Port | 443 | Används för Android Push Service (GCM)<br>Sök i AppStore / Play Store |
| **AppTec360 Apparat** | → | **emmconsole.com** |
| Portar | 443 | AppTec360 Appliance-uppdateringar, generering av APNS-certifikat |
| **AppTec360 Apparat** | → | **Apple-nätverket (17.0.0.0/8)** |
| Portar | 2195, 2196 | Apple Push Service & Feedback Service |
| | 443 | DEP & VPP |

# Säkerhetsuppdateringar

*Operativsystemet Debian bör uppdateras regelbundet för att få de senaste säkerhetsfixarna. Se dock till att du inte uppgraderar till en nyare huvudversion av Debian manuellt. När AppTec360 EMM är kompatibelt med en nyare större version kommer vi att lägga till ett sätt att uppgradera i en uppdatering av apparaten.*

## Standardlösenord för den virtuella apparaten

**Logga in användare (rotinloggning är inaktiverad. Använd "sudo" för administrationsuppgifter)**

apptec

**Logga in Lösenord**

apptec

**MySQL Root-användare**

rot

**Lösenord för MySQL-rot**

apptec

**MySQL Standardanvändare**

AppTec

**MySQL Standardlösenord för användare**

AppTec

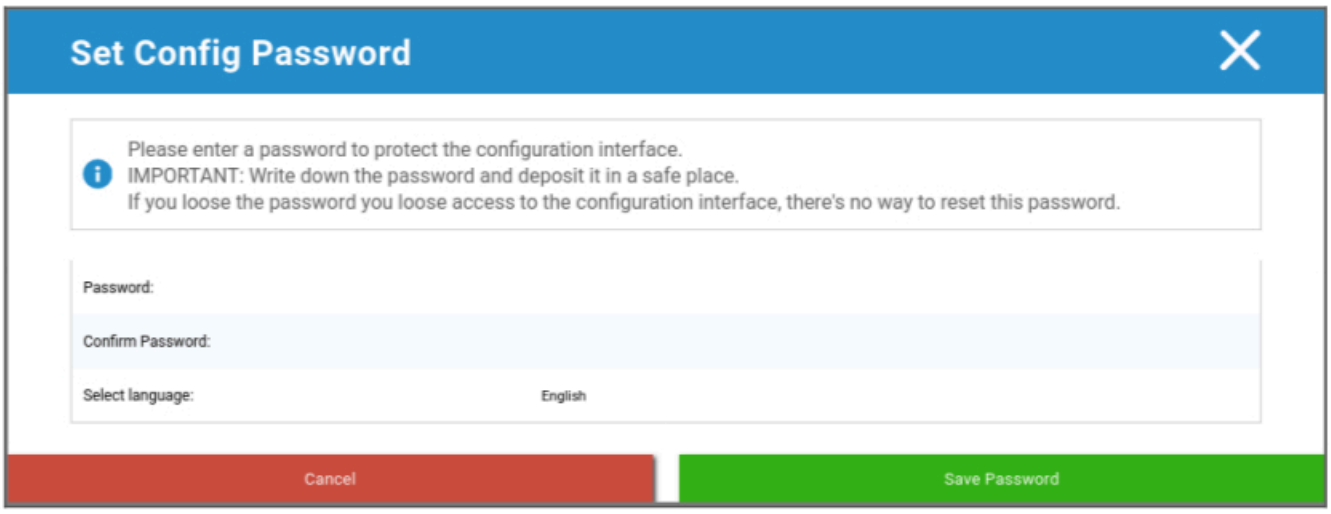
# Konfiguration av den virtuella apparaten

**Viktigt:** Innan du börjar konfigurera Virtual Appliance bör skärmupplösningen vara inställd på minst 1280 x 800 pixlar.

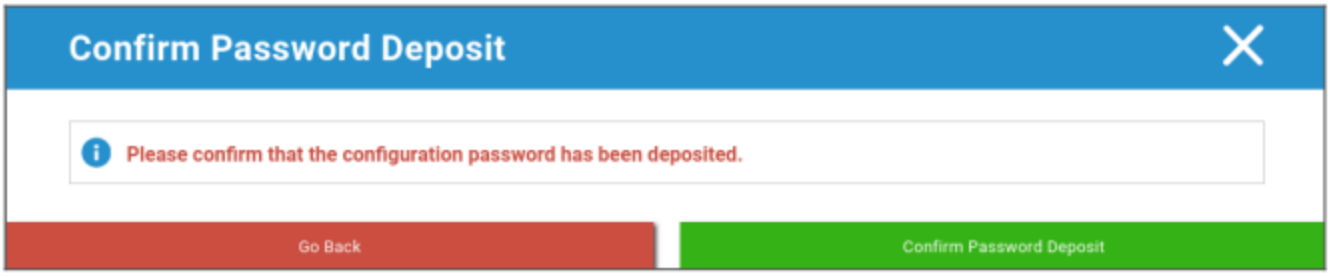
När du har kopplat in dig på apparaten bör Firefox starta automatiskt och visa konfigurationsgränssnittet.

## Förberedelser

Först måste du ange ett lösenord för konfigurationsgränssnittet. Detta lösenord används för att kryptera all information och alla filer som matas in i konfigurationsgränssnittet. Här kan du också ställa in vilket språk som gränssnittet ska visas på (kan ändras senare).

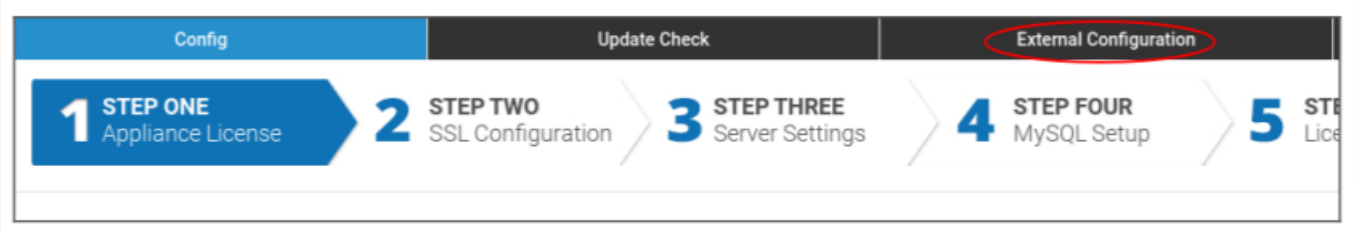



Lösenordet kan endast återställas av AppTec360 Support, så se till att förvara det på en säker plats och bekräfta den kommande popupen.



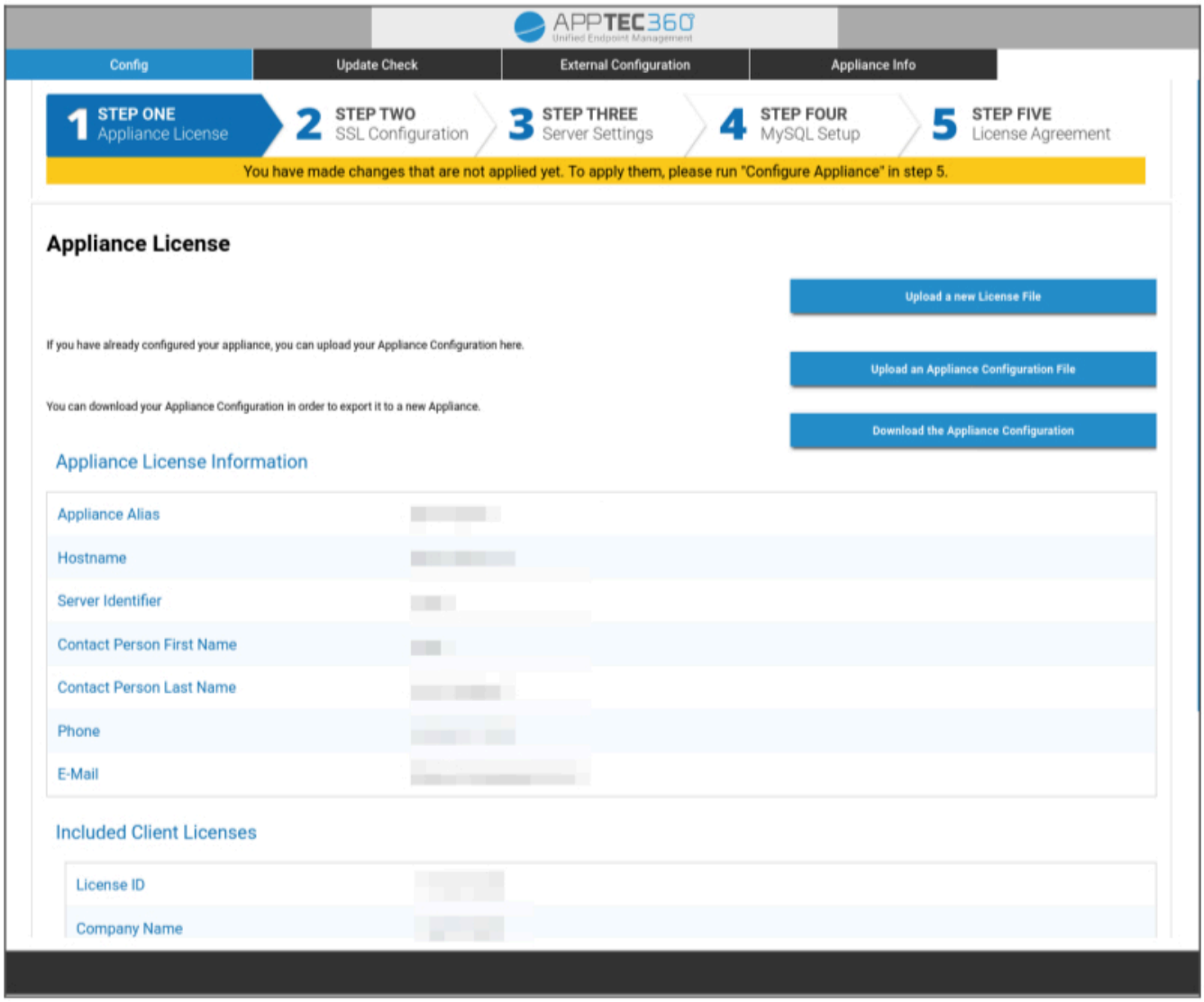
## Konfigurera från extern värd

För att underlätta installationsprocessen kan du göra konfigurationssidan tillgänglig från fjärranslutning. Följ då stegen i "Konfigurera från extern värd".



## Steg ett – Licens för apparat

1. Vänligen ladda upp den licensfil som du har fått från AppTec.
2. Om licensfilen har laddats upp framgångsrikt kan du se apparatens licensinformation som i skärmdumpen nedan.



## Steg två – SSL-certifikat

Du kan antingen använda den automatiska certifikatinställningen med Let's Encrypt eller tillhandahålla certifikaten själv (se SSL-Certificate för mer information).

### Automatisk

Certifikatet genereras automatiskt med hjälp av tjänsten Let's Encrypt.

AppTec360 EMM använder HTTP-01-utmaningen för validering av domänen, vilket innebär att HTTP-porten måste vara öppen från internet för den första begäran om ett certifikat. Efterföljande förnyelsebegäran kan valideras via HTTPS.

Ändra alternativknapparna till "Automatic (Let's Encrypt)" och tryck på "SAVE VALUES". Certifikatet kommer automatiskt att begäras när du tillämpar konfigurationen i steg fem - Licensavtal. Certifikatet förnyas automatiskt vid behov och du får ett e-postmeddelande om certifikatet är på väg att löpa ut (vilket innebär att förnyelsen kan ha misslyckats).

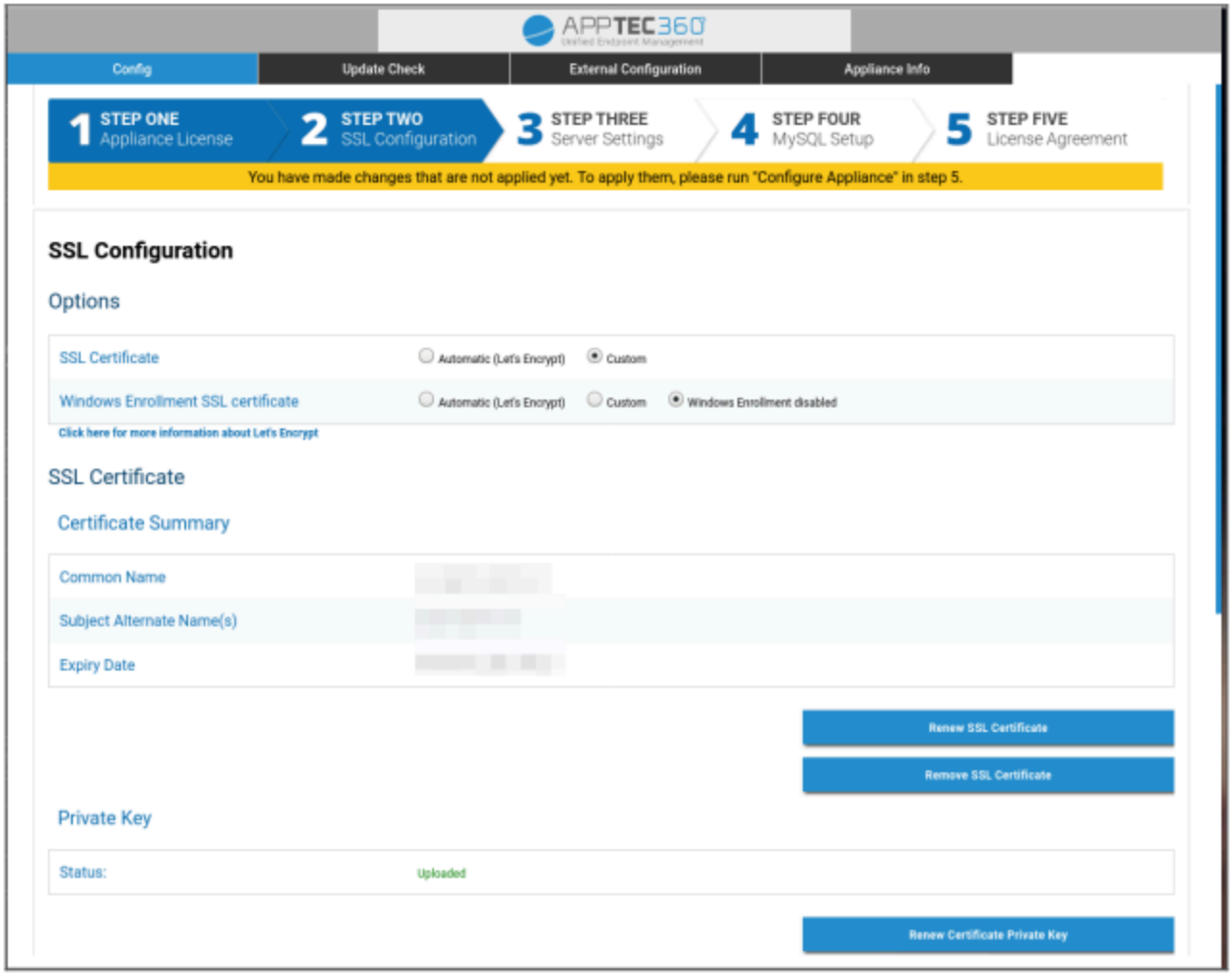
## Anpassad

1. Ladda upp SSL-certifikatet för ditt licensierade värdnamn. Du kan se värdnamnet i steg ett - Appliance License.

2. Ladda också upp den privata nyckeln för certifikatet och vid behov det mellanliggande certifikatet.

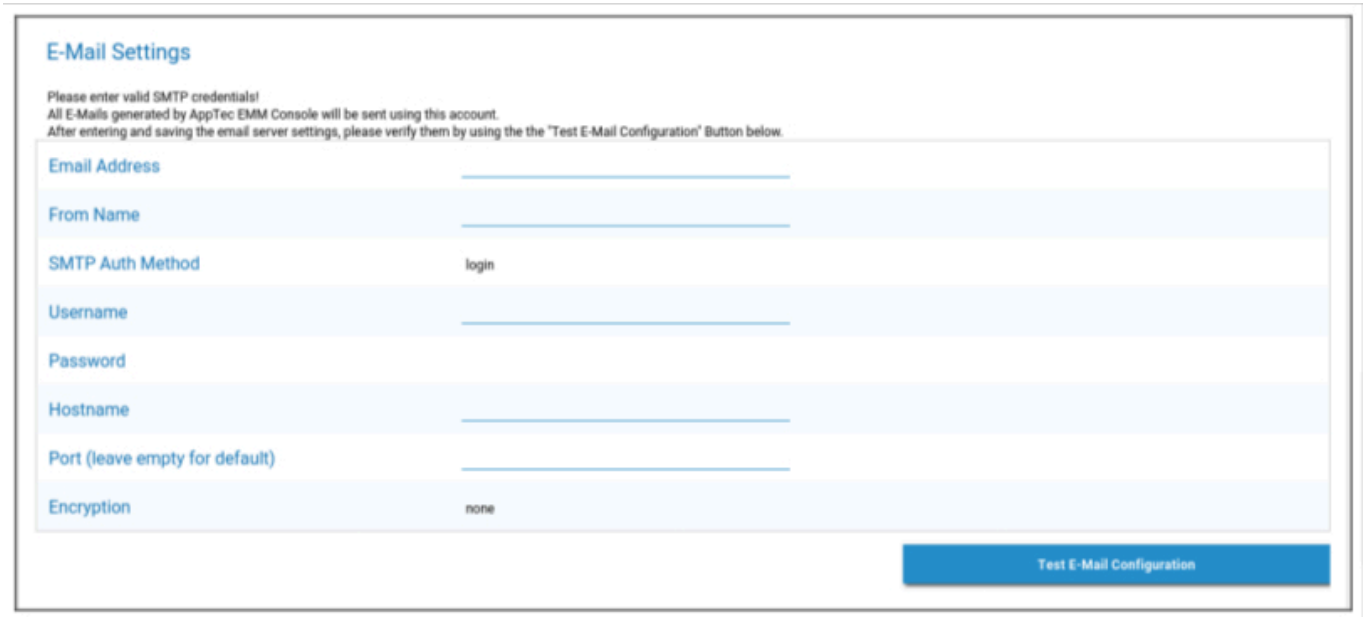
**Viktigt:** Nyckeln får inte vara lösenordsskyddad. Om den är det, ta bort lösenordet innan du laddar upp den.

**Tips:** Om du också vill använda Windows 10-enheter måste du aktivera "Windows Enrollment SSL certificate" och ladda upp certifikatet, den privata nyckeln och mellanliggande certifikat för din underdomän (beskrivs i IP-Address and DNS Resolution) längst ner på sidan.



## Steg tre – Serverinställningar

1. Vänligen ange en e-postadress för global support. Den här adressen kommer att användas i e-postmeddelanden till dina användare så att de vet vem de ska kontakta vid eventuella problem med deras enhet.
2. Ange e-postinställningar som ska användas av systemet för att skicka e-post. Inställningarna kommer att användas för att skicka e-post till användaren och även för att skicka felrapporter och funktionsförfrågningar till"support@apptec360.com".När du har sparat dina e-postinställningar måste du verifiera dem genom att klicka på "Test E-Mail Configuration" och följa instruktionerna.




## Steg fyra – MySQL-installation

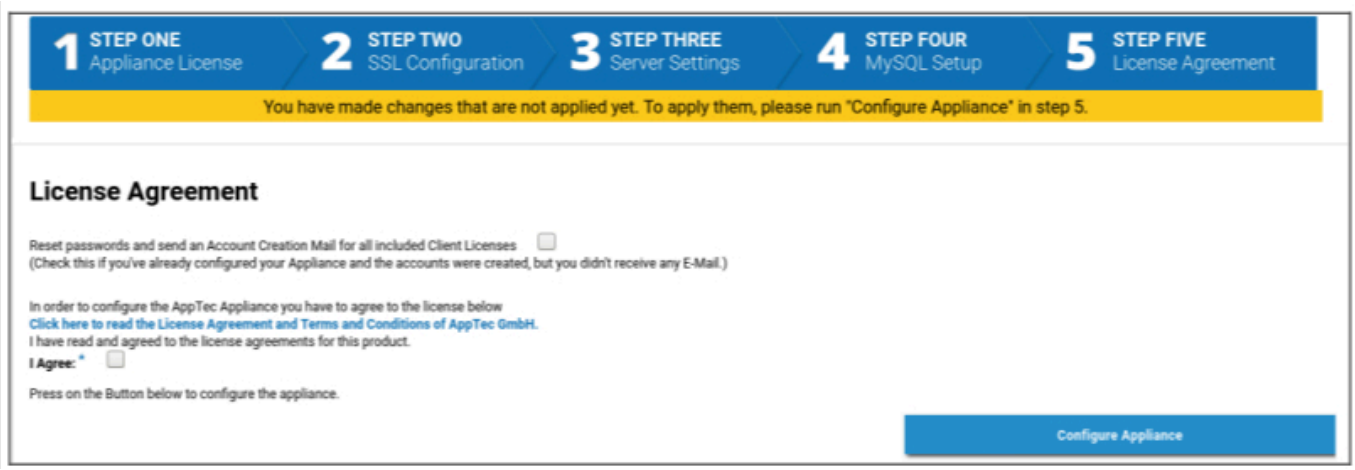
1. Om du vill använda den interna databasen kan du hoppa över det här steget. Annars kan du ange anslutningsinformationen för din externa databasserver.


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)

## Steg fem – Licensavtal

1. Vänligen läs igenom licensavtalet.
2. Markera "I Agree" och tryck på knappen "Configure Appliance" för att tillämpa inställningarna.

Tips: Du måste köra "Configure Appliance" varje gång du ändrar inställningar i de 5 stegen för att tillämpa inställningarna.




## Gratulerar!

Du har nu slutfört konfigurationen av den virtuella apparaten.

Ett e-postmeddelande med ditt lösenord skickades till den adress som du har angett för licensen (visas under "Inkluderade klientlicenser" i Steg 1 - Appliance-licens).

Du kan nu logga in på konsolen med hjälp av detta lösenord och den e-postadress du har fått det på.

För att logga in på konsolen ska du ange konsolens värdnamn i adressfältet i din webbläsare.

Du kan hitta värdnamnet för din apparat i Steg ett - Apparatlicens.

## Felsökning

1. Du fick inget e-postmeddelande när du konfigurerade apparaten i steg fem - Licensavtal:

Kontrollera att dina e-postinställningar i Steg 3 - Serverinställningar är korrekta. Om du vill skicka lösenordet igen ska du kontrollera "Återställ lösenord och skicka ett e-postmeddelande om skapande av konto för alla inkluderade klientlicenser" i Steg fem - Licensavtal innan du kör "Configure Appliance" igen.

2. Du har fått ett fel när det gäller Let's Encrypt under konfigurationen i Steg fem - Licensavtal:

Kontrollera att apparaten är nåbar via sitt domännamn på port 80. Let's encrypt skriver också en logg till "/var/log/letsencrypt" som kan hjälpa till med ytterligare felsökning.

## Rekommendationer för säkerhet

Vi rekommenderar att du utför följande steg för att säkra din AppTec360-appliance.

Detta är inte en fullständig uppsättning instruktioner, det är bara en rekommendation för en grundläggande konfiguration.

- Ändra lösenordet för AppTec360-användaren
- Ändra lösenordet för MySQL-användarna "root" och "AppTec" och uppdatera Steg 4 - MySQL-installation i enlighet med detta
- Ändra standardporten för SSH-servern
- Blockera port 80 i din konsol och avvisa inkommande HTTP-trafik, använd endast HTTPS. När konfigurationen är klar är det även möjligt att göra en extern konfiguration via HTTPS.
- Begränsa åtkomsten till hanteringsgränssnittet till endast vissa IP-adresser längst ner i Steg 3 - Serverinställningar
- Konfigurera brandväggen

# Allmänna inställningar

## Översikt över konton

### Kontoinformation

#### Översikt

Här kan du se en översikt över ditt AppTec360-konto.

| | |
|---|---|
| Företagets namn | Ditt företagsnamn |
| Datum för skapande | Datum för skapande av ditt konto |
| Typ av licens | Paid = betald licens<br>Gratis = obetald licens<br>Konton på en OnPremise Appliance kommer alltid att visas som betalda av tekniska skäl |
| Kundidentifierare | Identifierare för ditt konto (detta är INTE ditt kundnummer) |
| Licensens utgångsdatum | Utgångsdatum för din AppTec360-licens |
| ContentBox-licens | Free = gratis licens för 25 enheter<br>Paid = betald licens för x enheter |
| Startramp | Visar om du kan använda den anpassade startprogrammet för Android eller inte |
| Apparater | Antal licenser som används för närvarande / totalt antal licenser |
| Kontaktpersoner | Tillhandahållen kontaktperson |
| Telefon | Uppgivet telefonnummer |
| E-post* | Angiven e-postadress |
| Rotanvändare | Root-användare som kan logga in |
| Programvaruversion | Aktuell version av programvaran |

**Notera: Den e-postadress som visas här är den som du angav när du registrerade kontot. Baserat på detta kommer en användare att skapas i trädet för användare/enheter och kan modifieras. Om du redigerar den här användaren ändras e-postadressen som du måste använda för att logga in, men inte informationen i kontoöversikten. .*

## Bugg-rapport

En felrapport kan skickas direkt till supporten för att rapportera problem eller buggar och innehåller information och loggar om ditt konto och din installation.

| | |
|---|---|
| Ämne | Ämnet för felrapporten. Inkludera ett ärendenummer om du vill lägga till detta i ett befintligt supportärende. |
| Förväntat beteende | Beskriv i detalj vad du gjorde och vad du förväntade dig skulle hända |
| Faktiskt beteende | Beskriv i detalj vad som exakt hände. Vänligen citera felmeddelanden EXAKT. Det hjälper också om du lägger till skärmdumpar i bilagan. |
| Vid vilken tidpunkt upplevde du problemet? | Ange en exakt tidpunkt när du fick ett specifikt felmeddelande/problem.<br>I bästa fall inkludera även sekunder, t.ex. 18:55:27 |
| Kan problemet replikeras? Om ja, hur (i detalj)? | Beskriv i detalj hur du kan återskapa problemet. |
| Har denna funktion tidigare fungerat som du förväntade dig? Om ja, fram till när? | Lämna tom om du inte vet. |
| Gjordes några specifika ändringar i systemet innan detta problem uppstod? Om ja, vilka ändringar (i detalj)? | Nämn alltid vad din senaste förändring eller åtgärd var innan frågan dök upp, även om du tycker att det är irrelevant. |
| Om tillämpligt: Vilka enhetsmodeller och OS-versioner påverkas? | Ange alltid den exakta OS-versionen (t.ex. iOS 14.7.1 eller Android 11) |
| Om tillämpligt: Vilken är den offentliga IP-adressen och/eller serienumret för enheten? | Namnge minst en, även om alla enheter är drabbade. |
| Inkludera loggfiler | Markera detta för att skicka loggfilen med felrapporten. Detta är rekommenderat att göra. |
| Hämta aktuellt VPP-tillstånd från Apple och inkludera i buggrapporten | Innehåller information om VPP-licenstilldelningar. Aktivera detta endast om du ombeds att göra det av supporten eller om ditt problem handlar om VPP. |
| Bilaga | Bifoga alla filer som kan vara användbara (t.ex. skärmdumpar av ett felmeddelande) |

## Begäran om funktion

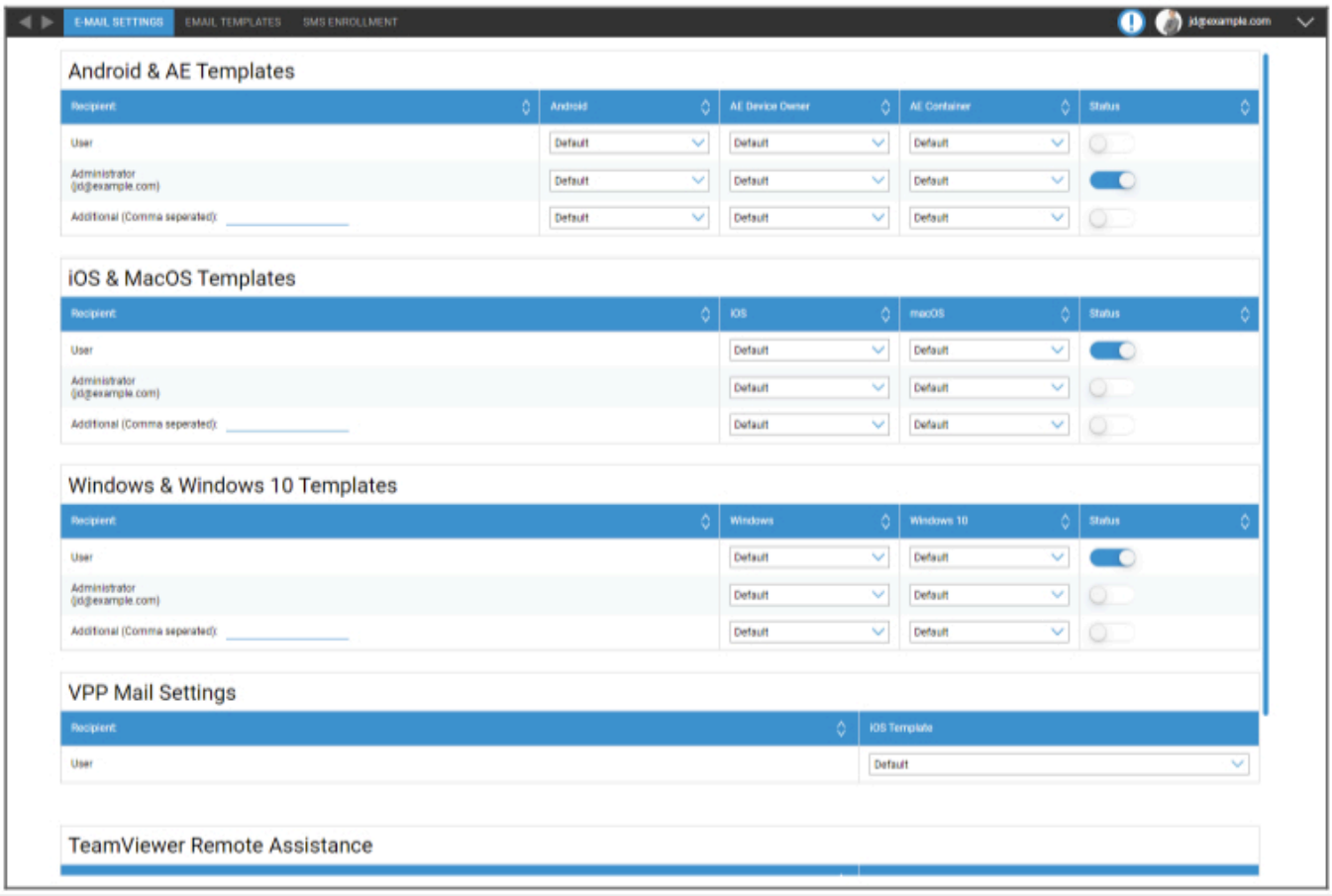
En funktionsbegäran kan skickas direkt till supporten. Den kan innehålla en begäran om en specifik funktion eller en förbättring av

| | |
|---|---|
| Sammanfattning | En kort sammanfattning av ditt problem |
| Beskrivning | En detaljerad beskrivning av ditt problem, var så specifik som möjligt |
| Bilaga | Bifoga filer till felrapporten |

# Global konfiguration

## Inställningar för eMail

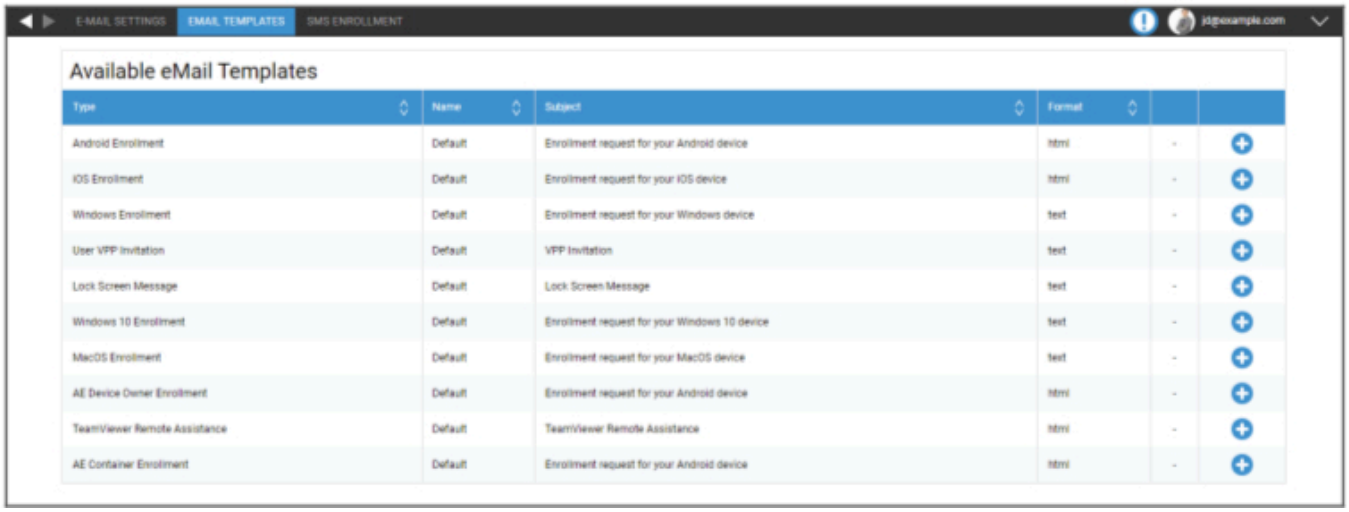
Här kan du ange vem som ska få ett e-postmeddelande när en registreringsbegäran genereras och vilken textmall som ska användas för det meddelandet.



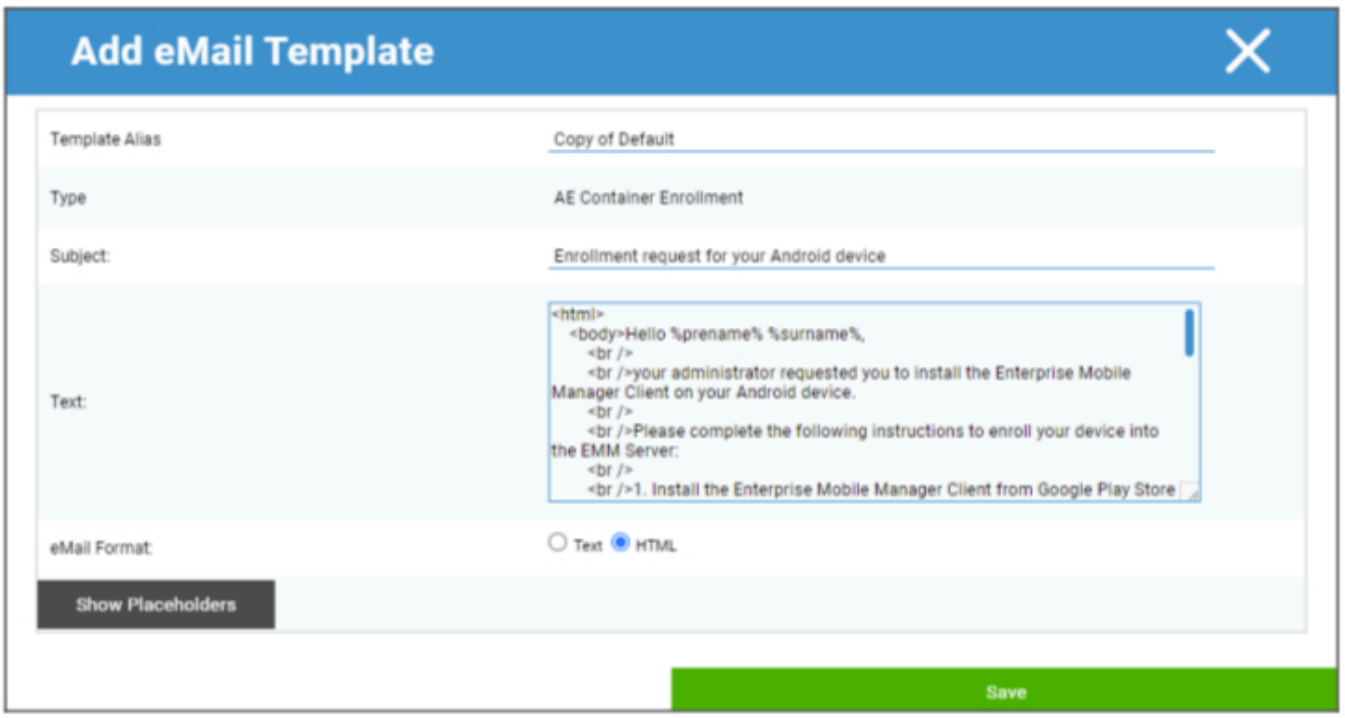
## Mallar för e-post

Här kan du skapa och redigera dina mallar för olika scenarier. Dessa kan vara i normal textform eller i HTML. Med HTML kan du bättre kontrollera formateringen av din text.

Standardmallarna kan inte redigeras eller raderas.




Du kan också använda platshållare som variabler som automatiskt ersätts. Klicka på "Visa platshållare" när du redigerar för att se tillgängliga platshållare. Olika kategorier har olika platshållare.




## SMS-inskrivning

Här kan du avaktivera/aktivera SMSregistreringsprocessen.

(Standard: avaktiverad)

Du kommer också att se en display som visar hur många SMS Credits som fortfarande finns tillgängliga.

SMS-krediter måste köpas separat.

# Integritet

## GPS-åtkomst

Här kan du skydda GPS-visningen för varje enhet med 1 eller 2 lösenord (fyrögonprincipen). Du kommer att uppmanas att ange ditt/dina lösenord varje gång du försöker få tillgång till en enhets plats.

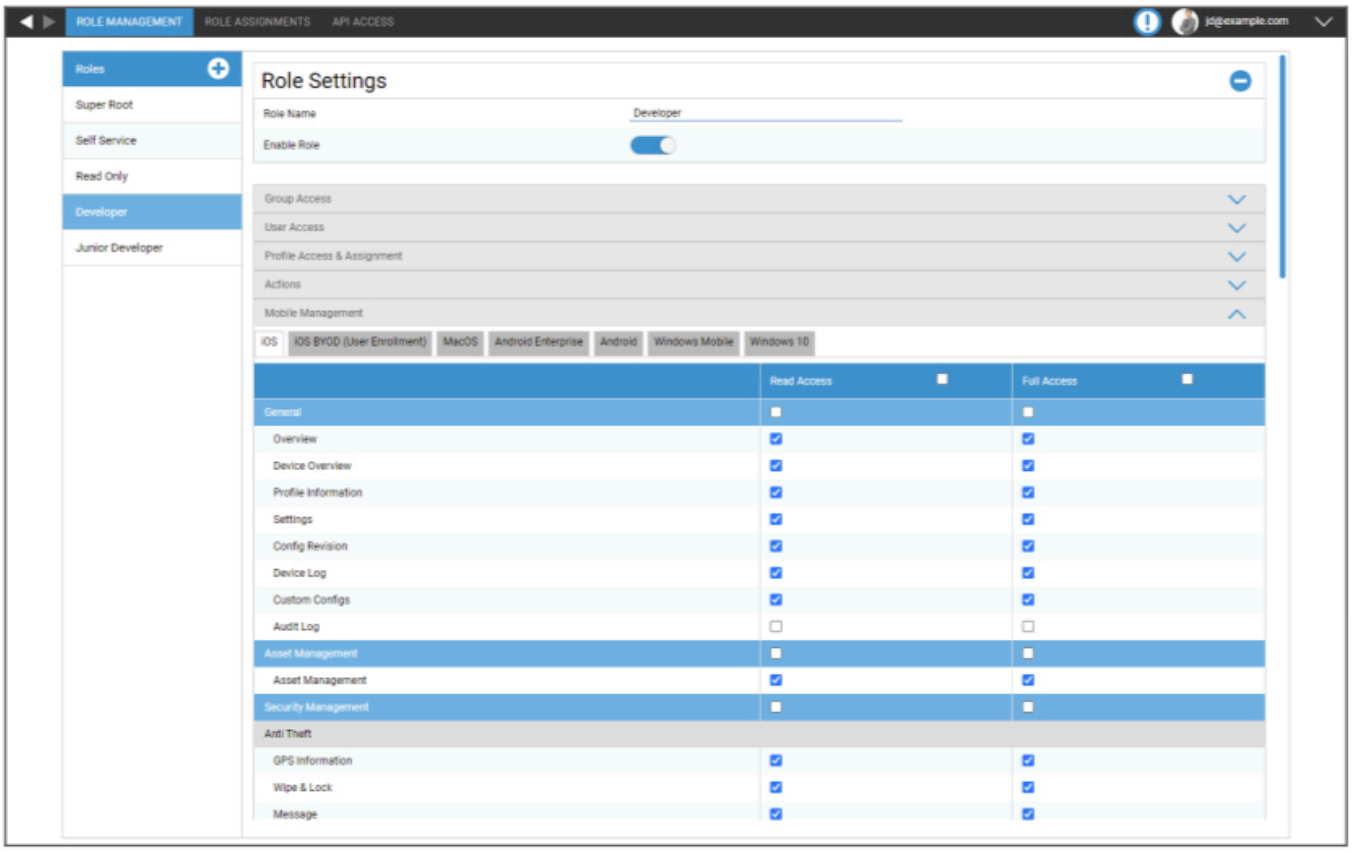
| | |
|---|---|
| Begränsa åtkomst till GPS-inställningar | Off = funktionen är avstängd och inget lösenord krävs för lokalisering |
| | On = funktionen är aktiverad och ett lösenord krävs för lokalisering |
| Skyddsmetod | Använd ett lösenord = använd ett lösenord för lokalisering |
| | Använd två lösenord = använd två lösenord för lokalisering |
| Ange lösenord (1) | Ange valt lösenord |
| Upprepa lösenord (1) | Ange valt lösenord på nytt |
| valfritt: Ange lösenord 2 | Ange det andra valda lösenordet |
| valfritt: Upprepa lösenord 2 | Ange det andra valda lösenordet igen |

Obs: Efter att du har ställt in din(a) lösenkod(er) måste du ange den en gång till innan den är helt aktiverad.

# Rollbaserad åtkomst

## Rollhantering

Rollerna definierar vad en användare kan se och göra när han eller hon loggar in på managementkonsolen. Detta gör att du kan skapa användare som kan logga in men har begränsad funktionalitet.



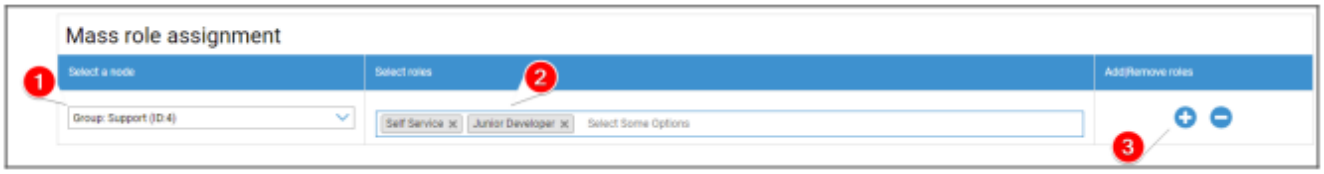

Super Root-rollen är en standardroll som alltid kan se och ändra allt. Den kan inte ändras eller raderas. Self Service-rollen kan bara se sina egna användare och enheter. Du kan kombinera Self Service och en anpassad roll för att t.ex. tillåta användare att logga in och registrera enheter på egen hand och endast för sin användare.

Anpassade roller kan aktiveras eller inaktiveras manuellt. Nya roller är inaktiverade som standard. Användare med en inaktiverad roll arbetar som om de inte hade rollen. Detta gör att du t.ex. tillfälligt kan begränsa en viss roll från deras åtgärder.

Alla behörigheter är uppdelade mellan "Läsbehörighet" och "Fullständig behörighet". Om du ger en roll läsbehörighet kan den se den specifika delen av konsolen. Om du ger dem full åtkomst kan rollen se och ändra den specifika delen av konsolen.

## Tilldelning av roller

Här får du en översikt över alla användare som har en roll och kan se vilken roll de har. Du kan också tilldela en roll till användare eller hela grupper här:

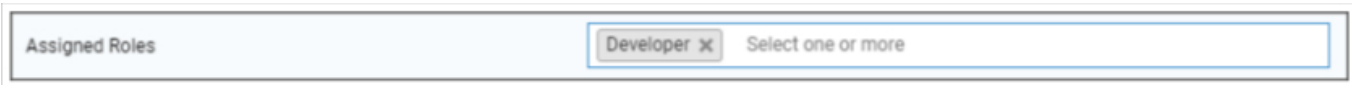



1. Välj vilken grupp eller användare som du vill lägga till eller ta bort roller för. Du kan antingen välja en enskild användare eller välja en grupp. När du väljer en grupp kommer din ändring att påverka alla användare i den gruppen och alla användare i undergrupper inom den valda gruppen.
2. Välj vilken roll du vill lägga till eller ta bort. Du kan välja en eller flera 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. Spara för att avsluta processen. Användare som tidigare inte hade någon roll och "Kan logga in" inaktiverat kommer automatiskt att få ett e-postmeddelande med en länk för att ange ett lösenord.

Under Massrolltilldelning hittar du en översikt över de tilldelade rollerna. Där kan du också manuellt ändra roller för specifika användare.

## Tilldelning av en roll

För att tilldela en roll till en användare måste du gå till Mobile Management, där du hittar trädet över dina grupper, användare och enheter. Redigera användaren för att tilldela en roll. Alternativt kan du använda den ovan nämnda metoden för endast enstaka användare också.



# API-åtkomst

## Åtkomst till AppTec360 REST API

AppTec360 REST API kräver en autentiseringstoken (API-nyckel) och en privat nyckel som måste genereras i Managment Console.

För att göra detta logga in i AppTec360 EMM och gå till

Allmänna inställningar → Rollbaserad åtkomst → API-åtkomst och lägg till en ny nyckel.

Du måste välja en användare vars behörigheter ska gälla för API-nyckeln.

Den privata nyckeln kan bara laddas ner en gång. När nedladdningen har påbörjats raderas nyckeln och knappen "Download" försvinner.

Om du tappar bort din privata nyckel måste du skapa en ny API-nyckel.

## Allmänna regler

- REST API finns tillgängligt under bas-URL:en:

/public/external/api

- Alla förfrågningar måste skickas via POST.
- REST API stöder endast förfrågningar via HTTPS.
- Förfrågningar måste innehålla följande rubriker:

| Rubrikens namn | Värde för rubrik | Beskrivning |
|---|---|---|
| Innehållstyp | applikation/json | fast |
| autentisering | 123...xyz | API-nyckel från fliken "API-åtkomst" |
| Underskrift | Base64-kodad signatur | Signatur för den nyttolast som genereras med privat nyckel från fliken "API-åtkomst" |

- Förfrågningsunderlaget måste vara ett json-kodat objekt som innehåller följande värden:

| Fält | Fält Exempel Värde | Beskrivning |
|---|---|---|
| Api | v2/enhet/listaenheter | Namn på API:et |
| tid | 1529662725 | Unix-tidsstämpel (UTC) för klientmaskinen.<br>Den maximalt tillåtna tidsskillnaden<br>mellan klienten och servern är 30<br>minuter. |

- Om API:et lyckas returnerar det de begärda uppgifterna (se Frågor nedan) och en HTTP-statuskod 200.
- Om ett fel inträffar kommer HTTP-statuskoden att vara mellan 4xx och 5xx beroende på felet och svarsobjektet kommer att innehålla en array med nyckeln "errors", som innehåller en lista över felmeddelanden som kan läsas av människor.
- Om det inte finns några matchande data för en enhet returneras en tom array.
- Om ett enhets-ID inte finns kommer returdata att vara null.

## Exempel på begäran

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]}}

## Frågor

**Lista alla enheter**

Funktionalitet: Returnerar en lista över alla enheter som innehåller enhets-ID, IMEI och serie
API URI: v2/device/listdevices
Obligatoriska parametrar: inga
Valfria parametrar: inga

Exempel på begäran Body


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


Exempel på svar Body


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

**Hämta lista över (GPS)-positioner**

Funktionalitet: Returnerar en lista över alla lagrade positionsloggposter för enhets-ID:n
API URI: v2/device/listposition
Obligatoriska parametrar: "ids" - Array av enhets-ID
Valfria parametrar: none

Exempel på begäran Body


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


Exempel på svar Body


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

**Hämta tillgångskarta**

Funktionalitet:
Returnerar en lista över alla lagrade möjliga tillgångar som kan begäras med Hämta alla tillgångsdata. Du kan antingen använda den mänskliga läsbara formen eller tillgångstaggen för att begära data.
API URI: v2/device/getassetmap
Obligatoriska parametrar: inga
Valfria parametrar: inga

Exempel på begäran Body

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

Exempel på svar Body

Detta svar förkortades för läsbarhetens skull.

{
"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": []
}

**Hämta alla tillgångsdata**

Funktionalitet: Returnerar en lista över begärda tillgångsdata för enhets-ID:n
API URI: v2/device/getassetdata
Obligatoriska parametrar: "ids" - Array av enhets-ID:n
Valfria parametrar:
"assetkeys" - Nycklar till tillgångsdata som ska returneras. Om inget anges kommer alla tillgängliga tillgångsdata att returneras
. Du kan få en lista över tillgångsnycklar med hjälp av Get asset map.

Exempel på begäran Body


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


Exempel på svar Body


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

## Exempel på kod i Python3

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

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

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

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

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

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

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

# Apple-konfiguration

## APNS-certifikat

Här kan du ladda upp ett APNS-certifikat. Detta krävs för att hantera iOS- och MacOS-enheter.

Obs: APNS-certifikatet är endast giltigt i ett år. Det måste förnyas innan det löper ut. Förnyelseprocessen är identisk med skapandet (se nedan) och tar bara några minuter.

Om du glömmer att förnya detta i tid kan du inte göra ändringar i dina redan registrerade enheter **och du måste registrera alla enheter igen**.


### Steg 1

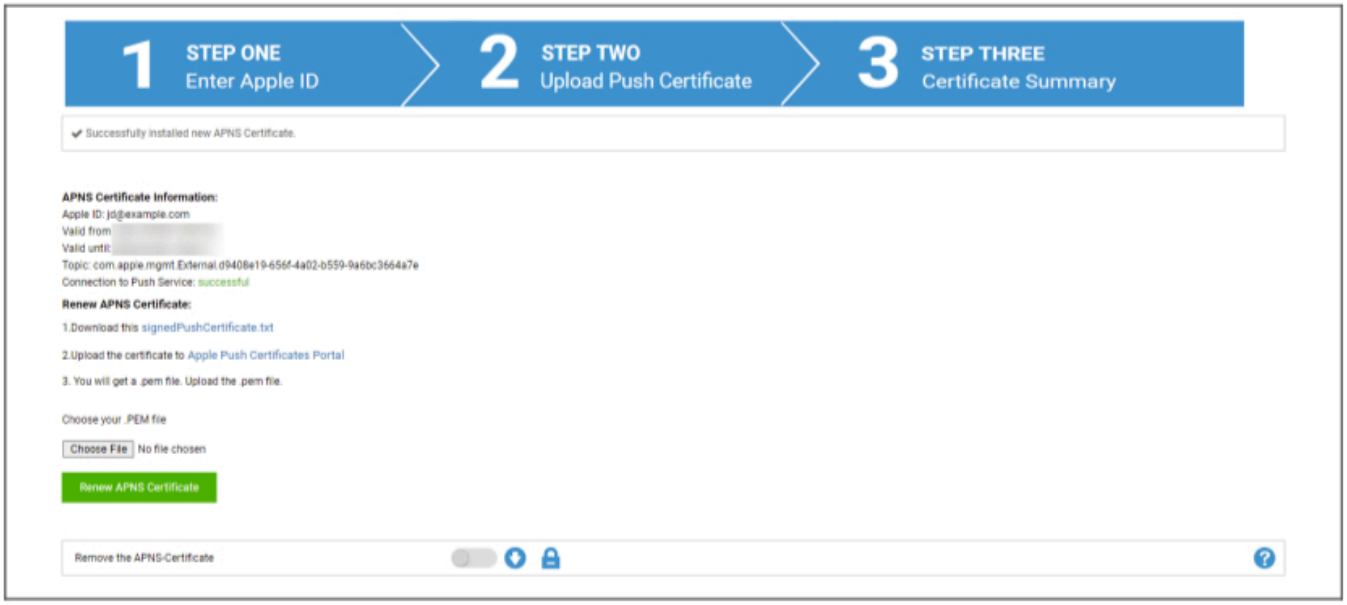
- Ange först ditt Apple-ID som du vill använda för att skapa APNS-certifikatet.

Obs: Detta Apple-ID används endast för att skapa APNS-certifikat. Detta Apple-ID har inget att göra med enheterna och enheterna kommer inte att känna till detta Apple-ID. Dessutom behöver du också tillgång till detta Apple-ID för att förnya APNS-certifikatet. Därför rekommenderas det att använda ett generiskt Apple-ID och dokumentera inloggningsuppgifterna. En påminnelse skickas till den använda e-postadressen för Apple ID innan APNS-certifikatet löper ut.

- Klicka på "Nästa steg" för att fortsätta.
- (valfritt) Du kan också återställa det tidigare raderade APNS-certifikatet om du raderade det av misstag


## Steg 2

- Ladda ner signedPushCertificate.txt
- Gå till https://identity.apple.com/pushcert/ och logga in med Apple-ID från steg 1
- Klicka på "Skapa ett certifikat"
- (valfritt) ange en anteckning. Detta kan vara användbart om du hanterar flera hyresgäster för att enkelt identifiera dem.
- Klicka på "Choose File" för att välja den tidigare nedladdade signedPushCertificate.txt
- Klicka på "Ladda upp".
- Du kommer nu att se en bekräftelse på att du har skapat ett APNS-certifikat.
- Klicka på "Download" och spara den.
- Gå tillbaka till hanteringskonsolen.
- Klicka på "Choose File" och välj det APNS-certifikat som du vill ladda upp.
- Klicka på "Ladda upp"




## Steg 3

Du har nu konfigurerat APNS-certifikatet och kan nu hantera iOS- och MacOS-enheter.

I steg 3 ser du en översikt över dina APNS-certifikat som används för närvarande.

Du har också möjlighet att förnya APNS-certifikatet genom att följa stegen som visas på skärmen. Tänk på att förnya det innan det löper ut.

När du förnyar APNS-certifikatet, kom ihåg att logga in med det Apple-ID som visas i steg 3 och även att förnya det tidigare använda certifikatet och INTE skapa ett nytt. Du kommer att se "ämnet" för APNS-certifikatet i steg 3 och när du klickar på "i" i Apple Push Certificate Portal. Detta är det unika ID som identifierar certifikatet. Detta hjälper dig att identifiera rätt och förnya rätt certifikat.

När du får "Error: The Push Certificate has a different topic!" när du förnyar betyder det att du har förnyat ett annat certifikat eller skapat ett nytt.

Om du vill ladda upp ett nytt certifikat, t.ex. om du inte längre kan komma åt det tidigare använda Apple-ID:t, måste du först radera det aktuella uppladdade certifikatet.

Om du tar bort APNS-certifikatet innebär det att du inte längre kan göra ändringar för de enheter som för närvarande är registrerade förrän du registrerar dem igen. Se därför till att du är förberedd på detta och ta endast bort certifikatet om det inte finns något annat sätt.

## Hanterad åtkomst

Här kan du aktivera User-Enrollment för iOS-enheter och Shared iPad för iOS-enheter.

### Registrering av användare

"User Enrollment" aktiverar ett särskilt läge för BYOD-enheter.

För varje användare måste ett hanterat Apple-ID skapas i Apple Business Portal.

Under registreringsprocessen kommer användarna att bli ombedda att uppge sina Apple-ID-referenser.

"User Enrollment" garanterar maximal säkerhet för användaren eftersom det endast tillåter en begränsad uppsättning inställningar och begränsningar som kan konfigureras av MDM.

Hanterad domän:

Den domän som används för att mappa användarens e-postadress till deras hanterade Apple-ID (måste vara i formatet: "@appleid.company.com"), t.ex. john.doe@example.com kommer att mappas till john.doe@appleid.company.com

Kontrollera Apple Business Manager för att se din Managed Domain

### Delad iPad

En delad iPad är en DEP-enhet som är konfigurerad med en speciell DEP-profil.

Detta gör att flera användare kan logga in på enheten med hjälp av sitt hanterade Apple-ID.

Det hanterade Apple-ID:t måste skapas i Apple Business Portal eller Apple School Manager.

Användare som loggar in på en delad iPad blir ombedda att ange sina Apple-ID-uppgifter.

Hanterad domän:

Den domän som används för att mappa användarens e-postadress till deras hanterade Apple-ID (måste vara i formatet: "@appleid.company.com"), t.ex. john.doe@example.com kommer att mappas till john.doe@appleid.company.com

Kontrollera Apple Business Manager för att se din Managed Domain

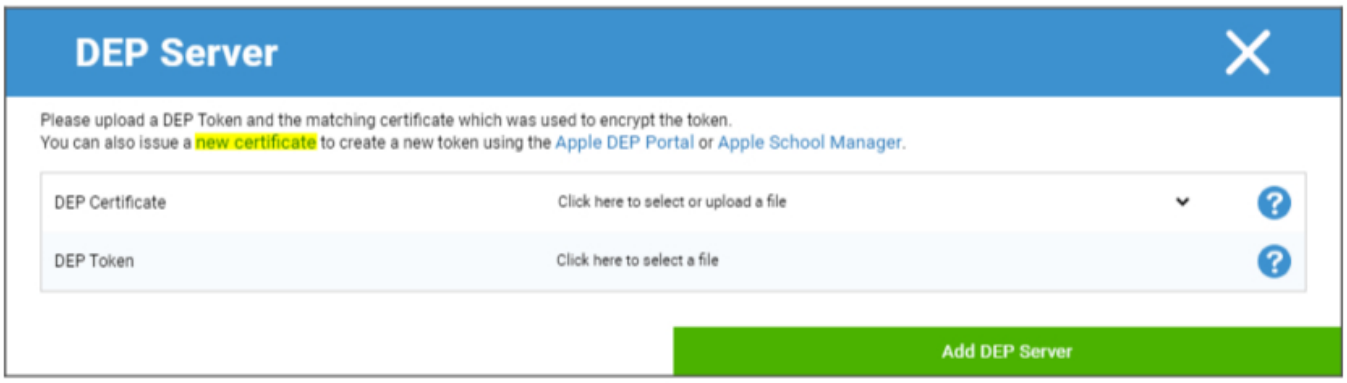
# DEP

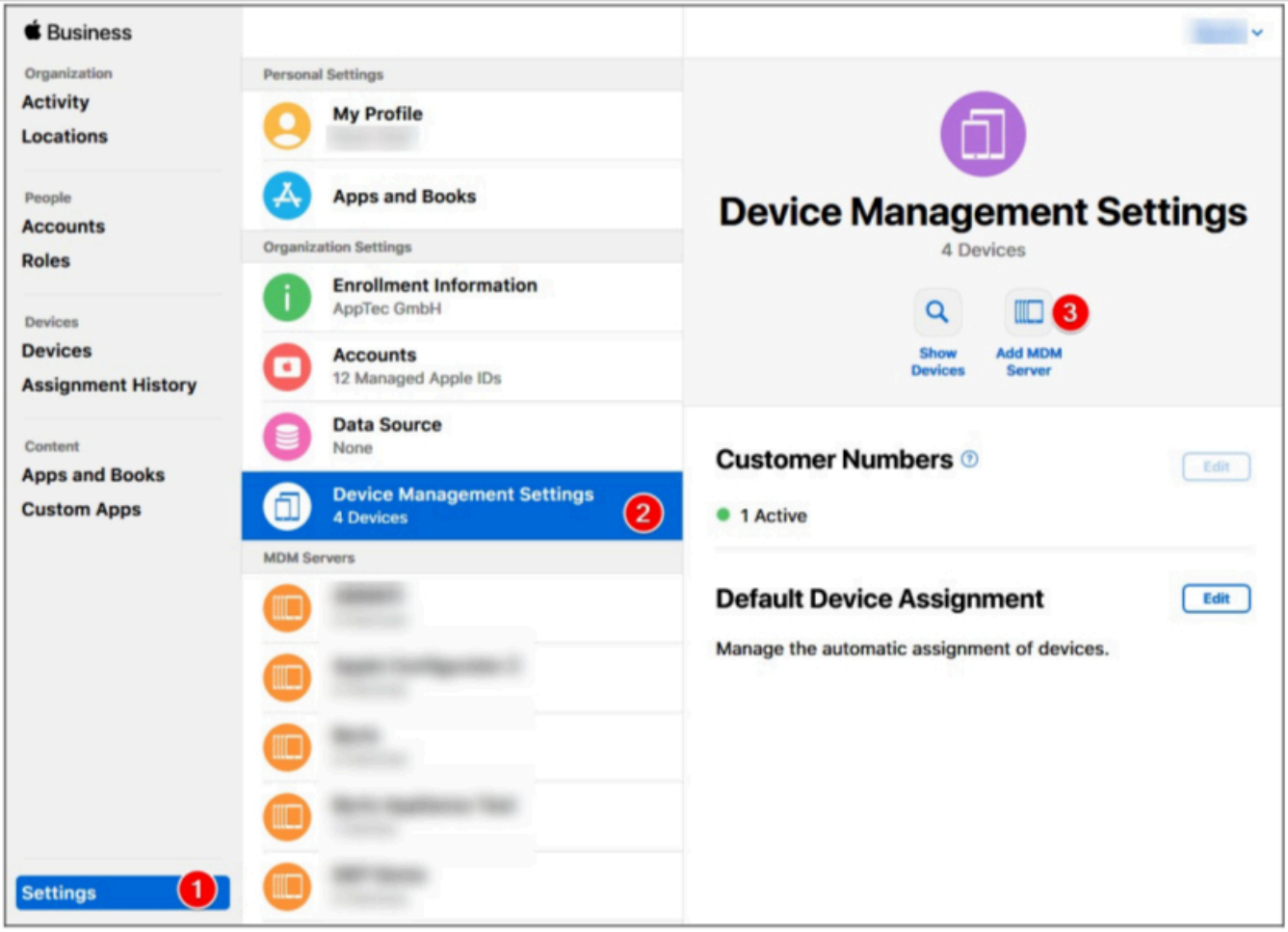
DEP (Device Enrollment Program) gör att du enkelt kan registrera enheter i MDM. När du använder DEP kommer enheterna automatiskt att anslutas till MDM när du konfigurerar enheten. Du kan också hoppa över nästan alla installationssteg som vanligtvis är obligatoriska på iOS.

Tänk på att du måste köpa enheterna från en återförsäljare som stöder DEP. Kontakta din återförsäljare eller Apple om du vill ha mer information.

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


Klicka på "+" för att lägga till en DEP Token. I popup-fönstret klickar du på "nytt certifikat" i texten (markerat med gult i bilden nedan). Detta kommer att generera och ladda ner ett DEP certifikat. Gå därefter till Apple Business Manager(https://business.apple.com/) eller Apple School Manager(https://school.apple.com/).

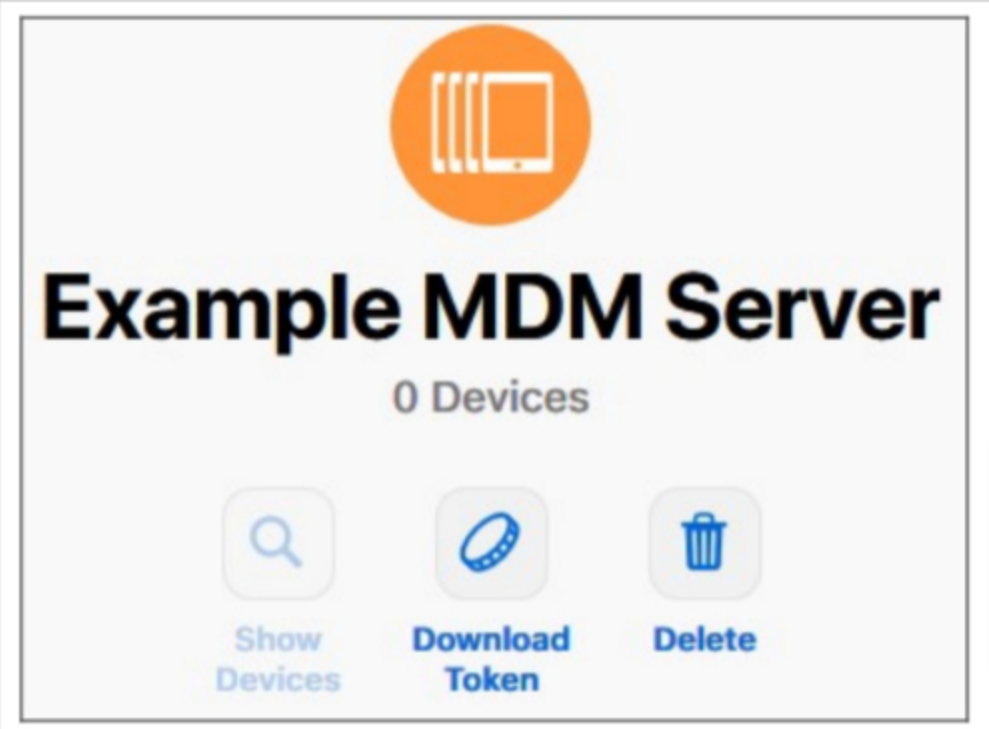





I Apple Business Manager följer du stegen som visas i bilden ovan. Inställningar → Inställningar för enhetshantering → Lägg till MDM-server.

Ge servern det namn du vill ha och ladda upp det tidigare nedladdade DEPcertifikatet under MDM Server Settings → Upload Public Key och klicka på "Save".

Du kommer nu att ha alternativet "Download Token". Klicka på detta och spara det. Token är endast giltig i 1 år. Men genom att klicka på "Download Token" igen får du en ny, vilket gör det mycket enkelt att förnya token.




Du kan nu gå tillbaka till MDM, där du tidigare hämtade DEPcertifikatet. Om du inte stängde fliken ska popup-fönstret för att lägga till en DEP-server fortfarande vara öppet och DEP Certificate ska redan vara valt. Du kan nu ladda upp din Token i fältet "DEP Token" och klicka på DEP Server.

I kolumnen "**Devices**" ser du antalet enheter som har tilldelats denna DEP-server. Enheter som läggs till i denna DEP-server skapas automatiskt i DEP-poolen i Mobile Management.

Du kan klicka på det här numret för att få en översikt över alla dina DEP-enheter och deras status.

Obs: Beroende på ditt arbetsflöde eller din konfiguration i Business Manager kan det hända att du måste tilldela dessa enheter till DEP-servern manuellt. Du kan också ställa in en standard DEP-server i Apple Business Manager för nya enheter.

I kolumnen "**Profiler**" ser du hur många DEP-profiler du har. Du kan också klicka på detta nummer för att se detaljer om dina DEP-profiler och du kan radera gamla/icke använda profiler här. Det är för närvarande inte möjligt att ändra dessa. Om du vill göra en ändring måste du skapa en ny.

I kolumnen "**Last Synchronization**" kan du manuellt synkronisera DEP-servern (t.ex. om du just har lagt till en ny enhet i DEP) och se datumet för den senaste lyckade synkroniseringen.

I kolumnen "**Auto Profile**" kan du ange en DEP-profil som automatisk standard. Denna profil kommer automatiskt att tilldelas nya enheter. Om du inte ställer in en Auto Profile måste du manuellt tilldela en profil till nya enheter varje gång.

I kolumnen "**Add Profile**" kan du lägga till en ny DEP-profil. Enheten kommer att ta emot denna i början av enhetens installation. DEP-profilen definierar hur enheten ska installeras och vilka installationssteg som ska hoppas över.

Obs: efter att en enhet har registrerats kan dessa inställningar endast ändras genom att utföra en fabriksåterställning och registrera enheten med en ny profil. Detta gäller särskilt för "**Flyttbar**" och "**Tillåt parkoppling**". När det gäller "**Allow pairing**" rekommenderas att du aktiverar detta, eftersom det kan inaktiveras via MDM-restriktioner, men det kan inte aktiveras igen om det har inaktiverats i DEP-profilen.

I kolumnen "**Edit**" kan du ladda upp en ny token, t.ex. när du förnyar Token.

## Konfigurator & URL

### URL:er för poolregistrering

Här kan du skapa en URL för registrering och en QR-kod för registrering som är giltig ett visst antal registreringar och fram till ett visst datum. Detta gör att du kan registrera flera enheter med endast en länk eller QR-kod.

Enheter som registrerats med denna URL eller QR-kod kommer att finnas i Pool i Mobile Management och du måste manuellt tilldela dem till en grupp eller användare i efterhand.

Obs: detta gäller endast för manuell registrering. Använd inte denna URL om du registrerar enheterna via Apple Configurator

### MDM-profil – Apple Configurator

Här kan du hämta den URL du behöver när du registrerar enheter via Apple Configurator. När du förbereder enheter med Apple Configurator kan du lägga till enheterna i MDM i samma process. Apple Configurator kräver den här URL:en för detta.

Enheter som läggs till via Apple Configurator kommer att finnas i Poolen i Mobile Management och du måste manuellt tilldela dem till en grupp eller användare efteråt.

Du hittar också en .mobileconfig-fil här som kan användas för att registrera enheterna via Apple Configurator. Hur som helst rekommenderas att du använder URL:en.

# Android-konfiguration

## Android-konfiguration

| | |
|---|---|
| Avinstallera skydd | Om den här funktionen är aktiverad kan användaren inte avaktivera enhetsadministratören utan att ange det lösenord som MDM-administratören har ställt in. Lösenordet ställs in under registreringen, så enheterna måste registreras på nytt för att lösenordet ska kunna uppdateras.<br>Det finns två alternativ för att ta bort enhetsadministratörerna:<br>1. Manuellt på enheten<br>◦ Öppna EMM-appen på enheten<br>◦ Växla till fliken Status<br>◦ Tryck på "Avinstallera skydd"<br>◦ Ange lösenordet Du kan använda Revision för att få rätt lösenord från "Lösenordshistorik" i konsolen.<br>◦ Bläddra ner och tryck på den nyligen tillagda punkten, "Tryck för att avinstallera AppTec360 MDM App" (du har 20 sekunder på dig att utföra denna uppgift)<br>◦ Bekräfta dialogen "Avinstallera AppTec360 MDM App" med "ok". Detta kommer att avregistrera enheten från konsolen.<br>◦ För att ta bort appen från enheten, bekräfta dialogen "AppTec360 MDM kommer att avinstalleras" med "UNINSTALL"<br>2. den automatiska (konsol)<br>◦ Välj enhet i konsolen<br>◦ Klicka på den blå kugghjulsikonen och välj "Enterprise Wipe"<br>Obs: Endast tillgängligt med Android 4.x och lägre versioner eller på enheter med KNOX API (Samsung-enheter) |

| | |
|---|---|
| Lösenord för avinstallation (Revision x) | Det fastställda lösenordet, med vilket användaren kan ta bort enhetsadministratören<br>Revision x = räknare, hur ofta lösenordet redan har ändrats Det är viktigt vilket lösenord användaren behöver, eftersom det är möjligt att enheten inte har kommunicerat med AppTec360-servern och att det senaste lösenordet därför inte har överförts ännu |
| Lösenordshistorik | När du klickar på den blå knappen ("Visa historik") kan du se de lösenord som du tidigare har skapat |
| Utökat skydd mot avinstallation | Detta alternativ ger skydd mot icke-SAFE-enheter<br>Så länge denna inställning är aktiverad är det inte möjligt att enkelt avaktivera enhetsadministratören |
| Uppmana användaren att avinstallera blockerade appar? | Om möjligt kommer blockerade appar inte bara att blockeras utan också avinstalleras automatiskt. Användaren uppmanas att avinstallera blockerade appar om ingen automatisk avinstallation är möjlig. |
| Intelligent System App Blockering | Om vitlistning är aktiverat blockerar Android MDM-klienten alla användarinstallerade appar. Aktivera den här inställningen för att blockera alla systemappar som kan startas i vitlistningsläge. |

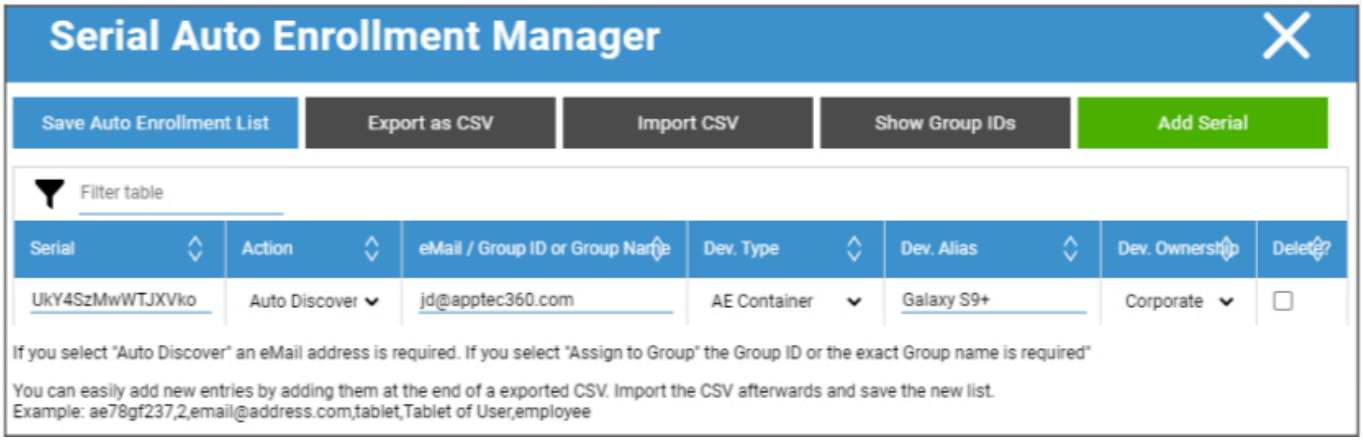
## Automatisk registrering

Här kan du aktivera funktionen Auto Enrollment så att dina enheter registreras automatiskt när AppTec360 MDM Client öppnas på enheten.

Viktigt: Denna registreringsmetod är föråldrad och fungerar inte längre på Android 10 eller högre. När du använder Android 7 eller högre bör du ändå registrera enheter som Android Enterprise fullt hanterade. Om du vill använda Android Enterprise BYOD-containern och du använder Android 10 eller senare måste du registrera enheten manuellt via referenser, QR-kod eller SMS. Hur som helst används Auto Enrollment List fortfarande för att automatisera registreringsprocessen för t.ex. AE Enrollment, Knox Enrollment, etc.

Hur som helst, Auto Enrollment List används fortfarande för att automatisera registreringsprocessen för t.ex. AE Enrollment, Knox Enrollment, etc.

Genom att antingen klicka på "Serial Manager" eller "IMEI Manager" kan du lägga till Serial respektive IMEI för dina enheter. Det är inte nödvändigt att göra båda för dina enheter, bara en räcker.




**Action** definierar om enheterna ska registreras i poolen, en användare eller en grupp.

Du kan också exportera och importera en .csv-fil och filtrera dina poster efter nyckelord.

# Android Företag

Här kan du konfigurera Android Enterprise. Detta är nödvändigt för att kunna använda alla funktioner i Android Enterprise.

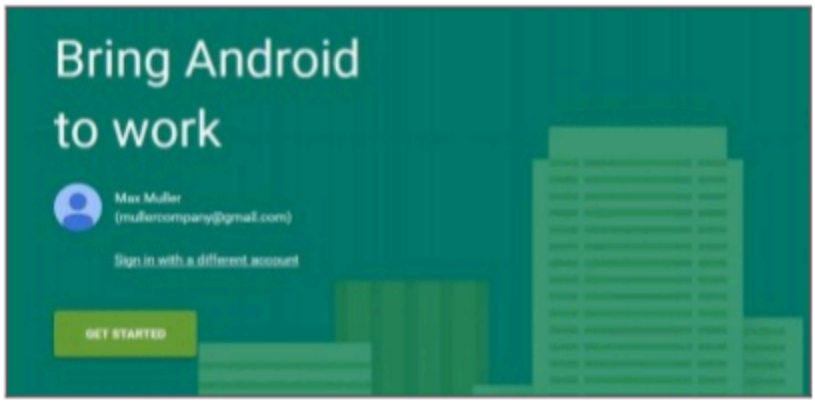
## Första metoden: Android Enterprise-konto (Google-konto)

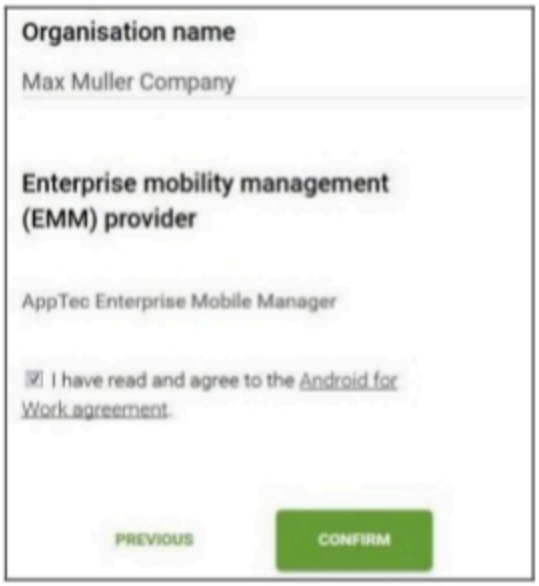
Tryck först på "Prepare Setup", och efter en kort stund ska knappen "Start Setup" visas.

Detta kommer att ta dig till Googles Android Enterprise Setup Page.

Logga in med det Google-konto som du vill använda, om du inte redan är inloggad, och tryck på "Kom igång".

Nu kan du ange namnet på ditt företag. När du har gjort det, markera kryssrutan och tryck på "Bekräfta"




I det sista steget kan du slutföra din registrering och bör återvända till konsolen. Om allt fungerade bör det se ut så här:

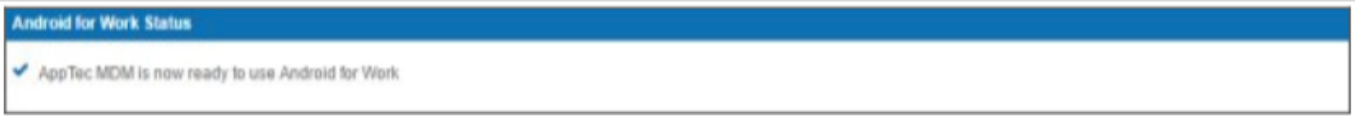

Nu kan du börja konfigurera din Android Enterprise Container.

## Andra metoden: G-Suite-konto

Tryck på "Use G-Suite" och logga in på ditt Google Admin-konto. Där går du till "Säkerhet" -> "Visa mer" -> "Hantera EMM-leverantör för Android" och genererar en Token. Obs: Om du inte ser Android Enterprise Settings i ditt G-Suite-konto måste du gå till "Hämta fler appar och tjänster" och lägga till Android-enhetshanteringen. Ange nu Token och din primära domän i vår konsol och klicka på "Spara ändringar". När du är klar klickar du på "Använd Android Enterprise-konto".

Nu bör du se knappen "Skapa servicekonto". Klicka på den. Denna process kan ta några ögonblick.

Om allt fungerade skulle det se ut så här:




Nu kan du börja konfigurera din Android Enterprise Container.

## Skydd mot fabriksåterställning

Med fabriksåterställningsskyddet kan du binda din enhet till ett valfritt Google-konto, vilket också åsidosätter eventuell befintlig bindning till ett Google-konto. För att använda fabriksåterställningsskyddet måste du först ställa in det här och sedan aktivera det i dina profiler.

För att ställa in Factory Reset Protection, klicka på "FRP Setup" och följ anvisningarna på skärmen.

**OBS: Läs noga igenom och utför stegen. Vi rekommenderar att du gör detta i ett nytt inkognito webbläsarfönster för att undvika att du automatiskt loggar in på fel Google-konto. Du kan helt låsa ut dig själv från enheten om du skulle ange ett felaktigt ID eller förlora åtkomsten till det använda Google-kontot!**

# AE Inskrivning

Här kan du aktivera Android Enterprise Ernollment. Om du använder den här metoden kommer dina enheter att registreras i Android Enterprise Device Owner Mode. I det här läget kommer du att ha full kontroll över enheten.

| | |
|---|---|
| Aktivera AE-registrering | Aktiverar AE-registrering Varning: Om du inaktiverar AE Enrollment kommer befintliga QR-koder och redan konfigurerade NFC-programmeringsenheter att sluta fungera. Om du aktiverar AE Enrollment igen måste du skicka NFC-pushkonfigurationer på nytt / generera nya QR-koder. |
| Aktivera automatisk upptäckt | När en enhet registrerar sig själv via "AE Enrollment" kommer systemet att försöka tilldela den till en användare baserat på den information som anges i Serial / IMEI Whitelist ("General Settings" > "Android Configuration" > "Auto Enrollment"). |
| Blockera okända enheter | Endast enheter som har vitlistats i Serial / IMEI Whitelist ("Allmänna inställningar" > "Android Configuration" > "Auto Enrollment") får registrera sig. |

*Obs för metod 1 & 2: "Välkomstskärm" avser den första skärmen du ser efter fabriksåterställningen. Detta kan se annorlunda ut beroende på vilken Android-version och/eller enhetsmodell du använder.*

## Metod 1: Registrering av QR-kod

(kräver Android 7.0 eller senare) Vi rekommenderar att du alltid använder den här metoden om du kör Android 7 eller senare.

1. Fabriksåterställning av enheten
2. Generera QR-koden för registreringen med hjälp av en av följande två metoder:
   - Klicka i "Allmänna inställningar -> Android-konfiguration -> AE-registrering" på "Generera QR-kod". Välj om du vill hoppa över lagringskrypteringen och/eller om alla systemappar ska tas bort.
   - (Alternativt) Välj en befintlig enhet. I "Device Overview" klickar du på QR-koden som visas där. Välj om du vill hoppa över lagringskrypteringen och/eller om alla systemappar ska tas bort.
3. Tryck nu 6 gånger på välkomstskärmen på din enhet. Detta bör starta QR-registreringsläget.
4. Anslut nu till ett trådlöst nätverk och vänta en kort stund tills QR-kodläsaren är installerad
5. Skanna nu QR-koden
6. Nu är det klart. Din enhet är nu inskriven i Android Enterprise Device Mode.

- a. Om du använde QR-koden i "Allmänna inställningar" kan du hitta din enhet i "Pool -> AE Device Owner Devices". (Tips: Det är möjligt att du måste ladda om webbplatsen för att se enheterna). Om du markerade "Enable Auto Discover" hittar du den i din Auto Discover-användare.
- Om du använde QR-koden för en befintlig enhetsprofil kommer enheten att registreras i den här profilen.

## Metod 2: NFC-registrering

(kräver NFC och Android 6.0 eller senare)

Förberedelser: Ange din WiFi-information i "Allmänna inställningar -> Android Configuration -> AE Enrollment -> Data for NFC provisioning". Använd nu "NFC Device" för att söka efter den enhet som ska bli programmerare. Den här enheten kommer att användas för att skicka registreringsinformationen till de andra enheterna via NFC.

1. Fabriksåterställ din enhet
2. Öppna NFC-parningsappen från AppTec360 på din programmerare
3. Välj om du vill hoppa över lagringskrypteringen och/eller om alla systemprogram ska tas bort.
4. Håll båda enheterna rygg mot rygg
5. Nu bör Android Enterprise Enrollment starkt
6. Du hittar nu din enhet i konsolen
    - a. I poolen, om du inte har konfigurerat Auto Discover
    - b. I användaren har du konfigurerat Auto Discover för
    - c. Tips: Det är möjligt att du måste ladda om webbplatsen för att se enheterna

## Metod 3: Google-konto

(kräver Android 5.1 eller senare)

(Obs: Om du använder den här metoden kommer enheten inte att registreras automatiskt. Istället måste du registrera den manuellt eller automatisera processen genom att använda Auto Enrollment).

1. Fabriksåterställ din enhet
2. Gå igenom installationsstegen tills du kan logga in med ett Google-konto
3. Ange "afw#apptec" som Användarnamn/Mail
4. Tryck på "Nästa"
5. Din enhet är nu en Android Enterprise-enhet

## KNOX Inskrivning

Här kan du aktivera KNOX Enrollment och hitta den information du behöver för att skapa en KNOX Enrollment-profil i KNOX Deployment Portal. Du behöver ett konto på KNOX Deployment Portal för att konfigurera och använda detta.

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

| | |
|---|---|
| Aktivera KNOX-registrering | Aktiverar KNOX-registreringen.<br>Varning för detta: Om du inaktiverar KNOX Enrollment kommer befintliga MDM-profiler att sluta fungera. Om du aktiverar KNOX Enrollment igen måste du uppdatera fältet "Custom JSON Data" i din MDM-profil |
| Aktivera automatisk upptäckt | När en enhet registrerar sig via "KNOX Enrollment" kommer systemet att försöka tilldela den till en användare baserat på den information som anges i Serial / IMEI Whitelist ("General Settings" > "Android Configuration" > "Auto Enrollment"). |

1. Logga in på Samsung KNOX Mobile Enrollment Portal https://eukme.samsungknox.com/itadmin
2. Gå till "MDM-profiler"
3. Klicka på "Lägg till"
4. Välj "Server URI krävs inte för min MDM" och klicka på "Nästa"
5. Skapa nu en profil med den information som visas i managementkonsolen

Nu kan denna KNOX Enrollment Profile installeras direkt på enheten av Samsung om du köper enheterna direkt från Samsung.

Alternativt kan du ladda ner KNOX Deployment App, logga in med ditt KNOX Deployment-konto och skicka KNOX Enrollment Profile via NFC till andra enheter.

Om enheten har en KNOX Enrollment Profile installerad kommer den att ladda ner vår app och registrera enheten, om den har en fungerande internetanslutning.

Enheter som registreras via KNOX Enrollment finns i "Pool -> KNOX Enrollment", eller inom den användare som du angav i Auto Discover.

## Noll beröring

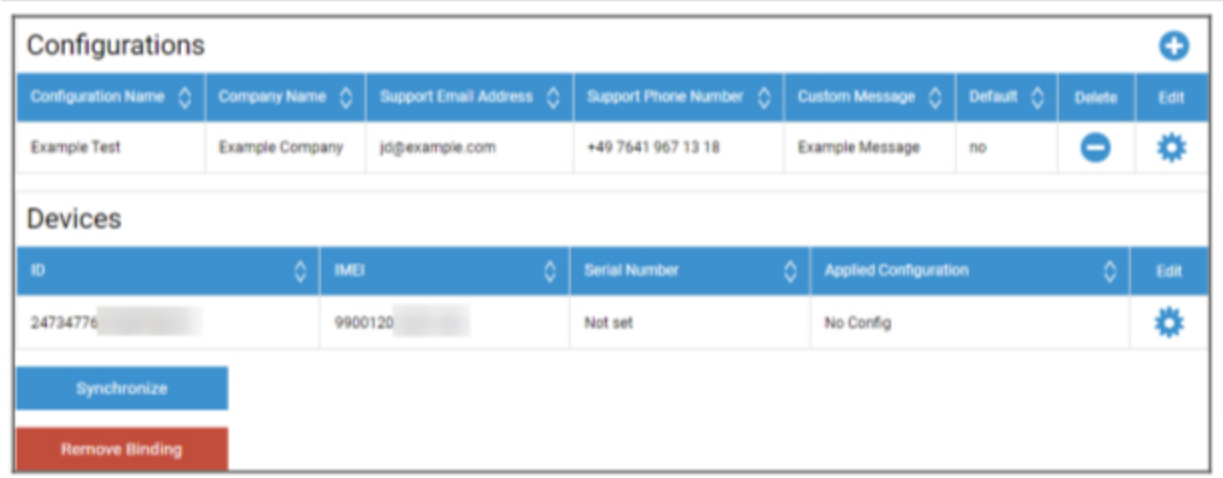
Med Zero-Touch kan du enkelt registrera dina enheter utan att behöva röra vid dem eller konfigurera något på själva enheten. Du behöver bara slå på den, gå igenom konfigurationen som vanligt och enheten kommer att få all information om hur den ska konfigureras och anslutas till MDM helt automatiskt.

För att använda Zero-Touch måste du köpa dina enheter från en återförsäljare som stöder Zero-Touch. Samma återförsäljare skapar också ett konto åt dig i Zero-Touch-portalen. Kontakta din återförsäljare för att få mer information om hur du går tillväga eller om du har problem med att komma åt Zero-Touch-portalen.

Klicka på "Starta installation" för att starta installationen. Du kommer att omdirigeras till en inloggningssida där du måste välja ditt Google-konto som har tillgång till Zero-Touch Portal.

**OBS:** Det är möjligt att välja vilket konto som helst. Se därför till att välja rätt konto i det här steget. Om du inte ser dina enheter/konfigurationer har du troligen använt fel konto.

När du har slutfört inloggningen ser det ut så här:




Klicka på "+" för att lägga till en konfiguration och fyll i fälten som visas på skärmen. Om du aktiverar konfigurationen som standardkonfiguration kommer den automatiskt att tilldelas de nya enheterna. Om du skapar eller ställer in en standardkonfiguration tilldelas den inte till redan befintliga enheter.

Om en enhet inte har någon konfiguration tilldelad kommer den att konfigureras som en vanlig enhet och inte ansluta till MDM. Se därför till att dina enheter har en konfiguration tilldelad.

När du har anslutit ditt konto, dina enheter är synliga och du har tilldelat en konfiguration till dem kan du börja konfigurera enheterna.

Du kan lägga till enheterna i Auto Enrollment List så att de automatiskt registreras i en angiven grupp eller användare. Om du inte har konfigurerat något i listan Auto Enrollment (Automatisk registrering) kommer enheterna att registreras i poolen.

# Windows-konfiguration

## Windows-konfiguration

Här har du möjlighet att aktivera följande konfigurationer på din Windows 10-dator:

| | |
|---|---|
| Omedelbar DM-anslutning | |
| Initial omprövningstid | Upprättar det första anslutningsförsöket till enheten, detta värde ökar exponentiellt |
| Försök med anslutning | Anger hur många anslutningsförsök DM-klienten ska göra vid ett anslutningsfel |
| Maximal sömntid | Anger den maximala vilotiden efter ett anslutningsfel |
| Första synkroniseringsförsöket | Intervaller, med vilka enheten ska kommunicera med servern, efter den första anslutningen |
| Första omprövningsintervall | Relaterar till "Första synkroniseringsförsök"<br>Här anges tiderna i minuter<br>Under "First Sync Retries" anges t.ex. värdet "2" och under "First Retry Interval" anges värdet "4 Minutes", vilket innebär att enheten kommunicerar 2 gånger var 4:e minut efter den första anslutningen |
| Andra synkroniseringsförsök | Intervall då enheten ska kommunicera med servern efter att "Första synkroniseringsförsöken" har slutförts |
| Sekund Retry Interval | Samma princip som för "First Retry Interval" - här gäller det bara för "Second Sync Retries" |
| Regelbundna synkroniseringsförsök | Intervall, för hur ofta enheten ska kommunicera med servern i framtiden<br>Standard: "Oändlig"<br>Vi rekommenderar att du inte ändrar detta värde, för om du anger "10" kommer enheten att kommunicera med servern 10x och sedan sluta Kommunikationen med AppTec360-servern bryts därför! |
| Regelbundet omprövningsintervall | Samma princip som för "First/Second Retry Interval" - men här gäller inställningarna för framtiden |
| Regelbundet omprövningsintervall | Samma princip som för "First/Second Retry Interval" - men här gäller inställningarna för framtiden |

# Innehållsruta

## Konfiguration

Här kan du konfigurera ContentBox. Du kan placera filer för grupper i ContentBox som du kan komma åt med ContentBox-appen på enheten.

| | |
|---|---|
| Aktivera innehållsrutan | Aktivera ContentBox. Om du avaktiverar detta om du inte använder ContentBox kan du spara resurser på OnPremise-maskiner. |
| Använd extern installation av ContentBox | ContentBox kan också drivas med ditt eget Nextcloud. |
| URL | Fullständig URL för Nextcloud-enheten |
| Rotanvändare | Root-användare av Nextcloud-kontot |
| Lösenord för rot | Rotlösenord för Nextcloud-kontot |
| Standardbehörigheter för gruppmappar | Standardbehörighet för gruppmappar, kan ändras individuellt av gruppen (i Mobile Management) |
| Dela gruppmapp med undergrupper | Om den är aktiv kan varje undergrupp läsa alla huvudgruppens mappar, kan också konfigureras individuellt för varje grupp (Mobile Management) |
| Behörigheter för undergrupper | Behörigheter för undergrupper<br>kan konfigureras individuellt för varje grupp (Mobile Management) |
| Tillåt delning | Gör det möjligt för användaren att dela innehållet via länkar, kan konfigureras individuellt för varje grupp |
| Maximal storlek för filuppladdning i MB | Maximal storlek på en fil<br>Standard: 512 MB<br>Maximal konfiguration: 2048 |
| **WebDAV-autentiseringsuppgifter** | |
| WebDAV-URL | Du kan också öppna ContentBox med WebDAV.<br>Ta inte bort följande mappar under några omständigheter:<br>/apptecgroups /apptecgroups/AppTecGroup-X |
| Rotanvändare | Namn på rotanvändare |
| Lösenord | Lösenord för rotanvändare |

Synkroniseringen med ContentBox sker automatiskt. Du kan dock utföra en manuell synkronisering med "Synchronize ContentBox".

Här kan du dessutom aktivera/avaktivera ContentBox på varje enskild enhet.

Detta är endast relevant om du inte har licensierat ContentBox ytterligare, då har du fortfarande tillgång till 25 enheter som du kan testa ContentBox med - här kan du aktivera detta för respektive enheter.

# LDAP-konfiguration

## LDAP-översikt

Här kan du upprätta en anslutning till din Active Directory via LDAP för att massimportera användare och grupper. Synkroniseringen måste utföras manuellt. Du kan konfigurera flera LDAP-anslutningar till olika system eller med olika konfigurationer/filter.

| | |
|---|---|
| Serverns namn | Serverns visningsnamn |
| Typ | För närvarande stöds endast Active Directories som stöder LDAP |
| LDAP-domän | Den primära LDAP-domänen (t.ex. example.com) |
| LDAP-värd | Endast nödvändigt om LDAP-värden inte är nåbar under den angivna LDAP-domänen. |
| Port | Lämna tomt om du vill använda standardport (389 eller 636 för SSL) |
| Användarnamn | T.ex. CN=John,OU=Users,DC=EXAMPLE,DC=COM Obs: De flesta system kräver användarnamnet i detta format och accepterar inte "John" som användarnamn |
| Lösenord | |
| Bekräfta lösenord | |
| Anslutningssäkerhet | Obs: När SSL eller TLS används kommer certifikatet för Active Directory att kontrolleras. Om detta är självsignerat måste du lägga till rotcertifikatutfärdaren i förtroendelagringen för den lokala maskinen. Om du befinner dig i molnet måste Active Directory tillhandahålla ett betrott certifikat, annars fungerar anslutningen endast utan kryptering. |
| Automatisk synkronisering. | Aktiverar automatisk synkronisering av LDAP-katalogen med det tidsintervall som anges i de allmänna LDAP-inställningarna. |
| Bas DN | Om du inte vill synkronisera hela katalogen kan du ange en OU här, t.ex. OU=AndroidUsers,OU=Users,DC=EXAMPLE,DC=COM |
| Medlem i | Alla importerade användare kommer att läggas till i den valda gruppen |
| Endast aktiverade användare? | När det är aktiverat kommer attributet userAccountControl att beaktas, användare utan det attributet kommer inte att importeras. |
| LDAP-filter | Du kan använda LDAP Filter för att filtrera vilka användare som ska importeras |
| Regex-filter | Du kan använda Regex-filter för att filtrera vilka användare som ska importeras |

| | |
|---|---|
| Testanslutning | Testar anslutningen när konfigurationen sparas |
| Återställ katalogstruktur vid synkronisering? | Om sant kommer alla LDAP-poster att flyttas tillbaka till sin ursprungliga plats i LDAP-trädet. Rekommenderas att vara aktiverad. |
| Återimportera borttagna användare och grupper? | När funktionen är aktiverad återskapas användare och grupper som har tagits bort. Rekommenderas att vara aktiverad. |
| Synkronisera borttagningar? | När denna funktion är aktiverad raderas grupper och användare när de raderas på LDAP-servern. Även enheter för borttagna användare kommer att raderas. |

Under listan över dina LDAP-konfigurationer kan du definiera den period under vilken systemet ska synkroniseras automatiskt. För automatisk synkronisering används endast de LDAP-konfigurationer där alternativet enligt ovan är aktiverat.

# App-hantering

## In-house App DB

### Android

Här kan du ladda upp de Android-appar som ditt företag har utvecklat och distribuera dem senare i Mobile Management i enhets- eller gruppprofiler.

Tänk på att vi rekommenderar att du endast distribuerar appar på detta sätt som inte finns tillgängliga i Google Play Store.

Klicka på "+" för att ladda upp APK:en för en app som du vill ladda upp. Endast APK-formatet stöds för närvarande.

Uppladdningsgränsen på OnPremise Appliances kan ökas i steg 3 i Appliance Configuration. Om du vill öka uppladdningsgränsen på Cloud, vänligen kontakta supporten för mer information.

Var medveten om att APK: er vanligtvis är lite mindre än deras innehåll. Det är möjligt att en uppladdning misslyckas på grund av detta, eftersom APK packas upp i processen. Det är t.ex. möjligt att en APK på 95 MB misslyckas med en uppladdningsgräns på 100 MB. I det här fallet, öka uppladdningsgränsen som nämnts ovan.

Vi rekommenderar också att du först flyttar APK:en manuellt till en testenhet (t.ex. via USB) och försöker installera den manuellt med enhetens Files-app. Om detta inte fungerar av någon anledning kommer det också att misslyckas via MDM.

**Uppdatera mål**

Med funktionen "Update Target" kan du välja vilken version av en app som ska installeras eller till vilken version en app ska uppdateras om du har aktiverat "Keep up to date" för en app.

Om du inte har valt något uppdateringsmål kommer den högsta versionen att användas.

Tänk på att Android inte kan nedgradera appar. Tänk också på att "Versionskoden" avgör om en version är högre, lägre eller densamma eller inte. Så se till att korrekt öka denna version i din app när du bygger en uppdatering.

## iOS

Här kan du ladda upp de iOS-appar som du har utvecklat och distribuera dem senare i Mobile Management i din enhets- eller grupprofil.

Klicka på "+" för att ladda upp IPA för en app som du vill ladda upp. Endast IPA-formatet stöds för närvarande.

Uppladdningsgränsen på OnPremise Appliances kan ökas i steg 3 i Appliance Configuration. Om du vill öka uppladdningsgränsen på Cloud, vänligen kontakta supporten för mer information.

**Uppdatera mål**

Med funktionen "Update Target" kan du välja vilken version av en app som ska installeras eller till vilken version en app ska uppdateras om du har aktiverat "Keep up to date" för en app.

Om du inte har valt något uppdateringsmål kommer den högsta versionen att användas.

## MacOS

Här kan du ladda upp de MacOS-appar som du har utvecklat och distribuera dem senare i Mobile Management i din enhets- eller grupprofil.

Klicka på "+" för att ladda upp PKG för en app som du vill ladda upp. Endast PKG-formatet stöds från och med nu.

Uppladdningsgränsen på OnPremise Appliances kan ökas i steg 3 i Appliance Configuration. Om du vill öka uppladdningsgränsen på Cloud, vänligen kontakta supporten för mer information.

**Uppdatera mål**

Med funktionen "Update Target" kan du välja vilken version av en app som ska installeras eller till vilken version en app ska uppdateras om du har aktiverat "Keep up to date" för en app.

Om du inte har valt något uppdateringsmål kommer den högsta versionen att användas.

## Windows 10

Här kan du ladda upp Windows 10-appar och distribuera dem senare i Mobile Management i din enhets- eller grupprofil.

Klicka på "+" för att ladda upp APPX, APPXBUNDLE eller MSI för en app som du vill ladda upp. Endast APPX-, APPXBUNDLE- eller MSI-format stöds för närvarande.

Du kan också ladda upp och definiera Dependencies för en App, som automatiskt distribueras och installeras innan du installerar den önskade Appen.

Uppladdningsgränsen på OnPremise Appliances kan ökas i steg 3 i Appliance Configuration. Om du vill öka uppladdningsgränsen på Cloud, vänligen kontakta supporten för mer information.

**Uppdatera mål**

Med funktionen "Update Target" kan du välja vilken version av en app som ska installeras eller till vilken version en app ska uppdateras om du har aktiverat "Keep up to date" för en app.

Om du inte har valt något uppdateringsmål kommer den högsta versionen att användas.

**Win32-paket (.exe)**

Du kan också distribuera .exe-filer/installatörer till dina enheter.

| | |
|---|---|
| Paketets namn | Det namn som kommer att visas i MDM |
| Beskrivning | Beskrivning som visas i MDM |
| Paketfil | Endast .zip-filer är tillåtna. Placera de filer du vill distribuera i den här zip-filen. |
| Kontext för distribution | **Systemet**: Installationskommandot körs med systembehörighet, vilket är högre än "User". När du använder "System" har processen inte heller något användargränssnitt, så den blir tyst och användarprofilen, t.ex. miljövariabler som %AppDat%, är inte tillgänglig. **User**: Installationskommandot har tillgång till användarprofilen och kan visa användargränssnittet om det behövs. Obs: Vissa processer kanske bara fungerar i ett sammanhang. Om t.ex. en programvara installerar sig själv i AppData fungerar den bara när du väljer "User" |
| Installera kommandot | Det kommando som används för att installera programmet. Exempelvis skulle installationskommandot för en zip-fil som innehåller "setup.exe" i roten och som stöder parametern "/s" för en tyst installation vara "setup.exe /s". Tänk på att olika program kan ha olika parametrar. |
| Avinstallera kommandot | Kommandot som ska köras för att avinstallera programvaran via MDM. Vanligtvis pekar detta på avinstalleraren. Till exempel "C:\Program Files\ExampleSoftware\uninstall.exe". |
| **Krav och önskemål** | |
| Obs: Alla uppställda krav måste uppfyllas för att programvaran ska kunna installeras. Annars kommer den inte att installeras. Vissa fält kan vara obligatoriska. Om inget värde anges för ett krav kommer kravet att ignoreras. | |
| OS-arkitektur | OS-arkitektur |
| Min OS-version | Min OS-version |
| Minsta lediga diskutrymme (MB) | Minsta lediga diskutrymme (MB) |
| Minsta fysiska minne (MB) | Minsta fysiska minne (MB) |
| Minsta antal logiska processorer | Minsta antal logiska processorer |

| | |
|---|---|
| Min CPU-hastighet (MHz) | Min CPU-hastighet (MHz) |
| Ytterligare krav | Du kan också manuellt definiera regler eller ladda upp ett skript här för att utföra ytterligare kravkontroller om du vill. |
| **Regler för detektering** | |
| Metod för detektering | Här kan du definiera hur du ska upptäcka om appen är installerad på enheten. Installera-kommandon körs bara när dessa regler upptäcker att appen INTE är installerad. Avinstallationskommandon körs endast när dessa regler upptäcker att appen inte är installerad. **Definiera regler manuellt**: Här kan du manuellt definiera en eller flera regler för att t.ex. kontrollera om en viss fil, mapp, MSI eller registernyckel finns. Om alla angivna detekteringsregler är sanna kommer appen att anses finnas. **Använd skript**: Ladda upp ditt eget skript med dina egna kontroller. Om skriptet returnerar "$TRUE" kommer appen att anses vara närvarande. |
| Regler för detektering | |

## Inställningar för appen

### Inställningar för iOS-appen

Här kan du definiera standardinställningarna för att lägga till en app i de obligatoriska apparna eller i företagets appbutik.

Obs: Detta anger endast vad som väljs som standard när du lägger till appar. Detta ändrar INTE befintliga inställningar för appar som redan har lagts till i de obligatoriska apparna eller i företagets appbutik.

| | |
|---|---|
| Håll dig uppdaterad | Håller automatiskt appen uppdaterad. Tänk på att det kan ta upp till 7 dagar efter att en uppdatering har släppts innan appen uppdateras. |
| Kör om när den inte hanteras | Om en app redan är installerad som ohanterad (av användaren) kommer appen att tas över och hanteras av MDM. |
| Ta bort appen när MDM-profilen tas bort | Avinstallerar appen när MDM tas bort. |
| Förhindra säkerhetskopiering av appdata | Förhindrar säkerhetskopiering av appdata. |

## Inställningar för Android-app

Här kan du definiera standardinställningarna för att lägga till en app i de obligatoriska apparna eller i företagets appbutik.

Obs: Detta ställer endast in vad som väljs som standard när du lägger till. Detta ändrar INTE inställningarna för appar som redan har lagts till i de obligatoriska apparna eller i företagets appbutik.

| | |
|---|---|
| Håll dig uppdaterad | Håller automatiskt appen uppdaterad. Endast tillgänglig för InHouse Apps. |
| Kontrollerad AppTec360 EMM Uppdatering av klient | Om det är aktiverat kan administratörer ange uppdateringsmål för AppTec360 EMM Client. En lista över alla tillgängliga versioner av AppTec360 EMM Client kommer att visas i "Allmänna inställningar" → "App Management" → "In-House App DB" → "Android". |

# Appar från tredje part

## Android

Här kan du ställa in din aktiveringskod för Ikarus.

Ställ in detta på "Use Activation Code" och ange din aktiveringskod här.

Obs: När du har angett koden och sparat den läggs koden ännu inte till i den profil som skickas till enheten. Du måste göra någon ändring i din profil för att koden ska läggas till i profilen. Ändra t.ex. någon strömbrytare i profilen från av → på → av - Spara → Tilldela nu.

## iOS

Här kan du ange din SecurePIM-licens. När du har angett licensen trycker du på "Spara ändringar" och du kan använda SecurePIM-alternativen.

# VPP / KNOX Premium

Apples Volume Purchase Program (VPP) gör att du enkelt kan distribuera betalda och gratis appar till dina enheter. Detta rekommenderas starkt eftersom du inte behöver ett Apple-ID på enheterna, användarna behöver inte bekräfta installationen (övervakad), användarna behöver inte ange lösenordet för Apple-ID och du kan enkelt distribuera betalda appar utan att köpa dem på varje enhet igen.

För att använda VPP måste du registrera dig i Apple Business Manager.

## VPP-licenser

Här kan du få en överblick över dina VPP-appar, hur många licenser som används och hur många som är tillgängliga.

Genom att klicka på hjulet kan du se vilka enheter som har en licens tilldelad och vad statusen för denna tilldelning är.

Genom att klicka på uppdateras VPP-cachen som jämför de licenser som tilldelats i MDM med de licenser som tilldelats på Apples sida. Detta kan lösa licensproblem i vissa fall.

## VPP Token

Här kan du ladda upp din VPP Token, som du hittar i Apple Business Manager i Inställningar → Appar & Böcker. Du kan ladda upp flera VPP-tokens.

Du kan förnya en Token genom att helt enkelt ladda ner en ny i Apple Business Manager, klicka på "Edit"-hjulet och ladda upp den nya.

"VPP Mode" bestämmer hur licenstilldelningen ska hanteras. Beroende på ditt scenario måste du använda olika lägen:

"Device based" måste användas när enheterna registreras via QR-kod, länk, Apple Configurator eller DEP.

"User based" krävs om enheterna är registrerade med User Enrollment eller som Shared iPad.

Om du aktiverar "Automatiserad licenshantering" kommer användare som flyttas från en grupp till en annan automatiskt att tilldelas Apple VPP-licenser baserat på den grupprofil som de flyttas till.

Befintliga Apple VPP-licenser från den grupp som de har flyttat från kommer inte att återkallas.

Nya användare som läggs till i en grupp kommer automatiskt att tilldelas Apple VPP-licenser baserat på respektive grupprofil.

### KNOX Premium Nyckel

Här kan du ange din KNOX Premium Key för att använda Samsung KNOX Container.

Tänk på att detta inte längre stöds sedan Android 10. Använd Android Enterprise Container istället.

## Inställningar för App Store

### Region & språk

Här kan du ställa in standardspråk och region för App Search i App Management.

Tänk på att inställningen för iTunes också definierar hur systemet hämtar information om vissa appar. Om du stöter på appar i dina listor som visas på ett konstigt sätt (t.ex. saknar ikon) kan du ha ställt in en region där den specifika appen inte är tillgänglig.

## AE Play Butik

Här hittar du alla alternativ för Play Store för Android Enterprise Devices för att godkänna appar, ladda upp egna appar till Play Store eller skapa dina egna webbappar.

### Godkända appar

Här kan du få en översikt över alla appar som du har godkänt.

### Appar i Play Store

Detta kommer att ladda en iFrame som visar Play Store. Sök efter den app du vill ha, klicka på den och godkänn den. När du godkänner appen kan du också definiera att godkännandet återkallas om de behörigheter som krävs ändras. Vi rekommenderar att du lämnar dessa inställningar som standard när du godkänner appar.

När en app har godkänts kan du lägga till den i dina profiler.

Knappen "Approve" ändras till "Revoke approval" när du har godkänt den, så att du alltid kan ta bort apparna om du inte behöver dem längre.

### Privata appar

Här kan du ladda upp din egen app som en privat app till Google Play Store. Detta gör att du kan distribuera appen via Googles tjänster och uppdatera den via dem. Detta har också den fördelen att dina egna appar kan installeras utan att användaren behöver bekräfta installationen, vilket normalt är nödvändigt.

## Webbappar

Här kan du skapa Web Apps, som är länkar till vissa webbsidor som kan tilldelas som appar.

Du kan också ge den en egen ikon och ytterligare definiera hur den ska visas.

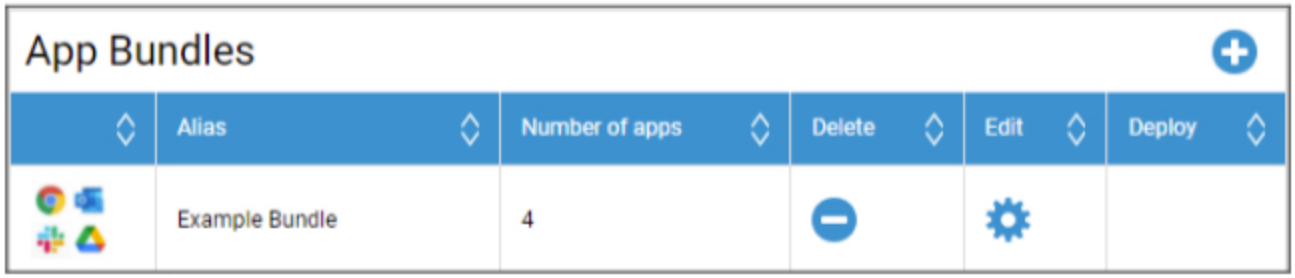
## Butikens layout

Butikslayouten definierar hur appar visas i Play Store eller om de visas överhuvudtaget.

Tänk på att om du vill visa appar i Play Store som användaren kan installera manuellt måste dessa läggas till här i layouten **OCH** i profilen till Enterprise Play Store. Om du bara lägger till en app i en av dem kommer den inte att visas.

# App-paket

Med App Bundles kan du definiera grupper av appar som kan tilldelas enhets- eller grupprofiler med ett enda klick.




Klicka på "+" för att skapa ett nytt App Bundle. När du har skapat ett App Bundle kan du klicka på "Edit" för att lägga till appar från olika källor i Bundle.

Ett paket kan läggas till i profiler på samma sätt som alla andra appar. När du lägger till appar kommer du att ha en extra flik med namnet "App Bundles" där du har dina Bundles.

Om du gör någon ändring i en App Bundle visas en knapp i kolumnen "Deploy". Detta gör att du kan skicka ändringarna till alla profiler som innehåller detta paket. Tänk på att du måste göra detta manuellt efter att du har lagt till eller tagit bort appar i ett paket.

# Fjärrkontroll

## TeamViewer

### TeamViewer-kontakt

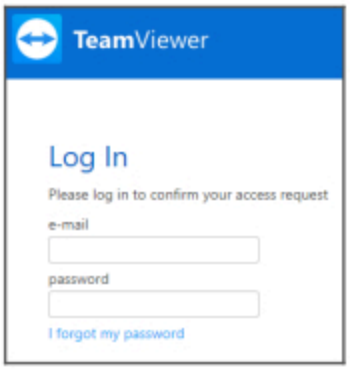
*Obs: I den kostnadsfria testversionen av vår molnversion kan du inte ansluta ditt TeamViewer-konto. Du kommer att få ett gratis demokonto länkat automatiskt istället.*

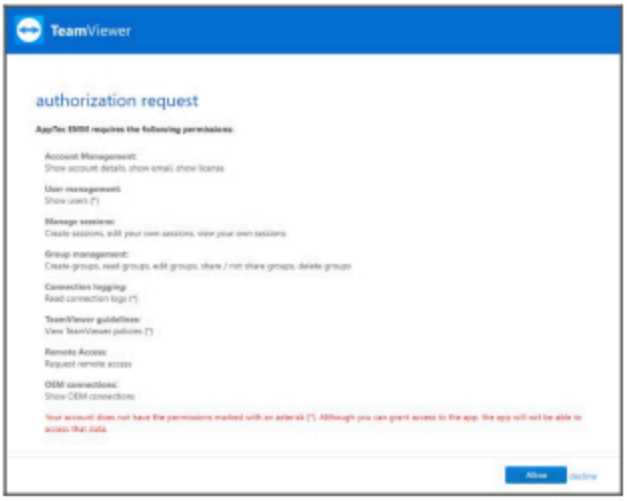
Gå till Allmänna inställningar -> Fjärrkontroll -> TeamViewer. Här kan du länka ditt TeamViewer-konto till konsolen eller se information om ditt för närvarande anslutna konto. Du kan också visa alla aktiva sessioner om du går till "Aktiva sessioner".

För att koppla ditt konto klickar du på "Starta installation".

Om du gör det kommer du till en ny sida där du måste logga in med ditt TeamViewer-konto.

När du loggar in måste du godkänna att AppTec360 MDM använder detta konto. Efter att ha bekräftat detta måste du vänta några sekunder och kontot är anslutet.


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


TeamViewer
authorization request

## Installera TeamViewer QuickSupport

Lägg till appen "TeamViewer QuickSupport" bland de obligatoriska apparna i din enhetsprofil eller grupprofil och klicka på "Tilldela nu". Vänta tills appen är installerad på enheten.

Om du försöker komma åt en enhet där appen inte är installerad kommer den att installeras eller så kommer du att bli ombedd att installera den, beroende på enhetens konfiguration.

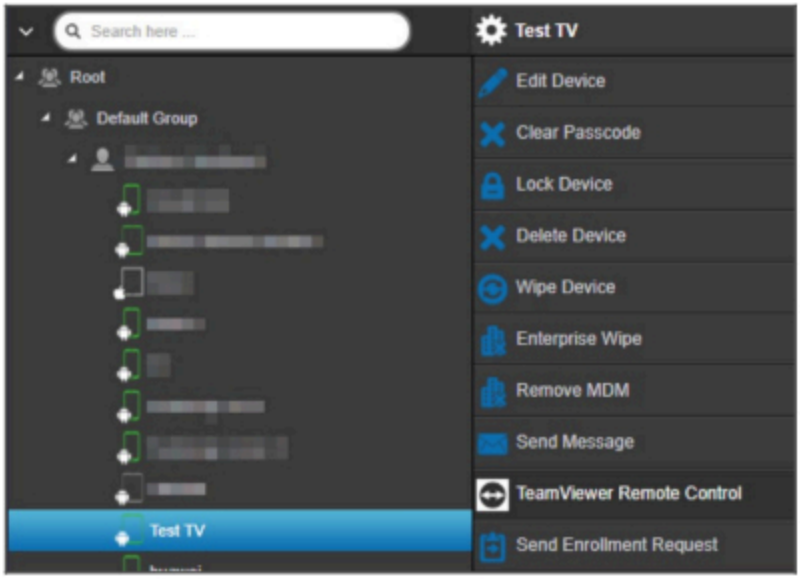
## Fjärrkontroll av din enhet

För att fjärrstyra din enhet väljer du enheten, klickar på hjulet och väljer "TeamViewer Remote Control"

Om det redan finns en aktiv session kan du antingen använda den gamla sessionen eller skapa en ny.

Bekräfta att du vill skapa en ny TeamViewer-session.

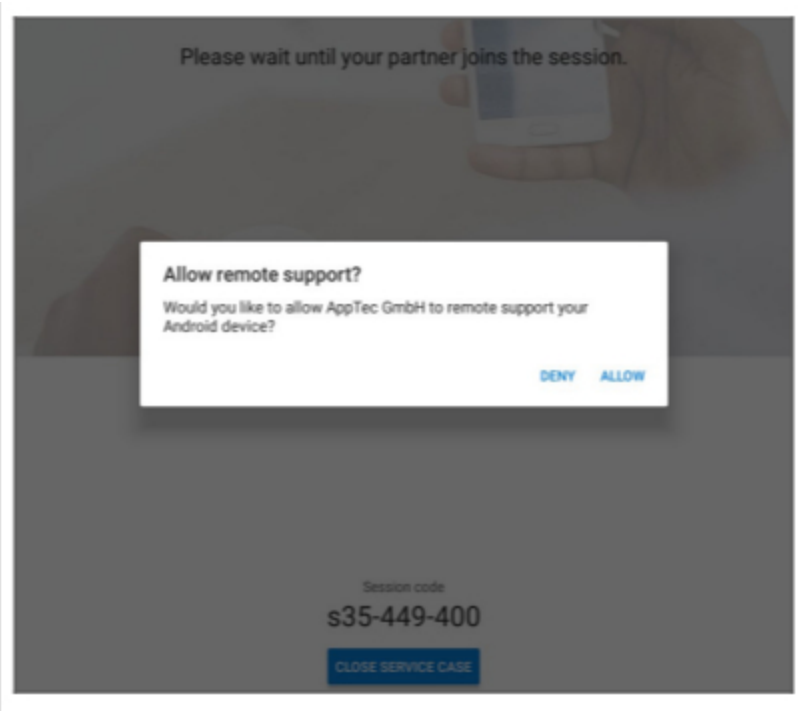
Efter några sekunder kommer du att få en länk till din TeamViewer-session. Du kan klicka på "Start" för att öppna länken i ett nytt fönster.


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

Den här länken öppnar din installerade TeamViewer och ansluter dig till din enhet.

Nu måste du bekräfta anslutningen på själva enheten för att kunna fjärrstyra den.

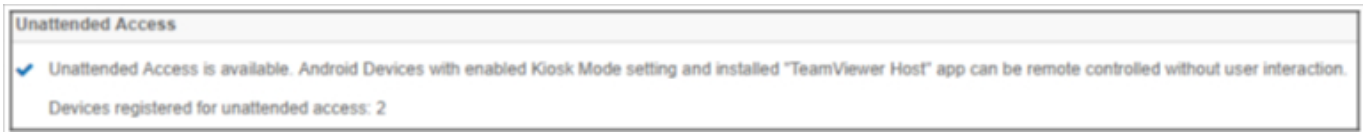



Om du använder iOS kommer du att få ett meddelande i AppTec360 MDM Client. Med den länken kommer enheten att ansluta sig till fjärrsessionen. Beroende på enhetens meddelandeinställningar är det möjligt att du inte får något meddelande och måste öppna AppTec360 MDM Client manuellt.

På vissa Android-enheter (t.ex. Samsung) måste du installera ytterligare en app som tillägg. TeamViewer-appen på enheten kommer att informera dig om detta, om det är nödvändigt på din enhet.

## Obevakad åtkomst

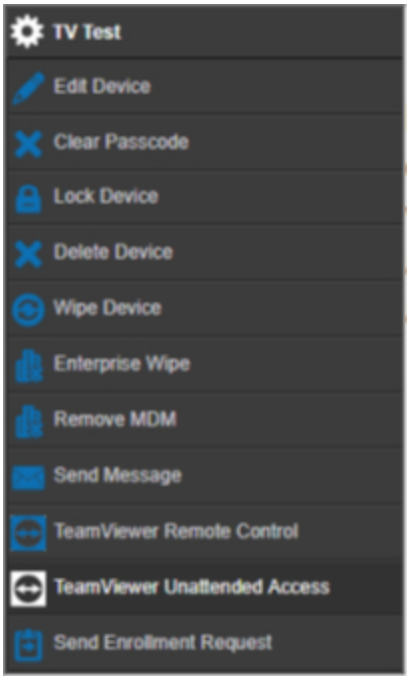
Obs: Obevakad åtkomst är endast möjlig på Android-enheter.




Du kan bara ansluta till dina enheter, utan att acceptera anslutningen på enheten, om ditt TeamViewer-konto använder en "Tensor"- eller "Corporate"-licens.

Du kan kontrollera detta efter att du har länkat ditt konto i "Allmänna inställningar"


För att använda obevakad åtkomst måste du installera appen "TeamViewer Host" och aktivera "Enable Unattended Access" under "Kiosk Mode & Launcher" i din profil. Tänk på att detta endast är möjligt om du använder kioskläget.




Nu kan du välja obevakad åtkomst om du väljer din enhet och klickar på hjulet. Detta kommer att ansluta dig till din enhet utan att du behöver bekräfta det på själva enheten. Tänk på att det kan ta några ögonblick innan du får länken för att komma åt din enhet.

## Splashtop

Om du aktiverar alternativet Splashtop ser du konfigurationsalternativen för Splashtop i dina profiler.

För att använda Splashtop måste du ställa in Splashtop Streamer (com.splashtop.streamer.csrs) som obligatorisk app i din profil. Därefter kan du aktivera Splashtop-konfigurationen i din profil under "Fjärrkontroll". Om du aktiverar detta kommer Splashtop Streamer-appen att konfigureras. Om du använder Splashtop Streamer men inte i kombination med MDM, bör du inte aktivera detta.

I din profil under "Fjärrkontroll" måste du också ange en deploy-kod. Gå till https://my.splashtop.com och logga in på ditt Splashtop-konto. Klicka på "Add Computer" och kopiera den 12-siffriga deploy-koden från den resulterande sidan.

Utan Deploy-koden är fjärrstyrning INTE möjlig.

När du har gjort det kan du högerklicka på din enhet och starta en fjärrsession genom att klicka på "Splashtop Remote Control"

# Sim-kortshantering

## CSV Bulk Import

Här visas en översikt över dina tilldelade SIM-kort och all information om dem. Detta hjälper dig att ha all information, inte bara om dina enheter utan även om dina SIM-kort i ett och samma system.

**OBS!** Detta är en manuell hantering/dokumentation. Det är inte möjligt att få dessa data automatiskt från enheterna på grund av operativsystemens sekretess-/säkerhetsmekanismer.

Du kan också exportera och importera listan som CSV.

## Transportör & tariff

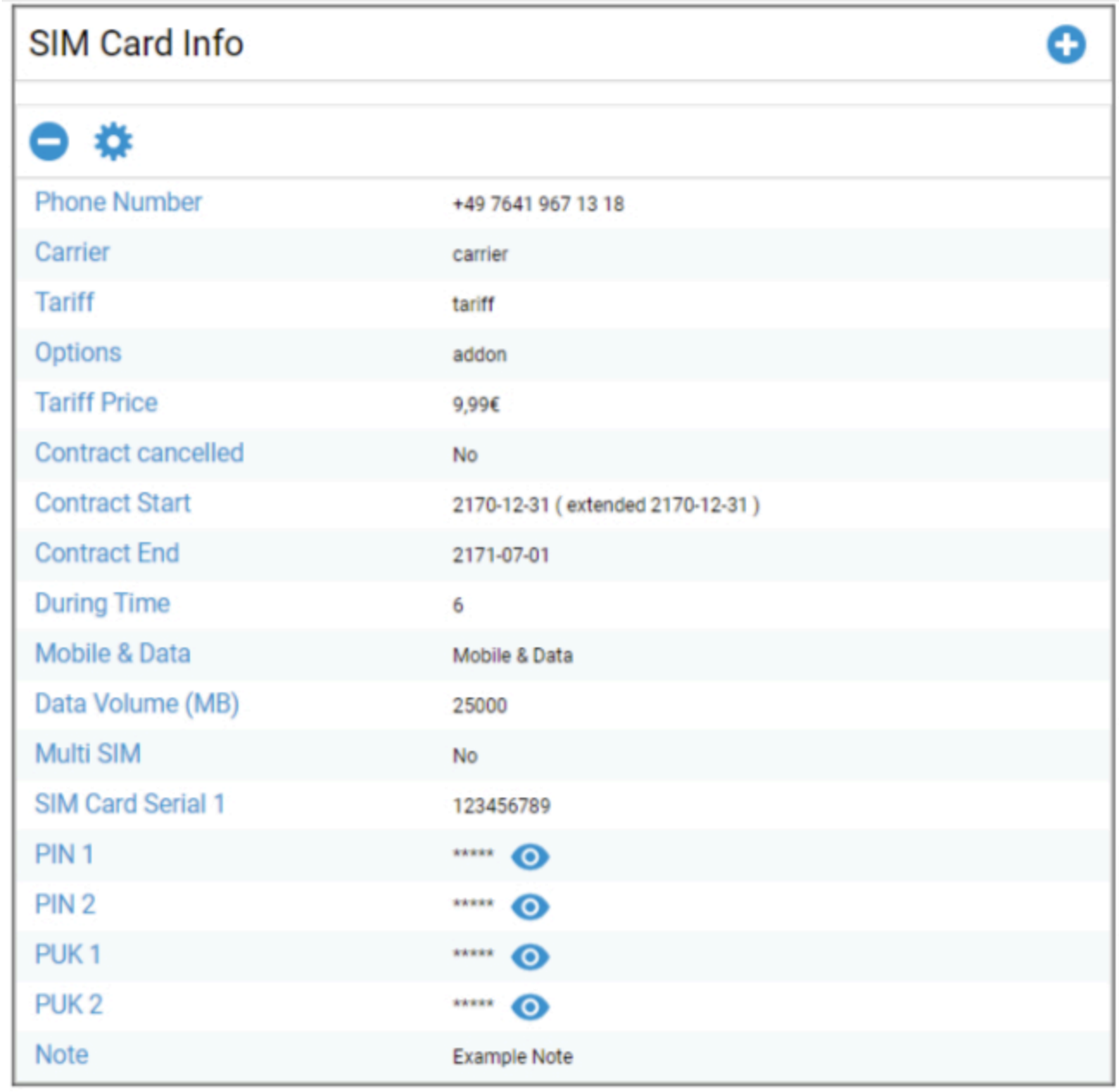

För att lägga till ett sim-kort klickar du först på knappen för att lägga till en eller flera operatörer.

Klicka sedan på "+" i "Tariff Information" för att lägga till en tariff för en transportör.

Eventuellt kan du lägga till valfria tillägg nedan om du har något liknande.

Detta förbereder allt du behöver för att lägga till ett faktiskt Sim-kort. Sim-kort är för närvarande tilldelade en användare. Gå därför till Mobile Management, välj en användare och gå till "Sim Card Overview".

Här ser du simkorten för den här användaren. Om det finns ett kan du redigera eller ta bort det. Användare kan ha flera sim-kort.

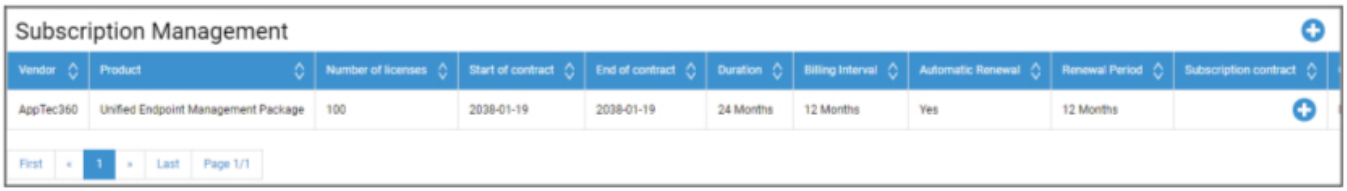



Klicka på "+" för att lägga till ett SIM-kort och lägg till all information du behöver. Dessa simkort kommer också att visas i listan över alla dina simkort i Allmänna inställningar → Simkortshantering.

# Hantering av prenumerationer

## Hantering av prenumerationer

Här kan du dokumentera löpande abonnemang, deras detaljer och även lagra olika filer, t.ex. undertecknat avtal, uppsägningsbrev etc. Du kan även ställa in påminnelser som påminner dig per mail innan abonnemanget avslutas och kanske förlängs automatiskt.



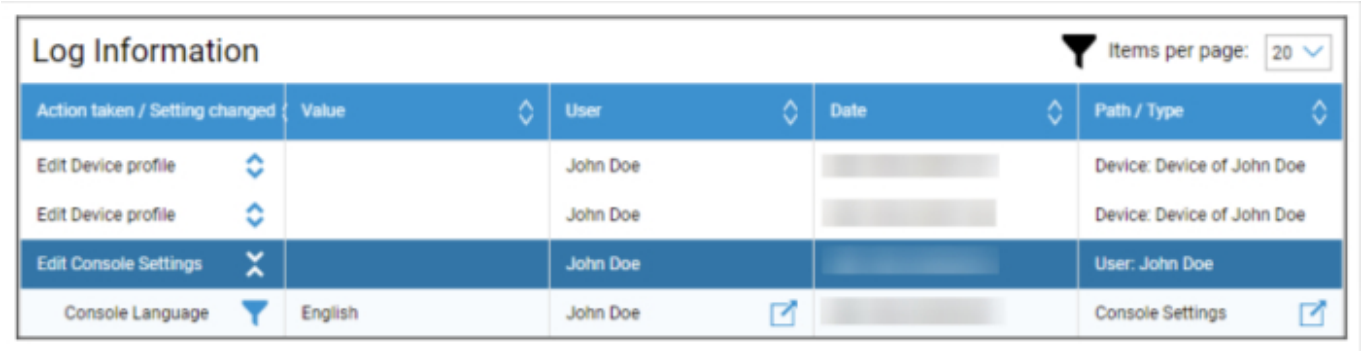

Klicka på "+" längst upp för att lägga till en prenumeration. Du kan lägga till hur många prenumerationer du vill.

Klicka på "+" i de olika fälten för att ladda upp filer som rör denna prenumeration. Du kan tekniskt sett ladda upp alla filtyper, men tänk på att inte alla filtyper kan förhandsgranskas i webbläsaren.

# Allmän revisionslogg

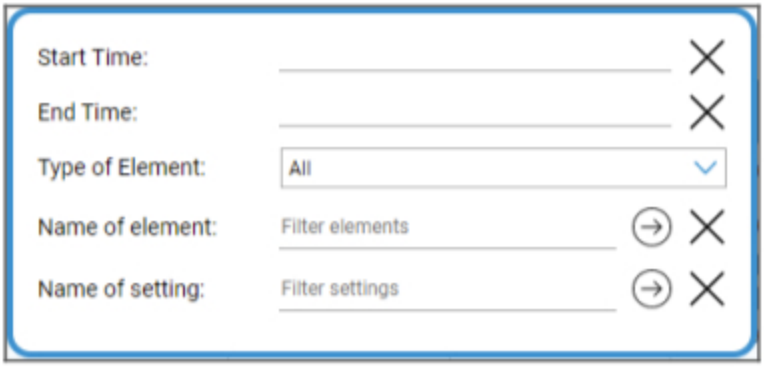
## Revisionslogg

Här har du en allmän granskningslogg som visar alla ändringar som gjorts. Medan granskningsloggen för en användare eller grupp endast visar ändringar som gäller den användaren eller gruppen, visar den här alla ändringar som gjorts var som helst i konsolen.




Du kan se vad som har ändrats, av vem, när och var. I vissa fall kan du också utöka posten för att se ytterligare detaljer.

Det är möjligt att klicka på användaren eller på posten i "Path / Type" för att komma till den plats där ändringen har gjorts.




Längst upp till höger kan du också definiera ett filter som kan hjälpa dig att hitta vissa förändringar i en miljö där många förändringar sker.

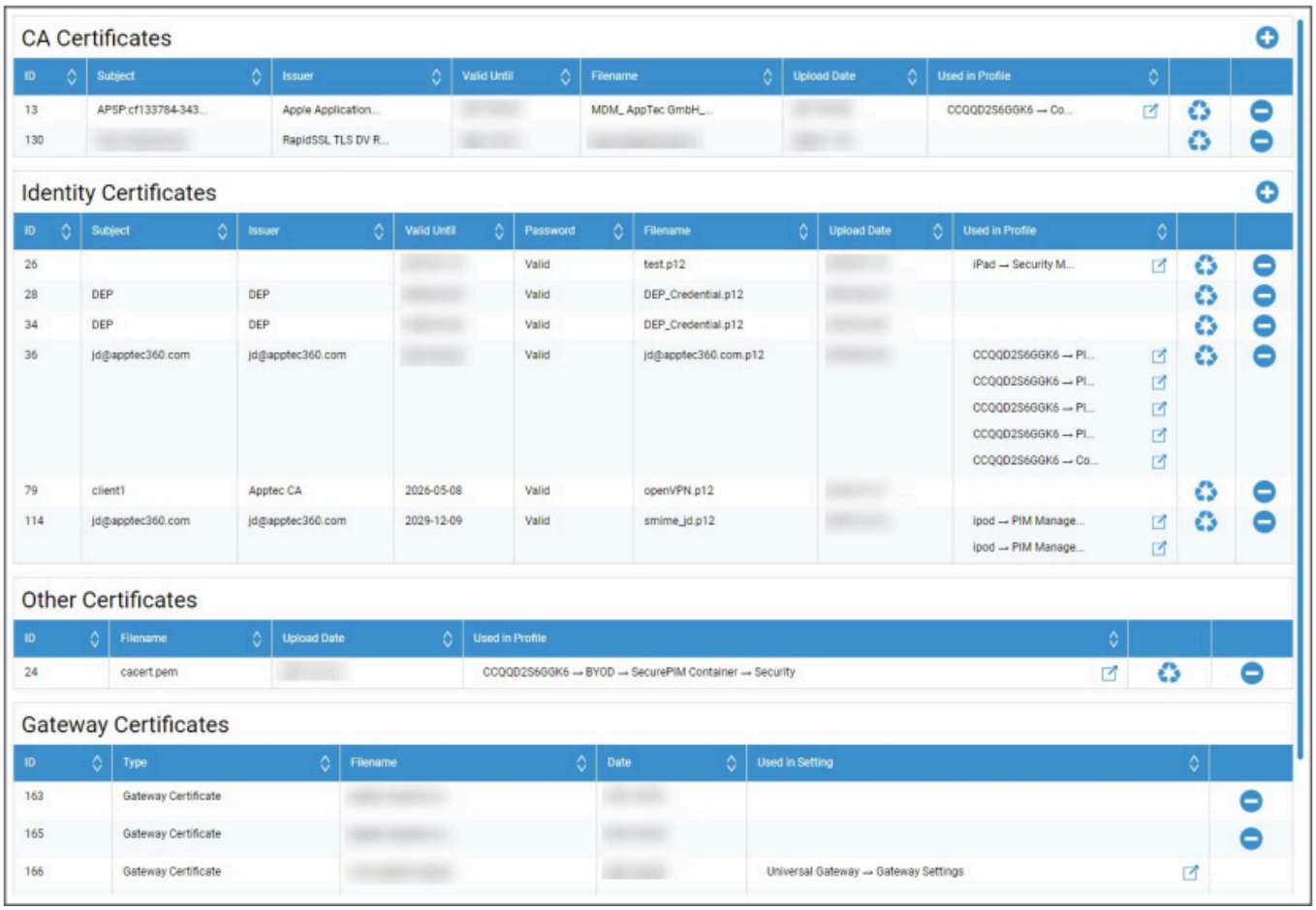
## Inställningar för granskningslogg

"Audit Log Retention Period" anger hur länge revisionsloggarna ska sparas innan de raderas.

# Certifikathantering

Här får du en översikt över alla certifikat som laddats upp och används i konsolen. Detta är endast en översikt. Den faktiska konfigurationen för t.ex. Wi-Fi-certifikat görs fortfarande i profilen på motsvarande plats.

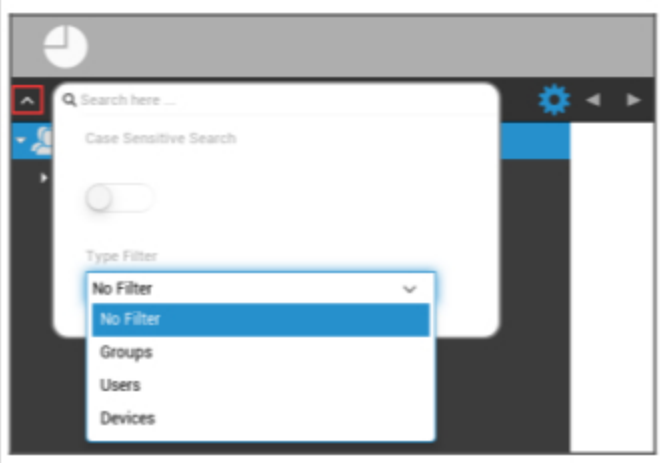
Här kan du också ta bort eller uppdatera certifikat, vilket automatiskt kommer att återspeglas i de berörda profilerna. Klicka på informationen i "Används i profil" för att se exakt var ett certifikat fortfarande är tilldelat.



# Mobil hantering

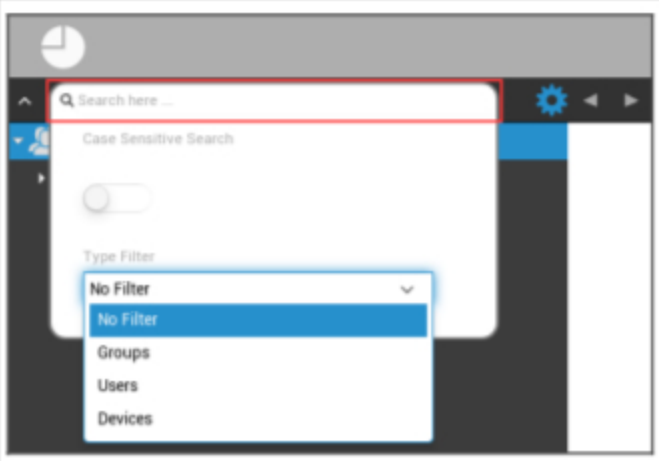
## Skärm för mobil hantering

### Filter för enheter




Med ett klick i det övre vänstra hörnet av skärmen kan du hitta en mängd olika filter för visning av enheter.

### Sökfönster




I sökfönstret kan du söka efter alla enheter och/eller användare med ett visst sökord.

### Alternativ växel

Efter att ha klickat på respektive symbol visas en lista över de alternativ som är tillgängliga för dig.

Dessa ändras för varje aktuellt fönster och förklaras i respektive kapitel.

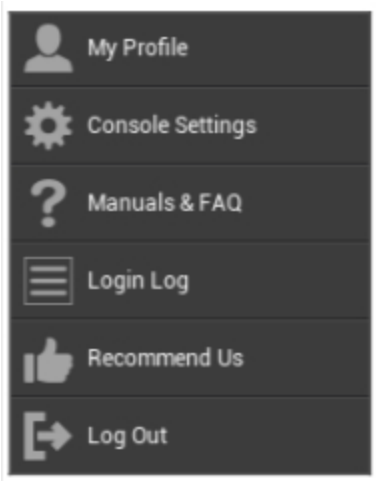
## Navigeringspilar

Genom att klicka på vänsterpilen kommer du till föregående sida.

När du sedan klickar på högerpilen kommer du tillbaka till den sida som du just lämnade.

# Administration kontoinställningar


Om du klickar på e-postadressen enligt bilden ovan visas följande meny:




| | |
|---|---|
| Min profil | Redigera kontouppgifterna för administratörer |
| Inställningar för konsol | Konfigurera konsolinställningar för kontot Admins |
| Manualer och vanliga frågor | Visa sidan "Manualer och vanliga frågor" i "Allmänna inställningar" |
| Logga in Logga in | Öppna "Inloggningslogg" |
| Rekommendera oss | Visa sidan "Rekommendera oss" i "Allmänna inställningar" |
| Logga ut | Logga ut från MDM-konsolen |

## Användarinformation

Här kan du redigera kontouppgifterna för den admin som är inloggad för tillfället.

| | |
|---|---|
| Användarnamn | Användarnamn och/eller e-postadress för kontot |
| Namn | Administratörens förnamn |
| Efternamn | Administratörens efternamn |
| Inloggningsnamn | Inloggningsnamn för administratörer |
| E-postadress | Administratörernas e-postadress |
| Alternativ eMail-adress | Administratörens alternativa e-postadress |
| Bild | Profilbild |
| Telefonnummer | Administratörens telefonnummer |
| Mobilnummer | Administratörens mobilnummer |
| Telefon anknytning | Telefontillägg |
| Plats | Plats |
| Position | Position i företaget |
| Användargrupp | Välj vilken användargrupp du vill tilldela administratörskontot till |
| Kommentar | Skriv en kommentar |
| Ange nytt lösenord | Ange lösenordet för en ändring av lösenordet |
| Upprepa nytt lösenord | Upprepa det nya lösenordet för att bekräfta |

*Observera att administrationsåtkomsten också kan arkiveras som ett lokalt användarkonto i hierarkistrukturen. Om inte ytterligare en administratör har inrättats bör denna inte tas bort!*

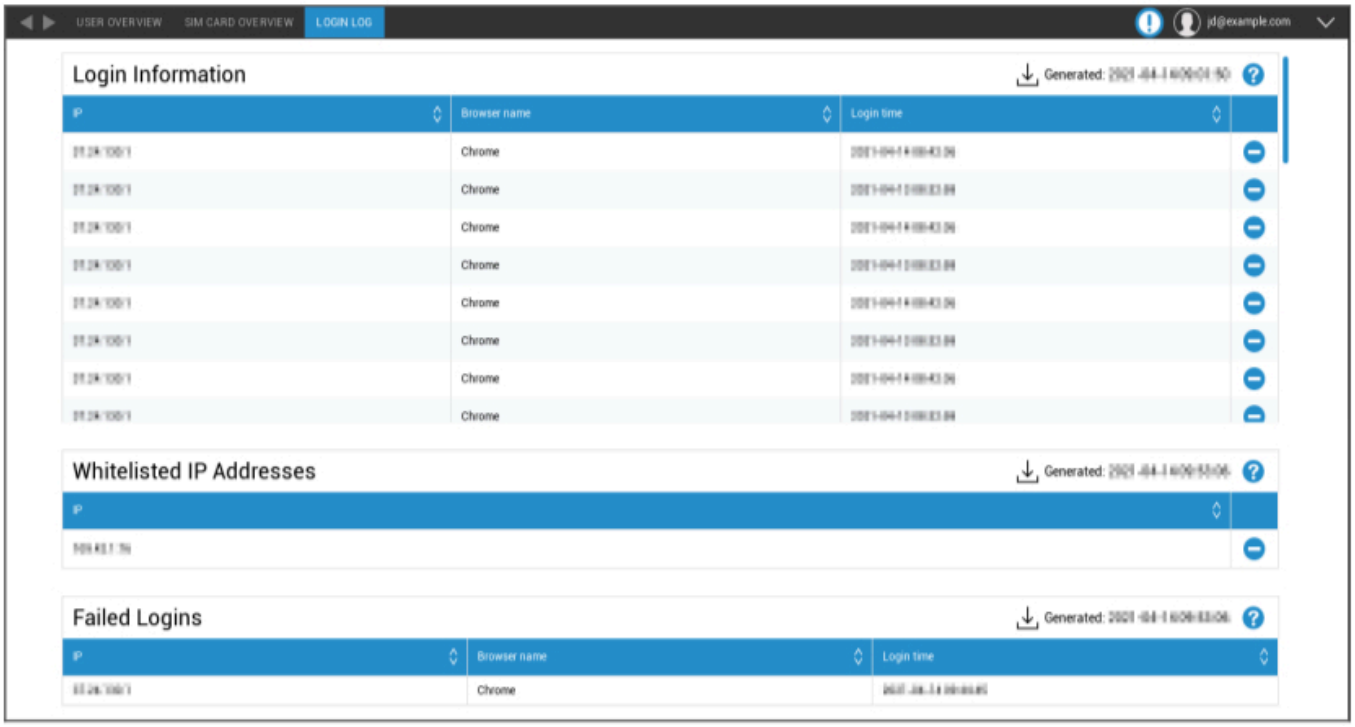
## Inställningar för konsol

Här kan du konfigurera följande konsolinställningar för kontot Admins:

| | |
|---|---|
| Alternativ för visning av kataloganvändare | Definiera hur användare ska märkas i trädet |
| Alternativ för visning av katalogenhet | Definiera hur enheter ska märkas i trädet |
| Timeout för session | Om användaren inte gör något inom den angivna tiden kommer användaren att loggas ut. Standardvärdet är 60 minuter. Logga ut och logga in igen när du har ändrat den här inställningen. |
| Tidszon | Välj den tidszon som ska användas |
| Tidsformat | Välj hur tidsstämplar ska visas |
| Konsolens språk | Välj det språk som konsolen ska visas på. Engelska och tyska är tillgängliga. |
| Huvudfärg | Du kan ange en färg som kommer att användas som bas för konsolens färgschema.<br>Du kan antingen använda färgväljaren eller ange en färg i HTML HEX-notation.<br>RGB-formatorer som "rosa", "gul" fungerar också. |
| Spara kommando | Nyckelkombinationen för att utlösa en sparning utan att trycka på "Spara"-knappen. |
| Använd tvåfaktorsautentisering | Aktivera användning av tvåfaktorsautentisering vid inloggning.<br>Du kommer att få ett e-postmeddelande vid inloggning med en kod som du måste ange för att logga in. |
| Timeout för tvåfaktorsautentisering | Ställ in en tidsperiod under vilken du inte kommer att bli ombedd att använda tvåfaktorsautentisering efter en redan lyckad autentisering. |
| Skicka verifieringskod via | Verifieringskoden kommer att skickas till de alternativ som valts.<br>Enhetsmeddelandet kommer att visas i AppTec360 MDM App på alla Android- och iOS-enheter som tillhör dig. |
| Skicka inloggningsmeddelande efter inloggning | Om den är aktiverad skickas ett e-postmeddelande för varje inloggning från en IP-adress som inte är vitlistad.<br>E-postmeddelandet innehåller information om inloggningen (t.ex. IP, webbläsare). |

## Logga in Logga in

Här kan du se information om inloggningarna för det adminkonto som för närvarande är inloggat.




| | |
|---|---|
| Inloggningsinformation | En lista som innehåller inloggningarna för det adminkonto som är inloggat för närvarande och som registrerades av konsolen.<br>Den här listan visar alla dina lyckade inloggningar under de senaste 30 dagarna. |
| Vitlistade IP-adresser | Detta är listan över alla dina vitlistade IP-adresser.<br>Om du loggar in från en IP som är listad här kommer du inte att få inloggningsmeddelandet.<br>Du kan lägga till en IP-adress i den här listan genom att klicka på knappen bredvid en post i listan "Inloggningsinformation" ovan.<br>Du kan ta bort en IP-adress från den här listan genom att klicka på knappen bredvid en post i den här listan eller i listan "Inloggningsinformation" ovan. |
| Misslyckade inloggningar | Detta är en lista över alla misslyckade inloggningsförsök under de senaste 30 dagarna.<br>Om du misslyckas med att ange rätt lösenord minst 3 gånger under 20 minuter visas en post i denna lista.<br>Du kommer också att informeras om misslyckade inloggningsförsök via e-post. |

# Företagsadministration (Root-Node) i Mobile Management


När du har nått Root-Node (första gruppen) kan du göra en rad olika inställningar för ditt företag när det gäller Mobile Management.

| | |
|---|---|
| Skapa en undergrupp | Skapa en undergrupp |
| Byt namn på rotnoden | Byte av namn på Root-Node (t.ex. ditt företagsnamn) |
| Massinskrivning | Registrera flera enheter/användare samtidigt |
| Uppgift om massa | Tilldela en profil för respektive grupp, med en enda blick |
| Snabb administration av appar | Skicka (Un-)Installationsbegäran för en applikation till respektive grupps enheter |
| CSV-import av användare | Importera användare från CSV till respektive grupp |

## Skapa en undergrupp

Med "Create a Subgroup" kan du skapa ytterligare en undergrupp.

Du kan ange under vilken grupp undergruppen ska placeras.


(Som standard skapas en ny grupp som tilldelas som en undergrupp i rotnoden)

## Byt namn på rotnoden


Här kan du byta namn på ditt rotnamn. Det är vanligt att företagsnamnet används i detta fall.

## Massinskrivning

Med "Mass Enrollment" kan du registrera flera enheter och användare.


Du kan välja direkt på vilket sätt användaren ska ta emot registreringen (eMail; alternativ eMail; SMS)

Beroende på vilken enhet användaren kommer att få (iOS, Android, Windows Phone) kan du markera det direkt här.

Skillnaden mellan om det är en smartphone eller en surfplatta kan också konfigureras här, vilket du måste välja korrekt, med en bockmarkering.

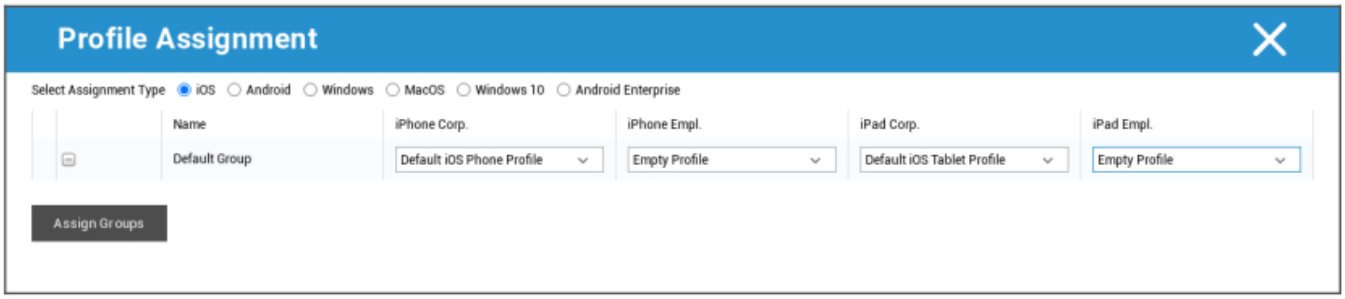
Som ett sista steg kan du fastställa om den aktuella enheten är företagsrelaterad eller privat (BYOD).

Med "Export as CSV" kan du exportera informationen som en CSV-datafil. I gengäld kan du också importera CSV-datafilen med "Import CSV", filen ska se ut som exemplet nedan:

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

## Uppgift om massa

Under Mass Assignment kan du tilldela en profil till alla grupper, denna är uppdelad i iOS - Android - Windows - MacOS - Windows 10 - Android Enterprise

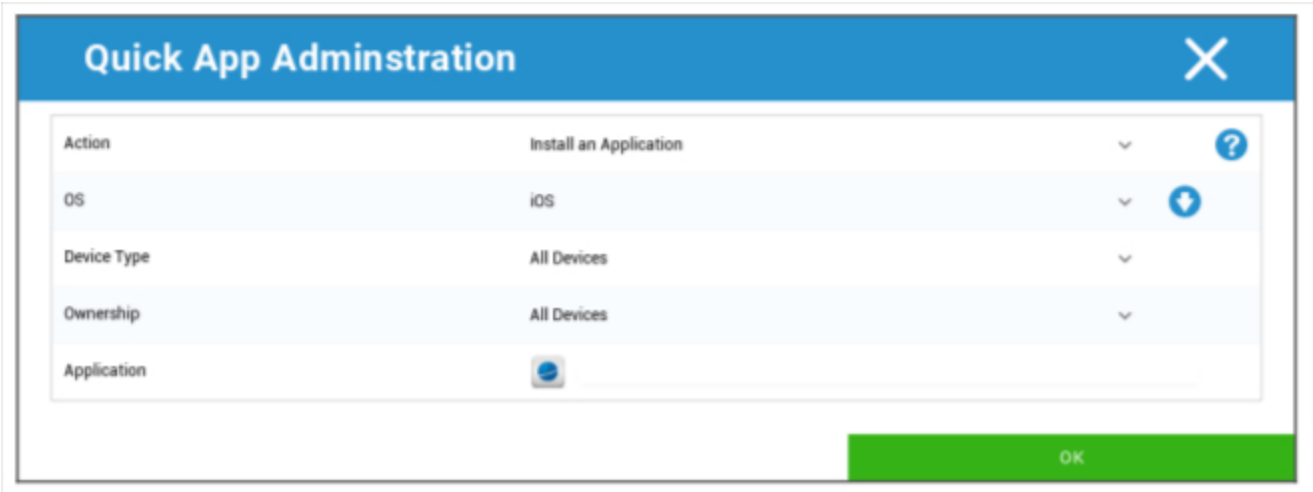



Windows - MacOS - Windows 10 - Android Enterprise

## Snabb administration av appar

Under Quick App Administration kan du skicka installations- eller avinstallationsförfrågningar för en viss applikation till ett valfritt operativsystem.

Du kan också ange om begäran ska skickas till alla enhetstyper i det valda operativsystemet eller bara till en viss enhetstyp.



## CSV-import av användare

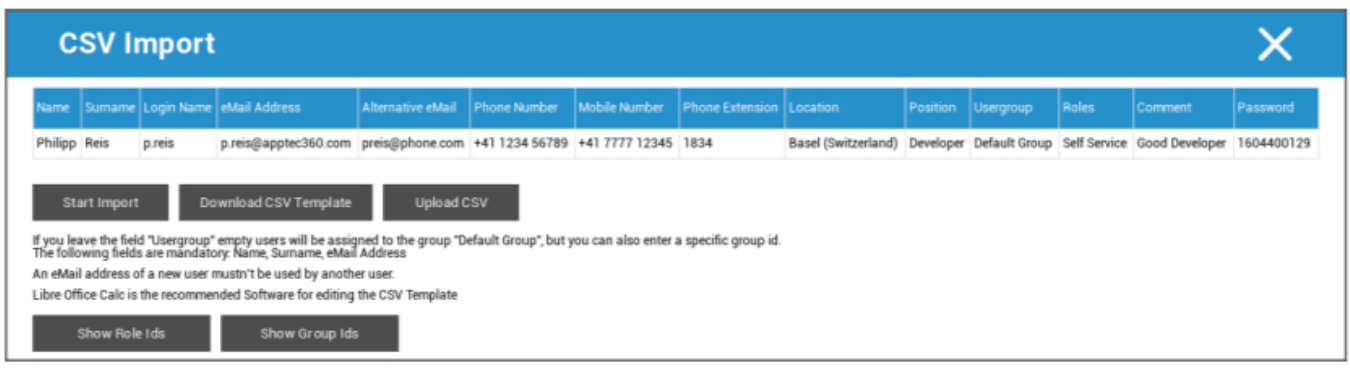
Importera användare från CSV till respektive grupp.

Med "Download CSV Template" kan du exportera en CSV-mallfil som du kan fylla i (eller använda som referens).

Du kan också använda alternativen "Show Role Ids" och "Show Group Ids" som referens för att skapa din egen CSV-fil.

CSV-filen kan laddas upp till MDM med "Upload CSV".

Som ett sista steg kan du starta importen genom att klicka på "Starta import".



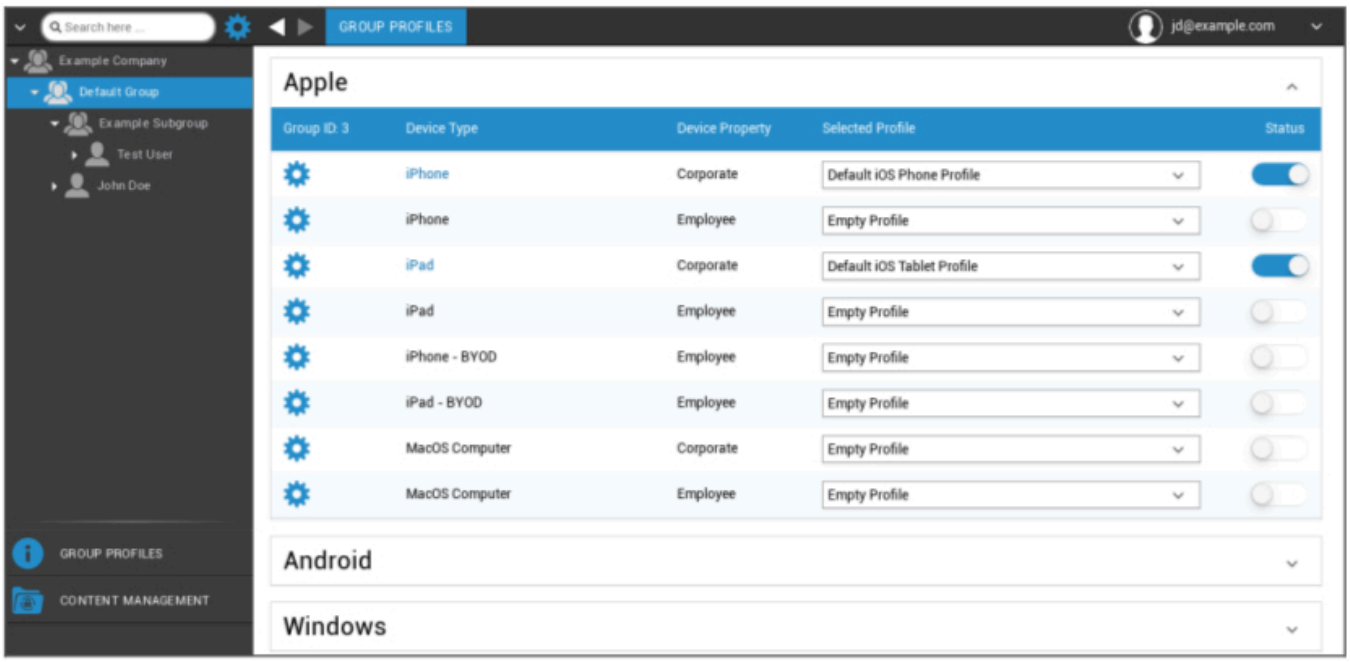
# Grupphantering i Mobile Management

Med ett klick på översikten visas de olika konfigurationsprofilerna för respektive plattform.

En profil innehåller alla inställningsmöjligheter som kan fastställas med AppTec360 i förväg på slutanvändarens enhet. På varje plattform kan du skapa profiler för företagsenheter (Corporate) eller Bring-Your-Own-Device-enheter (Employee).

För att kunna differentiera konfigurationer för enhetsgrupper, t.ex. baserat på plats eller funktion, rekommenderas att flera undergrupper skapas.

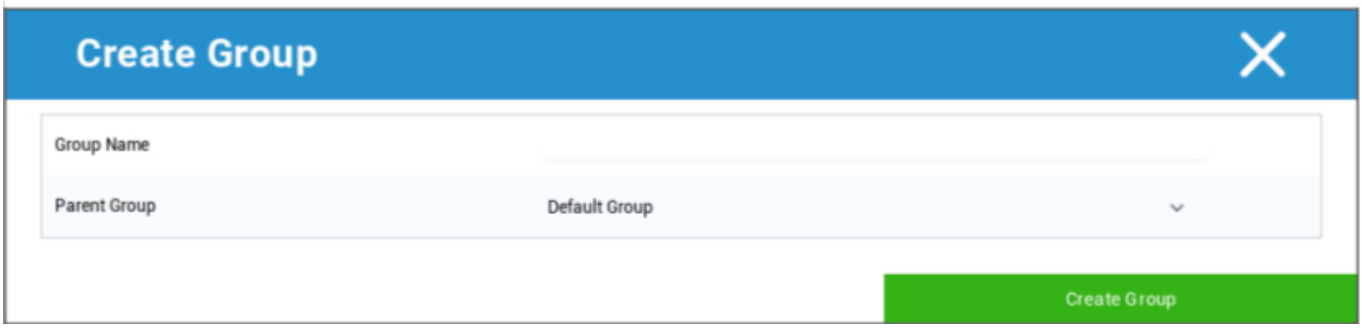
Observera profilhanteringen i Mobile Management




Med växelmenyn kan du göra en mängd olika inställningar för respektive (under)grupp.

| | |
|---|---|
| Skapa en undergrupp | Skapa undergrupp för respektive (under)grupp |
| Redigera vald grupp | Redigera vald grupp |
| Ta bort vald grupp | Ta bort vald grupp |
| Massinskrivning | Registrera många enheter/användare på en gång för den valda profilen |
| Uppgift om massa | Tilldela profiler till den grupp som för närvarande är vald |
| Skapa en undergrupp | Skapa undergrupp för respektive (under)grupp |
| Skapa en användare | Skapa en användare för respektive (under)grupp |

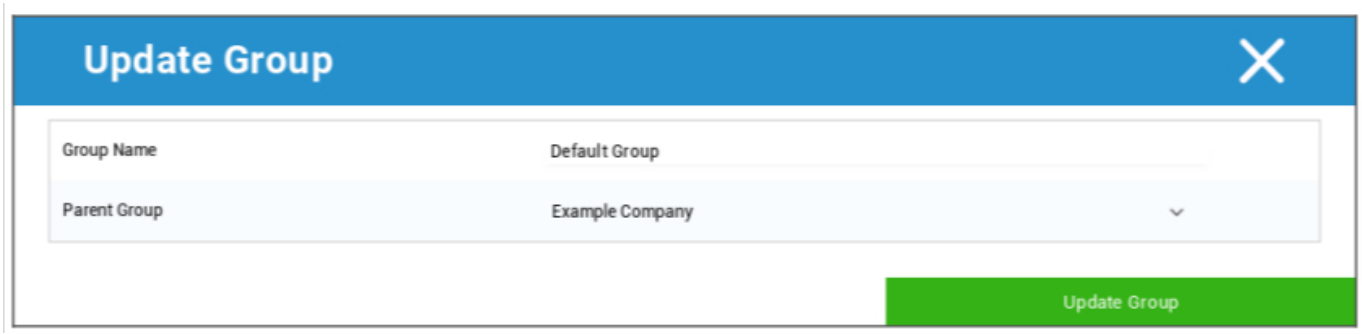
## Skapa en undergrupp




Med "Create a Subgroup" kan du skapa ytterligare en undergrupp.

Du kan ange vilken grupp undergruppen ska tilldelas (som standard tilldelas undergruppen den grupp som för närvarande är vald).

## Redigera vald grupp




Här kan du redigera profilen - här är följande inställningar möjliga:

- Gruppnamnet kan ändras
- Föräldragruppen kan ändras

## Ta bort vald grupp

Under "Ta bort vald grupp" listas alla användare och enheter som ingår i respektive grupp. Här har du möjlighet att ta bort dem.

För en användare kan du utföra följande raderingskommandon:

| | |
|---|---|
| Ta bort användare | Användaren är borttagen |
| Flytta användare till grupp: | Du kan flytta användaren till en annan grupp (följande kolumn, t.ex. "Admins") |

För en enhet kan du utföra följande raderingskommandon:

| | |
|---|---|
| Torka och ta bort | Torka och radera enheten |
| Ta bort från systemet | Ta bort endast enhet från AppTec |

Referens: Massinskrivning

Referens: Uppgift om massa

## Skapa en användare

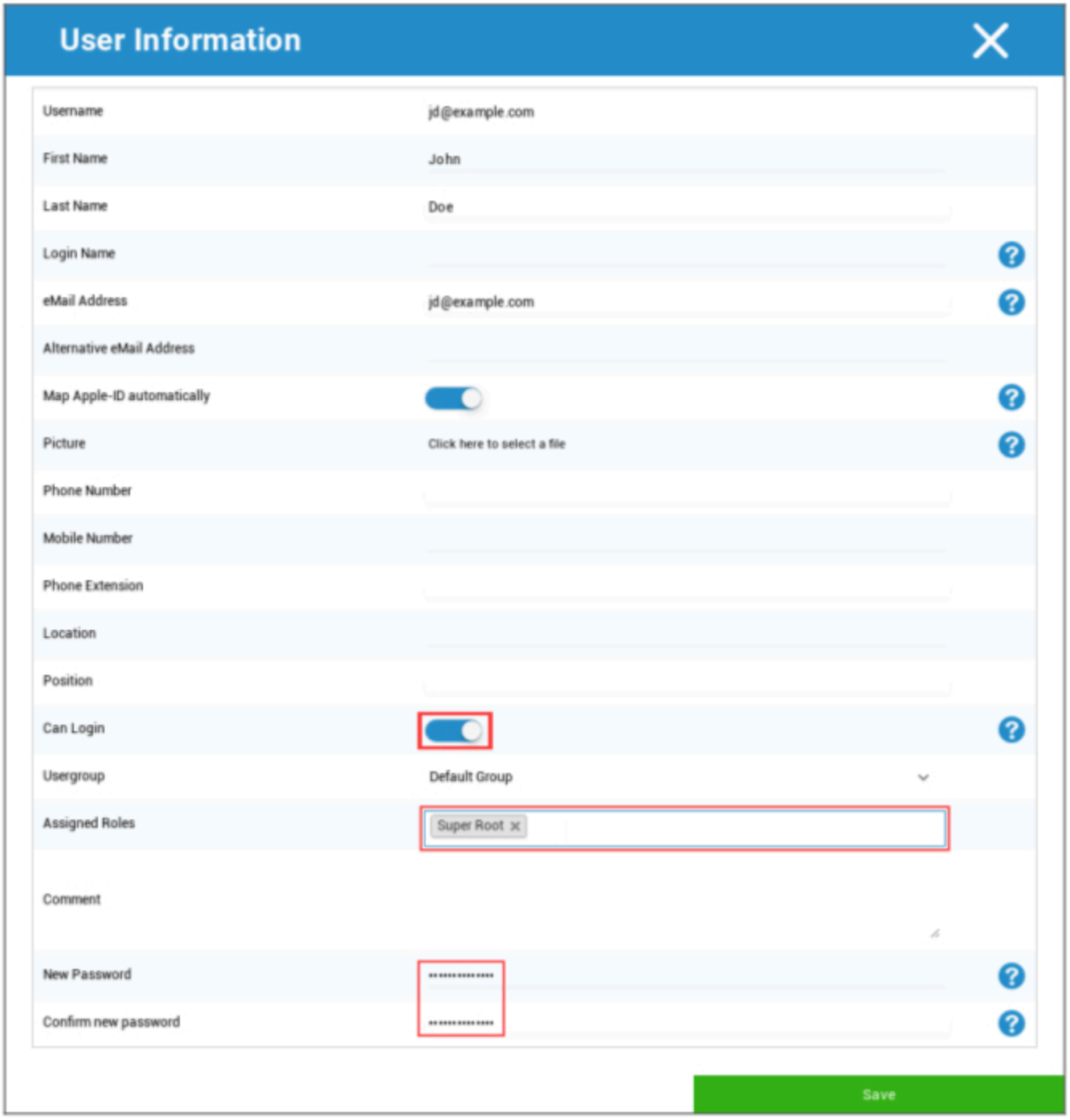
Med "Create a User" kan du lägga till en ny användare.

### Skapa en ny Admin-användare

Du kan ställa in en användare som Admin-User. Då får han behörighet att logga in på konsolen och även ändra användare/grupper/enheter.

Skapa en vanlig användare eller använd en befintlig användare. Välj den användare som du vill ge administratörsbehörighet, klicka på hjulet och välj "Redigera användare":

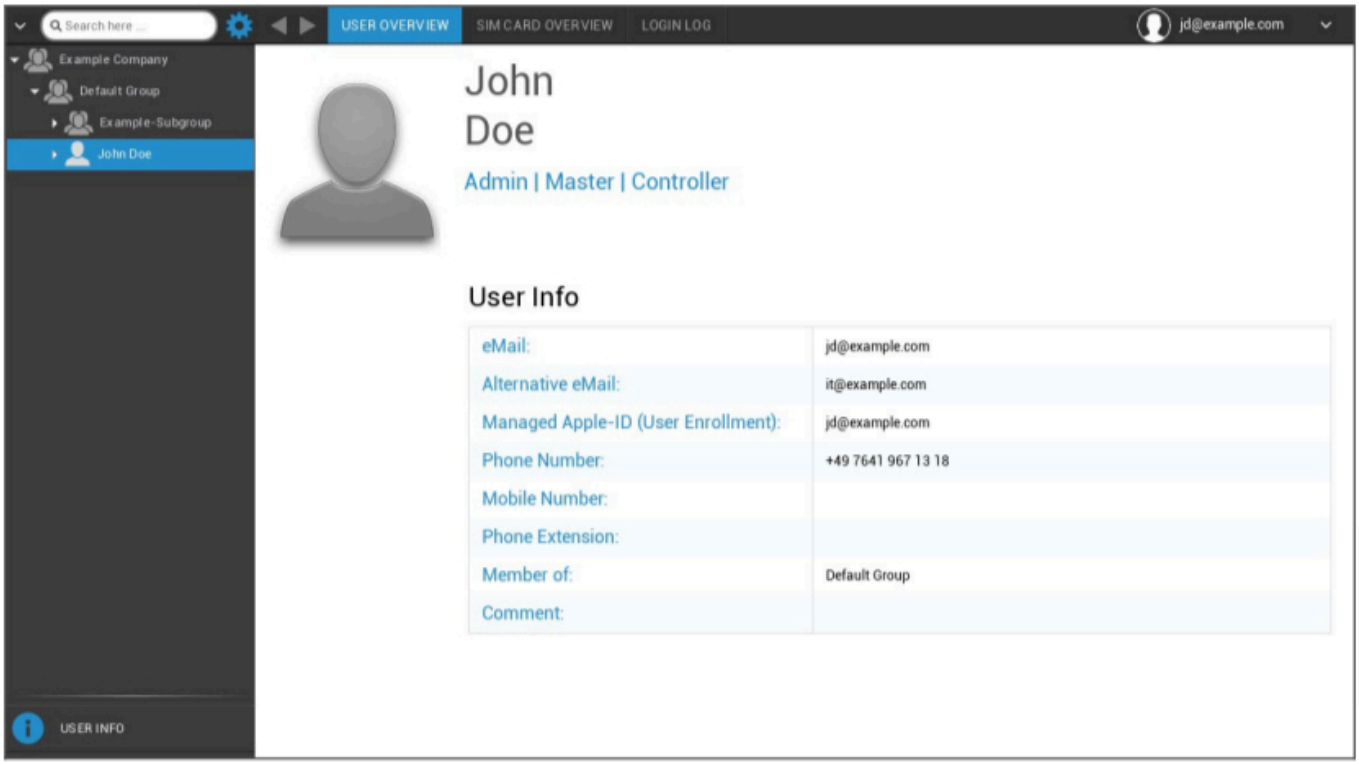
Aktivera omkopplaren för "Kan logga in", tilldela användaren rollen "Super-Root" och ange ett lösenord.




Spara detta och användaren kan nu logga in med användarnamn och lösenord.

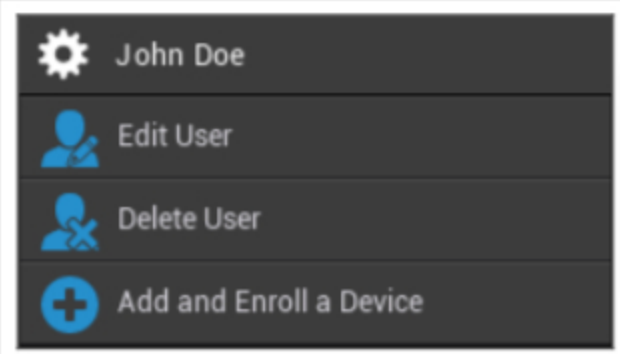
# Användarhantering i Mobile Management

När du väljer en viss användare ser du följande översikt:




Du får en översikt över all information som du angav tidigare i "Skapa en användare".

Med den utrustning som är installerad högst upp kan du utföra följande konfigurationer:




| | |
|---|---|
| Användarnamn | Användarnamn för vald användare |
| Redigera användare | Redigera användarinformation |
| Ta bort användare | Ta bort användare<br>• Delete from System = Enheten kommer att tas bort från AppTec |

| | |
|---|---|
| | • Wipe & Delete = Enheten återställs till fabriksinställningarna och tas bort från AppTec |
| Lägga till och registrera en enhet | Registrera en enhet för den valda användaren |

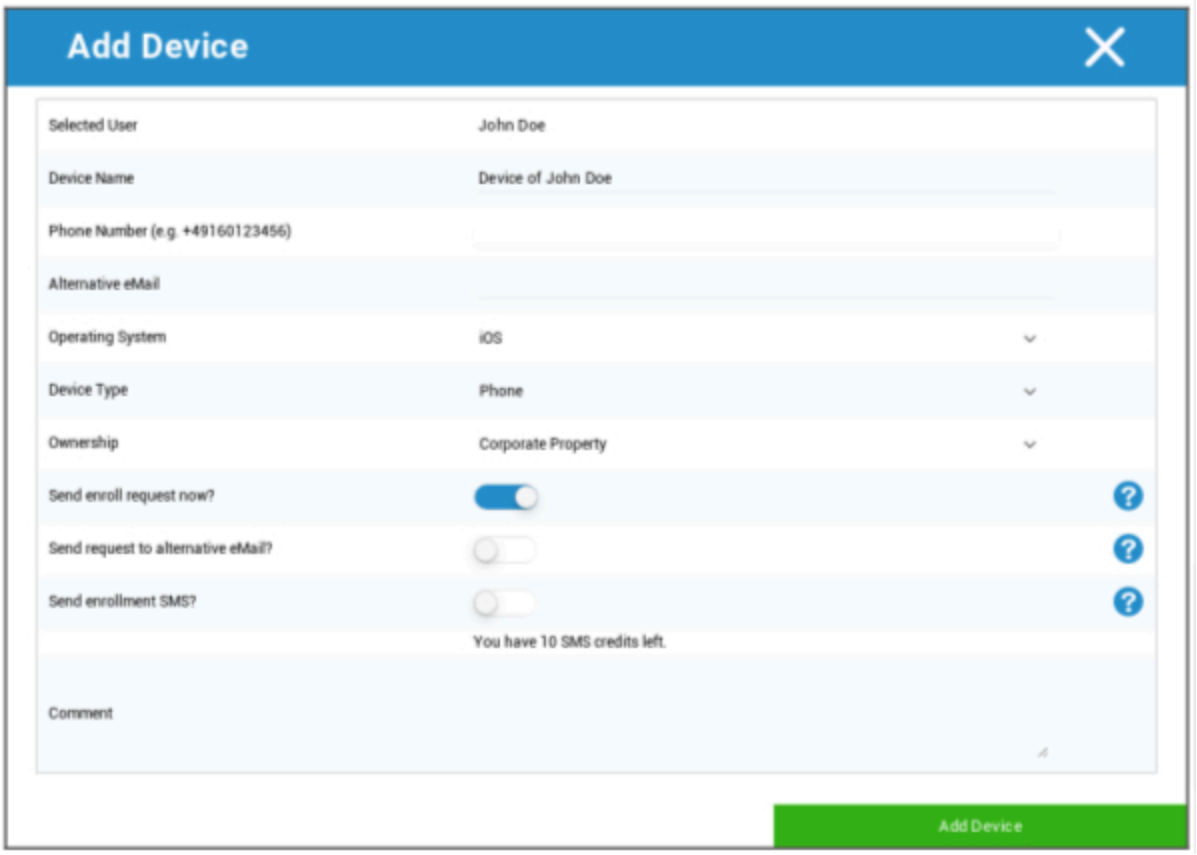
Observera att administrationsåtkomsten också kan arkiveras som ett lokalt användarkonto i hierarkistrukturen. Om inte ytterligare en administratör har inrättats bör denna inte tas bort!

## Lägga till och registrera en enhet

Här kan du välja en enhet för den valda användningen.

Alternativt kan du registrera enheter i en grupp direkt. Klicka då på gruppen, klicka på hjulet och välj "Lägg till och registrera en enhet".

Du bör se följande översikt:



Beroende på vilken typ av enhet du vill registrera måste du utföra följande konfigurationer:

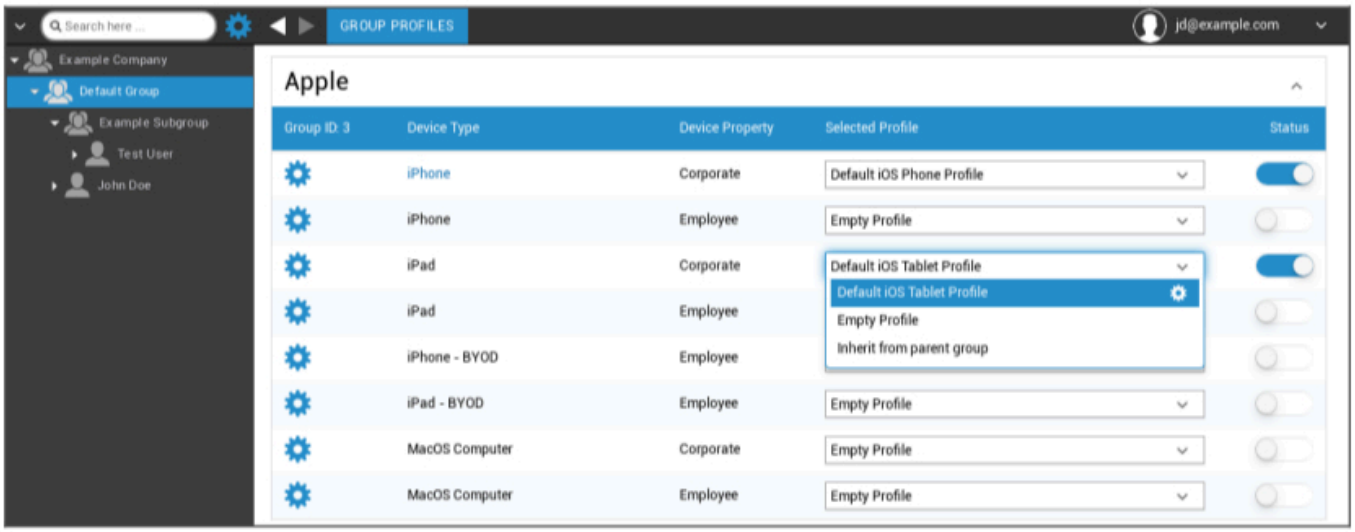
| | |
|---|---|
| Vald användare | Vald användare (fylls i automatiskt) |
| Enhetens namn | Fylls i automatiskt (enhet för "användarens namn") - kan dock ändras |
| Telefonnummer | Telefonnummer, fylls i automatiskt (så länge det har angetts av användaren) - här kan det dock läggas till eller ändras |
| Alternativ eMail | Alternativ e-postadress, fylls i automatiskt (så länge den har angetts av användaren) - här kan den dock läggas till eller ändras |
| Ägare av enheten | Företagets egendom = företagets enhet<br>Medarbetarens egendom = BYOD-enhet |
| Välj operationssystem | Här kan du välja mellan följande operativsystem:<br>• iOS<br>• iOS BYOD (registrering av användare)<br>• MacOS<br>• Android Företag<br>• Android<br>• Windows Mobile<br>• Windows 10 |
| Skicka inskrivningsbegäran? | E-postmeddelandet skickas omedelbart till den huvudsakliga e-postadressen och användaren uppmanas att ansluta sin enhet |
| Skicka förfrågan till alternativ eMail? | Skicka e-postmeddelandet dessutom eller enbart (om "Skicka inskrivningsbegäran?" avaktiverades) till den alternativa e-postadressen (e-postadressen skiljer sig från den "normala" e-postadressen för inskrivningsbegäran) |
| Skicka SMS om registrering? | Skicka en inskrivningsbegäran via SMS (telefonnumret måste anges) |

När registreringsbegäran har skickats kommer enheten att visas (rödmarkerad) direkt.

Så snart enheten har anslutits på ett framgångsrikt sätt kommer enheten att markeras med grönt kort därefter och är därmed redo att ta emot begränsningar, appar etc.

## Profilhantering i Mobile Management

När du har klickat på en grupp får du en översikt över alla enhetsplattformar som ska konfigureras och de profiler som har tilldelats dem.




| | |
|---|---|
| | Utför konfigurationen för den valda profilen |
| Enhetstyp | Enhetstyp och/eller modell |
| Enhetens egenskaper | Enhetens ägare (Företag = företagets egendom, Anställd = privatanställdas enhet) |
| Utvald profil | Vald profil (kugghjulet öppnar profilens konfigurationsdialog) |
| Status | On/Off (profilen är aktiverad/avaktiverad) |

När du väljer växeln får du följande alternativ:

## Skapa en profil

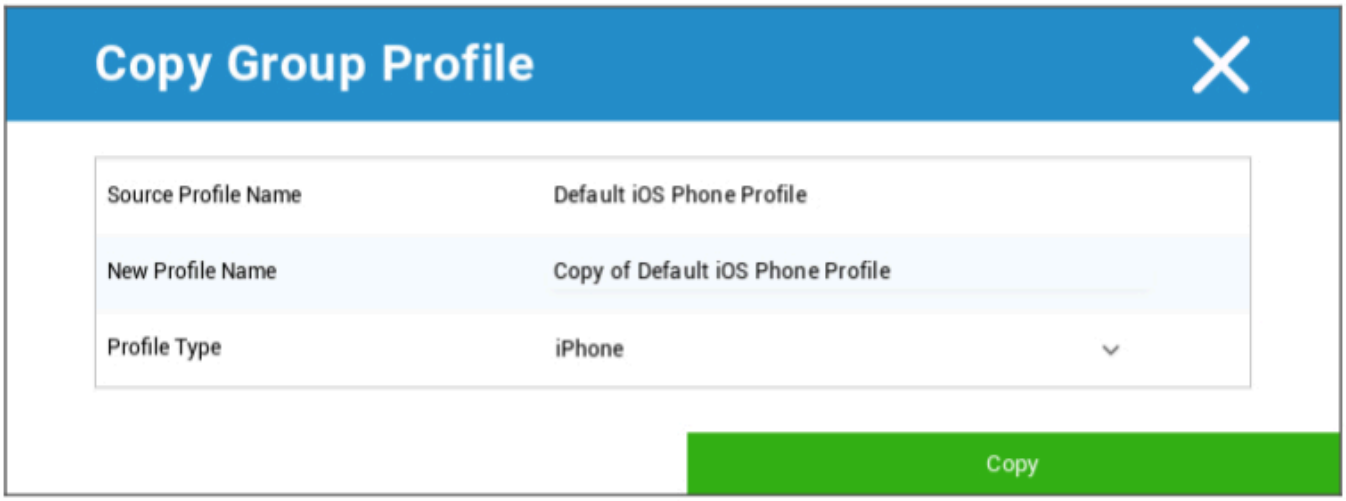
Du kan skapa och konfigurera en ny profil för varje post och/eller plattform. När du har klickat på denna underpunkt skapas profilen omedelbart och du kan börja konfigurera iOS, Android och Windows Phone direkt.

## Redigera profil

När du har klickat på "Edit Profile" kommer du till konfigurationsdisplayen för respektive profil, där du kan ställa in konfigurationerna.

## Kopiera profil

Med hjälp av funktionen "Copy Profile" kan du kopiera inställningar/konfigurationer från en redan befintlig profil och lägga till dem i en ny profil.

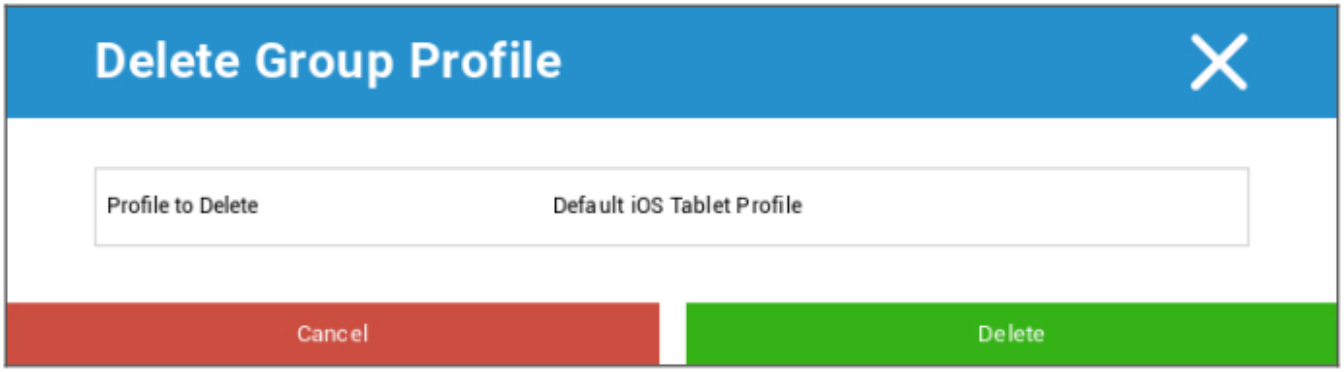



| | |
|---|---|
| Källa Profilnamn | Namn på den profil som ska kopieras |
| Nytt namn på profilen | Namn på den nya profilen |
| Typ av profil | Profiltyp (telefon/surfplatta) |

När du klickar på "Kopiera" skapas profilen och kan nu tilldelas till gruppen

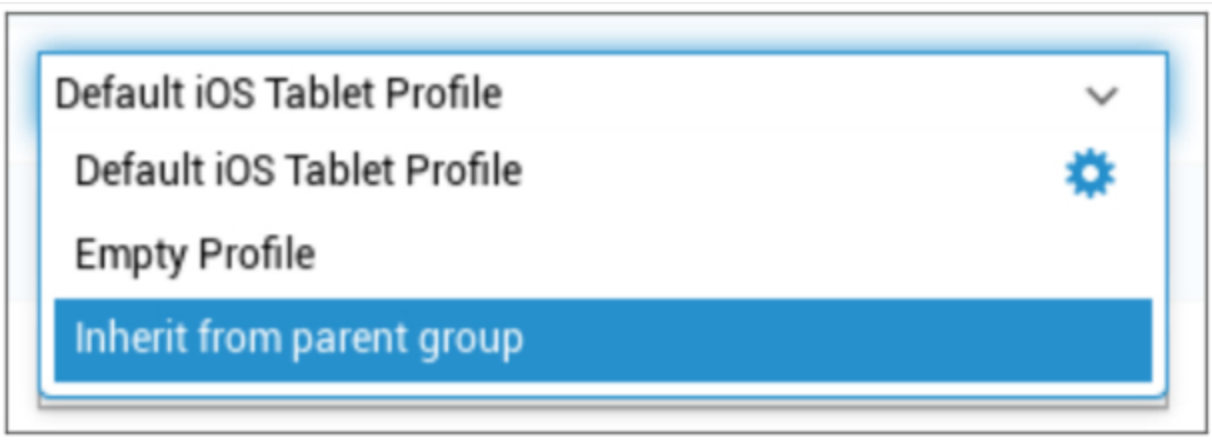
## Ta bort profil

Här kan du ta bort en profil permanent. Observera att under borttagningsprocessen och den följande "Tilldela nu"-processen för profilen kommer konfigurationen att försvinna på respektive enheter i en berörd grupp och kan inte återställas!


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

## Ärvning av profiler

Under valet av profiler finns alternativet "Ärva från föräldragrupp" tillgängligt.




När profilen aktiveras kommer profilen för den överordnade gruppen att användas för respektive vald enhet (och respektive enhetstyp). Observera också att ändringar i den här profilen kan påverka flera grupper.

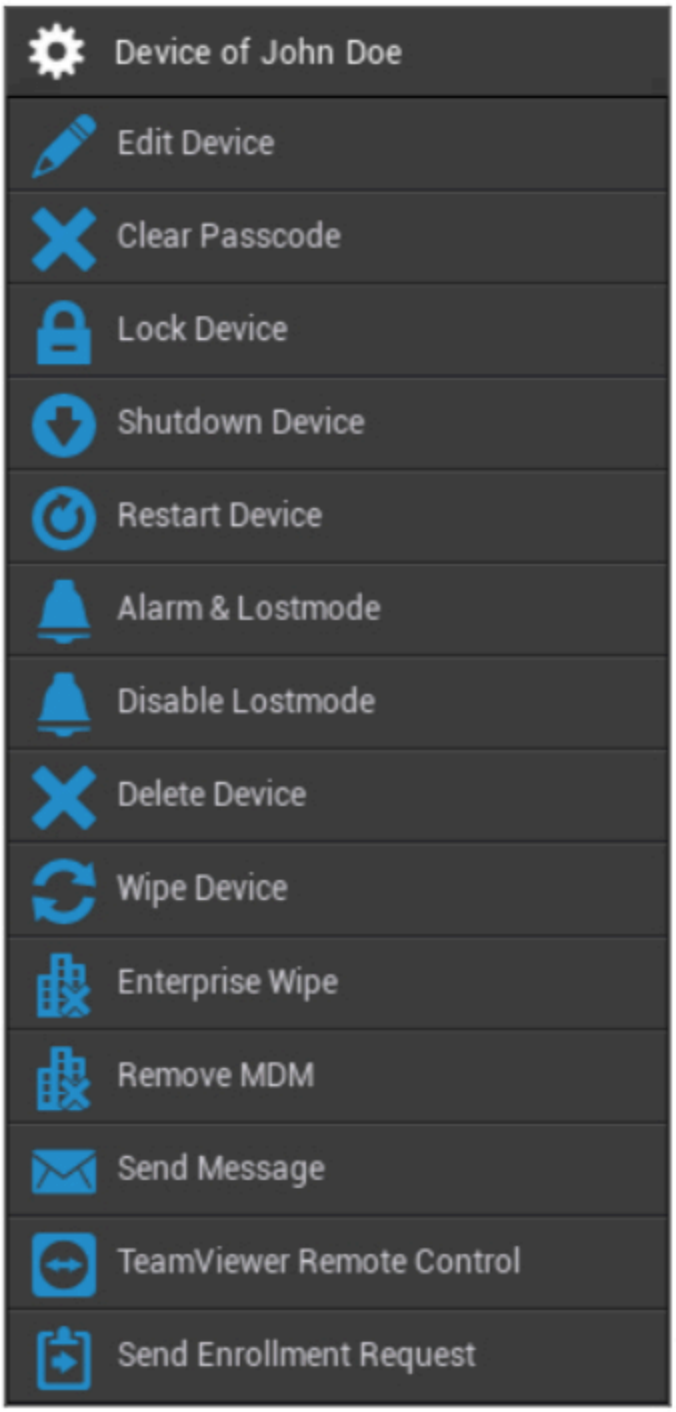
Denna konfiguration anges som standardvärde när en ny undergrupp skapas.

Konfigurationen "Empty Profile" finns också tillgänglig, vilket motsvarar en tom profil, vilket innebär att inga nya konfigurationer kommer att utföras på slutanvändarens enhet.

# Enhetshantering i Mobile Management

När du väljer en enhet kan du utföra en mängd olika uppgifter via "kugghjulet". Dessa är olika beroende på OS-plattformarna (iOS, Android Enterprise, Android, Windows Mobile, Windows 10).

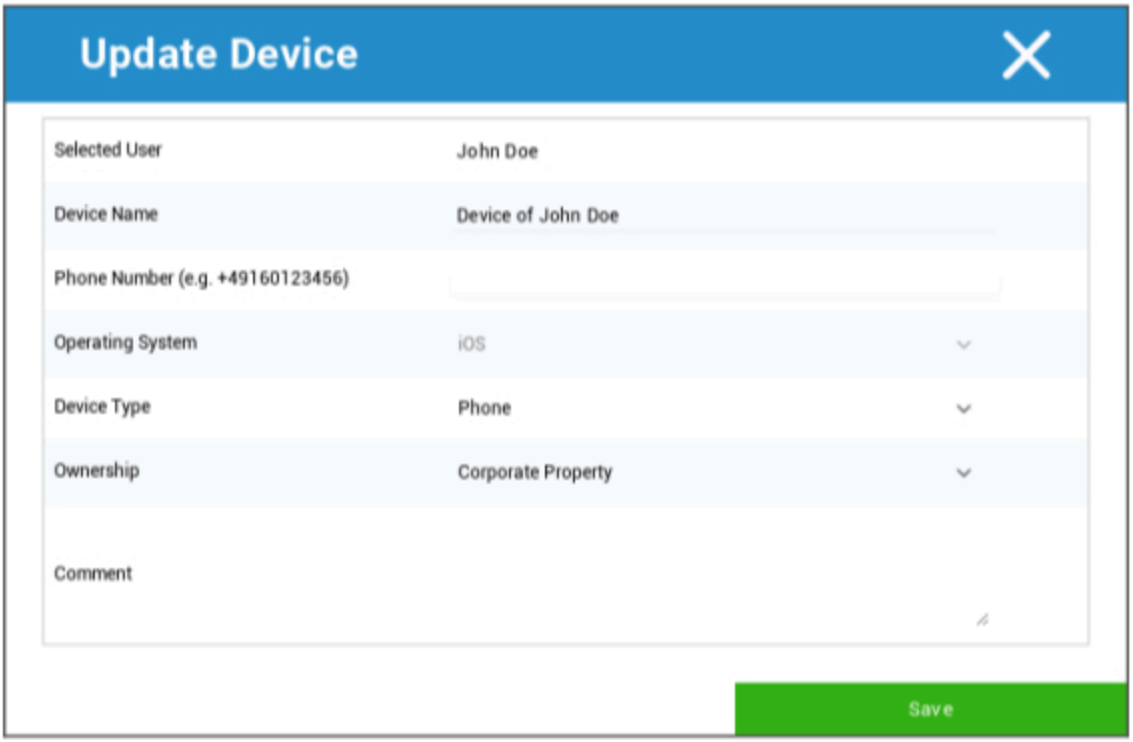
## IOS




| | |
|---|---|
| Redigera enhet | Redigera enhet |
| Rensa lösenord | Enhetens lösenord har raderats |
| Låsanordning | Lås enhet (låsskärm) |
| Avstängningsenhet | Avstängningsenhet |

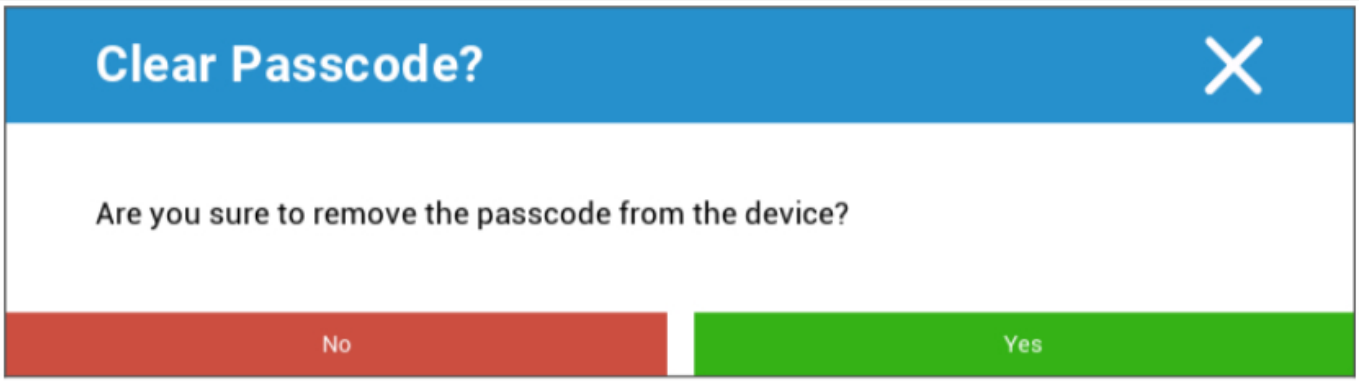
| | |
|---|---|
| Starta om enheten | Starta om enheten |
| Alarm & Lostmode | Startlarm & Lostmode |
| Inaktivera Lostmode | Inaktivera Lostmode |
| Ta bort enhet | Ta bort enheten från AppTec |
| Torka av enhet | Återställ enheten till fabriksinställningarna |
| Enterprise Wipe | Information, appar och profiler som tillhandahålls av AppTec360 raderas (enheten separeras från MDM) |
| Ta bort MDM | |
| Skicka meddelande | Skicka push-meddelanden till enheten<br>Meddelandet kommer att visas i AppTec360 App (fliken Meddelande) |
| TeamViewer Fjärrkontroll | Starta fjärrkontrollsession med hjälp av TeamViewer |
| Skicka inskrivningsbegäran | Skicka (upprepad) Inskrivningsbegäran |

## Redigera enhet



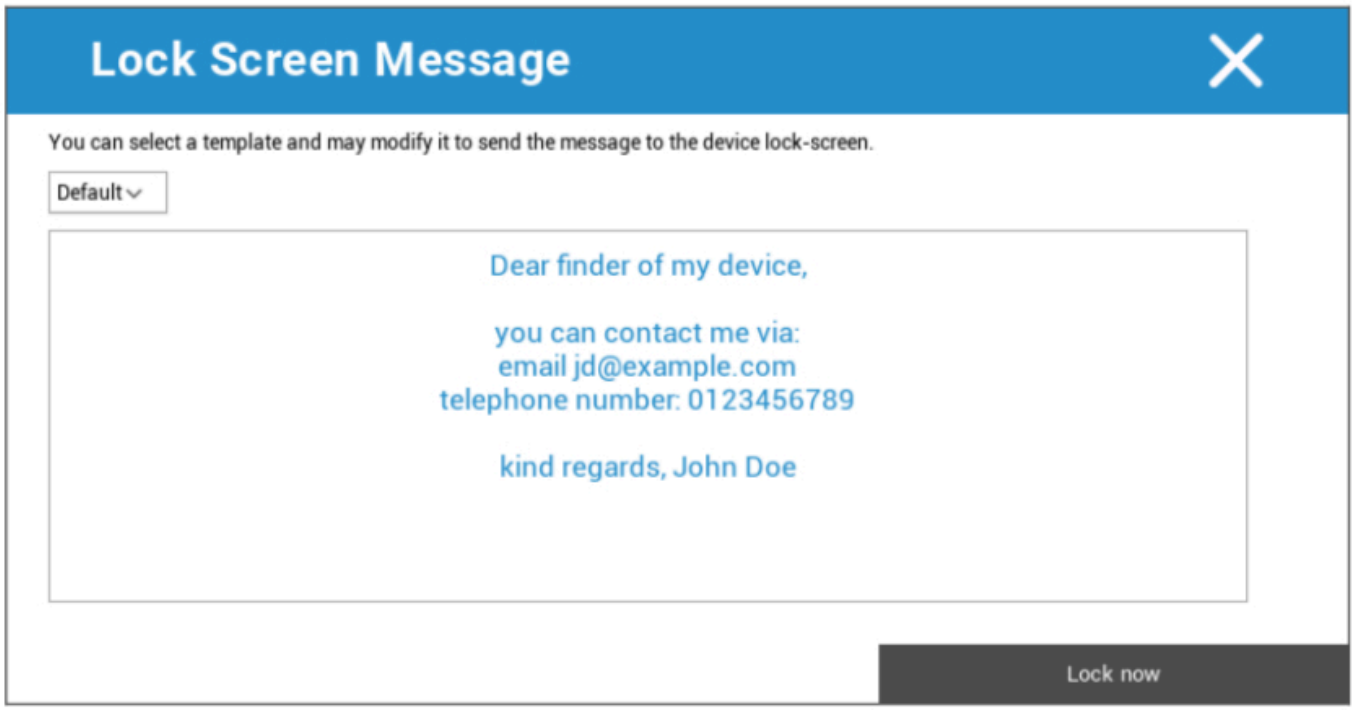

Här kan du uppdatera en mängd olika uppgifter om enheten.

## Rensa lösenord



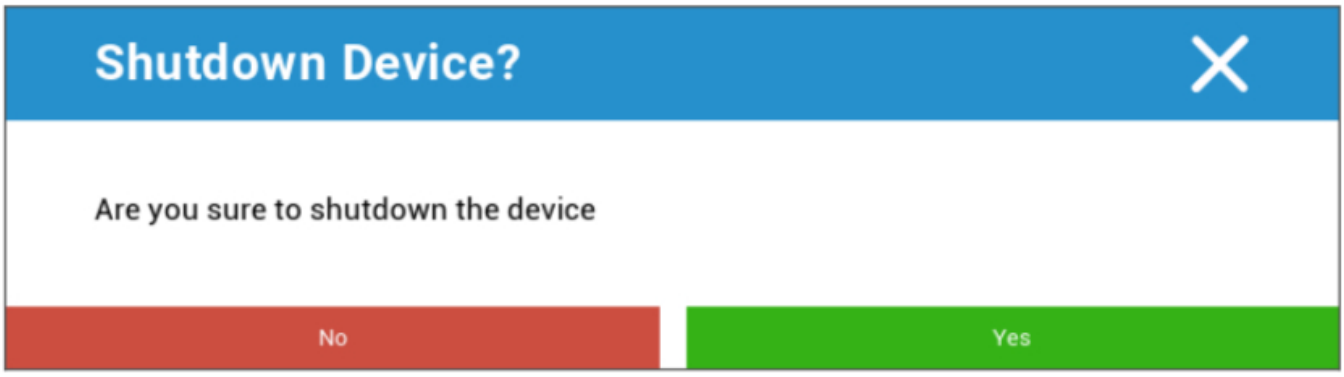

Under "Clear Passcode" kan du fjärrstyra bort lösenordet från enheten. Därefter kommer användaren att uppmanas att ange ett nytt lösenord (beroende på riktlinjerna för lösenord).

## Låsanordning



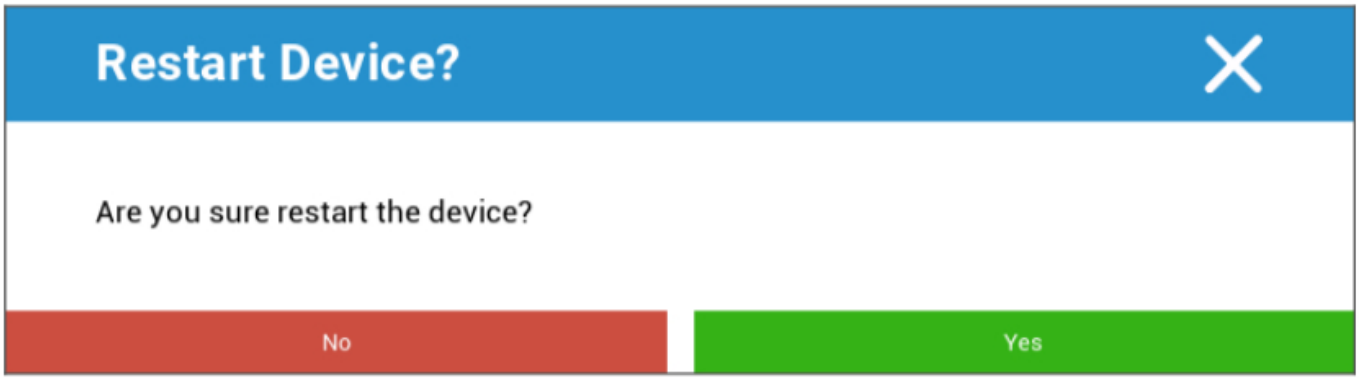

Här skickas ett låskommando till slutanvändarens enhet (låsskärm).

## Avstängningsenhet



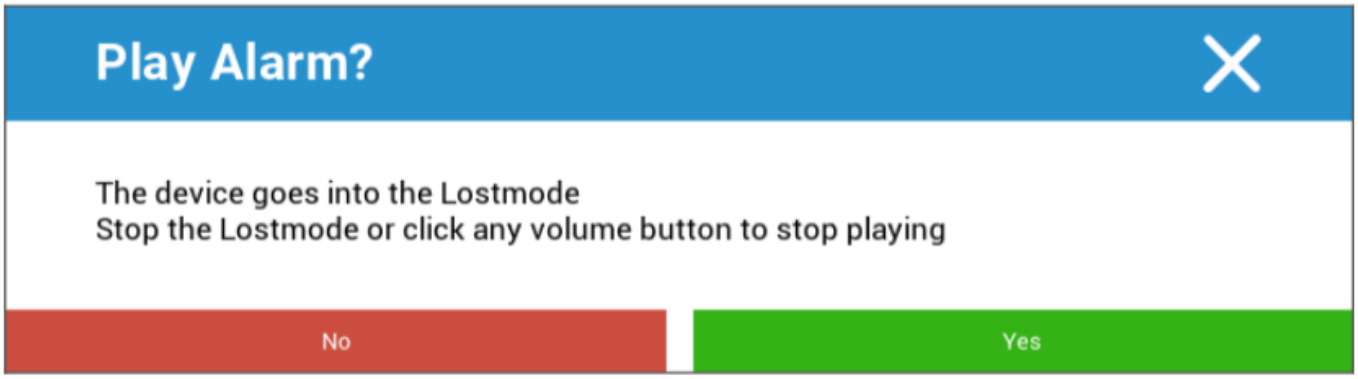

Här skickas ett avstängningskommando till slutanvändarens enhet.

## Starta om enheten

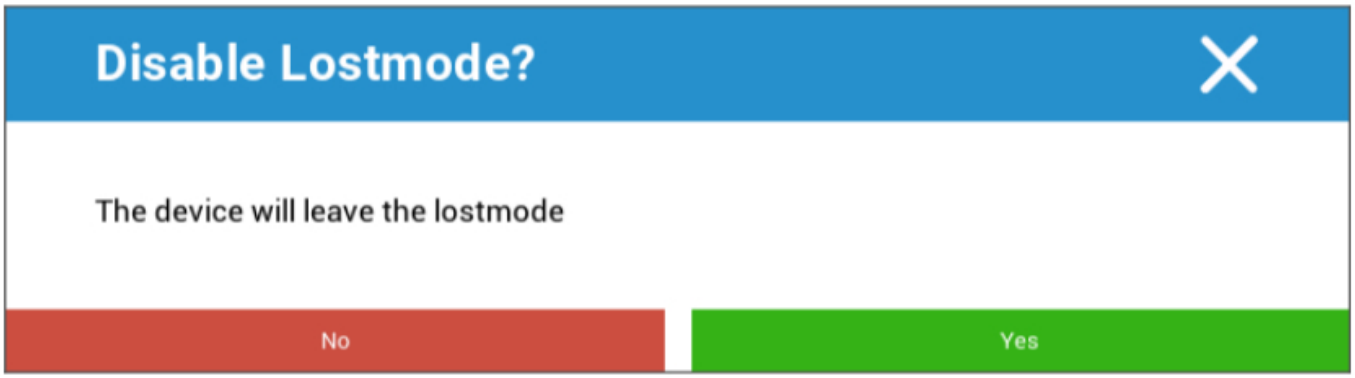



Här skickas ett omstartskommando till slutanvändarens enhet.

## Larm & Lostmode | Avaktivera Lostmode



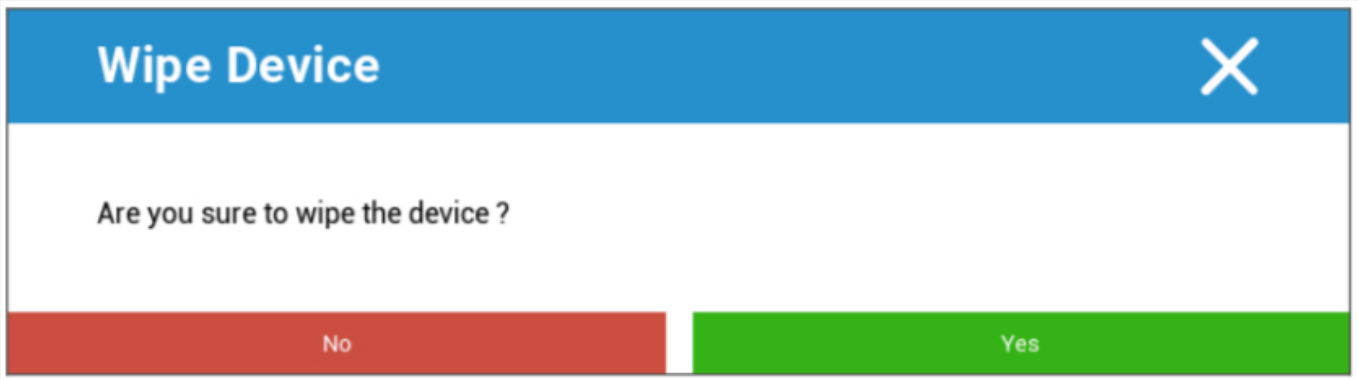

Här kan enheten ställas in i Lostmode, vilket innebär att enheten ständigt spelar upp ett larmljud. Lostmode kan avbrytas genom att trycka på valfri volymknapp på enheten eller på distans genom att klicka på "Disable Lostmode":



## Ta bort enhet


Här kan kommandot för borttagning utföras. Du kan återigen bestämma om enheten endast ska tas bort från AppTec360 ("Radera från systemet") eller om enheten ska tas bort från AppTec360 och även återställas till fabriksinställningarna ("Wipe & Delete").

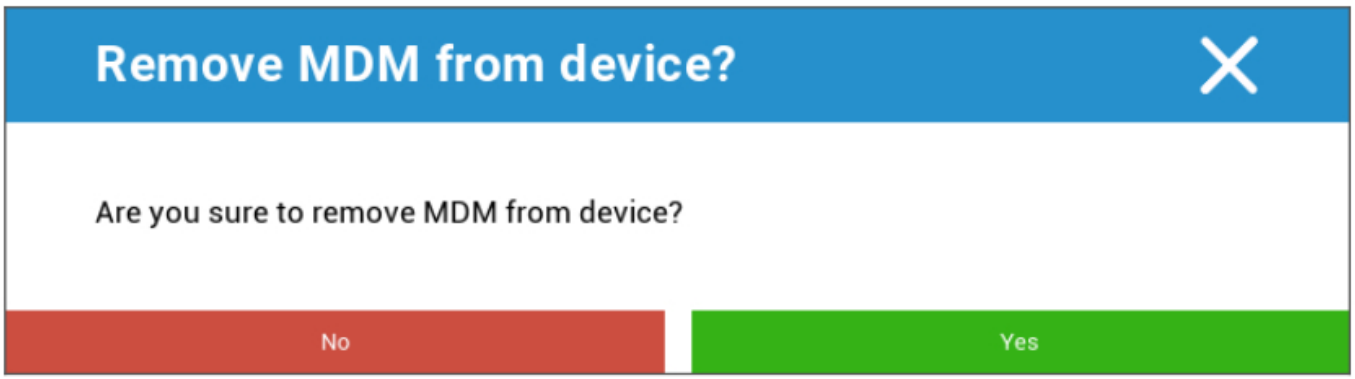
## Torka av enhet




Under "Wipe Device" kan du utföra en fullständig radering av enheten. Enheten återställs till sina fabriksinställningar.

## Enterprise Wipe | Ta bort MDM

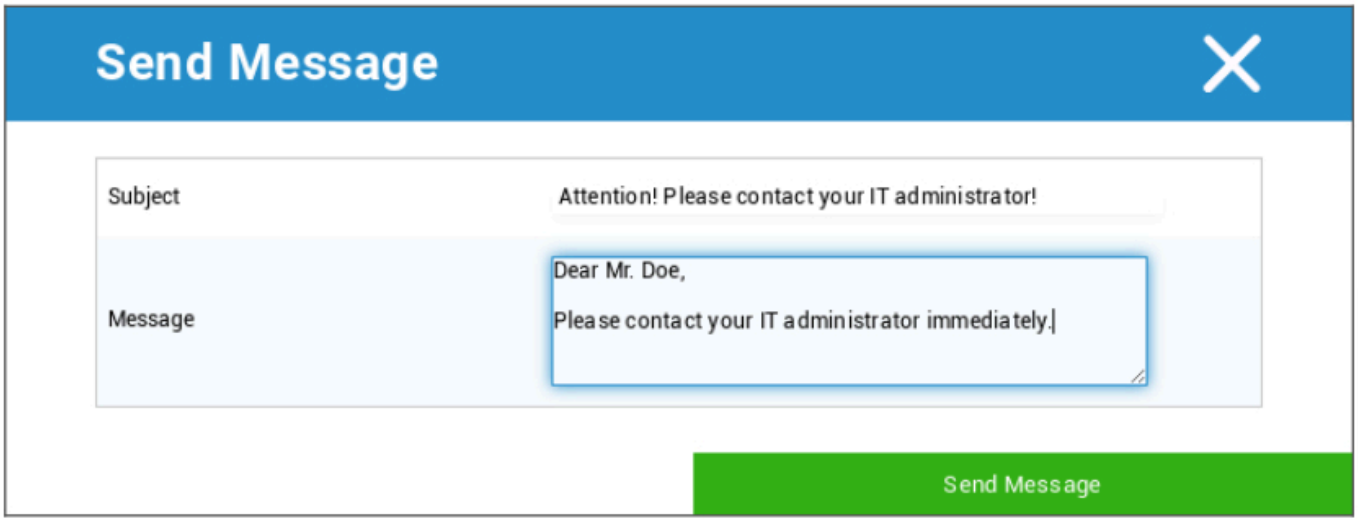
Endast den information, de appar och de profiler som tillhandahålls av AppTec360 raderas. På så sätt kommer företagsdata inte längre att vara tillgängliga på slutanvändarens enhet. Det privata området påverkas inte och fortsätter att finnas kvar på slutanvändarens enhet.




Med "Remove MDM" kan du ta bort MDM-profilen på slutanvändarens enhet och alla andra objekt som tillhandahålls av AppTec.

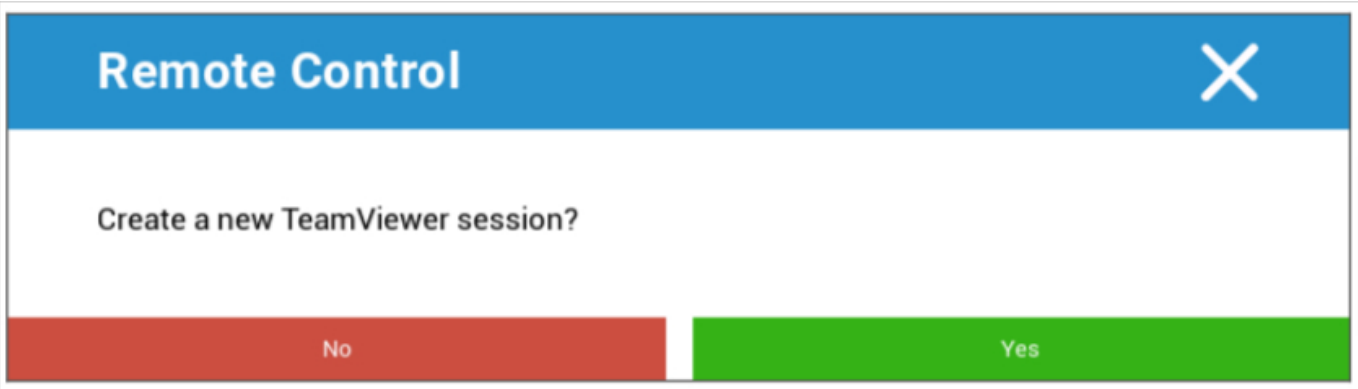
Detta kommando utför samma åtgärd som "Enterprise Wipe".

## Skicka meddelande




Här kan du skicka en push-notifiering till respektive enhet.

## TeamViewer Fjärrkontroll



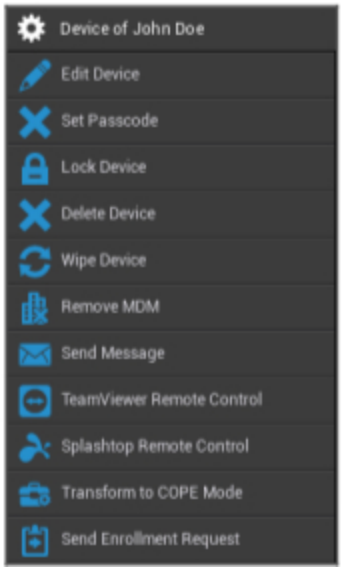

Här kan en Teamviewer Remote Control-session startas.

## Skicka inskrivningsbegäran

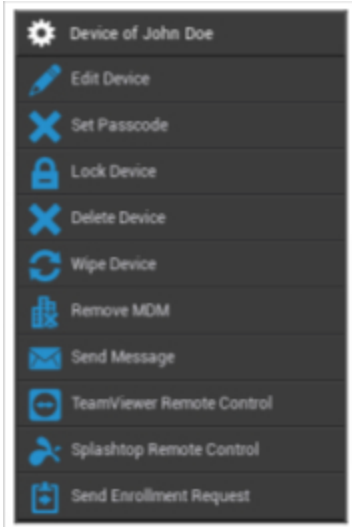
Med "Send Enrollment Request" kan du skicka en registreringsbegäran (igen) till respektive användare.

## Android

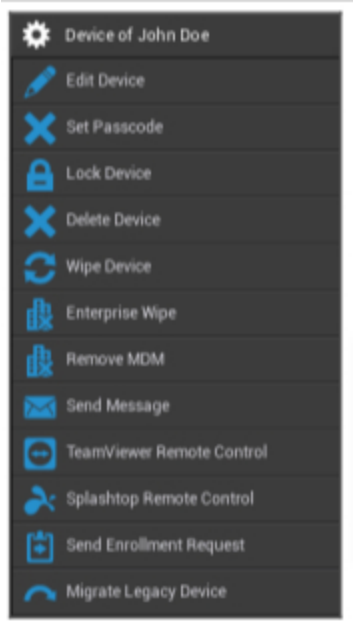
AE Fullt hanterad enhet (arbetshanterad)




AE-arbetsprofil (container)



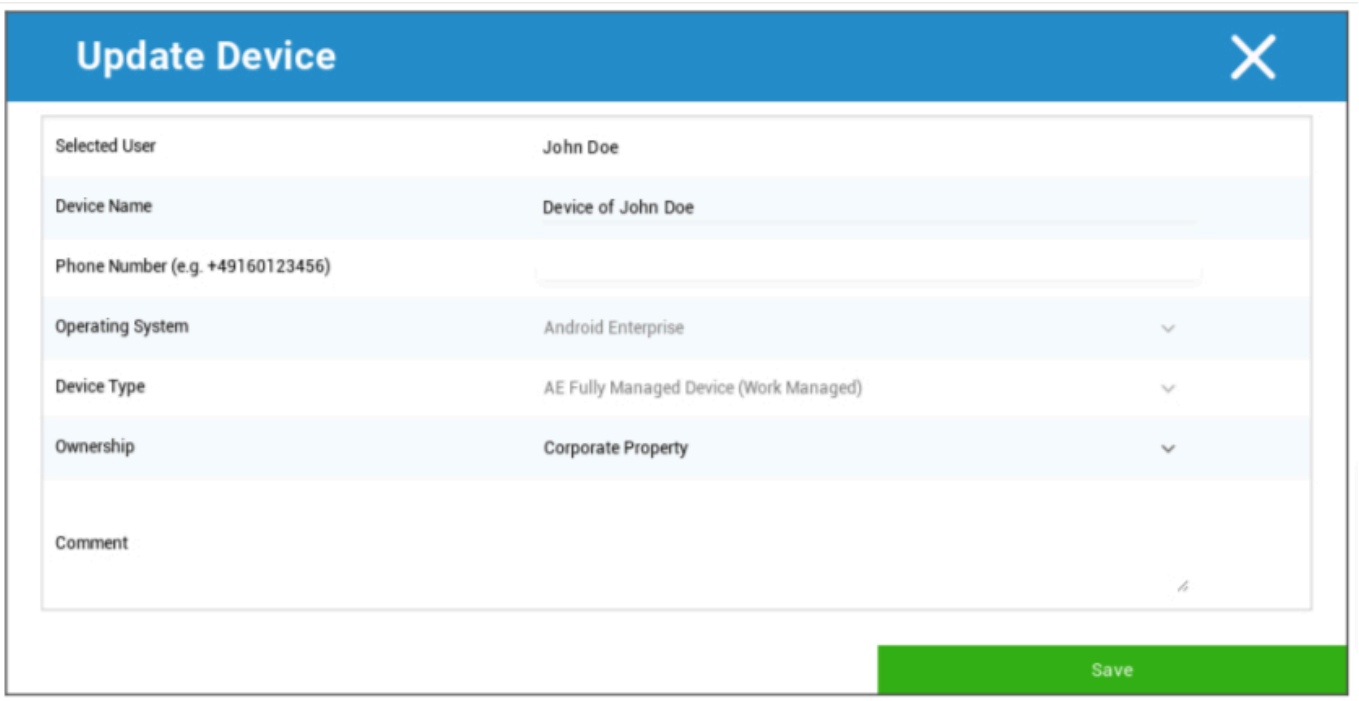

Android-telefon | surfplatta




| | |
|---|---|
| Redigera enhet | Redigera enhetsinformation |
| Ange lösenord | Ställ in enhetens lösenord |
| Låsanordning | Lås enhet (låsskärm) |
| Ta bort enhet | Ta bort enhet från AppTec |
| Torka av enhet | Återställ enheten till fabriksinställningarna |
| Enterprise Wipe | Information, appar, profiler som tillhandahålls av AppTec360 raderas (enheten separeras från MDM) |
| Ta bort MDM | |
| Skicka meddelande | Skicka push-meddelanden till enheten Meddelandet kommer att visas i AppTec360 App (fliken Meddelande) |
| TeamViewer Fjärrkontroll | Starta en fjärrkontrollsession för den här enheten med hjälp av TeamViewer |
| Splashtop Fjärrkontroll | Starta en fjärrkontrollsession för den här enheten med hjälp av Splashtop |
| Omvandla till COPE-läge (endast på AE Fullt hanterad enhet (arbetshanterad)) | Skapa en arbetsprofil på denna AE Fullt hanterade (arbetshanterade) enhet |
| Skicka inskrivningsbegäran | Skicka (upprepad) begäran om inskrivning |
| Migrera äldre enhet (endast på Android-telefoner/plattor när de registreras med hjälp av Device Owner Mode Provisioning) | Migrera Android Phone / Tablet-profil till AE Fullt hanterad enhet (arbetshanterad) profil |

## Redigera enhet

Här kan du uppdatera en mängd olika enhetsuppgifter.




| | |
|---|---|
| Vald användare | Enhetens användare |
| Enhetens namn | Enhetens namn |
| Telefonnummer | Enhetens telefonnummer |
| Operativsystem | Android Företag<br>Android |
| Enhetstyp | Android Enterprise:<br>• AE Fullt hanterad enhet (arbetshanterad)<br>• AE-läge för arbetsprofil (endast behållare)<br>• AE Fullt hanterad enhet med arbetsprofil (COPE)<br><br>Android:<br>• Telefon<br>• Tablett |
| Ägarskap | Corporate = företagsägd fastighet |

| | |
|---|---|
| | Anställd = egenskap för anställd |
| Kommentar | Ytterligare beskrivningar för enheten |

## Rensa lösenord

Här kan du ta bort enhetens lösenord på den valda enheten. Som standard på Android kommer lösenordet att ställas in på "123456" - detta kan och bör ändras av användaren efteråt.

## Låsanordning

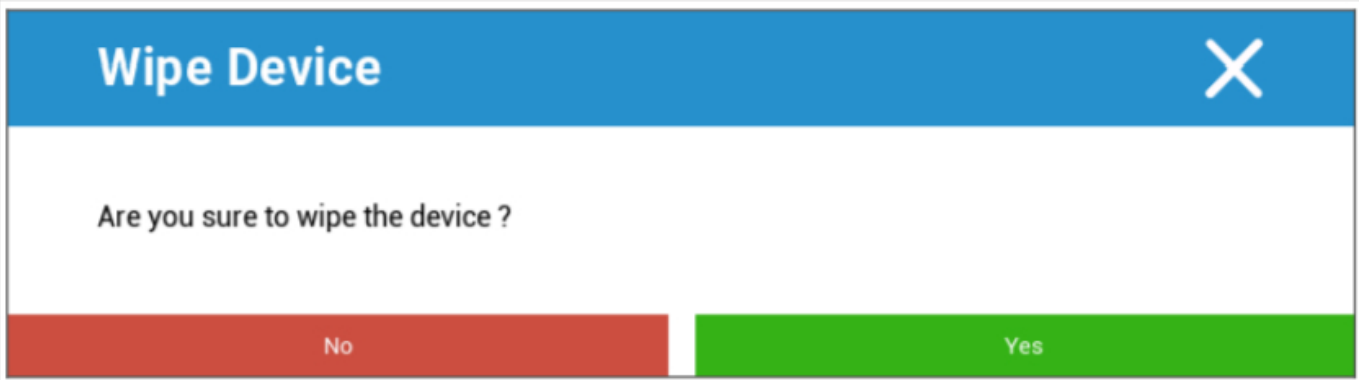
Här skickas ett kommando för att låsa enheten till enheten (låsskärm).

## Ta bort enhet


Här kan du utföra ett raderingskommando. Du kan återigen bestämma om enheten endast ska tas bort från AppTec360 ("Radera från systemet") eller om enheten ska tas bort från AppTec360 och dessutom återställas till fabriksinställningarna ("Wipe & Delete").

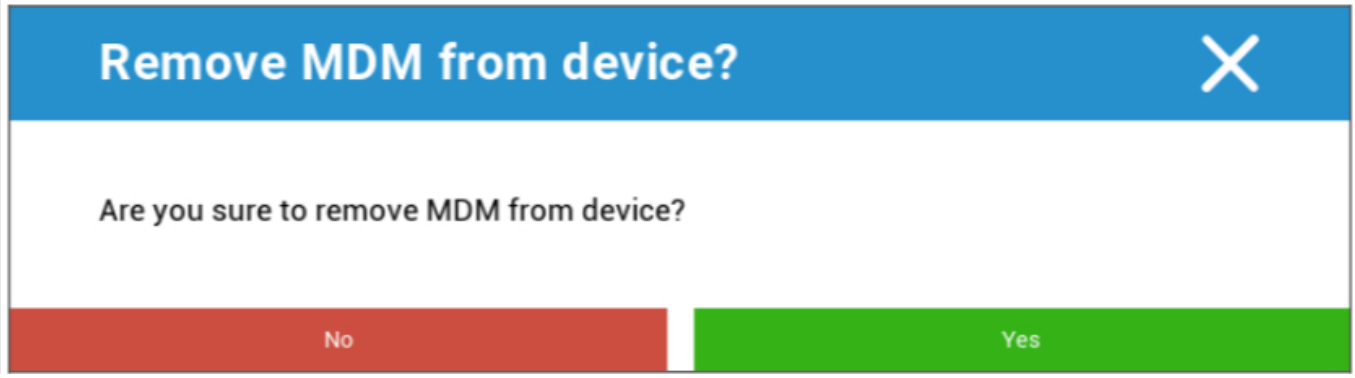
## Torka av enhet

Under "Wipe Device" kan du utföra en fullständig radering av enheten. Enheten kommer då att återställas till fabriksinställningarna.



Om enheten innehåller ett SD-kort kan du dessutom radera SD-kortet. Detta kan du göra genom att ställa in "Wipe SD Card too? " till "På".

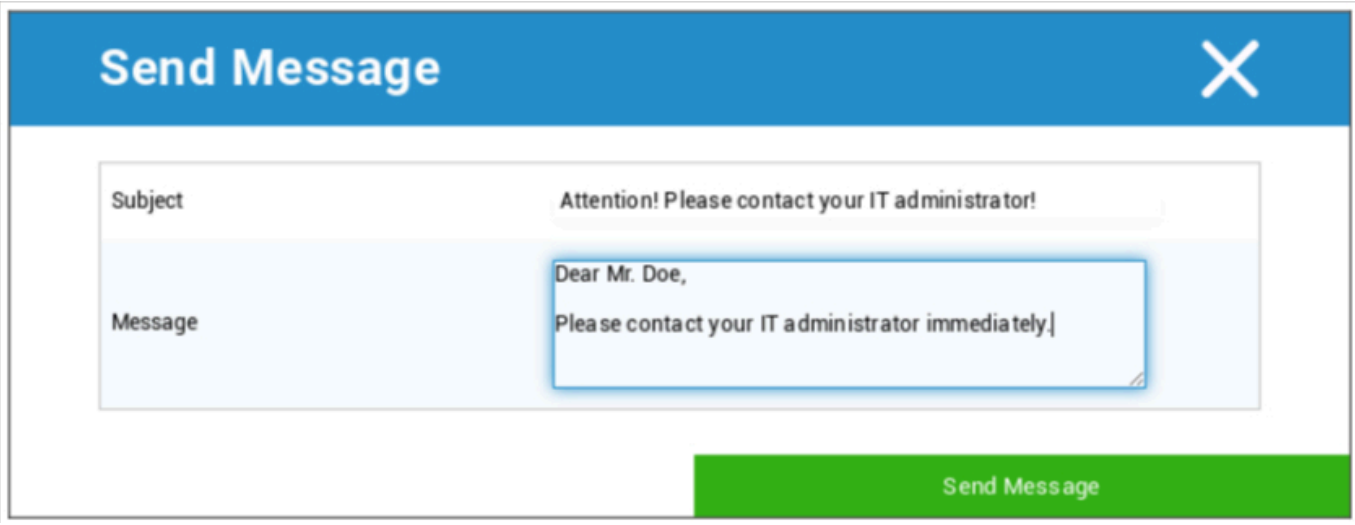
## Ta bort MDM




Detta är den rekommenderade metoden för att skapa en separation från MDM.

Endast den information, de appar och de profiler som tillhandahålls av AppTec360 raderas, vilket innebär att all företagsdata inte längre kommer att finnas tillgänglig på slutanvändarens enhet. Den privata sfären påverkas dock inte och fortsätter att finnas kvar på slutanvändarens enhet.

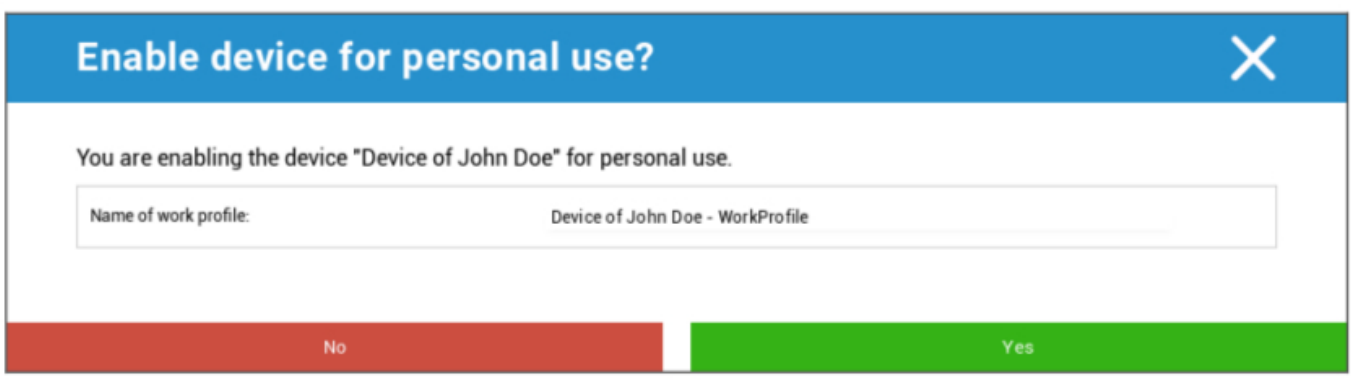
## Skicka meddelande



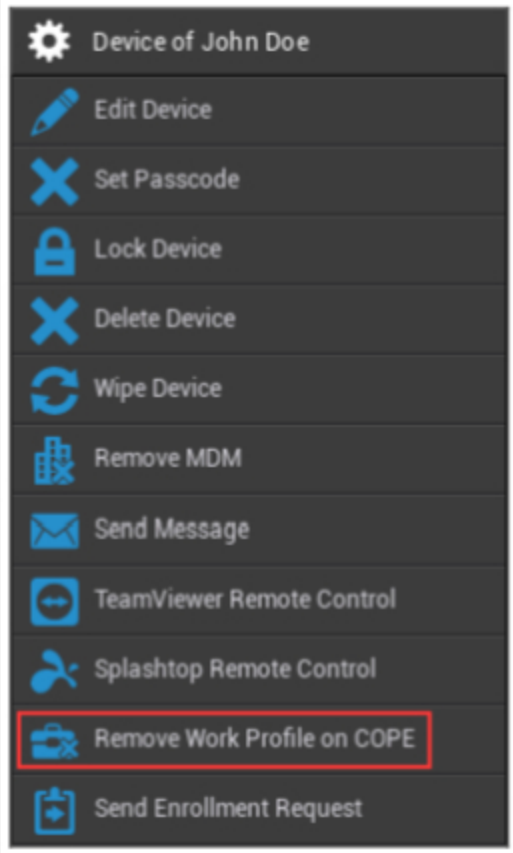

Här kan du skicka en push-notifiering till respektive slutanvändares enhet.

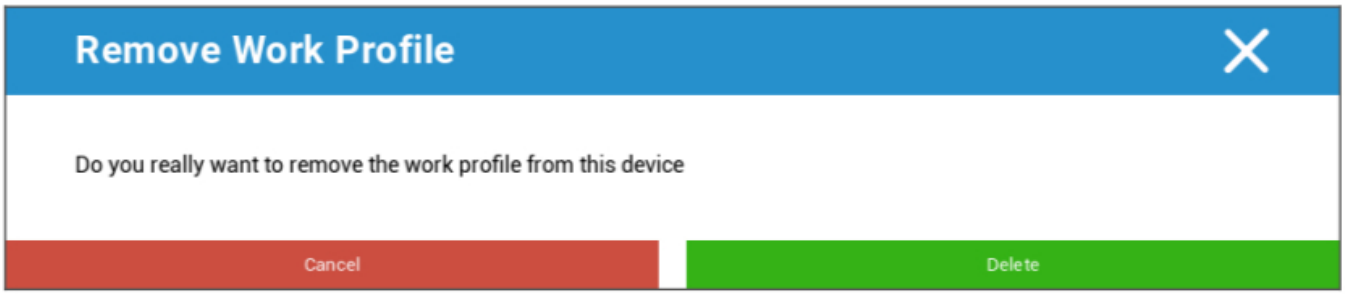
## Omvandla till COPE-läge

Skapa en arbetsprofil på denna AE Fullt hanterade (arbetshanterade) enhet




När du har omvandlat enheten till COPE-läge kan du ta bort arbetsprofilen genom att klicka på kugghjulsalternativet **Remove Work Profile on COPE**:




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

## Skicka inskrivningsbegäran

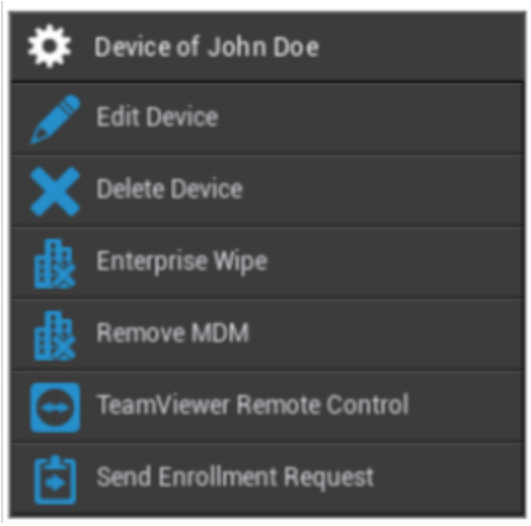
Med "Send Enrollment Request" kan du skicka en registreringsbegäran (igen) till respektive användare.

Observera att endast den senaste begäran om inskrivning är giltig.

## Migrera äldre enhet

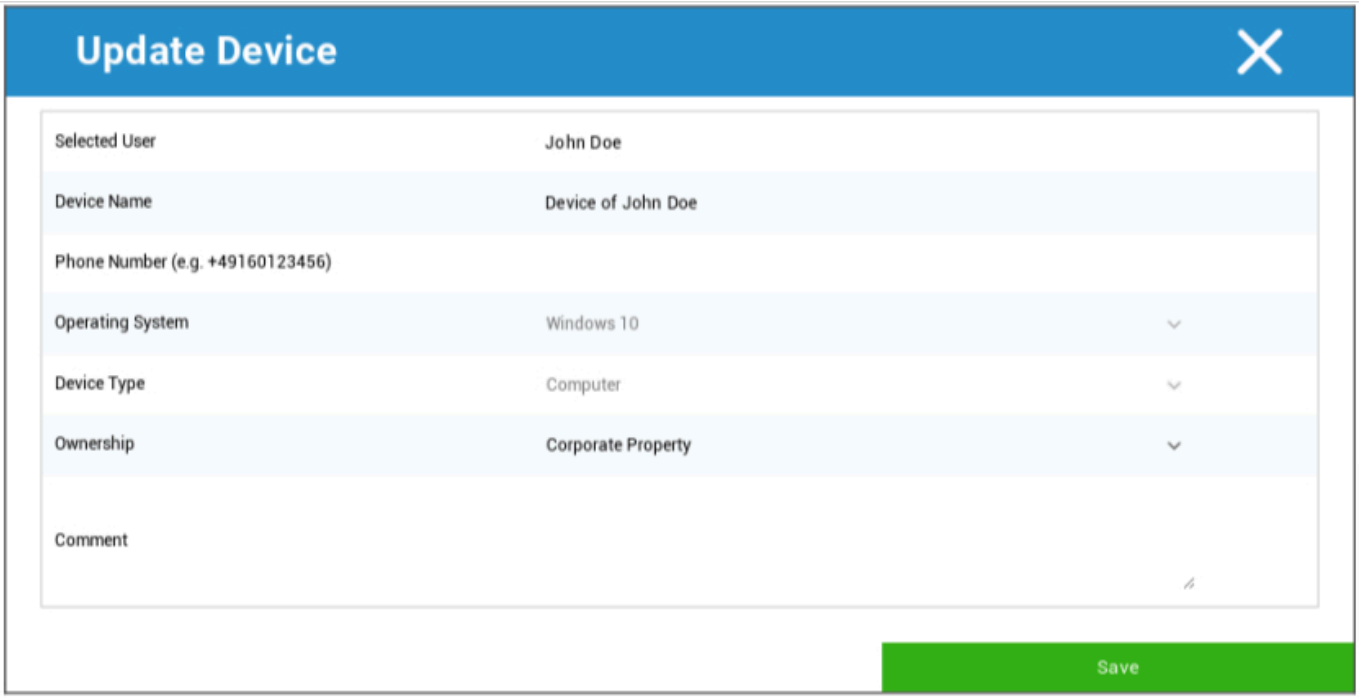
Migrera Android Phone / Tablet-profil till AE Fullt hanterad enhet (arbetshanterad) profil

## Fönster




| Enhetens namn | Namn på den valda enheten |
|---|---|
| Redigera enhet | Redigera enhet |
| Ta bort enhet | Ta bort enheten från AppTec |
| Enterprise Wipe | Information, appar och profil som tillhandahålls av AppTec360 raderas |
| Ta bort MDM | |
| TeamViewer Fjärrkontroll | Fjärrstyrning av enheten med TeamViewer |
| Skicka inskrivningsbegäran | Skicka inskrivningsbegäran (igen) |

## Redigera enhet

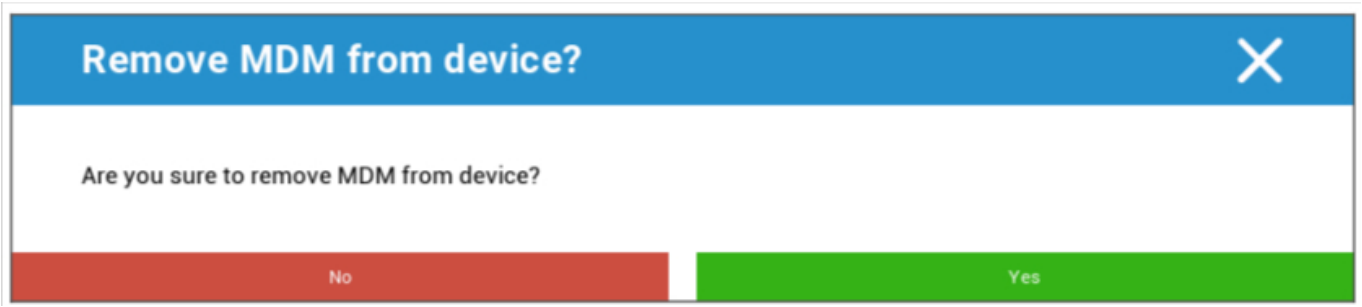



Här kan du uppdatera en mängd olika uppgifter om enheten.

## Ta bort enhet

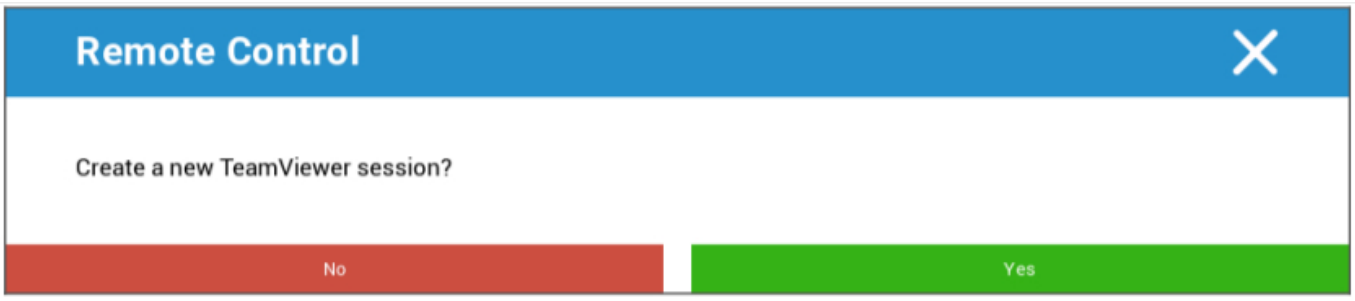
Här kan du utföra kommandot delete som endast tar bort enheten från AppTec360.


## Enterprise Wipe | Ta bort MDM




Endast den information, de appar och de profiler som tillhandahålls av AppTec360 raderas. På så sätt kommer företagsdata inte längre att vara tillgängliga på slutanvändarens enhet. Det privata området påverkas inte och fortsätter att finnas kvar på slutanvändarens enhet.

## TeamViewer Fjärrkontroll




Här kan du starta en TeamViewer-fjärrkontrollsession för den här enheten.

## Skicka inskrivningsbegäran

Med "Send Enrollment Request" kan du skicka en registreringsbegäran (igen) till respektive användare.

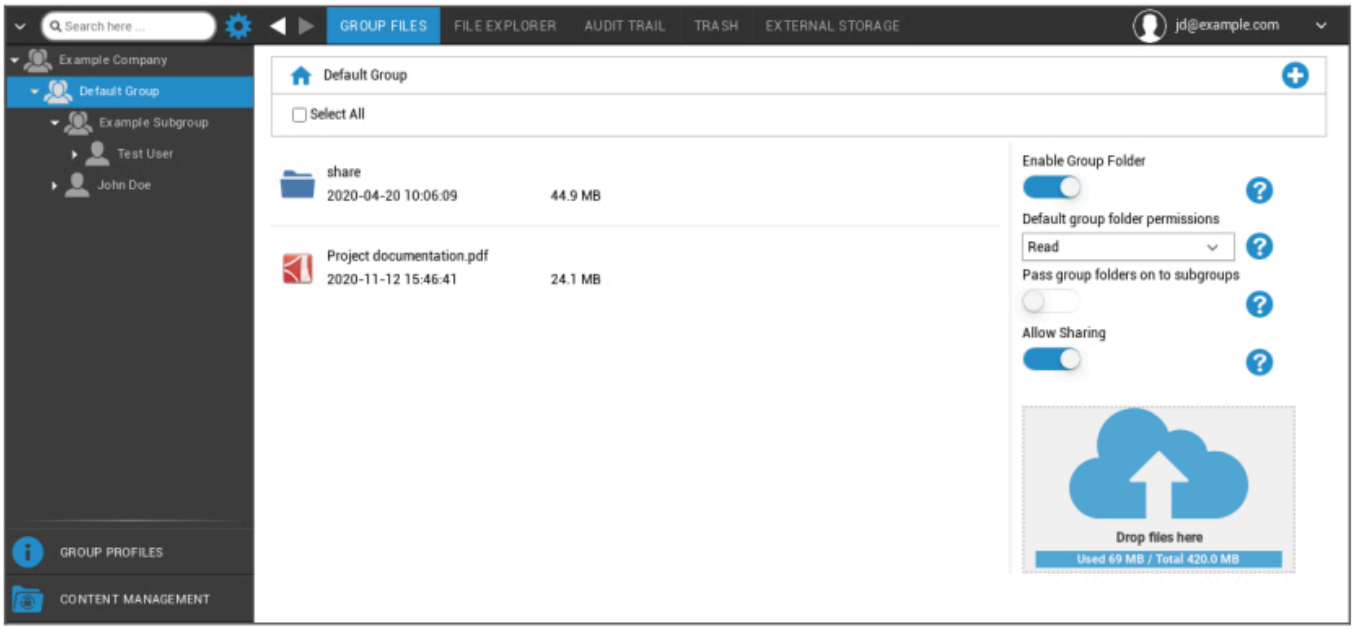
# Innehållshantering

När du är med i en grupp kan du hantera AppTecs ContentBox med "Content Management".

Med Content Box kan du på ett säkert sätt distribuera dokument och annan företagsdata till slutanvändarnas enheter.

## Gruppfiler

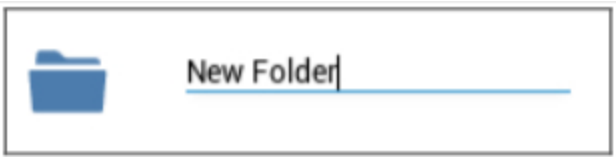
"Group Files" är en grundläggande del av ContentBox. Här kan du göra inställningar, ladda upp dokument, skapa nya mappar etc.




Med symbolen i det övre högra hörnet kan du skapa nya mappar som tilldelas respektive grupp med "Add Folder".

Med symbolen i det övre högra hörnet kan du skapa en ny mapp via "Add Folder", som ska tilldelas respektive grupp.

Du kan döpa mappen till vad du vill.



Via "Upload Files" kan du ladda upp data. Här kommer din Standard-Explorer att öppnas. Du kan naturligtvis utföra dessa två åtgärder i varje (under)mapp.

Med symbolen i det övre vänstra hörnet kan du återgå till huvudmenyn.

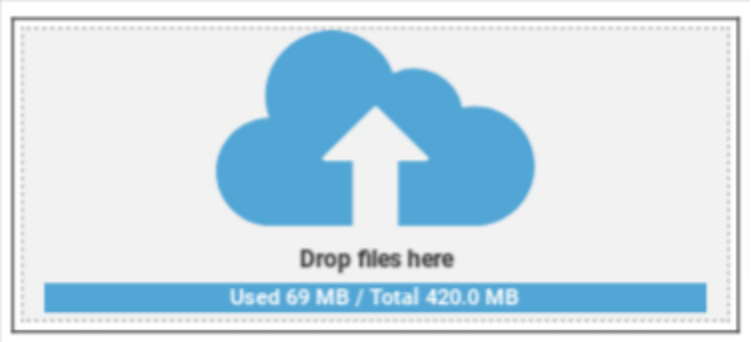
Du kan välja flera mappar och filer och ladda ner dem med "Download" eller radera dem genom att klicka på "Delete".

Du kan också markera alla filer och mappar med och utföra kommandona "Download" och "Delete".

När du för muspekaren över en mapp eller fil visas följande översikt:


- Med "Rename" kan du byta namn på mappen/filen
- Med "Download" kan du ladda ner mappen/filen
- Med "Delete" kan du radera mappen/filen

| | |
|---|---|
| Aktivera gruppmapp | Om den är aktiverad har alla medlemmar i gruppen tillgång till respektive mapp |
| Standardbehörigheter för gruppmappar | Behörigheter för användarna i den valda gruppen:<br>Read = endast läsrättigheter<br>Update = uppdatera behörighet<br>Create = behörighet att skapa<br>Delete = ta bort behörighet |
| Skicka gruppmappar vidare till undergrupper | Om den är aktiverad kan respektive undergrupp få tillgång till de överordnade datafilerna |
| Behörigheter för undergrupper | Behörigheter för användarna i den valda undergruppen:<br>Read = endast läsrättigheter<br>Update = uppdatera behörighet<br>Create = behörighet att skapa<br>Delete = ta bort behörighet |
| Tillåt delning | Om den är aktiverad kan användaren dela filer via en länk |



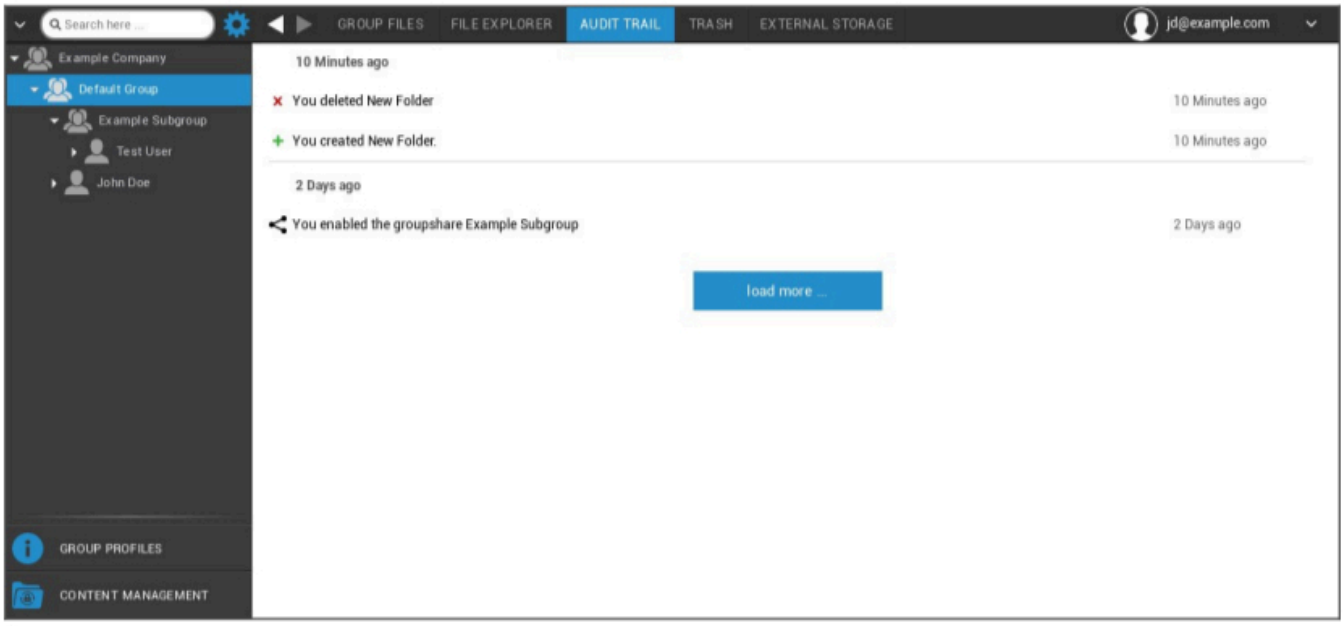

För att ladda upp filer kan du använda det här fältet genom att dra en fil via Drag & Drop till det här fönstret. Du kan också klicka på det här fältet för att välja och ladda upp en fil med hjälp av Internet Explorer.

## Filutforskaren


Med "File Explorer" kan du hantera alla mappar och filer - oavsett i vilken grupp de är arkiverade.

Du hittar också de inställningar och knappar som du lärde dig om i "Group Files".

## Revisionsspår




I "Audit Trail" kan du i historiken se vilken användare som har skapat, raderat eller delat vad. På så sätt kan du när som helst fastställa vad som har gjorts med företagets data.

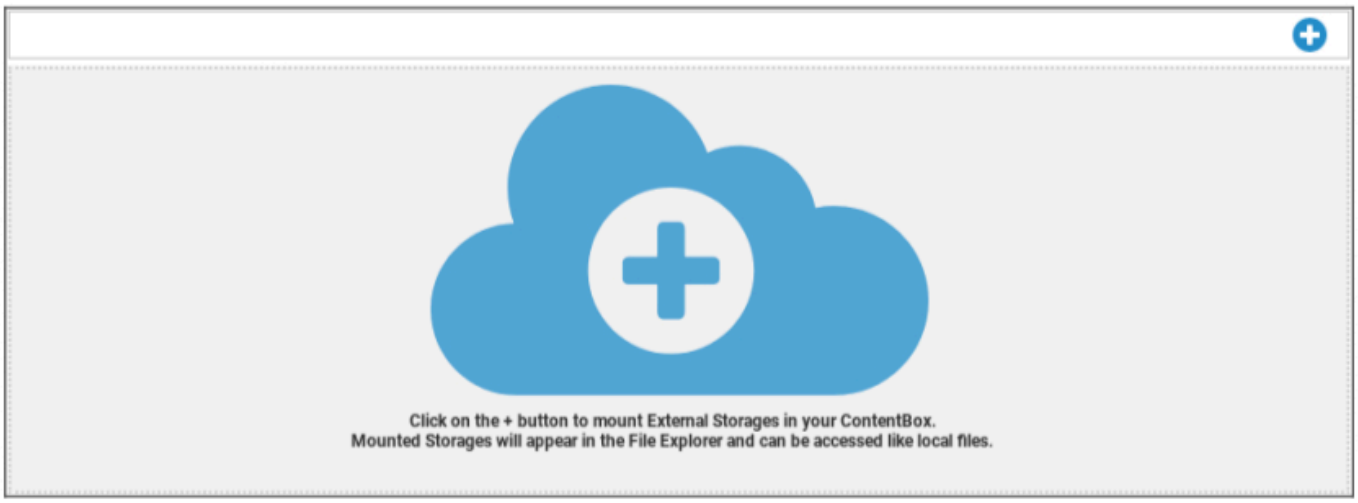
## Skräp

Om du har raderat något (av misstag) kan du se mapparna och filerna under "Papperskorgen" och återställa dem enligt dina önskemål.

- Med "Undelete" kan du återställa data / mapp.
- Med "Delete" kan du radera data/mappen permanent - du måste då bekräfta kommandot dele en gång till.


Observera att den lagringskapacitet som används i papperskorgen minskar det "totala utrymmet" som är tillgängligt - detta är ett krav från ownCloud.

# Extern lagring




Under rubriken "Extern lagring" kan du ansluta extern lagring.

Med symbolen kan (ytterligare) förvaring läggas till.

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

| **Amazon S3** | |
|---|---|
| Visa namn | Visa namn |
| Åtkomstnyckel | Åtkomstnyckel |
| Hemlig nyckel | Säkerhetsnyckel |
| Skopa | Definitiv identitet för den undermapp som har tilldelats dig |
| Värdnamn (valfritt) | Värdnamn (valfritt) |
| Port (tillval) | Port (tillval) |
| Region | Region (valfritt) |
| Aktivera SSL | Aktivera SSL |
| Aktivera Path Style | Clear Path Adress som har tilldelats dig |

| FTP | |
|---|---|
| Visa namn | Visa namn |
| Värd | Värdadress |
| Användarnamn | Användarnamn |
| Lösenord | Lösenord |
| Rot | Huvudmeny |
| Säker ftps:// | |

| SFTP | |
|---|---|
| Visa namn | Visa namn |
| Värd | Värdadress |
| Användarnamn | Användarens namn |
| Lösenord | Lösenord |
| Rot | Huvudmeny |

| ownCloud | |
|---|---|
| Visa namn | Visa namn |
| URL | ownCloud URL |
| Användarnamn | Användarnamn |
| Lösenord | Lösenord |
| Fjärrstyrd undermapp | Standardmapp |
| Säker https:// | |

| WebDAV | |
|---|---|
| Visa namn | Visa namn |
| URL | WebDAV-URL |
| Användarnamn | Användarens namn |
| Lösenord | Lösenord |
| Rot | Huvudmeny |
| Säker https:// | |
| Windows Share | Stöd för Windows Share kommer att finnas tillgängligt inom kort |
| SharePoint | Stöd för Microsoft SharePoint kommer att finnas tillgängligt inom kort |

# Revisionslogg

Här hittar du en logg som registrerar information om åtgärder som utförs i MDM-konsolen.

Med filterikonen kan du tillämpa filter på den lista som visas.

Med rullgardinsmenyn **Objekt per sida**: kan du välja hur många objekt som ska visas på en sida i listan.

| | |
|---|---|
| Åtgärd vidtagen / inställning ändrad | Den åtgärd som vidtogs / Den inställning som ändrades |
| Värde | Värdet av den vidtagna åtgärden/ändrade inställningen |
| Användare | Namnet på den användare som har vidtagit åtgärden/ändrat inställningen |
| Datum | Tidsstämpel för när denna åtgärd vidtogs/den här inställningen ändrades |
| Sökväg / Typ | Sökvägen till där denna åtgärd vidtogs/den här inställningen ändrades |

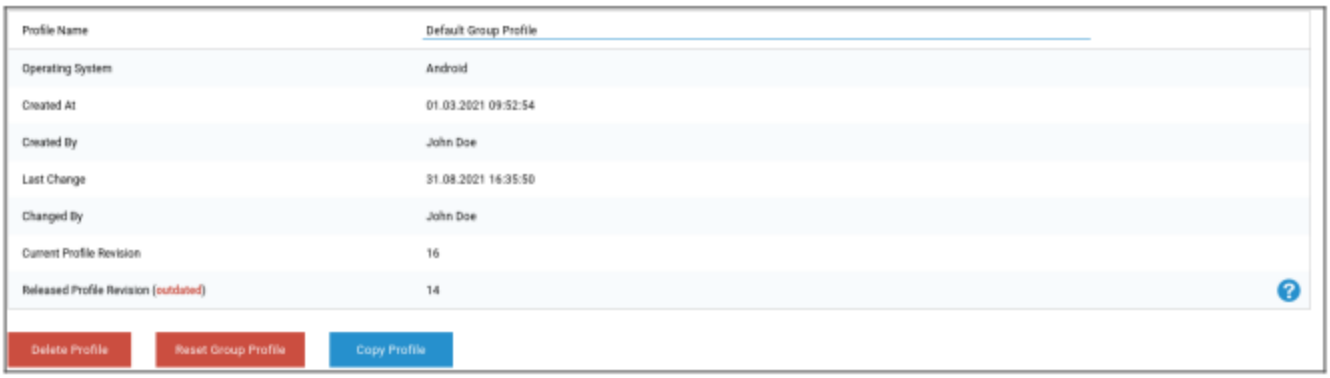
# iOS-konfiguration

## Allmänt

Beroende på om du för tillfället har valt en grupp eller en enhet är displayen och dess underpunkter olika - var uppmärksam på detta!

### Översikt över grupprofiler (endast på gruppnivå)

När du öppnar en grupprofil får du en snabb överblick över profilen




| | |
|---|---|
| Profilens namn | Profilens namn (kan ändras här) |
| Operativsystem | Operativsystem som profilen är avsedd för |
| Skapad vid | Tidpunkt för skapelse |
| Skapad av | Skaparen av profilen |
| Sista förändringen | Tidpunkt för senaste ändring av profilen |
| Förändrad av | Konto som gjorde de senaste ändringarna |
| Aktuell profil Revidering | Revidering av sparat profiltillstånd |
| Utgiven Profil Revision | Tilldelad profilrevision ("Tilldela nu"). Om etiketten visar "(outdated)" bakom texten betyder det att du har sparat profilen men inte tilldelat den ännu, så enheterna kommer fortfarande att få en äldre version. |

## Allmän information

Om du befinner dig direkt på enheten får du en kort översikt över den valda enheten.

| | |
|---|---|
| Enhetens namn | Enhetens namn |
| Telefonnummer | Enhetens telefonnummer |
| Modell | Modellnummer |
| Operativsystem | OS |
| Serienummer | Enhetens serienummer |
| Ägande av enhet | Företags- eller privat enhet<br>Företag = företagsenhet<br>Anställd = privat enhet |
| Enhetstyp | Typ av enhet (surfplatta eller telefon) |
| Jailbreakad | Om det finns en Jailbreak på enheten |
| Övervakad | Anger om detta är en övervakad enhet |
| Överensstämmande | Om några riktlinjer har överträtts |
| Senast sett | Status för när enheten senast kommunicerade med AppTec360 Server |

## Inställningar

Dessa inställningar innehåller enhetens namn och en fördefinierad bakgrund.

| | |
|---|---|
| Namnge enheten till systemnamn | Namnet som kommer att utfärdas i AppTec360 Console (i vänster hierarkistruktur), kommer att vara detsamma som på respektive slutanvändares enhet (kan ses i enhetens inställningar) |
| Använda anpassad bakgrundsbild (endast övervakade enheter) | Här kan du fördefiniera den bakgrund som ska visas på slutanvändarens enhet (t.ex. för en typ av företagsprofilering för enheten)<br>Är endast tillgänglig i Supervised Mode! |
| Automatiska OS-uppdateringar | Forcerar OS-uppdateringar om sådana finns tillgängliga. Endast för DEP-enheter i övervakat läge. |
| Anpassade teckensnitt | Här kan du lägga till egna teckensnitt. |
| Namn | Valfritt namn. Det användarvänliga namnet för teckensnittet. Detta fält ersätts av det faktiska namnet på teckensnittet efter installationen. |
| Typsnitt | Ladda upp filen med teckensnittet (.otf eller .ttf). |

## Konfig Revision

Här får du en översikt över vilken grupprofil som är kopplad till enheten.


Om du klickar på grupprofilen kommer du direkt till profilen och kan göra inställningar.

Med symbolen kan du återställa de tilldelade apparna till grupprofilens inställningar.

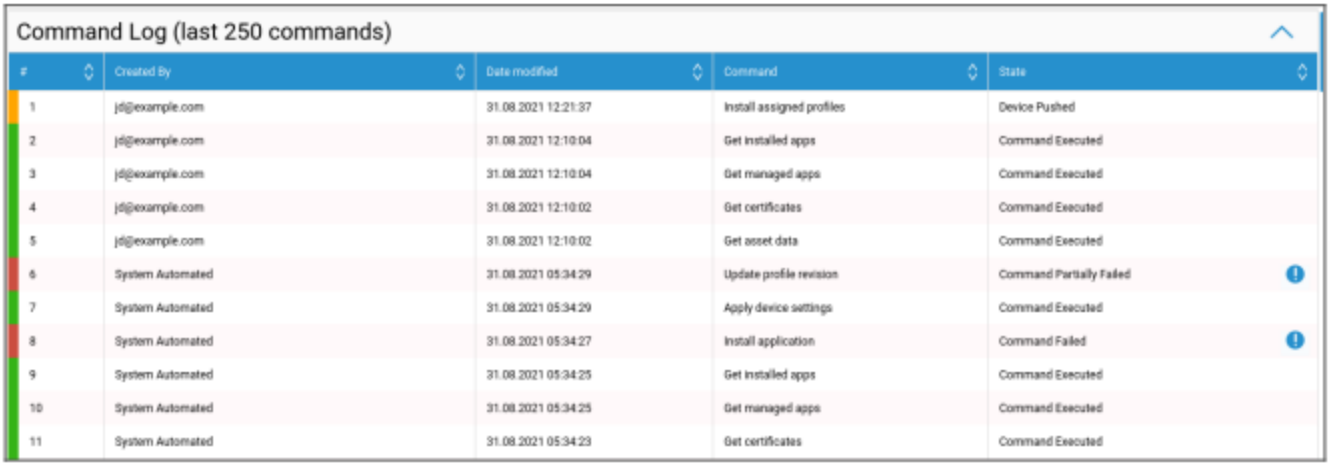
Med symbolen kan du återställa enhetens profil så att den inte har några inställningar alls.

"Nyare revision tillgänglig" anger att grupprofilen har ändrats och sparats men inte tilldelats.
Grupprofilen måste tilldelas med "Tilldela nu" på gruppnivå för att ändringarna ska gälla för enheterna.

## Enhetslogg (endast på enhetsnivå)

### Kommandologg

Här kan du se vilka kommandon som har utfärdats för enheten och vilken status de har.




Kommandon som skapats av "System Automated" skapas automatiskt av systemet.

## Möjliga kommandostatusar

| | |
|---|---|
| Enhet tryckt | En push-begäran har skickats till push-tjänsten (t.ex. APNS) för att tala om för enheten att den ska ansluta tillbaka till EMM-servern. |
| Kommando Skapat | Kommandot skapades i systemet. |
| Kommando skickat | Kommandot skickades till enheten efter att den anslutit till servern. |
| Kommando utfört | Kommandot har utförts framgångsrikt. |
| Kommandot misslyckades | Kommandot misslyckades. * |
| Kommandot delvis misslyckat | Beroende på enhetens operativsystem kan vissa kommandon grupperas tillsammans.<br>I detta misslyckades vissa delar av denna kommandogrupp. * |
| Kommando utfört, eventuellt misslyckat | Kommandot utfördes, men kanske inte. |
| Kommando Repushed | Kommandot återställdes av en användare. |
| Bortkastad | Kommandot kasserades. Till exempel för att det ersattes av ett annat kommando eller för att enheten registrerades på nytt och gamla kommandon togs bort |

Om det finns ett utropstecken bakom meddelandet kan du få mer information genom att hålla muspekaren över ikonen.

# Tillgångshantering (endast på enhetsnivå)

## Tillgångshantering (endast på enhetsnivå)

### Info om enhet

| | |
|---|---|
| Modell | Enhetens modellnummer |
| Operativsystem | OS |
| OS-version | OS-version |
| Serienummer | Serienummer |
| UDID | Enhet UDID |
| Enhetens namn | Enhetens namn |
| Övervakad | Visar om enheten är övervakad |
| Batteristatus | Batteriets status |

### Wi-Fi

| | |
|---|---|
| IP-adress | Enhetens IP-adress |
| WiFi MAC | WiFi MAC-adress |

## Cellulär

| | |
|---|---|
| Status | Status (SIM-kort finns) |
| Telefonnummer | Telefonnummer |
| Status för roaming | Aktuell roamingstatus |
| Roaming (röst/data) | Roamingstatus för röst/data |
| IP-adress | IP-adress |
| IMEI | IMEI-nummer |
| Operatör/transportör | Leverantör av mobiltjänster |
| SIM-operatör Nätverk | SIM-operatörens nätverk |
| Version för bärare | Version för bärare |
| Modem Firmware | Modemets firmware |
| Nuvarande MCC/MNC | Se "SIM MCC/MNC" |
| SIM MCC/MNC | Mobile Country Code är en etablerad landidentifiering av ITU enligt E.212-standarden, som tillsammans med Mobile Network Code (MNC) används för att identifiera ett cellulärt nätverk (= landskod)<br>När du går in i ett annat mobilnät är därför "Current MCC/MNC" och "SIM MCC/MNC" olika. |

## Bluetooth

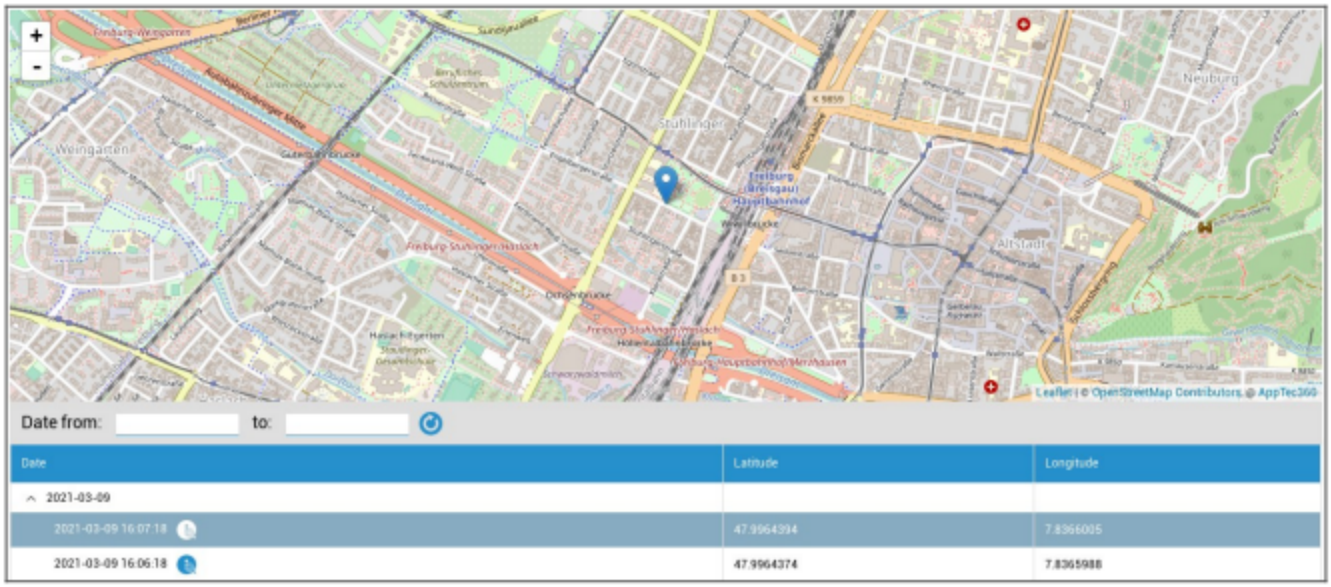
| | |
|---|---|
| Bluetooth MAC | Bluetooth MAC-adress |

# Säkerhetshantering

## Stöldskydd (endast på enhetsnivå)

### GPS-information (endast på enhetsnivå)

Här kan du bedöma enhetens aktuella/senaste plats. Lokaliseringen kan antingen skyddas med ett eller till och med två lösenord - se: Allmänna inställningar - Sekretess - GPS-åtkomst



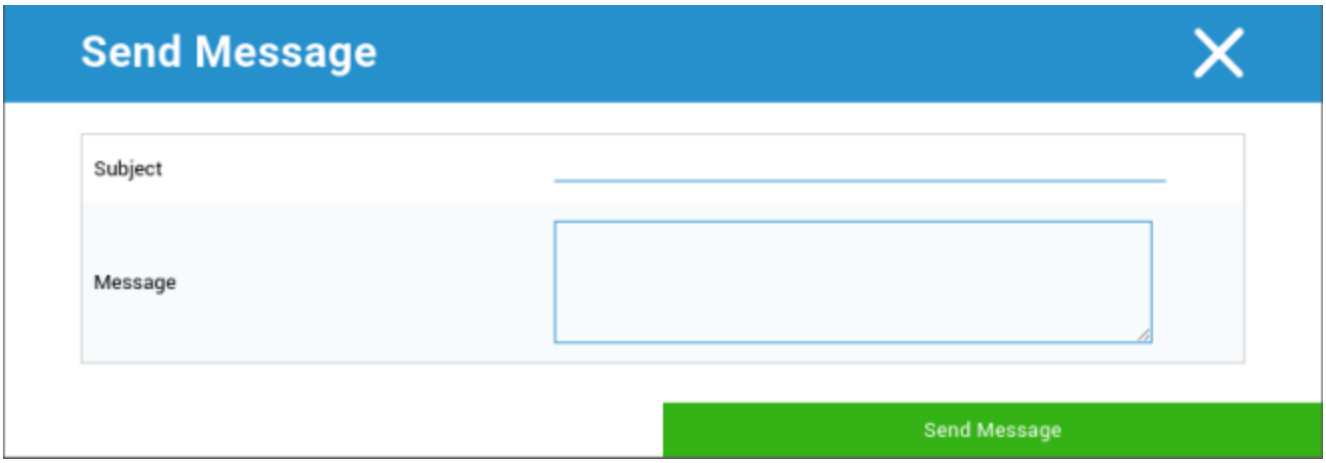

### Wipe & Lock (endast på enhetsnivå)

Under "Wipe & Lock" kan du utföra följande tre åtgärder:

| | |
|---|---|
| Fullständig avtorkning | Enheten återställs till fabriksinställningarna (både företagsdata och personuppgifter raderas) |
| Enterprise Wipe | Endast företagsdata tas bort från slutanvändarens enhet (alla appar, data etc. som tillhandahölls av AppTec) |
| Lås skärm | Om skärmlåset är aktiverat räcker det med att låsa upp enheten med enhetens lösenord/PIN |
| Forensisk nedstängning (endast övervakade enheter) | Om denna funktion aktiveras med symbolen  låses enheten genom att ett meddelande visas som inte kan stängas. Medarbetaren kan inte heller låsa upp enheten.<br>Endast administratören kan låsa upp enheten i konsolen med symbolen för upplåsning  . |
| Tillåt aktiveringslås (endast övervakade enheter) | Om denna funktion är aktiverad låses enheten så snart "Hitta min iPhone" är aktiverad i iCloud-inställningarna |

## Meddelande (endast på enhetsnivå)

I följande fönster kan du fylla i ämnet och ett meddelande och skicka det till en slutanvändares enhet:



# Säkerhetskonfiguration

## Lösenord

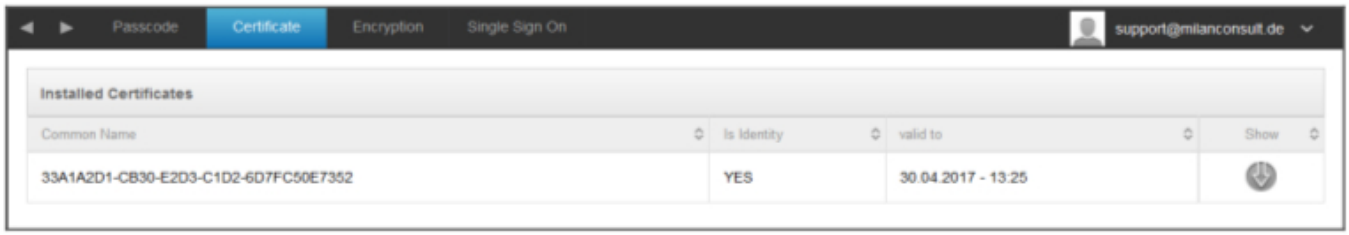
Här gör du inställningarna för enhetens lösenord

| | |
|---|---|
| Avaktivering av kod tillåten | När den här inställningen är aktiverad uppmanas du inte att ange ett lösenord<br>Så snart ett lösenord har skapats kan det inte avaktiveras |
| Tillåt enkelt värde | Tillåt användaren att använda samma, eskalerande och reducerande nummersträngar (t.ex. 1234, 1111) |
| Kräver alfanumeriskt värde | Lösenord måste innehålla minst en bokstav |
| Minsta längd på lösenkod | Minsta lösenordslängd |
| Minsta antal komplexa tecken | Minsta antal alfanumeriska symboler i lösenordet |
| Maximal ålder för lösenkod | Antal dagar efter vilka lösenordet måste ändras |
| Maximal automatisk låsning | Maximal tid efter vilken enheten är låst |
| Maximal frist för låsning av enhet | tid, varefter enheten går in i låst Stand-by-läge |
| Maximalt antal misslyckade försök | Fastställer hur ofta ett lösenord kan anges felaktigt innan en fullständig radering av enheten utförs |
| Maximal ålder på lösenordet (1-730 dagar) | Maximal lösenordsålder |
| Lösenordshistorik (1-50 lösenord) | Efter detta nummer är det tillåtet att använda ett gammalt lösenord |

Ett klick på papperskorgen öppnar dialogen Password-Reset, med vilken ett bortglömt lösenord för enheten kan raderas.

## Certifikat (endast på enhetsnivå)

Visar de certifikat som finns tillgängliga på enheten


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

## Kryptering

| | |
|---|---|
| Kräv kryptering av lagringsutrymme | Aktivera den installerade enhetens krypteringsfunktion |

## Enkel inloggning

Under punkten "Single Sign-On" kan du konfigurera Kerberos-autentiseringen.

Här fastställer du inloggningsuppgifterna och de respektive URL:er/appar som får använda Kerberos-tokens.

| **Tillgänglig i övervakat läge** | |
|---|---|
| Kontots namn | Kontots namn |
| Huvudmannens namn | Unik identitet till vilken Kerberos-biljetter kan distribueras |
| Realm | Din Kerberos Realm, som ska användas (t.ex. din domän) |

Med symbolen kan du skapa ytterligare webbadresser.

| | |
|---|---|
| URL-mönster som används för att begränsa detta konto | URL:er som ska fastställas, till vilka Kerberos-biljetter kan distribueras |

Med symbolen kan du skapa ytterligare appar.

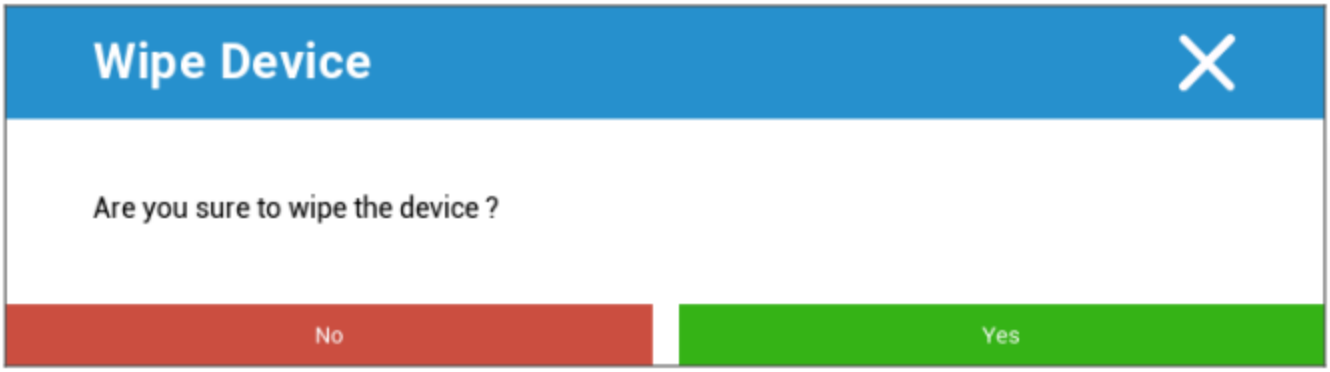
| | |
|---|---|
| Appar för att begränsa detta konto | Ska bestämmas Appar, till vilka Kerberos-biljetter kan distribueras |

# End of Life (endast på enhetsnivå)

## Torka (endast på enhetsnivå)

Under "Wipe" kan du återställa enheten till fabriksinställningarna. Här kommer företagsdata och privata data att raderas på slutanvändarens enhet.

Genom att klicka på "Minus-symbolen" får du följande meddelande




Med "Yes" kan du utföra torkningen.

Under "Wipe Report" kan följande objekt visas

| | |
|---|---|
| Raderad av | Historik över vem som utförde torkningen |
| Datum | Datum |
| Status | Status (t.ex. om rensningen utfördes framgångsrikt) |

# Inställningar för begränsning

## Enhetens funktionalitet

Här kan du blockera enskilda funktioner för slutanvändarens enhet

| | |
|---|---|
| Tillåt installation av appar | Tillåt installation av appar |
| Tillåt kamera | Tillåt användning av kameran |
| Tillåt FaceTime | Tillåt FaceTime |
| Tillåt skärmdump | Tillåt skärmdump |
| Tillåt automatisk synkronisering vid roaming | Tillåt automatisk synkronisering vid roaming |
| Tillåt Siri | Tillåt Siri |
| Tillåt röstuppringning | Tillåt röstuppringning |
| Tillåt köp i appen | Tillåt köp i appen |
| Kräver iTunes Store-lösenord för alla köp | Kräver iTunes Store-lösenord för alla köp |
| Tillåt multiplayer-spel | Tillåt multiplayer-spel |
| Tillåt att lägga till Game Center-vänner | Tillåt att lägga till Game Center-vänner |
| Tillåt öppning från förvaltad till oförvaltad | Tillåt öppning av innehåll i hanterade appar i ohanterade appar |
| Tillåt öppning från okontrollerat till kontrollerat | Tillåt öppning av innehåll i ohanterade appar i hanterade appar |
| Tillåt dagens vy i låsskärmen | När den här inställningen är aktiv visas vyn "Idag" i Notification Center på låsskärmen |
| Tillåt kontrollcenter i låsskärmen | Tillåt Control Center på låsskärmen |
| Tillåt TouchID | Tillåt TouchID |
| Tillåt uppdateringar av PKI under drift | Tillåt uppdateringar av PKI under drift |
| Tillåt passbook när du är låst | Tillåt passbook när enheten är låst |
| Begränsa spårning av annonser | Denna funktion avaktiverar annonsspårning (t.ex. annonsörer kan inte använda annonsspårning för att distribuera personliga annonser) |

| | |
|---|---|
| Tillåt överlämning | Tillåt överlämning |
| Låt internetresultat stå i rampljuset | Tillåt internetresultat i spotlight (t.ex. Bing eller Wikipedia) |
| Kräv lösenkod vid första AirPlay-parningen | Kräv lösenkod vid första AirPlay-parningen |
| Force Watch Handledsskydd | Om den är aktiverad tvingas Apple Watch att använda "Wrist Protection" (handledsigenkänning) |
| Tillåt iCloud Photo Library | Tillåter iCloud Photo Library. Om det inte tillåts kommer alla bilder som inte laddats ner helt från iCloud att raderas på det lokala lagringsutrymmet. |
| | **Tillgänglig i Supervised-mode** |
| Tillåt ändring av konto | Tillåt ändring av "e-post, kontakter, kalender" |
| Tillåt AirDrop | Tillåt AirDrop |
| Tillåt App Cellular Modification | Denna inställning blockerar inställningen för vilka appar som tillåts använda mobildata<br>Denna inställning kan t.ex. ställas in manuellt på slutanvändarens enhet och sedan kan denna begränsning aktiveras |
| Tillåt Siri att fråga efter användargenererat innehåll från webben | Webbsökning på vissa webbplatser är blockerad, t.ex. Wikipedia, eftersom alla kan göra ändringar som de vill |
| Aktivera Siri-filter för svordomar | Svordomar som riktas mot Siri censureras |
| Tillåt iBook Store | Tillåt iBook Store |
| Tillåt iBook Store Erotica | Tillåt iBook Store Erotica |
| Tillåt ändring av inställningarna för Hitta mina vänner | Tillåt ändring av inställningarna för Hitta mina vänner |
| Tillåt Game Center | Tillåt Game Center |
| Tillåt parning av värdar | Kontroll av datorparning |
| Tillåt installation av konfigurationsprofiler | Tillåt installation av konfigurationsprofiler |
| Tillåt Ta bort app | Borttagning av kontrollappar |
| Tillåt iMessage | Tillåt iMessage |
| Tillåt radering av allt innehåll och alla inställningar | Tillåt radering av allt innehåll och alla inställningar |

| | |
|---|---|
| Tillåt konfigurering av begränsningar | Tillåt konfigurering av begränsningar |
| Tillåt podcast | Tillåt podcast |
| Tillåt uppslagning av definitioner | Tillåt uppslagning av definition |
| Tillåt prediktivt tangentbord | Tillåt prediktivt tangentbord |
| Tillåt automatisk korrigering | Tillåt automatisk korrigering |
| Tillåt installation av UI-app | Om den är avaktiverad kan inga appar installeras från den offentliga AppStore (ikonen visas inte längre). Appar kan dock fortfarande installeras via iTunes och Configurator |
| Tillåt kortkommandon på tangentbordet | Tillåt kortkommandon om enheten är ansluten till ett fysiskt tangentbord |
| Tillåt parkoppling av Apple Watch | Förhindrar parkoppling mellan enheten och Apple Watch, befintliga anslutningar kommer att avbrytas |
| Tillåt ändring av lösenord | Om detta inte tillåts kan inget enhetslösenord läggas till, ändras eller tas bort |
| Tillåt ändring av devicenamn | Riktlinje för att avgöra om enhetsnamnet kan ändras |
| Tillåt ändring av bakgrundsbild | Riktlinjer för att avgöra om tapeten kan ändras |
| Tillåt automatiska appnedladdningar | Om den avaktiveras kommer en köpt app inte att installeras automatiskt på andra enheter. Gäller inte uppdateringar för befintliga appar |
| Tillåt nyheter | Tillåt nyheter på iOS-enheten |
| Tillåt förtroende för Enterprise-app | Om inställningen är false förhindras förtroende för företagsappar |

## iCloud

Blockera vissa funktioner under iCloud-parning

| | |
|---|---|
| Tillåt säkerhetskopiering | Tillåt säkerhetskopiering |
| Tillåt synkronisering av dokument | Tillåt synkronisering av dokument |
| Tillåt bildström | Tillåt bildström |
| Tillåt delad fotoström | Tillåt delad fotoström |
| Tillåt synkronisering av nyckelring i molnet | Tillåt synkronisering av nyckelring i molnet |
| Tillåt hanterade appar att lagra data | Tillåt hanterade appar att lagra data |
| Tillåt synkronisering av anteckningar och höjdpunkter för företagsböcker | Tillåt synkronisering av anteckningar och höjdpunkter för företagsböcker |
| Tillåt säkerhetskopiering av företagets böcker | Tillåt säkerhetskopiering av företagets böcker |

## Säkerhet och integritet

Blockera dessa funktioner som är kopplade till diagnostiska data

| | |
|---|---|
| Tillåt att diagnosdata skickas till Apple | Tillåt att diagnosdata skickas till Apple |
| Tillåt användaren att acceptera TLS-certifikat som inte är betrodda | Tillåt användare att acceptera TLS-certifikat som inte är betrodda |
| Tvinga fram krypterade säkerhetskopior | Tvinga fram krypterade säkerhetskopior |

# BYOD

## Inbyggd iOS-säkerhet (behållare)

iOS har alltid kunnat göra skillnad mellan managed (företag) och unmanaged (privat). Allt som kommer från MDM-systemet behandlas som hanterat. Om du t.ex. installerar en app via MDM eller konfigurerar ett Exchange-konto behandlas detta som hanterat av iOS.

Allt annat som konfigureras/installeras manuellt på enheten kommer att behandlas som icke-hanterat. Till exempel om användaren installerar WhatsApp på egen hand eller om han eller hon lägger till ett Exchange-konto. Denna separation påverkade dock aldrig kontakterna. Men sedan iOS 11.3 (och högre) har detta också lagts till för kontakterna.

Eftersom detta är en grundläggande funktion i operativsystemet behöver du inte installera något eller ställa in en särskild behållare.

Aktivera den inbyggda funktionen för att separera privata och affärsmässiga appar/information/filer. Denna inställning inaktiverar även vissa andra funktioner som annars kan stänga av delar av denna åtskillnad av misstag.

### Aktivering

Aktivera de Container-lösningar som stöds av AppTec360

| | |
|---|---|
| Aktivera Google Divide Container | Aktivera Google Divide Container |
| Aktivera SecurePIM Container | Aktivera SecurePIM Container |

Om du har aktiverat SecurePIM Container hittar du även följande punkt under "Aktivering". Dessutom öppnas genast ytterligare fyra flikar, som beskrivs nedan.

| | |
|---|---|
| E-postadress för support | E-postadress för support dit en användare kan vända sig med problem |

## SecurePIM Lösenord

Under "SecurePIM Password" kan du ange riktlinjer för lösenordets säkerhetsstyrka.

| | |
|---|---|
| Timeout för session | Här kan du bestämma efter hur många minuter ett nytt lösenord måste anges igen, när SecurePIM körs i bakgrunden |
| Lösenordslängd | Lösenordslängd för åtkomst till SecurePIM Container |
| Versala tecken | Minsta tecken i versaler |
| Tecken för gemener | Minsta antal gemena tecken |
| Specialtecken | Minsta antal specialtecken |
| Siffror | Minsta antal siffror |
| Torka av applikationen | Antal gånger som ett lösenord kan anges felaktigt innan SecurePIM-innehållet raderas<br>(Appen finns dock fortfarande kvar på slutanvändarens enhet) |

## SecurePIM Säkerhet

Under "SecurePIM Security" kan du göra en rad olika säkerhetsinställningar.

| | |
|---|---|
| Upptäck jailbreakade enheter | Om denna inställning är aktiverad kommer åtkomsten till SecurePIM Container att blockeras så snart enheten upptäcks som jailbreakad |
| Säkra textfält | Innehållet i inmatningsfälten kommer att krypteras, ingen information når operativsystemet (iOS)<br>Obs: Så länge denna inställning är aktiv är automatisk korrigering inte längre tillgänglig |
| Exportera kontaktdata till enhet | Om den här inställningen är aktiverad får användaren exportera Exchange-kontakterna till sin lokala enhet<br>Obs: Endast namnet och telefonnumret exporteras |
| Visa evenemangets plats | Om denna inställning är aktiverad visas platsen för de kommande evenemangen i meddelandefältet |
| Visa händelsens titel | Om denna inställning är aktiverad visas platsen för det kommande evenemangets titel i meddelandefältet |

## SecurePIM webbläsare


Här kan du konfigurera webbläsaren för SecurePIM.

Med hjälp av symbolen kan du definiera en ny URL.

Med hjälp av symbolen kan du ta bort en definierad URL igen.

"Vitlistade webbadresser" är webbadresser som kan laddas.

"Svartlistade URL:er" är URL:er som inte kan laddas och som därmed blockeras.

Observera att posterna på vitlistan har högre prioritet än posterna på svartlistan. Under "Bookmark Title" kan du ange en titel. Med "Bookmark URL" kan du associera URL-adressen med bokmärkets titel - på så sätt kan du distribuera individualiserade bokmärken till respektive användare.

## Utbyte

Under "Exchange" kan du konfigurera ett Exchange-konto.

| | |
|---|---|
| E-postadress för ActiveSync | Exchange-e-postadress (notera "platshållarna") |
| ActiveSync Exchange-inloggning | Exchange-användarnamn (notera "platshållarna") |
| ActiveSync Exchange Server | Exchange Server-adress (FQDN) |
| ActiveSync Exchange-domän | Exchange Domänadress |
| Användarcertifikat | Användarcertifikat |
| Certifikatbaserad autentisering | Användaren autentiserar sig med ett certifikat |
| Tillåt S/MIME-kryptering | Gör det möjligt för användaren att kryptera sin e-post |
| Tillåt S/MIME-signering | Gör det möjligt för användaren att signera sin e-post |
| CRL-kontroll | Om det är aktivt kommer det privata certifikatet att jämföras med CRL (Certificate Revocation List) |

# Hantering av anslutningar

## Wi-Fi

| | |
|---|---|
| Identifierare för tjänsteuppsättning (SSID) | SSID för det nätverk som ska anslutas |
| Automatisk anslutning | Aktivera automatisk anslutning när du ansluter till ett nätverk |
| Dolda nätverk | Aktivera, om AP:n inte sänder SSID |

## Proxy-inställning

Konfigurering av en proxy för varje accesspunkt

| | | |
|---|---|---|
| Ingen | | Upprätta ingen Proxy |
| Manuell | | Upprätta en manuell fullmakt |
| | URL för proxyserver | Adress för åtkomst till Proxy-inställningar |
| | Port | Fastställ porten för proxyservicen |
| | Autentisering | Användarnamn för autentisering på Proxy |
| | Lösenord | Lösenord för autentisering på proxyserver |
| Automatisk | | Upprätta en proxy automatiskt |
| URL för proxyserver | | URL för åtkomst till Proxy-inställningarna |

## Typ av säkerhet

Upprätta säkerhetstyp för AP:n

| WEP | |
|---|---|
| Lösenord | Lösenord för AP:n |

| WPA/WPA2 | |
|---|---|
| Lösenord | Lösenord för AP:n |

| | | | |
|---|---|---|---|
| WEP Enterprise - WPA / WPA2 Enterprise - Any Enterprise | | | |
| | Protokoll | | |
| | TLS | Aktivera/avaktivera | |
| | TTLS | Aktivera/avaktivera | |
| | LEAP | Aktivera/avaktivera | |
| | PEAP | Aktivera/avaktivera | |
| | EAP-FAST | Aktivera/avaktivera | |
| | EAP-SIM | Aktivera/avaktivera | |
| | Använd PAC | | Användning av PAC (Protected Access Controll) |
| | Tillhandahållande PAC | Konfiguration av Provision PAC | |
| | Tillhandahålla PAC anonymt | Anonymt tillhandahållande av PAC | |
| | Inre autentiseringar | Autentiseringsprotokoll som ska användas:<br>PAP, CHAP, MSCHAP, MSCHAPv2 | |
| | Användarnamn | Användarnamn för autentisering | |
| | Använd inte Per-Connection Password | Använd inte Per-Connection Password | |
| | Identitetscertifikat | Ladda upp/välja autentiseringscertifikat | |
| | Yttre identitet | Identitet som kan ses externt | |
| | Förtroende | | |
| | Betrott certifikat 1 | Ladda upp det första betrodda certifikatet | |
| | Betrott certifikat 2 | Ladda upp det andra betrodda certifikatet | |
| | Betrott certifikat 3 | Ladda upp ett tredje betrott certifikat | |
| | Namn på certifikat för betrodda servrar | Namnen på de förväntade servercertifikaten<br>(i en kommaseparerad lista) | |

| | |
|---|---|
| Ingen | Upprätta ingen säkerhet |

## VPN

| | |
|---|---|
| Namn på anslutning | Namn på VPN-profilen |

### VPN-typ

#### VPN

All nätverkstrafik för enheten kommer att dirigeras via en VPN-anslutning.

| Typ av anslutning | | Upprätta typ av VPN-anslutning |
|---|---|---|
| | IPsec (Cisco) | IPsec-protokoll från Cisco |
| | PPTP | PPTP-protokoll |
| | L2TP | L2TP-protokoll |
| | Cisco AnyConnect | AnyConnect-protokoll |
| | Juniper SSL | Juniper SSL-protokoll |
| | F5 SSL | F5 SSL-protokoll |
| | SonicWall mConnect | SonicWall mobil anslutning |
| | Aruba VIA | Aruba VIA-protokoll |
| | Anpassad SSL | Anslutning via anpassad SSL |
| | OpenVPN | OpenVPN-protokoll |

#### VPN per app

När du öppnar en viss app kommer en VPN-anslutning att upprättas

| | | |
|---|---|---|
| Starta automatiskt VPN-anslutning per app | | Starta automatiskt VPN-anslutning per app |
| Typ av anslutning | | Upprätta typ av VPN-anslutning |
| | Cisco AnyConnect | AnyConnect-protokoll |
| | Juniper SSL | Juniper SSL-protokoll |
| | F5 SSL | F5 SSL-protokoll |
| | SonicWall mConnect | SonicWall mobil anslutning |
| | Aruba VIA | Aruba VIA-protokoll |
| | Anpassad SSL | Anslutning via anpassad SSL |
| | OpenVPN | OpenVPN-protokoll |

## Proxy-inställning

Konfigurering av en proxy för VPN-anslutningen

| | |
|---|---|
| Ingen | Upprätta ingen Proxy |
| Manuell | Upprätta en proxy manuellt |
| URL för proxyserver | Adress för åtkomst till Proxy-inställningar |
| Port | Fastställ porten för proxyservicen |
| Autentisering | Användarnamn för autentisering hos proxyservicen |
| Lösenord | Lösenord för autentisering hos proxyservicen |
| Automatisk | Upprätta en proxy automatiskt |
| URL för proxyserver | URL för åtkomst till Proxy-inställningarna |

| | |
|---|---|
| Visa platshållare | Visar alla tillgängliga användarvariabler , som AppTec360 kan använda |

## APN

| | |
|---|---|
| Namn på åtkomstpunkt | Namn på åtkomstpunkt |
| Användarnamn för åtkomstpunkt | Användarnamn för åtkomstpunkt |
| Lösenord för åtkomstpunkt | Lösenord för åtkomstpunkt |
| Proxyserver | Adress till proxyserver |
| Port | Respektive Proxy-port |

## Cellulär

| | |
|---|---|
| Aktivera data-roaming | Aktivera data-roaming |
| Aktivera röstroaming | Aktivera röstroaming |
| Aktivera hotspot | Aktivera hotspot |

## HTTP-proxy

| | |
|---|---|
| Typ av proxy | |
| Manuell | Upprätta en proxy manuellt |
| URL för proxyserver | Adress för åtkomst till proxyinställningarna |
| Port | Upprätta Proxy-port |
| Autentisering | Användarnamn för autentisering hos proxyservicen |
| Lösenord | Lösenord för autentisering hos proxyservicen |
| Automatisk | Upprätta en proxy automatiskt |
| Proxy PAC URL | Proxy PAC URL |
| Tillåt direktanslutning om PAC inte går att nå | Tillåt direktanslutning (utan VPN) om PAC inte kan nås |
| Tillåt kringgående av proxy för åtkomst till slutna nätverk | Tillåt kringgående av proxy för åtkomst till interna nätverk |

## AirPrint

| | |
|---|---|
| IP-adress | IP-adress för skrivare |
| Resursväg | Definitiv väg till AirPrint-enheten |

## AirPlay

| | |
|---|---|
| Enhetens namn | Enhetens namn |
| Lösenord | Lösenord för parkoppling |
| Vitlista | Definiera en lista över enheter som enheten kan para ihop sig exklusivt med |

# PIM-hantering

## Exchange Active Sync

| | |
|---|---|
| Kontots namn | Namn på e-postkonto |
| Exchange ActiveSync-värd | Serverns adress/FQDN |
| Tillåt flyttning | Tillåt flytt av e-postmeddelanden |
| Använd endast i mail | Interaktioner kan endast ske i den inbyggda Mail-appen |
| Använd SSL | Använd SSL-kryptering |
| Domän | Domän för server |
| Användare | Användarnamn |
| E-postadress | E-postadress (endast på enhetsnivå) |
| Lösenord (endast på enhetsnivå) | Användarens lösenord |
| Identitetscertifikat | Välj respektive certifikat för autentisering på servern |
| Tidigare dagar av Mail to Sync | Antal dagar fram till dess att e-postmeddelandena ska synkroniseras tillbaka.<br>No Limit = obegränsat |
| Aktivera S/MIME | Aktivera S/MIME-kryptering |
| Signering av certifikat | Ladda upp respektive signeringscertifikat |
| Krypteringscertifikat | Ladda upp respektive krypteringscertifikat |

## E-post

Inställning av POP3-/IMAP-konton på slutanvändarens enhet

| | | | |
|---|---|---|---|
| Beskrivning av konto | Namn des e-postkonton | | |
| Typ av konto | IMAP | Prefix för sökväg | Sökvägsprefixet för specialmappar |
| | POP | | |
| Användarens visningsnamn | Användarens visningsnamn | | |
| E-postadress | Användarens e-postadress | | |
| Tillåt flyttning | Tillåt flytt av e-postmeddelanden | | |
| Aktivera S/MIME | Aktivera S/MIME-kryptering | | |
| Signering av certifikat | Ladda upp respektive signeringscertifikat | | |
| Krypteringscertifikat | Ladda upp respektive krypteringscertifikat | | |

## Inkommande post

Inställningar för inkommande server

| | |
|---|---|
| Adress till e-postserver | Adress till e-postserver |
| Port för e-postserver | Port för e-postserver |
| Användarnamn | Respektive användarnamn |
| Typ av autentisering | Typ av autentisering |
| Ingen | Ingen typ av autentisering |
| Lösenord (endast på enhetsnivå) | Lösenordsfråga |
| MDM-utmaning-svar | |
| NTLM | NTLM-autentisering |
| HTTP MD5-digest | |
| Använd SSL | Använd SSL, om det behövs |

## Utgående post

Inställningar för utgående server

| | |
|---|---|
| Adress till e-postserver | Adress till e-postserver |
| Port för e-postserver | Port för e-postserver |
| Användarnamn | Respektive användarnamn |
| Typ av autentisering | |
| Ingen | Ingen autentiseringsmetod |
| Lösenord (endast på enhetsnivå) | Lösenordsfråga |
| MDM-utmaning-svar | |
| NTLM | NTLM-autentisering |
| HTTP MD5-digest | |
| Använd SSL | Använd SSL, om det behövs |
| Utgående lösenord samma som inkommande | Utgående lösenord samma som inkommande |
| Använd endast i mail | Aktivera, om alla utgående e-postmeddelanden ska skickas via Mail-appen |

## CalDav

Konfigurera uppsättning och distribution av ett CalDav-konto

| | |
|---|---|
| Beskrivning av konto | Kontots visningsnamn |
| Värdnamn | Värdnamn och/eller IP-adress |
| Port | Hamn för CalDav-kontot |
| Huvud-URL | Kontots huvudsakliga webbadress |
| Användarnamn | Respektive CalDav-användarnamn |
| Lösenord (endast på enhetsnivå) | Respektive CalDav-lösenord |
| Använd SSL | Använd SSL, om det behövs |

## Prenumererade kalendrar

Konfigurera och distribuera prenumererade kalendrar

| | |
|---|---|
| Beskrivning | Kontots visningsnamn |
| URL | URL till kalenderdatabasen |
| Användarnamn | Användarnamn för kalenderprenumerationen |
| Lösenord (endast på enhetsnivå) | Lösenord för kalenderprenumerationen |
| Använd SSL | Använd SSL, om det behövs |

## LDAP

I det här området ska du konfigurera en LDAP-anslutning för att möjliggöra ett dynamiskt certifikatutbyte mellan slutanvändarenheten och Active Directory.

Observera att den valda användaren måste ha läsbehörighet.

| | |
|---|---|
| Beskrivning av konto | Beskrivning av konto |
| Användarnamn för konto | Användare för LDAP-åtkomst |
| Lösenord för konto | Lösenord för LDAP-åtkomst |
| Kontots värdnamn | LDAP-serverns värdnamn/IP-adress |
| Använd SSL | Använd SSL, om det behövs |

I den andra delen kan du definiera individuella filter för sökning i LDAP-registret.

| | | |
|---|---|---|
| Beskrivning | Omfattning | Sök bas |
| Beskrivning av filter | Söknivå i LDAP-registret | Definiera det individuella filtret |

# Webbförvaltning

## Webbklippen

På den här platsen kan du definiera bokmärken med länkar till webbsidor, intranätportaler etc. som kommer att visas som en applikation på slutanvändarens enhet.

| | |
|---|---|
| Etikett | Namnet på anslutningen på slutanvändarens enhet |
| URL | Länk till respektive webbplats |
| Avtagbar | Om den är aktiverad kan användaren ta bort webbclipsen |
| Ikon | Via denna dialog laddar du upp en logotyp för anslutningen: Mått 180x180, png-format |
| Förkomponerad ikon | Om den är aktiverad kommer inga ytterligare effekter (skugga, reflektion) att visas på ikonen |
| Full skärm | När du öppnar webbklipp öppnas webbläsaren i helskärmsläge |

## Filter för webbinnehåll

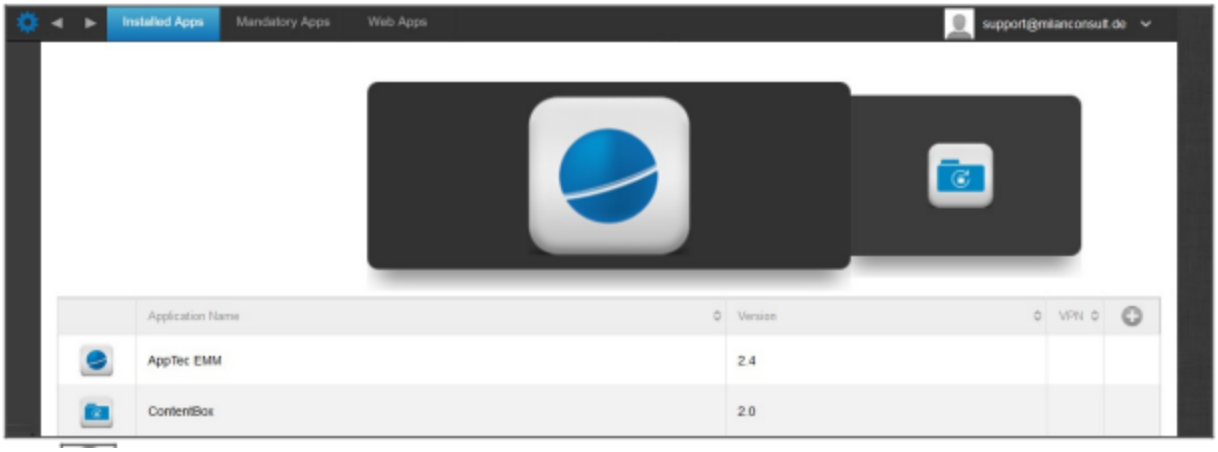
Web Content Filter gör det möjligt att begränsa åtkomsten till specifika internetsidor.

| **Tillåtna webbplatser** | |
|---|---|
| Begränsa innehåll för vuxna | Webbfilter tillämpas automatiskt för innehåll för vuxna |
| Tillåtna webbadresser | Med symbolen + lägger du till tillåtna sidor |
| Svartlistade webbadresser | Lägg till blockerade sidor med symbolen + |
| Endast specifika webbplatser | Endast specifikt innehåll kan visas, vilket du kan lägga till med symbolen +. |

# App-hantering

## Enterprise App Manager

### Installerade appar (endast på enhetsnivå)



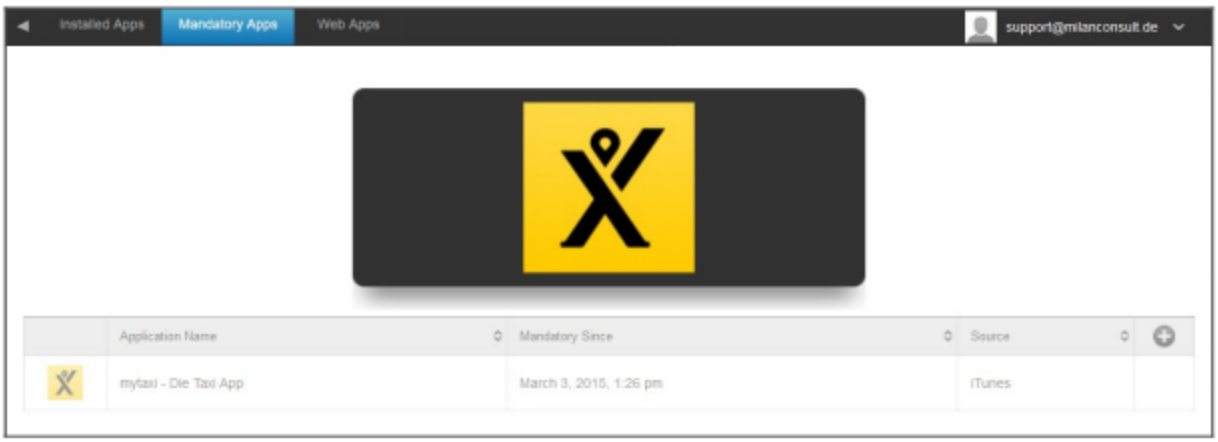

Här kan du se de appar som för närvarande är installerade på enheten.

### Obligatoriska appar

Under Obligatoriska appar kan du göra nödvändiga appar obligatoriska.

Användaren kommer kontinuerligt att påminnas om att installera den här appen.

Med hjälp av kan den obligatoriska appen definieras.




Det kan vara en app från Apple App Store, men också en intern app.

Om det rör sig om en övervakad enhet installeras appen automatiskt.

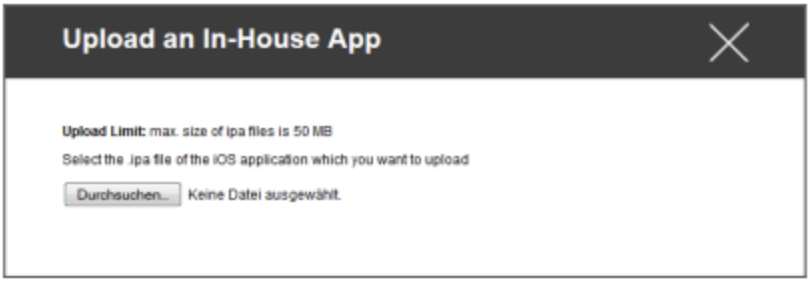
Du kan skicka en "Apple AppStore"-app från den offentliga AppStore till enheten, liksom en internt utvecklad In-House-app.

Eller så kan du välja från kategorin "iOS In-House Apps" och välja en In-House App, som du laddade upp under Allmänna inställningar.

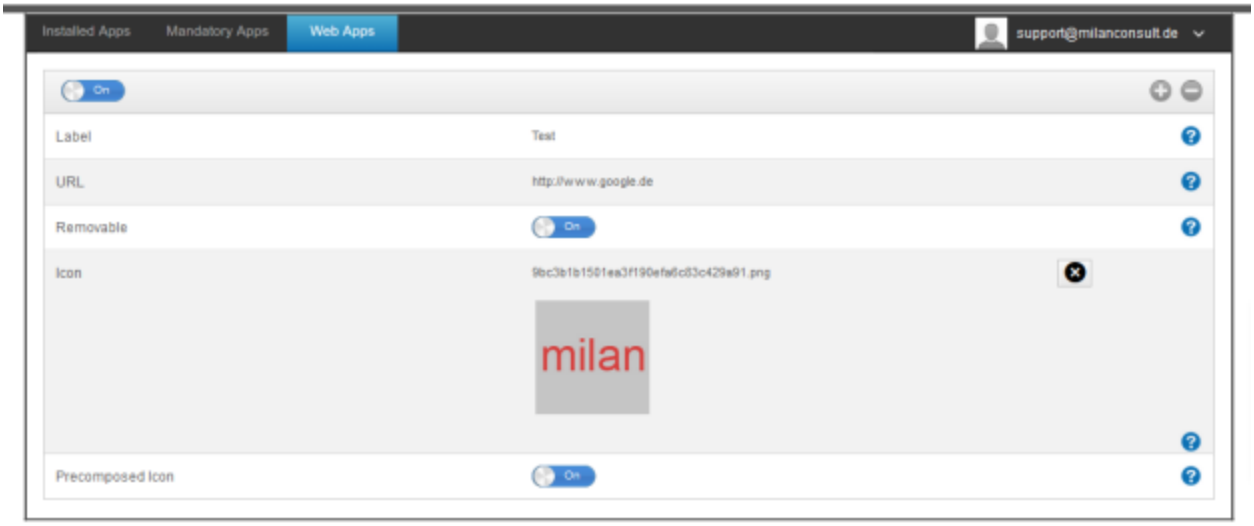
## Installationsalternativ

| | |
|---|---|
| Håll dig uppdaterad (stöds endast för VPP per enhet) | En gång i veckan kommer det att avgöras om det finns en uppdatering för appen. Om ja, kommer denna uppdatering att installeras<br>För interna appar kommer det uppdateringsmål som du konfigurerade i Allmänna inställningar att användas för uppdateringsprocessen. |
| Kör om när den inte hanteras | Om appen redan är installerad kommer MDM att ta över appen och hantera den |
| Ta bort appen när MDM-profilen tas bort | I händelse av borttagning av enhetshantering kommer appen att avinstalleras |
| Förhindra säkerhetskopiering av appdata | En säkerhetskopia av appspecifika data kommer inte att skapas |
| Inställning av app | Under "Appinställningar" kan du tilldela appen vissa värden i förgrunden (så länge appen stöder det, fråga vid behov appens utvecklare). |

Du kan också direkt välja och ladda upp en ipa-fil via "Upload In-House App".



## Webbappar




Under punkten "Web Apps" kan du, på samma sätt som med "Web Clips", skjuta upp internetsidor eller intranätportaler som en applikation på slutanvändarens enhet, i området Web Management. Som standard visas Web Apps i helskärmsläge, vilket kan konfigureras under Webclips.

| | |
|---|---|
| Etikett | Namnet på anslutningen på slutanvändarens enhet |
| URL | Länk till respektive webbplats |
| Avtagbar | Om den är aktiverad kan användaren ta bort webbclipsen |
| Ikon | Via denna dialog laddar du upp en logotyp för anslutningen: Mått 180x180, png-format |
| Förkomponerad ikon | Om den är aktiverad kommer inga ytterligare effekter (skugga, reflektion) att visas på ikonen |

# Begränsning & inställningar

## Svartlistade / vitlistade appar

Här kan du ställa in vilka appar som ska blockeras (eller tillåtas) beroende på dina inställningar i "Allmänna inställningar". Om du klickar på kommer du till den kända app-sökningen. Där kan du söka efter de appar du vill lägga till.

Observera att en övervakad enhet är nödvändig för denna funktion

## Begränsningar för SysApp

Blockera specifika appar eller funktioner på din enhet

| | |
|---|---|
| Tillåt användning av YouTube | Tillåt användning av YouTube |
| Tillåt användning av iTunes Store | Tillåt användning av iTunes Store |
| Tillåt användning av Safari | Tillåt användning av Safari |
| Aktivera autofyll | Tillåter autofyllning |
| Varning för bedrägerier | Kräver varning för bedrägeri |
| Aktivera JavScript | Möjliggör användning av JavaScript |
| Blockera popup-fönster | Blockerar alla typer av pup-ups |
| Tillåt cookies | Välj när Safari ska acceptera cookies |

## App-VPN

Via symbolen kan du definiera applikationer som automatiskt startar den valda VPN-anslutningen vid uppstart.

## Inställningar för appen

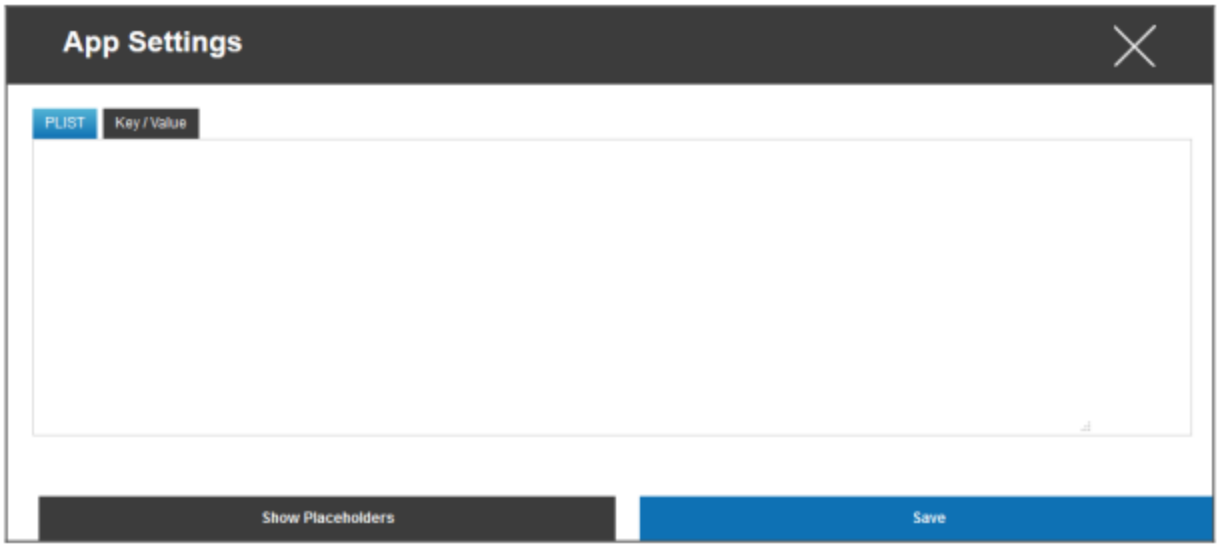
Under "Appinställningar" kan du tilldela appen vissa värden i förgrunden (så länge appen stöder det, fråga vid behov appens utvecklare).

Via symbolen lägger du till en (ytterligare) app. Du kommer återigen att hitta den välkända AppTec360-bilden av en App-Import.

Sök här efter den app som du vill konfigurera och välj den. Inställningarna kommer endast att gälla för hanterade appar.

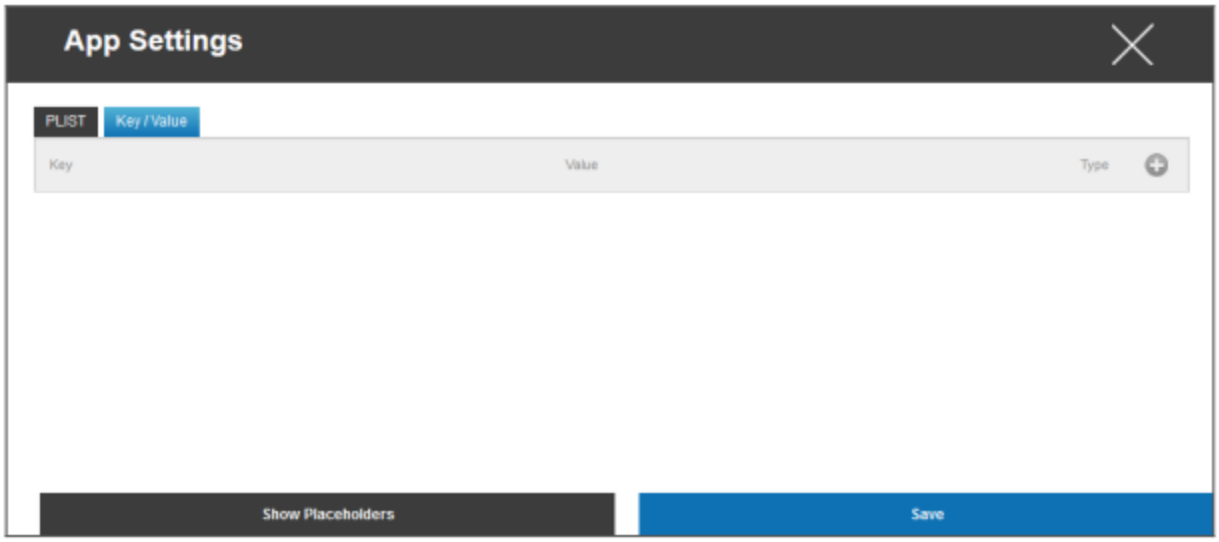
Om importen har lyckats ser du följande bildskärm:


Med ett klick på kan du nu utföra en mängd olika konfigurationer. Du kommer då att få följande översikt:

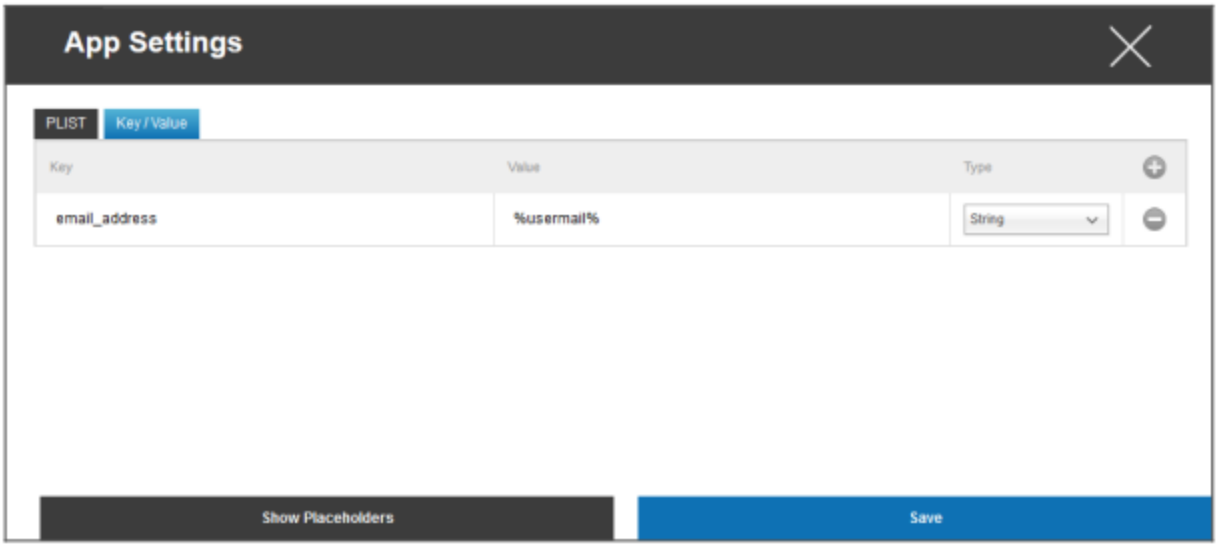



Om du redan har en PLIST (källtext för konfigurationen) kan du lägga till den här och spara allt med "Save".

Under "Key / Value" kan du koppla specifika konfigurationer till appen




Här kan du fastställa en ny nyckel och dess värde med hjälp av symbolen.




Naturligtvis står alla AppTecs platshållare till ditt förfogande

"Typ" -förklaring:

| | |
|---|---|
| Sträng | Text |
| Boolean | Sant/Falskt |
| Antal | Antal |

Med hjälp av symbolen kan du ta bort en app igen.

# App Store för företag

## iTunes-appar

Under denna punkt kan du distribuera valfria appar för din användare.

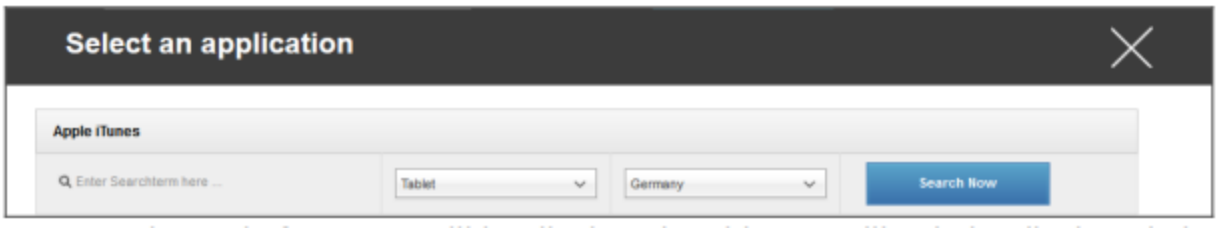
Om det finns en app här kommer den att installeras automatiskt på AppTec360 Stores slutanvändares enhet.

Dessa är helt enkelt länkar till den officiella Apple App Store. Av denna anledning måste varje slutanvändares enhet vara utrustad med ett Apple-ID.

I det här läget rekommenderar vi att varje användare har ett eget Apple-ID.

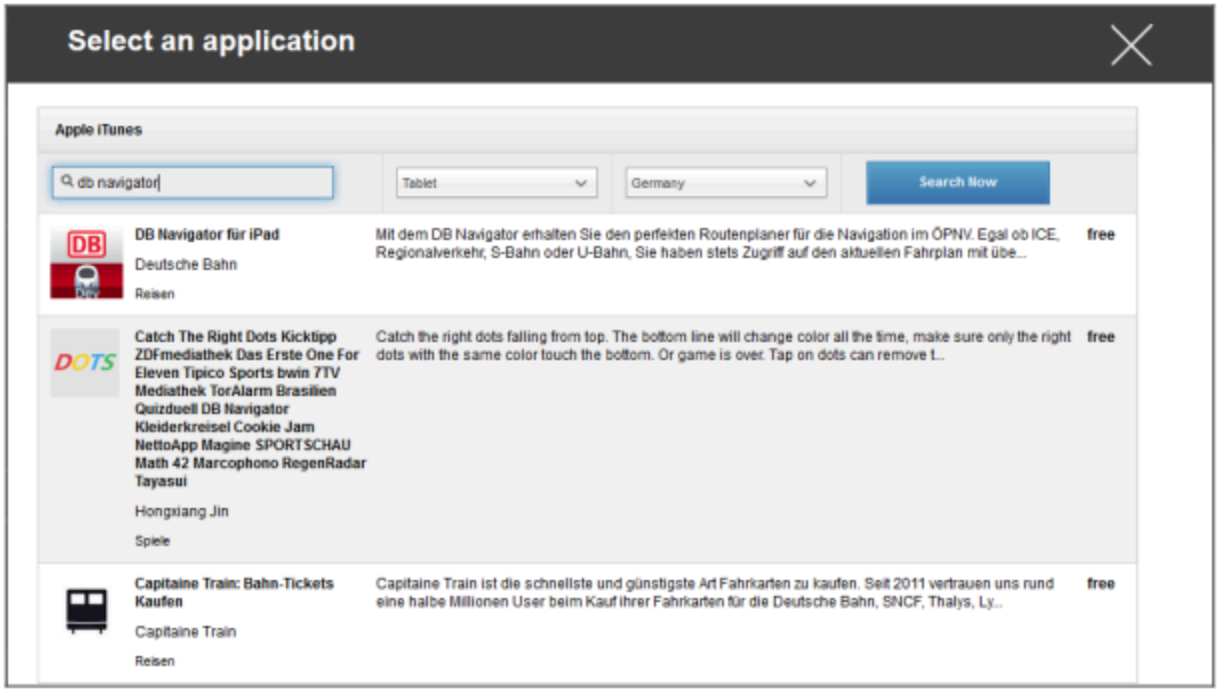
Med symbolen kan du lägga till ytterligare appar.


Därefter öppnas ett fönster med följande översikt.




Observera att endast gratisappar kommer att visas, betalappar visas endast via VPN.

Under "Ange sökterm här ..." kan du söka efter en app som finns i Apple App Store.




När du klickar på ikonen eller på appens namn kommer du att bli ombedd att utföra ytterligare konfigurationer.


| | |
|---|---|
| Håll dig uppdaterad | En gång i veckan kommer det att avgöras om det finns en uppdatering för appen. Om ja, kommer denna uppdatering att installeras |
| Ta bort appen när MDM-profilen tas bort | I händelse av borttagning av enhetshantering kommer appen att avinstalleras |
| Förhindra säkerhetskopiering av appdata | En säkerhetskopia av appspecifika data kommer inte att skapas |
| App-VPN | Välj en VPN-anslutning, som startar när du öppnar appen |

Efter ett klick på "Installera" kommer appen att läggas till i Enterprise App Store och kan sedan installeras på slutanvändarens enhet via AppTec360 AppStore.

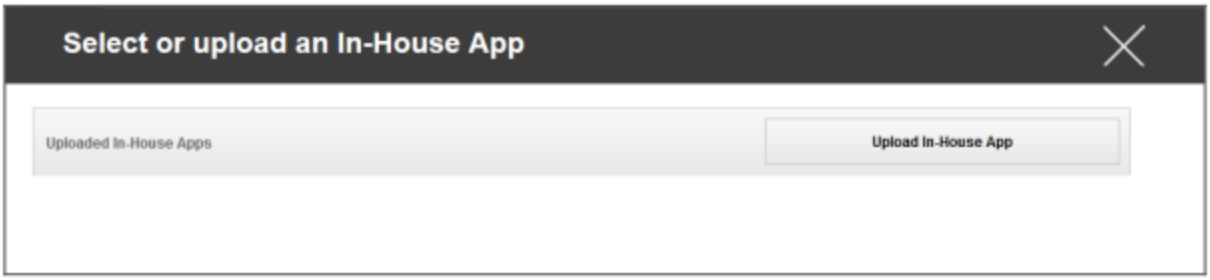
Om App-Store-importen har genomförts framgångsrikt får du följande översikt:

## Internt

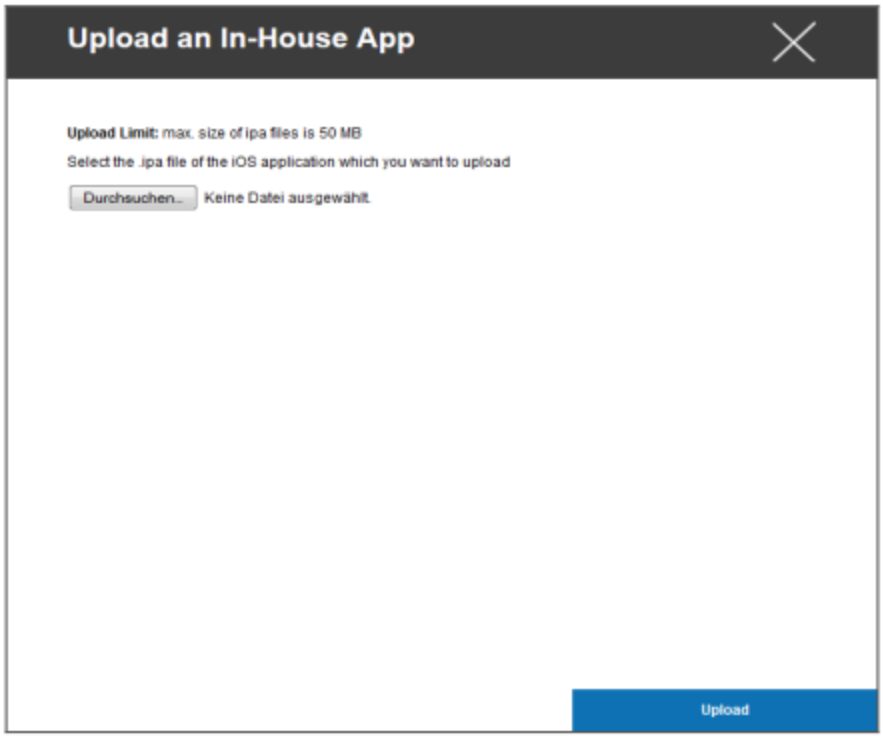
Under punkten "In-House" kan du ladda upp internt utvecklade appar och distribuera dem.

Med symbolen kan du distribuera ytterligare In-House Apps.

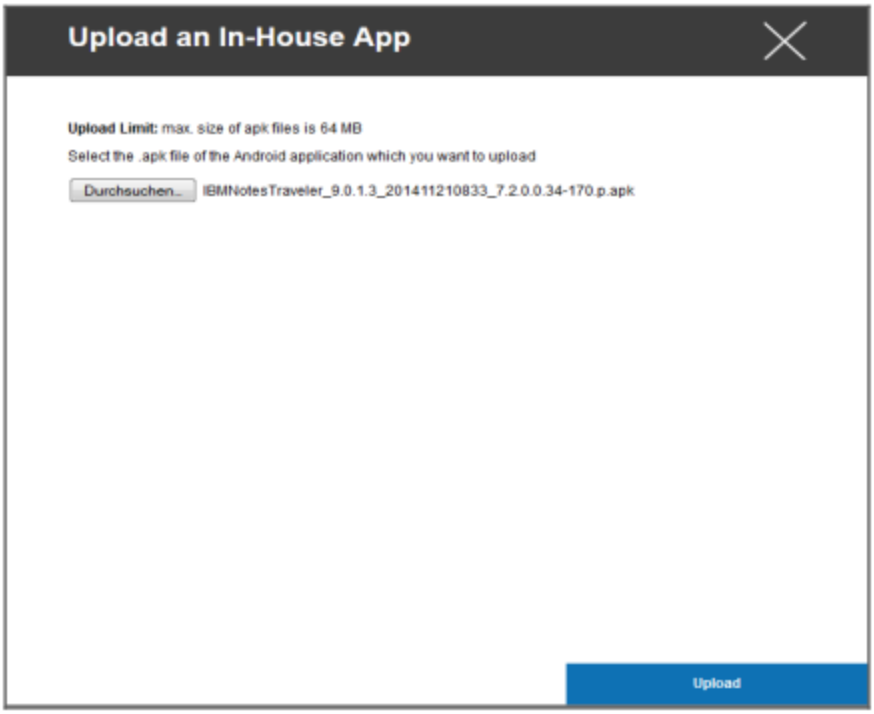
Om du aldrig har distribuerat In-House App kommer du att få följande genomgång:



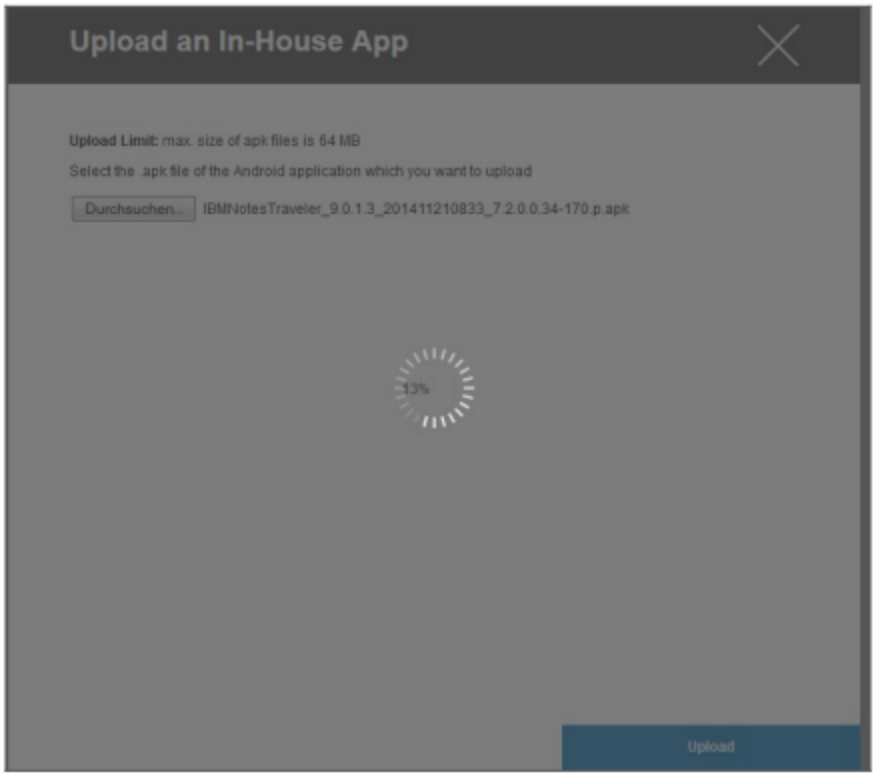

För detta klickar du på "Upload In-House App", du kommer då att få följande översikt:




Välj nu med "Sök ..." en .ipa-fil och klicka sedan på "Ladda upp"




Din app kommer nu att laddas upp. I mitten av cirkeln kan du se procentandelen av hur mycket av din app som redan har laddats upp.



Om uppladdningen av den interna appen har genomförts framgångsrikt kommer du att se den nyligen uppladdade appen i din appkatalog.

Användaren har nu möjlighet att se och installera denna app i AppTec360 Store på slutanvändarens enhet, under kategorin "In-House".

Eftersom det inte rör sig om en offentlig Apple AppStore-app behöver användaren inte ha ett lagrat Apple-ID på slutanvändarens enhet.

# Kiosk-läge

iOS Kiosk Mode är endast tillgängligt i Supervised Mode

I kioskläget kan du fördefiniera en app eller URL, så att det blir möjligt att köra/besöka enbart denna app/URL.

Dessutom kan du avaktivera olika hårdvaruknappar i Kiosk Mode.

## Tillämpningstyp

### Paket

*Om du vill starta appen i kioskläge väljer du "Paket" under "Applikationstyp"*

| | |
|---|---|
| Kiosk-applikation | Klicka här för att välja en app som ska starta i Kiosk Mode<br>Du kommer att hitta den aktuella översikten över App Management<br>Du kan välja mellan "Apple iTunes Apps" och "iOS In-House Apps" |

### URL

*Om du vill starta en URL i Kiosk Mode väljer du "URL" under "Application Type"*

| | |
|---|---|
| URL | Ange nu den önskade URL-adressen |
| Policy för samma ursprung | Om denna funktion är aktiv kan användaren bara surfa på undersidorna till den fördefinierade URL:en<br>Om du t.ex. har definierat följande URL:<br>www.mypage.com, då kan användaren surfa på<br>www.mypage.com/subpage |
| Vitlistade webbadresser | Här kan du upprätthålla en vitlista, alla dessa webbadresser är tillåtna<br>Högst 1 URL per rad<br>En URL måste börja med http:/ eller https:// |
| Svartlistade webbadresser | Här kan du skapa en svart lista, där alla dessa webbadresser inte tillåts<br>Högst 1 URL per rad<br>En URL måste börja med http:/ eller https:// |
| Rensa webbläsaren efter inaktivitet | Efter inaktivitet kommer webbläsarens cache att tömmas |
| Lösenord för utgång Aktiverad | Om du aktiverar den här funktionen har användaren möjlighet att avsluta Kiosk Mode med ett lösenord som du har fördefinierat |
| Avsluta lösenord | Detta är det lösenord som har fördefinierats av dig |

## Inställningar för kioskläge

| | |
|---|---|
| Schemalagt kioskläge | Baserat på tiden på dygnet kan du ställa in Kiosk Mode så att läget startas och avslutas automatiskt vid en tidpunkt som har bestämts i förväg |
| Starttid | Starttidpunkt |
| Tid i minuter | Tid i minuter, efter vilken Kiosk Mode ska avslutas igen |
| Inaktivera Touch | Om den är aktiverad är pekskärmen avaktiverad |
| Inaktivera enhetsrotation | Om den är aktiverad avaktiveras den automatiska anpassningen av skärmen |
| Omkopplare för avaktivering av ringsignal | Om den är aktiverad kommer ringsignalen att avaktiveras. Från och med då är beteendet beroende av den tidigare inställda funktionen |
| Inaktivera volymknappar | Om den är aktiverad kommer volymknapparna att avaktiveras |
| Inaktivera knappen för sömn och väckning | Om den är aktiverad kommer på/av-knappen att avaktiveras |
| Inaktivera automatiskt lås | Om den är aktiverad kommer enheten inte att växlas till standby |
| Aktivera röst över | Om den är aktiverad kommer Voice Over-assistenten att aktiveras |
| Aktivera zoom | Om den är aktiverad kommer zoomen att aktiveras |
| Aktivera invertera färger | Om den är aktiverad kommer det inverterade visningsläget att aktiveras |
| Aktivera hjälpmedelsberöring | Om den är aktiverad kommer AssistiveTouch att aktiveras |
| Aktivera val av talare | Om den är aktiverad kommer talvalet att aktiveras |
| Aktivera Mono Audio | Om den är aktiverad kommer Mono Audio att aktiveras |
| VoiceOver | Om den är aktiverad kan användaren aktivera VoiceOver |
| Zoom | Om den är aktiverad kan användaren aktivera Zoom |
| Invertera färger | Om den är aktiverad kan användaren aktivera inverterade färger |
| Hjälpmedelsberöring | Om den är aktiverad kan användaren aktivera hjälpande beröring |

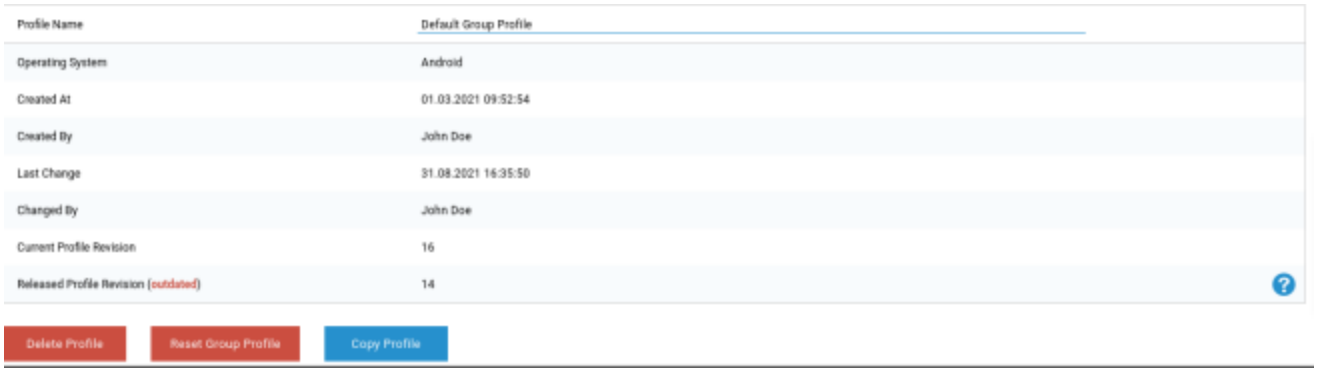
# Android Enterprise – Fullt hanterad enhetskonfiguration

Beroende på om du för närvarande har valt en grupprofil eller en enhet skiljer sig översikten och dess underpunkter åt - tänk på detta noga!

# Allmänt

## Översikt över grupprofiler (endast på gruppnivå)

När du öppnar en grupprofil får du en snabb överblick över profilen.




| | |
|---|---|
| Profilens namn | Profilens namn (kan ändras här) |
| Operativsystem | Operativsystem som profilen är avsedd för |
| Skapad vid | Tidpunkt för skapelse |
| Skapad av | Skaparen av profilen |
| Sista förändringen | Tidpunkt för senaste ändring av profilen |
| Förändrad av | Konto som gjorde de senaste ändringarna |
| Aktuell profil Revidering | Revidering av sparat profiltillstånd |
| Utgiven Profil Revision | Tilldelad profilrevision ("Tilldela nu"). Om etiketten visar "(outdated)" bakom texten betyder det att du har sparat profilen men inte tilldelat den ännu, så enheterna kommer fortfarande att få en äldre version. |

## Enhetsöversikt (endast på enhetsnivå)

Om du befinner dig på en enhet kommer du att få en översiktlig sammanfattning av den valda enheten, följande finns här:

| | |
|---|---|
| Enhetens namn | Enhetens namn |
| Plats | Koordinater för platsen |
| Telefonnummer | Telefonnummer |
| Tilldelade Obligatoriska appar | Antal tilldelade obligatoriska appar |
| OS-version | Enhetens OS-version |
| Operativsystem | Operativsystem (Android Enterprise) |
| Serienummer | Enhetens serienummer |
| Ägande av enhet | Företagsenhet eller privat enhet |
| Enhetstyp | AE Arbetshanterad enhet |
| Rotad | Status, anger om enheten har rotats |
| Överensstämmande | I enlighet med riktlinjerna |
| IP-adress | Enhetens IP-adress |
| Senast sett | Tidpunkt då enheten senast var ansluten till AppTec |
| Sista knuffen | Tidpunkt då den senaste push-meddelandet skickades till enheten |
| AE Enhetens ägarläge | Ja |
| Tilldelning av användare | Användaren eller gruppen som den här enheten är kopplad till |

## Config Revision (endast på enhetsnivå)

Här får du en överblick över vilken grupprofil som är tilldelad enheten.


Om du klickar på grupprofilen får du direktåtkomst till profilen och kan göra inställningar.

Med den här symbolen kan du återställa de distribuerade apparna till grupprofilens inställningar.

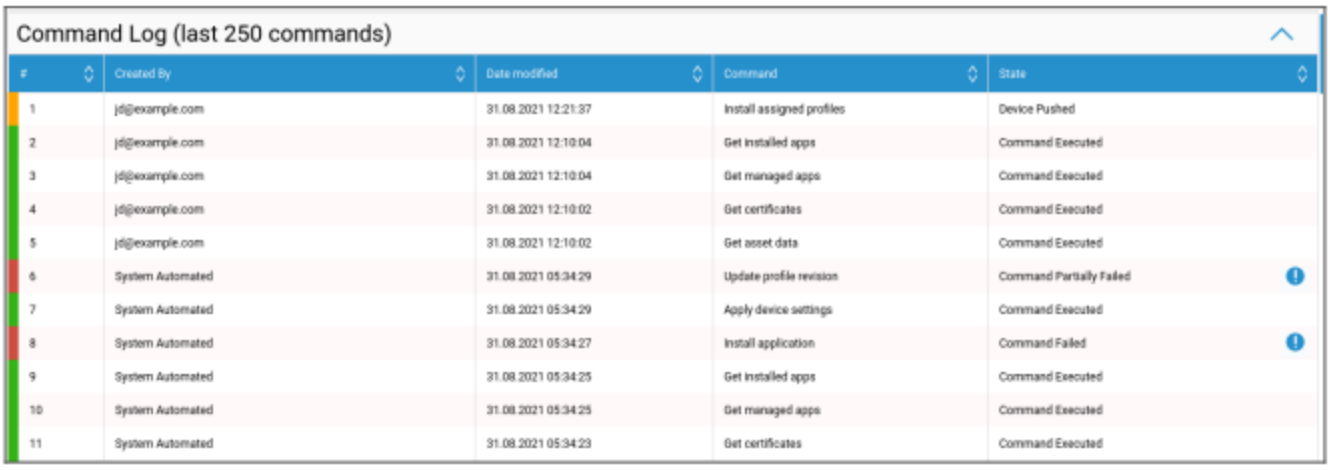
Med den här symbolen kan du återställa alla använda appar till grupprofilens inställningar.

"Nyare revision tillgänglig" anger att grupprofilen har ändrats och sparats men inte tilldelats. Grupprofilen måste tilldelas med "Tilldela nu" på gruppnivå för att ändringarna ska gälla för enheterna.

## Enhetslogg (endast på enhetsnivå)

### Kommandologg

Här kan du se vilka kommandon som har utfärdats för enheten och vilken status de har.




Kommandon som skapats av "System Automated" skapas automatiskt av systemet.

## Möjliga kommandostatusar

| | |
|---|---|
| Enhet tryckt | En push-begäran har skickats till push-tjänsten (t.ex. APNS) för att tala om för enheten att den ska ansluta tillbaka till EMM-servern. |
| Kommando Skapat | Kommandot skapades i systemet. |
| Kommando skickat | Kommandot skickades till enheten efter att den anslutit till servern. |
| Kommando utfört | Kommandot har utförts framgångsrikt. |
| Kommandot misslyckades | Kommandot misslyckades. * |
| Kommandot delvis misslyckat | Beroende på enhetens operativsystem kan vissa kommandon grupperas tillsammans.<br>I detta misslyckades vissa delar av denna kommandogrupp. * |
| Kommando utfört, eventuellt misslyckat | Kommandot utfördes, men kanske inte. |
| Kommando Repushed | Kommandot återställdes av en användare. |
| Bortkastad | Kommandot kasserades. Till exempel för att det ersattes av ett annat kommando eller för att enheten registrerades på nytt och gamla kommandon togs bort |

Om det finns ett utropstecken bakom meddelandet kan du få mer information genom att hålla muspekaren över ikonen.

# Inställningar för enhet

## Konfiguration av klient

Här kan du utföra följande konfigurationer på din Android-enhet:

| | |
|---|---|
| Tid för bristande efterlevnad | Tidsgräns för användarsvar efter vilken verkställighetsåtgärden tillämpas. |
| Verkställighetsåtgärd efter timeout för efterlevnad | Verkställighetsåtgärd när en användare inte utför åtgärder som leder till en kompatibel enhetsstatus |
| Frekvens för datainsamling | Frekvens med vilken enhet/GPS-information ska samlas in |
| Frekvens för enhetens hjärtslag | Intervall inom vilket enheten ska kontakta AppTec360 Server<br>Min. 1 minut<br>Max. 24 timmar |
| Aktivera platsuppdateringar | Om den är aktiverad skickar enheten platsuppdateringar till AppTec360 Server |
| Plats Uppdateringstid | Bestämmer i vilka tidsintervaller enheten skickar platsuppdateringar till AppTec360 |
| Använd Google Location Accuracy för platsuppdatering | Om den är aktiverad kommer nätverksplatsen att användas för platsuppdateringar (om den avaktiverades under "Begränsningar" påverkar inte den här inställningen någonting) |
| Använd GPS-position för platsuppdatering | Om den är aktiverad används GPS för platsuppdateringar |
| Tillåt falska platser (Mock) | Möjliggör förfalskning av platsinformation via appar från tredje part |
| Åtgärder vid förlorad anslutning | Om den är aktiverad kan du ange en åtgärd för det fall att en enhet inte får en anslutning till MDM-servern inom heartbeat-intervallet. Om enheten t.ex. har en heartbeat-tid på 5 minuter ansluter den till servern kl. 10.35. Efter det lämnar enheten Wi-Fi-området. Nästa heartbeat kl. 10:40 misslyckas och den angivna åtgärden utförs. |
| Åtgärd | Den åtgärd som ska vidtas så snart en enhet inte längre uppfyller kraven. |

| | | |
|---|---|---|
| | | • Lock Device = låsa enhet<br>• Wipe Device = enheten återställs till fabriksinställningarna<br>• Wipe Device & SD Card = enheten återställs till fabriksinställningarna och SD-kortets lagringsutrymme raderas |
| | Tröskelvärde | Du kan ange ett tröskelvärde för antalet misslyckade hjärtslag som krävs för att utlösa den angivna åtgärden. |

| | | |
|---|---|---|
| Läge för tillämpning av policy | Standard: | Användare kommer regelbundet att uppmanas att utföra utestående åtgärder |
| | Lazy Policy Enforcement: | Användare kommer aldrig att bli ombedda att utföra utestående åtgärder. Alla öppna åtgärder kommer att visas i AppTec360 Client |
| | Aggressivt genomförande av policyer: | Användare kommer att uppmanas att utföra utestående åtgärder hela tiden |
| AppTec360 Versionslås | Om aktiverat kan en versionskod för AppTec360 MDM Client anges. AppTec360-klienten kommer endast att uppdateras till den angivna versionen. Nyare versioner kommer att ignoreras. En nedgradering är INTE möjlig. | |
| Version Kod | Versionskod för AppTec360 MDM Client som ska låsas till. | |
| Avaktivera AppTec360 Notifiering | Om den är inaktiverad kommer AppTec360 Client inte att visa någon notifiering i Notifieringsfältet. Användare kan alltså stänga AppTec360-klienten via aktivitetshanteraren. Om AppTec360-klienten är stängd kommer flera funktioner, inklusive Kiosk Mode och App Black/Whitelisting, inte att fungera korrekt. Samsung-enheter erbjuder en skyddsmekanism för AppTec360 Client. Meddelandet är avaktiverat som standard på Samsung-enheter som stöder KNOX API:er. Meddelandet bör inte inaktiveras enheter med Android 8.0 eller högre. | |

## Bakgrund

| | |
|---|---|
| Ställ in anpassad bakgrundsbild | Aktivera/inaktivera den anpassade bakgrundsbilden |
| Bakgrund | Ställ in bakgrundsläget så att en färgkod eller en bild används |
| Ange en färg | Ange en bakgrundsfärg som hexvärde, t.ex. #000000 för svart eller #ffffff för vitt |
| Ange bild som bakgrundsbild | Ladda upp den bildfil som du vill använda som bakgrundsbild |

# Tillgångshantering (endast på enhetsnivå)

## Info om enhet

| | |
|---|---|
| Modell | Enhetens modellbeteckning |
| Operativsystem | OS |
| OS-version | OS-version |
| Serienummer | Serienummer |
| Enhetens namn | Enhetens namn |
| Batteristatus | Batteriets status |
| Fritt / totalt minne | Fritt / Totalt minne |
| Samsung Safe | Samsung SAFE-gränssnitt, krävs för en mängd olika inställningsalternativ |
| SD-kort tillgängligt | SD-kort tillgängligt |
| SD-kort emulerat | SD-kort emulerat |
| SD-kort löstagbart | SD-kort kan tas ut |
| SD Fritt / Totalt minne | SD Fritt / Totalt minne på SD-kort |

## Wi-Fi

| | |
|---|---|
| IP-adress | Enhetens IP-adress |
| WiFi MAC | WiFi MAC-adress |

## Cellulär

| | |
|---|---|
| Status | Status (SIM-kortet installerat) |
| Telefonnummer | Telefonnummer |
| Roaming (röst/data) | Roaming för röst/data |
| Status för roaming | Aktuell roamingstatus |
| IP-adress | IP-adress |
| Operatör/transportör | Operatör/transportör |
| Cellulär teknik | Cellulär teknik |
| IMEI | IMEI-nummer |
| ICCID | Detta är ID för SIM-kortet, ofta även ett smartkort eller ett Integrated Circuit Card (ICC) |
| IMSI | IMSI (International Mobile Subscriber Identity) ger i GSM- och UMTS-mobilnät en definitiv identifiering av nätanvändarna<br>IMSI består av maximalt 15 siffror och konfigureras på följande sätt:<br>• Mobil landskod (MCC), 3 siffror<br>• Mobilnätskod (MNC), 2 eller 3 siffror<br>• Identifieringsnummer för mobilabonnent (MSIN), 1-10 siffror |
| Nuvarande MCC/MNC | Se "SIM MCC/MNC" |
| SIM MCC/MNC | Mobile Country Code är en etablerad landsidentifierare, fastställd av ITU enligt E.212-standarden. Den fungerar tillsammans med Mobile Network Code (MNC) för identifiering av mobilnätet.<br>Betyder SIM-kortets landskod/Mobile Network Code.<br>Om du roamar till ett annat mobilnät kommer logiskt sett "Current MCC/MNC" och "SIM MCC/MNC" att vara olika. |

## Bluetooth

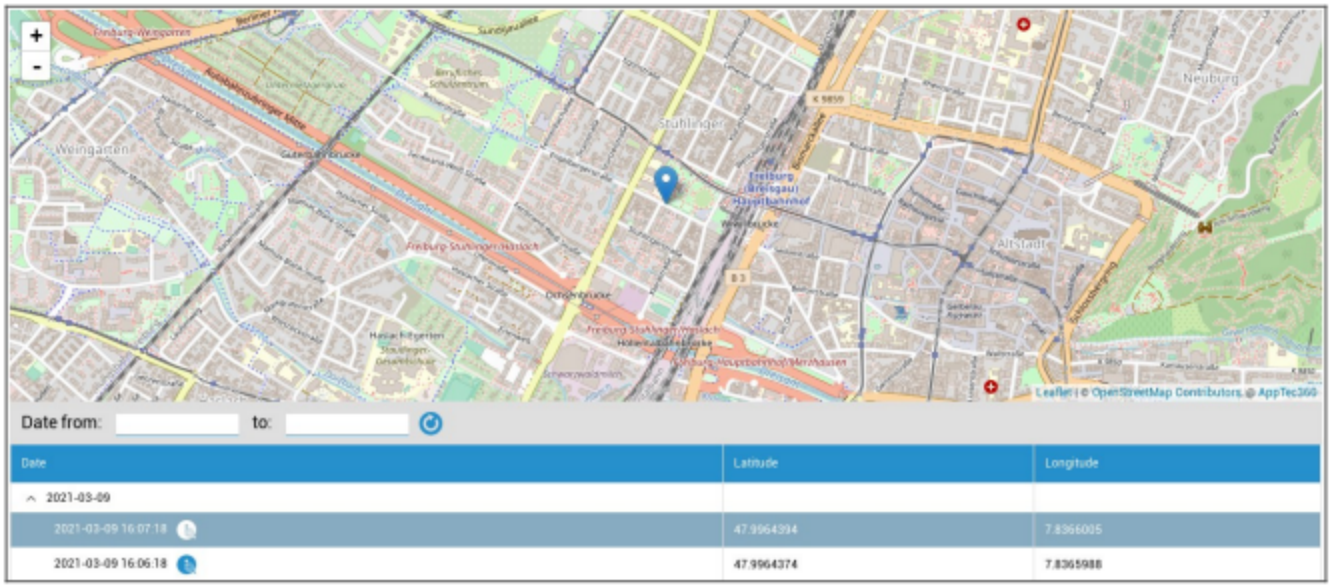
| | |
|---|---|
| Bluetooth MAC | Bluetooth MAC-adress |

# Säkerhetshantering

## Stöldskydd (endast på enhetsnivå)

### GPS-information (endast på enhetsnivå)

Här kan du ange aktuell/senaste enhetsplats. Lokaliseringen kan skyddas med ett eller till och med två lösenord - se: Allmänna inställningar - Sekretess - GPS-åtkomst



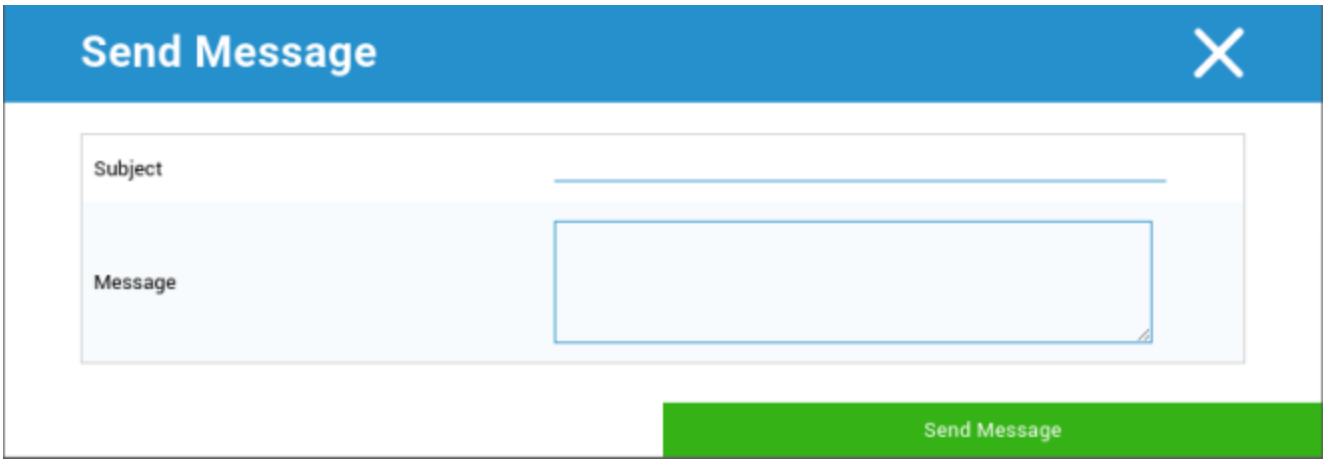

### Wipe & Lock (endast på enhetsnivå)

Under "Wipe & Lock" kan du utföra följande tre åtgärder:

| | |
|---|---|
| Fullständig avtorkning | Enheten återställs till fabriksinställningarna (både företagsdata och personuppgifter raderas) |
| Enterprise Wipe | Endast företagsdata tas bort från slutanvändarens enhet (alla appar, data etc. som tillhandahölls av AppTec360) |
| Lås skärm | Om skärmlåset är aktiverat räcker det med att låsa upp enheten med enhetens lösenord/PIN |

## Meddelande (endast på enhetsnivå)

Här kan du fylla i ämne och ett meddelande och skicka det till en slutanvändares enhet.



# Säkerhetskonfiguration

## Enhetens lösenord

Under "Passcode" kan du ange ett lösenord för enheten, följande inställningsalternativ är tillgängliga för dig

| | | |
|---|---|---|
| Minsta lösenordslängd | Fastställer det minsta antal symboler som ett lösenord måste innehålla | |
| Lösenordskvalitet | Ospecificerad | Denna policy innehåller inga krav på lösenord. |
| | Biometrisk svaghet | Denna policy tillåter teknik för biometrisk identifiering med låg säkerhet. Detta innebär teknik som kan känna igen en persons identitet till ungefär en 3-siffrig PIN-kod (falsk detektering är mindre än 1 på 1 000). |
| | Någonting | Denna policy kräver att någon form av lösenord eller mönster anges, men tillämpar inga specifika regler. |
| | Alfabetisk | Användaren måste ha angett ett lösenord som innehåller minst alfabetiska tecken (eller andra symboler). |
| | Alfanumerisk | Användaren måste ha angett ett lösenord som innehåller minst både numeriska och alfabetiska tecken (eller andra symboler). |
| | Komplex | Användaren måste ha angett ett lösenord som innehåller minst en bokstav, en siffra och en specialsymbol, som standard. Med denna lösenordskvalitet kan lösenord begränsas till att innehålla olika uppsättningar av tecken, t.ex. minst en versal etc. |
| Minsta lösenordslängd | Ange det antal tecken som krävs för lösenordet. Du kan t.ex. kräva att PIN-koder eller lösenord ska innehålla minst sex tecken. | |
| Minsta antal numeriska siffror som krävs i lösenordet | Minsta antal numeriska siffror som krävs i lösenordet | |
| Minst små bokstäver krävs i lösenordet | Minst små bokstäver krävs i lösenordet | |
| Minimikrav på versaler i lösenordet | Minimikrav på versaler i lösenordet | |

| | |
|---|---|
| Minsta antal tecken som inte är bokstäver som krävs i lösenordet | Minsta antal tecken som inte är bokstäver som krävs i lösenordet |
| Minsta antal symboler som krävs i lösenordet | Minsta antal symboler som krävs i lösenordet |

| | |
|---|---|
| Lås för maximal inaktivitetstid | Maximal inaktivitet för användaren tills tiden låses |
| Tidsgräns för lösenordsutgång | Fastställer, efter vilket tidsintervall lösenordet upphör att gälla och ett nytt lösenord måste utfärdas |
| Begränsning av lösenordshistorik | Antal tidigare använda lösenord som inte är tillåtna |
| Maximalt antal misslyckade lösenordsförsök | Fastställer hur ofta ett lösenord kan anges felaktigt innan en fullständig radering av enheten utförs |
| Tillåt biometrisk autentisering | Möjliggör autentisering via fingeravtryck eller irisskanning. Endast för Samsung KNOX 2.1 och högre |

## AntiVirus

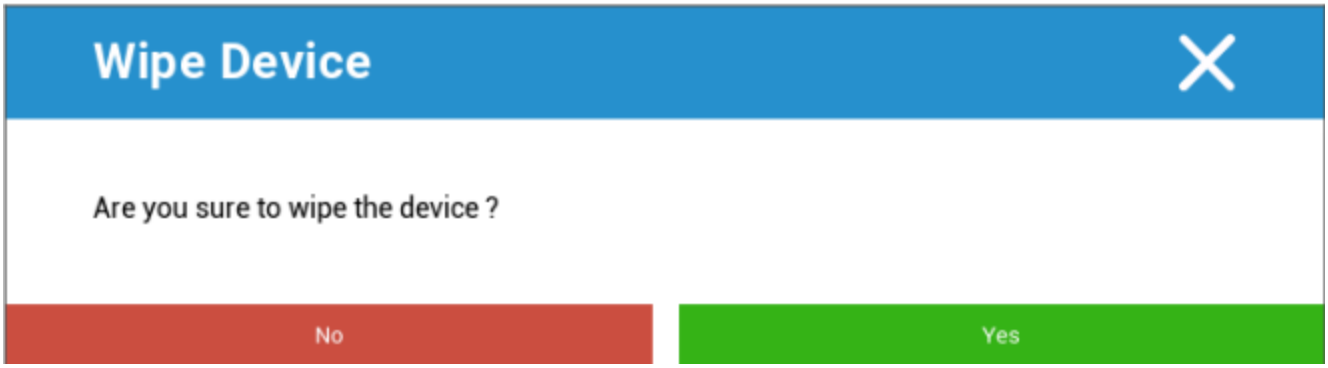
| | |
|---|---|
| Automatisk skanning | Aktivera periodiska automatiska skanningar |
| Skanningsintervall | Intervall för undersökning (snabb/full) |
| Fullständig automatisk skanning | Aktivera helautomatiska skanningar |
| Automatiska uppdateringar | Aktivera automatiska uppdateringar |
| Intervall för uppdateringskontroll | Hur ofta appen och dess databas ska uppdateras (virus/skadad kod) |
| Skydd för appar | Aktivera automatisk appskanning |
| Skydd för SD-kort | Aktivera automatisk skanning av SD-kort |
| Uppdatering endast för Wi-Fi | När den är aktiverad tillämpas uppdateringar endast när enheten är ansluten till ett Wi-Fi-nätverk |

# End of Life (endast på enhetsnivå)

## Torka (endast på enhetsnivå)

Under "Wipe" kan du återställa enheten till fabriksinställningarna. Här raderas både företagsdata och privata data på slutanvändarens enhet.

Genom att klicka på "Minus-symbolen" får du följande meddelande:




Med "Yes" kan du utföra torkningen.

Under "Wipe Report" kan följande objekt visas

| | |
|---|---|
| Raderad av | Historik över vem som utförde torkningen |
| Datum | Datum |
| Status | Status (t.ex. om rensningen utfördes framgångsrikt) |

# Inställningar för begränsning

## Begränsningar

Här kan en mängd olika saker begränsas och blockeras.

| Aktivera kamera | Tillåt användning av kamera | |
|---|---|---|
| Tvinga fram automatisk synkronisering | På | Synkroniseringen är permanent aktiverad |
| | Av | Synkroniseringen är permanent avaktiverad |
| | Användarens val | Väljs av användaren |
| Force Bluetooth | På | Bluetooth är permanent aktiverat |
| | Av | Bluetooth är permanent avaktiverat |
| | Användarens val | Väljs av användaren |
| Force GPS | På | GPS är permanent aktiverad |
| | Av | GPS är permanent avaktiverad |
| | Användarens val | Väljs av användaren |
| Force Network Plats | På | Permanent internet-lokalisering |
| | Av | Permanent avaktivering av internetlokalisering |
| | Användarens val | Väljs av användaren |

| Säkerhet | | |
|---|---|---|
| Avvisa delningsplats | Anger om en användare inte får aktivera platsdelning. | |
| Avvisa säker start | Anger om användaren inte har rätt att starta om enheten till säkert startläge. | |
| Tillåt inte återställning av nätverk | Anger om en användare inte får återställa nätverksinställningar från Settings. | |
| Avvisa fabriksåterställning | Anger om en användare inte får återställa enheten. | |
| Aktivera ADB | Möjliggör anslutning till en PC via ADB | |
| Avaktivera nyckelvakt | Avaktiverar nyckelvakt | |
| Enhetens ägare Info om låsskärm | Anger vilken information om enhetens ägare som ska visas på låsskärmen. | |
| Tillämpning av efterlevnad | Läge Prompt Användare | Användaren uppmanas att utföra de nödvändiga åtgärderna. |
| | Läge Lock-Down Container | Dölj alla appar tills alla krav har uppfyllts |

| App-hantering | |
|---|---|
| Tillåt applänkning över profilgränser | Tillåter appar i den överordnade profilen att hantera webblänkar från den hanterade profilen. |
| Avvisa appkontroll | Anger om en användare inte får ändra program i inställningar eller startprogram. |
| Avvisa installation av app | Anger om en användare inte får installera program. |
| Tillåt inte avinstallation av appar | Anger om en användare inte får avinstallera program. |
| Policy för körtidsbehörighet | Anger hur nya behörighetsförfrågningar från appar ska hanteras. |
| Tillåt okända källor | Om den är aktiverad kan användare ladda appar genom att installera en .apk-fil. |

| Anslutningsmöjligheter | |
|---|---|
| Avvisa konfiguration av mobilnätverk | Anger om en användare inte får konfigurera mobila nätverk. |
| Tillåt inte internetdelning Konfig | Anger om en användare inte får konfigurera internetdelning och portabla hotspots. |
| Avvisa VPN-konfiguration | Anger om en användare inte får konfigurera ett VPN. |
| Tillåt inte Wifi-konfiguration | Anger om en användare inte får ändra WiFi-åtkomstpunkter. |
| Avvisa utgående NFC-strålning | Anger om användaren inte får använda NFC för att skicka ut data från appar. |
| Lås WiFi-konfiguration | Den här inställningen styr om WiFi-konfigurationer som skapats av en app för enhetsägare ska vara låsta (dvs. endast kunna redigeras eller tas bort av appen för enhetsägare, inte ens av appen Settings). |
| Aktivera data-roaming | Aktiverar data-roaming |

| Bluetooth | |
|---|---|
| Avvisa Bluetooth | Anger om Bluetooth inte är tillåtet på enheten. Kräver Android 8.0 |
| Avaktivera Bluetooth-delning | Anger om utgående Bluetooth-delning inte är tillåten på enheten. Kräver Android 8.0 |
| Avvisa Bluetooth-konfiguration | Anger om en användare inte får konfigurera Bluetooth. |

| Kontohantering | |
|---|---|
| Tillåt inte att lägga till hanterad profil | Anger om en användare inte ska tillåtas att lägga till hanterade profiler. Kräver Android 8.0 |
| Tillåt inte att lägga till användare | Anger om en användare inte får lägga till nya användare. |
| Avvisa Ta bort hanterad profil | Anger om hanterade profiler för den här användaren kan tas bort av andra än profilägaren. Kräver Android 8.0 |
| Förbjuda ändring av konto | Anger om en användare inte ska tillåtas att lägga till och ta bort konton, såvida de inte läggs till programmatiskt av Authenticator. |

| Telefoni | |
|---|---|
| Avvisa utgående samtal | Anger att användaren inte får ringa utgående telefonsamtal. |
| Avvisa SMS | Anger att användaren inte får skicka eller ta emot SMS-meddelanden. |

| System | |
|---|---|
| Tillåt inte skapande av fönster | Anger att andra fönster än app-fönster inte ska skapas. |
| Avvisa inställd användarikon | Anger om en användare inte får ändra sin ikon. |
| Tillåt inte Set Wallpaper | Användarbegränsning för att inte tillåta inställning av bakgrundsbild. |
| Inaktivera statusfältet | Genom att inaktivera statusfältet blockeras aviseringar, snabbinställningar och andra skärmöverlägg som gör det möjligt att fly från en enhet som bara används en gång. |
| Aktivera automatisk tid | Ställer in tiden automatiskt. |
| Aktivera automatisk tidszon | Tidszonen ställs in automatiskt. |
| Står på när den är inkopplad | Enheten förblir aktiv när den är ansluten till en strömkälla. |

| Förvaring | |
|---|---|
| Avvisa inaktivera appverifiering | Anger om en användare inte får inaktivera programverifiering. |
| Tillåt inte montering av fysiska medier | Anger om en användare inte får montera fysiska externa media. |
| Aktivera säkerhetskopieringstjänst | Säkerhetskopieringstjänsten hanterar alla mekanismer för säkerhetskopiering och återställning på enheten. Om du anger false förhindras att data säkerhetskopieras eller återställs. Säkerhetskopieringstjänsten är avstängd som standard. Kräver Android 8.0 |
| Aktivera USB-masslagring | Aktiverar användning av USB Mass Storage. |

| Tangentbord | |
|---|---|
| Avvisa autofyllning | Anger om en användare inte får använda Autofyll Services. Kräver Android 8.0 |
| Förbjud kopiera och klistra in mellan profiler | Anger om det som kopieras i urklippet i den här profilen kan klistras in i relaterade profiler. |

| Ljud | |
|---|---|
| Avslå volymjustering | Anger om en användare inte får justera mastervolymen. |
| Avvisa Stäng av mikrofonen | Anger om en användare inte får justera mikrofonens volym. |
| Mute-enhet | Mute-enhet. |

## Certifikathantering

Här kan du distribuera Trusted Certificates och Identity Certificates till dina enheter.

Android 8 eller senare krävs för att distribuera Trusted Certificates och Android 9 eller senare krävs för att distribuera Identity Certificates.


Med "+" kan du lägga till flera certifikat.

Betrodda certifikat måste vara i PEM-format.

Identitetscertifikaten måste vara i PKCS12-format

# Hantering av anslutningar

## Wifi

För denna inställning, utför förkonfigurationen av slutanvändarens enheter, för åtkomst till intern åtkomst
Punkter

| | |
|---|---|
| Identifierare för tjänsteuppsättning (SSID) | SSID för det nätverk som ska anslutas |
| Dolda nätverk | Aktivera, om AP:n inte sänder SSID |

## Typ av säkerhet

Fastställ AP:ns säkerhetstyp

### WEP

| | |
|---|---|
| Lösenord | Lösenord för AP:n |

### WPA/WPA2

| | |
|---|---|
| Lösenord | Lösenord för AP:n |

## 802.1x EAP

| **EAP-metod** |
|---|

| | | |
|---|---|---|
| PWD | Identitet | Identitet |
| | Lösenord | Lösenord |

| | | | |
|---|---|---|---|
| PEAP | Fas 2 autentiseringsprotokoll | ingen | Inget ytterligare protokoll |
| | | MSCHAPV2 | MSCHAPV2-protokoll |
| | | GTC | GTC-protokoll |
| | CA-certifikat | CA-certifikat | |
| | Identitet | Identitet | |
| | Anonym identitet | Anonym identitet | |
| | Lösenord | Lösenord | |

| | | | |
|---|---|---|---|
| TTLS | Fas 2 autentiseringsprotokoll | ingen | Inget ytterligare protokoll |
| | | PAP | PAP-protokoll |
| | | MSCHAP | MSCHAP-protokoll |
| | | MSCHAPV2 | MSCHAPV2-protokoll |
| | | GTC | GTC-protokoll |
| | CA-certifikat | CA-certifikat | |
| | Identitet | Identitet | |
| | Anonym identitet | Anonym identitet | |
| | Lösenord | Lösenord | |

| | | |
|---|---|---|
| TLS | CA-certifikat | CA-certifikat |
| | Identitet | Identitet |
| | Lösenord | Lösenord |

# VPN

| | |
|---|---|
| Namn på anslutning | Namn på VPN-anslutningen |

## VPN-typ

### VPN

| **VPN-klient** |
|---|

| AppTec360 VPN-klient | |
|---|---|
| Gateway-konfiguration | Välj VPN-konfiguration för Gateway (se **Allmänna inställningar > Universal Gateway > VPN-inställningar**) |
| Alltid på VPN | Aktivera Native Lockdown |
| Aktivera AppTec360 Lockdown | Aktivera AppTec360 Lockdown |

| | | | |
|---|---|---|---|
| Inbyggd (endast tillgänglig på Samsung-enheter) | | | |
| Typ av anslutning | PPTP | Server | Server |
| | | Aktivera PPTP-kryptering | Aktivera PPTP-kryptering |
| | L2TP / IPSec PSK | Server | Server |
| | | IPSec Förhandsdelad nyckel | IPSec Förhandsdelad nyckel |
| | | Aktivera L2TP-hemlighet | Aktivera L2TP-hemlighet |
| | | L2TP-hemlighet | L2TP-hemlighet |
| | IPSec XAuth PSK | Server | Server |
| | | IPSec-identifierare | IPSec-identifierare |
| | | IPSec Förhandsdelad nyckel | IPSec Förhandsdelad nyckel |
| DNS-sökning Domäner | DNS-sökning Domäner | | |
| Expertinställningar | DNS-servrar | DNS-servrar | |
| | Vidarebefordran av rutter | Vidarebefordran av rutter | |

| | | |
|---|---|---|
| Öppet VPN | | |
| Server | Server | |
| OpenVPN-profil | OpenVPN-profil | |
| OpenVPN-app | OpenVPN för Android (rekommenderas) | |
| | Anslut till OpenVPN | |
| Expertinställningar | DNS-servrar | DNS-servrar |
| | Vidarebefordran av rutter | Vidarebefordran av rutter |

| Samsung / Starka svanen | | | |
|---|---|---|---|
| Typ av anslutning | PPTP | Server | Server |
| | | Användarnamn | Användarnamn |
| | | Lösenord | Lösenord |
| | | Aktivera PPTP-kryptering | Aktivera PPTP-kryptering |
| | L2TP / IPSec PSK | Server | Server |
| | | IPSec Förhandsdelad nyckel | IPSec Förhandsdelad nyckel |
| | | Användarnamn | Användarnamn |
| | | Lösenord | Lösenord |
| | | Aktivera L2TP-hemlighet | L2TP-hemlighet |
| | IPSec XAuth PSK | Server | Server |
| | | IPSec-identifierare | IPSec-identifierare |
| | | IPSec Förhandsdelad nyckel | IPSec Förhandsdelad nyckel |
| | | Användarnamn | Användarnamn |
| | | Lösenord | Lösenord |
| Expertinställningar | DNS-servrar | DNS-servrar | |
| | Vidarebefordran av rutter | Vidarebefordran av rutter | |

| Cisco Any Connect | | |
|---|---|---|
| Server | Server | |
| Certifikatläge | Inaktiverad | Inaktiverad |
| | Automatisk | Automatisk |
| Expertinställningar | DNS-servrar | DNS-servrar |
| | Vidarebefordran av rutter | Vidarebefordran av rutter |

## VPN per app

| **VPN-klient** |
|---|

| AppTec360 VPN-klient | | |
|---|---|---|
| Gateway-konfiguration | Välj VPN-konfiguration för Gateway (se **Allmänna inställningar > Universal Gateway > VPN-inställningar**) | |
| VPN-appar | VPN-appar | |
| Alltid på VPN | Aktivera Native Lockdown | Alltid på VPN |
| Aktivera AppTec360 Lockdown | Aktivera AppTec360 Lockdown | |

| | | | |
|---|---|---|---|
| Samsung / Starka svanen | | | |
| Typ av anslutning | PPTP | Server | Server |
| | | VPN-appar | VPN-appar |
| | | Användarnamn | Användarnamn |
| | | Lösenord | Lösenord |
| | | Aktivera PPTP-kryptering | Aktivera PPTP-kryptering |
| | L2TP / IPSec PSK | Server | Server |
| | | VPN-appar | VPN-appar |
| | | IPSec Förhandsdelad nyckel | IPSec Förhandsdelad nyckel |
| | | Användarnamn | Användarnamn |
| | | Lösenord | Lösenord |
| | | Aktivera L2TP-hemlighet | L2TP-hemlighet |
| | IPSec XAuth PSK | Server | Server |
| | | VPN-appar | VPN-appar |
| | | IPSec-identifierare | IPSec-identifierare |
| | | IPSec Förhandsdelad nyckel | IPSec Förhandsdelad nyckel |
| | | Användarnamn | Användarnamn |
| | | Lösenord | Lösenord |
| Expertinställningar | DNS-servrar | DNS-servrar | |
| | Vidarebefordran av rutter | Vidarebefordran av rutter | |

## Begränsningar

Här kan du ställa in begränsningarna i samband med anslutningshanteringen.

| | |
|---|---|
| Tillåt data-roaming | Tillåt mobildata vid roaming |
| Tvinga fram dataroaming | Om den är aktiverad är roaming för mobildata permanent aktiverad (rekommenderas inte!)<br>Denna inställning skriver över inställningen "Allow Data Roaming"! |
| Följande inställningar är endast tillgängliga för SAFE 2.x eller senare | |
| Tillåt endast nödsamtal | Tillåt endast nödsamtal |
| Tillåt WiFi | Tillåt WiFi |
| Miniminivå för säkerhet i WiFi-nätverk | WiFi-nätverkets lägsta säkerhetsnivå<br>Öppet = alla typer av WiFi är tillåtna |
| Förbjuda användare att lägga till WiFi-nätverk | Användaren kan inte själv lägga till ett WiFi-nätverk<br>Denna inställning är endast möjlig om en WiFi-profil har definierats under "Connection Management" |
| Tillåt SMS & MMS | All = All SMS- och MMS-trafik är tillåten<br>Incoming SMS Only = Endast inkommande SMS-meddelanden tillåts<br>Outgoing SMS Only = Endast utgående SMS-meddelanden tillåts<br>None = Ingen SMS/MMS-trafik är tillåten |
| Tillåt synkronisering under roaming | Tillåt synkronisering under roaming<br>På = aktiverad<br>Av = avaktiverad<br>Användarval = användarens val |
| Tillåt röstroaming | Tillåt röstroaming<br>På = aktiverad<br>Av = avaktiverad<br>User Choice = användarens val |
| Använd systemets http-proxyserver | Användningen av en HTTP-proxyserver, som tillhandahålls av systemets inställningar i Inställningar, är beroende av det anslutna nätverket (WiFi eller APN) |

# PIM-hantering

## Gmail Exchange

Information: Den här konfigurationen kommer att tillämpas på Gmail-appen. Du måste därför godkänna och installera Gmail.

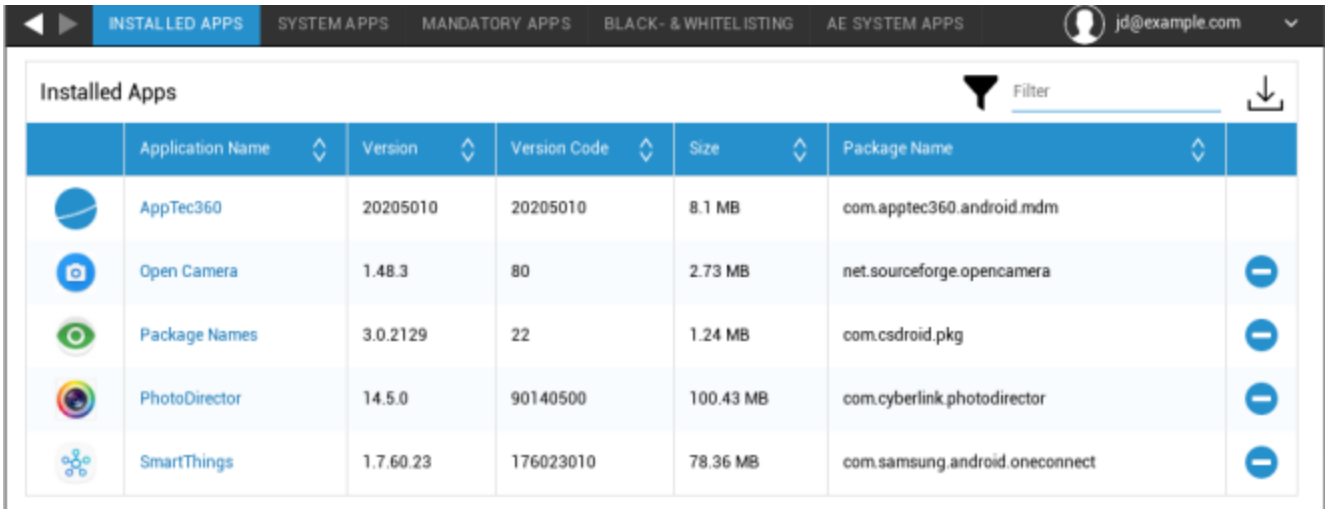
| | |
|---|---|
| E-postadress | Den angivna användarens e-postadress<br>Observera "platshållarna", som du kan använda för att arbeta med referenser och du behöver inte utföra ändringar manuellt på varje enhet<br>Med ett klick kan du visa dem för dig själv |
| Serverns värdnamn | Serveradress till dina Exchange-servrar |
| Inloggningsnamn | Inloggningsnamnet för respektive slutanvändarenhet, observera även "Platshållare här |
| Underskrift | En signatur kan bifogas (Tips: Vissa enheter kräver HTML-formatering för signaturen) |
| Antal föregående dagar att synkronisera | Antal dagar som avgör när e-postmeddelanden synkroniseras tillbaka |
| Enhetens identifierare | En sträng som innehåller EAS DeviceID. Detta är en del av EAS-protokollet och behövs i vissa områden |
| Använd SSL (Secure Sockets Layer) | Använd en SSL-anslutning |
| Acceptera alla certifikat | Alla certifikat accepteras. Välj detta alternativ om Exchange Server använder ett självsignerat certifikat |

# App-hantering

## Enterprise App Manager

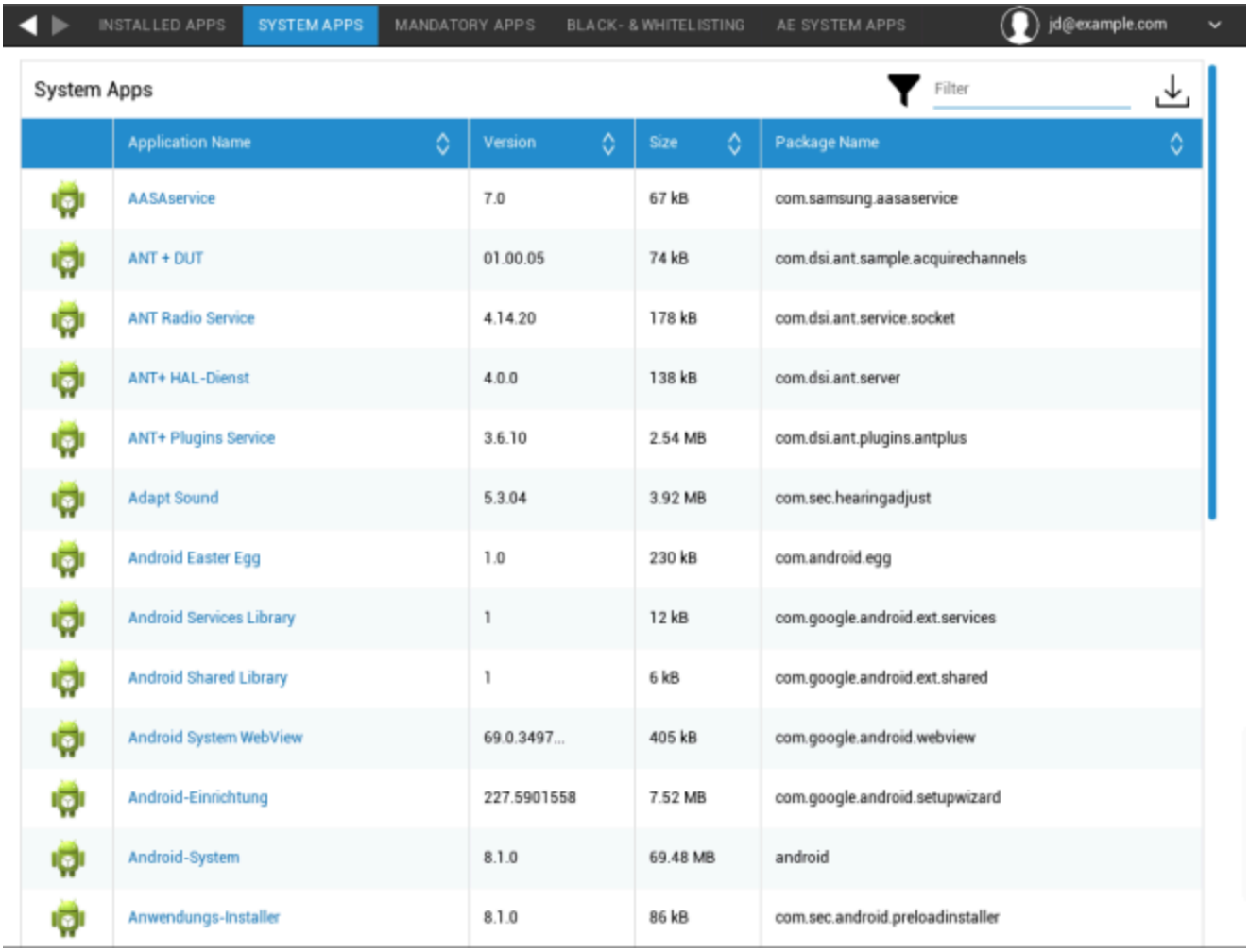
### Installerade appar (endast på enhetsnivå)

Här visas alla appar som för närvarande är installerade på slutanvändarens enhet.



## Systemappar (endast på enhetsnivå)

Under "System Apps" listas alla appar och tjänster som redan har installerats på slutanvändarens enhet av enhetens tillverkare.

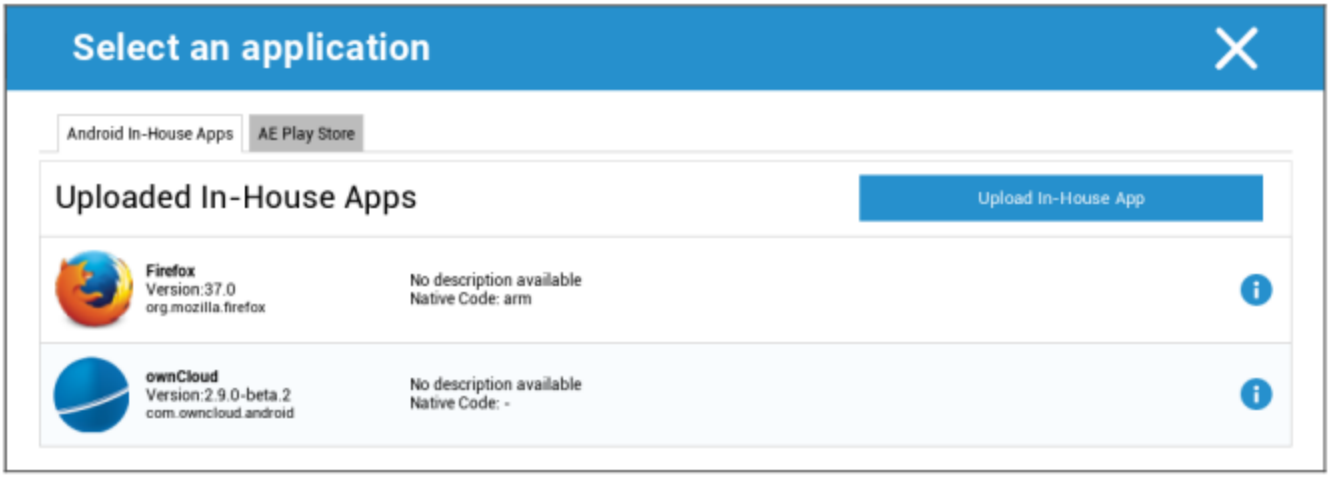


## Obligatoriska appar

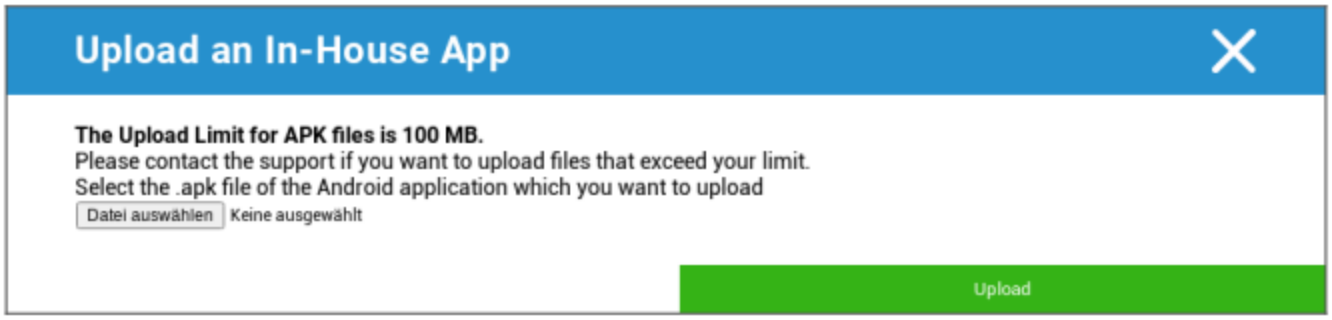
Under Obligatoriska appar kan du ange de obligatoriska appar som krävs. Användaren kommer kontinuerligt att uppmanas att installera den angivna appen.

Med hjälp av kan den obligatoriska appen definieras.

Detta kan vara en intern app från "Android In-House Apps", som du har laddat upp i Allmänna inställningar.

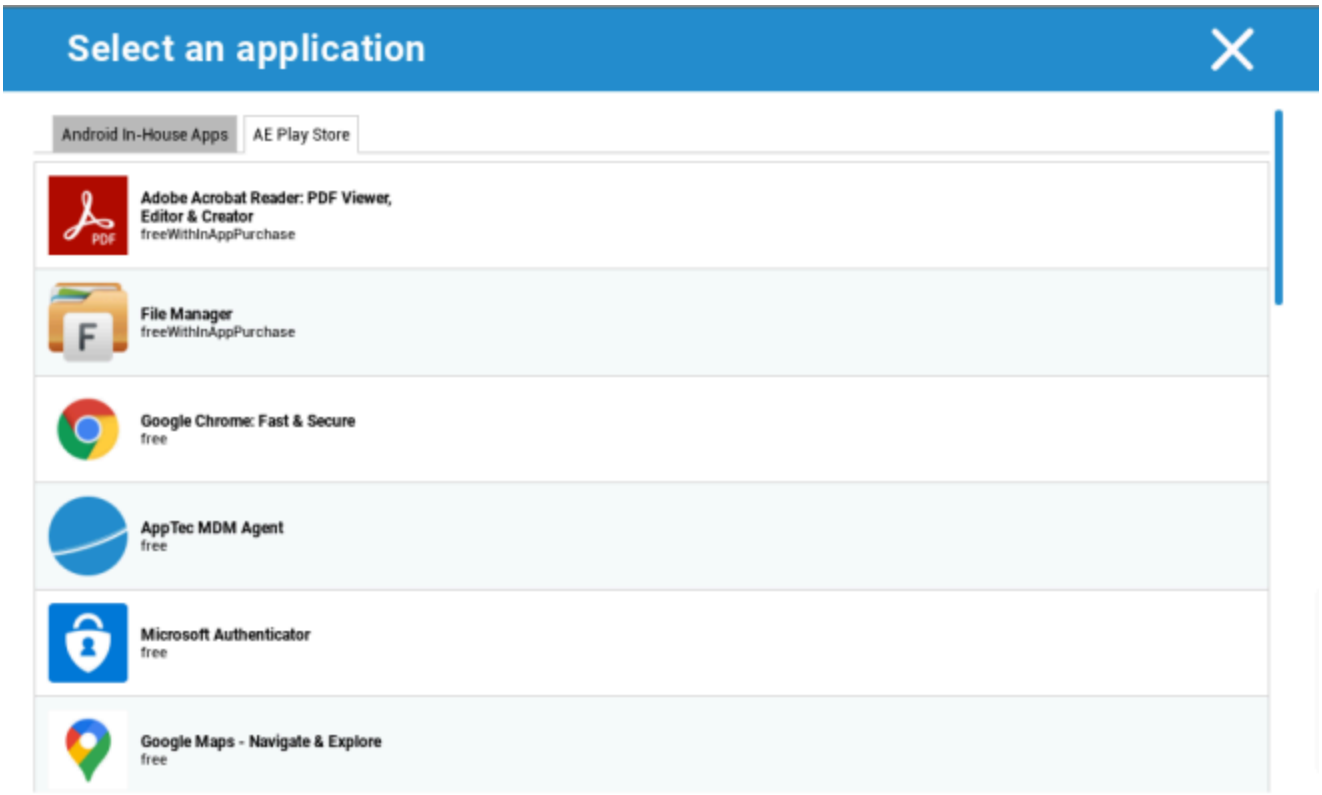



Du kan också direkt välja och ladda upp en apk-fil med "Upload In-House App".




Om du installerar en In-House App har du möjlighet att aktivera "Keep up to date". Om detta är aktiverat och du har definierat en nyare version i In-House App DB, kommer appen att uppdateras på enheten.

Eller så kan det vara en "AE Play Store"-app från Google Work Play Store.




Endast godkända "AE Play Store Apps" kommer att visas på den här fliken.

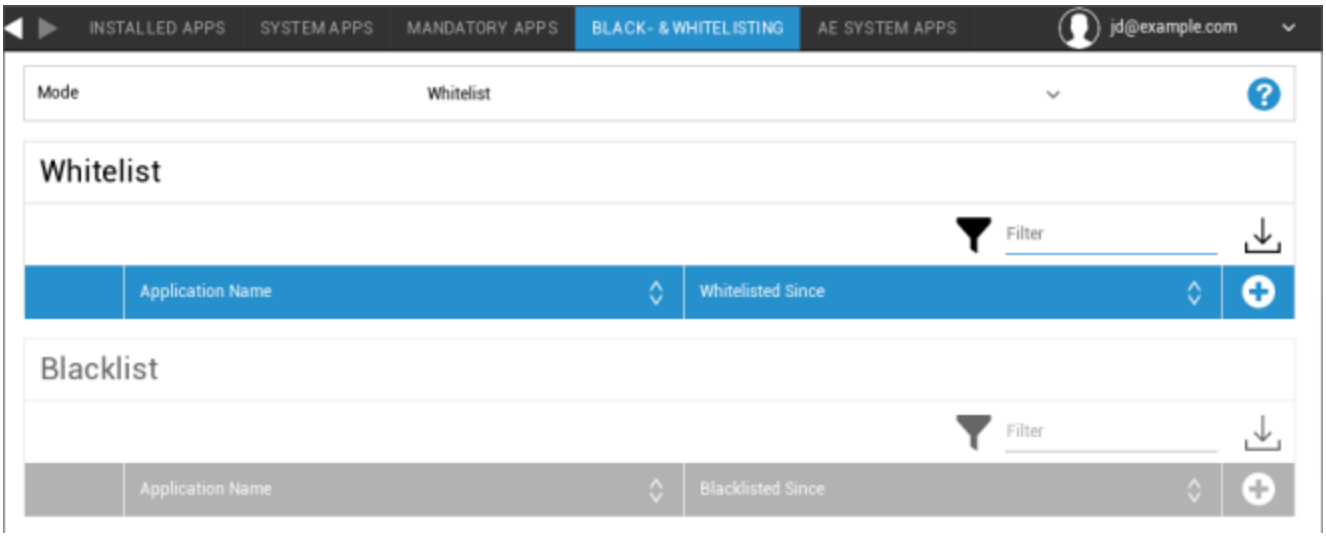
För att godkänna en "AE Play Store-app", gå till "Allmänna inställningar" > "Apphantering" > "AE Play

Store" och lägg till en app via knappen som kommer att omdirigera dig till fliken "Play Store Apps" (eller så kan du
direkt gå till fliken "Play Store Apps").

På fliken "Play Store Apps" kan du söka efter appar. När du klickar på en app öppnas appsidan och här kan du godkänna appen genom att klicka på "Approve".

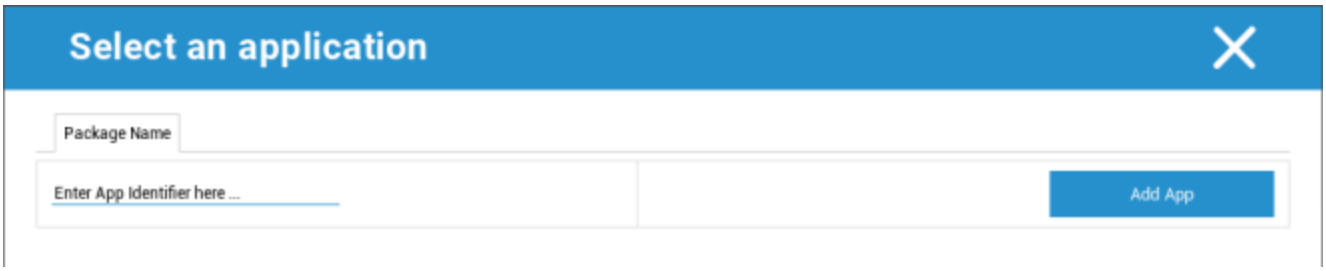
## Svart- och vitlistning

Under "Black- & Whitelisting" kan du välja mellan läget "Whitelist" och läget "Blacklist".



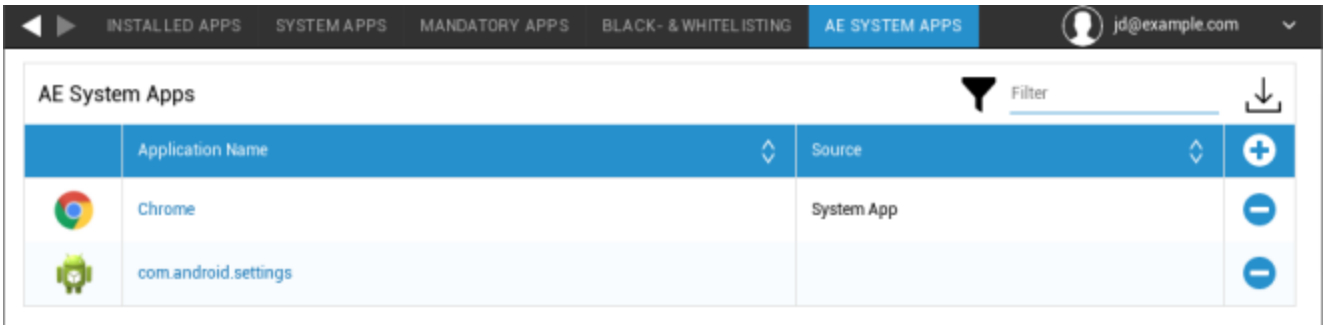

| | |
|---|---|
| Vitlista | Endast appar och tjänster som läggs till i listan kan installeras på slutanvändarens enhet. Om dessa redan är förinstallerade på slutanvändarens enhet kommer de att aktiveras och ställas in så att användaren kan köra dem. |
| | Alla andra appar som inte läggs till i listan kan inte installeras på slutanvändarens enhet. Om dessa redan är förinstallerade på slutanvändarens enhet kommer de att avaktiveras och ställas in så att användaren inte kan köra dem. |
| Svarta listan | Appar och tjänster som läggs till i listan kan inte installeras på slutanvändarens enhet. Om dessa redan är förinstallerade på slutanvändarens enhet kommer de att avaktiveras och ställas in så att användaren inte kan köra dem. |
| | Alla andra appar som inte har lagts till i listan kan installeras på slutanvändarens enhet. Om dessa redan är förinstallerade på slutanvändarens enhet kommer de att aktiveras och ställas in så att användaren kan köra dem. |

Via , lägger du till ytterligare appar eller tjänster i den lista som används för tillfället.
Via , lägger du till ytterligare appar eller tjänster i den lista som inte används för tillfället.
Du kan definiera ett "Packagename":

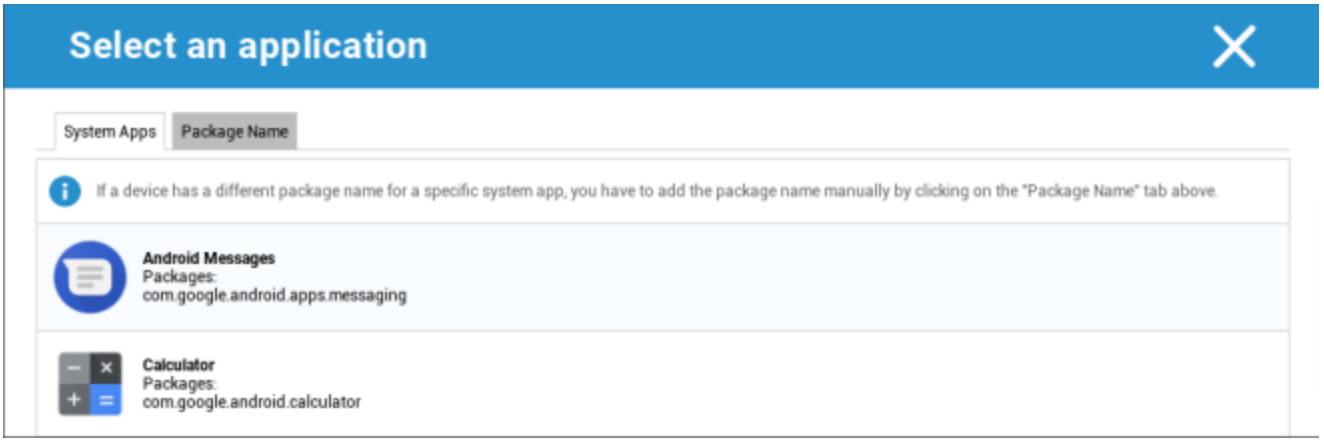

Select an application
Package Name
Enter App Identifier here ...
Add App

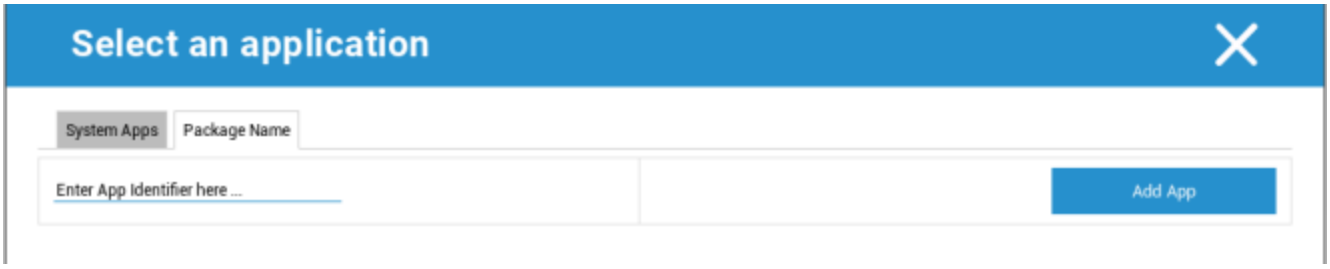
## Appar för AE-system

Här kan du definiera en lista som innehåller specifika systemappar som ska aktiveras på enheterna.




Om du klickar på knappen kan du välja från en lista med möjliga systemprogram som tillhandahålls av Google eller direkt ange paketnamnet på ett systemprogram som ska aktiveras.




Tänk på att systemapparna i listan från Google endast är appar som kan vara systemappar, men som inte nödvändigtvis måste vara systemappar på dina enheter.

Den här listan gäller dock bara appar som redan är förinstallerade.

Om du lägger till appar som inte är förinstallerade på dina enheter påverkas inte dina enheter, oavsett om appen finns med i listan från Google eller om appens paketnamn anges direkt.

# Begränsningar och inställningar

## Inställningar för apphantering

Här kan du konfigurera enhetens beteende när det gäller appuppdateringar.

| | |
|---|---|
| Frekvens för uppdateringskontroll | Ange i vilket intervall AppTec360 Client ska söka efter appuppdateringar. Standardvärdet är 24 timmar. |
| Tröskelvärde för Wi-Fi | Appar som är större än den angivna storleken laddas ner via Wi-Fi. Om "Endast Wi-Fi" väljs laddas alla appar ner via Wi-Fi. |

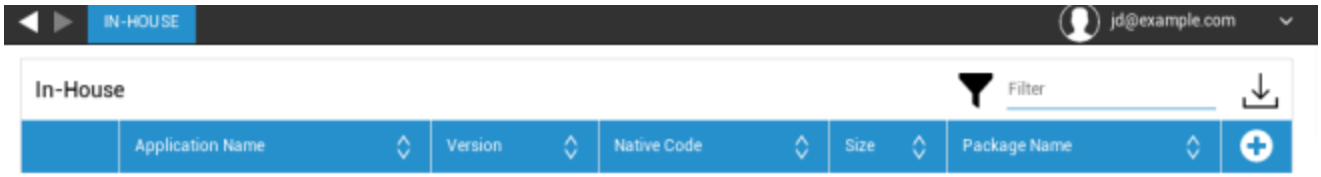
# App Store för företag

## Internt

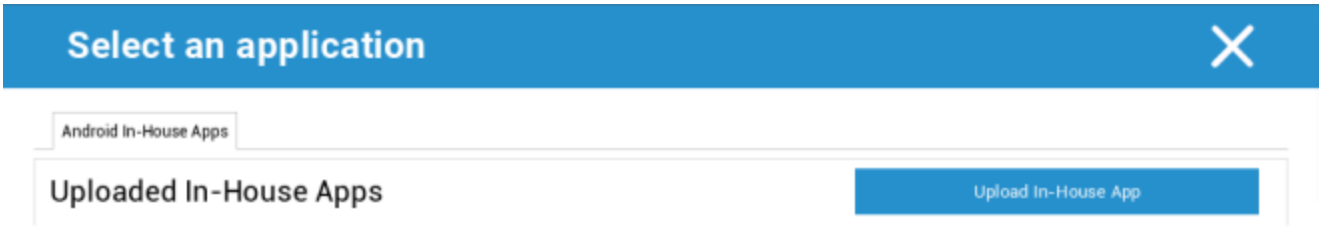
Under punkten "In-House" kan du ladda upp och distribuera internt utvecklade appar.

Med symbolen kan du distribuera ytterligare In-House Apps.

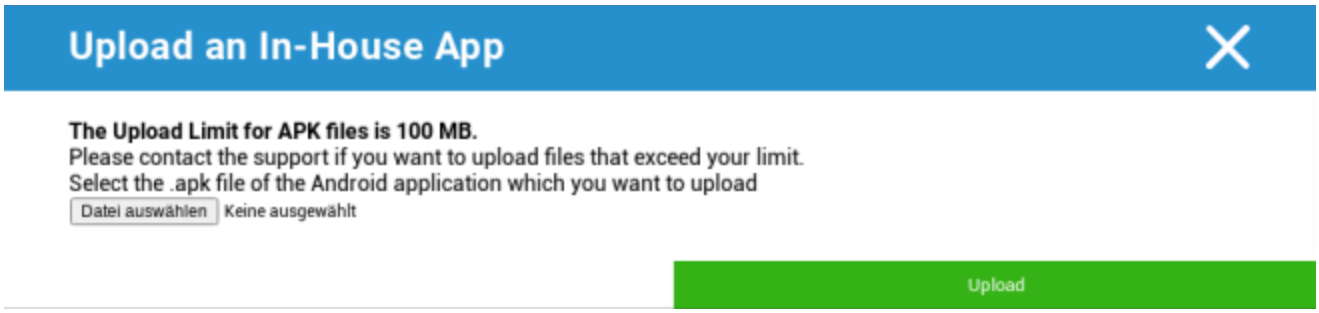
Om du installerar en In-House App har du möjlighet att aktivera "Keep up to date". Om är aktiverat och du har definierat en nyare version i In-House App DB, kommer appen att uppdateras på enheten.



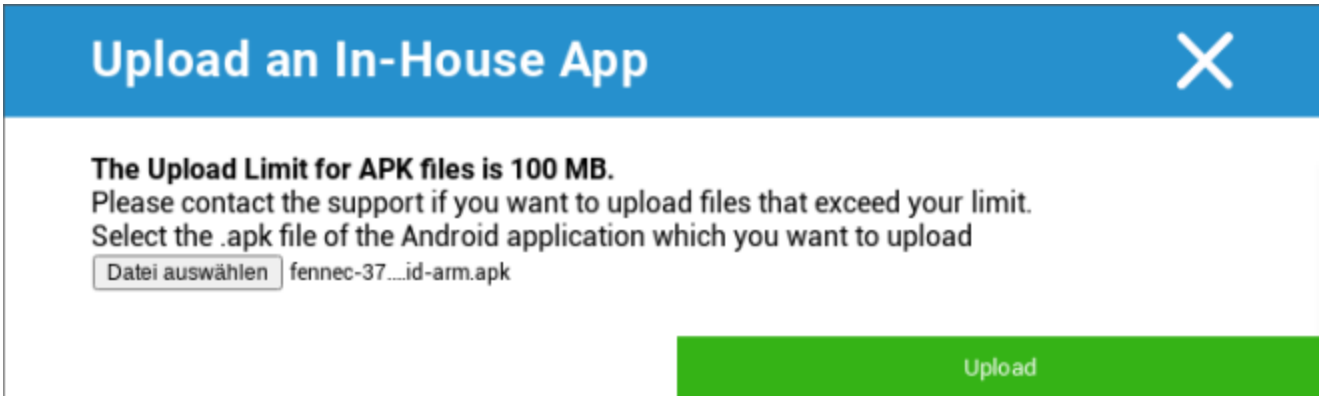

Om du inte har distribuerat In-House Apps kommer du att få följande översikt:



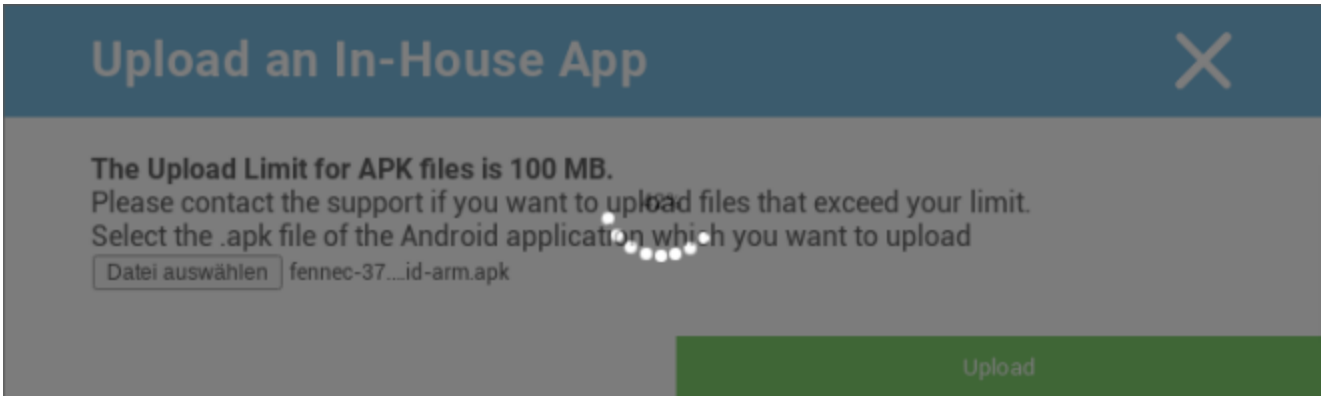
För detta klickar du på "Upload In-House App", du kommer då att få följande översikt:




Välj nu med "Sök ..." en .apk-fil och klicka sedan på "Ladda upp".




Din app kommer nu att laddas upp, i mitten av cirkeln ser du en procentindikator, som visar hur stor del av din app som redan har laddats upp.



Om uppladdningen av din In-House App har lyckats, kan du hitta den uppladdade appen i din App Catalog.

Användaren har nu möjlighet att se och installera denna app i AppTec360 Store på slutanvändarens enhet, under kategorin "In-House".


Eftersom det inte rör sig om en Google PlayStore-app behöver användaren inte ha ett lagrat Google ID på sin respektive slutanvändarenhet.

## Play Store för företag

### AE Play Butik

Här kan du lägga till appar i Android Enterprise Playstore. Observera att du måste godkänna Apps med ditt AE Administrator-konto innan du kan lägga till dem.

För godkännande av en app, se instruktionerna i Obligatoriska appar.

# Kioskläge och startprogram

## Kiosk-läge

Kioskläget gör att du kan fördefiniera en app eller en URL. Då kommer det endast att vara möjligt att köra/besöka denna app eller URL på

.

På samma sätt kan olika hårdvaruknappar avaktiveras i olika Kiosk Mode.

| | |
|---|---|
| Automatisk start | Startar automatiskt Kiosk-läget så snart profilen når slutanvändarens enhet |
| Schemalagt kioskläge? | Du kan planera en tid för kioskläget, som sedan startar och avslutas automatiskt vid en tidpunkt som du själv bestämmer |
| Starttid | Starttidpunkt |
| Tid i minuter | Tid i minuter, efter vilken Kiosk Mode ska avslutas igen |

| **Tillämpningstyp** |
|---|

| | |
|---|---|
| En enda app | Om du vill starta appen i kioskläge väljer du Package" under "Application Type" |
| Kiosk-applikation | Klicka här för att välja en app som ska startas i Kiosk Mode<br>Du kommer att hitta den vanliga App Management-översikten<br>Du kan välja mellan en "Google Play Store", "Android In-House Apps" och ett "Packagename" |

| Tillämpningstyp |
|---|

| | |
|---|---|
| URL | Om du vill starta en URL i Kiosk Mode väljer du "URL" under "Application Type"<br>Ange sedan önskad URL-adress |
| Rensa webbläsaren efter inaktivitet | Här kan du definiera ett tidsintervall i minuter, efter vilket kioskläget ska startas om |
| Rensa webbcache och cookies | Om du aktiverar den här funktionen kommer webbcachen (cookies och cachade bilder) att raderas efter en omstart av kioskläget |
| Policy för samma ursprung | Om denna funktion är aktiv kan användaren bara surfa på undersidorna till en definierad URL<br>Du har till exempel definierat följande URL:www.mypage.com Sedan kan användaren surfa på: www.mypage.com/subpage |
| Vitlistade webbadresser | Här kan du upprätthålla en vitlista, alla dessa webbadresser är tillåtna<br>Högst 1 URL per rad<br>En URL måste börja med http:/ eller https:// |
| Svartlistade webbadresser | Här kan du upprätthålla en svart lista, alla dessa webbadresser är inte tillåtna<br>Högst 1 URL per rad<br>En URL måste börja med http:/ eller https:// |
| Skärmorientering | Denna inställning avser skärmens justeringar<br>Automatisk = automatisk<br>Stående = vertikalt format<br>Landscape = liggande läge |

| | |
|---|---|
| Multi App | Om du väljer kioskläget "Multi App" kommer användningen av AppTec360 Launcher att vara obligatorisk. |
| Appar | Applikation: Välj en Playstore eller en egen app som kioskapplikation. Det är också möjligt att ange ett paketnamn. Den valda kioskapplikationen måste vara installerad på enheten. Kom ihåg att ställa in Kiosk Application som obligatorisk.<br>Genväg på startskärmen: Om inställningen är "På" skapas en genväg på hemskärmen. Om inställningen är "Av" kommer appen fortfarande att visas i applistan. |

| | |
|---|---|
| Lösenord för utgång Aktiverad | Om du aktiverar den här funktionen är det möjligt för användaren att avsluta kioskläget med ett lösenord som du har fördefinierat |
| Avsluta lösenord | Detta är det lösenord som du har angett i förväg |
| Automatisk kollaps av statusfältet | Om det är aktiverat kommer statusfältet automatiskt att vara kollapsat. Med det alternativet kan användare se informationen i statusfältet, men inte komma åt dess funktioner |
| Inaktivera statusfältet | Statusfältet innehåller aviseringar, genvägar och information. Endast tillgängligt för Samsung-enheter med SAFE 4.0 eller senare. |
| Inaktivera volymknappar | Inaktivera volymknappar (endast tillgängligt på Samsung-enheter med SAFE 3.0 eller högre) |
| Inaktivera på/av-omkopplare | Inaktivera På/Av-omkopplaren (endast tillgänglig på Samsung-enheter med SAFE 3.0 eller högre) |
| Inaktivera hemknappen | Inaktivera hemknappen. Om denna funktion har aktiverats, kan Kiosk Mode endast avslutas i AppTec360 Console<br>(endast tillgängligt på Samsung-enheter med SAFE 3.0 eller högre) |
| Inaktivera navigeringsfältet | Med denna funktion kan du inaktivera navigeringsfältet (Tillbaka/Meny)<br>Om denna funktion har aktiverats, kan Kiosk Mode endast avslutas i AppTec360 Console<br>(endast tillgängligt på Samsung-enheter med SAFE 3.0 eller högre) |

## AppTec360 Launcher

| | |
|---|---|
| Aktivera AppTec360 Launcher | På: Aktiverar AppTec360 Launcher. Användaren måste ställa in den som standard Launcher en gång.<br>Obs: Om kioskläget är aktiverat och kioskläget är inställt på "Multi App", kommer användningen av AppTec360 launcher att vara obligatorisk. |
| Stora ikoner | På: Visar en större version av appikonerna i startprogrammet |
| Dölj AppTec360 App-ikonen | På: Döljer AppTec360-appen helt och hållet |
| Dölj AppTec360 Butiksikon | På: Döljer AppTec360 Enterprise AppStore helt och hållet |

## AppTec360 Inställningar

| | |
|---|---|
| Aktivera AppTec360 Inställningar App | AppTec360 Settings App ger kontroll över WiFi- och Bluetooth-anslutningar |
| Aktivera inställningar i Multi App<br>Kiosk-läge | Om aktiverat, kan användare komma åt AppTec360 Settings App medan Multi App Kiosk Mode är aktivt |

# Fjärrkontroll

## Splashtop

För att starta en fjärrkontrollsession för din enhet måste appen "Splashtop Streamer" installeras på enheten genom att lägga till appen i **Apphantering** → **Enterprise App Manager** → **Obligatoriska** appar.

Därefter konfigurerar du följande inställningar för Splashtop:

| | |
|---|---|
| Aktivera Splashtop | Om det är aktiverat kommer AppTec360 att konfigurera Splashtop-appen för att tillåta fjärrstyrning |
| Distribuera kod | Gå till https://my.splashtop.com och logga in på ditt Splashtop-konto. Klicka på "Add Computer" och kopiera den 12-siffriga deploy-koden från den sida som visas. |
| Ange Gateway för anpassad distribution? | Distribuera Gateway |
| Distribuera Gateway-domän/värd | Distribuera Gateway |
| Verifiering av certifikat | Verifiering av certifikat |

Sedan kan du använda alternativet Splashtop Remote Control i snabbmenyn (kugghjulet bredvid sökfältet när enheten är markerad eller högerklicka på enheten i trädet) för att starta fjärrkontrollsessionen.

## TeamViewer

För att starta en fjärrkontrollsession för din enhet måste appen "TeamViewer QuickSupport" installeras på enheten genom att lägga till appen i **Apphantering** → **Enterprise App Manager** → **Obligatoriska** appar.

Sedan kan du använda alternativet **TeamViewer Remote Control** i snabbmenyn (kugghjulet bredvid sökfältet när enheten är markerad eller högerklicka på enheten i trädet) för att starta fjärrkontrollsessionen.

# Innehållshantering

## Innehållsruta

Här kan du aktivera ContentBox.

Så snart du sätter "Enable ContentBox" till "On" kommer en separat ContentBox-app att installeras automatiskt på slutanvändarens enhet.

## Säker webbläsare

Här kan du konfigurera inställningar för AppTec360 Secure Browser.

Så snart du ställer in "Secure Browser" på "On" kommer en separat webbläsarapplikation att installeras automatiskt på slutanvändarens enhet.

| | |
|---|---|
| Kräv lösenord | Kräv att användaren ställer in och använder ett lösenord för att få tillgång till webbläsaren. |
| Minimal längd på lösenord som krävs | Ange det antal tecken som krävs för lösenordet |
| Erforderlig lösenordskvalitet | Ställ in önskad lösenordskvalitet |
| Begränsa nedladdningar / Öppna i | |
| Begränsa uppladdningar | |
| Ladda upp vitlista | En lista med URL:er som alltid ska tillåtas att laddas upp. |
| Tillåt kopiering | Tillåt kopiering, klippning eller delning av text på webbsidorna. |
| Tillåt skärmupptagning | Tillåt att ta skärmdumpar. |
| Frekvens för rensning av data | Välj med vilken frekvens ALL användardata (historik, cache etc.) ska tas bort automatiskt. |
| Bokmärken för företag | Bokmärkena kommer att visas i mappen "Företagsbokmärken" i webbläsarens bokmärken.<br>De kan inte redigeras av användaren. |
| Dölj adressfältet | |
| Vitlistning i webbläsaren (utan Universal Gateway) | Aktiverar vitlistning av URL:er på klientsidan.<br>• Företagets bokmärken är alltid vitlistade<br>• Stöd för endast 100 webbadresser<br>• Använd Universal Gateway för obegränsad svart- och vitlistning |
| Vitlistade webbadresser | En lista över tillåtna webbadresser. |
| Gateway-baserad svart- och vitlistning | Svartlistning har följande krav:<br>• En fungerande AppTec360 Universal Gateway ("Allmänna inställningar" → "Universal Gateway") |

| | |
|---|---|
| | • En fungerande VPN-konfiguration med en angiven DNS-server ("Allmänna inställningar" → "Universal Gateway" → "VPN-inställningar")<br>• En konfiguration för svart lista ("Allmänna inställningar" → "Universal Gateway" → "Svart lista för domäner")<br>• En giltig VPN-anslutning i profilen ("Anslutningshantering" → "VPN") |

# Ytterligare API

## Samsung KNOX

### Begränsningar

| | |
|---|---|
| Tillåt SD-kort | |
| Tillåt skrivning av SD-kort | |
| Tillåt skärmupptagning | |
| Tillåt urklipp | |
| Säkerhetskopiera inställningar och appdata i Google Cloud | |
| Återställ inställningar från Google Cloud när du installerar om en app | |
| Tillåt USB-felsökning | |
| Tillåt Googles kraschrapport | |
| Tillåt fabriksåterställning | |
| Tillåt OTA-uppgradering | |
| Tillåt USB-hostlagring | Om den är aktiverad kan användaren ansluta en pennstation (bärbar USB-lagring), extern HD eller SD-kortläsare (Secure Digital) och den monteras som en lagringsenhet på enheten. |
| Tillåt USB Media Player (MTP,PTP) | |
| Tillåt mikrofon | Inaktiverar mikrofonen för tredjepartsapplikationer |
| Tillåt NFC (Near Field Communication) | |
| Tillåt okända källor (APK Sideloading) | Om den är aktiverad tillåts sidoladdning av appar (APK-filer). När den här inställningen är inaktiverad måste användaren aktivera den manuellt när du tillåter installation av APK:er från okända källor. |
| Tillåt skapande av användare | Om det är aktiverat får användaren skapa flera konton på enheten, t.ex. gästkonton |

## E-post

| | |
|---|---|
| E-postadress | |
| Protokoll för inkommande server | |
| Adress till inkommande server | |
| Port för inkommande server | |
| Inloggning/användarnamn för inkommande server | |
| Lösenord för inkommande server | |
| Inkommande server använder SSL | |
| Inkommande server använder TLS | |
| Inkommande server accepterar alla certifikat | |
| Protokoll för utgående server | |
| Utgående serveradress | |
| Utgående serverport | |
| Utgående server använder extra autentiseringsuppgifter | Om den inaktiveras använder systemet de inkommande autentiseringsuppgifterna även för den utgående servern. |
| Inloggning/användarnamn för utgående server | |
| Lösenord för utgående server | |
| Utgående server använder SSL | |
| Utgående server använder TLS | |
| Utgående server accepterar alla certifikat | |
| Ställ in signatur | |
| Underskrift | Obs: För vissa enheter måste signaturen anges i HTML-format. |
| Meddela användaren om mottagande av nytt eMail | |

## Utbyte

| | |
|---|---|
| E-postadress | |
| Serverns värdnamn | Värdnamnet på Exchange Server |
| Inloggningsnamn | Det användarnamn som används för att logga in på Exchange Server |
| Domän | Om en ACL Gateway konfiguration är aktiverad och fältet Domän inte är tomt kommer AppTec360 Universal Gateway att autentisera enheten med följande namn "Domän\Login namn |
| Lösenord | |
| Antal föregående dagar att synkronisera | |
| Frekvens för synkronisering av eMail | |
| Synkronisering under roaming | |
| Ställ in signatur | |
| Underskrift | Obs: För vissa enheter måste signaturen anges i HTML-format. |
| Standardkonto | |
| Använd SSL (Secure Sockets Layer) | |
| Använd TLS (Transport Layer Security) | |
| Acceptera alla certifikat | |

## APN

| | |
|---|---|
| APN-visningsnamn | |
| Namn på åtkomstpunkt | Namn på APN |
| Protokoll för utgående server | |
| MCC - Mobil landskod | Lämna tomt för att använda mmc för installerad SIM |
| MNC - Kod för mobilnät | Lämna tomt för att använda mnc för installerat SIM-kort |
| Serveradress | |
| Serverns portnummer | |
| Serverns proxy-adress | |
| Adress till MMS-server | Lämna tomt för standard |
| MMS-portnummer | Lämna tomt för standard |
| MMS-proxyadress | Lämna tomt för standard |
| Användarnamn | |
| Lösenord | |
| Typ av åtkomstpunkt | Accepterade typer är "default", "mms", "supl". |
| | Om null eller empty anges används som standard "default,supl,mms". |
| | Lämna tomt för standard. |
| Företrädesvis APN | |

## Bluetooth

| | |
|---|---|
| Tillåt enhetsidentifiering via Bluetooth | |
| Tillåt parkoppling med Bluetooth | |
| Tillåt Bluetooth-headset-enheter | |
| Tillåt handsfree-enheter från Bluetooth | |
| Tillåt Bluetooth A2DP-enheter | A2DP, Advanced Audio Distribution Profile, möjliggör ljudstreaming mellan enheter |
| Tillåt utgående samtal | |
| Tillåt dataöverföring via Bluetooth | |
| Tillåt Bluetooth-internetdelning | |
| Tillåt anslutning till dator via Bluetooth | |

## Anslutning

| | |
|---|---|
| Tillåt endast nödsamtalTillåt Wi-Fi | |
| Wi-Fi-nätverkets lägsta säkerhetsnivå | |
| Förbjud användaren att lägga till Wi-Fi-nätverk | Denna begränsning kan endast aktiveras om minst en aktiv Wi-Fi-profil har definierats under Connection Management |
| Tillåt SMS & MMS | |
| Tillåt synkronisering under roaming | |
| Tillåt röstroaming | |

# Android Enterprise – Fullt hanterad enhet med arbetsprofil (COPE)

## Allmän förklaring av COPE

COPE är en förkortning för **Corporate Owned Personally Enabled**.

COPE-läget gör att en Android-enhet kan registreras som en **Android Enterprise - Fullt hanterad enhet** med integrerad **Android Enterprise - Container-profil**.

Detta kan antingen vara en Android-enhet som redan är registrerad som en **Android Enterprise - Fully Managed Device** och på vilken Android **Enterprise - Container** dessutom är installerad, eller en nyregistrerad Android-enhet som är direkt registrerad som en Android **Enterprise - Fully Managed Device** tillsammans med **Android Enterprise - Container** ovanpå den.

COPE-läget är endast tillgängligt för enheter med Android 8, 9 och 10

## Konfiguration av profiler för COPE-enheter

Eftersom det inte finns någon konfigurationsprofil för COPE-läget i sig, är konfigurationen av **Android Enterprise - Fullt hanterad enhet** och **Android Enterprise - Container** uppdelad i två profiler inom COPE-profilen. Det är möjligt att växla mellan de två profilerna för konfigurationen av varje profil genom att klicka på respektive knapp till vänster i konsolen:


Båda profilerna kan konfigureras på det sätt som beskrivs för varje enskild profil:

**Android Enterprise - Fullt hanterad enhet**

**Android Enterprise - Container**

## Återgå till AE Fullständigt hanterad enhet

Profilen **Android Enterprise - Container** kan tas bort enligt beskrivningen i **Mobile Management**.

Genom att ta bort Container-profilen kommer COPE-profilen att omvandlas till en **Android Enterprise - Fully Managed Device-profil**.

# Android Enterprise – Konfiguration av behållare

Beroende på om du för närvarande har valt en grupprofil eller en enhet skiljer sig översikten och dess underpunkter åt - tänk på detta noga!

## Allmänt

### Profilöversikt (endast på profilnivå)

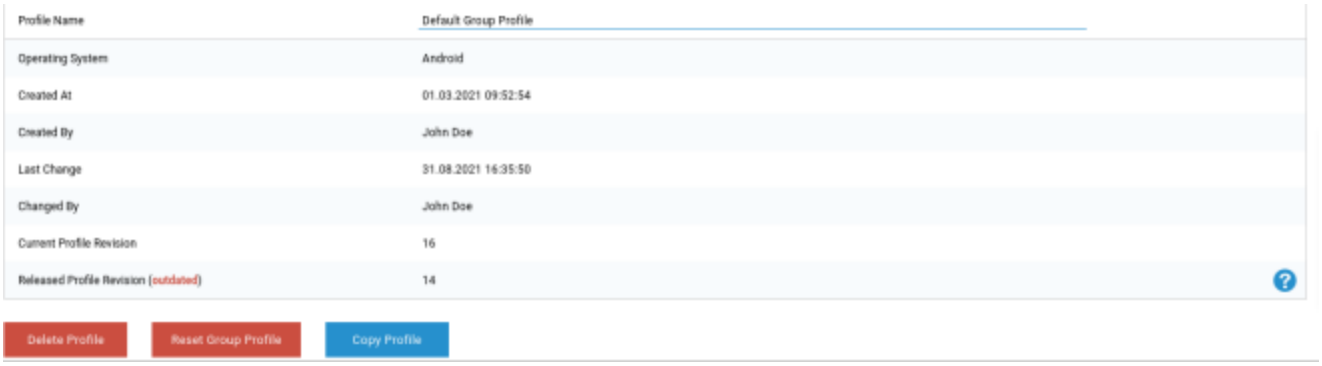
Om du befinner dig i en profil får du en kort översikt över profilen med avseende på namn, operativsystem, skapandedatum, författare etc.

| | |
|---|---|
| Profilens namn | Profilnamn - kan namnändras direkt här |
| Operativsystem | Giltigt operativsystem för profilen |
| Skapad vid | Datum för skapande |
| Skapad av | Skapad av |
| Sista förändringen | Senaste ändringsdatum |
| Förändrad av | Den användare som utförde de senaste ändringarna i den här profilen |
| Aktuell profil Revidering | Antal gånger profilen redan har uppdaterats |
| Utgiven Profil Revision | Antal gånger profilen redan har uppdaterats och har tilldelats enheter |

| | |
|---|---|
| Ta bort profil | Ta bort profil |
| Återställ grupprofil | Återställ grupprofil |
| Kopiera profil | Kopiera profil |

## Översikt över grupprofiler (endast på gruppnivå)

När du öppnar en grupprofil får du en snabb överblick över profilen.




| | |
|---|---|
| Profilens namn | Profilens namn (kan ändras här) |
| Operativsystem | Operativsystem som profilen är avsedd för |
| Skapad vid | Tidpunkt för skapelse |
| Skapad av | Skaparen av profilen |
| Sista förändringen | Tidpunkt för senaste ändring av profilen |
| Förändrad av | Konto som gjorde de senaste ändringarna |
| Aktuell profil Revidering | Revidering av sparat profiltillstånd |
| Utgiven Profil Revision | Tilldelad profilrevision ("Tilldela nu"). Om etiketten visar "(outdated)" bakom texten betyder det att du har sparat profilen men inte tilldelat den ännu, så enheterna kommer fortfarande att få en äldre version. |

## Enhetsöversikt (endast på enhetsnivå)

Om du befinner dig på en enhet kommer du att få en översiktlig sammanfattning av den valda enheten, följande finns här:

| | |
|---|---|
| Enhetens namn | Enhetens namn |
| Plats | Koordinater för platsen |
| Telefonnummer | Telefonnummer |
| Tilldelade Obligatoriska appar | Antal tilldelade obligatoriska appar |
| OS-version | Enhetens OS-version |
| Operativsystem | Operativsystem (Android Enterprise) |
| Serienummer | Enhetens serienummer |
| Ägande av enhet | Företagsenhet eller privat enhet |
| Enhetstyp | AE Arbetshanterad enhet |
| Rotad | Status, anger om enheten har rotats |
| Överensstämmande | I enlighet med riktlinjerna |
| IP-adress | Enhetens IP-adress |
| Senast sett | Tidpunkt då enheten senast var ansluten till AppTec |
| Sista knuffen | Tidpunkt då den senaste push-meddelandet skickades till enheten |
| Tilldelning av användare | Användaren eller gruppen som den här enheten är kopplad till |

## Konfig Revision

Här får du en överblick över vilken grupprofil som är tilldelad enheten.


Om du klickar på grupprofilen får du direktåtkomst till profilen och kan göra inställningar.

Med den här symbolen kan du återställa de distribuerade apparna till grupprofilens inställningar.

Med den här symbolen kan du återställa alla använda appar till grupprofilens inställningar.

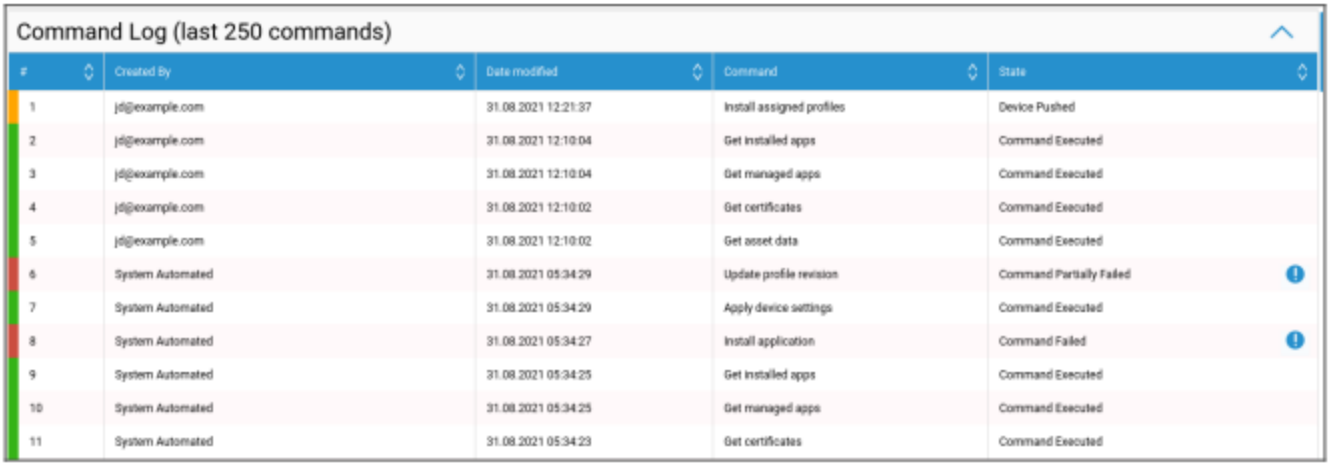
"Nyare revision tillgänglig" anger att grupprofilen har ändrats och sparats men inte tilldelats. Grupprofilen måste tilldelas med "Tilldela nu" på gruppnivå för att ändringarna ska gälla för enheterna.

## Enhetslogg (endast på enhetsnivå)

Här kommer du att få olika enhetsloggar. Om det behövs kan du direkt ta reda på orsaken till ett fel här.

## Kommandologg

Här kan du se vilka kommandon som har utfärdats för enheten och vilken status de har.




## Möjliga kommandostatusar

| | |
|---|---|
| Enhet tryckt | En push-begäran har skickats till push-tjänsten (t.ex. APNS) för att tala om för enheten att den ska ansluta tillbaka till EMM-servern. |
| Kommando Skapat | Kommandot skapades i systemet. |
| Kommando skickat | Kommandot skickades till enheten efter att den anslutit till servern. |
| Kommando utfört | Kommandot har utförts framgångsrikt. |
| Kommandot misslyckades | Kommandot misslyckades. * |
| Kommandot delvis misslyckat | Beroende på enhetens operativsystem kan vissa kommandon grupperas tillsammans.<br>I detta misslyckades vissa delar av denna kommandogrupp. * |
| Kommando utfört, eventuellt misslyckat | Kommandot utfördes, men kanske inte. |
| Kommando Repushed | Kommandot återställdes av en användare. |
| Bortkastad | Kommandot kasserades. Till exempel för att det ersattes av ett annat kommando eller för att enheten registrerades på nytt och gamla kommandon togs bort |

*Om det finns ett utropstecken bakom meddelandet kan du få mer information genom att hålla muspekaren över ikonen.

# Inställningar för enhet

## Konfiguration av klient

Här kan du utföra följande konfigurationer på din Android-enhet:

| | |
|---|---|
| Tid för bristande efterlevnad | Tidsgräns för användarsvar efter vilken verkställighetsåtgärden tillämpas. |
| Verkställighetsåtgärd efter timeout för efterlevnad | Verkställighetsåtgärd när en användare inte utför åtgärder som leder till en kompatibel enhetsstatus |
| Frekvens för datainsamling | Frekvens med vilken enhet/GPS-information ska samlas in |
| Frekvens för enhetens hjärtslag | Intervall inom vilket enheten ska kontakta AppTec Server<br>Min. 1 minut<br>Max. 24 timmar |
| Aktivera platsuppdateringar | Om den är aktiverad skickar enheten platsuppdateringar till AppTec Server |
| Plats Uppdateringstid | Bestämmer i vilka tidsintervall enheten skickar platsuppdateringar till AppTec |
| Använd Google Location Accuracy för platsuppdatering | Om den är aktiverad kommer nätverksplatsen att användas för platsuppdateringar (om den avaktiverades under "Begränsningar" påverkar inte den här inställningen någonting) |
| Använd GPS-position för platsuppdatering | Om den är aktiverad används GPS för platsuppdateringar |
| Tillåt falska platser (Mock) | Möjliggör förfalskning av platsinformation via appar från tredje part |
| Åtgärder vid förlorad anslutning | Om den är aktiverad kan du ange en åtgärd för det fall att en enhet inte får en anslutning till MDM-servern inom heartbeat-intervallet. Om enheten t.ex. har en heartbeat-tid på 5 minuter ansluter den till servern kl. 10.35. Efter det lämnar enheten Wi-Fi-området. Nästa heartbeat kl. 10:40 misslyckas och den angivna åtgärden utförs. |
| Åtgärd | Den åtgärd som ska vidtas så snart en enhet inte längre uppfyller kraven. |

| | | |
|---|---|---|
| | | • Lock Enhet = låsenhet<br>• Wipe Device = enheten återställs till fabriksinställningarna<br>• Wipe Device & SD Card = enheten återställs till fabriksinställningarna och SD-kortets lagringsutrymme raderas |
| | Tröskelvärde | Du kan ange ett tröskelvärde för antalet misslyckade hjärtslag som krävs för att utlösa den angivna åtgärden. |

| | | |
|---|---|---|
| Läge för tillämpning av policy | Standard: | Användare kommer regelbundet att uppmanas att utföra utestående åtgärder |
| | Lazy Policy Enforcement: | Användare kommer aldrig att bli ombedda att utföra utestående åtgärder. Alla öppna åtgärder kommer att visas i AppTec Client |
| | Aggressivt genomförande av policyer: | Användare kommer att uppmanas att utföra utestående åtgärder hela tiden |
| AppTec Versionslås | Om den är aktiverad kan en versionskod för AppTec-appen anges. AppTec-klienten kommer endast att uppdateras till den angivna versionen. Nyare versioner kommer att ignoreras. En nedgradering är INTE möjlig. | |
| Version Kod | Versionskod för AppTec-appen som ska låsas fast på. | |
| Avaktivera AppTec Notifiering | Om den är inaktiverad kommer AppTec Client inte att visa någon notifiering i Notifieringsfältet. Användare kan alltså stänga AppTec-klienten via aktivitetshanteraren. Om AppTec-klienten är stängd kommer flera funktioner, inklusive Kiosk Mode och App Black/Whitelisting, inte att fungera korrekt. Samsung-enheter erbjuder en skyddsmekanism för AppTec Client. Meddelandet är avaktiverat som standard på Samsung-enheter som stöder KNOX API:er. Meddelandet bör inte inaktiveras enheter med Android 8.0 eller högre. | |

## Bakgrund

| | |
|---|---|
| Ställ in anpassad bakgrundsbild | Aktivera/inaktivera den anpassade bakgrundsbilden |
| Bakgrund | Ställ in bakgrundsläget så att en färgkod eller en bild används |
| Ange en färg | Ange en bakgrundsfärg som hexvärde, t.ex. #000000 för svart eller #ffffff för vitt |
| Ange bild som bakgrundsbild | Ladda upp den bildfil som du vill använda som bakgrundsbild |

# Tillgångshantering (endast på enhetsnivå)

## Info om enhet

| | |
|---|---|
| Modell | Enhetens modellbeteckning |
| Operativsystem | OS |
| OS-version | OS-version |
| Serienummer | Serienummer |
| Enhetens namn | Enhetens namn |
| Batteristatus | Batteriets status |
| Fritt / totalt minne | Fritt / Totalt minne |
| Samsung Safe | Samsung SAFE-gränssnitt, krävs för en mängd olika inställningsalternativ |
| SD-kort tillgängligt | SD-kort tillgängligt |
| SD-kort emulerat | SD-kort emulerat |
| SD-kort löstagbart | SD-kort kan tas ut |
| SD Fritt / Totalt minne | SD Fritt / Totalt minne på SD-kort |

## Wi-Fi

| | |
|---|---|
| IP-adress | Enhetens IP-adress |
| WiFi MAC | WiFi MAC-adress |

## Cellulär

| | |
|---|---|
| Status | Status (SIM-kortet installerat) |
| Telefonnummer | Telefonnummer |
| Roaming (röst/data) | Roaming för röst/data |
| Status för roaming | Aktuell roamingstatus |
| IP-adress | IP-adress |
| Operatör/transportör | Operatör/transportör |
| Cellulär teknik | Cellulär teknik |
| IMEI | IMEI-nummer |
| ICCID | Detta är ID för SIM-kortet, ofta även ett smartkort eller ett Integrated Circuit Card (ICC) |
| IMSI | IMSI (International Mobile Subscriber Identity) ger i GSM- och UMTS-mobilnät en definitiv identifiering av nätanvändarna<br>IMSI består av maximalt 15 siffror och konfigureras på följande sätt:<br>• Mobil landskod (MCC), 3 siffror<br>• Mobilnätskod (MNC), 2 eller 3 siffror<br>• Identifieringsnummer för mobilabonnent (MSIN), 1-10 siffror |
| Nuvarande MCC/MNC | Se "SIM MCC/MNC" |
| SIM MCC/MNC | Mobile Country Code är en etablerad landsidentifierare, fastställd av ITU enligt E.212-standarden. Den fungerar tillsammans med Mobile Network Code (MNC) för identifiering av mobilnätet.<br>Betyder SIM-kortets landskod/Mobile Network Code.<br>Om du roamar till ett annat mobilnät kommer logiskt sett "Current MCC/MNC" och "SIM MCC/MNC" att vara olika. |

## Bluetooth

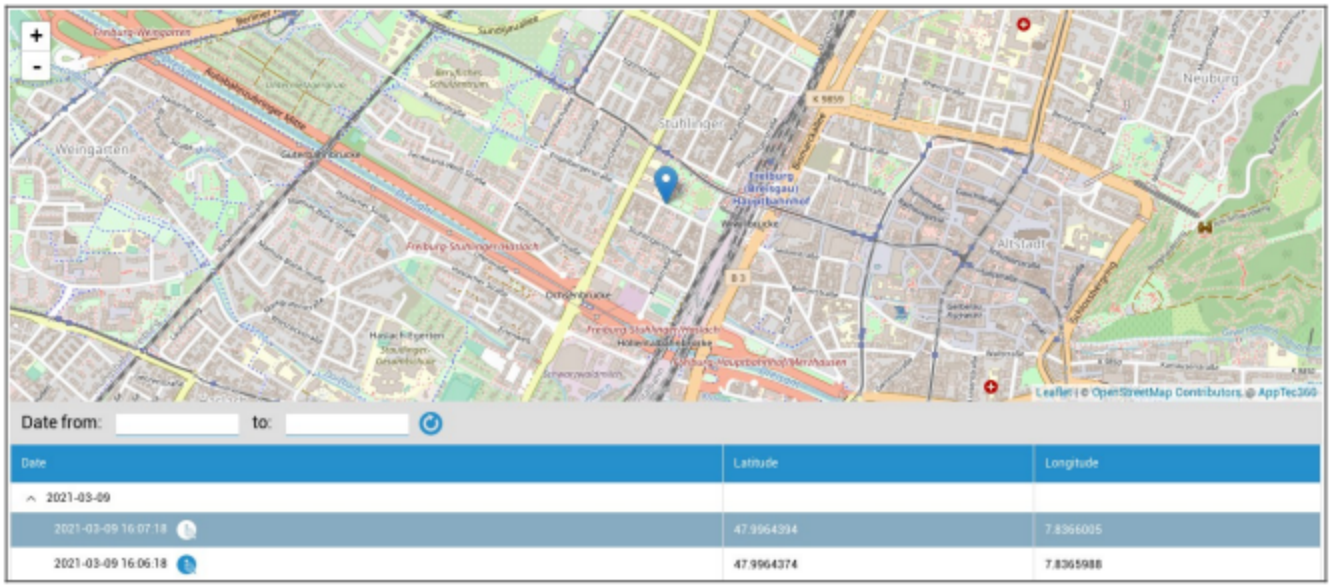
| | |
|---|---|
| Bluetooth MAC | Bluetooth MAC-adress |

# Säkerhetshantering

## Stöldskydd (endast på enhetsnivå)

### GPS-information (endast på enhetsnivå)

Här kan du ange aktuell/senaste enhetsplats. Lokaliseringen kan skyddas med ett eller till och med två lösenord - se: Allmänna inställningar - Sekretess - GPS-åtkomst



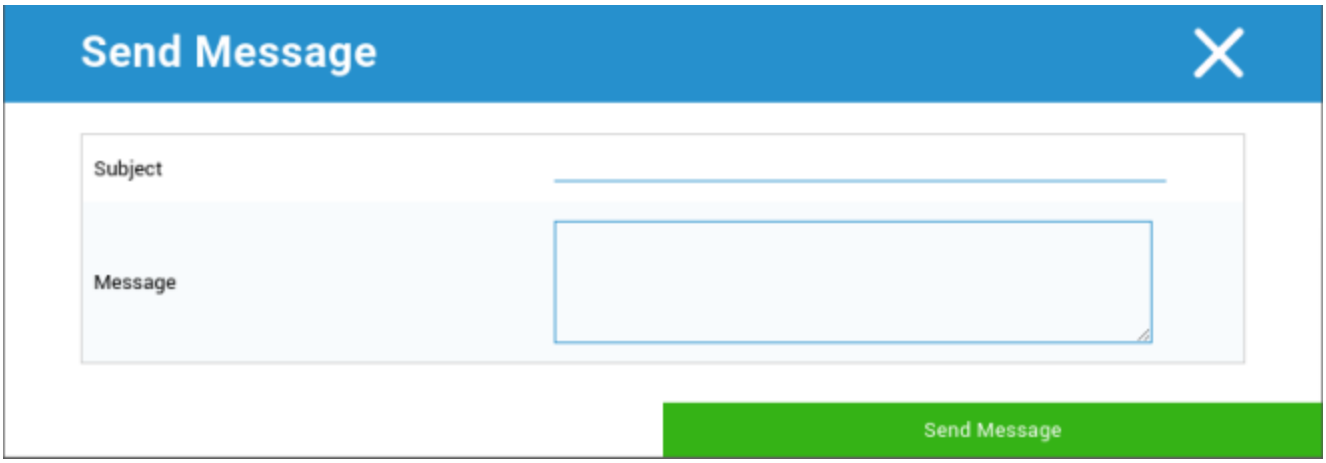

### Wipe & Lock (endast på enhetsnivå)

Under "Wipe & Lock" kan du utföra följande tre åtgärder:

| | |
|---|---|
| Fullständig avtorkning | Enheten återställs till fabriksinställningarna (både företagsdata och personuppgifter raderas). Fungerar endast för Enhanced Work Profile |
| Enterprise Wipe | Endast företagsdata tas bort från slutanvändarens enhet (alla appar, data etc. som tillhandahölls av AppTec) |
| Lås skärm | Om skärmlåset är aktiverat räcker det med att låsa upp enheten med enhetens lösenord/PIN |

## Meddelande (endast på enhetsnivå)

Här kan du fylla i ämnet och ett meddelande och skicka det till en slutanvändarenhet



# Säkerhetskonfiguration

## Enhetens lösenord

Under "Passcode" kan du ange ett lösenord för enheten, följande inställningsalternativ är tillgängliga för dig

| | | |
|---|---|---|
| Minsta lösenordslängd | Fastställer det minsta antal symboler som ett lösenord måste innehålla | |
| Lösenordskvalitet | Ospecificerad | Denna policy innehåller inga krav på lösenord. |
| | Biometrisk svaghet | Denna policy tillåter teknik för biometrisk identifiering med låg säkerhet. Detta innebär teknik som kan känna igen en persons identitet till ungefär en 3-siffrig PIN-kod (falsk detektering är mindre än 1 på 1 000). |
| | Någonting | Denna policy kräver att någon form av lösenord eller mönster anges, men tillämpar inga specifika regler. |
| | Alfabetisk | Användaren måste ha angett ett lösenord som innehåller minst alfabetiska tecken (eller andra symboler). |
| | Alfanumerisk | Användaren måste ha angett ett lösenord som innehåller minst både numeriska och alfabetiska tecken (eller andra symboler). |
| | Komplex | Användaren måste ha angett ett lösenord som innehåller minst en bokstav, en siffra och en specialsymbol, som standard. Med denna lösenordskvalitet kan lösenord begränsas till att innehålla olika uppsättningar av tecken, t.ex. minst en versal etc. |
| Minsta lösenordslängd | Ange det antal tecken som krävs för lösenordet. Du kan t.ex. kräva att PIN-koder eller lösenord ska innehålla minst sex tecken. | |
| Minsta antal numeriska siffror som krävs i lösenordet | Minsta antal numeriska siffror som krävs i lösenordet | |
| Minst små bokstäver krävs i lösenordet | Minst små bokstäver krävs i lösenordet | |
| Minimikrav på versaler i lösenordet | Minimikrav på versaler i lösenordet | |

| | |
|---|---|
| Minsta antal tecken som inte är bokstäver som krävs i lösenordet | Minsta antal tecken som inte är bokstäver som krävs i lösenordet |
| Minsta antal symboler som krävs i lösenordet | Minsta antal symboler som krävs i lösenordet |

| | |
|---|---|
| Lås för maximal inaktivitetstid | Maximal inaktivitet för användaren tills tiden låses |
| Tidsgräns för lösenordsutgång | Fastställer, efter vilket tidsintervall lösenordet upphör att gälla och ett nytt lösenord måste utfärdas |
| Begränsning av lösenordshistorik | Antal tidigare använda lösenord som inte är tillåtna |
| Maximalt antal misslyckade lösenordsförsök | Fastställer hur ofta ett lösenord kan anges felaktigt innan en fullständig radering av enheten utförs |
| Tillåt biometrisk autentisering | Möjliggör autentisering via fingeravtryck eller irisskanning. Endast för Samsung KNOX 2.1 och högre |

## Container lösenord

Under "Passcode" kan du ange ett containerlösenord, följande inställningsmöjligheter finns tillgängliga för dig

| | | |
|---|---|---|
| Minsta lösenordslängd | Fastställer det minsta antal symboler som ett lösenord måste innehålla | |
| Lösenordskvalitet | Ospecificerad | Denna policy innehåller inga krav på lösenord. |
| | Biometrisk svaghet | Denna policy tillåter teknik för biometrisk identifiering med låg säkerhet. Detta innebär teknik som kan känna igen en persons identitet till ungefär en 3-siffrig PIN-kod (falsk detektering är mindre än 1 på 1 000). |
| | Någonting | Denna policy kräver att någon form av lösenord eller mönster anges, men tillämpar inga specifika regler. |
| | Alfabetisk | Användaren måste ha angett ett lösenord som innehåller minst alfabetiska tecken (eller andra symboler). |
| | Alfanumerisk | Användaren måste ha angett ett lösenord som innehåller minst både numeriska och alfabetiska tecken (eller andra symboler). |
| | Komplex | Användaren måste ha angett ett lösenord som innehåller minst en bokstav, en siffra och en specialsymbol, som standard. Med denna lösenordskvalitet kan lösenord begränsas till att innehålla olika uppsättningar av tecken, t.ex. minst en versal etc. |
| Minsta lösenordslängd | Ange det antal tecken som krävs för lösenordet. Du kan t.ex. kräva att PIN-koder eller lösenord ska innehålla minst sex tecken. | |
| Minsta antal numeriska siffror som krävs i lösenordet | Minsta antal numeriska siffror som krävs i lösenordet | |
| Minst små bokstäver krävs i lösenordet | Minst små bokstäver krävs i lösenordet | |
| Minimikrav på versaler i lösenordet | Minimikrav på versaler i lösenordet | |
| Minsta antal tecken som inte är bokstäver som krävs i lösenordet | Minsta antal tecken som inte är bokstäver som krävs i lösenordet | |

| | |
|---|---|
| Minsta antal symboler som krävs i lösenordet | Minsta antal symboler som krävs i lösenordet |

| | |
|---|---|
| Lås för maximal inaktivitetstid | Maximal inaktivitet för användaren tills tiden låses |
| Tidsgräns för lösenordsutgång | Fastställer, efter vilket tidsintervall lösenordet upphör att gälla och ett nytt lösenord måste utfärdas |
| Begränsning av lösenordshistorik | Antal tidigare använda lösenord som inte är tillåtna |
| Maximalt antal misslyckade lösenordsförsök | Fastställer hur ofta ett lösenord kan anges felaktigt innan en fullständig radering av enheten utförs |

## AntiVirus

| | |
|---|---|
| Automatisk skanning | Aktivera periodiska automatiska skanningar |
| Skanningsintervall | Intervall för undersökning (snabb/full) |
| Fullständig automatisk skanning | Aktivera helautomatiska skanningar |
| Automatiska uppdateringar | Aktivera automatiska uppdateringar |
| Intervall för uppdateringskontroll | Hur ofta appen och dess databas ska uppdateras (virus/skadad kod) |
| Skydd för appar | Aktivera automatisk appskanning |
| Skydd för SD-kort | Aktivera automatisk skanning av SD-kort |
| Uppdatering endast för Wi-Fi | När den är aktiverad tillämpas uppdateringar endast när enheten är ansluten till ett Wi-Fi-nätverk |

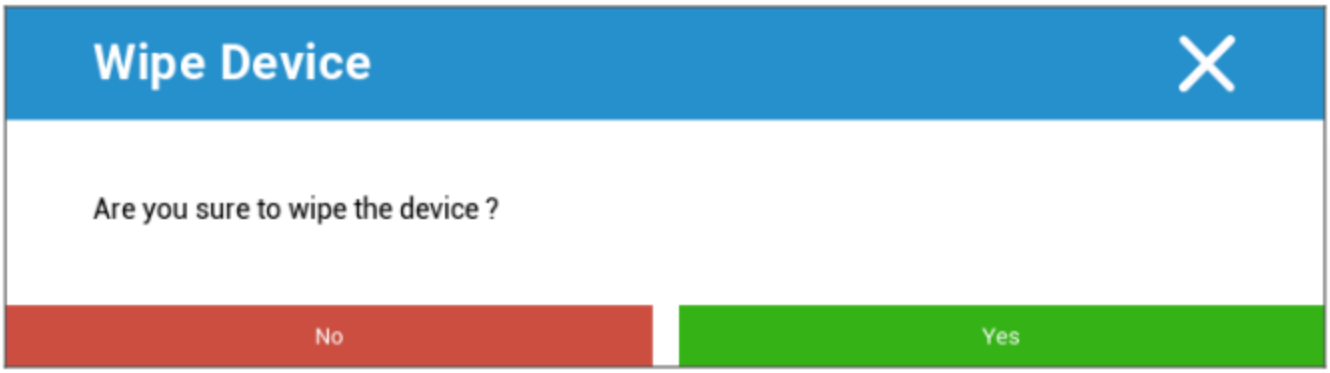
# End of Life (endast på enhetsnivå)

## Torka (endast på enhetsnivå)

Under "Wipe" kan du återställa enheten till fabriksinställningarna (endast för Enhanced Work Profile).

Här raderas både företagsdata och privata data på slutanvändarens enhet.

Genom att klicka på "Minus-symbolen" får du följande meddelande:




Med "Yes" kan du utföra torkningen.

Under "Wipe Report" kan följande objekt visas

| | |
|---|---|
| Raderad av | Historik över vem som utförde torkningen |
| Datum | Datum |
| Status | Status (t.ex. om rensningen utfördes framgångsrikt) |

# Inställningar för begränsning

## Begränsningar

Här kan en mängd olika saker begränsas och blockeras.

| | |
|---|---|
| Tillämpning av efterlevnad | Mode Prompt User - Användaren kommer att uppmanas att utföra nödvändiga åtgärder.<br>Mode Lock-Down Container - Dölj alla appar tills alla krav har uppfyllts |
| Policy för körtidsbehörighet | Fråga användaren om nya behörighetsförfrågningar<br>Bevilj alltid nya ansökningar om tillstånd<br>Avslå alltid nya förfrågningar om tillstånd<br>Varning för problem: Vissa appar har problem med att känna igen behörigheterna om dessa ställs in automatiskt. Om du alltid beviljar behörigheter och får problem med appar som säger att behörigheter saknas, ställ in detta på "fråga användaren" och installera om appen |
| Tillåt utgående urklipp | Tillåter kopiering och klistring från insidan av behållaren till utsidan |
| Tillåt upplösning av nummerpresentation | Visar namnet för ett inkommande samtal baserat på kontakter i behållaren |
| Tillåt kontaktsökningsupplösning | Gör det möjligt att söka efter namn i behållarens kontakter när du ringer |
| Tillåt kontaktdelning via Bluetooth | Tillåter åtkomst till behållarkontakt i en bil |
| Avvisa utgående NFC-strålning | Avaktiverar NFC för behållaren |
| Tillåt okända källor | Om den är aktiverad kan användare ladda appar genom att installera en .apk-fil. |
| Tillåt USB-felsökning | Om den är aktiverad kan användare aktivera USB Debugging. |
| Förbjuda ändring av konto | Tillåter inte att konton i behållaren skapas, raderas eller ändras<br>Tänk på att vissa appar behöver skapa eller ändra konton för att fungera som förväntat |

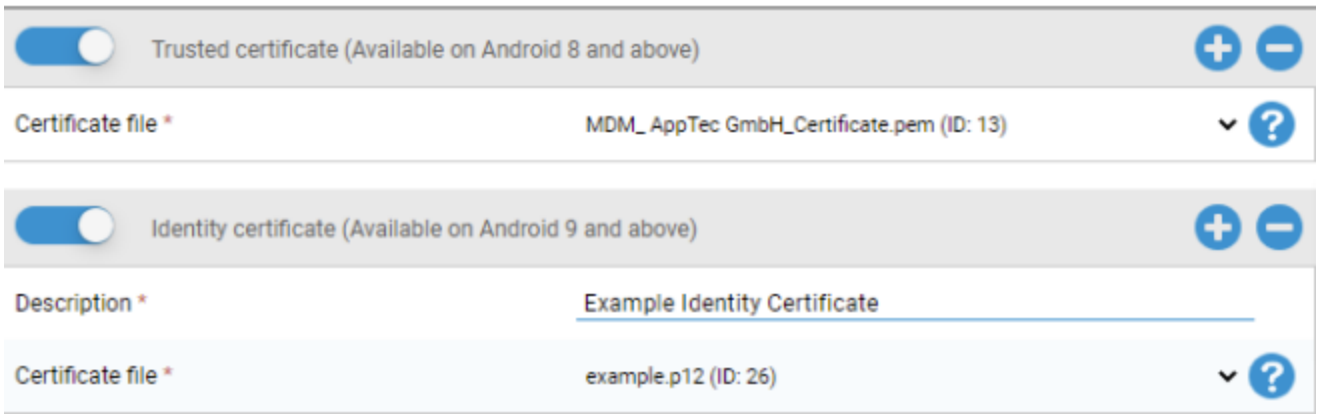
| **Begränsningar för arbetsprofilen. Endast tillgängligt på Android 11-enheter och högre, med Enhanced Work Profile** | |
|---|---|
| Avvisa kamera | Anger om kameran inte är tillåten i arbetsprofilen. |
| Avvisa Bluetooth | Anger om Bluetooth inte är tillåtet i arbetsprofilen. |

| | |
|---|---|
| Aktivera skydd mot fabriksåterställning | Aktivera detta för att åsidosätta skyddet mot fabriksåterställning av Android till det Google-konto som du definierade i "Allmänna inställningar" → "Androidkonfiguration" → "Android Enterprise" → "Skydd mot fabriksåterställning" Om detta är aktiverat och du återställer enheten måste du ange det konfigurerade Google-kontot för att konfigurera enheten igen. |
| Uppdatering av styrsystem | Aktivera detta för att ställa in uppdateringsbeteendet till automatiskt, i fönster eller uppskjutet. |
| Uppdateringspolicy | Automatisk: Installeras automatiskt så snart en uppdatering finns tillgänglig. Fönster: Installeras automatiskt inom ett dagligt underhållsfönster. Detta konfigurerar även Play-appar så att de uppdateras inom fönstret. Detta rekommenderas starkt för kioskenheter eftersom det är det enda sättet som appar som ständigt är fästa i förgrunden kan uppdateras av Play. Skjut upp: Skjut upp automatisk installation upp till maximalt 30 dagar. |

| **Begränsningar för personlig profil. Endast tillgängligt på Android 11-enheter och senare, med Enhanced Work Profile** | |
|---|---|
| Avvisa kamera | Anger om kameran inte är tillåten i den personliga profilen. |
| Avvisa Bluetooth | Anger om Bluetooth inte är tillåtet i den personliga profilen. |
| Tillåt okända källor | Om den är aktiverad kan användare av arbetsprofiler ladda appar på sidan genom att installera en .apk-fil. |

## Certifikathantering

Här kan du distribuera Trusted Certificates och Identity Certificates till dina enheter. Android 8 eller senare krävs för att distribuera Trusted Certificates och Android 9 eller senare krävs för att distribuera Identity Certificates.




Med "+" kan du lägga till flera certifikat.

Betrodda certifikat måste vara i PEM-format.

Identitetscertifikaten måste vara i PKCS12-format.

# Hantering av anslutningar

## Wifi

För denna inställning, utför förkonfigurationen av slutanvändarens enheter, för åtkomst till intern åtkomst
Punkter

| | |
|---|---|
| Identifierare för tjänsteuppsättning (SSID) | SSID för det nätverk som ska anslutas |
| Dolda nätverk | Aktivera, om AP:n inte sänder SSID |

## Typ av säkerhet

Fastställ AP:ns säkerhetstyp

### WEP

| | |
|---|---|
| Lösenord | Lösenord för AP:n |

### WPA/WPA2

| | |
|---|---|
| Lösenord | Lösenord för AP:n |

## 802.1x EAP

| **EAP-metod** |
|---|

| | | |
|---|---|---|
| PWD | Identitet | Identitet |
| | Lösenord | Lösenord |

| | | | |
|---|---|---|---|
| PEAP | Fas 2 autentiseringsprotokoll | ingen | Inget ytterligare protokoll |
| | | MSCHAPV2 | MSCHAPV2-protokoll |
| | | GTC | GTC-protokoll |
| | CA-certifikat | CA-certifikat | |
| | Identitet | Identitet | |
| | Anonym identitet | Anonym identitet | |
| | Lösenord | Lösenord | |

| | | | |
|---|---|---|---|
| TTLS | Fas 2 autentiseringsprotokoll | ingen | Inget ytterligare protokoll |
| | | PAP | PAP-protokoll |
| | | MSCHAP | MSCHAP-protokoll |
| | | MSCHAPV2 | MSCHAPV2-protokoll |
| | | GTC | GTC-protokoll |
| | CA-certifikat | CA-certifikat | |
| | Identitet | Identitet | |
| | Anonym identitet | Anonym identitet | |
| | Lösenord | Lösenord | |

| | | |
|---|---|---|
| TLS | CA-certifikat | CA-certifikat |
| | Identitet | Identitet |
| | Lösenord | Lösenord |

# VPN

| | |
|---|---|
| Namn på anslutning | Namn på VPN-anslutningen |

## VPN-typ

### VPN

| **VPN-klient** |
|---|

| AppTec VPN-klient | |
|---|---|
| Gateway-konfiguration | Välj VPN-konfiguration för Gateway (se **Allmänna inställningar > Universal Gateway > VPN-inställningar**) |
| Alltid på VPN | Aktivera Native Lockdown |
| Aktivera AppTec Lockdown | Aktivera AppTec Lockdown |

| | | | |
|---|---|---|---|
| Inbyggd (endast tillgänglig på Samsung-enheter) | | | |
| Typ av anslutning | PPTP | Server | Server |
| | | Aktivera PPTP-kryptering | Aktivera PPTP-kryptering |
| | L2TP / IPSec PSK | Server | Server |
| | | IPSec Förhandsdelad nyckel | IPSec Förhandsdelad nyckel |
| | | Aktivera L2TP-hemlighet | Aktivera L2TP-hemlighet |
| | | L2TP-hemlighet | L2TP-hemlighet |
| | IPSec XAuth PSK | Server | Server |
| | | IPSec-identifierare | IPSec-identifierare |
| | | IPSec Förhandsdelad nyckel | IPSec Förhandsdelad nyckel |
| DNS-sökning Domäner | DNS-sökning Domäner | | |
| Expertinställningar | DNS-servrar | DNS-servrar | |
| | Vidarebefordran av rutter | Vidarebefordran av rutter | |

| | | |
|---|---|---|
| Öppet VPN | | |
| Server | Server | |
| OpenVPN-profil | OpenVPN-profil | |
| OpenVPN-app | OpenVPN för Android (rekommenderas) | |
| | Anslut till OpenVPN | |
| Expertinställningar | DNS-servrar | DNS-servrar |
| | Vidarebefordran av rutter | Vidarebefordran av rutter |

| Samsung / Starka svanen | | | |
|---|---|---|---|
| Typ av anslutning | PPTP | Server | Server |
| | | Användarnamn | Användarnamn |
| | | Lösenord | Lösenord |
| | | Aktivera PPTP-kryptering | Aktivera PPTP-kryptering |
| | L2TP / IPSec PSK | Server | Server |
| | | IPSec Förhandsdelad nyckel | IPSec Förhandsdelad nyckel |
| | | Användarnamn | Användarnamn |
| | | Lösenord | Lösenord |
| | | Aktivera L2TP-hemlighet | L2TP-hemlighet |
| | IPSec XAuth PSK | Server | Server |
| | | IPSec-identifierare | IPSec-identifierare |
| | | IPSec Förhandsdelad nyckel | IPSec Förhandsdelad nyckel |
| | | Användarnamn | Användarnamn |
| | | Lösenord | Lösenord |
| Expertinställningar | DNS-servrar | DNS-servrar | |
| | Vidarebefordran av rutter | Vidarebefordran av rutter | |

| Cisco Any Connect | | |
|---|---|---|
| Server | Server | |
| Certifikatläge | Inaktiverad | Inaktiverad |
| | Automatisk | Automatisk |
| Expertinställningar | DNS-servrar | DNS-servrar |
| | Vidarebefordran av rutter | Vidarebefordran av rutter |

## VPN per app

| **VPN-klient** |
|---|

| AppTec VPN-klient | | |
|---|---|---|
| Gateway-konfiguration | Välj VPN-konfiguration för Gateway (se **Allmänna inställningar > Universal Gateway > VPN-inställningar**) | |
| VPN-appar | VPN-appar | |
| Alltid på VPN | Aktivera Native Lockdown | Alltid på VPN |
| Aktivera AppTec Lockdown | Aktivera AppTec Lockdown | |

| | | | |
|---|---|---|---|
| Samsung / Starka svanen | | | |
| Typ av anslutning | PPTP | Server | Server |
| | | VPN-appar | VPN-appar |
| | | Användarnamn | Användarnamn |
| | | Lösenord | Lösenord |
| | | Aktivera PPTP-kryptering | Aktivera PPTP-kryptering |
| | L2TP / IPSec PSK | Server | Server |
| | | VPN-appar | VPN-appar |
| | | IPSec Förhandsdelad nyckel | IPSec Förhandsdelad nyckel |
| | | Användarnamn | Användarnamn |
| | | Lösenord | Lösenord |
| | | Aktivera L2TP-hemlighet | L2TP-hemlighet |
| | IPSec XAuth PSK | Server | Server |
| | | VPN-appar | VPN-appar |
| | | IPSec-identifierare | IPSec-identifierare |
| | | IPSec Förhandsdelad nyckel | IPSec Förhandsdelad nyckel |
| | | Användarnamn | Användarnamn |
| | | Lösenord | Lösenord |
| Expertinställningar | DNS-servrar | DNS-servrar | |
| | Vidarebefordran av rutter | Vidarebefordran av rutter | |

## Begränsningar

Här kan du ställa in begränsningarna i förhållande till anslutningshanteringen

| | |
|---|---|
| Tillåt data-roaming | Tillåt mobildata vid roaming |
| Tvinga fram dataroaming | Om den är aktiverad är roaming för mobildata permanent aktiverad (rekommenderas inte!)<br>Denna inställning skriver över inställningen "Allow Data Roaming"! |
| Använd systemets http-proxyserver | Användningen av en HTTP-proxyserver, som tillhandahålls av systemets inställningar i Inställningar, är beroende av det anslutna nätverket (WiFi eller APN) |

# PIM-hantering

## Gmail Exchange

Information: Den här konfigurationen kommer att tillämpas på Gmail-appen. Du måste därför godkänna och installera Gmail.

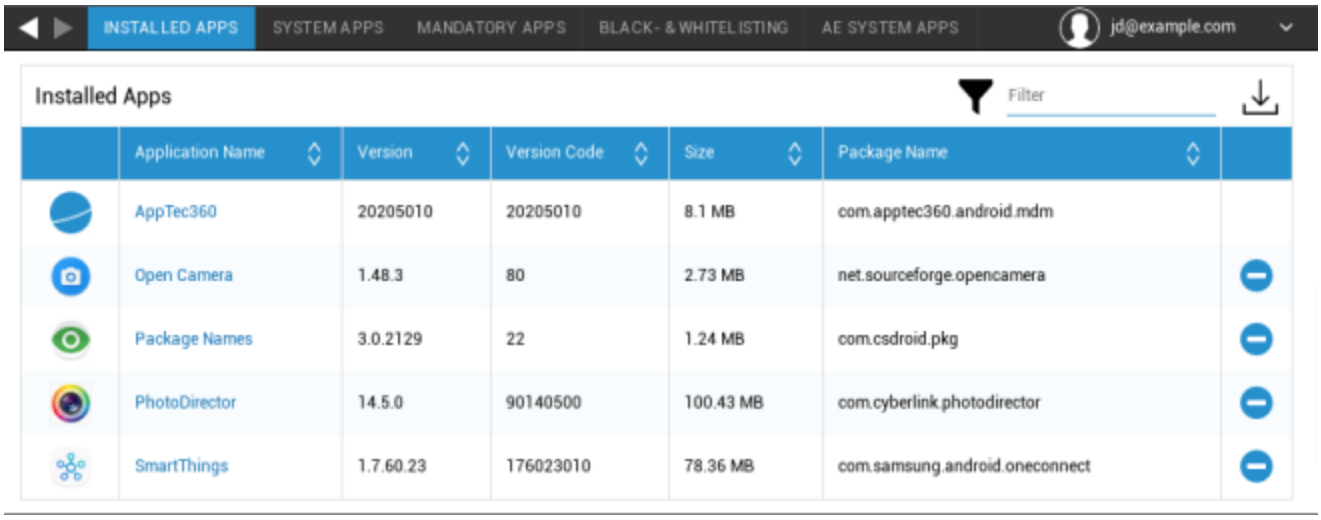
| | |
|---|---|
| E-postadress | Den angivna användarens e-postadress<br>Observera "platshållarna", som du kan använda för att arbeta med referenser och du behöver inte utföra ändringar manuellt på varje enhet<br>Med ett klick kan du visa dem för dig själv |
| Serverns värdnamn | Serveradress till dina Exchange-servrar |
| Inloggningsnamn | Inloggningsnamnet för respektive slutanvändarenhet, observera även "Platshållare här |
| Underskrift | En signatur kan bifogas (Tips: Vissa enheter kräver HTML-formatering för signaturen) |
| Antal föregående dagar att synkronisera | Antal dagar som avgör när e-postmeddelanden synkroniseras tillbaka |
| Enhetens identifierare | En sträng som innehåller EAS DeviceID. Detta är en del av EAS-protokollet och behövs i vissa områden |
| Använd SSL (Secure Sockets Layer) | Använd en SSL-anslutning |
| Acceptera alla certifikat | Alla certifikat accepteras. Välj detta alternativ om Exchange Server använder ett självsignerat certifikat |
| Tillåt oadministrerade konton | Tillåt användare att lägga till eller ta bort andra Exchange-konton än det konto som anges i den här hanterade konfigurationen. Om den här inställningen är aktiverad kan du inte hindra användare från att lägga till andra Exchange-konton i Gmail. Du kan inte heller kontrollera datadelning mellan andra appar och Exchange-konton som läggs till av användare. Den här inställningen bör endast aktiveras om användarna behöver ha mer än ett arbetsrelaterat Exchange-konto i Gmail. |
| Kundcertifikat | Klientcertifikat. Krävs endast om din e-postserver förväntar sig att detta ska finnas. |

# App-hantering

## Enterprise App Manager

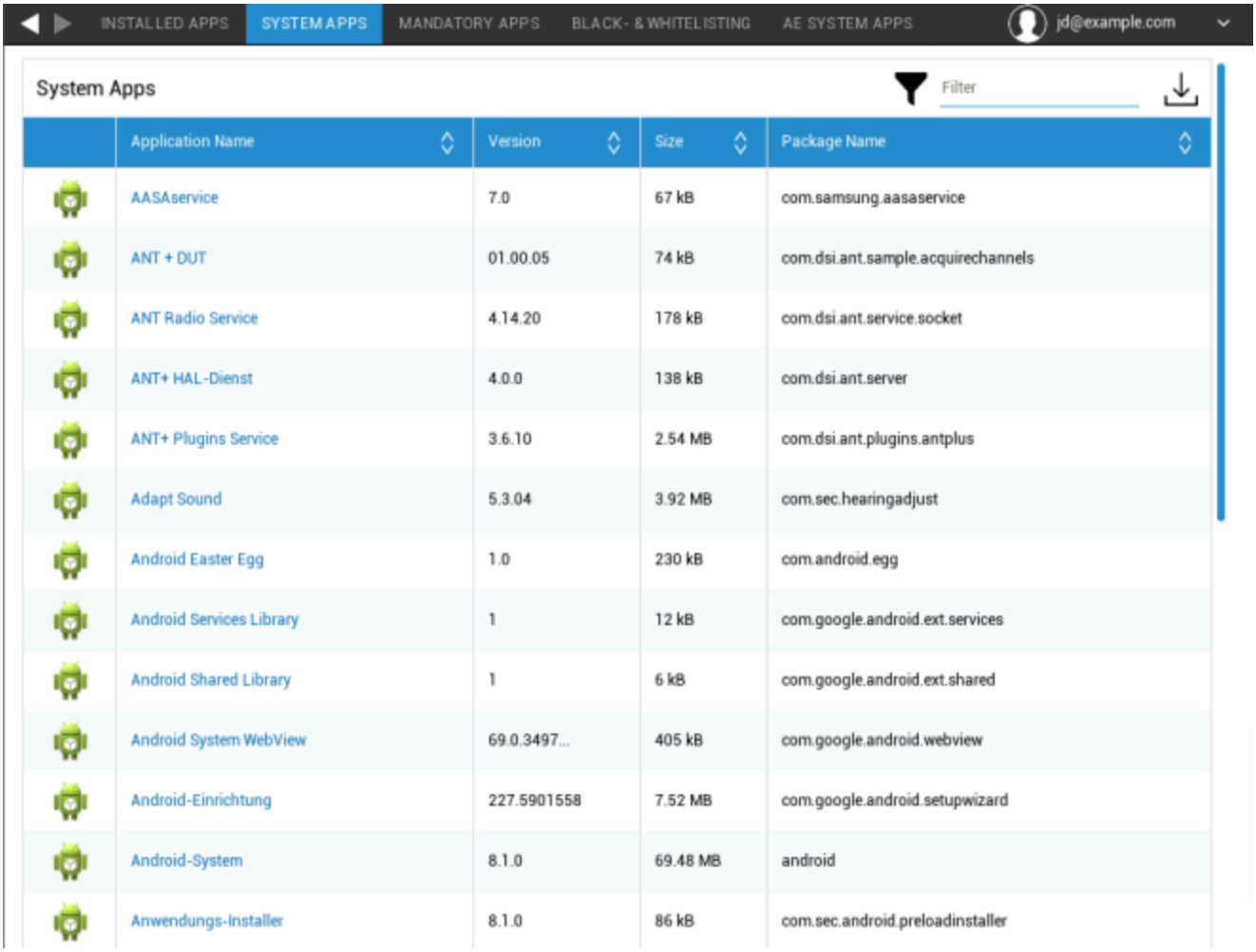
### Installerade appar (endast på enhetsnivå)

Här visas alla appar som för närvarande är installerade i behållaren.



## Systemappar (endast på enhetsnivå)

Under "System Apps" listas alla appar och tjänster som redan har installerats på slutanvändarens enhet av enhetens tillverkare.

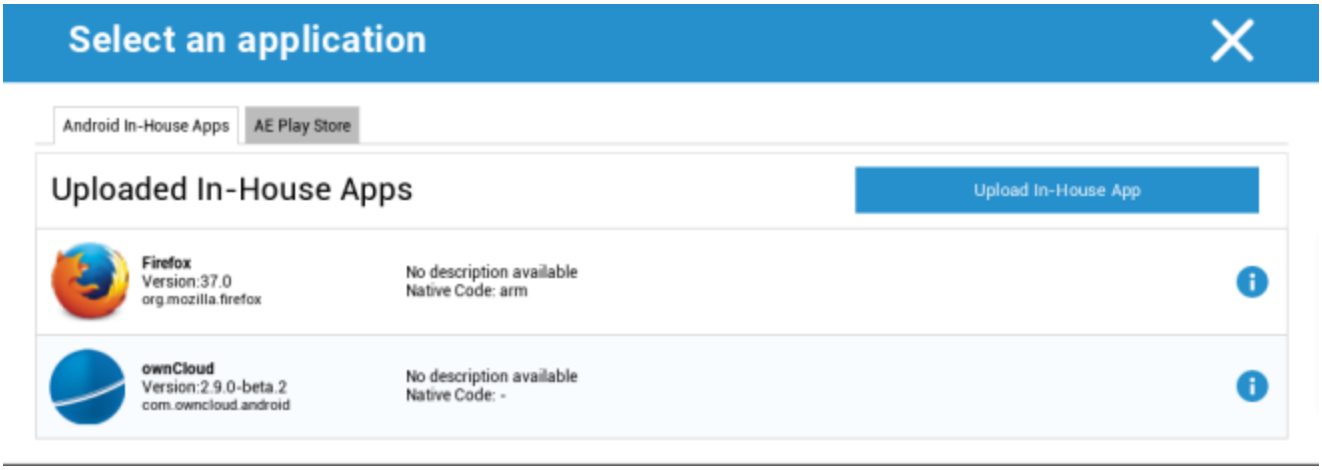


## Obligatoriska appar

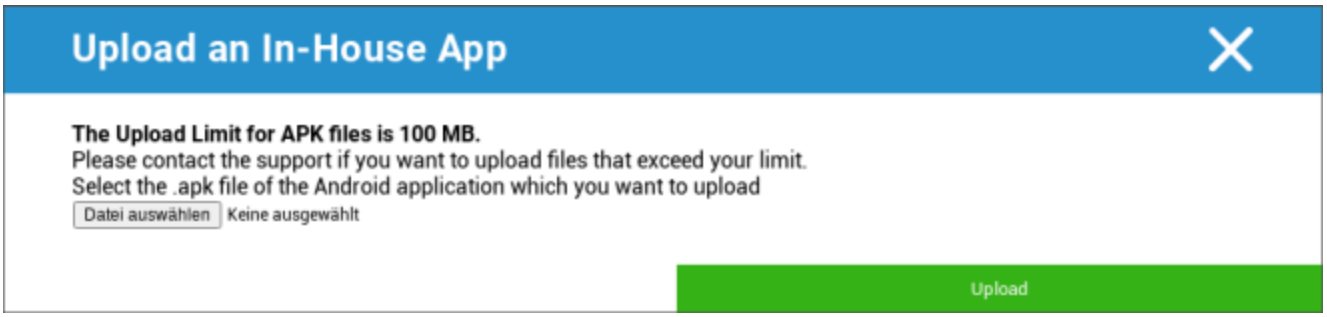
Under Obligatoriska appar kan du ange de obligatoriska appar som krävs. Användaren kommer kontinuerligt att uppmanas att installera den angivna appen, om det är en InHouse-app. Appar från Play Store installeras automatiskt.

Med hjälp av kan den obligatoriska appen definieras.

Detta kan vara en intern app från "Android In-House Apps", som du har laddat upp i Allmänna inställningar.

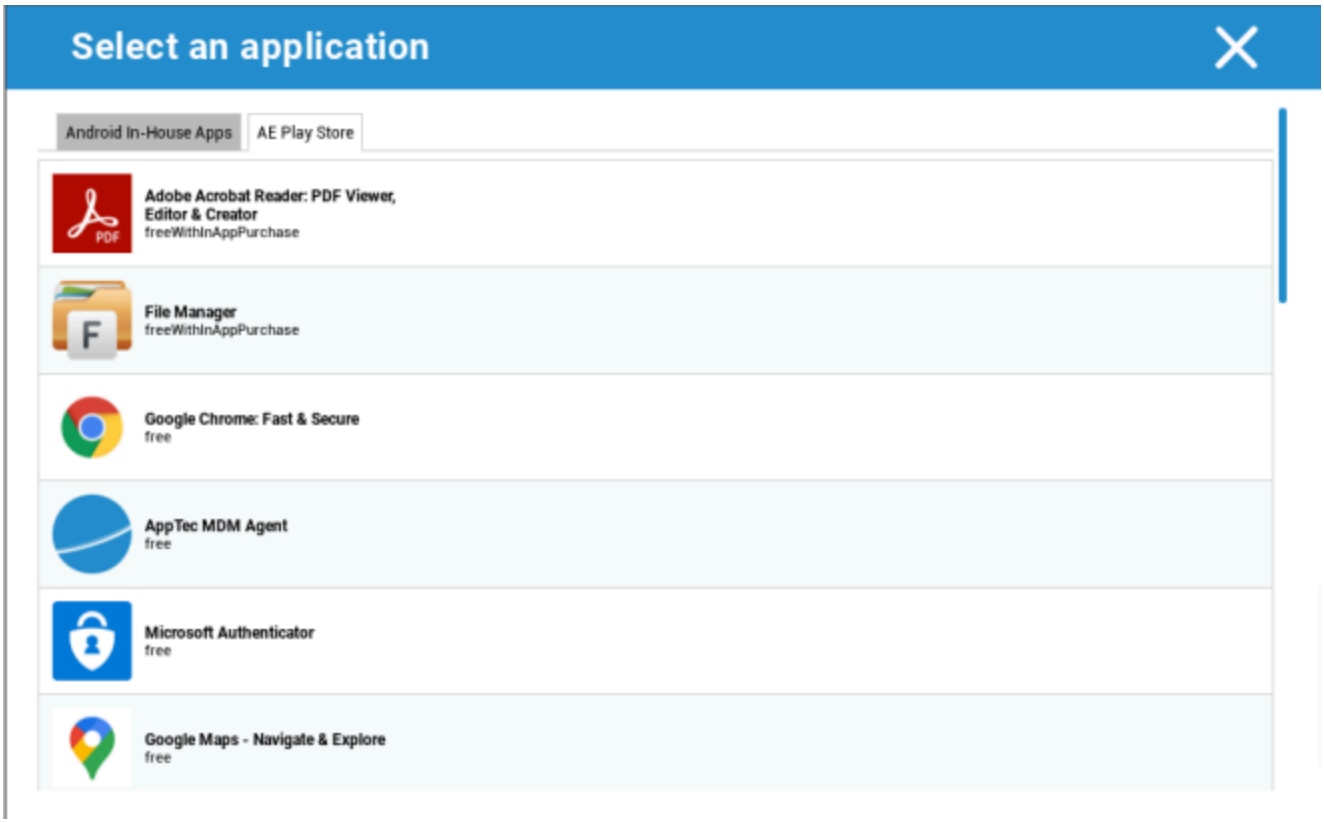



Du kan också direkt välja och ladda upp en apk-fil med "Upload In-House App".




Om du installerar en In-House App har du möjlighet att aktivera "Keep up to date". Om detta är aktiverat och du har definierat en nyare version i In-House App DB, kommer appen att uppdateras på enheten.

Eller så kan det vara en "AE Play Store"-app från Google Work Play Store.



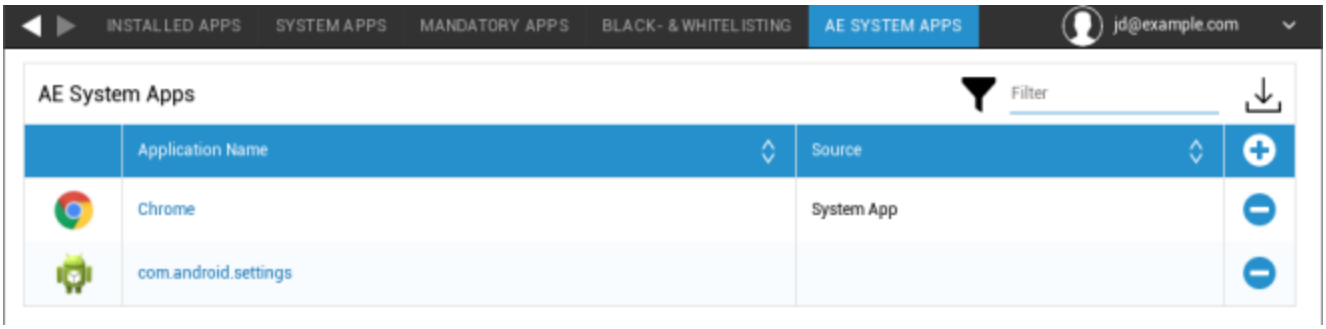

Endast godkända "AE Play Store Apps" kommer att visas på den här fliken.

För att godkänna en "AE Play Store-app", gå till "Allmänna inställningar" > "Apphantering" > "AE Play Store" och lägg till en app via knappen som omdirigerar dig till fliken "Play Store Apps" (eller så kan du gå direkt till fliken "Play Store Apps").

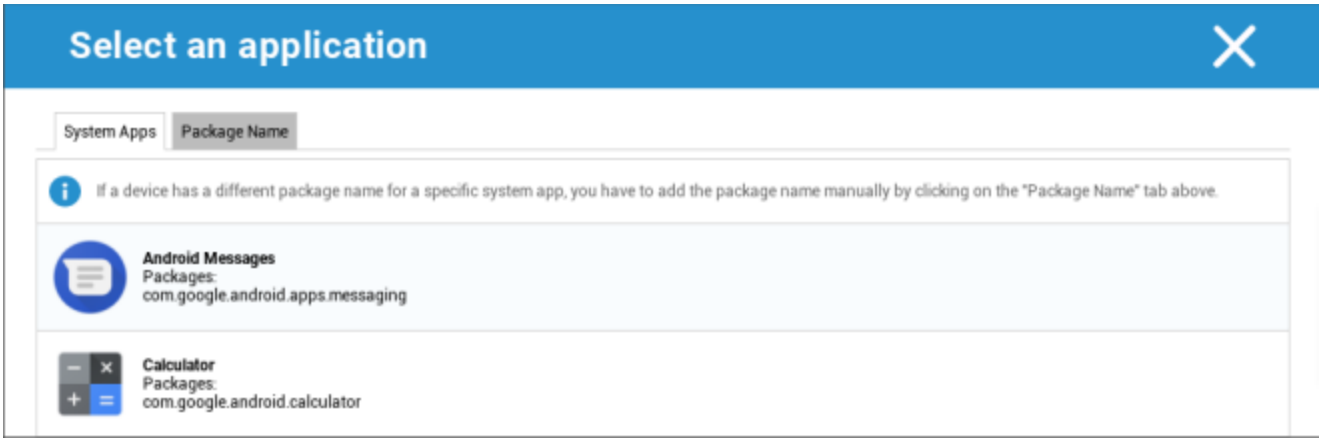
På fliken "Play Store Apps" kan du söka efter appar. När du klickar på en app öppnas appsidan och här kan du godkänna appen genom att klicka på "Approve".

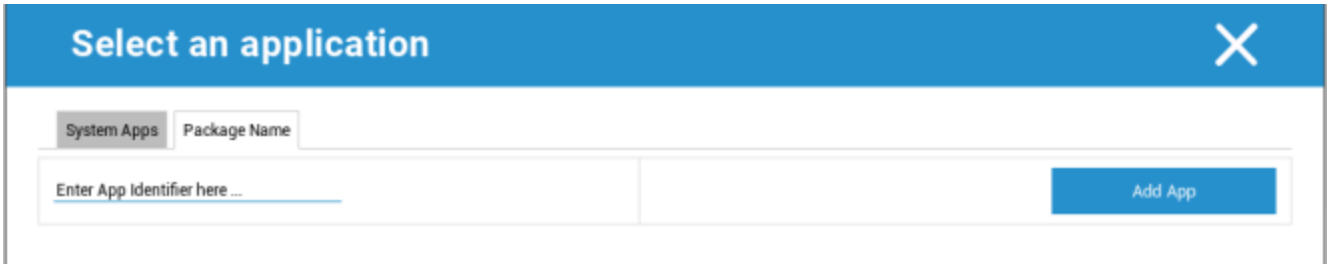
## Appar för AE-system

Här kan du definiera en lista som innehåller specifika systemappar som ska aktiveras på enheterna.




Om du klickar på knappen kan du välja från en lista med möjliga systemprogram som tillhandahålls av Google eller direkt ange paketnamnet på ett systemprogram som ska aktiveras.




Tänk på att systemapparna i listan från Google endast är appar som kan vara systemappar, men som inte nödvändigtvis måste vara systemappar på dina enheter.

Den här listan gäller dock bara appar som redan är förinstallerade.

Om du lägger till appar som inte är förinstallerade på dina enheter påverkas inte dina enheter, oavsett om appen finns med i listan från Google eller om appens paketnamn anges direkt.

# Begränsningar och inställningar

## Inställningar för apphantering

Här kan du konfigurera enhetens beteende när det gäller appuppdateringar.

| | |
|---|---|
| Frekvens för uppdateringskontroll | Ange i vilket intervall AppTec Client ska söka efter appuppdateringar. Standardvärdet är 24 timmar. |
| Tröskelvärde för Wi-Fi | Appar som är större än den angivna storleken laddas ner via Wi-Fi. Om "Endast Wi-Fi" väljs laddas alla appar ner via Wi-Fi. |

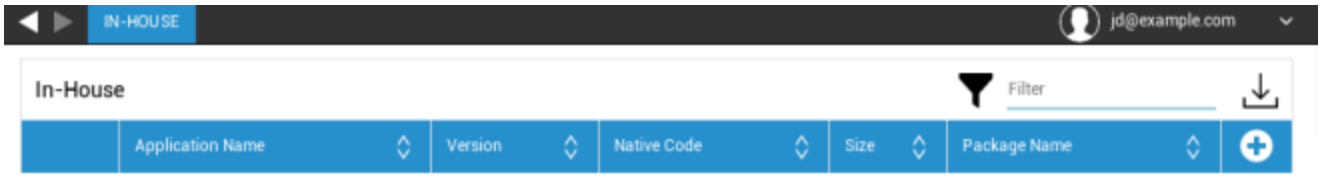
# App Store för företag

## Internt

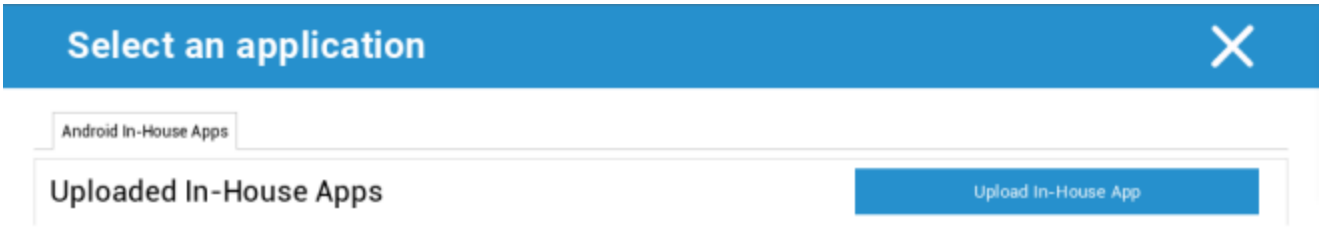
Under punkten "In-House" kan du ladda upp och distribuera internt utvecklade appar.

Med symbolen kan du distribuera ytterligare In-House Apps.

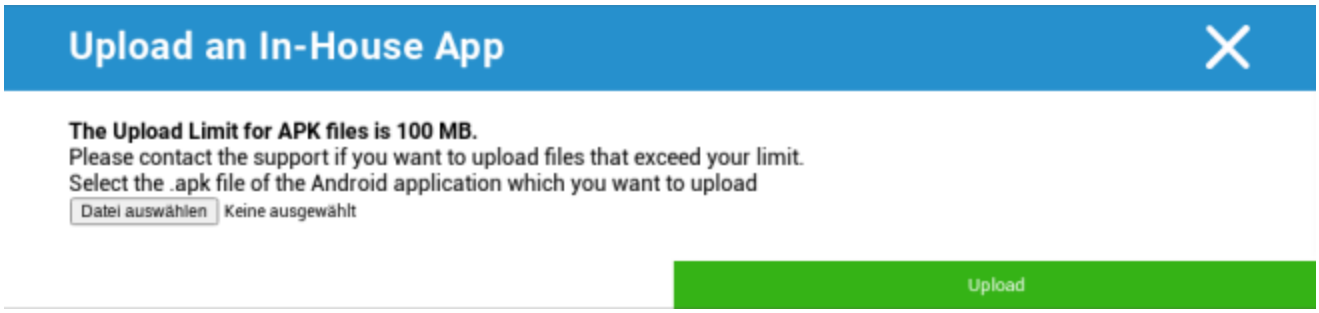
Om du installerar en In-House App har du möjlighet att aktivera "Keep up to date". Om detta är aktiverat och du har definierat en nyare version i In-House App DB, kommer appen att uppdateras på enheten.



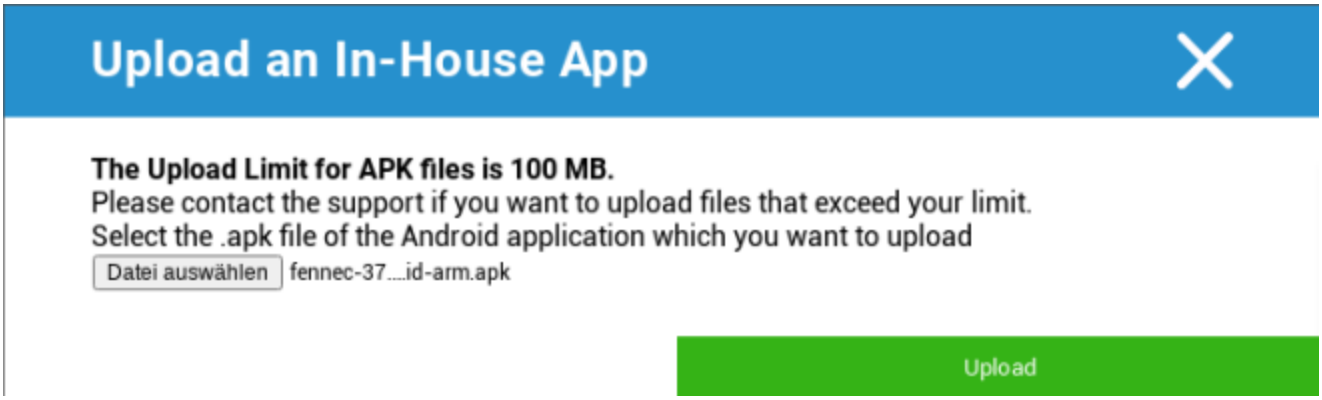

Om du inte har distribuerat In-House Apps kommer du att få följande översikt:



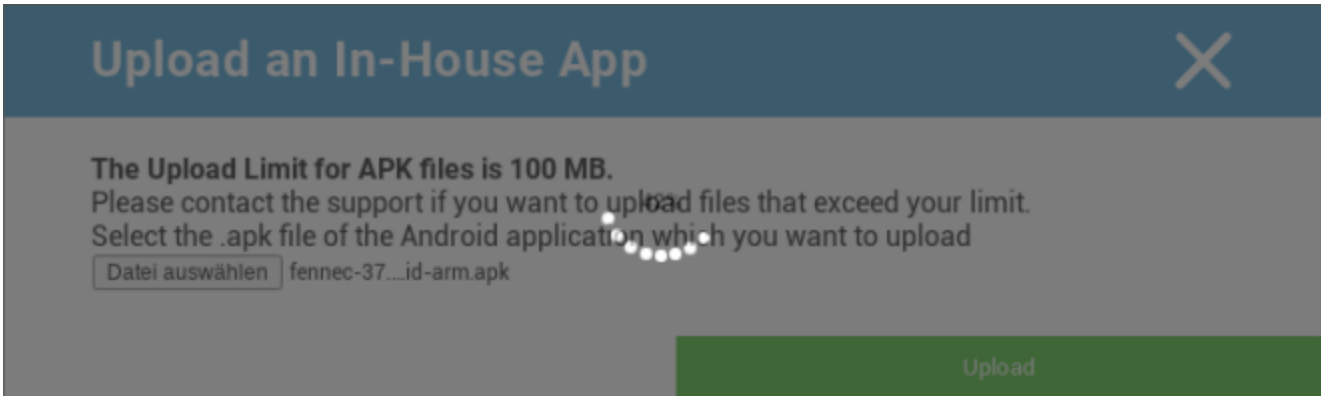
För detta klickar du på "Upload In-House App", du kommer då att få följande översikt:




Välj nu med "Sök ..." en .apk-fil och klicka sedan på "Ladda upp".




Din app kommer nu att laddas upp, i mitten av cirkeln ser du en procentindikator som visar hur stor del av din app som redan har laddats upp.



Om uppladdningen av din In-House App har lyckats kan du hitta den uppladdade appen i din App Catalog.

Användaren har nu möjlighet att se och installera den här appen i AppTec Store på slutanvändarens enhet, under kategorin "In-House".


Eftersom det inte handlar om en Google PlayStore-app behöver användaren inte ha ett lagrat Google-ID på sin respektive slutanvändarenhet.

## Play Store för företag

### AE Play Butik

Här kan du lägga till appar i Android Enterprise Playstore. Observera att du måste godkänna appar med ditt AE-administratörskonto innan du kan lägga till dem.

För godkännande av en app, se instruktionerna i Obligatoriska appar.

# Innehållshantering

## Innehållsruta

Här kan du aktivera ContentBox.

Så snart du ställer in "Enable ContentBox" på "On" installeras en separat ContentBox-app automatiskt på slutanvändarens enhet.

## Säker webbläsare

Här kan du konfigurera inställningar för AppTec Secure Browser.

Så snart du ställer in "Secure Browser" på "On" kommer en separat webbläsarapp att installeras automatiskt på slutanvändarens enhet.

| | |
|---|---|
| Kräv lösenord | Kräv att användaren ställer in och använder ett lösenord för att få tillgång till webbläsaren. |
| Minimal längd på lösenord som krävs | Ange det antal tecken som krävs för lösenordet |
| Erforderlig lösenordskvalitet | Ställ in önskad lösenordskvalitet |
| Begränsa nedladdningar / Öppna i | |
| Begränsa uppladdningar | |
| Ladda upp vitlista | En lista med URL:er som alltid ska tillåtas att laddas upp. |
| Tillåt kopiering | Tillåt kopiering, klippning eller delning av text på webbsidorna. |
| Tillåt skärmupptagning | Tillåt att ta skärmdumpar. |
| Frekvens för rensning av data | Välj med vilken frekvens ALL användardata (historik, cache etc.) ska tas bort automatiskt. |
| Bokmärken för företag | Bokmärkena kommer att visas i mappen "Företagsbokmärken" i webbläsarens bokmärken.<br>De kan inte redigeras av användaren. |
| Dölj adressfältet | |
| Vitlistning i webbläsaren (utan Universal Gateway) | Aktiverar vitlistning av URL:er på klientsidan.<br>• Företagets bokmärken är alltid vitlistade<br>• Stöd för endast 100 webbadresser<br>• Använd Universal Gateway för obegränsad svart- och vitlistning |
| Vitlistade webbadresser | En lista över tillåtna webbadresser. |
| Gateway-baserad svart- och vitlistning | Svartlistning har följande krav:<br>• En fungerande AppTec Universal Gateway ("Allmänna inställningar" → "Universal Gateway") |

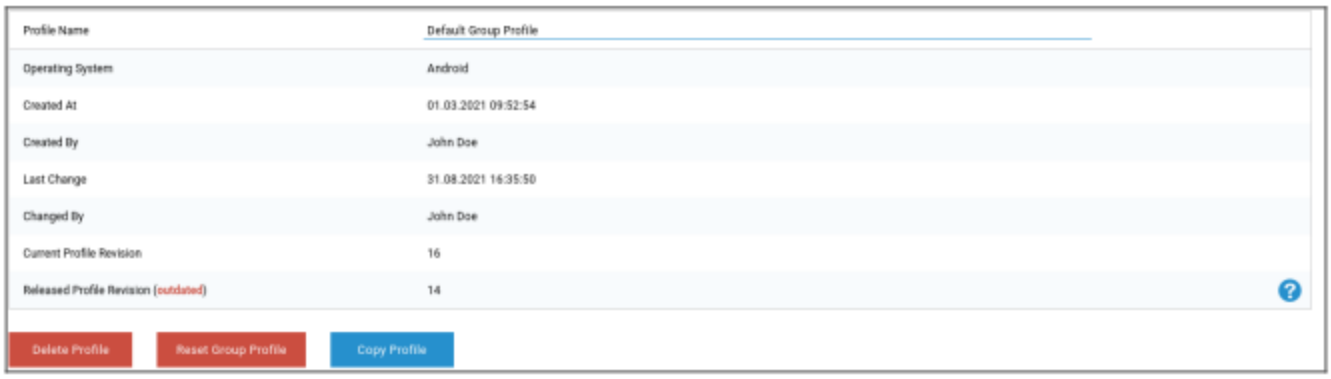
| | |
|---|---|
| | • En fungerande VPN-konfiguration med en angiven DNS-server ("Allmänna inställningar" → "Universal Gateway" → "VPN-inställningar")<br>• En konfiguration för svart lista ("Allmänna inställningar" → "Universal Gateway" → "Svart lista för domäner")<br>• En giltig VPN-anslutning i profilen ("Anslutningshantering" → "VPN") |

# Android-konfiguration

## Allmänt

### Översikt över grupprofiler (endast på gruppnivå)

När du öppnar en grupprofil får du en snabb överblick över profilen.




| | |
|---|---|
| Profilens namn | Profilens namn (kan ändras här) |
| Operativsystem | Operativsystem som profilen är avsedd för |
| Skapad vid | Tidpunkt för skapelse |
| Skapad av | Skaparen av profilen |
| Sista förändringen | Tidpunkt för senaste ändring av profilen |
| Förändrad av | Konto som gjorde de senaste ändringarna |
| Aktuell profil Revidering | Revidering av sparat profiltillstånd |
| Utgiven Profil Revision | Tilldelad profilrevision ("Tilldela nu"). Om etiketten visar "(outdated)" bakom texten betyder det att du har sparat profilen men inte tilldelat den ännu, så enheterna kommer fortfarande att få en äldre version. |

## Enhetsöversikt (endast på enhetsnivå)

Om du befinner dig på en enhet kommer du att få en översiktlig sammanfattning av den valda enheten, följande finns här:

| | |
|---|---|
| Enhetens namn | Enhetens namn |
| Senast kända plats | De senast kända GPS-koordinaterna |
| Telefonnummer | Telefonnummer |
| Tilldelade Obligatoriska appar | Antalet tilldelade obligatoriska appar |
| OS-version | Enhetens OS-version |
| Operativsystem | Operativsystem (Android / iOS / Windows Phone) |
| Serienummer | Enhetens serienummer |
| Ägande av enhet | Företagsenhet eller privat enhet |
| Enhetstyp | Telefon eller surfplatta |
| Rotad | Status, anger om enheten har rotats |
| Överensstämmande | I enlighet med riktlinjerna |
| IP-adress | IP-adress |
| Senast sett | Tidpunkt då enheten senast var ansluten till AppTec |
| Sista knuffen | Tidpunkt då servern skickade en push till enheten |
| Tilldelning av användare | En rullgardinsmeny för att tilldela enheten till en annan användare |

## Config Revision (endast på enhetsnivå)

Här får du en översikt över vilken grupprofil som är tilldelad enheten.


Om du klickar på grupprofilen kommer du direkt till profilen och kan göra inställningar.

Med symbolen kan du återställa de tilldelade apparna till grupprofilens inställningar.

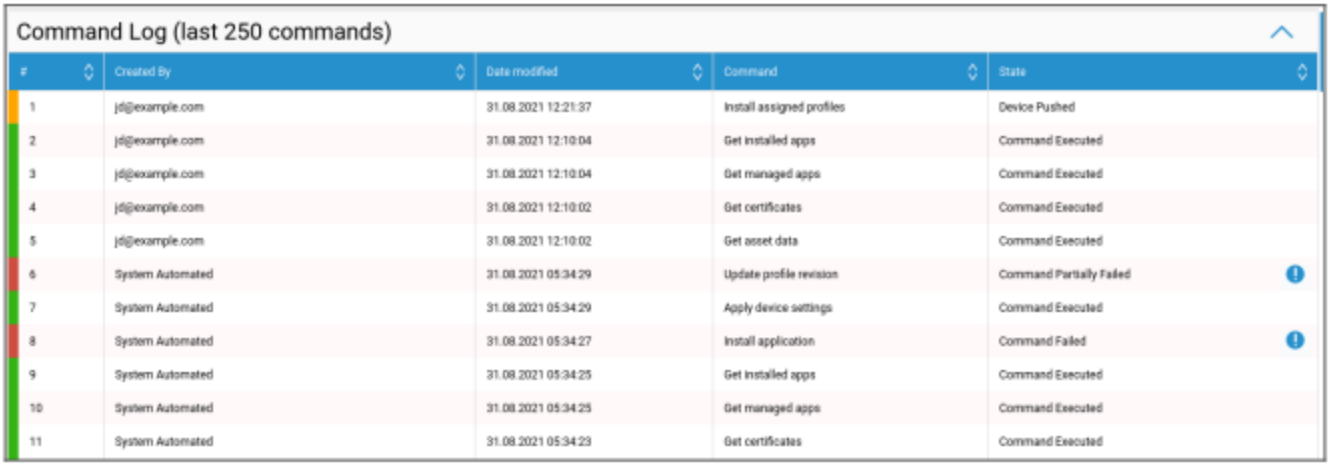
Med symbolen kan du återställa enhetens profil så att den inte har några inställningar alls.

"Nyare revision tillgänglig" anger att grupprofilen har ändrats och sparats men inte tilldelats.
Grupprofilen måste tilldelas med "Tilldela nu" på gruppnivå för att ändringarna ska gälla för enheterna.

## Enhetslogg (endast på enhetsnivå)

### Kommandologg

Här kan du se vilka kommandon som har utfärdats för enheten och vilken status de har.




Kommandon som skapats av "System Automated" skapas automatiskt av systemet.

## Möjliga kommandostatusar

| | |
|---|---|
| Enhet tryckt | En push-begäran har skickats till push-tjänsten (t.ex. APNS) för att tala om för enheten att den ska ansluta tillbaka till EMM-servern. |
| Kommando Skapat | Kommandot skapades i systemet. |
| Kommando skickat | Kommandot skickades till enheten efter att den anslutit till servern. |
| Kommando utfört | Kommandot har utförts framgångsrikt. |
| Kommandot misslyckades | Kommandot misslyckades. * |
| Kommandot delvis misslyckat | Beroende på enhetens operativsystem kan vissa kommandon grupperas tillsammans.<br>I detta misslyckades vissa delar av denna kommandogrupp. * |
| Kommando utfört, eventuellt misslyckat | Kommandot utfördes, men kanske inte. |
| Kommando Repushed | Kommandot återställdes av en användare. |
| Bortkastad | Kommandot kasserades. Till exempel för att det ersattes av ett annat kommando eller för att enheten registrerades på nytt och gamla kommandon togs bort |

*Om det finns ett utropstecken bakom meddelandet kan du få mer information genom att hålla muspekaren över ikonen.

# Inställningar för enhet

## Konfiguration av klient

Här kan du utföra följande konfigurationer på din Android-enhet:

| | |
|---|---|
| Varningsmeddelande efter inaktivering av Enhetshantering | Upprättat varningsmeddelande efter inaktivering av Device Management |
| Tid för bristande efterlevnad | Tidsgräns efter vilken "verkställighetsåtgärd efter överensstämmelse" kommer att utföras om enheten inte överensstämmer med kraven.<br>Min. 1 minut<br>Max. 24 timmar |
| Verkställighetsåtgärd efter timeout för efterlevnad | Den åtgärd som ska vidtas så snart en enhet inte längre uppfyller kraven.<br>• gör ingenting = ingen åtgärd<br>• Lock Device = låsa enhet<br>• Wipe Device = enheten återställs till fabriksinställningarna |
| Frekvens för datainsamling | Frekvens med vilken enhet/GPS-information ska samlas in |
| Frekvens för enhetens hjärtslag | Intervall inom vilket enheten ska kontakta AppTec360 Server<br>Min. 1 minut<br>Max. 24 timmar |
| Aktivera platsuppdateringar | Om den är aktiverad skickar enheten platsuppdateringar till AppTec360 Server |
| Plats Uppdateringstid | Bestämmer i vilka tidsintervall enheten skickar platsuppdateringar till AppTec |
| Använd Google Location Accuracy för platsuppdatering | Om den är aktiverad kommer Google Location Accuracy (tidigare känd som nätverksposition) att användas för platsuppdateringar (om detta avaktiverades under "Begränsningar" kommer den här inställningen inte att påverka någonting) |
| Använd GPS-position för platsuppdatering | Om den är aktiverad används GPS för platsuppdateringar |
| Tillåt falska platser (Mock) | Möjliggör förfalskning av platsinformation via appar från tredje part |

| | |
|---|---|
| Åtgärder vid förlorad anslutning | Gör det möjligt att ställa in en viss åtgärd som ska utföras efter ett visst antal misslyckade hjärtslag |
| Läge för tillämpning av policy | Definierar hur aggressivt AppTec360 Client ber användaren att utföra vissa åtgärder som kräver användarinmatning.<br>Interval (Default) = fråga i intervaller, så att användaren kan låta den gå i bakgrunden ett tag.<br>Ingen varning = ingen popup för någon nödvändig interaktion. Du måste öppna AppTec360 Client manuellt för att kontrollera om det finns en nödvändig åtgärd<br>Constant Alert = Användaren kan bara utföra den åtgärd som krävs. AppTec360 Client kommer att tvinga sig in i förgrunden om användaren försöker undvika det |
| AppTec360 Versionslås | Låter dig definiera en version av AppTec360 Client som är den maximala versionen som klienten uppdaterar sig själv till. |

### Bakgrund

Här kan du definiera en anpassad bakgrundsbild.

Med "Specify a Color" kan du definiera en färg i hex-format (t.ex. #000000). Endast hexadecimala värden är tillåtna.

"Ange bild som bakgrundsbild" låter dig ladda upp en bild. Tänk på att olika enheter med olika startprogram och OS-versioner fungerar på olika sätt. Det finns inga generella riktlinjer för storlek och förhållande, eftersom detta beror på enheten.

Använd JPG (eller JPEG) eller PNG som filformat.

## Tillgångshantering (endast på enhetsnivå)

### Kapitalförvaltning

## Info om enhet

| **Modell** | **Enhetens modellbeteckning** |
|---|---|
| Operativsystem | OS |
| OS-version | OS-version |
| AE Support | Stöd för Android Enterprise (container och fullt hanterad) |
| Serienummer | Serienummer |
| Enhetens namn | Enhetens namn |
| Batteristatus | Batteriets status |
| Fritt / totalt minne | Fritt / Totalt minne |
| Samsung KNOX | Samsung KNOX API-nivå |
| SD-kort tillgängligt | SD-kort tillgängligt |
| SD-kort emulerat | SD-kort emulerat |
| SD-kort löstagbart | SD-kort kan tas ut |
| SD Fritt / Totalt minne | SD Fritt / Totalt minne på SD-kort |

## Wi-Fi

| | |
|---|---|
| IP-adress | Enhetens IP-adress |
| WiFi MAC | WiFi MAC-adress |

## Cellulär

| | |
|---|---|
| Status | Status (SIM-kortet installerat) |
| Telefonnummer | Telefonnummer |
| Roaming (röst/data) | Roaming för röst/data |
| Status för roaming | Aktuell roamingstatus |
| IP-adress | IP-adress |
| Operatör/transportör | Operatör/transportör |
| Cellulär teknik | Cellulär teknik |
| IMEI | IMEI-nummer |
| ICCID | Detta är ID för SIM-kortet, ofta även ett smartkort eller ett Integrated Circuit Card (ICC) |
| IMSI | IMSI (International Mobile Subscriber Identity) ger i GSM- och UMTS-mobilnät en definitiv identifiering av nätanvändarna<br>IMSI består av maximalt 15 siffror och konfigureras på följande sätt:<br>• Mobil landskod (MCC), 3 siffror<br>• Mobilnätskod (MNC), 2 eller 3 siffror<br>• Identifieringsnummer för mobilabonnent (MSIN), 1-10 siffror |
| Nuvarande MCC/MNC | Se "SIM MCC/MNC" |
| SIM MCC/MNC | Mobile Country Code är en etablerad landsidentifierare, fastställd av ITU enligt E.212-standarden. Den fungerar tillsammans med Mobile Network Code (MNC) för identifiering av mobilnätet.<br>Betyder SIM-kortets landskod/Mobile Network Code.<br>Om du roamar till ett annat mobilnät kommer logiskt sett "Current MCC/MNC" och "SIM MCC/MNC" att vara olika. |

## Bluetooth

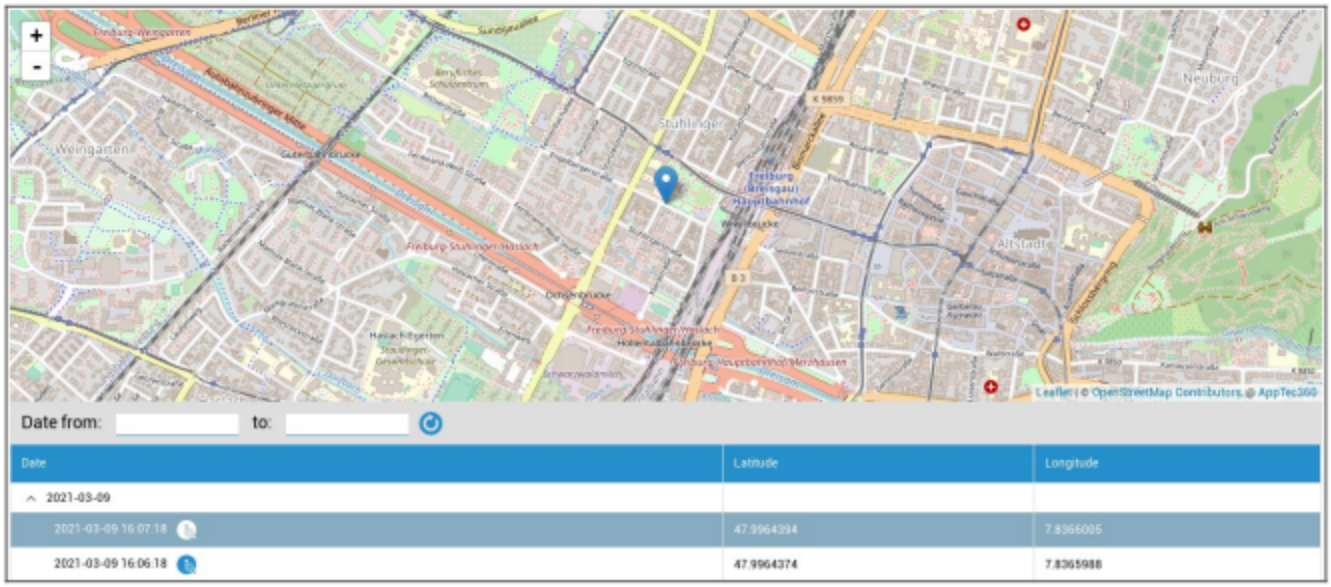
| | |
|---|---|
| Bluetooth MAC | Bluetooth MAC-adress |

# Säkerhetshantering

## Stöldskydd (endast på enhetsnivå)

### GPS-information (endast på enhetsnivå)

Här kan du ange aktuell/senaste enhetsplats. Lokaliseringen kan skyddas med ett eller till och med två lösenord - se: Allmänna inställningar - Sekretess - GPS-åtkomst



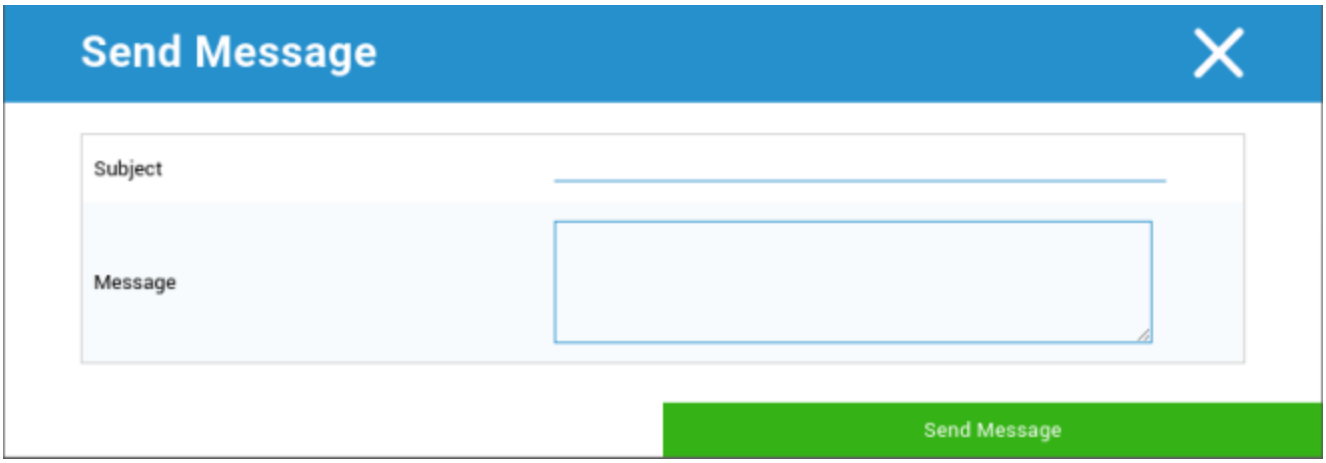

## Wipe & Lock (endast på enhetsnivå)

Under "Wipe & Lock" kan du utföra följande tre åtgärder:

| | |
|---|---|
| Fullständig avtorkning | Enheten återställs till fabriksinställningarna (både företagsdata och personuppgifter raderas) |
| Enterprise Wipe | Endast företagsdata tas bort från slutanvändarens enhet (alla appar, data etc. som tillhandahölls av AppTec360) |
| Lås skärm | Om skärmlåset är aktiverat räcker det med att låsa upp enheten med enhetens lösenord/PIN |

## Meddelande (endast på enhetsnivå)

Du kan fylla i ämnet och ett meddelande och skicka det till en slutanvändarenhet. Detta meddelande kommer att visas i AppTec360 Client.




## Säkerhetskonfiguration

### Lösenord

Under "Passcode" kan du ange ett lösenord för enheten, följande inställningsalternativ är tillgängliga för dig

| | |
|---|---|
| Minsta lösenordslängd | Fastställer det minsta antal symboler som ett lösenord måste innehålla |
| Lösenordskvalitet | Lösenordets styrka<br>Ospecificerad = inte specificerad<br>Varje lösenord är ok = varje lösenord är acceptabelt<br>at least numeric characters = måste innehålla minst numeriska tecken<br>minst komplexa tecken = måste innehålla minst specialtecken<br>at least alphanumerical characters = måste innehålla minst alfanumeriska tecken<br>at least alphabetic characters = måste innehålla minst alfabetiska tecken |
| Lås för maximal inaktivitetstid | Maximal timeout för skärmen. Detta konfigurerar endast det maximala värde som kan väljas av användaren |
| Minst små bokstäver krävs i lösenordet | Minst små bokstäver krävs i lösenordet |
| Minimikrav på versaler i lösenordet | Minimikrav på versaler i lösenordet |
| Minsta antal tecken som inte är bokstäver som krävs i lösenordet | Minsta antal tecken som inte är bokstäver som krävs i lösenordet |
| Minsta antal numeriska siffror som krävs i lösenordet | Minsta antal numeriska siffror som krävs i lösenordet |
| Minsta antal symboler som krävs i lösenordet | Minsta antal symboler som krävs i lösenordet |
| Tidsgräns för lösenordsutgång | Fastställer, efter vilket tidsintervall lösenordet upphör att gälla och ett nytt lösenord måste utfärdas |
| Begränsning av lösenordshistorik | Antal tidigare använda lösenord som inte är tillåtna |
| Maximalt antal misslyckade lösenordsförsök | Fastställer hur ofta ett lösenord kan anges felaktigt innan en fullständig radering av enheten utförs |

## Kryptering

Under denna punkt kan du kryptera enhetens interna minne samt SD-kortets minne.

| | |
|---|---|
| Kräv kryptering av lagringsutrymme | Om den här inställningen är aktiverad krypteras enhetens minne, så länge enheten har stöd för den här funktionen.<br>När enhetens minne har krypterats för första gången är det inte längre möjligt att avkryptera det.<br>På samma sätt kommer lösenordspolicyn automatiskt att ändras till 6 alfanumeriska symboler |
| Kräv kryptering av SD-kort | Denna inställning gäller endast för Samsung-enheter!<br>Om denna inställning är aktiverad kan det externa SD-kortet krypteras och kan endast avkrypteras manuellt på slutanvändarens enhet.<br>På samma sätt kommer lösenordspolicyn automatiskt att ändras till 6 alfanumeriska symboler |

## AntiVirus

Om du aktiverar AntiVirus kommer Ikarus att installeras på enheterna. Observera att detta kräver en separat licens som kan anges i Allmänna inställningar → Apphantering → Tredjepartsappar.

| | |
|---|---|
| Automatisk skanning | Definierar om Ikarus skannar automatiskt eller inte och hur ofta den utför denna skanning<br>Om du aktiverar "Full Automatic Scan" utförs en fullständig skanning. I annat fall utförs en snabb skanning |
| Automatiska uppdateringar | Aktiverar automatiska uppdateringar av virusdatabasen och ställer in hur ofta detta ska ske |
| Skydd för appar | Möjliggör skanning av appar utöver den vanliga skanningen som bara skannar filer |
| Skydd för SD-kort | Aktiverar skydd för SD-kort. Utan detta begränsas skanningen till det lokala lagringsutrymmet |
| Uppdatering endast för Wi-Fi | Begränsar uppdatering till Wi-Fi |

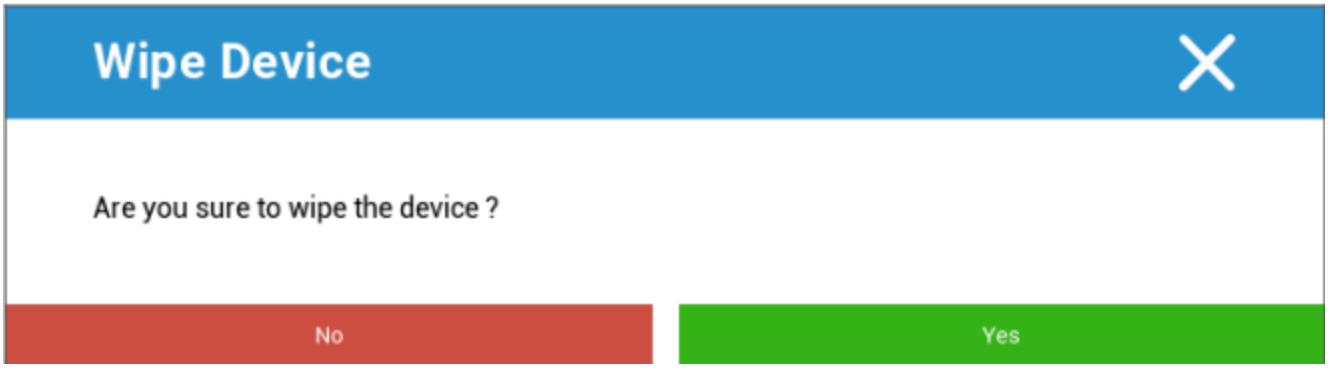
# End of Life (endast på enhetsnivå)

## Torka (endast på enhetsnivå)

Under "Wipe" kan du återställa enheten till fabriksinställningarna. Här kommer företagsdata och privata data att raderas på slutanvändarens enhet.

Genom att klicka på "Minus-symbolen" får du följande meddelande

| | |
|---|---|
| Torka SD-kort också? | SD-kortets minne kommer också att raderas |




Med "Yes" kan du utföra torkningen.

Under "Wipe Report" kan följande objekt visas

| | |
|---|---|
| Raderad av | Historik över vem som utförde torkningen |
| Datum | Datum |
| Status | Status (t.ex. om rensningen utfördes framgångsrikt) |

## Inställningar för begränsning

### Begränsningar

Här kan en mängd olika saker begränsas och blockeras.

| | |
|---|---|
| Aktivera kamera | Tillåt användning av kamera |
| Tvinga fram automatisk synkronisering | Relaterar till "Sync"-gränssnittet<br>On = synkroniseringen är permanent aktiverad<br>Off = synkroniseringen är permanent avaktiverad<br>Användarval = väljs av användaren |
| Force Bluetooth | On = Bluetooth är permanent aktiverat<br>Off = Bluetooth är permanent avaktiverat<br>Användarval = väljs av användaren |
| Force GPS | On = GPS är permanent aktiverad<br>Off = GPS är permanent avaktiverad<br>Användarval = väljs av användaren |
| Forcera Googles platsnoggrannhet | On = Permanent internetlokalisering<br>Off = Permanent avaktivering av internetlokalisering<br>Användarval = väljs av användaren |

För Samsung-enheter med gränssnittet KNOX 1.0 eller högre finns följande inställningsmöjligheter tillgängliga.

| | |
|---|---|
| Tillåt SD-kort | Tillåt SD-kort |
| Tillåt skrivning av SD-kort | Tillåt "skrivning" på SD-kortet |
| Tillåt skärmupptagning | Tillåt skärmdump |
| Tillåt urklipp | Tillåt urklipp |
| Säkerhetskopiera inställningar och appdata i Google Cloud | Av = inaktivera Google Backup<br>On = aktivera Google Backup<br>User Choice = väljs av användaren |
| Tillåt USB-felsökning | Tillåt USB-felsökning (används t.ex. för att skapa enhetsloggar (ADB)) |
| Tillåt Googles kraschrapport | Tillåt att Google Crash Report skickas från apparna |
| Tillåt fabriksåterställning | Gör det möjligt för användaren att återställa enheten till fabriksinställningarna |
| Tillåt OTA-uppgradering | Tillåt uppdateringar "over-the-Air" |
| Tillåt USB-hostlagring | Om den är aktiverad kan ett USB-minne i form av en HD- eller SD-kortläsare anslutas |
| Tillåt USB Media Player (MTP,PTP) | Tillåt USB Media Player (MTP,PTP) |
| Tillåt mikrofon | On = tillåt mikrofon för appar från tredje part<br>Off = blockera mikrofonen för appar från tredje part<br>User Choice = användarna kan välja om 3rd Party-appen har tillgång till mikrofonen |
| Tillåt NFC (Near Field Communication) | Tillåt NFC |
| Tillåt okända källor (APK Sideloading) | Om den är aktiverad tillåts sidoladdning av appar (APK-filer). När den här inställningen är inaktiverad måste användaren aktivera den manuellt när du tillåter installation av APK:er från okända källor. |
| Tillåt skapande av användare | Möjliggör skapande av flera användare |

## Ägare av AE-enhet

(Enheten måste vara i Android Enterprise Device Owner Mode) Det rekommenderas att skapa enheterna som "Android Enterprise"-enhet och inte som "Android"-enhet.

| Säkerhet | |
|---|---|
| Avvisa delningsplats | Anger om en användare inte får aktivera platsdelning. |
| Avvisa säker start | Anger om användaren inte har rätt att starta om enheten till säkert startläge. |
| Tillåt inte återställning av nätverk | Anger om en användare inte får återställa nätverksinställningar från Settings. |
| Avvisa fabriksåterställning | Anger om en användare inte får återställa enheten. |
| Aktivera ADB | Möjliggör anslutning till en PC via ADB |
| Avaktivera nyckelvakt | Avaktiverar nyckelvakt |
| Enhetens ägare Info om låsskärm | Anger vilken information om enhetens ägare som ska visas på låsskärmen. |
| Tillämpning av efterlevnad | Mode Prompt User - Användaren kommer att uppmanas att utföra nödvändiga åtgärder.<br>Mode Lock-Down Container - Dölj alla appar tills alla krav har uppfyllts |

| App-hantering | |
|---|---|
| Tillåt applänkning över profilgränser | Tillåter appar i den överordnade profilen att hantera webblänkar från den hanterade profilen. |
| Avvisa appkontroll | Anger om en användare inte får ändra program i inställningar eller startprogram. |
| Avvisa installation av app | Anger om en användare inte får installera program. |
| Tillåt inte avinstallation av appar | Anger om en användare inte får avinstallera program. |
| Policy för körtidsbehörighet | Anger hur nya behörighetsförfrågningar från appar ska hanteras. |
| Tillåt okända källor | Om den är aktiverad kan användare ladda appar genom att installera en .apk-fil. |

| Anslutningsmöjligheter | |
|---|---|
| Avvisa konfiguration av mobilnätverk | Anger om en användare inte får konfigurera mobila nätverk. |
| Tillåt inte internetdelning Konfig | Anger om en användare inte får konfigurera internetdelning och portabla hotspots. |
| Avvisa VPN-konfiguration | Anger om en användare inte får konfigurera ett VPN. |
| Tillåt inte Wifi-konfiguration | Anger om en användare inte får ändra WiFi-åtkomstpunkter. |
| Avvisa utgående NFC-strålning | Anger om användaren inte får använda NFC för att skicka ut data från appar. |
| Lås WiFi-konfiguration | Den här inställningen styr om WiFi-konfigurationer som skapats av en app för enhetsägare ska vara låsta (dvs. endast kunna redigeras eller tas bort av appen för enhetsägare, inte ens av appen Settings). |
| Aktivera data-roaming | Aktiverar data-roaming |

| Bluetooth | |
|---|---|
| Avvisa Bluetooth | Anger om Bluetooth inte är tillåtet på enheten. Kräver Android 8.0 |
| Avaktivera Bluetooth-delning | Anger om utgående Bluetooth-delning inte är tillåten på enheten. Kräver Android 8.0 |
| Avvisa Bluetooth-konfiguration | Anger om en användare inte får konfigurera Bluetooth. |

| Kontohantering | |
|---|---|
| Tillåt inte att lägga till hanterad profil | Anger om en användare inte ska tillåtas att lägga till hanterade profiler. Kräver Android 8.0 |
| Tillåt inte att lägga till användare | Anger om en användare inte får lägga till nya användare. |
| Avvisa Ta bort hanterad profil | Anger om hanterade profiler för den här användaren kan tas bort av andra än profilägaren. Kräver Android 8.0 |
| Förbjuda ändring av konto | Anger om en användare inte ska tillåtas att lägga till och ta bort konton, såvida de inte läggs till programmatiskt av Authenticator. |

| Telefoni | |
|---|---|
| Avvisa utgående samtal | Anger att användaren inte får ringa utgående telefonsamtal. |
| Avvisa SMS | Anger att användaren inte får skicka eller ta emot SMS-meddelanden. |

| System | |
|---|---|
| Tillåt inte skapande av fönster | Anger att andra fönster än app-fönster inte ska skapas. |
| Avvisa inställd användarikon | Anger om en användare inte får ändra sin ikon. |
| Tillåt inte Set Wallpaper | Användarbegränsning för att inte tillåta inställning av bakgrundsbild. |
| Inaktivera statusfältet | Genom att inaktivera statusfältet blockeras aviseringar, snabbinställningar och andra skärmöverlägg som gör det möjligt att fly från en enhet som bara används en gång. |
| Aktivera automatisk tid | Ställer in tiden automatiskt. |
| Aktivera automatisk tidszon | Tidszonen ställs in automatiskt. |
| Står på när den är inkopplad | Enheten förblir aktiv när den är ansluten till en strömkälla. |

| Förvaring | |
|---|---|
| Avvisa inaktivera appverifiering | Anger om en användare inte får inaktivera programverifiering. |

| | |
|---|---|
| Tillåt inte montering av fysiska medier | Anger om en användare inte får montera fysiska externa media. |
| Aktivera säkerhetskopieringstjänst | Säkerhetskopieringstjänsten hanterar alla mekanismer för säkerhetskopiering och återställning på enheten. Om du anger false förhindras att data säkerhetskopieras eller återställs. Säkerhetskopieringstjänsten är avstängd som standard. Kräver Android 8.0 |
| Aktivera USB-masslagring | Aktiverar användning av USB Mass Storage. |

| **Tangentbord** | |
|---|---|
| Avvisa autofyllning | Anger om en användare inte får använda Autofyll Services. Kräver Android 8.0 |
| Förbjud kopiera och klistra in mellan profiler | Anger om det som kopieras i urklippet i den här profilen kan klistras in i relaterade profiler. |

| **Ljud** | |
|---|---|
| Avslå volymjustering | Anger om en användare inte får justera mastervolymen. |
| Avvisa Stäng av mikrofonen | Anger om en användare inte får justera mikrofonens volym. |
| Mute-enhet | Mute-enhet. |

| **Policy för systemuppdateringar** | |
|---|---|
| Kontrollera OS-uppdateringar | Aktivera detta för att ställa in uppdateringsbeteendet till automatiskt, i fönster eller uppskjutet. |

# BYOD Container

## Android Företag

### Android Företag

| | |
|---|---|
| Aktivera Android Enterprise | Aktivera Android Enterprise (AE). AE stöds från och med Android 5.1 och senare. |
| Tillämpning av efterlevnad | Mode Prompt User - Användaren kommer att uppmanas att utföra nödvändiga åtgärder.<br>Mode Lock-Down Container - Dölj alla appar tills alla krav har uppfyllts |
| Policy för körtidsbehörighet | Fråga användaren om nya behörighetsförfrågningar<br>Bevilj alltid nya ansökningar om tillstånd<br>Avslå alltid nya förfrågningar om tillstånd<br>Varning för problem: Vissa appar har problem med att känna igen behörigheterna om dessa ställs in automatiskt. Om du alltid beviljar behörigheter och får problem med appar som säger att behörigheter saknas, ställ in detta på "fråga användaren" och installera om appen |
| Tillåt utgående urklipp | Tillåter kopiering och klistring från insidan av behållaren till utsidan |
| Tillåt upplösning av nummerpresentation | Visar namnet för ett inkommande samtal baserat på kontakter i behållaren |
| Tillåt kontaktsökningsupplösning | Gör det möjligt att söka efter namn i behållarens kontakter när du ringer |
| Tillåt kontaktdelning via Bluetooth | Tillåter åtkomst till behållarkontakt i en bil |
| Avvisa utgående NFC-strålning | Avaktiverar NFC för behållaren |
| Tillåt okända källor | Om den är aktiverad kan användare ladda appar genom att installera en .apk-fil. |
| Tillåt USB-felsökning | Om den är aktiverad kan användare aktivera USB Debugging. |
| Förbjuda ändring av konto | Tillåter inte att konton i behållaren skapas, raderas eller ändras<br>Tänk på att vissa appar behöver skapa eller ändra konton för att fungera som förväntat |

## Gmail Exchange

Gör att du kan konfigurera Gmail i containern. Tänk på att appen inte installeras automatiskt om du aktiverar den här konfigurationen. Du måste fortfarande lägga till den här appen som obligatorisk app.

| | |
|---|---|
| E-postadress | E-postadress |
| Serverns värdnamn | Serverns värdnamn |
| Inloggningsnamn | Inloggningsnamn |
| Underskrift | Underskrift |
| Antal föregående dagar att synkronisera | Antal föregående dagar som ska synkroniseras. |
| Enhetens identifierare | EAS-identifierare. Lämna detta tomt om din miljö inte kräver detta |
| Använd SSL (Secure Sockets Layer) | Aktiverar användning av SSL. Om du avaktiverar detta kan säkerheten försämras |
| Acceptera alla certifikat | Accepterar alla certifikat. Om du aktiverar detta kan säkerheten försämras |
| Tillåt oadministrerade konton | Gör det möjligt för användaren att lägga till ytterligare konton |
| Kundcertifikat | Ladda upp klientcertifikat om din Exchange-server kräver detta |

## Appar för AE-system

Här kan du aktivera systemappar för Android Enterprise Container. Tänk på att den angivna appen måste finnas i systemets lagringsutrymme, annars händer ingenting.

## Container lösenord

Endast för Android 7.0 eller högre

Gör det möjligt att ställa in ett specifikt lösenordskrav för behållaren.

| | |
|---|---|
| Minsta lösenordslängd | Fastställer det minsta antal symboler som ett lösenord måste innehålla |
| Lösenordskvalitet | Lösenordets styrka<br>Ospecificerad = inte specificerad<br>Varje lösenord är ok = varje lösenord är acceptabelt<br>at least numeric characters = måste innehålla minst numeriska tecken<br>minst komplexa tecken = måste innehålla minst specialtecken<br>at least alphanumerical characters = måste innehålla minst alfanumeriska tecken<br>at least alphabetic characters = måste innehålla minst alfabetiska tecken |
| Lås för maximal inaktivitetstid | Maximal tid tills containern blir låst. Detta konfigurerar endast det maximala värdet som kan väljas av användaren |
| Minst små bokstäver krävs i lösenordet | Minst små bokstäver krävs i lösenordet |
| Minimikrav på versaler i lösenordet | Minimikrav på versaler i lösenordet |
| Minsta antal tecken som inte är bokstäver som krävs i lösenordet | Minsta antal tecken som inte är bokstäver som krävs i lösenordet |
| Minsta antal numeriska siffror som krävs i lösenordet | Minsta antal numeriska siffror som krävs i lösenordet |
| Minsta antal symboler som krävs i lösenordet | Minsta antal symboler som krävs i lösenordet |
| Tidsgräns för lösenordsutgång | Fastställer, efter vilket tidsintervall lösenordet upphör att gälla och ett nytt lösenord måste utfärdas |
| Begränsning av lösenordshistorik | Antal tidigare använda lösenord som inte är tillåtna |
| Maximalt antal misslyckade lösenordsförsök | Fastställer hur ofta ett lösenord kan anges felaktigt innan behållaren raderas |

# Samsung KNOX

## Aktivering

Här kan du aktivera Samsung KNOX Container. Tänk på att detta inte längre stöds av Samsung på Android 10 eller senare. Använd Android Enterprise Container på Android 10 eller högre

## Knox-lösenord

Upprätta riktlinjer för inställningarna av enhetens lösenord

| | |
|---|---|
| Minsta lösenordslängd | Fastställer, hur många symboler lösenordet måste ha |
| Lösenordskvalitet | Lösenordets styrka<br>Alla lösenord är ok = Alla lösenord är ok<br>Minst numeriska tecken = Minst numeriska tecken måste finnas<br>Minst komplexa tecken = Minst specialtecken måste finnas<br>Minst alfanumeriska tecken = Minst alfanumeriska tecken måste finnas<br>Minst alfabetiska tecken = Minst alfabetiska tecken måste finnas |
| Minst komplexa tecken krävs | Minst komplexa tecken måste finnas |
| Maximal tidsgräns för inaktivitet | Maximal tidsgräns för inaktivitet hos användaren, före tangentbordslås |
| Tillåt autentisering med fingeravtryck | Tillåt autentisering med fingeravtryck |
| Tillåt Iris-autentisering | Tillåt autentisering med irisigenkänning |
| Max lösenordsålder | Fastställer efter vilken tid lösenordet upphör att gälla och ett nytt lösenord måste utfärdas |
| Historik över sparade lösenord | Antal tidigare lösenord som inte är tillåtna |
| Maximalt antal misslyckade lösenordsförsök | Fastställer hur ofta lösenordet får anges felaktigt innan en fullständig radering av enheten sker |

## Knox Säkerhet

Begränsa specifika enhetsfunktioner

| | |
|---|---|
| Aktivera kamera | Tillåt användning av kameran |
| Tillåt Samsung KNOX App Store | Tillåt användning av Samsung KNOX App Store |
| Tillåt Google Play-tjänster | Tillåt Google Play-tjänster |
| Tillåt webbläsare | Tillåt användning av den inbyggda webbläsaren |
| Tillåt skärmdumpar | Tillåt skapande av skärmdumpar |
| Tillåt import av kontakter | Om den är aktiverad tillåts åtkomst till enhetskontakter från KNOX-behållaren |

| | |
|---|---|
| Tillåt export av kontakter | Om den är aktiverad är åtkomst till KNOX-kontakterna från enheten tillåten |
| Tillåt import av kalender | Om den är aktiverad tillåts åtkomst till enhetskalendern från KNOX-behållaren |
| Tillåt export av kalender | Om den är aktiverad är åtkomst till KNOX-kalendern från enheten tillåten |
| Tillåt icke-säkert tangentbord | Tillåt användning av en icke-säker knappsats |
| Aktivera filimport | Aktivera filimport till KNOX-behållaren |
| Aktivera filexport | Aktivera filexport från KNOX-behållaren |

## Knox Exchange

Här kan du konfigurera Exchange-profilen för KNOX-behållaren

| | |
|---|---|
| E-postadress | Den angivna användarens e-postadress<br>Observera "platshållarna", som du kan använda för att arbeta med referenser och du behöver inte utföra ändringar manuellt på varje enhet<br>Med ett klick på **Show Placeholders** kan du visa dem för dig själv |
| Serverns värdnamn | Serveradress till dina Exchange-servrar |
| Inloggningsnamn | Inloggningsnamnet för respektive slutanvändarenhet, observera även "platshållarna" här |
| Domän | Domänadress |
| Lösenord (endast på enhetsnivå) | Alternativt kan en enskild enhet förses med ett lösenord, om detta förblir tomt kommer användaren att uppmanas att ange sitt Exchange-lösenord |
| Antal föregående dagar att synkronisera | Antal dagar som avgör när e-postmeddelanden synkroniseras tillbaka |
| Underskrift | En signatur kan bifogas |
| Standardkonto | Fastställer att det här e-postkontot är standardkontot |
| Använd SSL (Secure Sockets Layer) | Använd en SSL-anslutning |
| Använd TLS (Transport Layer Security) | Använd en TLS-anslutning |
| Acceptera alla certifikat | Alla certifikat accepteras. Välj detta alternativ om Exchange Server använder ett självsignerat certifikat |

## Knox eMail

| | |
|---|---|
| E-postadress | Den angivna användarens e-postadress<br>Observera "platshållarna", som du kan använda för att arbeta med referenser och du behöver inte utföra ändringar manuellt på varje enhet<br>Med ett klick på **Show Placeholders** kan du visa dem för dig själv |
| Protokoll för inkommande server | Protokoll för inkommande server<br>IMAP eller POP |
| Adress till inkommande server | Adress till inkommande server |
| Port för inkommande server | Port för inkommande server |
| Inloggning/användarnamn för inkommande server | Inloggning/användarnamn för inkommande server |
| Lösenord för inkommande server | Lösenord för inkommande server |
| Inkommande server använder SSL | Inkommande server använder SSL |
| Inkommande server använder TLS | Inkommande server använder TLS |
| Inkommande server accepterar alla certifikat | Den inkommande servern accepterar alla typer av certifikat |
| Protokoll för utgående server | Protokoll för utgående server<br>SMTP |
| Utgående serverport | Utgående serverport |
| Utgående server använder extra autentiseringsuppgifter | Ytterligare autentiseringsuppgifter för den utgående servern. Om den här inställningen är "off" används inställningarna för den inkommande servern |
| Inloggning/användarnamn för utgående server | Inloggning/användarnamn för utgående server |
| Lösenord för utgående server | Lösenord för utgående server |
| Utgående server använder SSL | Utgående server använder SSL |
| Utgående server använder TLS | Utgående server använder TLS |
| Utgående server accepterar alla certifikat | Utgående server accepterar alla typer av certifikat |
| Underskrift | Här kan en signatur bifogas |
| Meddela användaren om mottagande av nytt eMail | Meddela användaren om mottagande av nytt eMail |

### Knox Appar

Här kan du skapa appar som du vill distribuera till slutanvändarens enheter. Dessa kommer sedan att finnas tillgängliga i KNOX-Containern. För att lägga till en app ska du gå tillväga på samma sätt som i menyn Obligatoriska appar

| | |
|---|---|
| Applikationens namn | Applikationens namn |
| Obligatoriskt sedan | Tidpunkt, när appen lades till |
| Källa | Appens källa (Play Store \| Internt) |

Genom att klicka på symbolen kan respektive app tas bort igen

## Hantering av anslutningar

### Wifi

För denna inställning, utför förkonfigurationen av slutanvändarens enheter, för åtkomst till interna åtkomstpunkter

| | |
|---|---|
| Identifierare för tjänsteuppsättning (SSID) | SSID för det nätverk som ska anslutas |
| Dolda nätverk | Aktivera, om AP:n inte sänder SSID |
| Typ av säkerhet | Fastställ AP:ns säkerhetstyp |

### Typ av säkerhet

#### WEP

| | |
|---|---|
| Lösenord | Lösenord för AP:n |

#### WPA/WPA2

| | |
|---|---|
| Lösenord | Lösenord för AP:n |

#### 802.1x EAP

| | |
|---|---|
| **EAP-metod** | |

| | | |
|---|---|---|
| PWD | Identitet | Identitet |

| | | |
|---|---|---|
| | Lösenord | Lösenord |

| | | | |
|---|---|---|---|
| PEAP | Fas 2 autentiseringsprotokoll | ingen | Inget ytterligare protokoll |
| | | MSCHAPV2 | MSCHAPV2-protokoll |
| | | GTC | GTC-protokoll |
| | CA-certifikat | CA-certifikat | |
| | Identitet | Identitet | |
| | Anonym identitet | Anonym identitet | |
| | Lösenord | Lösenord | |

| | |
|---|---|
| **EAP-metod** | |

| | | | |
|---|---|---|---|
| TTLS | Fas 2 autentiseringsprotokoll | ingen | Inget ytterligare protokoll |
| | | PAP | PAP-protokoll |
| | | MSCHAP | MSCHAP-protokoll |
| | | MSCHAPV2 | MSCHAPV2-protokoll |
| | | GTC | GTC-protokoll |
| | CA-certifikat | CA-certifikat | |
| | Identitet | Identitet | |
| | Anonym identitet | Anonym identitet | |
| | Lösenord | Lösenord | |

| | | |
|---|---|---|
| TLS | CA-certifikat | CA-certifikat |
| | Identitet | Identitet |
| | Lösenord | Lösenord |

## VPN

| | |
|---|---|
| **Typ av anslutning** | **Upprätta typ av VPN-anslutning** |

Om du väljer "Per-App VPN" som VPN-typ ändras de tillgängliga VPN-klienterna. Per-App VPN begränsar VPN till vissa appar och startar VPN-anslutningen automatiskt om en specifik app startas.

| | |
|---|---|
| AppTec360 VPN-klient | Använder AppTec360 VPN Client i kombination med Universal Gateway |
| Namn på anslutning | Namn på VPN-anslutning |
| Gateway-konfiguration | Välj VPN-konfiguration för Universal Gateway |
| Alltid på VPN | Tvingar VPN att alltid vara aktivt, så att all trafik går genom VPN. |
| Aktivera Native Lockdown | Blockerar allt nätverkande när enheten inte är ansluten till VPN. Använd detta med försiktighet eftersom det kan leda till att hela anslutningen bryts om det inte konfigureras korrekt. Endast för Android Enterprise på Android 7 eller högre |
| Aktivera AppTec360 Lockdown | Blockerar användningen av alla appar tills VPN-anslutningen har startats |

| Cisco AnyConnect | |
|---|---|
| Namn på anslutning | Namn på VPN-anslutning |
| Server | Serveradress |
| Certifikatläge | Disabled = avaktiverad<br>Automatisk = automatisk |

| | |
|---|---|
| L2TP (endast KNOX) | Endast tillgänglig på Samsung-enheter |
| Namn på anslutning | Namn på anslutning |
| Server | Serveradress |
| Aktivera L2TP-hemlighet | |
| DNS-sökning Domäner | DNS-sökning domäner |

| **Typ av anslutning** | **Upprätta typ av VPN-anslutning** |
|---|---|

| | |
|---|---|
| PPTP (endast KNOX) | Endast tillgänglig på Samsung-enheter |
| Namn på anslutning | Namn på VPN-anslutning |
| Server | Serveradress |
| Aktivera kryptering | Aktivera kryptering |
| DNS-sökning Domäner | DNS-sökning domäner |

| | |
|---|---|
| L2TP / IPSec PSK (endast KNOX) | Endast tillgänglig på Samsung-enheter |
| Namn på anslutning | Namn på VPN-anslutning |
| Server | Serveradress |
| IPSec Förhandsdelad nyckel | Förhandsdelad nyckel för autentisering |
| Aktivera L2TP-hemlighet | |
| L2TP-hemlighet | |
| DNS-sökning Domäner | DNS-sökning domäner |

| | |
|---|---|
| IPSec XAuth PSK (endast KNOX) | Endast tillgänglig på Samsung-enheter |
| Namn på anslutning | Namn på VPN-anslutning |
| Server | Serveradress |
| IPSec-identifierare | Användarnamn för anslutningen |
| IPSec Förhandsdelad nyckel | Lösenord för anslutningen |
| DNS-sökning Domäner | DNS-sökning domäner |

| | |
|---|---|
| OpenVPN | |

| | |
|---|---|
| Namn på anslutning | Namn på anslutning |
| OpenVPN-profil | Här är var innehållet i filen .ovpn kommer att kopieras |
| OpenVPN-app | Det finns två olika appar för användning av OpenVPN<br>Vi rekommenderar appen "OpenVPN för Android". Men i alternativet kan appen "OpenVPN Connect" användas |

## Begränsningar

Här kan du ställa in begränsningarna i samband med anslutningshanteringen.

| | |
|---|---|
| Tillåt data-roaming | Tillåt mobildata vid roaming |
| Tvinga fram dataroaming | Om den är aktiverad är roaming för mobildata permanent aktiverad (rekommenderas inte!)<br>Denna inställning skriver över inställningen "Allow Data Roaming"! |
| Följande inställningar är endast tillgängliga på Samsung KNOX 2.0 eller högre | |
| Tillåt endast nödsamtal | Tillåt endast nödsamtal |
| Tillåt WiFi | Tillåt WiFi |
| Miniminivå för säkerhet i WiFi-nätverk | WiFi-nätverkets lägsta säkerhetsnivå<br>Öppet = alla typer av WiFi är tillåtna |
| Förbjuda användare att lägga till WiFi-nätverk | Användaren kan inte själv lägga till ett WiFi-nätverk<br>Denna inställning är endast möjlig om en WiFi-profil har definierats under "Connection Management" |
| Tillåt SMS & MMS | All = All SMS- och MMS-trafik är tillåten<br>Incoming SMS Only = Endast inkommande SMS-meddelanden tillåts<br>Outgoing SMS Only = Endast utgående SMS-meddelanden tillåts<br>None = Ingen SMS/MMS-trafik är tillåten |
| Tillåt synkronisering under roaming | Tillåt synkronisering under roaming<br>På = aktiverad<br>Av = avaktiverad<br>Användarval = användarens val |
| Tillåt röstroaming | Tillåt röstroaming<br>På = aktiverad<br>Av = avaktiverad<br>User Choice = användarens val |
| Använd systemets http-proxyserver | Användningen av en HTTP-proxyserver, som tillhandahålls av systemets inställningar i Inställningar, är beroende av det anslutna nätverket (WiFi eller APN) |

## APN

Följande inställningar är endast tillgängliga på Samsung SAFE 2.0 eller senare!

| | | |
|---|---|---|
| APN-visningsnamn | APN-visningsnamn | |
| Namn på åtkomstpunkt | APN:s namn | |
| Protokoll för utgående server | Inte inställd | |
| | Ingen | |
| | PAP | PAP-protokoll |
| | CHAP | CHAP-protokoll |
| | PAP eller CHAP | Antingen PAP- eller CHAP-protokollet |
| MCC - Mobil landskod | MCC anges här, lämna detta fält tomt om det isatta SIM-kortets MCC ska användas | |
| MNC - Kod för mobilnät | MNC anges här, lämna fältet tomt om det isatta SIM-kortets MCC ska användas | |
| Serveradress | Serveradress | |
| Serverns portnummer | Serverns portnummer | |
| Serverns proxy-adress | Serverns proxy-adress | |
| Adress till MMS-server | Adress till MMS-server, för Standard, lämna tom | |
| MMS-portnummer | MMS-portnummer | |
| MMS-proxyadress | MMS-proxyadress | |
| Användarens namn | Användarens namn | |
| Lösenord | Lösenord | |
| Typ av åtkomstpunkt | Tillåtna typer är: "standard", "mms", "supl" Om fältet lämnas tomt kommer "default,supl,mms" att användas | |
| Företrädesvis APN | APN är att föredra | |

## Bluetooth

Här kan du göra en rad olika Bluetooth-inställningar.

Följande inställningar är endast tillgängliga på Samsung KNOX 1.0 eller högre!

| | |
|---|---|
| Tillåt enhetsidentifiering via Bluetooth | Tillåt upptäckt av enheter via Bluetooth |
| Tillåt parkoppling med Bluetooth | Tillåt parkoppling med Bluetooth |
| Tillåt Bluetooth-headset-enheter | Tillåt Bluetooth-headset-enheter |
| Tillåt handsfree-enheter från Bluetooth | Tillåt handsfree-enheter från Bluetooth |
| Tillåt Bluetooth A2DP-enheter | Tillåt Bluetooth A2DP ljudstreaming mellan enheter |
| Tillåt utgående samtal | Tillåt utgående samtal viaBT |
| Tillåt dataöverföring via Bluetooth | Tillåt dataöverföring via Bluetooth |
| Tillåt Bluetooth-internetdelning | Gör det möjligt att använda enheten som ett modem (internetanslutning via Bluetooth) |
| Tillåt anslutning till dator via Bluetooth | Tillåt anslutning till dator via Bluetooth |

# PIM-hantering

## Utbyte

| |
|---|
| Endast tillgänglig för Samsung KNOX 1.0 eller högre! |

| | |
|---|---|
| E-postadress | Den angivna användarens e-postadress<br>Observera "platshållarna", som du kan använda för att arbeta med referenser och du behöver inte utföra ändringar manuellt på varje enhet<br>Med ett klick på **Show Placeholders** kan du visa dem för dig själv |
| Serverns värdnamn | Serveradress till dina Exchange-servrar |
| Inloggningsnamn | Inloggningsnamnet för respektive slutanvändarenhet, observera även "Platshållare här |
| Domän | Domänadress |
| Lösenord (endast på enhetsnivå) | Alternativt kan en enskild enhet förses med ett lösenord, om detta förblir tomt kommer användaren att uppmanas att ange sitt Exchange-lösenord |
| Antal föregående dagar att synkronisera | Antal dagar som avgör när e-postmeddelanden synkroniseras tillbaka |
| Underskrift | En signatur kan bifogas (Tips: Vissa enheter kräver HTML-formatering för signaturen) |
| Standardkonto | Fastställer, att detta e-postkonto är standardkontot |
| Använd SSL (Secure Sockets Layer) | Använd en SSL-anslutning |
| Använd TLS (Transport Layer Security) | Använd en TLS-anslutning |
| Acceptera alla certifikat | Alla certifikat accepteras. Välj detta alternativ om Exchange Server använder ett självsignerat certifikat |

## E-post

Här kan du distribuera IMAP- och POP-konton till respektive slutanvändares enheter.

| | | |
|---|---|---|
| Följande inställningar är endast tillgängliga på Samsung KNOX 1.0 eller högre! | | |
| E-postadress | Den angivna användarens e-postadress<br>Observera "platshållarna", som du kan använda för att arbeta med referenser och du behöver inte utföra ändringar manuellt på varje enhet<br>Med ett klick på **Show Placeholders** kan du visa dem för dig själv | |
| Protokoll för inkommande server | Protokoll för inkommande server | IMAP eller POP |
| Adress till inkommande server | Adress till inkommande server | |
| Port för inkommande server | Port för inkommande server | |
| Inloggning/användarnamn för inkommande server | Inloggning/användarnamn för inkommande server | |
| Lösenord för inkommande server (endast på enhetsnivå) | Lösenord för inkommande server (endast på enhetsnivå) | |
| Inkommande server använder SSL | Inkommande server använder SSL | |
| Inkommande server använder TLS | Inkommande server använder TLS | |
| Inkommande server accepterar alla certifikat | Den inkommande servern accepterar alla typer av certifikat | |
| Protokoll för utgående server | Protokoll för utgående server | SMTP |
| Utgående serverport | Utgående serverport | |
| Utgående server använder extra autentiseringsuppgifter | Ytterligare autentiseringsuppgifter för den utgående servern. Om den här inställningen är "off" används inställningarna för den inkommande servern | |
| Inloggning/användarnamn för utgående server | Inloggning/användarnamn för utgående server | |
| Lösenord för utgående server (endast på enhetsnivå) | Lösenord för utgående server | |
| Utgående server använder SSL | Utgående server använder SSL | |
| Utgående server använder TLS | Utgående server använder TLS | |

| | |
|---|---|
| Utgående server accepterar alla certifikat | Utgående server accepterar alla typer av certifikat |
| Underskrift | En underskrift kan bifogas här (Tips: Vissa enheter kräver HTML-formatering för underskriften) |
| Meddela användaren om mottagande av nytt eMail | Meddelar användaren när ett nytt e-postmeddelande tas emot |

## AE Gmail Exchange

Information: Den här konfigurationen kommer att tillämpas på Gmail-appen. Du måste därför godkänna och installera Gmail.

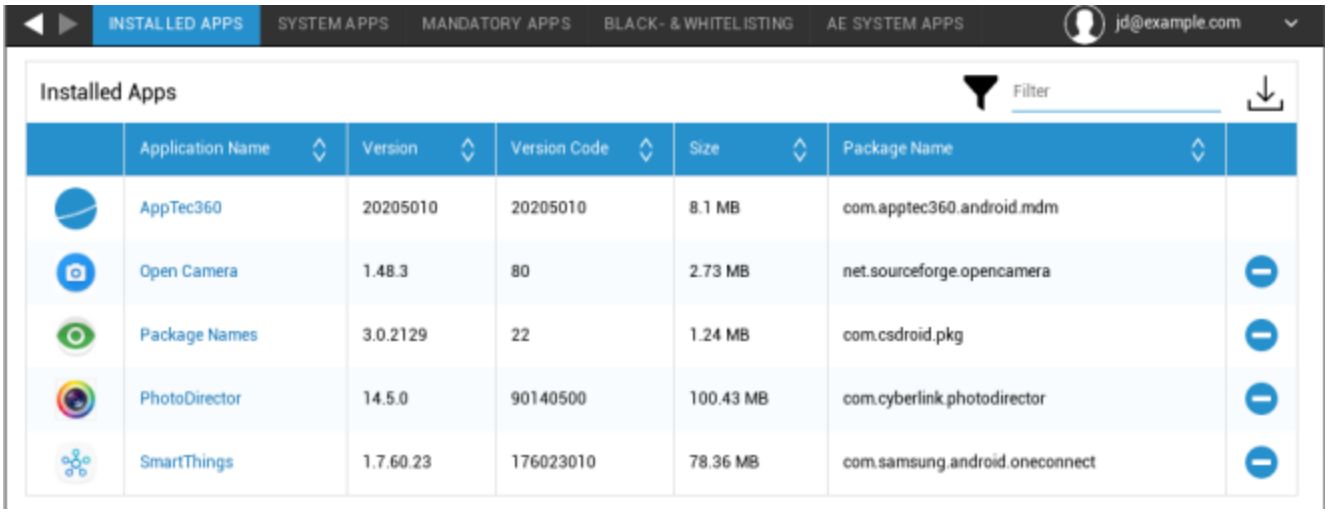
| | |
|---|---|
| E-postadress | Den angivna användarens e-postadress<br>Observera "platshållarna", som du kan använda för att arbeta med referenser och du behöver inte utföra ändringar manuellt på varje enhet<br>Med ett klick på Show Placeholders kan du visa dem för dig själv |
| Serverns värdnamn | Serveradress till dina Exchange-servrar |
| Inloggningsnamn | Inloggningsnamnet för respektive slutanvändarenhet, observera även "Platshållare här |
| Underskrift | En signatur kan bifogas (Tips: Vissa enheter kräver HTML-formatering för signaturen) |
| Antal föregående dagar att synkronisera | Antal dagar som avgör när e-postmeddelanden synkroniseras tillbaka |
| Enhetens identifierare | EAS-identifierare. Lämna detta tomt om din miljö inte kräver detta |
| Använd SSL (Secure Sockets Layer) | Använd en SSL-anslutning |
| Acceptera alla certifikat | Alla certifikat accepteras. Välj detta alternativ om Exchange Server använder ett självsignerat certifikat |
| Tillåt oadministrerade konton | Gör det möjligt för användaren att lägga till ytterligare konton |
| Kundcertifikat | Ladda upp klientcertifikat om din Exchange-server kräver detta |

# App-hantering

## Enterprise App Manager

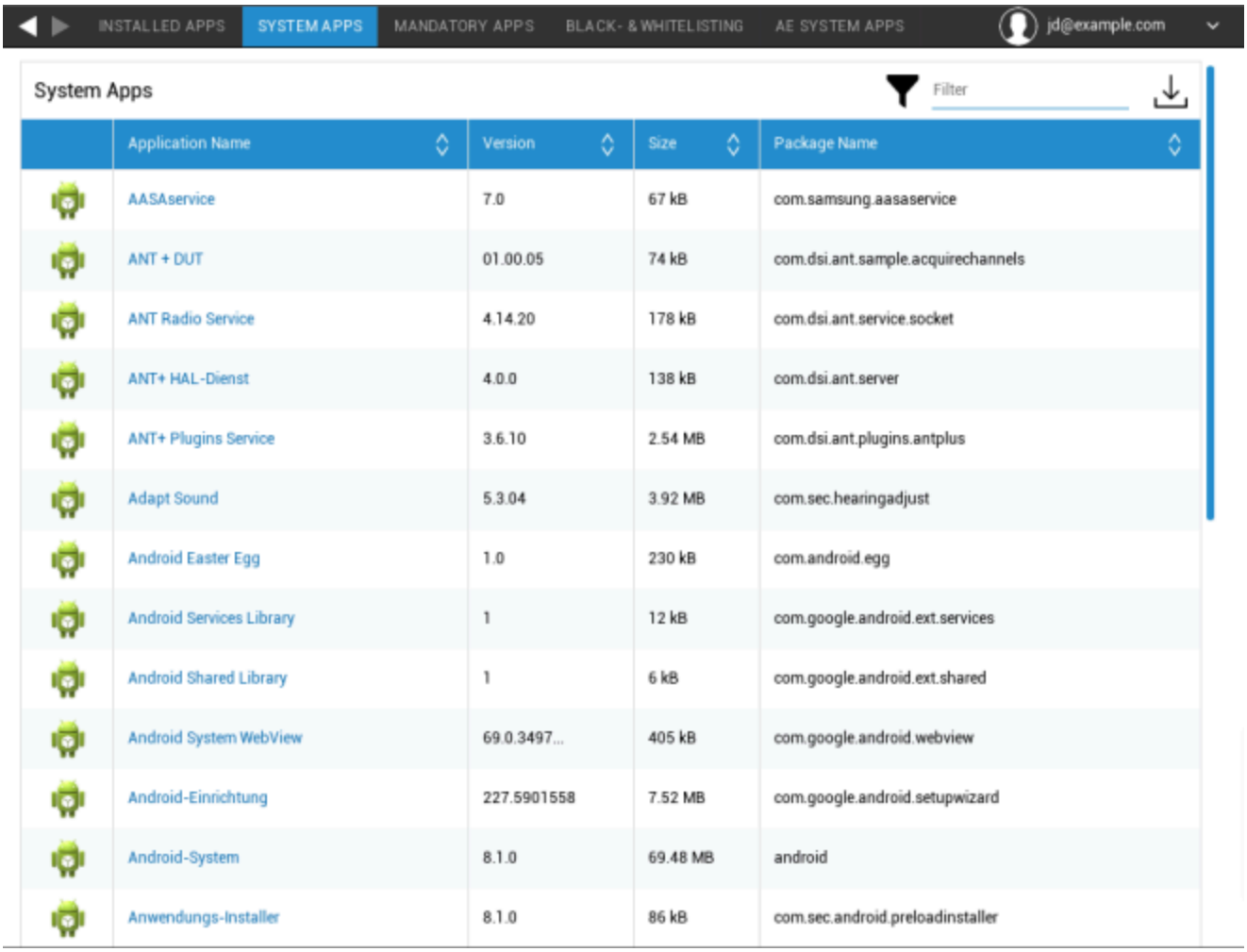
### Installerade appar (endast på enhetsnivå)

Här visas alla appar som för närvarande är installerade på slutanvändarens 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

## Systemappar (endast på enhetsnivå)

Under "System Apps" listas alla förinstallerade system med paketnamn och version.



## Obligatoriska appar

I Obligatoriska appar kan du definiera vilka appar som måste installeras på enheten. Beroende på din konfiguration och enhet installeras appen automatiskt eller så uppmanas användaren att installera den.

Tänk på att det är rekommenderat att använda Android Enterprise för enkel apphantering.

Scenarierna är de som anges nedan:

Normala Play Store-appar

Installationer av Playstore-appar kräver alltid en användarinteraktion. Dessutom måste ett Google-konto konfigureras på enheten.

In-house installation av app

På Samsung-enheter kommer dessa appar att installeras tyst. Enda undantaget är containern, där användaren måste bekräfta installationen.

I alla andra fall måste användaren bekräfta installationen av appen.

Android Företag Play Store Appar

Dessa appar kommer alltid att installeras tyst, utan att användaren behöver ingripa.

För att lägga till en obligatorisk app, klicka på "+" och välj önskad app från listan. Tänk på att du inte kan installera appar från fliken "Google Play Store" om enheten är konfigurerad med Android Enterprise antingen som helt hanterad eller som container.

Om du använder Android Enterprise väljer du apparna från avsnittet "AE Play Store". Om du vill göra appar tillgängliga här måste du bekräfta dem i Google Enterprise Play Store genom att gå till Allmänna inställningar → AE Play Store → Appar i Play Store.

När du tar bort en obligatorisk app kommer den också att avinstalleras från enheten.

Du kan klicka på namnet på en app i listan över obligatoriska appar och gå till fliken "Konfiguration" för att konfigurera en app. Detta kräver användning av Android Enterprise och appen måste ha stöd för detta. Därför beror de tillgängliga alternativen på den valda appen.

## Appar för AE-system

Här kan du aktivera systemappar för Android Enterprise-enheter. Tänk på att den angivna appen måste finnas i systemets lagringsutrymme, annars händer ingenting. 296

# Begränsningar och inställningar

## Svart- och vitlistning

Här kan du definiera en svart- eller vitlista. Alla appar på den svarta listan kommer att blockeras. Alla appar som inte finns med på vitlistan blockeras. En tom svartlista blockerar ingenting, medan en tom vitlista blockerar allt*.

**Alla obligatoriska appar och appar från Enterprise App Store kommer att vitlistas automatiskt. Du behöver inte lägga till dem manuellt*

När du klickar på "+" kan du antingen söka efter en app som du vill lägga till i din svarta eller vita lista eller ange ett paketnamn manuellt.

## Sys App Begränsningar

Under "Sys App Restrictions" kan du bland annat blockera förinstallerade appar och tjänster som du vill.

| | |
|---|---|
| Inaktivera webbläsare | Inaktivera standardwebbläsare |
| Inaktivera kalender | Inaktivera inbyggd kalender |
| Inaktivera kalkylator | Inaktivera kalkylator |
| Inaktivera webbläsaren Chrome | Inaktivera webbläsaren Chrome |
| Avaktivera klocka | Avaktivera klocka |
| Inaktivera kontakter | Inaktivera kontakter |
| Inaktivera uppringare | Inaktivera inbyggd uppringare |
| Inaktivera eMail | Inaktivera e-post |
| Avaktivera Exchange | Inaktivera Exchange-konton |
| Avaktivera Facebook | Inaktivera Facebook-appen |
| Inaktivera galleri | Inaktivera inbyggd galleriapp |
| Inaktivera Gmail | Inaktivera Gmail |
| Inaktivera Google Books | Inaktivera Google Books |
| Inaktivera Google Play Kiosk | Inaktivera Google Play Kiosk |
| Inaktivera Google Maps | Inaktivera Google Maps |
| Avaktivera Google Music | Avaktivera Google Music |
| Inaktivera Google Movies | Inaktivera Google Movies |
| Inaktivera Google Play Store | Inaktivera Google Play Store (offentlig App Store) |
| Inaktivera Google Plus | Inaktivera Google Plus |
| Inaktivera Google-sökning | Inaktivera Google-sökning |
| Inaktivera Google Talk / Google Hangouts | Inaktivera Google Talk / Google Hangouts |
| Inaktivera musikspelare | Inaktivera inbyggd musikspelarapp |
| Inaktivera inställningar | Inaktivera enhetens inställningar |
| Inaktivera Sim Toolkit | Inaktivera Sim Toolkit-tjänster |
| Avaktivera SMS / MMS | Avaktivera SMS / MMS |
| Avaktivera Street View | Inaktivera Street View-tjänster |
| Avaktivera Youtube | Avaktivera Youtube |

## Samsung-appar

Under "Samsung Apps" kan du definiera ytterligare inställningar och/eller begränsningar för Samsung-enheter.

| | |
|---|---|
| Avaktivera AllShare Play / Samsung Link | Avaktivera AllShare Play / Samsung Link |
| Inaktivera ChatON | Inaktivera ChatON |
| Avaktivera Game Hub | Avaktivera Game Hub |
| Avaktivera gruppspel | Avaktivera gruppspel |
| Inaktivera hjälp | Inaktivera Samsung Hjälp |
| Avaktivera KNOX | Avaktivera Samsung KNOX Container |
| Inaktivera Memo | Avaktivera röstmemo |
| Inaktivera mina filer | Inaktivera mina filer |
| Avaktivera optisk läsare | Avaktivera optisk läsare |
| Inaktivera Polaris Office | Inaktivera Polaris Office |
| Inaktivera Readers Hub / Samsung Books | Inaktivera Readers Hub / Samsung Books |
| Inaktivera S Memo | Inaktivera Samsung Memo app |
| Inaktivera S Translator | Inaktivera Samsung Translator-appen |
| Inaktivera S Voice | Inaktivera S Röstassistent |
| Inaktivera Samsung-appar | Inaktivera Samsung App Store |
| Inaktivera Samsung Hub | Inaktivera Samsung Entertainment Stores |
| Avaktivera videospelare | Avaktivera videospelare |
| Inaktivera röstinspelare | Inaktivera röstinspelare |
| Avaktivera WatchON | Avaktivera WatchON (simulerar en fjärrkontroll) |

### Appar från Huawei

Under "Huawei Apps" kan du definiera ytterligare inställningar och/eller begränsningar för Huawei-enheten.

| | |
|---|---|
| Avaktivera DLNA | Avaktivera DLNA |
| Avaktivera App Installer | Avaktivera App Installer |
| Inaktivera filhanteraren | Inaktivera filhanteraren |
| Inaktivera Backup Manager | Inaktivera Backup Manager |
| Inaktivera systemuppdatering | Inaktivera systemuppdatering |
| Inaktivera verktygslåda | Inaktivera verktygslåda |
| Avaktivera väder | Avaktivera väder |
| Avaktivera FM-radio | Avaktivera FM-radio |

## Inställningar för apphantering

Här kan du definiera uppdateringsbeteendet för InHouse Apps.

Frekvens för uppdateringskontroll definierar hur ofta AppTec360 App letar efter uppdateringar för InHouse-appar. När en ny version har upptäckts kommer den att laddas ner och installeras.

Wi-Fi Threshold definierar om nedladdningen ska begränsas till Wi-Fi-anslutningar om appen är större än ditt konfigurerade tröskelvärde. Om tröskelvärdet är mindre eller om du inte definierar något tröskelvärde laddas appen ner via Wi-Fi och mobilnät.

## App Store för företag

Tänk på att appar som läggs till här (Enterprise App Store) INTE kommer att installeras automatiskt på enheten/enheterna. Användaren måste öppna Enterprise App Store på enheten och installera appen manuellt.

Om du vill installera appar automatiskt på enheten ska du gå till "Apphantering" → "Enterprise App Manager" → "Obligatoriska appar" och lägga till önskade appar där.

Under denna punkt kan du distribuera valfria appar till dina användare.

### Playstore

Klicka på "+" för att lägga till en Play Store-app i butiken. Om du använder Android Enterprise ska du gå till "App Management Enterprise Play Store". Tänk också på att ett Google-konto måste konfigureras på → enheten för att installera de appar som definieras här.

### Internt

Under punkten "In-House" kan du ladda upp och distribuera internt utvecklade appar.

Klicka på "+" för att lägga till en InHouse-app i företagets appbutik som sedan kan installeras av användaren. I den här dialogen kan du också ladda upp en ny InHouse-app.

## Play Store för företag

Tänk på att appar som läggs till här (Enterprise Play Store) INTE kommer att installeras automatiskt på enheten/enheterna. Användaren måste öppna Play Store på enheten och installera appen manuellt.

Om du vill installera appar automatiskt på enheten ska du gå till "Apphantering" → "Enterprise App Manager" → "Obligatoriska appar" och lägga till önskade appar där.

Under denna punkt kan du distribuera valfria appar till dina användare.

Här kan du lägga till appar i Android Enterprise Playstore. Observera att du måste godkänna appar i Allmänna inställningar → AE Play Store → Appar i Play Store. Dessa appar kommer att läggas till i den vanliga Google Play Store.

Tänk också på att du först måste definiera en layout med appar i Allmänna inställningar → Apphantering → AE Play Store → Butikens layout.

Appar måste finnas i en layout innan du kan lägga till dem i butiken.

# Kioskläge och startprogram

## Kiosk-läge

Kioskläget gör att du kan fördefiniera en app eller en URL. Då kommer det endast att vara möjligt att köra/besöka denna app och eller URL.

På samma sätt kan olika hårdvaruknappar avaktiveras i olika Kiosk Mode.

| | |
|---|---|
| Automatisk start | Startar automatiskt Kiosk-läget så snart profilen når slutanvändarens enhet |
| Schemalagt kioskläge? | Du kan planera en tid för kioskläget, som sedan startar och avslutas automatiskt vid en tidpunkt som du själv bestämmer |
| Starttid | Starttidpunkt |
| Tid i minuter | Tid i minuter, efter vilken Kiosk Mode ska avslutas igen |

| **Tillämpningstyp** |
|---|

| | |
|---|---|
| En enda app | Om du vill starta appen i kioskläge väljer du Package" under "Application Type" |
| Kiosk-applikation | Klicka här för att välja en app som ska startas i Kiosk Mode<br>Du kommer att hitta den vanliga App Management-översikten<br>Du kan välja mellan en "Google Play Store", "Android In-House Apps" och ett "Packagename" |

| Tillämpningstyp |
|---|

| | |
|---|---|
| URL | Om du vill starta en URL i Kiosk Mode väljer du "URL" under "Application Type"<br>Ange sedan önskad URL-adress |
| Rensa webbläsaren efter inaktivitet | Här kan du definiera ett tidsintervall i minuter, efter vilket kioskläget ska startas om |
| Rensa webbcache och cookies | Om du aktiverar den här funktionen kommer webbcachen (cookies och cachade bilder) att raderas efter en omstart av kioskläget |
| Policy för samma ursprung | Om denna funktion är aktiv kan användaren bara surfa på undersidorna till en definierad URL<br>Du har till exempel definierat följande URL:www.mypage.com Sedan kan användaren surfa på: www.mypage.com/subpage |
| Vitlistade webbadresser | Här kan du upprätthålla en vitlista, alla dessa webbadresser är tillåtna<br>Högst 1 URL per rad<br>En URL måste börja med http:/ eller https:// |
| Svartlistade webbadresser | Här kan du upprätthålla en svart lista, alla dessa webbadresser är inte tillåtna<br>Högst 1 URL per rad<br>En URL måste börja med http:/ eller https:// |
| Skärmorientering | Denna inställning avser skärmens justeringar<br>Automatisk = automatisk<br>Stående = vertikalt format<br>Landscape = liggande läge |

| | |
|---|---|
| Multi App | Om du väljer kioskläget "Multi App" kommer användningen av AppTec360 Launcher att vara obligatorisk. |
| Appar | Applikation: Välj en Playstore eller en egen app som kioskapplikation. Det är också möjligt att ange ett paketnamn. Den valda kioskapplikationen måste vara installerad på enheten. Kom ihåg att ställa in Kiosk Application som obligatorisk.<br>Genväg på startskärmen: Om inställningen är "På" skapas en genväg på hemskärmen. Om inställningen är "Av" kommer appen fortfarande att visas i applistan. |

| | |
|---|---|
| Lösenord för utgång Aktiverad | Om du aktiverar den här funktionen är det möjligt för användaren att avsluta kioskläget med ett lösenord som du har fördefinierat |
| Avsluta lösenord | Detta är det lösenord som du har angett i förväg |
| Automatisk kollaps av statusfältet | Om det är aktiverat kommer statusfältet automatiskt att vara kollapsat. Med det alternativet kan användare se informationen i statusfältet, men inte komma åt dess funktioner |
| Inaktivera statusfältet | Statusfältet innehåller aviseringar, genvägar och information. Endast tillgängligt för Samsung-enheter med KNOX 1.0 eller senare. |
| Inaktivera volymknappar | Inaktivera volymknappar (endast tillgängligt på Samsung-enheter med KNOX 1.0 eller högre) |
| Inaktivera på/av-omkopplare | Inaktivera På/Av-omkopplaren (endast tillgänglig på Samsung-enheter med KNOX 1.0 eller högre) |
| Inaktivera hemknappen | Inaktivera hemknappen. Om denna funktion har aktiverats, kan Kiosk Mode endast avslutas i AppTec360 Console<br>(endast tillgängligt på Samsung-enheter med KNOX 1.0 eller högre) |
| Inaktivera navigeringsfältet | Med denna funktion kan du inaktivera navigeringsfältet (Tillbaka/Meny)<br>Om denna funktion har aktiverats, kan Kiosk Mode endast avslutas i AppTec360 Console<br>(endast tillgängligt på Samsung-enheter med KNOX 1.0 eller högre) |

| Inställningar för appuppdatering | |
|---|---|
| Tillåt uppdateringar av appar | Användare kommer att uppmanas att utföra appuppdateringar även när Kiosk Mode är aktivt. På enheter med Samsung KNOX kommer apparna att uppdateras tyst. |
| Uppdatera fönster | Ställ in ett intervall där användarna uppmanas att installera appuppdateringar. |

| TeamViewer | |
|---|---|
| Aktivera obevakad åtkomst | Om den är aktiverad kan administratörer fjärrstyra enheten utan att användaren behöver interagera. Appen TeamViewer Host måste installeras på enheten. |

### AppTec360 Launcher

| | |
|---|---|
| Aktivera AppTec360 Launcher | På: Aktiverar AppTec360 Launcher. Användaren måste ställa in den som standard Launcher en gång.<br>Obs: Om kioskläget är aktiverat och kioskläget är inställt på "Multi App", kommer användningen av AppTec360 launcher att vara obligatorisk. |
| Stora ikoner | På: Visar en större version av appikonerna i startprogrammet |
| Dölj AppTec360 App-ikonen | På: Döljer AppTec360-appen helt och hållet |
| Dölj AppTec360 Butiksikon | På: Döljer AppTec360 Enterprise AppStore helt och hållet |

### AppTec360 Inställningar

| | |
|---|---|
| Aktivera AppTec360 Inställningar App | AppTec360 Settings App ger kontroll över WiFi- och Bluetooth-anslutningar |
| Aktivera inställningar i Multi App<br>Kiosk-läge | Om aktiverat, kan användare komma åt AppTec360 Settings App medan Multi App Kiosk Mode är aktivt |

## Fjärrkontroll

### Splashtop

Visar aktuell status för Splashtop Setup. Här ser du de steg du behöver utföra för att få fjärråtkomst till enheten via Splashtop. Här måste du också ange din deploy-kod som du kan hämta från Splashtops webbplats. Deploy-koden krävs för att ansluta till enheten.

### Teamviewer

Visar aktuell status för Teamviewer Setup. Här visas de steg som du måste utföra för att få fjärråtkomst till enheten via Teamviewer.

## Innehållshantering

### Innehållsbox

Här kan du aktivera Contentbox för den här enheten. När den är aktiverad kommer Contentbox-appen att installeras på enheten.

## Säker webbläsare

Här kan du aktivera Secure Browser för den här enheten. När den är aktiverad kommer appen Secure Browser att installeras på enheten. Den här webbläsaren kan konfigureras så att den erbjuder en webbläsare på enheten som är begränsad till dina behov.

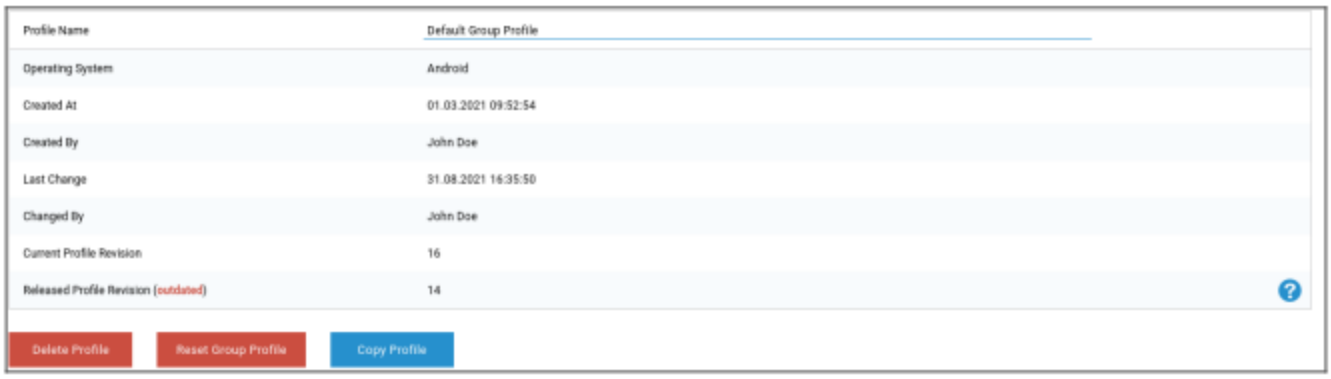
| | |
|---|---|
| Kräv lösenord | Kräv att användaren ställer in och använder ett lösenord för att få tillgång till webbläsaren. |
| Begränsa nedladdningar / Öppna i | Blockerar nedladdningar från webbplatser |
| Begränsa uppladdningar | Begränsar uppladdningar till vissa webbadresser. Ange ingen URL för att blockera uppladdningen helt och hållet |
| Tillåt kopiering | Tillåt kopiering, klippning eller delning av text på webbsidorna. |
| Tillåt skärmupptagning | Tillåt att ta skärmdumpar. |
| Frekvens för rensning av data | Välj med vilken frekvens ALL användardata (historik, cache etc.) ska tas bort automatiskt. |
| Bokmärken för företag | Bokmärkena visas i mappen "Företagsbokmärken" i webbläsarens bokmärken. De är inte redigerbara av användaren. |
| Dölj adressfältet | Döljer adressfältet så att användaren inte ser den URL som han besöker |
| Vitlistning i webbläsaren (utan Universal Gateway) | Aktiverar vitlistning av URL:er på klientsidan. - Företagets bokmärken är alltid vitlistade - Stöd för endast 100 URL:er - Använd Universal Gateway för obegränsad svart- och vitlistning |
| Gateway-baserad svart- och vitlistning | Svartlistning har följande krav: - En fungerande AppTec360 Universal Gateway ("Allmänna inställningar" → "Universal Gateway") - En fungerande VPN-konfiguration med en specificerad DNS-server ("Allmänna inställningar" → "Universal Gateway" → "VPN-inställningar") - En Blacklist-konfiguration ("Allmänna inställningar" → "Universal Gateway" → "Domain Blacklist") - En giltig VPN-anslutning i profilen ("Connection Management" → "VPN") |

# Konfiguration Windows 10 PC

## Allmänt

### Översikt över grupprofiler (endast på gruppnivå)

När du öppnar en grupprofil får du en snabb överblick över profilen.




| | |
|---|---|
| Profilens namn | Profilens namn (kan ändras här) |
| Operativsystem | Operativsystem som profilen är avsedd för |
| Skapad vid | Tidpunkt för skapelse |
| Skapad av | Skaparen av profilen |
| Sista förändringen | Tidpunkt för senaste ändring av profilen |
| Förändrad av | Konto som gjorde de senaste ändringarna |
| Aktuell profil Revidering | Revidering av sparat profiltillstånd |
| Utgiven Profil Revision | Tilldelad profilrevision ("Tilldela nu"). Om etiketten visar "(outdated)" bakom texten betyder det att du har sparat profilen men inte tilldelat den ännu, så enheterna kommer fortfarande att få en äldre version. |

## Enhetsöversikt (endast på enhetsnivå)

Enhetens sammanfattade översikt, som innehåller följande:

| | |
|---|---|
| PC namn | Namn på datorn |
| Klient | Enheterna Windows-typ |
| Senast kända plats | latitud och longitud för enhetens senast kända plats |
| Tilldelade Obligatoriska appar | Antal obligatoriska appar som tilldelats enheten |
| PC UID | UID för datorn |
| OS-utgåva | Visar din Windows Edition |
| OS-version | För närvarande installerad Windows-version |
| OS-byggnad | Nuvarande Windows-byggnad |
| Operativsystem | Nuvarande installerat operativsystem |
| Serienummer | Enhetens serienummer |
| Ägande av enhet | Den konfigurerade ägartypen |
| Enhetstyp | Typ av enhet |
| Rotad | Visar om enheten är rotad |
| Överensstämmande | Visar om enheten är kompatibel |
| Senast sett | Datum och tid för när ändringar gjordes i profilen |
| Tilldelning av användare | Visar den användare eller grupp som den här enheten för närvarande är tilldelad.<br>Du kan flytta enheten genom att välja en annan användare eller grupp i rullgardinsmenyn. |

## Inställningar

| | |
|---|---|
| Tillåt automatisk uppdatering | Tillåt eller avvisa automatiska uppdateringar av operativsystemet. |

## Config Revision (endast på enhetsnivå)

Här får du en översikt över vilken grupprofil som är tilldelad enheten.


Om du klickar på grupprofilen kommer du direkt till profilen och kan göra inställningar.

Med symbolen kan du återställa de tilldelade apparna till grupprofilens inställningar.

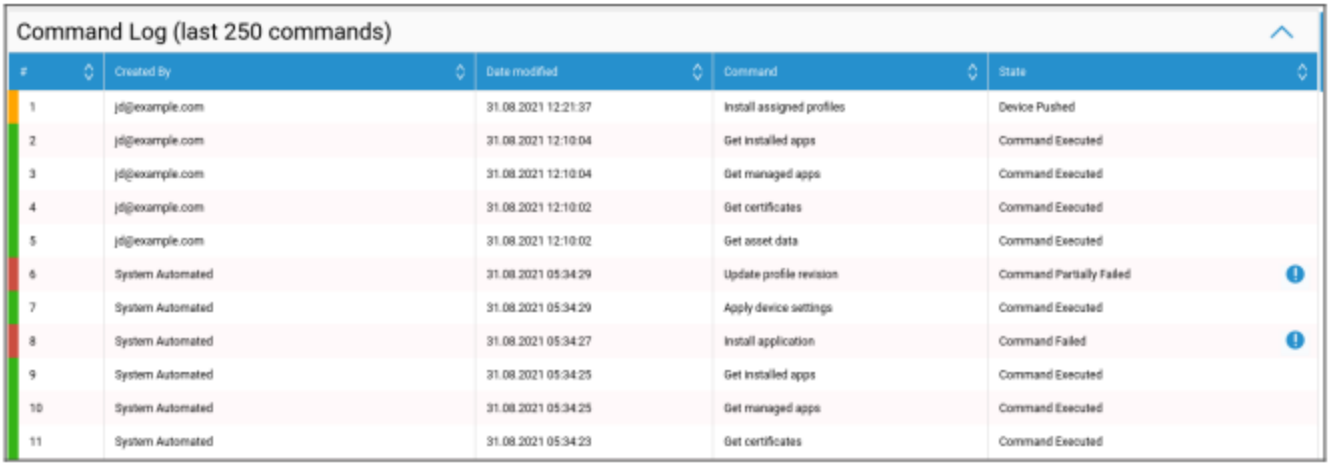
Med symbolen kan du återställa enhetens profil så att den inte har några inställningar alls.

"Nyare revision tillgänglig" anger att grupprofilen har ändrats och sparats men inte tilldelats.
Grupprofilen måste tilldelas med "Tilldela nu" på gruppnivå för att ändringarna ska gälla för enheterna.

## Enhetslogg (endast på enhetsnivå)

### Kommandologg

Här kan du se vilka kommandon som har utfärdats för enheten och vilken status de har.




Kommandon som skapats av "System Automated" skapas automatiskt av systemet.

## Möjliga kommandostatusar

| | |
|---|---|
| Enhet tryckt | En push-begäran har skickats till push-tjänsten (t.ex. APNS) för att tala om för enheten att den ska ansluta tillbaka till EMM-servern. |
| Kommando Skapat | Kommandot skapades i systemet. |
| Kommando skickat | Kommandot skickades till enheten efter att den anslutit till servern. |
| Kommando utfört | Kommandot har utförts framgångsrikt. |
| Kommandot misslyckades | Kommandot misslyckades. * |
| Kommandot delvis misslyckat | Beroende på enhetens operativsystem kan vissa kommandon grupperas tillsammans.<br>I detta misslyckades vissa delar av denna kommandogrupp. * |
| Kommando utfört, eventuellt misslyckat | Kommandot utfördes, men kanske inte. |
| Kommando Repushed | Kommandot återställdes av en användare. |
| Bortkastad | Kommandot kasserades. Till exempel för att det ersattes av ett annat kommando eller för att enheten registrerades på nytt och gamla kommandon togs bort |

*Om det finns ett utropstecken bakom meddelandet kan du få mer information genom att hålla muspekaren över ikonen.

# Tillgångshantering (endast på enhetsnivå)

## Info om enhet

| | |
|---|---|
| Tillverkare | Tillverkare av enheten |
| Modell | Enhetsmodell |
| Modellnummer | Modellnummer |
| Operativsystem | Operativsystem |
| OS-version | OS-version |
| Serienummer | Serienummer |
| ExchangeID | ExchangeID |
| Totalt RAM-minne | Totalt RAM-minne |
| Displayupplösning | Displayupplösning |
| Språk i telefon | Enhetens språk |
| Firmware-version | Firmware-version |
| DM-klientversion | Version av klienten för enhetshantering |
| Hårdvaruversion | Enhetens hårdvaruversion |
| CPU-arkitektur | CPU-arkitektur (processortyp) |

## Cellulär

| | |
|---|---|
| SIM-operatör Nätverk | Bärarnätverk |
| Telefonnummer | Telefonnummer |
| Status för roaming | Status för roaming |
| IMEI | IMEI |
| IMSI | IMSI |
| Modem Firmware | Modem Firmware |

## Synkroniseringsinformation

| | |
|---|---|
| Omedelbar DM-anslutning | Enheten bör omedelbart skapa en anslutning till AppTec |
| Initial omprövningstid | Initial omprövningstid för denna första anslutning |
| Försök med anslutning | Antal nya anslutningsförsök efter att anslutningen från Connection Manager har brutits eller efter ett fel på WinInet-nivå |
| Maximal sömntid | Maximal sömntid efter felaktig paketutskick |
| Första synkroniseringsförsöket | Tid för det första steget efter inskrivningen |
| Första omprövningsintervall | Tid för det första steget efter inskrivningen |
| Andra synkroniseringsförsök | Tid för det andra steget efter inskrivningen |
| Sekund Retry Interval | Tid för det andra steget efter inskrivningen |
| Regelbundna synkroniseringsförsök | Tid för de ytterligare stegen efter inskrivningen |
| Regelbundet omprövningsintervall | Tid för de ytterligare stegen efter inskrivningen |

# Säkerhetshantering

## Stöldskydd (endast på enhetsnivå)

### GPS-information (endast på enhetsnivå)

Här kan du ange aktuell/senaste enhetsplats. Lokaliseringen kan skyddas med ett eller till och med två lösenord - se: "Allmänna inställningar" > "Sekretess" > "GPS-åtkomst"

### GPS-inställningar

| | |
|---|---|
| Aktivera GPS-spårning | Möjliggör regelbunden synkronisering av GPS-information. |
| Spårningsintervall | Ställ in intervallet för synkronisering av GPS-information. |

## Säkerhetskonfiguration

### Lösenord

| | | |
|---|---|---|
| Minsta lösenordslängd | Minsta lösenordslängd | |
| Sammansättning av lösenord | Anger antalet specifika tecken som lösenordet måste innehålla<br>Dessa består av stora bokstäver, små bokstäver, siffror och specialsymboler | |
| Lösenordskvalitet | Här kan du ställa in lösenordets kvalitet | |
| | Alfanumerisk | Endast siffror och bokstäver |
| | Numerisk | Endast siffror |
| | Numerisk eller alfanumerisk | Siffror eller siffror och bokstäver |
| Maximal inaktivitetstid Lås | Antal minuter av inaktivitet från användarens sida på enheten, varefter enheten låses. Användaren måste låsa upp enheten efter denna tid genom att ange enhetens lösenord. | |
| Lösenordets utgång | Ställ in tiden tills ett nytt lösenord måste anges | |
| Begränsning av lösenordshistorik | Antal tidigare använda lösenord som inte är tillåtna | |
| Maximalt antal misslyckade lösenordsförsök | Antal gånger som lösenordet kan anges felaktigt, innan en fullständig radering av enheten utförs | |

## Antivirus

| **Antivirusinställningar - Ställ in skanningskonfiguration** | |
|---|---|
| Typ av skanning | Väljer om en snabbsökning eller en fullständig sökning ska utföras |
| Ställ in scanningsstart | Väljer vilken tid på dagen som Windows Defender ska starta skanningen |
| Skanningsfrekvens | Väljer den dag som Windows Defender-sökningen ska köras |
| Frekvens för uppdatering av signaturer | Speciefies det intervall i timmar som ska användas för att kontrollera signaturer |

| Konfigurera typ av filer för skanning | |
|---|---|
| Tillåt skanning av arkivfiler | Tillåt eller avvisa skanning av arkiv (t.ex. .zip) när de öppnas. |
| Tillåt skanning av skript | Tillåter eller förbjuder Windows Defender Script Scanning-funktionalitet. |
| Tillåt skanning av e-postmeddelanden | Tillåt eller förbjud skanning av e-postmeddelanden. |
| Tillåt skanning av nätverksfiler | Tillåt eller förbjud skanning av nätverksfiler. |
| Tillåt fullständig skanning av mappade nätverksenheter | Tillåt eller förbjud skanning av mappade nätverksenheter (aktiveras endast när fullständig skanning är aktiverad). |
| Styr dubbelriktad skanning | Styr vilka uppsättningar av filer som ska övervakas. |
| Tillåt fullständig skanning av flyttbara enheter | Tillåt eller avvisa fullständig skanning av flyttbara enheter. Endast under fullständig skanning initieras. |

| Typ av filer som ska undantas från skanning | |
|---|---|
| Ignorera filtyper för skanning | Definiera en uppsättning filnamnstillägg för olika typer av filer. Varje filtillägg för varje fält. |
| Ignorera katalogsökvägar | Definiera en uppsättning katalogsökvägar för att inte skanna dem. En sökväg per fält. Exempel på sökvägar: "C:\Example", "C:\Windows" eller "C:\Users". |
| Uteslut processer från skanning | Uteslut filer som har öppnats av specifika processer från Microsoft Defender Antivirus-skanningar. . En sökväg per fält. Exempel på sökvägar: "C:\myFile.exe", "C:\Windows\myProcess.exe", "C:\myScript.bat |

| Extra inställningar | |
|---|---|
| Tillåt övervakning i realtid | Tillåt eller avvisa Windows Defender Realtime Monitoring-funktionalitet |
| Tillåt övervakning av beteende | Tillåt eller avvisa funktionen Windows Behavior Monitoring |
| Tillåt skydd av molnet | Tillåt eller förbjud att Windows Defender skickar information till Microsoft om alla problem som upptäcks. Microsoft analyserar den informationen, lär sig mer om problemet som påverkar enheten och erbjuder förbättrade lösningar |
| | Beteende för att skicka prover |
| Tillåt Windows Defender IOAV-skydd | Tillåt eller avvisa Windows Defender IOAV-skydd |
| Tillåt åtkomst till Defenders "On Access protection" UI | |
| Genomsnittlig belastningsfaktor för CPU | Representerar den genomsnittliga CPU-belastningsfaktorn för Windows Defender-sökningen (i procent) |

| Hantering av skadlig kod | |
|---|---|
| Låg svårighetsgrad | Du kan definiera hur enheten ska hantera skadlig programvara för varje allvarlighetsgrad.<br>Tillgängliga alternativ är:<br>• Ren<br>• Karantän<br>• Ta bort<br>• Tillåt<br>• Användare definierad<br>• Block |
| Måttlig svårighetsgrad | |
| Hög svårighetsgrad | |
| Allvarlig svårighetsgrad | |
| Dagar för att behålla rensad skadlig kod | Tidsperiod i dagar som filer/objekt i karantän lagras på systemet. Standardvärdet är 0, vilket innebär att objekten hålls i karantän och inte tas bort automatiskt. Maxvärdet är 90. |

## Säkerhetscenter

| Windows Security Center - Inställningar för Windows-säkerhet | |
|---|---|
| Avaktivera UI för skydd mot virus och hot | |
| Hide Ransomware Data Recovery UI | |
| Inaktivera kontoskydd UI | |
| Inaktivera brandvägg och nätverksskydd UI | |
| Inaktivera användargränssnittet för app- och webbläsarkontroll | |
| Tillåt inte ändringar i Exploit-skydd | Användaren får inte göra ändringar i inställningarna för Exploit-skydd |
| Avaktivera enhetens säkerhet UI | |
| Dölj felsökning av TPM | Dölj felsökningsinställningar för TPM |
| Inaktivera knappen Clear TPM | |
| Inaktivera gränssnittet för enhetens prestanda och hälsa | |
| Inaktivera familjealternativ UI | |

| Anpassa skålar | |
|---|---|
| Aktivera anpassad supportinformation | Aktivera för att visa anpassad supportkontaktinformation för ditt företag längst ned till höger i appen för säkerhetscentret. |
| E-postadress | Ange företagets e-postadress |
| Företagets namn | Ange företagets namn |
| Företagets telefon | Ställ in företagets telefon |
| URL för hjälp | Ange företagets hjälp-URL |

| Extra inställningar | |
|---|---|
| Avaktivera meddelanden | Inaktivera visning av meddelanden från Windows Defender Security Center. |
| Dölj rekommendationer för uppdatering av firmware för TPM | Dölj rekommendationen att uppdatera TPM Firmware när en sårbar firmware upptäcks. |
| Visa företagsnamn och kontaktalternativ | Visa ditt företagsnamn och kontaktalternativ i en kontaktkortsvy i Windows Defender Security Center. |
| Dölj Secure Boot | Dölj Security Boot-området. |
| Dölj säkerhetsmeddelande kontrollområde | Dölj kontrollen för Windows Security-meddelandefältet. |

## Konfiguration av brandvägg

| Konfiguration av brandvägg - Globala inställningar | |
|---|---|
| Ignorera inställd autentisering | Ignorera hela autentiseringsuppsättningen om de inte stöder alla autentiseringssviter som anges i uppsättningen |
| Typ av paketkö | Anger hur skalning för programvaran på mottagningssidan aktiveras för både krypterad mottagning och rensning av vidarebefordringsvägen för IPsec-tunnelgatewayscenariot. |
| Inaktivera utför statlig FTP-filtrering | Om den är inaktiverad utförs ingen FTP-filtrering (Stateful File Transfer Protocol) för att tillåta sekundära anslutningar |
| Inaktivitetstid för säkerhetsassociation | I det här fältet konfigureras säkerhetsassociationens inaktivitetstid i sekunder. Säkerhetsassociationer tas bort efter att ingen nätverkstrafik har setts under den angivna tidsperioden. |
| Kodning av förhandsdelad nyckel | Ange kodning för den förhandsdelade nyckeln |
| Undantag för IPSec | Konfigurera undantag för Internetprotokoll |
| Kontroll av lista över spärrade certifikat | |

| Brandväggsprofiler (domänprofil / privat profil / offentlig profil) | |
|---|---|
| Aktivera brandvägg för den här profilen | |
| Avaktivera meddelanden | Inaktivera visning av meddelande till användaren när ett program blockeras från att lyssna på en port. |
| Blockera unicast-svar på multicast-sändningar | |
| Genomdriva brandväggsregler för auktoriserade applikationer | Om den inte verkställs ignoreras och verkställs inte auktoriserade brandväggsregler för applikationer i det lokala lagret |
| Tillämpa globala brandväggsregler för portar | Om den inte verkställs ignoreras och verkställs inte brandväggsregler för globala portar i det lokala arkivet. Inställningen har bara betydelse om den har angetts eller räknas upp i grupprinciparkivet eller om den räknas upp från GroupPolicyRSoPStore |
| Tillämpa brandväggsregler | Om den inte verkställs ignoreras brandväggsregler från den lokala butiken och verkställs inte |
| Tillämpa säkerhetsregler för anslutningar | Om den inte upprätthålls ignoreras och upprätthålls inte anslutningssäkerhetsreglerna från den lokala butiken |
| Standardåtgärd för utgående sändning | Den åtgärd som brandväggen gör som standard på utgående anslutningar |
| Standardåtgärd för inkommande | Den åtgärd som brandväggen gör som standard på inkommande anslutningar |
| Avaktivera Stealth-läge | Stealth-läget är en mekanism i Windows Firewall som hjälper till att förhindra att illasinnade användare hittar information om nätverksdatorer och de tjänster som de kör. |
| Inaktivera förhindrande av att svara på oönskad trafik | Om den är inaktiverad får brandväggens regler för stealth-läge inte hindra värddatorn från att svara på oönskad nätverkstrafik om trafiken skyddas av IPsec |

## Brandväggsregler

| Brandväggsregler | |
|---|---|
| Namn | Regelns namn |
| Beskrivning | Beskrivning av regeln |
| Åtgärd | Ange om denna regel ska blockera trafiken eller tillåta den. Tänk på att alternativet Block också kan blockera trafiken (beroende på resten av konfigurationen) mellan MDM-servern och enheten |
| Riktning | |
| Enable Edge traversal (Endast tillgängligt när **Direction** är inställt på **inkommande trafik**) | Anger att viss inkommande trafik tillåts tunnla genom NAT och andra edge-enheter med hjälp av Teredo-tunneltekniken. |

| Program & tjänster | |
|---|---|
| Definiera applikationer, allt annat | Om den inte är aktiverad kommer den att beakta alla ansökningar |
| Paket Familj Namn | Paketets familjenamn som regeln ska gälla för. |
| Filsökväg för applikationen | Det fullständiga programmet, till exempel C:\Windows\System\Notepad.exe, som regeln kommer att gälla för |
| Fullständigt kvalificerat binärt namn | Det fullständigt kvalificerade binära namn som regeln ska tillämpas på. Ett FQBN är en sträng i följande form: {Publisher\Product\Filename,Version}. |
| Tjänstens namn | Ange namnet på en tjänst (t.ex. "EventLog"). Du kan få en lista över servicenamn i Powershell genom att köra kommandot "Get-Service". |

| Protokoll och portar | | | | |
|---|---|---|---|---|
| Protokoll | Det protokoll som används av regeln. | | | |
| | Tillgängliga värden:<br>- Alla<br>- Anpassad<br>- HOPORT<br>- ICMPv4<br>- IGMP<br>- TCP<br>- UDP<br>- IPv6<br>- IPv6-rutten<br>- IPv6-Frag<br>- GRE<br>- ICMPv6<br>- IPv6-NoNxt<br>- IPv6-Opts<br>- VRRP<br>- PGM<br>- L2TP | När den är inställd på Anpassad | Ange ett protokollnummer mellan 0 och 255 | Protokollets nummer |
| | | När inställningen är TCP eller UDP | Ange lokala portar, annars kommer alla att användas | Lokala portar som regeln ska använda, även portar i intervallet är tillåtna |
| | | | Lokal hamn | Enstaka port eller ett antal portar. T.ex. 100-120,200,300-320. |
| | | | Ange fjärrportar, annars kommer alla att användas | Fjärrportar som regeln ska använda, även portar i intervallet är tillåtna |
| | | | Fjärrport | Enstaka port eller ett antal portar. T.ex. 100-120,200,300-320. |

| Omfattning | |
|---|---|
| Ange lokala IP-nummer, annars valfritt IP-nummer | Uppsättning av lokala IP-adresser, det kan också vara ett intervall av IP-adresser åtskilda av -. |
| Lokal IP-adress | Uppsättning av enskilda IP-adresser eller ett antal IP-adresser åtskilda av -. |
| Ange fjärr-IP, annars valfri fjärr-IP | Ange en uppsättning fjärr-IP:er, det kan också vara ett intervall av IP:er som separeras med "-". |
| Fjärr-IP-adress | Ange enstaka IP-adresser eller ett intervall av IP-adresser |
| Tokens | Tokens som kan ställas in tillsammans med fjärradresser. Tokens Intranet, RmtIntranet och Ply2Renders stöds i Windows 10, version 1809 och senare. |

| Avancerade inställningar | |
|---|---|
| Ange profiler, annars kommer alla att användas | Om inaktiverad kommer alla profiler att användas |

| | |
|---|---|
| Domän | Domänprofil |
| Privat | Privat profil |
| Allmänheten | Allmän profil |
| Ange gränssnitt, annars kommer alla att användas | Om inaktiverad kommer alla gränssnitt att användas |
| Lokalt nätverk | Gränssnitt för lokalt nätverk |
| Fjärråtkomst | Gränssnitt för fjärråtkomst |
| Trådlös | Trådlöst gränssnitt |

| **Lokala rektorer** | |
|---|---|
| Lägg till auktoriserade lokala användare | Tillåt att lägga till en lista över lokala användare som ska använda den här regeln |
| Behöriga användare | Lista över auktoriserade lokala användare för denna regel. Användaren måste vara i SDDL-format (Security Description Definition language), t.ex. PC_NAME\USERNAME. Det här fältet får inte fyllas i om ett servicenamn är inställt på att använda den här regeln |

## Inställningar för begränsning

### Enhetens funktionalitet

| | |
|---|---|
| Tillåt SD-kort | Tillåt användning av ett SD-kort |
| Tillåt kamera | Tillåt användning av kameran |
| Tillåt platstjänst | Tillåt enhetens platstjänst |
| Tillåt sidoladdning av app | Tillåt installation av appar från okända källor |
| Tillåt utvecklarläge | Tillåter utvecklarläge |
| Tillåt roaming av mobildata | Tillåt roaming av mobildata |
| Tillåt Cortana | Tillåt röstassistenten Cortana |
| Tillåt sökning att använda plats | Tillåt att sökningen använder plats |
| Tillåt att lägga till e-postkonto som inte är Microsoft | Ange om användaren får lägga till e-postkonton som inte tillhör MSA. |
| Tillåt anslutning av Microsoft-konto | Ange om du vill tillåta att MSA-kontot används för autentisering och tjänster för anslutningar som inte är e-postrelaterade. |
| Tillåt synkronisering av mina inställningar | Möjliggör synkronisering av inställningar över hela enheten |
| Företagsskyddade domännamn | Anger företagets domännamn åtskilda av ";". |
| Tillåt användaren att inaktivera systemåterställning | Gör det möjligt för användaren att inaktivera Systemåterställning.<br>**VARNING!**<br>Den här funktionen bör endast användas på enheter som ägs eller tillhandahålls av företaget eller organisationen eller på en användarägd enhet, där användaren tillåter att enheten helt hanteras av företaget. Om du inaktiverar den här principinställningen stängs Systemåterställning av och guiden Systemåterställning är inte tillgänglig. Möjligheten att konfigurera Systemåterställning eller skapa en återställningspunkt via Systemskydd inaktiveras också. |
| Tillåt avregistrering av användare | Gör det möjligt för användaren att ta bort företagsdelen från enheten och därmed koppla bort sig från AppTec360-servrarna. Om detta skulle hända kommer det inte längre att vara möjligt att hantera enheten |

| | |
|---|---|
| | **VARNING!**<br>Den här funktionen ska endast användas på enheter som ägs eller tillhandahålls av företaget eller organisationen eller på en användarägd enhet, där användaren tillåter att enheten helt hanteras av företaget. Om du inaktiverar den här principinställningen kan användare inte ta bort MDM-registreringar.<br>Ange om användaren får ta bort arbetsplatskontot via arbetsplatsens kontrollpanel. MDM-servern kan alltid radera kontot på distans. |

# BitLocker

## BitLocker-konfiguration

| | |
|---|---|
| **Allmänna inställningar** | |
| Kräv kryptering av enheter | Be användarna att aktivera enhetskryptering.beroende på Windows-utgåva och systemkonfiguration kan användarna bli tillfrågade:<br>- För att bekräfta att kryptering från en annan leverantör inte är aktiverad.<br>- Så här stänger du av BitLocker Drive Encryption och slår sedan på BitLocker igen. |
| Krypteringsmetoder | |
| Krypteringsmetod för operativsystemets hårddiskar | |
| Krypteringsmetod för fasta dataenheter | |
| Krypteringsmetod för flyttbara dataenheter | |
| Avaktivera varning om diskkryptering från tredje part | Inaktivera varningsmeddelandet om en diskkrypteringstjänst från tredje part som används på enheten.<br>Från och med Windows 10, version 1803, stöds den här inställningen endast för Azure Active Directory-anslutna enheter. |
| Tillåt körning av kryptering när en användare som inte är administratör är inloggad | Stöds endast för Azure Active Directory-anslutna enheter |

| AppTec360 Tillägg | |
|---|---|
| Tyst kryptering | Om detta väljs tillsammans med "Kräv enhetskryptering", kommer AppTec360 Management Service att köra automatisk tyst kryptering av enhetens enheter. |
| Generera automatiskt användarlegitimation | Den krypterade OS-enheten kommer att skyddas med automatiskt genererade användaruppgifter.<br>Antingen en TPM PIN-kod, när en TPM är tillgänglig, eller ett 6-ställigt textlösenord.<br>De genererade autentiseringsuppgifterna skickas till den e-postadress som registrerats för den aktuella enheten.<br>Om det här alternativet är avstängt är det enda möjliga skyddet för tyst kryptering att använda TPM.<br>I så fall misslyckas den tysta krypteringen för enheter utan TPM. |
| Kryptera fasta enheter | Alla tillgängliga fasta dataenheter kommer också att krypteras och skyddas med "Automatic Unlock" med hjälp av en nyckel som lagras på OS-enheten. |

| Inställningar för OS-enhet |
|---|

| Kräv ytterligare autentisering vid start | Med den här inställningen kan du konfigurera om BitLocker ska kräva autentisering varje gång datorn startas.<br>Den här inställningen används under installationen av BitLocker.<br>Om du aktiverar den här inställningen kan användare konfigurera avancerade startalternativ i installationsguiden för BitLocker. |
|---|---|
| Blockera BitLocker utan en kompatibel TPM | |
| Endast TPM | |
| TPM och PIN-kod | |
| TPM och nyckel | |
| TPM, nyckel och PIN-kod | Om du vill kräva att en PIN-kod och ett USB-minne (nyckel) används måste användaren konfigurera BitLocker med kommandoradsverktyget "manage-bde" i stället för med installationsguiden för BitLocker Drive Encryption. |

| Kräver minsta PIN-längd | |
|---|---|
| | Minst tecken |

| | |
|---|---|
| Konfigurera meddelande och URL för återställning före start | Konfigurera hela återställningsmeddelandet eller ersätt den befintliga URL:en som visas på skärmen för återställning av nyckeln före start när OS-enheten är låst.<br>Obs: Alla tecken och språk stöds inte i pre-boot. Vi rekommenderar starkt att du testar att de tecken du använder visas korrekt på återställningsskärmen före start. |
| | Alternativ för återställningsmeddelande före start |
| | Anpassat återställningsmeddelande |
| | Anpassad URL för återställning |

| | | |
|---|---|---|
| Alternativ för återställning av OS-enheter | | Med den här inställningen kan du styra hur BitLocker-skyddade operativsystemenheter ska återställas om det inte finns nödvändiga autentiseringsuppgifter.<br>Den här inställningen används under installationen av BitLocker.<br>Som standard tillåts en certifikatbaserad dataåterställningsagent, återställningsalternativen kan anges av användaren, inklusive återställningslösenord och återställningsnyckel, och återställningsinformation säkerhetskopieras inte till AD DS. |
| | Blockcertifikatbaserad agent för dataåterställning | Ange om en dataåterställningsagent kan användas med BitLocker-skyddade operativsystemenheter.<br>Innan en dataåterställningsagent kan användas måste den läggas till från posten Principer för offentliga nycklar i antingen konsolen Grupprinciphantering eller Redigeraren för lokala grupprinciper.<br>Mer information om hur du lägger till dataåterställningsagenter finns i BitLocker Drive Encryption Deployment Guide på Microsoft TechNet. |
| | Lösenordsinställningar för BitLocker-återställning | |
| | Inställningar för BitLocker-återställningsnyckel | |
| | Spara information om BitLocker-återställning till Active Directory Domain Services | |
| | Konfiguration av AD DS BitLocker-lagring för återställning | Förvaring av nyckelpaketet stöder återställning av data från en enhet som har skadats fysiskt. |
| | Kräv lagring av återställningsdata i AD DS | Förhindra användare från att aktivera BitLocker om inte datorn är ansluten till domänen och |

| Fasta inställningar för frekvensomriktare | |
|---|---|
| Alternativ för återställning av fasta enheter | Med den här inställningen kan du styra hur BitLocker-skyddade fasta enheter återställs om de inte har de nödvändiga inloggningsuppgifterna. Den här inställningen används under installationen av BitLocker. Som standard tillåts en certifikatbaserad dataåterställningsagent, återställningsalternativen kan anges av användaren, inklusive återställningslösenord och återställningsnyckel, och återställningsinformation säkerhetskopieras inte till AD DS. |
| Blockcertifikatbaserad agent för dataåterställning | |
| Lösenordsinställningar för BitLocker-återställning | |
| Inställningar för BitLocker-återställningsnyckel | |
| Spara information om BitLocker-återställning till Active Directory Domain Services | |
| Konfiguration av AD DS BitLocker-lagring för återställning | Förvaring av nyckelpaketet stöder återställning av data från en enhet som har skadats fysiskt. |
| Kräv lagring av återställningsdata i AD DS | Förhindra användare från att aktivera BitLocker om inte datorn är ansluten till domänen och säkerhetskopieringen av BitLocker-återställningsinformation till AD DS lyckas. Obs: Lösenordet för återställning genereras automatiskt. |
| Neka skrivåtkomst till oskyddade fasta enheter | |

| Inställningar för flyttbar enhet | |
|---|---|
| Neka skrivåtkomst till oskyddade flyttbara enheter | Neka skrivåtkomst till flyttbara dataenheter som inte skyddas av Bitlocker. Obs: Om "Flyttbara diskar: Neka skrivåtkomst" är aktiverat i grupprincipen ignoreras den här policyinställningen. |
| Neka skrivåtkomst till enheter som konfigurerats i en annan organisation | Endast enheter med identifieringsfält som matchar datorns identifieringsfält kommer att ges skrivåtkomst. Dessa fält definieras av grupprincipinställningen "Ange de unika identifierarna för din organisation". |

## BitLocker-tillstånd

Här kan du se det aktuella läget för BitLocker-krypterade enheter

| **C [OS Drive]** |
| --- |
| Status för kryptering |
| Krypterad (%) |
| Skyddsstatus |
| Krypteringsmetod |
| Nyckelskydd |
| Återställ lösenord |

Med ett klick på knappen "Rotate recovery password" kan du rotera BitLocker-återställningslösenordet.

# Certifikathantering

## Certifikatlista

Här finns en lista över certifikat som är installerade på den enhet som visas.

## Konfiguration av certifikat

Här kan du konfigurera certifikat och hur de ska installeras på enheten.

| **Betrodd certifikat** | |
|---|---|
| Beskrivning | Beskrivning av certifikat |
| Omfattning | Omfattning av certifikatsdistribution: Aktuell användare vs enhet |
| Förvaring av certifikat | "Otillförlitliga certifikat" är endast tillgängligt från och med Windows 10, version 1803 |
| Certifikatfil | Ladda upp en PKCS#1-fil |

| **Identitetscertifikat** | | | |
|---|---|---|---|
| Beskrivning | Beskrivning av certifikat | | |
| Omfattning | Omfattning av certifikatsdistribution: Aktuell användare vs enhet | | |
| Viktigt läge | Den Key Storage Provider som den privata nyckeln ska installeras på. | | |
| | | TPM. Misslyckas om ingen TPM finns | |
| | TPM. Om ingen TPM finns, återgår man till Software KSP | | |
| | Leverantör av programvara för lagring av nycklar | | Markera privat nyckel som exporterbar |
| | Windows Hello för företag | Container namn | Anger behållarnamnet för Windows Hello for Business (tidigare känt som Microsoft Passport for Work). |
| | | Text för PIN-meddelande | Anger den anpassade text som ska visas i PIN-prompten för Windows Hello for Business under certifikatregistreringen. |
| Legitimation | Ladda upp en PKCS#12-fil | | |

## SCEP

| | | | |
|---|---|---|---|
| Beskrivning | Beskrivning av SCEP-server | | |
| Driftsättningens omfattning | Omfattning av certifikatsdistribution: Aktuell enhet vs användare | | |
| URL:er för SCEP-server | En eller flera servrar som utfärdar certifikat via SCEP | | |
| Ämne | Representation av ett X.500-namn. T.ex. "C=US, O=Microsoft Corporation, CN=foo, 1.2.5.3=bar" | | |
| Ämnets alternativa namn | Typ | E-postadress | |
| | | DNS | |
| | | URI | |
| | | Användarens huvudnamn (UPN) | |
| CA Fingeravtryck | SHA1-fingeravtrycket för certifikatutfärdarens certifikat. E.g. 31:8F:1E:78:5C:D5:12:9F:7E:3B:AD:F3:1C:C0:19:03:96:43:A9:E5 | | |
| Giltighetstid enheter | Dagar, månader eller år | | |
| Giltighetstid | | | |
| Utmaning | Används som den för-delade hemligheten för automatisk registrering | | |
| Försök på nytt | Antalet gånger som enheten ska försöka igen om servern skickar ett PENDING-svar. Standardvärdet är 5. Högsta värdet är 30. | | |
| Fördröjning för omprövning | Antal minuter att vänta innan ny försök görs. Standardvärdet är 5. Minsta värde är 1. | | |
| Nyckelstorlek | Nyckelstorlek i bitar | | |
| Hash-algoritm | Hash-algoritmfamilj | | |
| Nyckelanvändning | Tillägget key usage definierar syftet (t.ex. kryptering, signatur) med den nyckel som finns i certifikatet. Minst ett av alternativen "Digital signature" eller "Key encipherment" måste väljas. | | |
| Utökad nyckelanvändning | Anger användning av utökade nycklar. Beroende på SCEP-serverns konfiguration. Ange listan över motsvarande OID:er, t.ex. 1.3.6.1.5.5.7.3.2 (Klientautentisering) | | |
| Viktigt läge | Den Key Storage Provider som den privata nyckeln ska installeras på. | | |
| | | TPM. Misslyckas om ingen TPM finns | |

| | | | | |
|---|---|---|---|---|
| | TPM. Om ingen TPM finns, återgår man till Software KSP | | | |
| | Leverantör av programvara för lagring av nycklar | | | |
| | Windows Hello för företag | Container namn | Anger behållarnamnet för Windows Hello for Business (tidigare känt som Microsoft Passport for Work). | |
| | | Text för PIN-meddelande | Anger den anpassade text som ska visas i PIN-prompten för Windows Hello for Business under certifikatregistreringen. | |

# Hantering av anslutningar

## Wifi

Med den här inställningen utför du förkonfigurationen av slutanvändarens enheter för åtkomst till interna åtkomstpunkter

| | |
|---|---|
| SSID (Service Set Identifier) | SSID till det nätverk som anslutningen kommer att upprättas till |
| Automatisk anslutning | Aktivera automatisk anslutning till nätverket |
| Dolda nätverk | Aktivera, om AP:n inte sänder SSID |

### Typ av säkerhet

Upprätta AP-säkerhetstyp

| **WEP öppet system** | |
|---|---|
| Lösenord | Lösenord för AP:n |

| **WPA PSK** | |
|---|---|
| Lösenord | Lösenord för AP:n |

| WPA EAP | |
|---|---|
| Typ av autentisering | Autentiseringstyp, endast möjlig med "PEAP-MSCAHPv2" |
| Snabb återanslutning | Enheter kan växla mellan accesspunkter utan att behöva autentisera sig på nytt |
| Tillträde för gäster | Användaren har inget konto och ska därför registrera sig som gäst |
| Karantänkontroller | Klienten måste utföra NAP-kontroller (Network Access Protection) och dela resultaten med systemet, som sedan avgör om klienten kan ansluta |
| Kräver Crypto Binding | Autentisering är endast möjlig via Crypto Binding |
| Servervalidering | Klienten kontrollerar om servercertifikatet är giltigt. Om så är fallet kommer en anslutning att upprättas |
| Fråga efter certifikat | Tillåter användaren att acceptera certifikat som inte är betrodda |
| Namn på server | Ger möjlighet att visa namnet på den RADIUS-server som erbjuder autentisering och auktorisering av nätverket |

| WPA2-PSK | |
|---|---|
| Lösenord | AP-lösenord |

| WPA2 EAP | |
|---|---|
| Typ av autentisering | Autentiseringstyp, endast möjlig med "PEAP-MSCAHPv2" |
| Snabb återanslutning | |
| Tillträde för gäster | |
| Karantänkontroller | Aktiverar skydd för nätverksåtkomst NAP |
| Kräver Crypto Binding | Autentisering är endast möjlig via Crypto Binding |
| Servervalidering | |
| Fråga efter certifikat | Frågar efter ett validerat servercertifikat, namn eller en CA (Root certificate authentication) |
| Namn på server | Lista över de servrar som ska vara betrodda av enheterna |
| Ingen | Ingen etablerad säkerhet |
| Använd proxyserver | Användning av en proxyserver |
| Serveradress | Proxyserverns adress |
| Serverport | Proxyserverns serverport |

### Använd proxyserver

Aktivera användning av proxyserver.

| | |
|---|---|
| Serveradress | Proxyserveradress som används av detta nätverk. |
| Serverport | Proxyserverport som används av detta nätverk. |

## Begränsningar för Wifi

Här kan du definiera olika Wifi-begränsningar.

| | |
|---|---|
| Tillåt WiFi | Tillåt/förbjud WiFi |
| Tillåt delning av Internet | Tillåt användning av en hotspot |
| Tillåt automatisk anslutning till WiFi Sense Hot Spots | Tillåt automatisk anslutning till WiFi Sense Hot Spots |
| Tillåt manuell WiFi-konfiguration | Tillåta användaren att ansluta till WiFi-nätverk som inte har definierats av AppTec |
| Frekvens för WLAN-sökning | Fastställer intervallet för WLAN-scanning. Här ökar förmågan att känna igen WIFI-nätverk med ett högre värde. |

## VPN

Gör lämpliga inställningar här för att konfigurera VPN-anslutningar

| | | | |
|---|---|---|---|
| Namn på anslutning | Angivet anslutningsnamn | | |
| VPN-typ | En VPN-anslutning per app används för att säkra trafiken i vissa appar. | | |
| | VPN | Alltid på | Detta kommer automatiskt att ansluta VPN vid inloggning och förblir anslutet tills användaren manuellt kopplar från. |
| | VPN per app | VPN-appar | Definiera appar som använder den här VPN-anslutningen |
| | | Låsning per app | Per-App Lockdown gör att de valda apparna endast har anslutning via den här VPN-anslutningen.<br>Den här funktionen är beroende av Windows Defender Firewall. |
| | WIP-profil | WIP-domän för denna anslutning | Företags-ID, som krävs för att ansluta den här VPN-profilen till en WIP-policy (Windows Information Protection) |

### Typ av anslutning

| **AppTec360 VPN** | |
|---|---|
| För "AppTec360 VPN" krävs det att sidoladdning av appar är tillåtet. Aktivera "Allow App Sideloading" i "Security Management" → "Restriction Settings" → "Device Functionality". | |
| Gateway-konfiguration | För att konfigurera en VPN-anslutning med svartlistning måste du välja en VPN-konfiguration med en angiven DNS-server. Du kan ställa in en VPN-konfiguration i "Allmänna inställningar" → "Universal Gateway" → "VPN-inställningar". |

| **IKEv2** | | |
|---|---|---|
| Servrar | Lista över VPN-servrar | |
| Enhet Tunnel | Aktivera anslutning innan användaren loggar in. | |
| Autentiseringsmetod | EAP | EAP XML |
| | Maskincertifikat | |
| Krypteringsalgoritm | | |
| Algoritm för integritetskontroll | | |
| Diffie-Hellman-grupp | | |
| Algoritm för chiffertransformation | | |
| Algoritm för autentiseringstransformation | | |
| PFS (Perfect Forward Secrecy)-grupp | | |

| **PPTP** | | |
|---|---|---|
| Servrar | Lista över VPN-servrar | |
| Autentiseringsmetod | EAP | EAP XML |

| **L2TP** | | |
|---|---|---|
| Servrar | Lista över VPN-servrar | |
| Autentiseringsmetod | EAP | EAP XML |
| Krypteringsalgoritm | | |
| Algoritm för integritetskontroll | | |
| Diffie-Hellman grupp | | |
| Algoritm för chiffertransformation | | |
| Algoritm för autentiseringstransformation | | |
| PFS (Perfect Forward Secrecy)-grupp | | |

| **Automatisk** | | |
|---|---|---|
| Servrar | Lista över VPN-servrar | |
| Autentiseringsmetod | EAP | EAP XML |

## Generiska VPN-konfigurationer

| | |
|---|---|
| Kom ihåg inloggningsuppgifterna vid varje inloggning | |
| Registrera IP-adresser med intern DNS | |
| Regler för filtrering av nätverkstrafik | Begränsa VPN-anslutningen till den definierade regeluppsättningen. |
| Sökningslista för DNS-suffix | DNS-suffix som ska läggas till i DNS-söklistan för routning av kortnamn. |
| NRPT-regler (Name Resolution Policy Table) | NRPT-regler (Name Resolution Policy table) definierar hur DNS löser namn när den är ansluten till VPN. |
| Detektering av betrodda nätverk | Lista över DNS-suffix för identifiering av betrodda nätverk. |
| Delad tunnling | Split tunneling innebär att trafiken kan gå över vilket gränssnitt som helst, vilket bestäms av nätverksstacken. |
| Dela upp tunnlande rutter | Lista över rutter som ska läggas till i routningstabellen för VPN-gränssnittet. |
| Proxy-inställning | Konfigurerar Proxy som används i detta nätverk |
| Fullmaktsadress | Proxyserverns adress som ett fullständigt kvalificerat värdnamn eller en IP-adress. |
| Port | Port för proxyserver. |
| URL för automatisk konfigurering av proxy | URL för att automatiskt hämta proxyinställningarna. |

## VPN-begränsningar

Här kan du definiera olika VPN-begränsningar.

| | |
|---|---|
| Tillåt VPN-inställningar | Denna riktlinje tillåter/förbjuder användaren att avaktivera och ändra VPN-inställningarna |
| Tillåt VPN över mobilnätet | Tillåter/förbjuder enheten att upprätta en VPN-anslutning om enheten använder mobildata |
| Tillåt VPN-roaming över mobilnätet | Tillåter/förbjuder enheten att upprätta en VPN-anslutning, om enheten roamar |

## Bluetooth

Här kan du bestämma om Bluetooth ska vara tillåtet/förbjudet.

| | |
|---|---|
| Tillåt Bluetooth | Aktivera/avaktivera Bluetooth |

# PIM-hantering

## Exchange Active Sync

Inställning av ActiveSync-kontot på slutanvändarens enhet

| | |
|---|---|
| Kontots namn | Namn på e-postkonto |
| Serverns värdnamn | Serveradress/FQDN |
| Domännamn | Domän för server |
| E-postadress | E-postadress |
| Användarnamn | Användarens namn |
| Användarens lösenord | Alternativt kan du redan här koppla ett lösenord till användaren |
| Använd SSL | Använd SSL-anslutning |
| Synkroniseringsintervall | Här kan synkroniseringsintervallet fastställas<br>Manuell synkronisering = Användaren måste ladda ner sina e-postmeddelanden och utföra en manuell synkronisering |
| Åldersfilter för e-post | Tidsperiod tills e-postmeddelandena ska synkroniseras<br>Inget filter = obegränsat |
| Loggnivå | Fastställande av loggningsnivåer för ActiveSync-trafiken |
| Synkronisera e-post | Aktiverad = e-postmeddelanden synkroniseras |
| Synka kontakter | Aktiverad = kontakterna är synkroniserade |
| Synkronisera kalender | Aktiverad = kalendern är synkroniserad |
| Synka uppgifter | Aktiverad = uppgifterna är synkroniserade |

## E-post

Upprättande av POP3/IMAP4-konton på slutanvändarens enhet.

| | |
|---|---|
| Beskrivning av konto | Namn på e-postkonto |
| Avsändarens namn | Visat avsändarnamn |
| Domännamn | Domännamn för e-postkontot |
| E-postadress | Användarens e-postadress |
| Användarnamn | Användarens namn |
| Användarens lösenord | Alternativt kan du redan här koppla ett lösenord till användaren |
| Alternativa autentiseringsuppgifter för utgående server | Här kan det definieras om andra autentiseringsuppgifter krävs för den utgående servern |
| Utgående domännamn | Utgående domännamn |
| Användarnamn för utgående server | Användarnamn för utgående server |
| Lösenord för utgående server | Lösenord för utgående server |
| E-postprotokoll | POP3 eller IMAP4, kan användas som protokoll |
| Hostnamn för server för inkommande e-post | Värdnamn för server för inkommande e-post |
| Använd SSL för inkommande e-post | Använd SSL för inkommande e-post |
| Hostnamn för server för utgående e-post | Värdnamn för server för utgående e-post |
| Använd SSL för utgående e-postmeddelanden | Använd SSL för utgående e-post |
| Autentisering av utgående server | En autentisering av utgående server krävs |
| Synkroniseringsintervall | Här kan synkroniseringsintervallet fastställas<br>Manuell synkronisering = Användaren måste ladda ner sina e-postmeddelanden och utföra en manuell synkronisering |
| Åldersfilter för e-post | Tidsperiod tills e-postmeddelandena ska synkroniseras<br>Inget filter = obegränsat |

# App-hantering

## Enterprise App Manager

### Installerade appar

Här finns en lista över de appar som för närvarande är installerade på den enhet som visas.

### Obligatoriska appar

Här kan du konfigurera en lista över appar som är obligatoriska på enheten.

Den här listan kontrolleras varje gång enheten ansluts till MDM och alla appar i listan som inte är installerade på enheten installeras, oavsett om appen har avinstallerats eller aldrig har installerats tidigare.

Du kan ladda upp Windows 10 In-House Apps och sedan lägga till dem i den här listan eller så kan du lägga till Microsoft Office-konfigurationer som måste konfigureras i förväg i "Allmänna inställningar" > "Apphantering" > "Microsoft Office".

## Sys App Begränsningar

| **Appar för inkorg** |
| --- |
| Tillåt larm och klocka |
| Tillåt kalkylator |
| Tillåt kamera |
| Tillåt kontaktstöd |
| Tillåt Cortana |
| Tillåt filutforskaren |
| Tillåt komma igång |
| Tillåt Groove Music |
| Tillåt kartor |
| Tillåt meddelanden |
| Tillåt Microsoft Edge |
| Tillåt filmer och TV |
| Tillåt pengar |
| Tillåt nyheter |
| Tillåt OneDrive |
| Tillåt OneNote |
| Tillåt Outlook-kalender och e-post |
| Tillåt människor |
| Tillåt telefon |
| Tillåt foton |
| Tillåt Powerpoint |
| Tillåt inställningar |
| Tillåt Skype |
| Tillåt sport |
| Tillåt butik |
| Tillåt röstinspelare |
| Tillåt plånbok |
| Tillåt väder |

| |
|---|
| Tillåt Windows Feedback Hub |
| Tillåt ord |
| Tillåt Xbox |

| **Inställning av sidor** |
| --- |
| Tillåt konton på arbetsplatsen |
| Tillåt avancerad information |
| Tillåt appar hörnet |
| Tillåt blockering och filtrering |
| Tillåt färgprofil |
| Tillåt körläge |
| Tillåt e-post och konton |
| Tillåt Equalizer |
| Tillåt tangentbord |
| Tillåt navigeringsfält |
| Tillåt flygplansläge för nätverk |
| Tillåt delning av nätverk och internet |
| Tillåt nätverkstjänster |
| Tillåt nätverk Wi-Fi |
| Tillåt PC-system Bluetooth |
| Tillåt betygsättning av din enhet |
| Tillåt återställning av uppdatering |
| Tillåt delning |
| Tillåt start |
| Tillåt tid Språk |
| Tillåt tid Region |
| Tillåt Windows standardlåsskärm |
| Tillåt konto för arbete eller skola |

## Svart- och vitlistning

Under "Black- & Whitelisting" kan du välja mellan läget "Whitelist" och läget "Blacklist".

| | |
|---|---|
| Vitlista | Endast appar och tjänster som läggs till i listan kan installeras på slutanvändarens enhet. Om dessa redan är förinstallerade på slutanvändarens enhet kommer de att aktiveras och ställas in så att användaren kan köra dem. |
| | Alla andra appar som inte läggs till i listan kan inte installeras på slutanvändarens enhet. Om dessa redan är förinstallerade på slutanvändarens enhet kommer de att avaktiveras och ställas in så att användaren inte kan köra dem. |
| Svarta listan | Appar och tjänster som läggs till i listan kan inte installeras på slutanvändarens enhet. Om dessa redan är förinstallerade på slutanvändarens enhet kommer de att avaktiveras och ställas in så att användaren inte kan köra dem. |
| | Alla andra appar som inte har lagts till i listan kan installeras på slutanvändarens enhet. Om dessa redan är förinstallerade på slutanvändarens enhet kommer de att aktiveras och ställas in så att användaren kan köra dem. |

Med kan du lägga till ytterligare appar eller tjänster i den lista som används för tillfället.

Med kan du lägga till ytterligare appar eller tjänster i den inaktiva listan.

Du kan antingen lägga till en app från "Windows App Store" eller direkt ange en "App Identifier" för att lägga till den i den svarta eller vita listan.

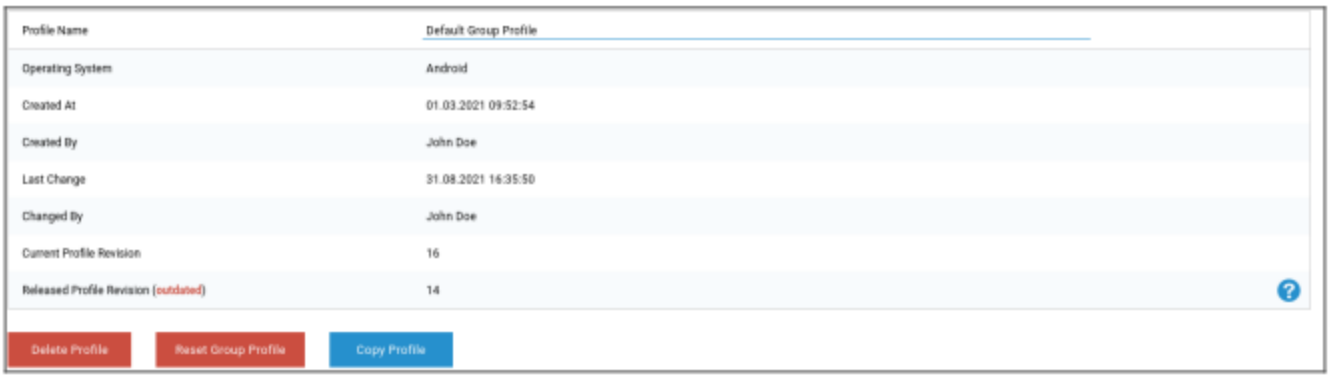
# MacOS-konfiguration

Beroende på om du har valt en profil eller en enhet är displayen och dess underpunkter olika - var uppmärksam på detta!

## Allmänt

### Översikt över grupprofiler (endast på gruppnivå)

När du öppnar en grupprofil får du en snabb överblick över profilen.




| | |
|---|---|
| Profilens namn | Profilens namn (kan ändras här) |
| Operativsystem | Operativsystem som profilen är avsedd för |
| Skapad vid | Tidpunkt för skapelse |
| Skapad av | Skaparen av profilen |
| Sista förändringen | Tidpunkt för senaste ändring av profilen |
| Förändrad av | Konto som gjorde de senaste ändringarna |
| Aktuell profil Revidering | Revidering av sparat profiltillstånd |
| Utgiven Profil Revision | Tilldelad profilrevision ("Tilldela nu"). Om etiketten visar "(outdated)" bakom texten betyder det att du har sparat profilen men inte tilldelat den ännu, så enheterna kommer fortfarande att få en äldre version. |

### Enhetsöversikt (endast på enhetsnivå)

Enhetens sammanfattade översikt.

| | |
|---|---|
| Enhetens namn | Enhetens namn |
| Modell | Modell |
| Operativsystem | Operativsystem |
| Serienummer | Enhetens serienummer |
| Ägande av enhet | Den konfigurerade ägartypen |
| Enhetstyp | Typ av enhet |
| Överensstämmande | Visar om enheten är kompatibel |
| IP-adress | IP-adressen för den enhet som är ansluten till servern från |
| Senast sett | Tidpunkt för den senaste anslutningen från enheten |
| Sista knuffen | Tidpunkt för den senaste push som skickades till enheten |
| Uppdrag | Här kan du flytta enheten till en annan användare eller grupp |

## Config Revision (endast på enhetsnivå)

Här får du en översikt över vilken grupprofil som är tilldelad enheten.


Om du klickar på grupprofilen kommer du direkt till profilen och kan göra inställningar.

Med symbolen kan du återställa de tilldelade apparna till grupprofilens inställningar.

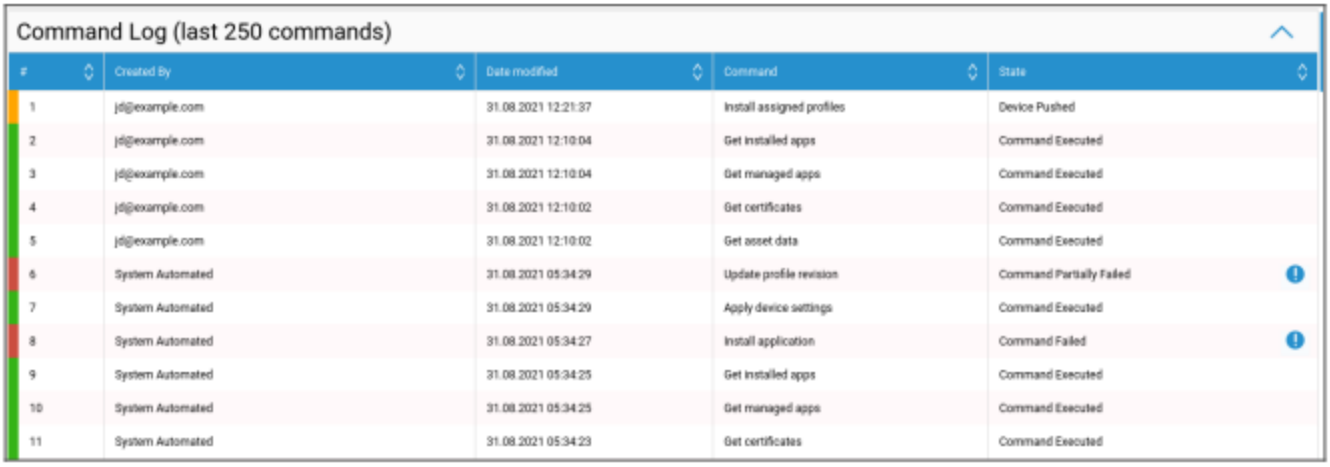
Med symbolen kan du återställa enhetens profil så att den inte har några inställningar alls.

"Nyare revision tillgänglig" anger att grupprofilen har ändrats och sparats men inte tilldelats.
Grupprofilen måste tilldelas med "Tilldela nu" på gruppnivå för att ändringarna ska gälla för enheterna.

## Enhetslogg (endast på enhetsnivå)

### Kommandologg

Här kan du se vilka kommandon som har utfärdats för enheten och vilken status de har.




Kommandon som skapats av "System Automated" skapas automatiskt av systemet.

## Möjliga kommandostatusar

| | |
|---|---|
| Enhet tryckt | En push-begäran har skickats till push-tjänsten (t.ex. APNS) för att tala om för enheten att den ska ansluta tillbaka till EMM-servern. |
| Kommando Skapat | Kommandot skapades i systemet. |
| Kommando skickat | Kommandot skickades till enheten efter att den anslutit till servern. |
| Kommando utfört | Kommandot har utförts framgångsrikt. |
| Kommandot misslyckades | Kommandot misslyckades. * |
| Kommandot delvis misslyckat | Beroende på enhetens operativsystem kan vissa kommandon grupperas tillsammans.<br>I detta misslyckades vissa delar av denna kommandogrupp. * |
| Kommando utfört, eventuellt misslyckat | Kommandot utfördes, men kanske inte. |
| Kommando Repushed | Kommandot återställdes av en användare. |
| Bortkastad | Kommandot kasserades. Till exempel för att det ersattes av ett annat kommando eller för att enheten registrerades på nytt och gamla kommandon togs bort |

*Om det finns ett utropstecken bakom meddelandet kan du få mer information genom att hålla muspekaren över ikonen.

# Tillgångshantering (endast på enhetsnivå)

## Info om enhet

| | |
|---|---|
| Modellnummer | Modellnummer |
| Värdnamn | Värdnamn |
| Lokalt värdnamn | Lokalt värdnamn |
| Operativsystem | Operativsystem |
| OS-version | OS-version |
| UDID | UDID |
| Fritt / totalt minne | Fritt / totalt minne |

## WiFi

| | |
|---|---|
| IP-adress | IP-adress |
| WiFi MAC | WiFi MAC |

## Cellulär

| | |
|---|---|
| Telefonnummer | Telefonnummer |
| Status för roaming | Status för roaming |
| Roaming (röst/data) | Roaming (röst/data) |
| IP-adress | IP-adress |
| Operatör/transportör | Operatör/transportör |
| SIM-operatör Nätverk | Bärarnätverk |
| Version för bärare | Version för bärare |
| ICCID | ICCID |
| Nuvarande MCC/MNC | Nuvarande MCC/MNC |
| SIM MCC/MNC | SIM MCC/MNC |

## Bluetooth

| | |
|---|---|
| Bluetooth MAC | Bluetooth MAC |

# Uppdateringshantering (endast på enhetsnivå)

## Uppdatera information

Den här fliken visar information om inställningarna för systemuppdatering på enheten.

| | |
|---|---|
| Autocheck aktiverad | Om systemet söker efter uppdateringar automatiskt. |
| Automatisk app-uppdatering aktiverad | Om systemet ska installera appuppdateringar automatiskt. |
| Automatiska OS-uppdateringar aktiverade | Om systemet ska installera systemuppdateringar automatiskt. |
| Automatiska säkerhetsuppdateringar aktiverade | Om systemet ska installera säkerhetsuppdateringar automatiskt. |
| Appuppdatering Bakgrund - Nedladdning aktiverad | Om systemet kommer att ladda ner appuppdateringar i bakgrunden. |
| Katalog URL | URL till den katalog för programuppdateringar som klienten använder. |
| Är standardkatalog | Om "ja", Catalog är standardkatalogen. |
| Utför periodisk kontroll | Om "ja", starta en ny skanning. |
| Datum för tidigare skanning | Datum för den senaste skanningen av programuppdateringen. |
| Resultat från tidigare skanning | Resultatkoden för den senaste programuppdateringssökningen. |

# Säkerhetshantering

## Stöldskydd

### Torka och lås

| | |
|---|---|
| Fullständig avtorkning | Skicka ett kommando för att fabriksåterställa enheten |
| Enterprise Wipe | Ta bort MDM från enheten och ta bort alla MDM-data (t.ex. konton, appar) |
| Lås skärm | Få enheten att återgå till låsskärmen |

## Säkerhetskonfiguration

### Lösenord

| | |
|---|---|
| Avaktivering av kod tillåten | Bestämmer om användaren måste ange en PIN-kod. Om du bara anger detta värde (och inte andra) tvingas användaren att ange ett lösenord, utan att ange längd eller kvalitet. |
| Tillåt enkelt värde | Tillåt användaren att använda samma, eskalerande och reducerande nummersträngar (t.ex. 1234, 1111) |
| Kräver alfanumeriskt värde | Lösenord måste innehålla minst en bokstav |
| Minsta längd på lösenkod | Minsta lösenordslängd |
| Minsta antal komplexa tecken | Minsta antal alfanumeriska symboler i lösenordet |
| Maximal ålder för lösenkod | Antal dagar efter vilka lösenordet måste ändras |
| Maximal automatisk låsning | Maximal tid efter vilken enheten är låst |
| Maximal frist för låsning av enhet | Den tid som enheten kan låsas utan att lösenord efterfrågas vid upplåsning |
| Maximal lösenordsålder (1-730 dagar, eller ingen) | Dagar efter vilka lösenordet måste ändras |
| Lösenordshistorik (1-50 lösenord, eller inga) | Antal unika lösenord före återanvändning |

## Certifikat

| **PKCS#1** | |
|---|---|
| Beskrivning | Ange en beskrivning för certifikatet |
| Legitimation | Ladda upp en pkcs1-fil |

| **PKCS#12** | |
|---|---|
| Beskrivning | Ange en beskrivning för certifikatet |
| Legitimation | Ladda upp en pkcs12-fil |

# Inställningar för begränsning

## Enhetens funktionalitet

| | |
|---|---|
| Tillåt kamera | Tillåt användning av kameran |
| Tillåt Game Center | Om den är falsk inaktiveras Game Center och dess ikon tas bort från startskärmen. |
| Tillåt multiplayer-spel | När den är falsk förbjuds multiplayer-spel. |
| Tillåt att lägga till Game Center-vänner | När false, förbjuder att lägga till vänner i Game Center. |
| Tillåt iCloud Photo Library | Om inställningen är false inaktiveras iCloud Photo Library. Alla foton som inte har laddats ner helt från iCloud Photo Library till enheten kommer att tas bort från det lokala lagringsutrymmet. |
| Tillåt Touch ID | Om false, förhindrar Touch ID från att låsa upp en enhet. |

## iCloud

Blockera vissa funktioner under iCloud-parning

| | |
|---|---|
| Tillåt synkronisering av dokument | Tillåt synkronisering av dokument |
| Tillåt synkronisering av iCloud-nyckelring | Tillåt synkronisering av iCloud-nyckelring |
| Tillåt iCloud-anteckningar | När false, avaktiverar MacOS iCloud Notes-tjänster |
| Tillåt iCloud BTMM | När false, avaktiverar MacOS iCloud-tjänsten Tillbaka till min Mac. |
| Tillåt iCloud FMM | När false, avaktiverar MacOS Find My Mac iCloud-tjänsten. |
| Tillåt iCloud-bokmärken | När false, avaktiveras synkronisering av MacOS iCloud-bokmärken. |
| Tillåt iCloud Mail | När false, avaktiverar MacOS Mail iCloud-tjänster. |
| Tillåt iCloud-kalender | När false, avaktiverar MacOS Cloud iCloud-tjänster. |
| Tillåt iCloud-påminnelser | När false, avaktiverar iCloud påminnelsetjänster. |
| Tillåt iCloud Adressbok | När false, avaktiverar MacOS iCloud Address Book-tjänster. |

## Mediahantering

| | |
|---|---|
| Utmatning vid utloggning | Mata ut alla flyttbara media vid utloggning |
| Tillåt nätverk | Tillåt åtkomst för nätverksmedia |
| Tillåt intern disk | Tillåt åtkomst för intern disk. |
| Kräver autentisering | Kräv autentisering för användning av detta media |
| Endast läsning | Användaren kan endast läsa data från mediet |
| Tillåt extern disk | Tillåt åtkomst för extern disk. |
| Kräver autentisering | Kräv autentisering för användning av detta media |
| Endast läsning | Användaren kan endast läsa data från mediet |
| Tillåt användning av diskavbildningar | Tillåt åtkomst för bilder. |
| Kräver autentisering | Kräv autentisering för användning av detta media |
| Endast läsning | Användaren kan endast läsa data från mediet |
| Tillåt användning av DVD-RAM | Tillåt åtkomst för DVD-RAM-disk. |
| Kräver autentisering | Kräv autentisering för användning av detta media |
| Endast läsning | Användaren kan endast läsa data från mediet |
| Tillåt användning av DVD-skivor | Tillåt åtkomst för DVD-skiva. |
| Kräver autentisering | Kräv autentisering för användning av detta media |
| Tillåt användning av CD-skivor | Tillåt åtkomst för CD-skiva. |
| Kräver autentisering | Kräv autentisering för användning av detta media |

# Hantering av anslutningar

## Wi-Fi

Här kan du lägga till och konfigurera Wi-Fi-anslutningar

| | |
|---|---|
| SSID (Service Set Identifier) | SSID för det nätverk som anslutningen kommer att upprättas till |
| Automatisk anslutning | Aktivera automatisk anslutning för nätverket |
| Dolda nätverk | Aktivera, om AP:n inte sänder SSID |
| Proxy-inställning | Konfigurering av en proxy för varje accesspunkt |
| Ingen | Använd inte en proxyserver |
| Manuell | Upprätta en manuell fullmakt |
| URL för proxyserver | Adress för åtkomst till Proxy-inställningar |
| Port | Fastställ porten för proxyservicen |
| Autentisering | Användarnamn för autentisering på Proxy |
| Lösenord | Lösenord för autentisering på proxyserver |
| Automatisk | Upprätta en proxy automatiskt |
| URL för proxyserver | URL för filen med proxyinställningar |
| Typ av säkerhet | Upprätta säkerhetstyp för AP:n |
| WEP | |
| Lösenord | Lösenord för AP:n |
| WPA/WPA2 | |
| Lösenord | Lösenord för AP:n |
| WEP Enterprise - WPA / Företag<br>WPA2 Enterprise / Företag<br>Alla företag | Se tabell Fel: Referenskälla hittades inte nedan |
| Ingen | Upprätta ingen säkerhet |
| Avaktivera randomisering av MAC-adress | Inaktiverar randomisering av MAC-adresser för det Wi-Fi-nätverket när det är associerat med nätverket. Detta visar också en sekretessvarning i Inställningar som anger att nätverket har minskat sekretesskydd. |

## Konfiguration av Wi-Fi för företag

Obs: Endast tillgängligt när "Security Type" är inställt på en Enterprise Type.

| | |
|---|---|
| Protokoll | Autentiseringsprotokoll som stöds i målnätverket |
| TLS | Aktivera / Inaktivera användning |
| TTLS | Aktivera / Inaktivera användning |
| Inre autentiseringar | Autentiseringsprotokoll som ska användas: PAP, CHAP, MSCHAP, MSCHAPv2 |
| LEAP | Aktivera / Inaktivera användning |
| PEAP | Aktivera / Inaktivera användning |
| EAP-FAST | Aktivera / Inaktivera användning |
| EAP-SIM | Aktivera / Inaktivera användning |
| Använd PAC | Användning av PAC (Protected Access Control) |
| Tillhandahållande PAC | Konfiguration av Provision PAC |
| Tillhandahålla PAC anonymt | Anonymt tillhandahållande av PAC |
| Autentisering | |
| Användarnamn | Användarnamn för autentisering |
| Använd inte Per anslutning Lösenord | Använd inte Per-Connection Password |
| Lösenord | Lösenordet som ska användas |
| Identitetscertifikat | Ladda upp/välja autentiseringscertifikat |
| Yttre identitet | Identitet som kan ses externt |
| Förtroende | |
| Betrott certifikat 1 | Ladda upp det första betrodda certifikatet |
| Betrott certifikat 2 | Ladda upp det andra betrodda certifikatet |
| Betrott certifikat 3 | Ladda upp ett tredje betrott certifikat |
| Betrodd server Namn på certifikat | Namnen på de förväntade servercertifikaten (i en kommaseparerad lista) |

## VPN

Beroende på vilken Connection Type som valts kan olika fält vara synliga.

| | |
|---|---|
| Namn på anslutning | Namn på VPN-profilen |
| VPN-typ | |
| VPN | All nätverkstrafik för enheten kommer att dirigeras via en VPN-anslutning. |
| Typ av anslutning | Upprätta typ av VPN-anslutning |
| IPsec (Cisco) | IPsec-protokoll från Cisco |
| L2TP | L2TP-protokoll |
| Anpassad SSL | Anslutning via anpassad SSL |
| IKEv2 | IKEv2-protokoll |
| Proxy-inställning | Konfigurering av en proxy för VPN-anslutningen |
| Ingen | Upprätta ingen Proxy |
| Manuell | Upprätta en proxy manuellt |
| URL för proxyserver | Adress för åtkomst till Proxy-inställningar |
| Port | Fastställ porten för proxyservicen |
| Autentisering | Användarnamn för autentisering hos proxyservicen |
| Lösenord | Lösenord för autentisering hos proxyservicen |
| Automatisk | Upprätta en proxy automatiskt |
| URL för proxyserver | URL för åtkomst till Proxy-inställningarna |

## HTTP-proxy

| Typ av proxy | |
|---|---|
| Manuell | Upprätta en proxy manuellt |
| URL för proxyserver | Adress för åtkomst till proxyinställningarna |
| Port | Upprätta Proxy-port |
| Autentisering | Användarnamn för autentisering hos proxyservicen |
| Lösenord | Lösenord för autentisering hos proxyservicen |
| Automatisk | Upprätta en proxy automatiskt |
| Proxy PAC URL | Proxy PAC URL |
| Tillåt direktanslutning om PAC inte går att nå | Tillåt direktanslutning (utan VPN) om PAC inte kan nås |
| Tillåt kringgående av proxy för åtkomst till slutna nätverk | Tillåt kringgående av proxy för åtkomst till interna nätverk |

## AirPrint

| | |
|---|---|
| IP-adress | IP-adress för skrivare |
| Resursväg | Definitiv väg till AirPrint-enheten |

## AirPlay

| | |
|---|---|
| Enhetens namn | Enhetens namn |
| Lösenord | Lösenord för parkoppling |
| Vitlista | Definiera en lista över enheter som enheten kan para ihop sig exklusivt med |

# PIM-hantering

## Exchange Active Sync

| | |
|---|---|
| Kontots namn | Kontots namn. |
| E-postadress | Adressen till kontot (t.ex. max@company.com) |
| Serverns värdnamn | Internt värdnamn |
| Inloggningsnamn | "Domain" och "Login Name" måste vara tomma för att enheten ska fråga efter användare. |
| Domän | "Domain" och "Login Name" måste vara tomma för att enheten ska fråga efter användare.<br>Om en ACL Gateway konfiguration är aktiverad och fältet Domain inte är tomt kommer AppTec360 Universal Gateway att autentisera enheten med följande namn "Domain\Login Name" |
| Lösenord | Lösenordet för kontot (t.ex. secretUserPassword) |
| Tidigare dagar av Mail to Sync | Antalet senaste dagar med post som ska synkroniseras |
| Använd SSL | Använd SSL för intern Exchange-värd |
| Avancerat alternativ | Visa avancerade alternativ |
| Serverport | Intern port |
| Serverväg | Intern väg |
| Externt värdnamn | Extern värd |
| Extern port | Extern port |
| Extern sökväg | Extern sökväg |
| Använd SSL för externa Utbytesvärd | Använd SSL för extern Exchange-värd |

## E-post

Inställning av POP3-/IMAP-konton på slutanvändarens enhet

| | |
|---|---|
| Beskrivning av konto | Namn des e-postkonton |
| Typ av konto | |
| IMAP | |
| Prefix för sökväg | Sökvägsprefixet för specialmappar |
| POP | |
| Användarens visningsnamn | Användarens visningsnamn |
| E-postadress | Användarens e-postadress |

| | |
|---|---|
| Inkommande post | Inställningar för inkommande server |
| Adress till e-postserver | Adress till e-postserver |
| Port för e-postserver | Port för e-postserver |
| Användarens namn | Respektive användarnamn |
| Typ av autentisering | Typ av autentisering |
| Ingen | Ingen typ av autentisering |
| Lösenord (endast på enhetsnivå) | Lösenordsfråga |
| MDM-utmaning-svar | |
| NTLM | NTLM-autentisering |
| HTTP MD5-digest | |
| Använd SSL | Använd SSL, om det behövs |

| | |
|---|---|
| Utgående post | Inställningar för utgående server |
| Adress till e-postserver | Adress till e-postserver |
| Port för e-postserver | Port för e-postserver |
| Användarnamn | Respektive användarnamn |
| Typ av autentisering | |
| Ingen | Ingen autentiseringsmetod |
| Lösenord (endast på enhetsnivå) | Lösenordsfråga |
| MDM-utmaning-svar | |
| NTLM | NTLM-autentisering |
| HTTP MD5-digest | |
| Använd SSL | Använd SSL, om det behövs |
| Utgående lösenord samma som inkommande | Utgående lösenord samma som inkommande |
| Använd endast i mail | Aktivera, om alla utgående e-postmeddelanden ska skickas via Mail-appen |

## CalDav

Konfigurera uppsättning och distribution av ett CalDav-konto

| | |
|---|---|
| Beskrivning av konto | Kontots visningsnamn |
| Värdnamn | Värdnamn och/eller IP-adress |
| Port | Hamn för CalDav-kontot |
| Huvud-URL | Kontots huvudsakliga webbadress |
| Användarnamn | Respektive CalDav-användarnamn |
| Lösenord (endast på enhetsnivå) | Respektive CalDav-lösenord |
| Använd SSL | Använd SSL, om det behövs |

## KortDav

Konfigurera uppsättning och distribution av ett CardDav-konto

| | |
|---|---|
| Beskrivning av konto | Kontots visningsnamn |
| Värdnamn | Värdnamn och/eller IP-adress |
| Port | Port för CardDav-kontot |
| Huvud-URL | Kontots huvudsakliga webbadress |
| Användarnamn | Respektive CardDav-användarnamn |
| Lösenord (endast på enhetsnivå) | Respektive CardDav-lösenord |
| Använd SSL | Använd SSL, om det behövs |

## LDAP

I det här området konfigurerar du en LDAP-anslutning för att möjliggöra ett dynamiskt certifikatutbyte mellan slutanvändarenheten och Active Directory.

Observera att den valda användaren måste ha läsbehörighet.

| | |
|---|---|
| Beskrivning av konto | Beskrivning av konto |
| Användarnamn för konto | Användare för LDAP-åtkomst |
| Lösenord för konto | Lösenord för LDAP-åtkomst |
| Kontots värdnamn | LDAP-serverns värdnamn/IP-adress |
| Använd SSL | Använd SSL, om det behövs |

I den andra delen kan du definiera individuella filter för sökning i LDAP-registret.

| | | |
|---|---|---|
| Beskrivning | Omfattning | Sök bas |
| Beskrivning av filter | Söknivå i LDAP-registret | Definiera det individuella filtret |

# Instrumentpanel & rapportering

## Inställningar för instrumentpanelen

Här kan du se vilka dashboards som finns, redigera dem eller skapa nya. Varje dashboard har sin egen uppsättning data som ska visas och grafkonfiguration.


Kontroll av inställningar för instrumentpanelen

| | |
|---|---|
| Allmänheten | Gör kontrollpanelen publik, så att andra användare kan se kontrollpanelen. Användarna måste naturligtvis kunna logga in och visa Dashboards. Om "Public" inte är aktiverat är det bara skaparen som kan se den. |
| Standard | Ställer in Dashboard som standard så att den öppnas automatiskt nästa gång du öppnar Dashboard View. |
| | Visa instrumentpanelen och dess grafer |
| | Ta bort instrumentpanelen |
| | Redigera instrumentpanelens namn och inställningar |
| | Gör en kopia av Dashboard |
| | Lägg till en helt ny instrumentpanel |

# Dashboard-vy

Här visas data och diagram för den valda instrumentpanelen och du kan även ändra dessa.


Kontroll av instrumentpanelen

| | |
|---|---|
| | Låter dig definiera vilka data som ska visas i Dashboard, mängden data som ska visas och i vilken storlek dessa data ska visas |
| | Tar dig tillbaka till översikten över instrumentpanelen |
| | Återställer den aktuella instrumentpanelen till standardinställningen |
| | Sparar alla ändringar som du har gjort i den aktuella instrumentpanelen (t.ex. vilka data som ska visas) |
| | Ändra diagramtyp till pelardiagram |
| | Ändra diagramtyp till cirkeldiagram |
| | Ändra diagramtyp till munkdiagram |
| | Ändra diagramtyp till polarområdesdiagram |
| | Ändra sorteringsordning |

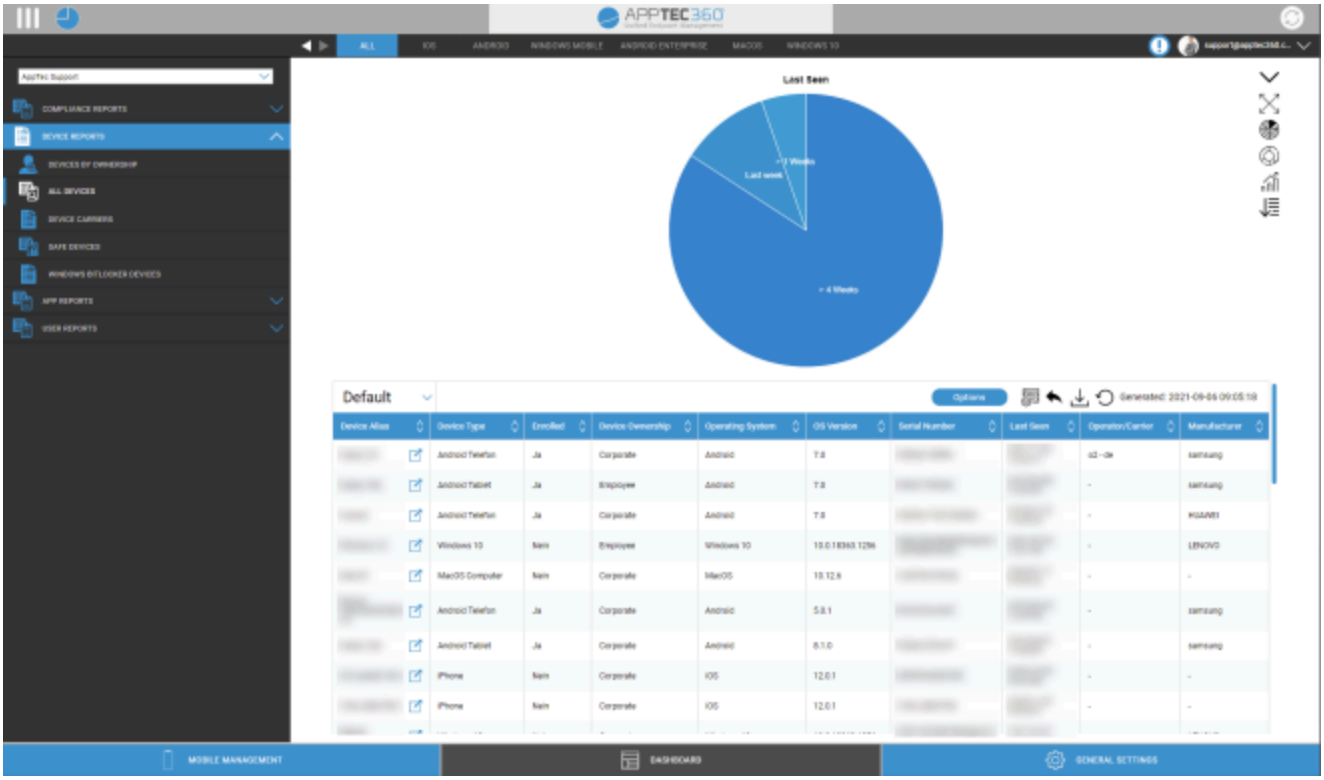
# Utökad rapportering

"Utökad rapportering" ger detaljerade översikter och grafer över enhets- och användarinformation.

Det finns några standardrapporter, men alla kan ändras manuellt för att lägga till eller ta bort data som ska visas.

Observera att du endast manuellt kan ändra vilka data som visas. Den valda rapportkategorin definierar vilka data den baseras på. Du kommer t.ex. aldrig att kunna se Android-enheter i iOS-rapporten i Enhetsrapporter Alla enheter iOS

Längst upp till vänster kan du begränsa rapporteringsdata till en viss grupp (och alla dess undergrupper). Som standard är detta inställt på din rotnod, så den tar hänsyn till ALLA enheter och användare.



Utökad rapporteringskontroll

I varje översikt kan du använda följande funktioner för att ändra rapporten på det sätt du vill:

| | |
|---|---|
| | Dölj diagram (om diagram visas) |
| | Visa diagrammet (om diagrammet är dolt) |
| | Expandera diagrammet (om diagrammet är hopfällt) |
| | Kollapsa diagrammet (om diagrammet är expanderat) |
| | Ändra diagramtyp till pelardiagram |
| | Ändra diagramtyp till cirkeldiagram |
| | Ändra diagramtyp till munkdiagram |
| | Ändra diagramtyp till polarområdesdiagram |
| | Ändra sorteringsordning |
| | Ändra följande delar av den översikt som visas:<br>• Lägg till/ta bort kolumner<br>• Ange i vilken ordning kolumnerna ska visas<br>• Visa/dölj diagrammet ovanför tabellen<br>• Välj den kolumn som ska användas för diagrammet<br>• Filtrera data från din tabell |
| | Öppna inställningshanteraren för att spara och ladda olika rapporter |
| | Återställer den aktuella öppna rapporten till standardvärdet |
| | Exportera den aktuella rapporten som en .csv-fil |
| | Regenerera data och ladda om den aktuella rapporten |

Du hittar en lista över alla standardrapporter på nästa sida.

# Rapporter om efterlevnad

## Förankrade enheter

Översikt över de enheter som har rotats/jailbreakats.

Standardkolumner för denna rapport:

| |
|---|
| Alias för enhet |
| Ägare av enheten |
| E-post |
| Operativsystem |
| Telefonnummer |
| Senast sett |
| Tillverkare |

## Roaming-enheter

Översikt över alla enheter som roamar

Standardkolumner för denna rapport:

| |
|---|
| Alias för enhet |
| Ägare av enheten |
| E-post |
| Enhetstyp |
| Operativsystem |
| Telefonnummer |
| Senast sett |

## Roaming-aktiverade enheter

Översikt över alla enheter som har aktiverat roaming men som inte nödvändigtvis roamar för närvarande.

Standardkolumner för denna rapport:

| |
|---|
| Alias för enhet |
| Ägare av enheten |
| E-post |
| Enhetstyp |
| Operativsystem |
| Telefonnummer |
| Senast sett |

## Övervakade enheter

Översikt över alla enheter som övervakas i övervakat läge (endast iOS)

Standardkolumner för denna rapport:

| |
|---|
| Alias för enhet |
| Ägare av enheten |
| E-post |
| Enhetstyp |
| Senast sett |

## Inaktiva enheter

Översikt över alla enheter som inte har anslutit till servern under de senaste 7 dagarna

Standardkolumner för denna rapport:

| |
|---|
| Alias för enhet |
| Ägare av enheten |
| E-post |
| Enhetstyp |
| Operativsystem |
| Senast sett |

# Rapporter om enheter

## Enheter efter ägarförhållande

Här kan du se hur många enheter som för närvarande har distribuerats som företagsenheter (företagsenheter) och medarbetarenheter (privata enheter).

Standardkolumner för denna rapport:

| |
|---|
| Alias för enhet |
| Ägare av enheten |
| Enhetstyp |
| Ägande av enhet |
| Operativsystem |

## Alla enheter

Här kan du se en översikt över alla enheter med den viktigaste informationen.

Standardkolumner för denna rapport:

| |
|---|
| Alias för enhet |
| Enhetstyp |
| Inskriven |
| Ägande av enhet |
| Operativsystem |
| OS-version |
| Serienummer |
| Senast sett |
| Operatör/transportör |
| Tillverkare |

## Bärare av enheter

Här kan du se en översikt över operatören (mobilleverantören).

Standardkolumner för denna rapport:

| |
|---|
| Alias för enhet |
| Ägare av enheten |
| E-post |
| Operativsystem |
| OS-version |
| Operatör/transportör |

## SAFE-enheter

Här kan du se en översikt över vilka enheter som använder SAFE Version.

Eftersom översikten och/eller SAFE endast är tillgänglig för Samsung-enheter, ser du inte de vanliga flikarna under denna punkt.

Standardkolumner för denna rapport:

| |
|---|
| Alias för enhet |
| Ägare av enheten |
| E-post |
| Enhetstyp |
| Senast sett |
| SAFE-version |

## Windows BitLocker-enheter

Här kan du se en översikt över de Windows-enheter som använder BitLocker.

Standardkolumner för denna rapport:

| |
|---|
| Alias för enhet |
| Ägare av enheten |
| E-post |

| |
|---|
| BitLocker-tillstånd |

## App-rapporter

Här får du en mängd olika översikter när det gäller appar. I alla dessa rapporter kan du klicka på en post för att ytterligare se vilka versioner som är installerade på enheterna och hur ofta. I den här vyn kan du klicka på en specifik version igen för att se vilka enheter som har den specifika versionen installerad.

**Obs:** Det kan ta en viss tid innan systemet får aktuell information från enheten. Dessutom uppdateras inte rapporterna varje minut. Du kan behöva ha tålamod för att se den aktuella statusen om du precis har tilldelat en ny app eller version. Om du laddar om rapporten manuellt kommer den att visa de mest aktuella uppgifterna som finns tillgängliga

### Installerade appar

Här får du en översikt över alla installerade appar.

Standardkolumner för denna rapport:

| | |
|---|---|
| Namn | Namn på respektive app och/eller tjänst |
| Identifierare | Definitivt ID för app/tjänst |
| Totalt antal | Hur ofta den här appen/tjänsten har installerats på slutanvändarens enheter |

### Mest installerade appar

Här får du en överblick över de appar som har installerats mest.

Standardkolumner för denna rapport:

| | |
|---|---|
| Namn | Namn på respektive app och/eller tjänst |
| Identifierare | Definitivt ID för app/tjänst |
| Totalt antal | Hur ofta den här appen/tjänsten har installerats på slutanvändarens enheter |

## Obligatoriska appar

Här får du en översikt över obligatoriska (obligatoriskt nödvändiga) appar.

Standardkolumner för denna rapport:

| | |
|---|---|
| Namn | Namn på respektive app och/eller tjänst |
| Identifierare | Definitivt ID för app/tjänst |
| App-källa | Vilken AppStore är inblandad:<br>• Google PlayStore (Android)<br>• iTunes AppStore (iOS) |
| OS | Operativsystem |

## Svartlistade appar

Här får du en översikt över alla definierade svartlistade appar.

Standardkolumner för denna rapport:

| | |
|---|---|
| Namn | Namn på respektive app och/eller tjänst |
| Identifierare | Definitivt ID för app/tjänst |
| App-källa | Vilken AppStore är inblandad:<br>• Google PlayStore (Android)<br>• iTunes AppStore (iOS) |
| OS | Operativsystem |

# Användarrapporter

## Tariff

Här får du en översikt över dina användares telefonabonnemang och SIM-kort.

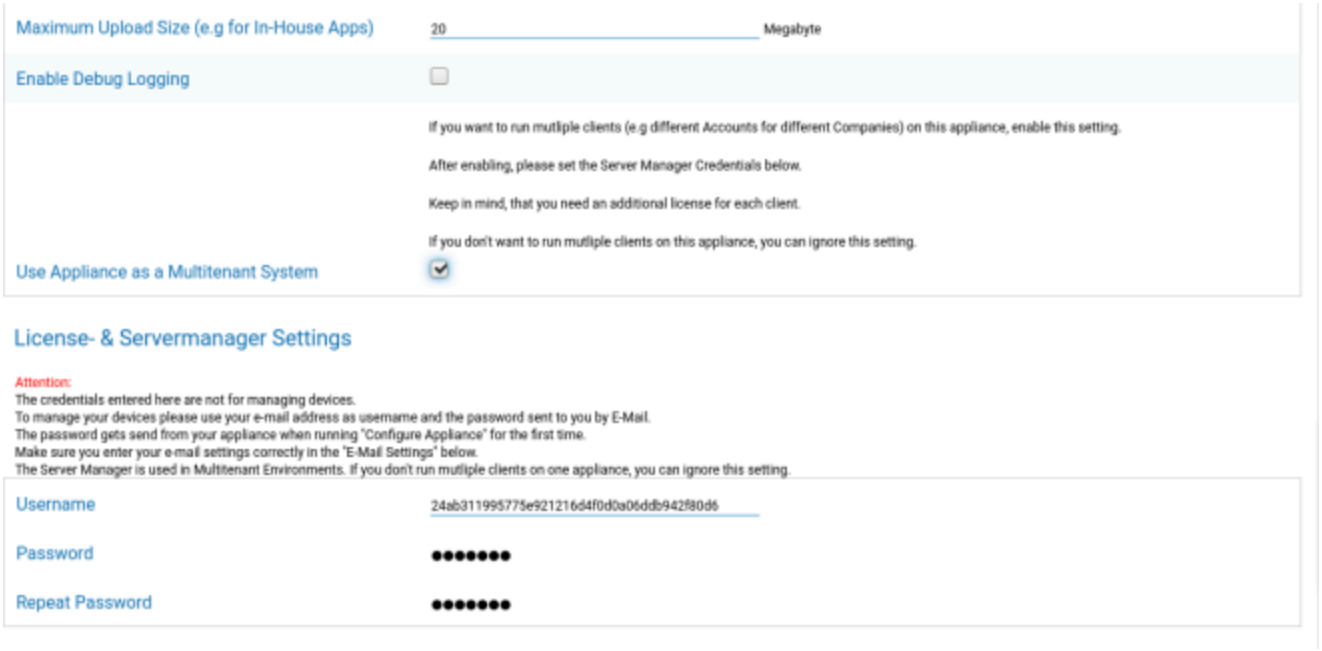
Standardkolumner för denna rapport:

| |
|---|
| E-post |
| Namn |
| telefonNummer |
| transportör |
| tariff |
| alternativ |
| pris |
| avtalAvbrutet |
| kontraktStart |
| underTid |
| mobilAndData |
| dataVolym |
| multiSIM |
| typ |
| simCardSerial1 |
| simCardSerial2 |
| simCardSerial3 |
| stift 1 |
| pin2 |
| puk1 |
| puk2 |
| notera |

# Hantering av flera hyresgäster

AppTec360 EMM kan vara värd för flera separata hyresgäster, var och en med sina egna användare och grupper, behörigheter och globala inställningar.

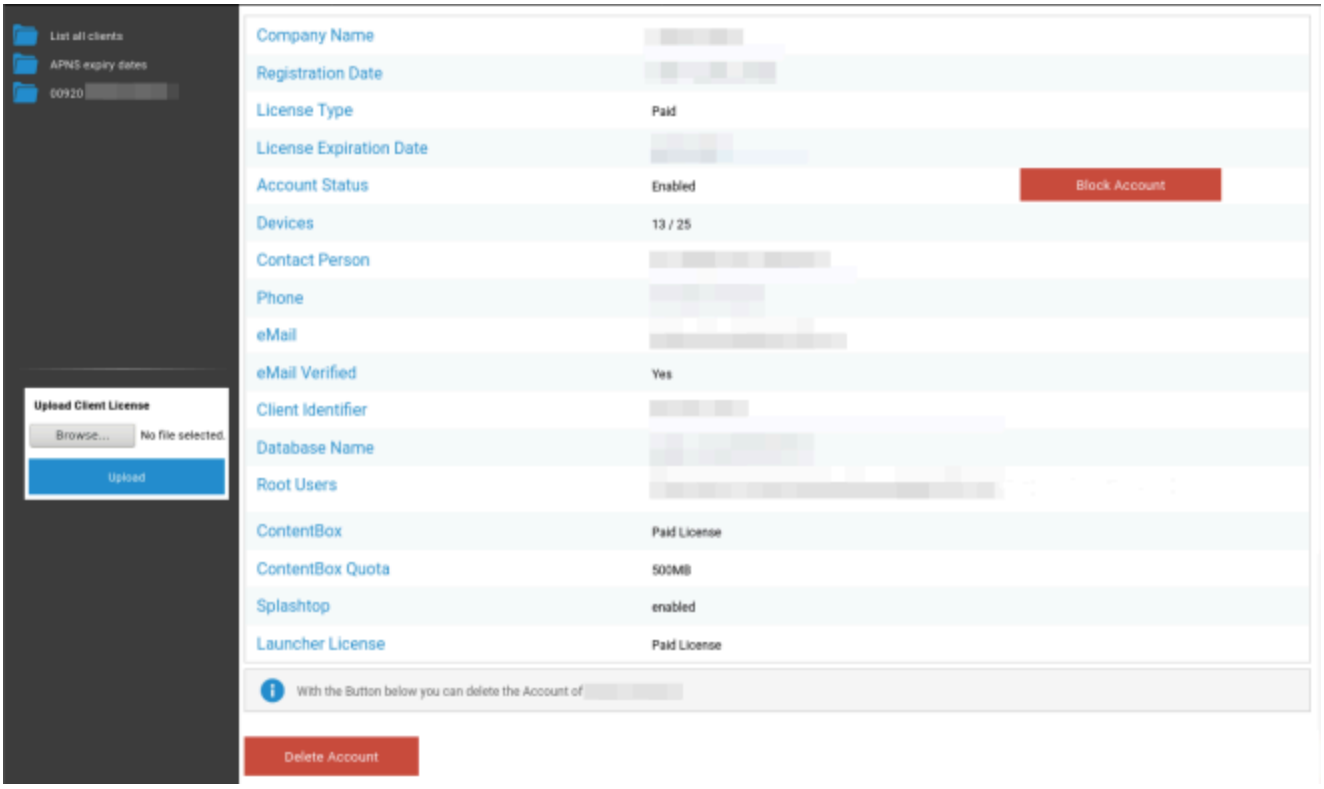
För att aktivera Multitenant-funktioner måste du aktivera det i konfigurationsgränssnittet för Appliance i "Steg tre - Serverinställningar".




I den nya menyn anger du ett användarnamn och ett lösenord för Servermanager. Spara inställningarna och kör "Configure Appliance" i "Steg fem - Licensavtal" för att tillämpa inställningen.

När konfigurationen är klar kan du nu logga in med de angivna inloggningsuppgifterna via det vanliga Mobile Management-gränssnittet.

Efter inloggning kan du se följande vy.




Till vänster kan du se alla hyresgäster (i det här fallet endast en med id 920) och till höger informationen om den här klienten. Du har också möjlighet att blockera åtkomst till kontot samt att radera klienten (OBS: Detta kommer att ta bort all data som är relaterad till den klienten).

Till vänster kan du ladda upp en ny klientlicens, som antingen kan vara en licensuppdatering för en befintlig klient eller en ny licens som automatiskt skapar en ny klient. När en ny klient skapas skickas ett e-postmeddelande med inloggningslösenordet automatiskt till den e-postadress som licensen utfärdades för.

För att få en ny eller uppdaterad klientlicens (t.ex. vid behov av fler enhetslicenser), kontakta din försäljningsrepresentant.

# Ytterligare vyer

## Lista alla kunder

Visar en översikt över alla klienter i systemet.

| | |
|---|---|
| Klient-ID | Klient-ID |
| Identifierare | Kundidentifierare |
| Databas | Databas |
| Företagets namn | Företagets namn |
| E-post | Kontaktperson eMail |
| Verifierad | Om kontaktpersonens eMail är verifierat eller inte |
| Land | Land |
| Apparater | Antal registrerade enheter |
| Registreringsdatum | Tidpunkt för licenstilldelningen |
| Senaste inloggning | Senaste inloggning för administratörskonto |
| Licens | Visning av licenstyp (gratis\|betald) |
| CB-licens | ContentBox licenstyp (gratis\|betald) |
| Status | Aktuell status för AppTec-klient |
| Utgått | Visas om licensen har löpt ut |
| iOS | Antal iOS-enheter |
| Android | Antal Android-enheter |
| Windows Mobile | Antal Windows Mobile-enheter |
| MacOS | Antal MacOS-enheter |
| Windows 10 | Antal Windows 10-enheter |
| Android Företag | Antal Android-enheter för företag |
| IOS BYOD (registrering av användare) | Antal IOS BYOD-enheter (användarregistrering) |
| IoT | Antal IoT-enheter |

## APNS utgångsdatum

Visar en översikt över alla utgångsdatum för APNS-certifikat för alla klienter.

| | |
|---|---|
| Klient-ID | Klient-ID |
| Företagets namn | Företagets namn |
| Utgångsdatum | Utgångsdatum för Apple APNS-certifikatet |
| Information | Information om utgångsdatum |

# Kontakt

Ytterligare frågor? Kontakta oss helt enkelt under:

## För allmänna tekniska frågor

support@apptec360.com

+41 61 511 3210

## För frågor som rör installation av en virtuell appliance

consulting@apptec360.com

+41 61 511 3214

# Ansvarsfriskrivning