AppTec360 Enterprise Mobile Manager & ContentBox

Administratiehandleiding | Versie 5.0 (202110)

Inhoudsopgave

- SecurePIM Beveiliging
- VeiligePIM-browser
- Uitwisseling

Verbindingsbeheer

- Wi-Fi
  - Proxy-instelling
  - Type beveiliging
- VPN
  - VPN-type
    - VPN
    - VPN per app
  - Proxy-instelling
- APN
- Cellulair
- HTTP-proxy
- AirPrint
- AirPlay

PIM-beheer

- Exchange Actieve Synchronisatie
- e-mail
  - Inkomende post
  - Uitgaande post
- CalDav
- Geabonneerde kalenders
- LDAP

Webbeheer

- Webclips
- Filter voor webinhoud

App-beheer

- Enterprise App Manager
  - Geïnstalleerde apps (alleen op apparaatniveau)
  - Verplichte apps
    - Installatie-opties
  - Webtoepassingen

- Beperkingen en instellingen
  - Apps op zwarte lijst / witte lijst
  - SysApp-beperkingen
  - App-VPN
  - App-instellingen
- App Store voor ondernemingen
  - iTunes-apps
  - Intern
- Kioskmodus
  - Type toepassing
    - Pakket
    - URL
  - Instellingen Kioskmodus

Android Enterprise – Apparaatconfiguratie volledig beheerd

Algemeen

- Overzicht groepsprofiel (alleen op groepsniveau)
- Apparaatoverzicht (alleen op apparaatniveau)
- Configuratie Revisie (alleen op apparaatniveau)
- Apparaatlogboek (alleen op apparaatniveau)
  - Opdrachtlogboek
  - Mogelijke opdrachtstatussen
- Apparaatinstellingen
  - Configuratie klant
  - Behang

Activabeheer (alleen op apparaatniveau)

- Apparaat info
  - Wi-Fi
- Cellulair
- Bluetooth

Beveiligingsbeheer

- Anti diefstal (alleen op apparaatniveau)
  - GPS-informatie (alleen op apparaatniveau)
  - Vegen en vergrendelen (alleen op apparaatniveau)
  - Bericht (alleen op apparaatniveau)

- Beveiligingsconfiguratie
  - Toestelwachtwoord
  - AntiVirus
- Einde levensduur (alleen op apparaatniveau)
  - Vegen (alleen op apparaatniveau)
- Beperkende instellingen
  - Beperkingen
- Beheer van certificaten

Verbindingsbeheer

- Wifi
  - Type beveiliging
    - WEP
    - WPA/WPA2
    - 802.1x EAP
- VPN
  - VPN-type
    - VPN
    - VPN per app
- Beperkingen

PIM-beheer

- Gmail Uitwisseling

App-beheer

- Enterprise App Manager
  - Geïnstalleerde apps (alleen op apparaatniveau)
  - Systeemapps (alleen op apparaatniveau)
  - Verplichte apps
  - Zwarte lijsten en witte lijsten
  - AE-systeemapps
- Beperkingen en instellingen
  - App Beheer Instellingen
- App Store voor ondernemingen
  - Intern
- Play Store voor bedrijven
  - AE Play Store
- Kioskmodus & Launcher

- Behang

Activabeheer (alleen op apparaatniveau)

- Apparaat info
  - Wi-Fi
- Cellulair
- Bluetooth

Beveiligingsbeheer

- Anti diefstal (alleen op apparaatniveau)
  - GPS-informatie (alleen op apparaatniveau)
  - Vegen en vergrendelen (alleen op apparaatniveau)
  - Bericht (alleen op apparaatniveau)
- Beveiligingsconfiguratie
  - Toestelwachtwoord
  - Container Wachtwoord
  - AntiVirus
- Einde levensduur (alleen op apparaatniveau)
  - Vegen (alleen op apparaatniveau)
- Beperkende instellingen
  - Beperkingen
- Beheer van certificaten

Verbindingsbeheer

- Wifi
  - Type beveiliging
    - WEP
    - WPA/WPA2
    - 802.1x EAP
- VPN
  - VPN-type
    - VPN
    - VPN per app
- Beperkingen

PIM-beheer

- Gmail Uitwisseling

App-beheer

- Enterprise App Manager

- Bericht (alleen op apparaatniveau)
- Beveiligingsconfiguratie
  - Wachtwoord
  - Encryptie
  - AntiVirus
- Einde levensduur (alleen op apparaatniveau)
  - Vegen (alleen op apparaatniveau)
- Beperkende instellingen
  - Beperkingen
  - AE Apparaateigenaar

BYOD-container

- Android Onderneming
  - Android Onderneming
  - Gmail Uitwisseling
  - AE-systeemapps
  - Container Wachtwoord
- Samsung KNOX
  - Activering
  - Knox-toegangscode
  - Knox Beveiliging
  - Knox Uitwisseling
  - Knox e-mail
  - Knox-apps

Verbindingsbeheer

- Wifi
  - Type beveiliging
    - WEP
    - WPA/WPA2
    - 802.1x EAP
- VPN
- Beperkingen
- APN
- Bluetooth

PIM-beheer

- Uitwisseling

- e-mail
- AE Gmail Uitwisseling

App-beheer

- Enterprise App Manager
  - Geïnstalleerde apps (alleen op apparaatniveau)
  - Systeemapps (alleen op apparaatniveau)
  - Verplichte apps
  - AE-systeemapps
- Beperkingen en instellingen
  - Zwarte lijsten en witte lijsten
  - Beperkingen voor systeemtoepassingen
    - Samsung-apps
    - Huawei Apps
  - App Beheer Instellingen
- App Store voor ondernemingen
  - Playstore
  - Intern
- Play Store voor bedrijven
- Kioskmodus & Launcher
  - Kioskmodus
  - AppTec360 Launcher
  - AppTec360-instellingen

Afstandsbediening

- Splashtop
- Teamviewer

Beheer van inhoud

- Inhoudsvak
- Veilige browser

Configuratie Windows 10 PC

Algemeen

- Overzicht groepsprofiel (alleen op groepsniveau)
- Apparaatoverzicht (alleen op apparaatniveau)
- Instellingen
- Configuratie Revisie (alleen op apparaatniveau)

- Exchange Actieve Synchronisatie
- e-mail
- App-beheer
  - Enterprise App Manager
    - Geïnstalleerde apps
    - Verplichte apps
    - Beperkingen voor systeemtoepassingen
    - Zwarte lijsten en witte lijsten

MacOS-configuratie

Algemeen

- Overzicht groepsprofiel (alleen op groepsniveau)
- Apparaatoverzicht (alleen op apparaatniveau)
- Configuratie Revisie (alleen op apparaatniveau)
- Apparaatlogboek (alleen op apparaatniveau)
  - Opdrachtlogboek
  - Mogelijke opdrachtstatussen

Activabeheer (alleen op apparaatniveau)

- Apparaat info
- WiFi
- Cellulair
- Bluetooth

Updatebeheer (alleen op apparaatniveau)

- Info bijwerken

Beveiligingsbeheer

- Anti diefstal
  - Vegen en vergrendelen
- Beveiligingsconfiguratie
  - Wachtwoord
  - Certificaat
- Beperkende instellingen
  - Functionaliteit van het apparaat
  - iCloud
  - Mediabeheer

Verbindingsbeheer

Algemeen overzicht

Inleiding tot AppTec360

AppTec's Enterprise-Mobile-Management-Solution biedt de mogelijkheid om alle mobiele apparaten te beheren en configureren met de intuïtieve beheerconsole. In dit scenario kan de EMM-server in je eigen omgeving draaien of je kunt gebruik maken van onze cloudgebaseerde oplossing.

Zelfs voor een centrale installatie van bedrijfsapplicaties op smartphones ben je hier aan het juiste adres. Met Enterprise Mobile Manager kunt u binnen enkele seconden bedrijfstoepassingen en -documenten distribueren naar apparaten of ongewenste toepassingen blokkeren met white/blacklisting.

Het gebruik van privéapparaten in bedrijven vormt een nieuwe uitdaging voor de beveiliging van smartphones en tablets. Omdat werknemers hun smartphones steeds vaker willen gebruiken, moeten IT-beheerders een groot aantal verschillende soorten apparaten beschermen. We helpen je bij het beveiligen van alle apparaten en de gevoelige gegevens die erop zijn opgeslagen en beheren ze vanuit een intuïtieve console.

Ondersteunde besturingssystemen voor apparaten

AppTec360 biedt ondersteuning voor iOS-, Android- en Windows-apparaten. Houd er rekening mee dat de functiecapaciteit van de genoemde platformen per besturingssysteem kan verschillen.

- Apple iOS 11.0 of hoger*
- Apple macOS 10.11 of hoger
- Google Android 4.4 of hoger** op de cloudversie
- Google Android 4.1 of hoger** op de OnPrem-versie
- MS Windows 10 of hoger*** (desktopcomputer, notebook en tablet)

**Houd er rekening mee dat apparaten met iOS 10 of eerder niet kunnen worden geregistreerd vanwege drastische wijzigingen die Apple heeft aangebracht in het registratieproces.*

***Apparaten kunnen worden aangesloten en geconfigureerd, zelfs als ze een versie gebruiken die niet langer wordt ondersteund door de fabrikant. Houd er rekening mee dat er functies kunnen zijn waarvoor een bepaalde Android-versie vereist is. In ondersteuningsgevallen volgen we de officiële ondersteuning van de fabrikant. In het geval van problemen of bugs die worden veroorzaakt door een verouderde versie die niet langer wordt ondersteund door de fabrikant, behouden we ons het recht voor om slechts beperkte ondersteuning te bieden.*

****De thuisversie van Windows wordt niet ondersteund vanwege beperkingen van het besturingssysteem. We raden ten zeerste aan om een OS-versie te gebruiken die nog steeds wordt ondersteund door de fabrikant. Niet alleen voor compatibiliteit, maar ook om veiligheidsredenen. Daarom raden we iOS 12 of hoger en Android 9 of hoger aan.*

Ondersteunde LDAP-directory’s

- Microsoft Active Directory
- LDAP openen

Actuele informatie over "Ondersteunde besturingssystemen voor apparaten" en "Ondersteunde LDAP-directory's" vindt u hier:

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

Uitleg van de “bewaakte modus” op Apple apparaten

De bewaakte modus vertegenwoordigt een uitgebreide interface voor iOS-apparaten.

Op het respectievelijk geconfigureerde apparaat kunnen aanvullende beperkingen worden toegepast die betrekking hebben op de functionaliteit van het eindgebruikersapparaat. Deze staan ook in het administratiehandboek en zijn gemarkeerd met een banner.

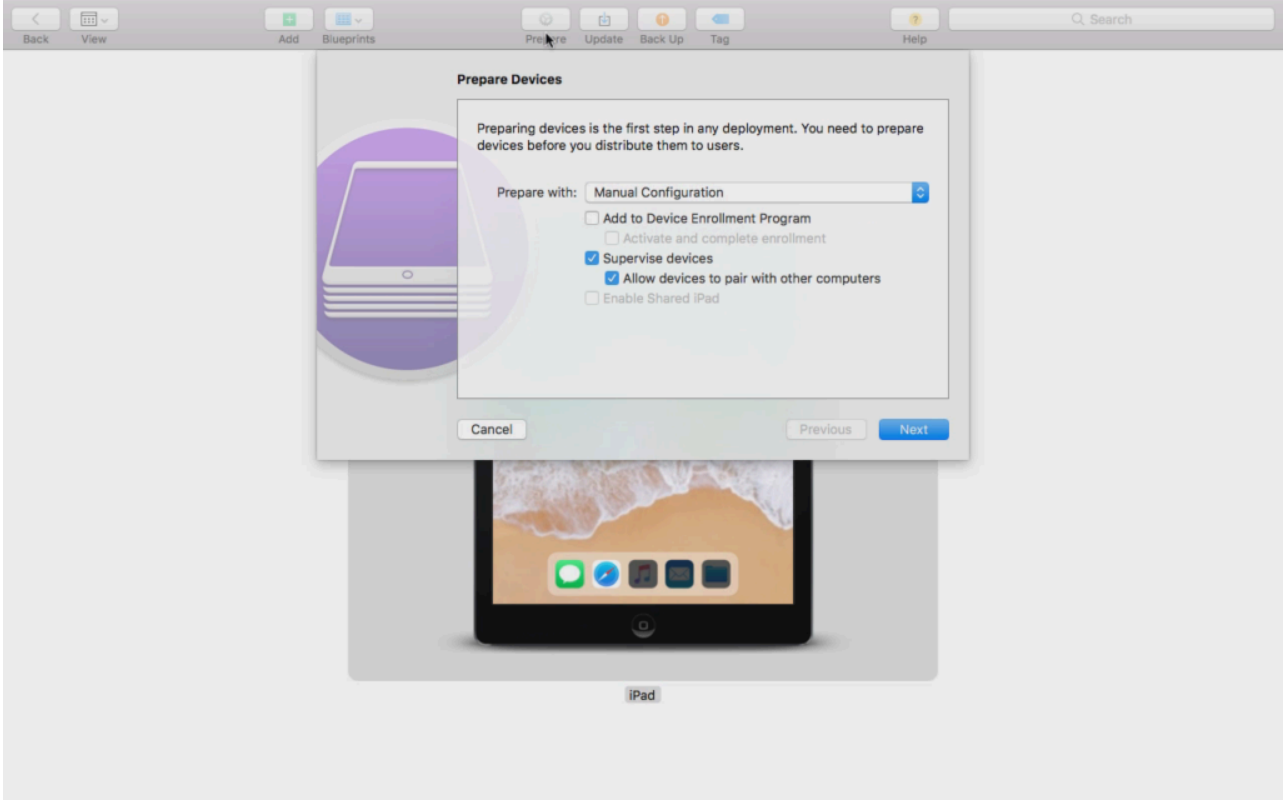
Beschikbaar in de bewaakte modus

De "bewaakte modus" kan worden geactiveerd met het programma "Apple Configurator". De Apple Configurator kan de standaardinstellingen op nieuwe iOS-apparaten instellen als configuratietool (via de USB-interface).

De tool kan niet alleen configuratieprofielen installeren, maar ook apps. Het is gratis, maar je hebt wel een Mac-computer nodig.

De bewaakte modus activeren

1. Open de Apple Configurator



2. Klik op het apparaat en kies "Prepare".
3. Kies "Handmatige configuratie" en "Apparaten bewaken".
4. Klik op "Volgende".
5. (Optioneel) Nu kun je een MDM-server toevoegen waar het apparaat zal worden geregistreerd. De link hiervoor kun je vinden onder "Algemene instellingen - iOS Configuratie - Configurator & URL" Kies je organisatie of maak een nieuwe aan
6. Kies uw organisatie of maak een nieuwe aan
7. Kies welke stappen moeten worden overgeslagen bij de eerste installatie en klik op "Volgende" (LET OP: Als u doorgaat, wordt uw apparaat verwijderd!)

Nu wordt je apparaat in de bewaakte modus gezet. Dit kan enkele minuten duren. Nadat dit is gebeurd, start het apparaat opnieuw op.

Nu staat je apparaat onder toezicht!

Een apparaat toevoegen aan de DEP

Je kunt ook apparaten toevoegen aan het DEP (Device Enrollment Programm) via de Apple Configurator, als je apparaten iOS 11 of hoger hebben.

Meer informatie over DEP: https://www.apple.com/business/dep/

Volg dezelfde stappen als bij het toezicht houden op een apparaat en vink ook "Add to Device Enrollment Programm" aan. U wordt om uw DEP-logingegevens gevraagd als u zich nooit eerder bij DEP hebt aangemeld met de Apple Configurator.

Nadat het proces is voltooid, is het apparaat te vinden in de DEP-server "Devices Added by Apple Configurator 2". U kunt deze server nu gebruiken en verbinden met de beheerconsole of het apparaat overbrengen naar een reeds bestaande server.

U hebt nu met succes een apparaat toegevoegd aan de DEP!

Uitleg van Android Enterprise

Wat is Android Enterprise?

Android Enterprise biedt een betere controle over werkapparaten die worden beheerd met een MDM. Hierdoor kunnen beheerders ofwel volledige controle hebben over hun Android-apparaten of de bedrijfsgegevens scheiden van privégegevens op containerapparaten. Bovendien maakt Android Enterprise een eenvoudigere registratie van de apparaten en een eenvoudige app-distributie mogelijk.

Wat zijn de vereisten om Android Enterprise te gebruiken?

Android Enterprise kan door iedereen gratis worden gebruikt. Je hoeft alleen een Google-account te koppelen aan de MDM om alle Android Enterprise-functies in te schakelen. Meer hierover kun je vinden in de Android Enterprise sectie.

Android Enterprise kan worden gebruikt op toestellen met Android 5.1 of hoger, met uitzondering van Enhanced Work Profile (zie hieronder). We raden ten minste Android 7 of hoger aan voor een eenvoudigere inschrijving of Android 11 om gebruik te maken van alle beschikbare functies.

Wat zijn de beschikbare modi met Android Enterprise?

Er zijn 3 verschillende modi die je kunt gebruiken als je Android Enterprise gebruikt.

AE Volledig beheerd apparaat (Work Managed): Een volledig beheerd apparaat dat alleen voor het werk wordt gebruikt. De beheerder heeft volledige controle over het apparaat. Privégebruik van het apparaat is niet mogelijk. Om apparaten in deze modus te registreren, moeten apparaten worden gereset en geregistreerd met een QR Code (zie AE Enrollment) of geregistreerd via Knox Enrollment of Zero Touch.

AE BYOD-container: Met de BYOD-container (bring your own device) hebben gebruikers toegang tot bedrijfsgegevens op hun privételefoon in een aparte container. In deze modus kunnen privé-apps geen bedrijfsgegevens en -apps zien en vice versa. Om apparaten in deze modus te registreren, moet de AppTec app worden gedownload en kan een QR-code worden gescand. Maak een apparaat aan in de console en selecteer "AE Container (BYOD & Enahnced Work Profile)" als apparaattype. Klik op de QR Code op het nieuw aangemaakte apparaat om de QR Code te krijgen en stel de eerste schakelaar in op "Legacy & BYOD".

AE Enhanced Work Profile: (vereist Android 11 of hoger) Terwijl de hierboven genoemde BYOD-container bedrijfsgegevens op een privéapparaat plaatst, doet het Enhanced Work Profile hetzelfde, maar dan voor een apparaat dat eigendom is van het bedrijf. Het creëert dezelfde container, maar geeft de beheerder iets meer controle over het apparaat, zodat de gebruiker niet zomaar de MDM van het apparaat kan verwijderen. Maak een apparaat aan in de console en selecteer "AE Container

(BYOD & Enahnced Work Profile)" als apparaattype. Klik op de QR Code op het nieuw aangemaakte apparaat om de QR Code te krijgen en zet de eerste schakelaar op "Enhanced Work Profile". Deze QR Code kan gescand worden na het resetten van het apparaat en 6 keer tikken op het scherm zoals uitgelegd in Methode 1 in AE Enrollment.

Hoe kan ik apps toewijzen aan Android Enterprise-apparaten?

Eerst moet u de apps die u wilt gebruiken goedkeuren in Algemene instellingen → Appbeheer → AE Play Store → Play Store Apps. Na het goedkeuren van een app kunt u deze toevoegen aan de verplichte app-lijst → van uw profiel door op de "+" te klikken en de app te selecteren op het tabblad "AE Play Store". De app wordt dan automatisch gedownload en geïnstalleerd. Er is geen Google-account op het apparaat vereist en de gebruiker hoeft dit niet te bevestigen of toe te staan.

Uw eigen apps uploaden naar de Google Play Store

Het is mogelijk om je Inhouse Apps te uploaden naar de Google Play Store. Op deze manier kunt u profiteren van verschillende voordelen, zoals het updatemechanisme van de Play Store.

Hiervoor heb je een Google Developer Account nodig. Log in via de Google Play Console(https://play.google.com/apps/publish).

Klik op "Applicatie maken". Kies je standaardtaal en de titel van de app.

Create application

Default language *

English (United Kingdom) – en-GB ▾

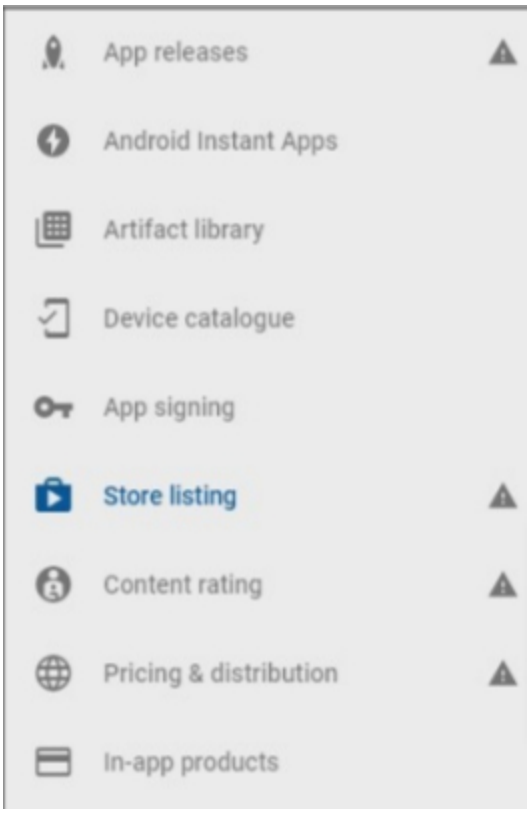
Title *

AppTec Demo App

15/50

CANCEL CREATE

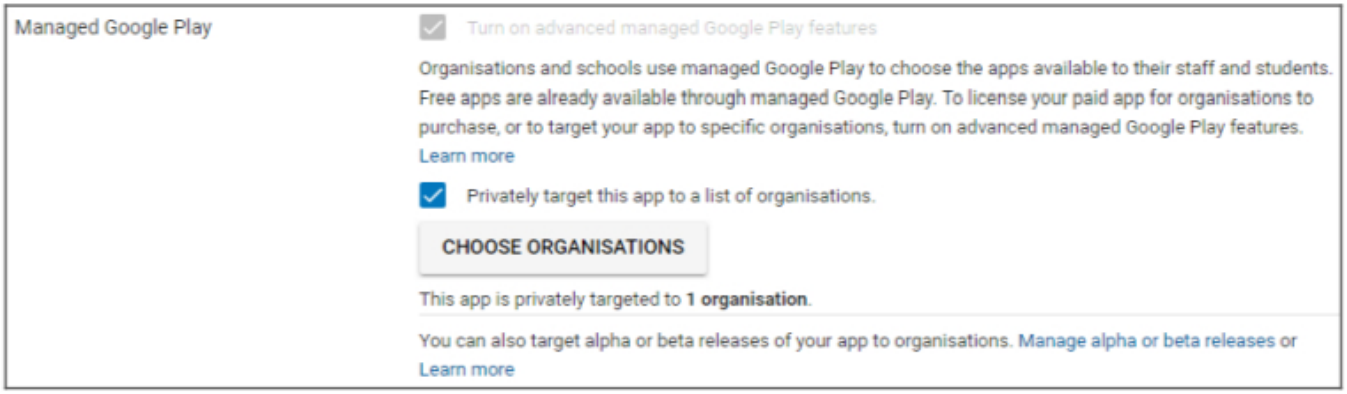
Op de volgende pagina wordt je gevraagd om verschillende details over je app in te voeren.



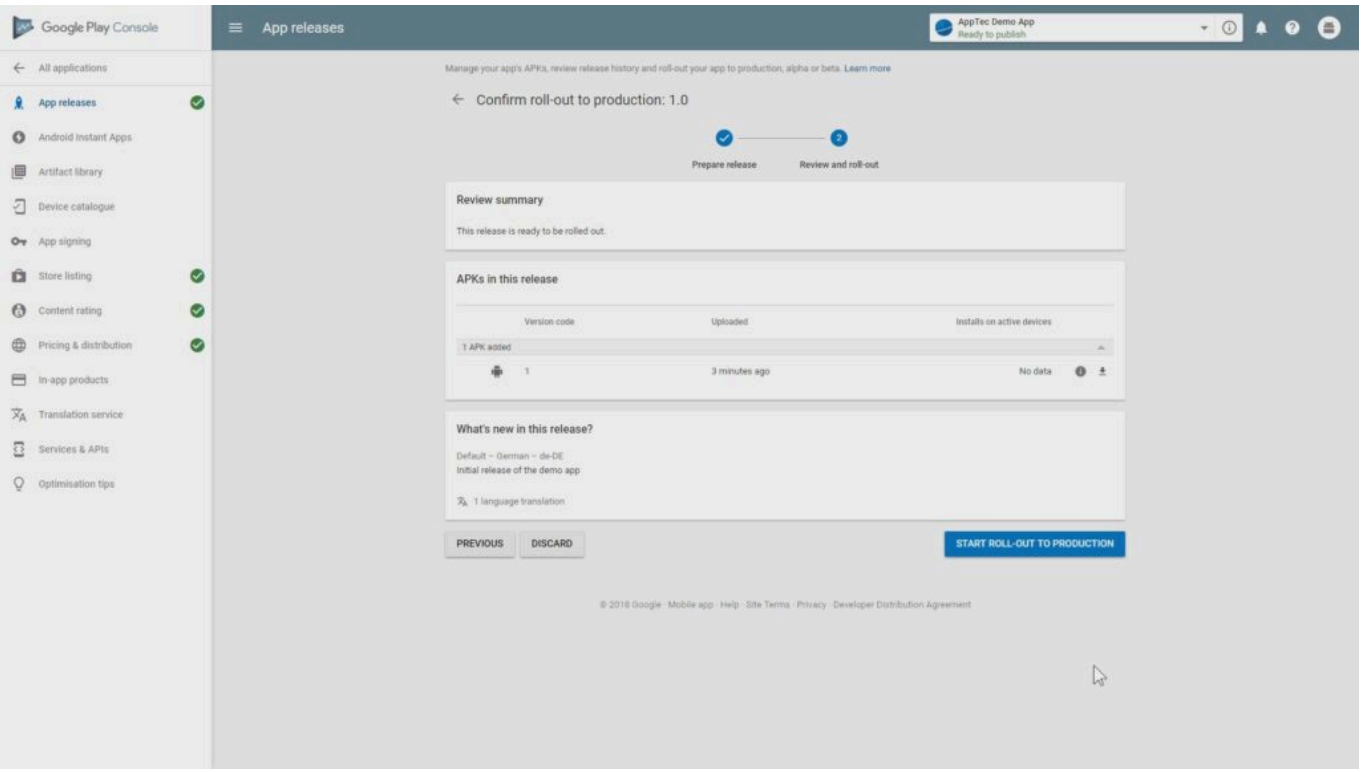
Nadat je alle gegevens hebt ingevoerd, zie je aan de linkerkant verschillende hintsymbolen.

Beweeg erover om te zien welke stappen er nog over zijn en volg deze in elke gewenste volgorde.

Opmerking: Zorg ervoor dat je de twee selectievakjes aanvinkt bij "Google Play beheren" onder "Prijzen & distributie". Anders is de app openbaar en voor iedereen toegankelijk. Zorg er ook voor dat je het land voor distributie kiest.



Nadat je alle stappen hebt voltooid, kun je naar "App releases" gaan. Klik op "Review" en "Start Roll-Out to Production" om je concept af te ronden en de app te publiceren.



Het kan even duren voordat de app beschikbaar is in de Play Store. Nadat het proces is voltooid, kun je je app zoeken in de Play for Work-winkel en goedkeuren. Daarna kun je de app eenvoudig toewijzen aan apparaten via de EMM-console, net zoals je dat met andere apps doet.

Vereisten en installatie

Vereisten

Systeemvereisten

Het virtuele apparaat is beschikbaar in het Open Virtualization Format (VMWare, VirtualBox, Citrix Xen Server) en als gecomprimeerd .vhdx (Hyper-V) bestand*.

*Note: De machine moet worden gemaakt met Generatie 1 als Hyper-V wordt gebruikt.

De virtuele schijf heeft een doelgrootte van 20 GB en de machine heeft 4 GB RAM nodig.

Het apparaat is gebaseerd op Debian 9 64bit

Upgrade de geïmporteerde machine naar de nieuwste compatibiliteit (bijvoorbeeld in VMWare) en zorg ervoor dat het OS-type van de machine correct is ingesteld in je hypervisor.

Licentiesleutel

Om de server succesvol te activeren en installeren, heb je een geldig licentiebestand nodig. Deze kun je rechtstreeks bij AppTec360 en/of bij je reseller verkrijgen.

IP-adres en DNS-resolutie

De AppTec360-appliance moet bereikbaar zijn via het apparaat met de hostnaam waarvoor de licentie is uitgegeven.

Om Windows 10-apparaten in te schrijven moet je ook een extra subdomein instellen in de vorm van "enterpriseenrollment.", dat naar het apparaat wijst.

SSL-certificaat

Omdat alle verbindingen van en naar de apparaten beveiligd moeten worden met SSL, heb je een geldig certificaat nodig voor de hostnaam, uitgegeven door een certificaatautoriteit die door het apparaat wordt vertrouwd. De privésleutel voor het certificaat moet worden geüpload zonder wachtwoordbeveiliging. In de meeste gevallen is een tussenliggend certificaat voor de CA nodig om de apparaten het servercertificaat te laten herkennen.

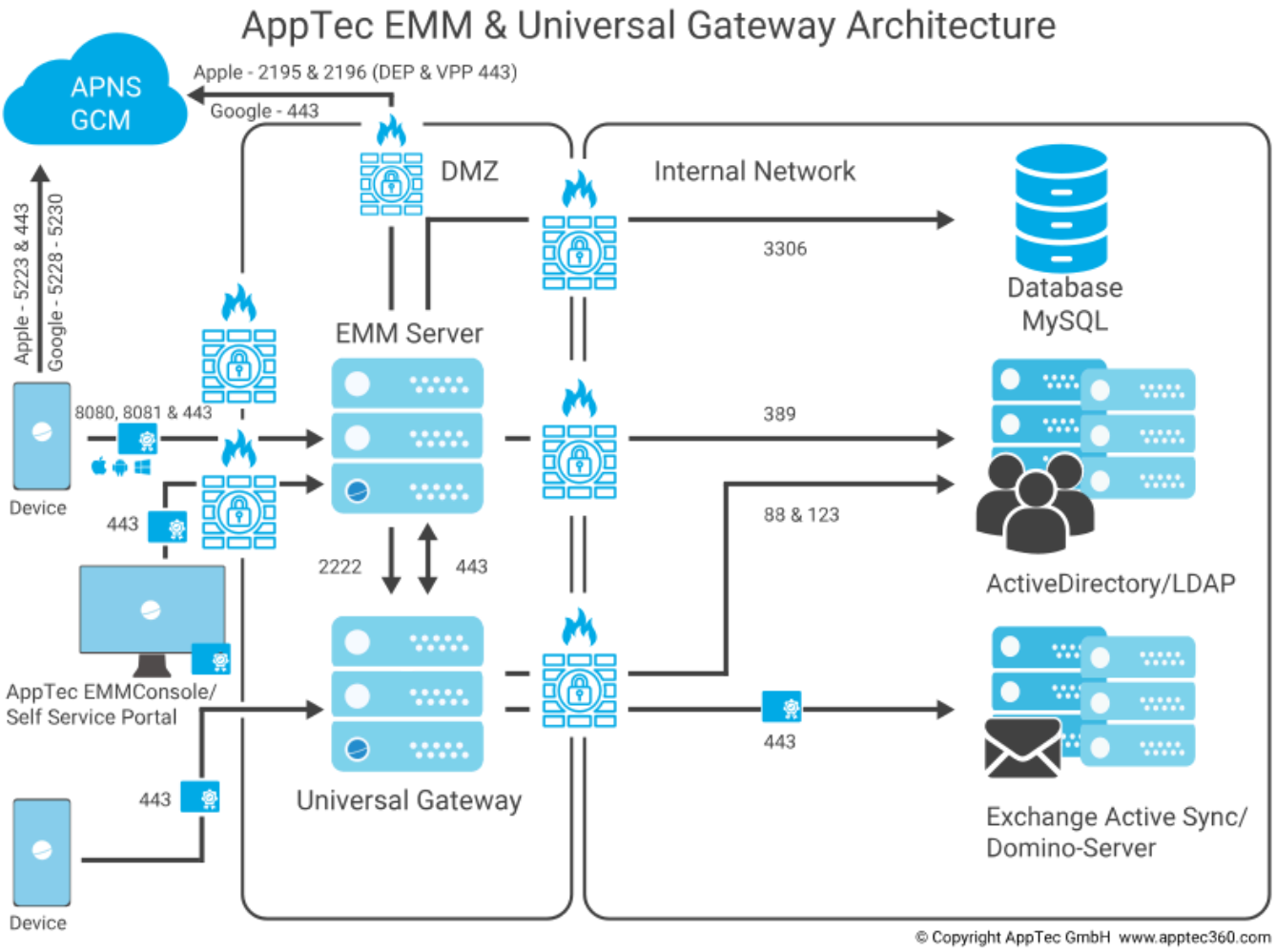
Windows 10-apparaten hebben een specifiek certificaat nodig voor je subdomein voor enterprise-registratie.

Vanaf versie 202104 kunt u ook Let's Encrypt-certificaten gebruiken, die automatisch worden gegenereerd (beschreven in Stap Twee - SSL-certificaat).

SMTP-server

Er is een e-mailserver en/of een e-mailrelay nodig om de AppTec360 EMM e-mails te laten versturen (bijvoorbeeld voor apparaatregistratie en accountvalidatie).

Firewall-regels



Dit diagram laat zien welke verbinding nodig is, afhankelijk van de services die je wilt gebruiken.

Zie de tabel op de volgende pagina voor een meer gedetailleerde beschrijving.

Alle (extern/apparaten)	→	**AppTec360-toestel / emmconsole.com**
Poorten	443	Beheer, Enterprise AppStore & Windows Phone Communicatie
	8080	Android- en iOS-communicatie
	80	Eerste installatie van Let´s Encrypt. Gebruikt daarna 443.
Alle (apparaten)	→	**Om het even welk (extern)**
Poorten	5223, 443	Apple Push Service, moet bereikbaar zijn zonder proxy, 443 als Fallback, zie https://support.apple.com/en-us/HT203609
	5228-5230	Android Push Service (FCM), moet bereikbaar zijn zonder proxy
AppTec360 Toestel	→	**Domeincontroller**
Poorten	389, (LDAPS 636)	Gebruikerssynchronisatie met LDAP
AppTec360 Toestel	→	**Elke**
Haven	443	Gebruikt voor de Android Push Service (GCM) Zoeken in AppStore / Play Store
AppTec360 Toestel	→	**emmconsole.com**
Poorten	443	AppTec360 Appliance Updates, APNS-certificaat genereren
AppTec360 Toestel	→	**Apple netwerk (17.0.0.0/8)**
Poorten	2195, 2196	Apple Push Service en feedbackservice
	443	DEP & VPP

Beveiligingsupdates

Het Debian besturingssysteem moet regelmatig worden bijgewerkt om de nieuwste beveiligingsoplossingen te krijgen. Zorg er echter voor dat je niet handmatig upgrade naar een nieuwere hoofdversie van Debian. Als AppTec360 EMM compatibel is met een nieuwere hoofdversie zullen we een manier toevoegen om te upgraden in een appliance update.

Standaard wachtwoorden van de Virtual Appliance

Login Gebruiker (Root login is uitgeschakeld. Gebruik "sudo" voor beheertaken)

apptec

Login Wachtwoord

apptec

MySQL root gebruiker

wortel

MySQL root wachtwoord

apptec

MySQL standaard gebruiker

AppTec

MySQL standaard gebruikerswachtwoord

AppTec

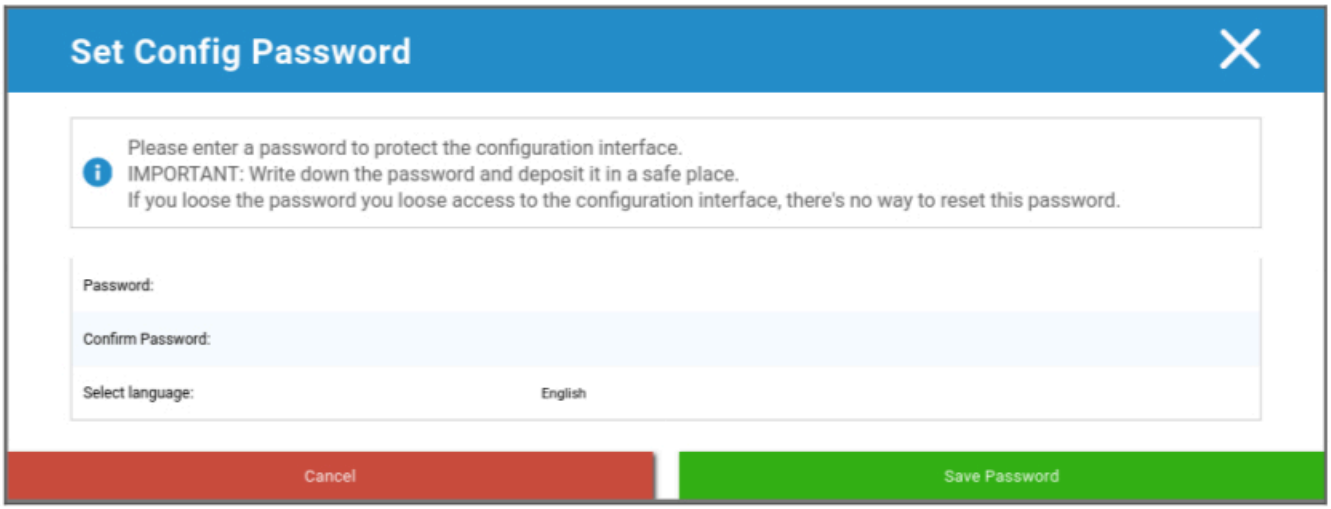
Configuratie van de Virtual Appliance

Belangrijk: Voordat je begint met de configuratie van de Virtual Appliance moet de beeldschermresolutie worden ingesteld op ten minste 1280 x 800 pixels.

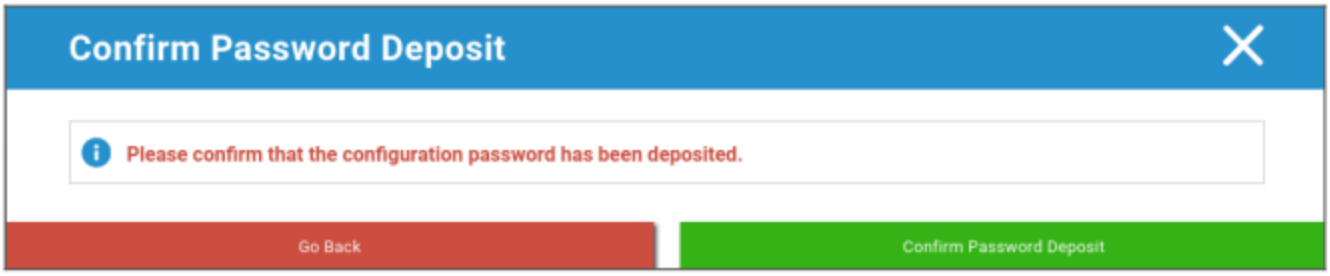
Na het inloggen op de Appliance moet Firefox automatisch opstarten en de configuratie-interface weergeven.

Voorbereiding

Eerst moet je een wachtwoord opgeven voor de configuratie-interface. Dit wachtwoord wordt gebruikt om alle informatie en bestanden te coderen die in de configuratie-interface worden ingevoerd. Hier kun je ook de taal instellen waarin de interface moet worden weergegeven (kan later worden gewijzigd).

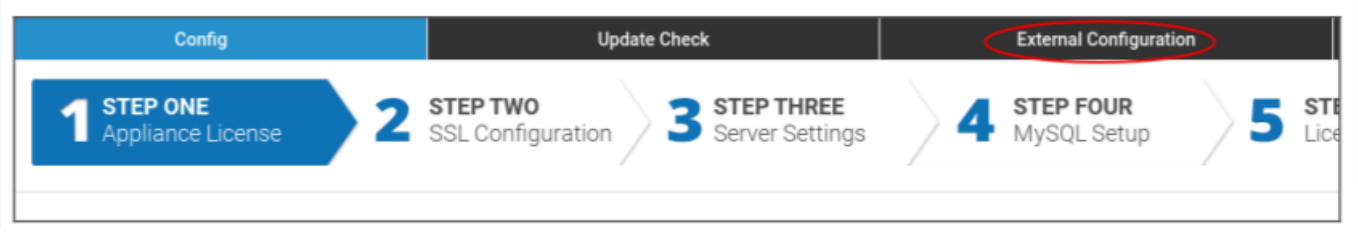


Het wachtwoord kan alleen worden gereset door AppTec360 Support, dus zorg ervoor dat je het op een veilige plaats opbergt en bevestig de popup die verschijnt.



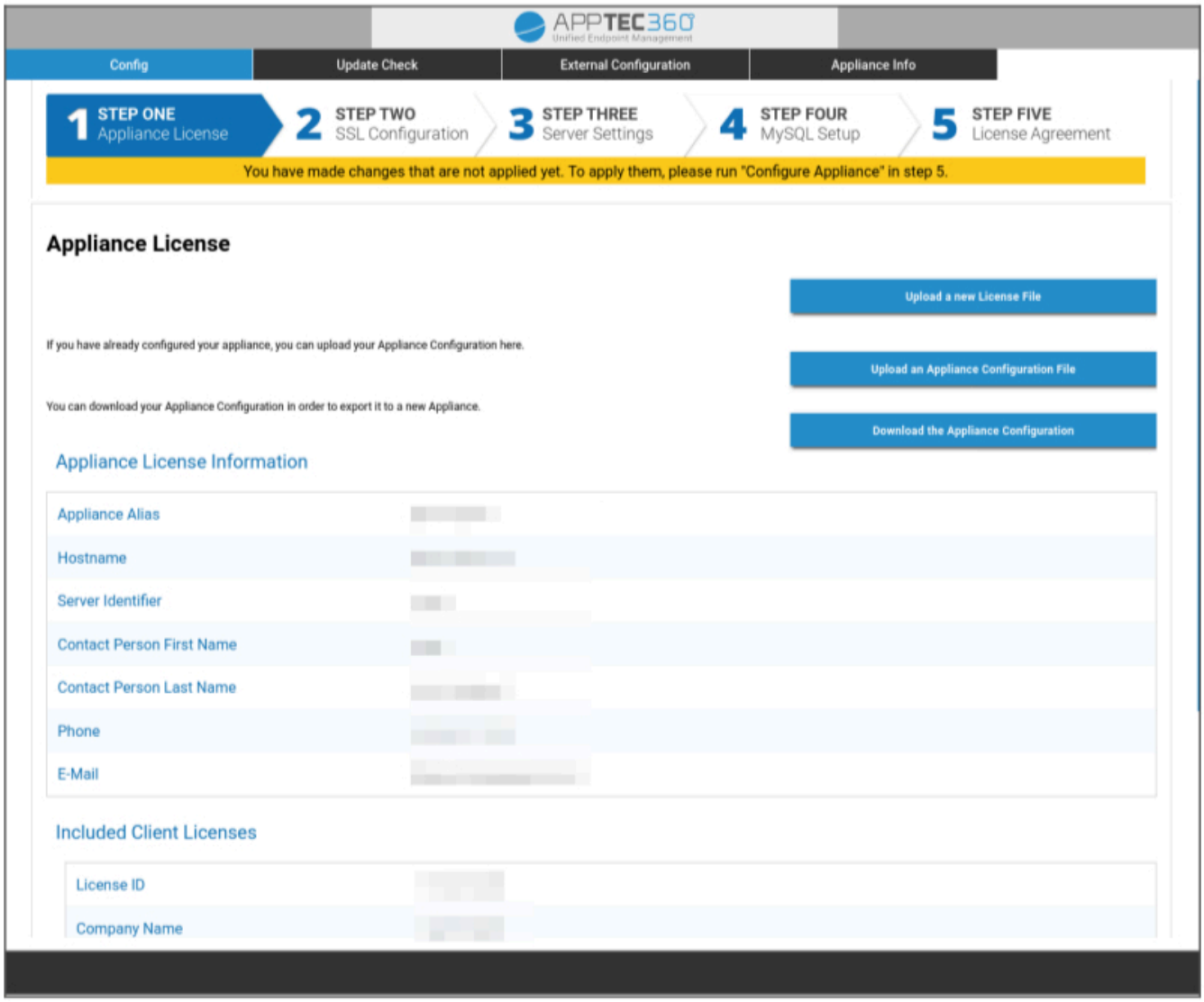
Configureren vanaf externe host

Om het installatieproces te vergemakkelijken, kun je de configuratiepagina toegankelijk maken vanaf een externe host. Volg hiervoor de stappen in "Configureren vanaf externe host".



Stap één – Toestellicentie

1. Upload het licentiebestand dat je van AppTec hebt ontvangen.
2. Als het licentiebestand succesvol is geüpload, kun je de licentie-informatie van het apparaat zien, zoals in de onderstaande schermafbeelding.



Stap Twee – SSL Certificaat

Je kunt de automatische certificaatinstelling met Let's Encrypt gebruiken of de certificaten zelf aanleveren (zie SSL-Certificaat voor meer informatie).

Automatisch

Het certificaat wordt automatisch gegenereerd met de Let's Encrypt-service.

De AppTec360 EMM gebruikt de HTTP-01 challenge voor validatie van het domein, wat betekent dat de HTTP-poort vanaf het internet open moet staan voor de eerste aanvraag van een certificaat. Latere verlengingsaanvragen kunnen via HTTPS worden gevalideerd.

Zet de keuzerondjes op "Automatisch (Let's Encrypt)" en druk op "WAARDE OPSLAAN". Het certificaat wordt automatisch aangevraagd bij het toepassen van de configuratie in Stap Vijf - Licentieovereenkomst. Het certificaat wordt indien nodig automatisch vernieuwd en je ontvangt een e-mail als het certificaat bijna verloopt (wat betekent dat de vernieuwing mogelijk is mislukt).

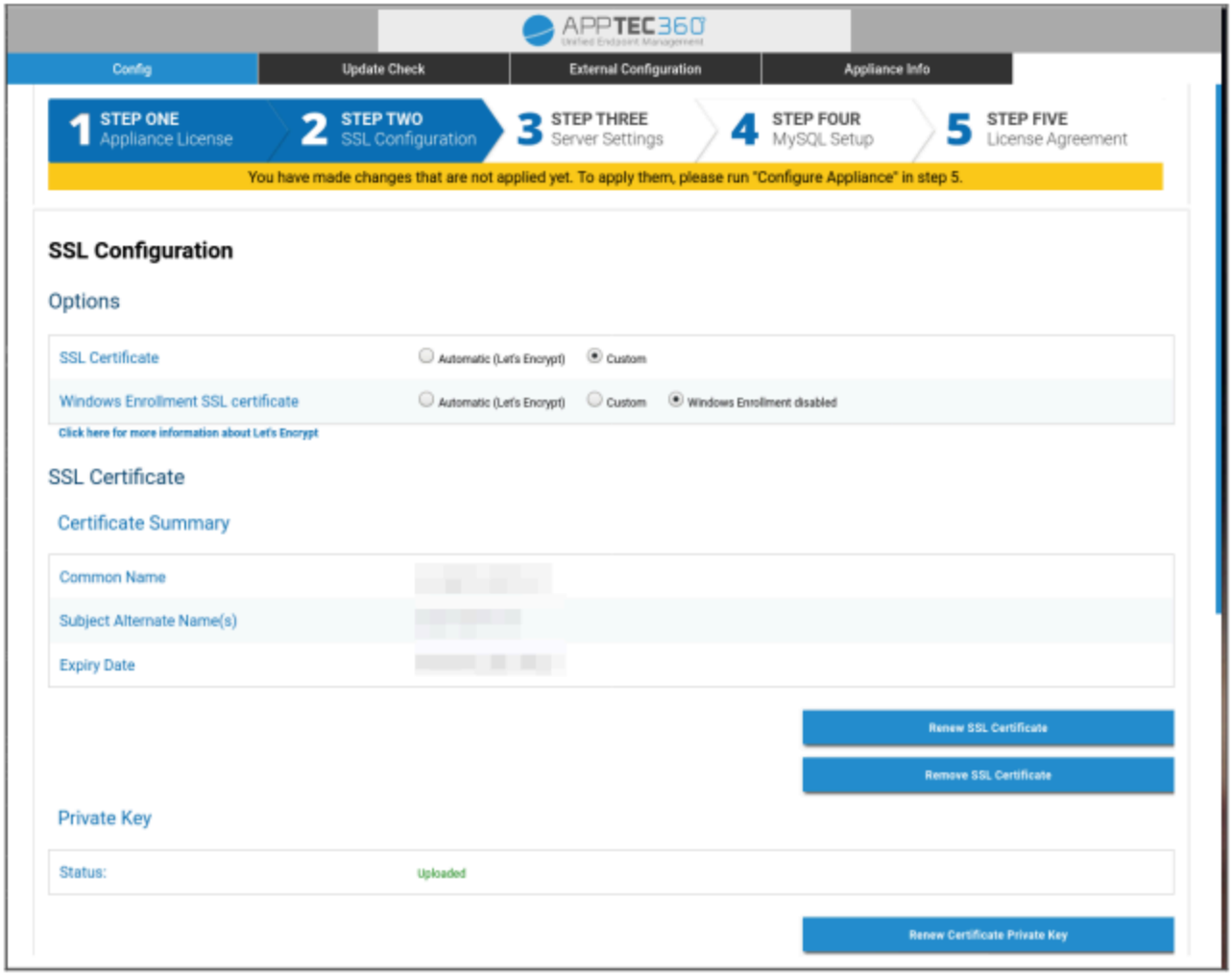
Aangepast

1. Upload het SSL-Certificaat voor uw gelicentieerde hostnaam. U kunt de hostnaam zien in Stap Een - Apparaatlicentie.

2. Upload ook de privésleutel voor het certificaat en indien nodig het tussenliggende certificaat.

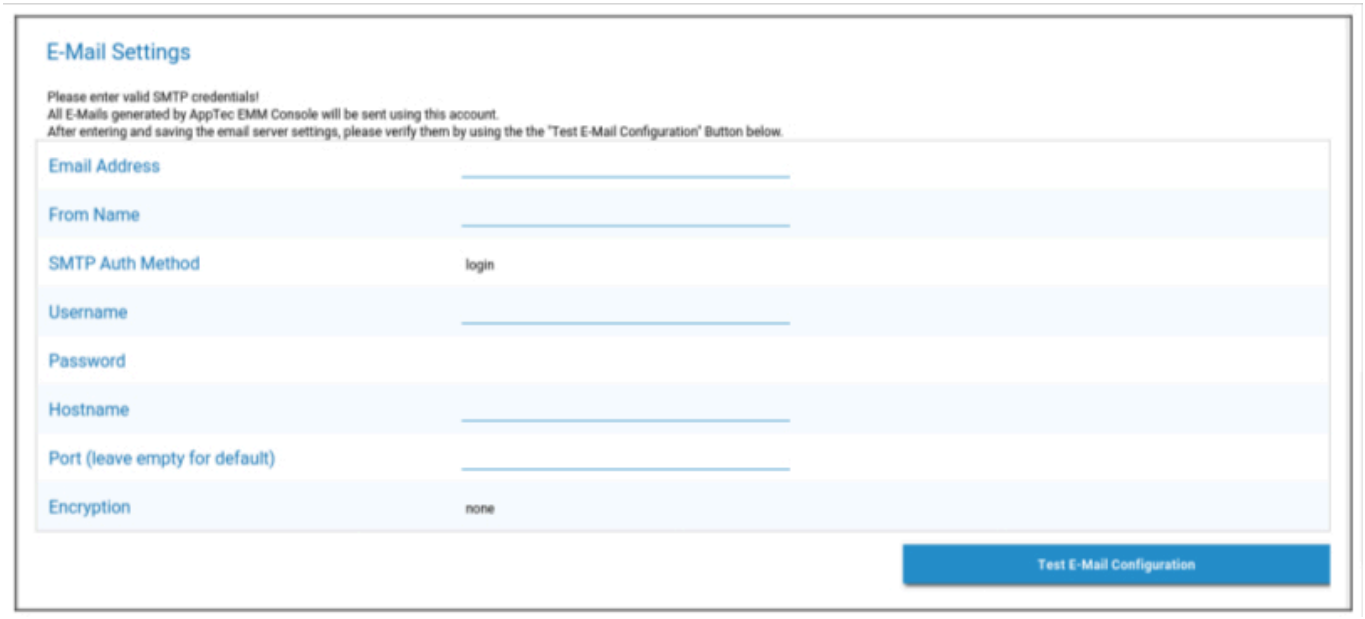
Belangrijk: De sleutel mag niet beveiligd zijn met een wachtwoord. Als dat wel het geval is, verwijder dan het wachtwoord voordat je de sleutel uploadt.

Tip: Als je ook Windows 10-apparaten wilt gebruiken, moet je "Windows Enrollment SSL certificate" inschakelen en het certificaat, de privésleutel en het tussenliggende certificaat voor je subdomein uploaden (beschreven in IP-Adres en DNS Resolution) onderaan de pagina.



Stap drie – serverinstellingen

1. Voer een algemeen e-mailadres voor ondersteuning in. Dit adres wordt gebruikt in e-mails aan uw gebruikers, zodat ze weten met wie ze contact moeten opnemen in geval van problemen met hun apparaat.
2. Geef e-mailinstellingen op die door het systeem worden gebruikt om e-mails te versturen. De instellingen worden gebruikt om e-mails naar de gebruiker te sturen en ook om Bug Reports en Feature Requests naar"support@apptec360.com"te sturen.Na het opslaan van je e-mailinstellingen moet je ze controleren door te klikken op "Test E-Mail Configuration" en de instructies te volgen.



Stap vier – MySQL instellen

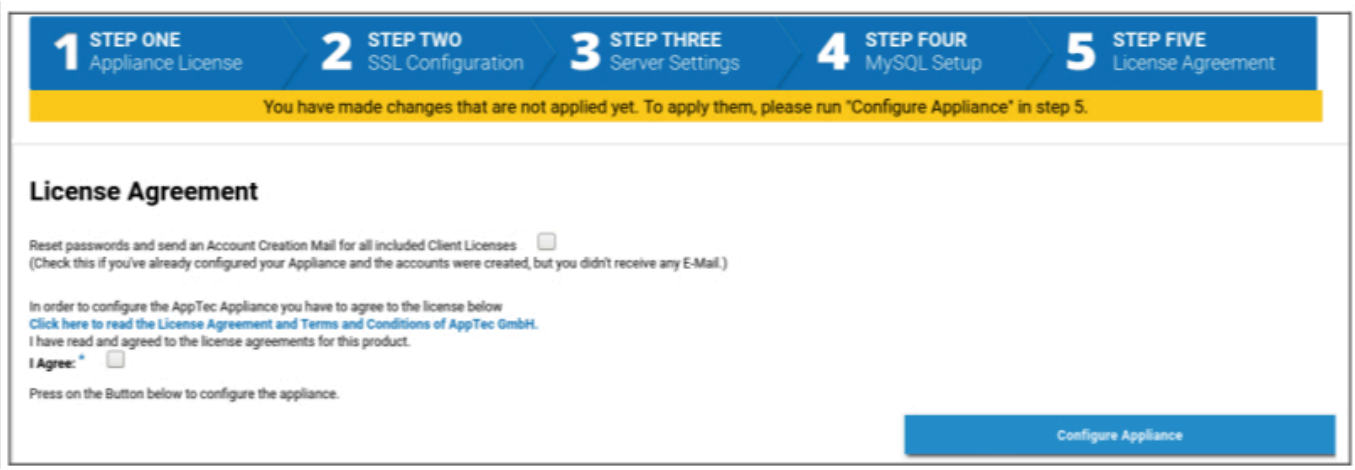
1. Als je de interne database wilt gebruiken, kun je deze stap overslaan. Anders kun je de verbindingsinformatie voor je externe databaseserver invoeren.


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)

Stap vijf – Licentieovereenkomst

1. Lees de licentieovereenkomst.
2. Vink "I Agree" (Ik ga akkoord) aan en druk op de knop "Configure Appliance" (Apparaat configureren) om de instellingen toe te passen.

Tip: U moet "Configure Appliance" uitvoeren elke keer dat u instellingen wijzigt in de 5 stappen om de instellingen toe te passen.



Gefeliciteerd!

Je bent klaar met de configuratie van de virtuele appliance.

Een e-mail met je wachtwoord is gestuurd naar het adres dat je hebt opgegeven voor de licentie (zichtbaar bij "Included Client Licenses" in Step One - Appliance License).

Je kunt nu inloggen op de console met dit wachtwoord en het e-mailadres waarop je het hebt ontvangen.

Om in te loggen op de console, voert u de hostnaam van de console in de adresbalk van uw browser in.

Je kunt de hostnaam van je apparaat vinden in Stap Een - Apparaatlicentie.

Problemen oplossen

1. Je hebt geen e-mail ontvangen bij het configureren van het apparaat in Stap Vijf - Licentieovereenkomst:

Zorg ervoor dat uw e-mailinstellingen in Stap Drie - Serverinstellingen correct zijn. Om het wachtwoord opnieuw te versturen, controleer "Reset passwords and send an Account Creation Mail for all included Client Licenses" in Stap Vijf - Licentieovereenkomst voordat je "Configure Appliance" opnieuw uitvoert.

2. Je hebt een fout ontvangen met betrekking tot Let's Encrypt tijdens de configuratie in Stap Vijf - Licentieovereenkomst:

Zorg ervoor dat het apparaat bereikbaar is via zijn domeinnaam op poort 80. Let's encrypt schrijft ook een log naar "/var/log/letsencrypt" wat kan helpen bij het verder oplossen van problemen.

Aanbevelingen voor beveiliging

Het wordt aanbevolen om de volgende stappen uit te voeren om je AppTec360-appliance te beveiligen.

Dit is geen volledige set instructies, het is slechts een aanbeveling voor een basisconfiguratie.

- Het wachtwoord voor de AppTec360-gebruiker wijzigen
- Wijzig het wachtwoord voor MySQL-gebruikers "root" en "AppTec" en pas Stap Vier - MySQL Setup dienovereenkomstig aan
- De standaard SSH-serverpoort wijzigen
- Blokkeer poort 80 in je console en verbied inkomend HTTP-verkeer, gebruik alleen HTTPS. Eenmaal geconfigureerd, is een externe configuratie via HTTPS ook mogelijk.
- Beperk de toegang tot de beheerinterface tot bepaalde Ips onderaan Stap Drie - Serverinstellingen
- De firewall configureren

Algemene instellingen

Account Overzicht

Accountgegevens

Overzicht

Hier zie je een overzicht van je AppTec360-account.

Bedrijfsnaam	Uw bedrijfsnaam
Aanmaakdatum	Aanmaakdatum van je account
Licentie Type	Betaald = betaalde licentie Gratis = onbetaalde licentie Opmerking: Accounts op een OnPremise Appliance worden om technische redenen altijd als betaald weergegeven.
Klant	Identificatiecode van je account (dit is NIET je klantnummer)
Vervaldatum licentie	Vervaldatum van je AppTec360-licentie
ContentBox-licentie	Gratis = gratis licentie voor 25 apparaten Betaald = betaalde licentie voor x apparaten
Lanceerinrichting	Geeft aan of je de aangepaste launcher voor Android kunt gebruiken of niet.
Apparaten	Aantal momenteel gebruikte / totale licenties
Contactpersoon	Contactpersoon opgegeven
Telefoon	Telefoonnummer opgegeven
e-mail*	E-mailadres opgegeven
Hoofdgebruiker	Root-gebruikers die kunnen inloggen
Softwareversie	Huidige softwareversie

**Opmerking: het e-mailadres dat hier wordt weergegeven, is het e-mailadres dat je hebt ingevoerd om de account te registreren. Op basis hiervan wordt een gebruiker aangemaakt in de gebruikers-/apparatenstructuur en deze kan worden gewijzigd. Als u deze gebruiker bewerkt, wordt het e-mailadres dat u moet gebruiken om in te loggen gewijzigd, maar niet de informatie in het accountoverzicht. .*

Bug rapport

Een bugrapport kan rechtstreeks naar support worden gestuurd om problemen of bugs te melden en bevat informatie en logbestanden over je account en instellingen.

Onderwerp	Het onderwerp van het bugrapport. Voeg een ticketnummer toe als u dit wilt toevoegen aan een bestaand supportticket.
Verwacht gedrag	Beschrijf in detail wat je deed en wat je verwachtte dat er zou gebeuren
Feitelijk gedrag	Beschrijf in detail wat er precies gebeurt. Citeer foutmeldingen EXACT. Het helpt ook als u schermafbeeldingen toevoegt aan de bijlage.
Op welk moment trad het probleem op?	Geef een precies tijdstip waarop u een specifieke foutmelding/probleem kreeg. Voeg in het beste geval ook seconden toe, bijvoorbeeld 18:55:27
Kan het probleem worden gerepliceerd? Zo ja, hoe (in detail)?	Beschrijf in detail hoe je het probleem kunt reproduceren.
Heeft deze functie eerder gewerkt zoals u verwachtte? Zo ja, tot wanneer?	Laat leeg als je het niet weet.
Zijn er specifieke wijzigingen aangebracht in het systeem voordat dit probleem zich voordeed? Zo ja, welke wijzigingen (in detail)?	Vermeld altijd wat je laatste verandering of actie was voordat het probleem verscheen, zelfs als je denkt dat het irrelevant is.
Indien van toepassing: Welke apparaatmodellen en OS-versies worden beïnvloed?	Vermeld altijd de exacte OS-versie (bijv. iOS 14.7.1 of Android 11)
Indien van toepassing: Wat is het openbare IP-adres en/of serienummer van het apparaat?	Noem er minstens één, zelfs als alle apparaten zijn getroffen.
Logbestanden opnemen	Vink dit aan om het logbestand met het bugrapport mee te sturen. Dit wordt aanbevolen om te doen.
Huidige VPP-status ophalen bij Apple en toevoegen aan bugreport	Bevat informatie over VPP licentietoewijzingen. Activeer dit alleen als je daarom wordt gevraagd door support of als je probleem te maken heeft met VPP.

Bijlage	Voeg een bestand bij dat nuttig kan zijn (bijvoorbeeld schermafbeeldingen van een foutmelding)

Functieverzoek

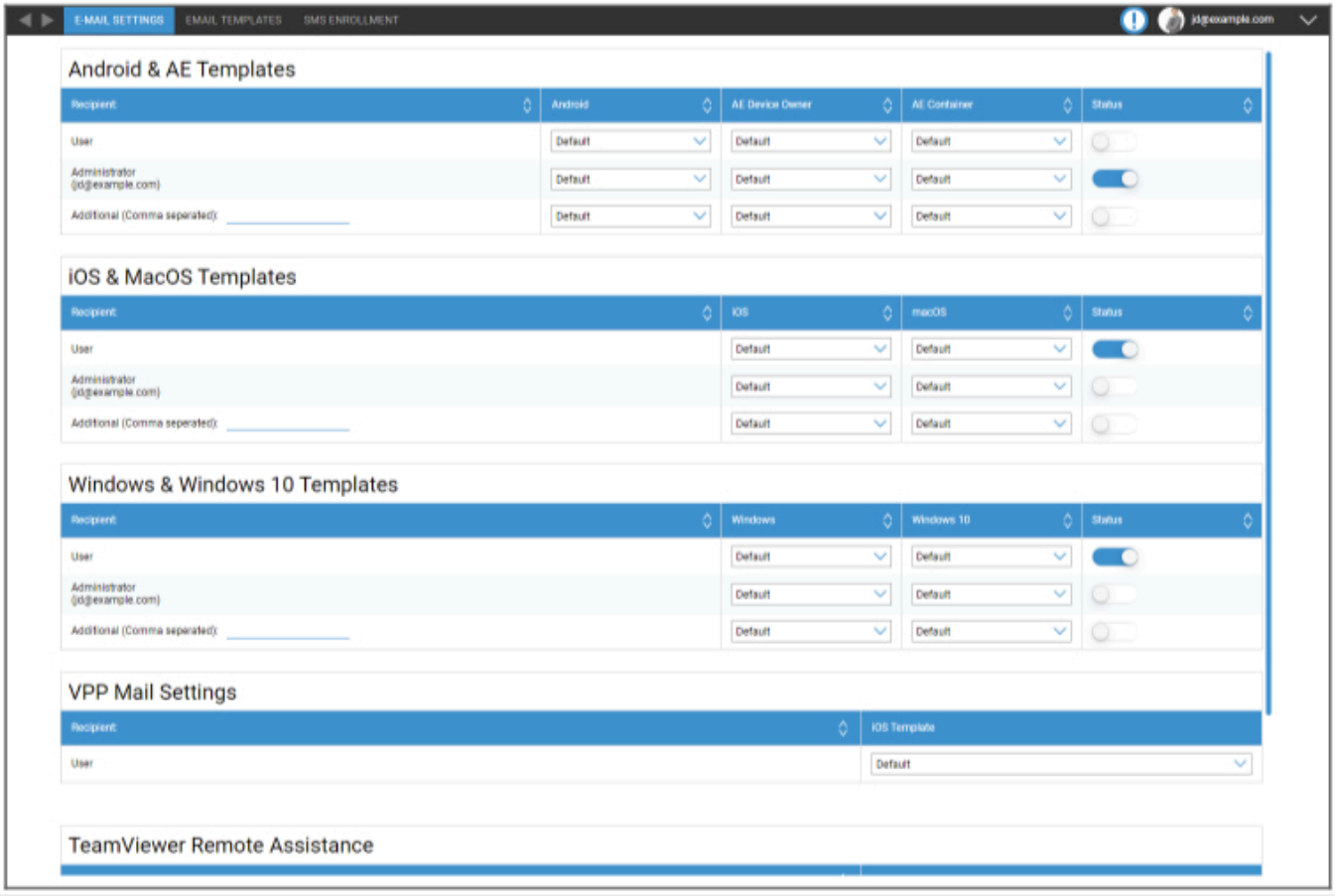
Een functieverzoek kan rechtstreeks naar support worden gestuurd. Dit kan een verzoek bevatten voor een specifieke functie of een verbetering voor

Samenvatting	Een korte samenvatting van je probleem
Beschrijving	Een gedetailleerde beschrijving van je probleem, wees zo specifiek mogelijk
Bijlage	Bestanden bij het bugrapport voegen

Globale configuratie

Instellingen eMail

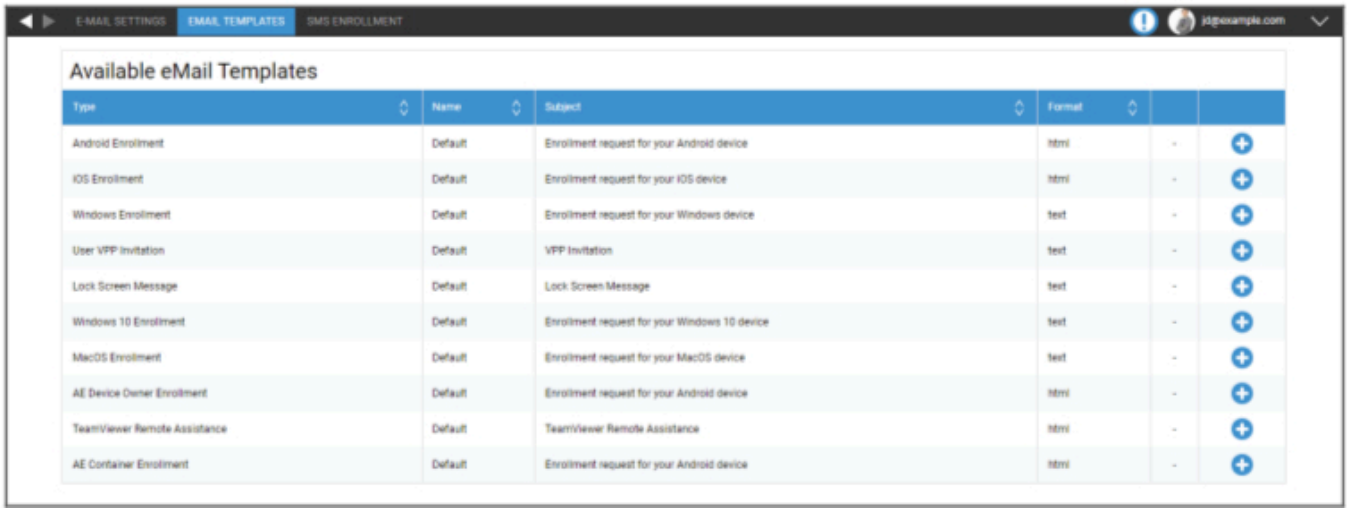
Hier kun je instellen wie er een e-mail krijgt wanneer er een inschrijvingsverzoek wordt gegenereerd en welke tekstsjabloon wordt gebruikt voor die e-mail.



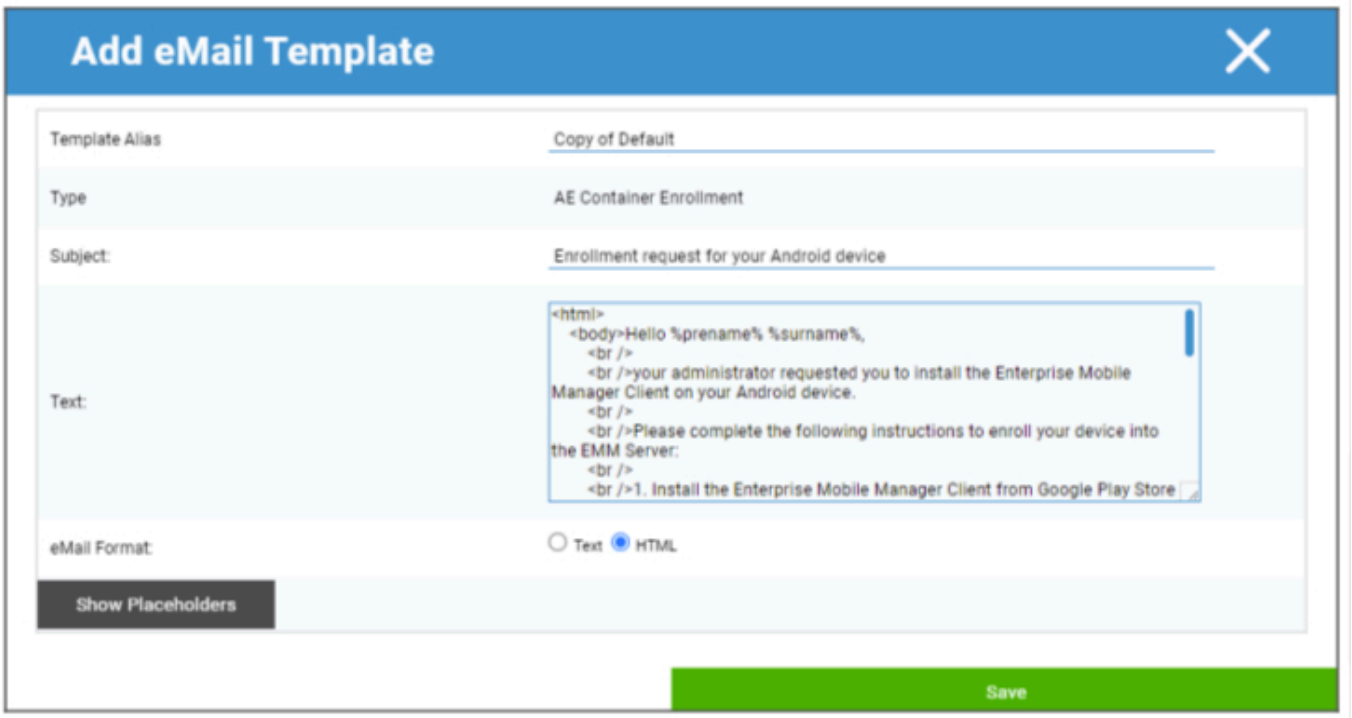
eMail Sjablonen

Hier kun je sjablonen voor verschillende scenario's genereren en bewerken. Deze kunnen in normale tekstvorm of in HTML zijn. Met HTML kun je de opmaak van je tekst beter beheren.

De standaardsjablonen kunnen niet worden bewerkt of gewist.



Je kunt ook Plaatshouders als variabele gebruiken die automatisch worden vervangen. Klik tijdens het bewerken op "Placeholders weergeven" om de beschikbare Placeholders te zien. Verschillende categorieën hebben verschillende plaatsaanduidingen.



SMS Inschrijving

Hier kunt u het SMS Enrollment proces deactiveren.

(Standaard: gedeactiveerd)

Je ziet ook een scherm dat aangeeft hoeveel SMS-credits er nog beschikbaar zijn.

SMS Credits moeten apart worden gekocht.

Privacy

GPS-toegang

Hier kun je de GPS-weergave voor elk apparaat beveiligen met 1 of 2 wachtwoorden (vier ogen principe). Telkens wanneer u de locatie van een apparaat probeert te openen, wordt u gevraagd uw wachtwoord(en) in te voeren.

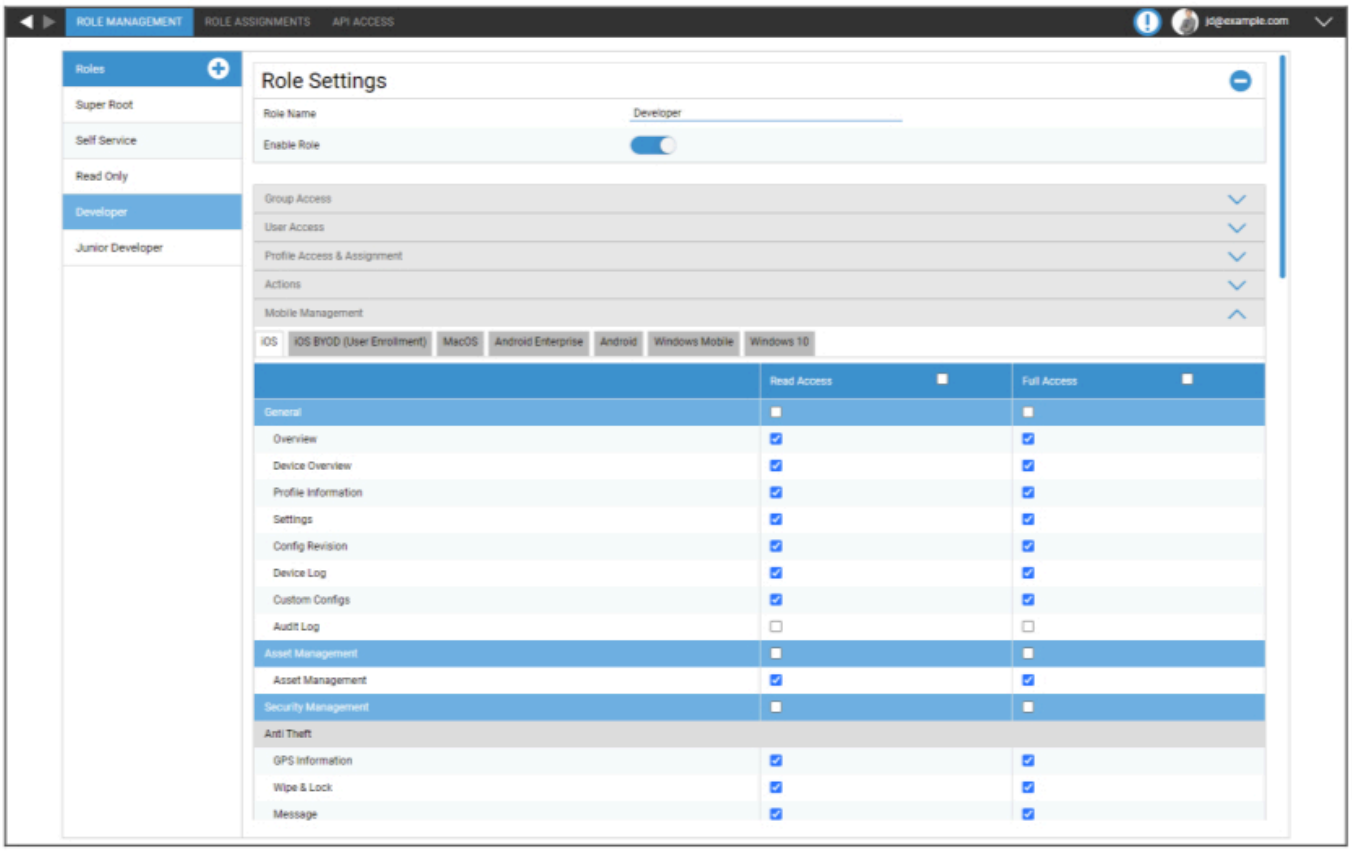
Toegang tot GPS-instellingen beperken	Uit = functie is uitgeschakeld en er is geen wachtwoord nodig voor lokalisatie
	Aan = functie is ingeschakeld en een wachtwoord is vereist voor lokalisatie
Beschermingsmethode	Gebruik één wachtwoord = gebruik één wachtwoord voor lokalisatie
	Gebruik twee wachtwoorden = gebruik twee wachtwoorden voor lokalisatie
Wachtwoord invoeren (1)	Voer het gekozen wachtwoord in
Herhaal wachtwoord (1)	Voer het gekozen wachtwoord opnieuw in
optioneel: Voer wachtwoord 2 in	Voer het 2e gekozen wachtwoord in
optioneel: Herhaal wachtwoord 2	Voer het 2e gekozen wachtwoord opnieuw in

Opmerking: Nadat u uw wachtwoordcode(s) hebt ingesteld, moet u deze nogmaals invoeren voordat deze volledig is ingeschakeld.

Rolgebaseerde toegang

Rolmanagement

De Rollen bepalen wat een gebruiker kan zien en doen als hij inlogt op de beheerconsole. Hierdoor kun je gebruikers aanmaken die wel kunnen inloggen, maar beperkte functionaliteit hebben.



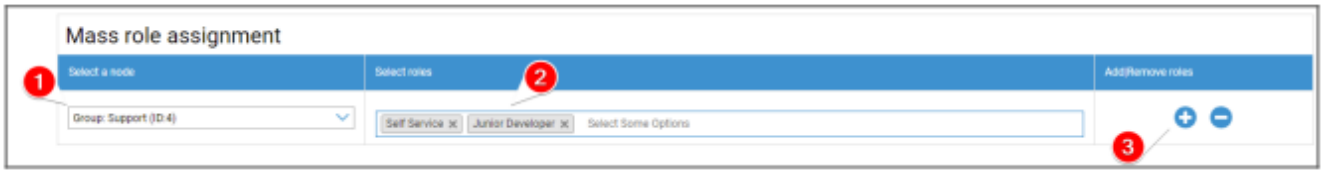
De Super root rol is een standaard rol die altijd alles kan zien en wijzigen. Deze kan niet worden gewijzigd of verwijderd. De Self Service rol kan alleen zijn eigen gebruikers en apparaten zien. Je kunt Self Service combineren met een aangepaste rol om gebruikers bijvoorbeeld toe te staan zelf en alleen voor hun gebruiker in te loggen en apparaten aan te melden.

Aangepaste rollen kunnen handmatig worden in- of uitgeschakeld. Nieuwe rollen zijn standaard uitgeschakeld. Gebruikers met een uitgeschakelde rol werken alsof ze de rol niet hebben. Hierdoor kun je bijvoorbeeld tijdelijk de acties van een bepaalde rol beperken.

Alle rechten zijn verdeeld tussen "Leestoegang" en "Volledige toegang". Als je een rol leestoegang geeft, kunnen ze het specifieke deel van de console zien. Door volledige toegang te geven kan de rol het specifieke deel van de console zien en wijzigen.

Rolverdeling

Hier krijg je een overzicht van alle gebruikers die een rol hebben en kun je zien welke rol ze hebben. Je kunt hier ook een rol toewijzen aan gebruikers of hele groepen:

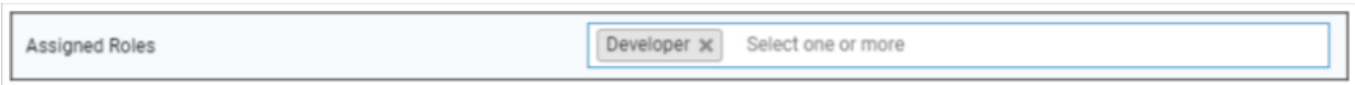


1. Selecteer voor welke groep of gebruiker je rollen wilt toevoegen of verwijderen. Je kunt een enkele gebruiker of een groep selecteren. Als je een groep selecteert, heeft je wijziging invloed op alle gebruikers binnen die groep en op alle gebruikers van subgroepen binnen de geselecteerde groep.
2. Selecteer welke rol je wilt toevoegen of verwijderen. Je kunt één of meerdere rollen selecteren.
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. Opslaan om het proces te voltooien. Gebruikers die eerder geen rol hadden en "Kan inloggen" hadden uitgeschakeld, ontvangen automatisch een e-mail met een link om een wachtwoord in te stellen.

Onder de Massa-roltoewijzing vind je een overzicht van de toegewezen rollen. Je kunt hier ook handmatig rollen wijzigen voor specifieke gebruikers.

Toewijzing van een rol

Om een rol toe te wijzen aan een gebruiker, moet je naar Mobile Management gaan, waar je de boomstructuur van je groepen, gebruikers en apparaten vindt. Bewerk de gebruiker om een rol toe te wijzen. Je kunt de bovenstaande methode ook gebruiken voor afzonderlijke gebruikers.



API-toegang

Toegang tot AppTec360 REST API

De AppTec360 REST API vereist een authenticatietoken (API-sleutel) en een privésleutel die moeten worden gegenereerd in de beheerconsole.

Om dit te doen log je in op AppTec360 EMM en ga je naar

Algemene instellingen → Rolgebaseerde toegang → API-toegang en voeg een nieuwe sleutel toe.

Je moet een gebruiker selecteren wiens rechten van toepassing zijn op de API-sleutel.

De privésleutel kan maar één keer worden gedownload. Nadat het downloaden is gestart, wordt de sleutel verwijderd en verdwijnt de knop "Downloaden".

Als je je privésleutel verliest, moet je een nieuwe API-sleutel genereren.

Algemene regels

- De REST API is beschikbaar onder de basis URL:

/public/external/api

- Alle verzoeken moeten via POST worden verzonden.
- De REST API ondersteunt alleen verzoeken via HTTPS.
- Verzoeken moeten de volgende Headers bevatten:

Naam koptekst	Koptekst Waarde	Beschrijving
Inhoudstype	toepassing/json	vaste
auth	123...xyz	API-sleutel van het tabblad "API-toegang
handtekening	Base64-gecodeerde handtekening	Handtekening van de payload gegenereerd met de privésleutel van het tabblad "API-toegang

- De verzoektekst moet een json-gecodeerd object zijn dat de volgende waarden moet bevatten:

Veld	Veld Voorbeeld Waarde	Beschrijving
api	v2/device/listdevices	Naam van de API
tijd	1529662725	Unix Timestamp (UTC) van de clientcomputer. Het maximaal toegestane tijdsverschil tussen de client en de server is 30 minuten.

- Bij succes retourneert de API de aangevraagde gegevens (zie de Queries hieronder) en een HTTP-statuscode 200.
- Als er een fout optreedt, zal de HTTP-statuscode tussen 4xx en 5xx zijn, afhankelijk van de fout, en het antwoordobject zal een array bevatten met de sleutel "errors", die een lijst met menselijk leesbare foutmeldingen bevat.
- Als er geen overeenkomende gegevens zijn voor een apparaat, wordt een lege matrix geretourneerd.
- Als een apparaat-id niet bestaat, zijn de retourgegevens nul.

Voorbeeld verzoek

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]}}

Query’s

Alle apparaten weergeven

Functionaliteit: Geeft een lijst van alle apparaten met de apparaat-ID, IMEI en serienummer
API URI: v2/device/listdevices
Verplichte parameters: geen
Optionele parameters: geen

Voorbeeld Aanvraaginstantie


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


Voorbeeld Response Body


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

Lijst met (GPS-)posities opvragen

Functionaliteit: Retourneert een lijst met alle opgeslagen positielogboekvermeldingen voor apparaat-id's
API URI: v2/device/listposition
Verplichte parameters: "ids" - Array van apparaat-ID's
Optionele parameters: geen

Voorbeeld Aanvraaginstantie

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

Voorbeeld Response 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":[],
]
}

Activakaart ophalen

Functionaliteit:
Retourneert een lijst met alle opgeslagen mogelijke assets die kunnen worden opgevraagd met Get any asset data.
U kunt ofwel de menselijk leesbare vorm of de asset tag gebruiken om de data op te vragen.
API URI: v2/device/getassetmap
Verplichte parameters: geen
Optionele parameters: geen

Voorbeeld Aanvraaginstantie

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

Voorbeeld Response Body

Dit antwoord is ingekort voor de leesbaarheid.

{
"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": []
}

Verkrijg alle activagegevens

Functionaliteit: Retourneert een lijst met aangevraagde activagegevens voor apparaat-id's
API URI: v2/device/getassetdata
Verplichte parameters: "ids" - Array van apparaat-ID's
Optionele parameters:
"assetkeys" - Activadatasleutels die moeten worden geretourneerd. Indien niet gespecificeerd worden alle beschikbare assetgegevens geretourneerd
. Je kunt een lijst van assetkeys krijgen met Get asset map.

Voorbeeld Aanvraaginstantie

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

Voorbeeld Response Body

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

Voorbeeldcode in 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 configuratie

APNS-certificaat

Hier kun je een APNS-certificaat uploaden. Dit is nodig om iOS- en MacOS-apparaten te beheren.

Opmerking: Het APNS-certificaat is slechts één jaar geldig. Dit moet worden vernieuwd voordat het verloopt. Het verlengingsproces is identiek aan het aanmaken (zie hieronder) en duurt slechts een paar minuten.

Als u vergeet om dit op tijd te vernieuwen, kunt u geen wijzigingen aanbrengen aan uw reeds aangemelde apparaten **en moet je alle apparaten opnieuw registreren**.

Stap 1

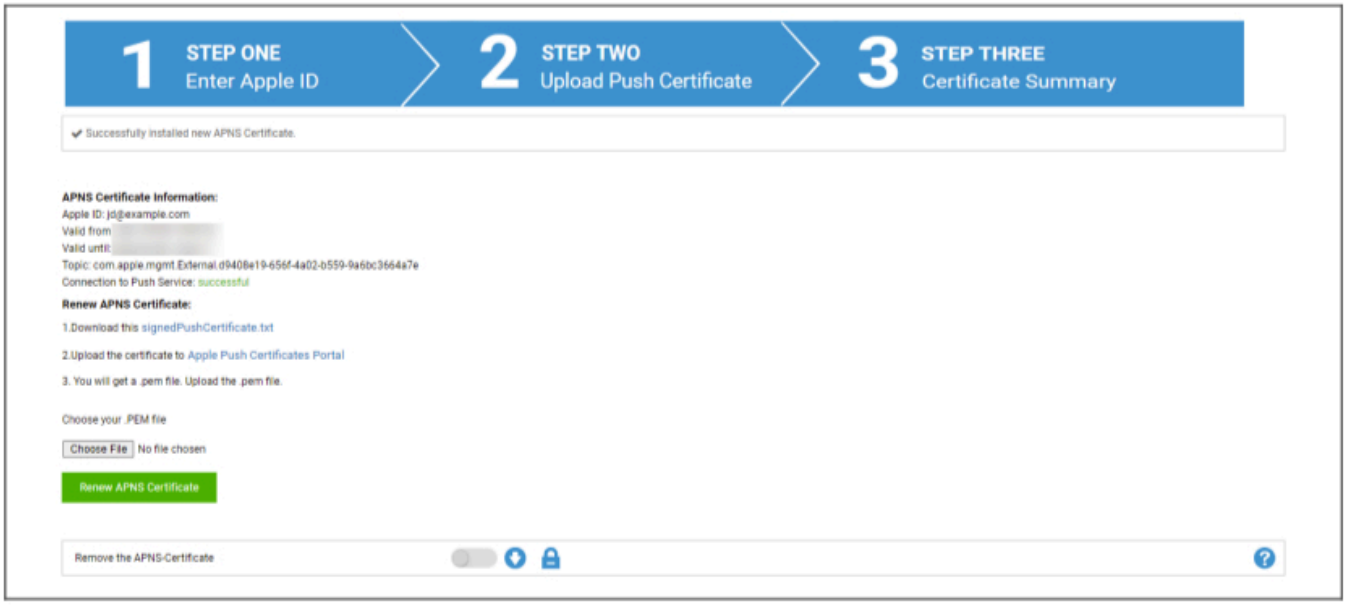
- Voer eerst uw Apple ID in die u wilt gebruiken om het APNS-certificaat aan te maken.

Opmerking: deze Apple ID wordt alleen gebruikt voor het aanmaken van het APNS-certificaat. Deze Apple ID heeft niets te maken met de apparaten en de apparaten zijn niet op de hoogte van deze Apple ID. Daarnaast heeft u ook toegang nodig tot deze Apple ID om het APNS Certificaat te vernieuwen. Daarom is het aan te raden om een generieke Apple ID te gebruiken en de inloggegevens te documenteren. Er wordt een herinnering gestuurd naar het gebruikte e-mailadres van de Apple ID voordat het APNS-certificaat verloopt.

- Klik op "Volgende stap" om verder te gaan.
- (optioneel) U kunt ook het eerder verwijderde APNS-certificaat herstellen als u het per ongeluk hebt verwijderd.

Stap 2

- Het ondertekendePushCertificate.txt downloaden
- Ga naar https://identity.apple.com/pushcert/ en log in met de Apple ID uit stap 1.
- Klik op "Een certificaat maken".
- (optioneel) voer een Opmerking in. Dit kan handig zijn als je meerdere huurders beheert om ze gemakkelijk te kunnen identificeren.
- Klik op "Choose File" om het eerder gedownloade signedPushCertificate.txt te selecteren
- Klik op "Uploaden".
- U ziet nu de bevestiging dat u een APNS-certificaat heeft aangemaakt.
- Klik op "Downloaden" en sla het op.
- Ga terug naar de beheerconsole.
- Klik op "Bestand kiezen" en selecteer het APNS-certificaat dat u wilt uploaden.
- Klik op "Uploaden".



Stap 3

U hebt nu met succes het APNS-certificaat ingesteld en kunt nu iOS- en MacOS-apparaten beheren.

In stap 3 ziet u een overzicht van uw huidige APNS-certificaat.

U kunt ook het APNS-certificaat vernieuwen door de stappen op het scherm te volgen. Denk eraan dit te vernieuwen voordat het verloopt.

Wanneer u het APNS-certificaat vernieuwt, moet u er rekening mee houden dat u inlogt met de Apple ID die u ziet in stap 3 en dat u het eerder gebruikte certificaat vernieuwt en GEEN nieuw certificaat aanmaakt. U ziet het "onderwerp" van het APNS-certificaat in Stap 3 en wanneer u op de "i" klikt in de Apple Push Certificate Portal. Dit is de unieke ID die het certificaat identificeert. Dit helpt je bij het identificeren en vernieuwen van het juiste certificaat.

Wanneer je "Error: The Push Certificate has a different topic!" tijdens het vernieuwen, betekent dit dat je een ander certificaat hebt vernieuwd of een nieuw hebt aangemaakt.

Als je een nieuw Certificaat wilt uploaden, bijvoorbeeld als je geen toegang meer hebt tot de eerder gebruikte Apple ID, moet je eerst het huidige geüploade Certificaat verwijderen.

Hoe dan ook, het verwijderen van het APNS Certificaat betekent dat je geen wijzigingen meer kunt maken voor de huidige aangemelde apparaten totdat je ze opnieuw aanmeldt. Zorg er dus voor dat je hierop voorbereid bent en verwijder het certificaat alleen als het echt niet anders kan.

Beheerde toegang

Hier kun je User-Enrollment voor iOS-apparaten en Shared iPad voor iOS-apparaten inschakelen.

Gebruikersregistratie

User Enrollment' maakt een speciale modus mogelijk voor BYOD-apparaten.

Voor elke gebruiker moet een beheerde Apple-ID worden aangemaakt in de Apple Business Portal.

Tijdens het registratieproces worden de gebruikers gevraagd naar hun Apple-ID gegevens.

Gebruikersregistratie' garandeert maximale veiligheid voor de gebruiker, omdat de MDM slechts een beperkte set instellingen en beperkingen kan configureren.

Beheerdomein:

Het domein dat wordt gebruikt om het e-mailadres van de gebruiker toe te wijzen aan zijn beheerde Apple-ID (moet het volgende formaat hebben: '@appleid.company.com'). john.doe@example.com wordt bijvoorbeeld toegewezen aan john.doe@appleid.company.com.

Controleer de Apple Business Manager om uw Managed Domain te zien

Gedeelde iPad

Een gedeelde iPad is een DEP-apparaat dat geconfigureerd is met een speciaal DEP-profiel.

Hierdoor kunnen meerdere gebruikers inloggen op het apparaat met hun beheerde Apple-ID.

De beheerde Apple-ID moet worden aangemaakt in de Apple Business Portal of de Apple School Manager.

Gebruikers die inloggen op een gedeelde iPad worden gevraagd om hun beheerde Apple-ID-referenties.

Beheerdomein:

Het domein dat wordt gebruikt om het e-mailadres van de gebruiker toe te wijzen aan zijn beheerde Apple-ID (moet het volgende formaat hebben: '@appleid.company.com'). john.doe@example.com wordt bijvoorbeeld toegewezen aan john.doe@appleid.company.com.

Controleer de Apple Business Manager om uw Managed Domain te zien

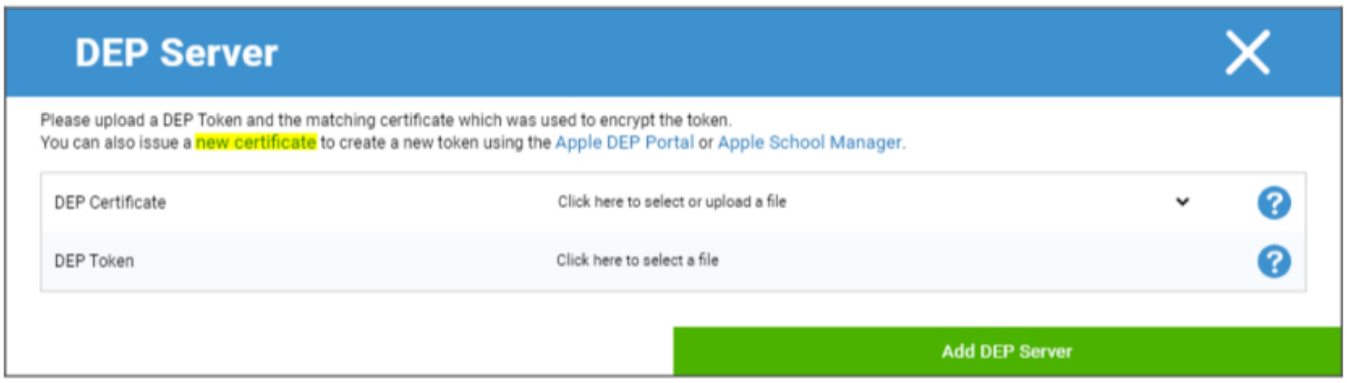
DEP

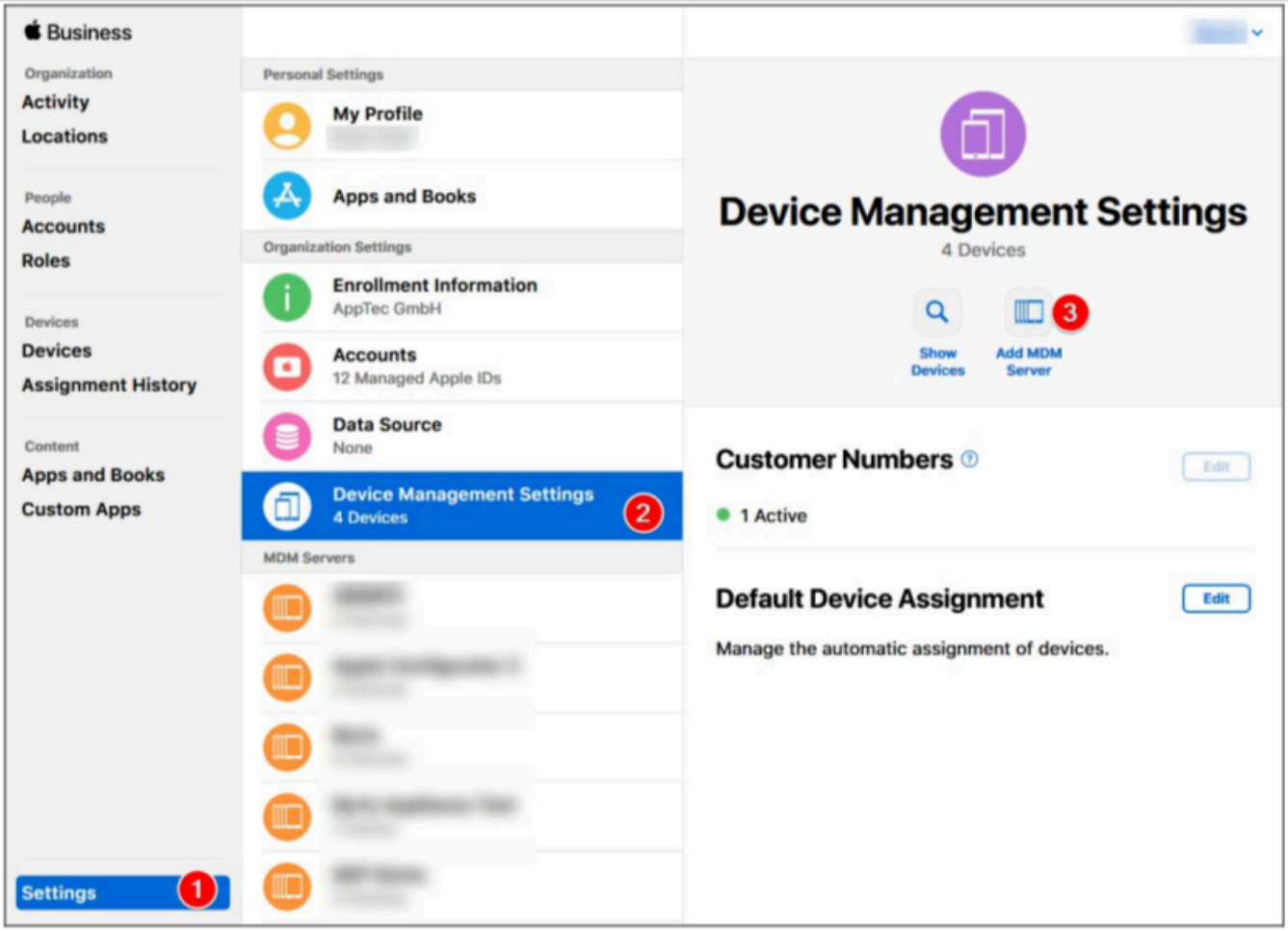
Met DEP (Device Enrollment Program) kun je apparaten eenvoudig aanmelden bij de MDM. Wanneer je DEP gebruikt, worden de apparaten automatisch verbonden met de MDM wanneer je het apparaat instelt. Je kunt ook bijna alle installatiestappen overslaan die meestal verplicht zijn op iOS.

Houd er rekening mee dat je de apparaten moet kopen bij een reseller die DEP ondersteunt. Neem voor meer informatie contact op met je reseller of Apple.

Meer informatie over DEP: https://www.apple.com/business/dep/

Klik op de "+" om een DEP Token toe te voegen. Klik in de popup op "nieuw certificaat" in de tekst (geel gemarkeerd in de afbeelding hieronder). Hierdoor wordt een DEP-certificaat gegenereerd en gedownload. Ga daarna naar de Apple Business Manager(https://business.apple.com/) of Apple School Manager(https://school.apple.com/).

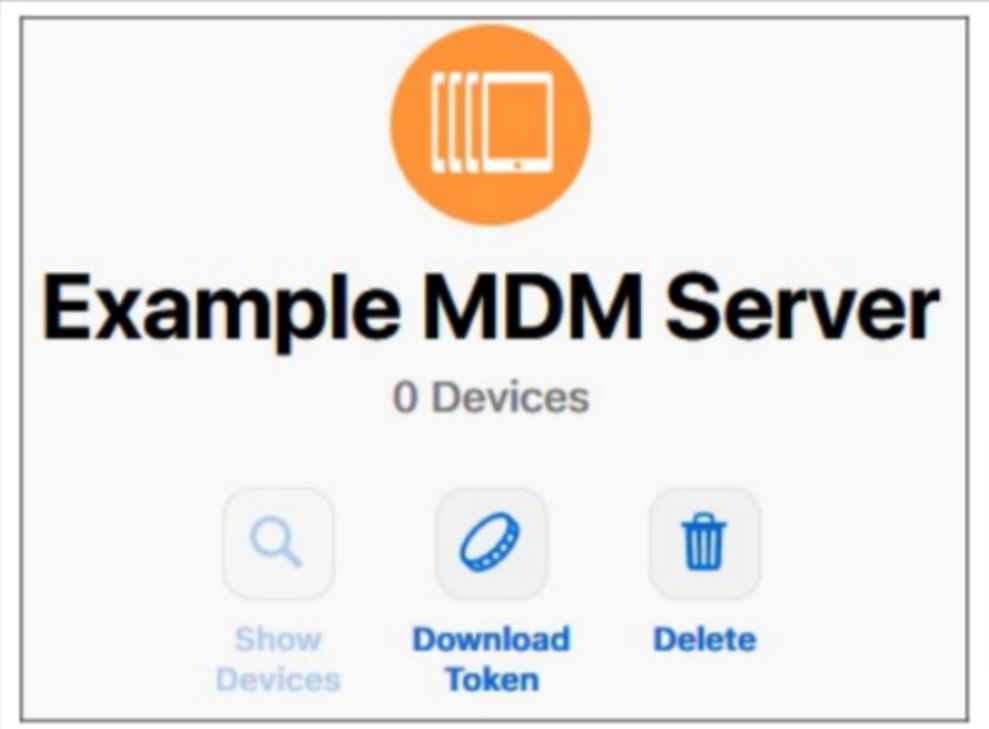




Volg in Apple Business Manager de stappen zoals in de bovenstaande afbeelding. Instellingen → Instellingen apparaatbeheer → MDM-server toevoegen.

Geef de server een naam naar keuze en upload het eerder gedownloade DEP-certificaat onder MDM Server Settings → Upload Public Key en klik op "Save".

Je krijgt nu de optie "Token downloaden". Klik hierop en sla het op. Het token is slechts 1 jaar geldig. Maar door nogmaals op "Download Token" te klikken, krijg je een nieuwe, waardoor het vernieuwen van het token heel eenvoudig wordt.



U kunt nu teruggaan naar de MDM, waar u eerder het DEP-certificaat hebt gedownload. Als u het tabblad niet hebt gesloten, zou het pop-upvenster voor het toevoegen van een DEP-server nog steeds geopend moeten zijn en zou het DEP-certificaat al geselecteerd moeten zijn. U kunt nu uw Token uploaden in het veld "DEP Token" en op DEP Server klikken.

In de kolom "**Devices" (Apparaten)**ziet u het aantal apparaten dat is toegewezen aan deze DEP-server. Apparaten die worden toegevoegd aan deze DEP-server worden automatisch aangemaakt in de DEP-pool in Mobile Management.

U kunt op dit nummer klikken om een overzicht te krijgen van al uw DEP-apparaten en hun status.

Opmerking: Afhankelijk van uw workflow of configuratie in de Business Manager is het mogelijk dat u deze apparaten handmatig moet toewijzen aan de DEP Server. U kunt ook een standaard DEP Server instellen in de Apple Business Manager voor nieuwe apparaten.

In de kolom "**Profiles**" zie je het aantal DEP Profiles dat je hebt. U kunt ook op dit aantal klikken om details te zien over uw DEP Profiles en u kunt hier oude/ongebruikte profielen verwijderen. Het is momenteel niet mogelijk om deze te wijzigen. Als u een wijziging wilt aanbrengen, moet u een nieuwe aanmaken.

In de kolom "**Laatste synchronisatie**" kunt u de DEP-server handmatig synchroniseren (bijv. als u net een nieuw apparaat aan DEP hebt toegevoegd) en de datum van de laatste succesvolle synchronisatie zien.

In de kolom "**Auto profiel**" kun je een DEP-profiel instellen als automatische standaard. Dit profiel wordt automatisch toegewezen aan nieuwe apparaten. Als u geen Auto Profile instelt, moet u telkens handmatig een profiel toewijzen aan nieuwe apparaten.

In de kolom "**Add Profile**"**(Profiel toevoegen)**kunt u een nieuw DEP-profiel toevoegen. Het apparaat zal dit ontvangen aan het begin van de apparaatinstelling. Het DEP-profiel bepaalt hoe het apparaat wordt ingesteld en welke instelstappen worden overgeslagen.

Opmerking: nadat een apparaat is geregistreerd, kunnen deze instellingen alleen worden gewijzigd door een fabrieksreset uit te voeren en het apparaat te registreren met een nieuw profiel. Dit is vooral relevant voor "**Verwijderbaar**" en "**Koppeling toestaan**". In het geval van "**Koppeling toestaan**" is het aan te raden om dit aan te zetten, aangezien dit kan worden uitgeschakeld via MDM-beperkingen, maar het kan niet opnieuw worden ingeschakeld als het is uitgeschakeld in het DEP-profiel.

In de kolom "**Bewerken**" kunt u een nieuw token uploaden, bijvoorbeeld wanneer u het token vernieuwt.

Configurator & URL

URL’s voor zwembadinschrijving

Hier kun je een URL en QR Code aanmaken die geldig zijn tot een bepaalde datum en voor een bepaald aantal aanmeldingen. Zo kun je meerdere apparaten aanmelden met slechts één link of QR-code.

Apparaten die zijn geregistreerd met deze URL of QR-code worden in de pool in Mobile Management geplaatst en je moet ze daarna handmatig toewijzen aan een groep of gebruiker.

Opmerking: dit is alleen voor handmatig aanmelden. Gebruik deze URL niet als u de apparaten aanmeldt via Apple Configurator

MDM-profiel – Apple Configurator

Hier vind je de URL die je nodig hebt om apparaten te registreren via Apple Configurator. Tijdens het voorbereiden van apparaten met de Apple Configurator kun je de apparaten in hetzelfde proces toevoegen aan het MDM. De Apple Configurator heeft hiervoor deze URL nodig.

Apparaten die zijn toegevoegd via Apple Configurator worden in de pool in Mobile Management geplaatst en je moet ze daarna handmatig toewijzen aan een groep of gebruiker.

Je vindt hier ook een .mobileconfig bestand dat je kunt gebruiken om de apparaten aan te melden via Apple Configurator. In ieder geval wordt aangeraden om de URL te gebruiken.

Android-configuratie

Android-configuratie

Bescherming verwijderen	Als deze functie is geactiveerd, kan de gebruiker de apparaatbeheerder niet deactiveren zonder het wachtwoord in te voeren dat is ingesteld door de MDM-beheerder. Het wachtwoord wordt ingesteld tijdens de registratie, dus apparaten moeten opnieuw worden geregistreerd om het wachtwoord bij te werken. Er zijn twee opties om de apparaatbeheerders te verwijderen: 1. Handmatig op het apparaat ◦ Open de EMM-app op het apparaat ◦ Ga naar het tabblad Status ◦ Tik op "Bescherming verwijderen". ◦ Voer het wachtwoord in Je kunt de Revision gebruiken om het juiste wachtwoord op te halen uit de "Password History" in de console. ◦ Scroll naar beneden en tik op het nieuw toegevoegde punt "Tik op om AppTec360 MDM App te verwijderen" (je hebt 20 seconden om deze taak uit te voeren). ◦ Bevestig het dialoogvenster "AppTec360 MDM App verwijderen" met "ok". Hierdoor wordt het apparaat van de console verwijderd. ◦ Om de app van het apparaat te verwijderen bevestig je het dialoogvenster "AppTec360 MDM wordt verwijderd" met "UNINSTALL". 2. de automaat (Console) ◦ Selecteer het apparaat in de console ◦ Klik op het blauwe tandwielpictogram en selecteer "Enterprise Wipe". Opmerking: alleen beschikbaar met Android 4.x en lagere versies of op apparaten met de KNOX API (Samsung-apparaten).

Wachtwoord verwijderen (revisie x)	Het vastgestelde wachtwoord waarmee de gebruiker de apparaatbeheerder kan verwijderen Revisie x = teller, hoe vaak het wachtwoord al is gewijzigd Het is belangrijk welk wachtwoord de gebruiker nodig heeft, want het kan zijn dat het apparaat nog niet met de AppTec360 Server heeft gecommuniceerd en het nieuwste wachtwoord dus nog niet is doorgegeven.
Wachtwoord Geschiedenis	Als u op de blauwe knop ("Geschiedenis weergeven") klikt, kunt u de eerder ingestelde wachtwoorden bekijken.
Uitgebreide bescherming tegen verwijderen	Deze optie biedt bescherming tegen niet-SAFE-apparaten Zolang deze instelling geactiveerd is, is het niet mogelijk om de apparaatbeheerder eenvoudig te deactiveren.
De gebruiker vragen om geblokkeerde apps te verwijderen?	Indien mogelijk worden geblokkeerde Apps niet alleen geblokkeerd, maar ook automatisch verwijderd. De gebruiker wordt gevraagd om geblokkeerde Apps te verwijderen als automatische verwijdering niet mogelijk is.
Intelligent systeem App-blokkering	Als Whitelisting is ingeschakeld, blokkeert de Android MDM-client alle door de gebruiker geïnstalleerde apps. Schakel deze instelling in om alle startbare systeem-apps te blokkeren in de Whitelisting-modus.

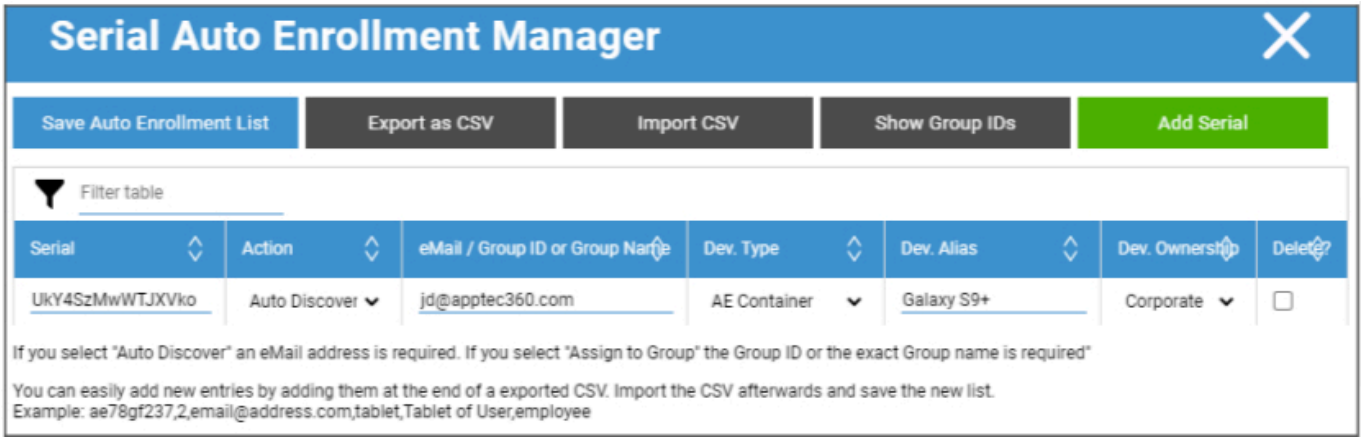
Automatische inschrijving

Hier kun je de functie Auto Enrollment inschakelen om je apparaten automatisch te registreren wanneer de AppTec360 MDM Client op het apparaat wordt geopend.

Belangrijk: Deze aanmeldingsmethode is deprecated en werkt niet meer op Android 10 of hoger. Hoe dan ook, als je Android 7 of hoger gebruikt, moet je apparaten sowieso aanmelden als Android Enterprise volledig beheerd. Als je de Android Enterprise BYOD-container wilt gebruiken en je gebruikt Android 10 of hoger, moet je het apparaat handmatig aanmelden via referenties, QR-code of sms. Hoe dan ook, de Auto Enrollment List wordt nog steeds gebruikt om het aanmeldingsproces te automatiseren voor bijvoorbeeld AE Enrollment, Knox Enrollment, enz.

Hoe dan ook, de Auto Enrollment List wordt nog steeds gebruikt om het aanmeldingsproces te automatiseren voor bijvoorbeeld AE Enrollment, Knox Enrollment, enz.

Door te klikken op "Serial Manager" of "IMEI Manager" kun je respectievelijk de Seriële of IMEI van je apparaten toevoegen. Het is niet nodig om beide apparaten toe te voegen, één is voldoende.



Actie bepaalt of de apparaten worden aangemeld bij de pool, een gebruiker of een groep.

Je kunt ook een .csv-bestand exporteren en importeren en je vermeldingen filteren op trefwoorden.

Android Onderneming

Hier kunt u Android Enterprise instellen. Dit is nodig om alle functies van Android Enterprise te kunnen gebruiken.

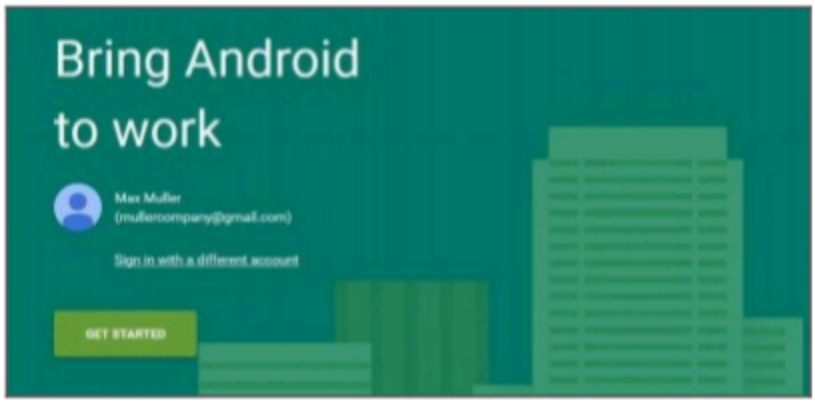
Eerste methode: Android Ondernemingsaccount (Google-account)

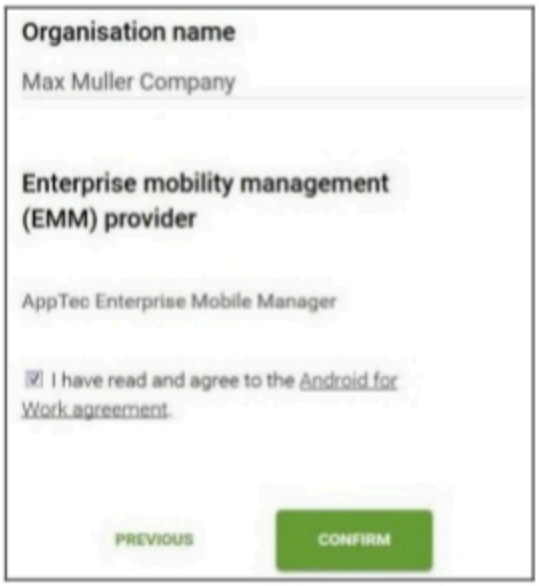
Druk eerst op "Prepare Setup" en na een kort moment zou er een knop "Start Setup" moeten verschijnen.

Dit brengt je naar de Android Enterprise Setup-pagina van Google.

Log in met het Google-account dat je wilt gebruiken, als je nog niet bent ingelogd en druk op "Aan de slag".

Nu kun je de naam van je bedrijf invoeren. Schakel daarna het selectievakje in en druk op "Bevestigen".





In de laatste stap kun je de registratie voltooien en zou je terug moeten keren naar de console. Als alles gewerkt heeft zou het er zo uit moeten zien:

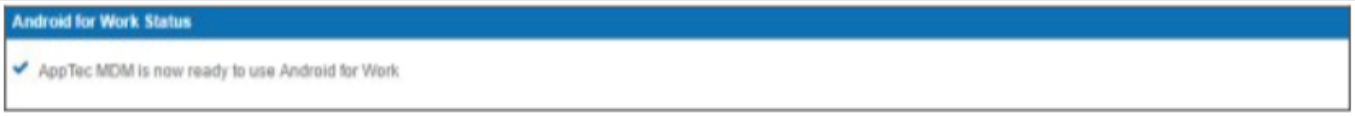
Nu kunt u beginnen met het configureren van uw Android Enterprise Container.

Tweede methode: G-Suite account

Druk op "Use G-Suite" en log in op je Google Admin Account. Daar ga je naar "Beveiliging" -> "Meer weergeven" -> "EMM-provider voor Android beheren" en genereer je een Token. Opmerking: Als je de Android Enterprise Settings niet ziet in je G-Suite-account, moet je naar "Get more apps and services" gaan en Android device management toevoegen. Voer nu het Token en uw primaire domein in onze console in en klik op "Wijzigingen opslaan". Wanneer u klaar bent, klikt u op "Android Enterprise-account gebruiken".

Nu zou je de knop "Serviceaccount aanmaken" moeten zien. Klik erop. Dit proces kan enkele ogenblikken duren.

Als alles werkte, zou het er zo uit moeten zien:



Nu kunt u beginnen met het configureren van uw Android Enterprise Container.

Bescherming tegen fabrieksreset

Met de Factory Reset Protection kun je je apparaat binden aan een google-account naar keuze, die ook een bestaande binding aan een google-account overschrijft. Om de beveiliging tegen fabrieksinstellingen te gebruiken, moet je deze eerst hier instellen en daarna activeren in je profielen.

Om de Factory Reset Protection in te stellen, klik je op "FRP Setup" en volg je de instructies op het scherm.

OPMERKING: Lees en voer de stappen zorgvuldig uit. We raden aan om dit in een nieuw incognitovenster te doen om te voorkomen dat je automatisch inlogt op het verkeerde Google-account. Je kunt jezelf volledig uitsluiten van het apparaat als je een verkeerde ID invoert of de toegang tot het gebruikte Google-account verliest!

AE Inschrijving

Hier kunt u de Android Enterprise Ernollment activeren. Als u deze methode gebruikt, worden uw apparaten ingeschreven in de Android Enterprise Device Owner Mode. In deze modus hebt u de volledige controle over het toestel.

AE-registratie inschakelen	Hiermee activeert u AE Enrollment Let op: Als u AE Enrollment uitschakelt, werken bestaande QR-codes en reeds geconfigureerde NFC programmeerapparaten niet meer. Als u AE Enrollment weer inschakelt, moet u NFC push configuraties opnieuw verzenden / nieuwe QR codes genereren.
Automatisch ontdekken inschakelen	Wanneer een apparaat zich aanmeldt via "AE Enrollment", zal het systeem proberen het toe te wijzen aan een gebruiker op basis van de informatie die is ingesteld in de Whitelist Serial / IMEI ("Algemene instellingen" > "Android-configuratie" > "Auto Enrollment").
Onbekende apparaten blokkeren	Alleen apparaten die zijn opgenomen in de whitelist voor seriële/IMEI-gegevens ("Algemene instellingen" > "Android-configuratie" > "Automatische registratie") kunnen worden geactiveerd.

Opmerking over methode 1 & 2: "Welkomstscherm" verwijst naar het eerste scherm dat je ziet na de fabrieksreset. Dit kan er anders uitzien afhankelijk van de Android-versie en/of het apparaatmodel dat je gebruikt.

Methode 1: QR Code Inschrijving

(vereist Android 7.0 of hoger) We raden aan om deze methode altijd te gebruiken als je Android 7 of hoger gebruikt.

1. Het apparaat resetten
2. Genereer de QR Code voor de inschrijving met een van de twee volgende methoden:
    - Klik in "Algemene instellingen -> Androidconfiguratie -> AE-registratie" op "QR-code genereren". Kies of u de opslagcodering wilt overslaan en/of alle systeemapps wilt verwijderen.
    - (Als alternatief) Kies een bestaand Apparaat. Klik in het "Apparaatoverzicht" op de QR-code die daar wordt weergegeven. Kies of je de opslagcodering wilt overslaan en/of alle systeemapps wilt verwijderen.
3. Tik nu 6 keer op het welkomstscherm van je apparaat. Dit zou de QR Inschrijvingsmodus moeten starten.
4. Maak nu verbinding met een draadloos netwerk en wacht even tot de QR-codelezer is geïnstalleerd
5. Scan nu de QR-code
6. Dat is het. Uw toestel is nu geregistreerd in de Android Enterprise Device Mode.

- a. Als je de QR-code hebt gebruikt in "Algemene instellingen" kun je je apparaat vinden in "Pool -> AE Device Owner Devices". (Tip: Het is mogelijk dat u de site opnieuw moet laden om de apparaten te zien). Als u "Enable Auto Discover" (Automatisch ontdekken inschakelen) hebt aangevinkt, kunt u het vinden in uw gebruiker voor automatische ontdekking.
- Als je de QR-code van een bestaand apparaatprofiel hebt gebruikt, wordt het apparaat in dit profiel geregistreerd.

Methode 2: NFC-registratie

(NFC en Android 6.0 of hoger vereist)

Voorbereiding: Voer uw WiFi-gegevens in bij "Algemene instellingen -> Android-configuratie -> AE-registratie -> Gegevens voor NFC provisioning". Gebruik nu "NFC Device" om het apparaat te zoeken dat de programmeur wordt. Dit apparaat zal worden gebruikt om de aanmeldingsinformatie via NFC naar de andere apparaten te sturen.

1. Fabrieksreset van je apparaat
2. Open de NFC-koppelapp van AppTec360 op je programmer
3. Kies of u de opslagcodering wilt overslaan en/of alle systeemapps wilt verwijderen.
4. Houd beide apparaten tegen elkaar
5. Nu moet de Android Enterprise-inschrijving grimmig
6. Je vindt je apparaat nu in de console
    - a. In de pool, als u Automatisch ontdekken niet hebt geconfigureerd
    - b. Binnen de gebruiker, die u hebt geconfigureerd voor de Auto Discover
    - c. Tip: Het is mogelijk dat je de site opnieuw moet laden om de apparaten te zien.

Methode 3: Google-account

(Android 5.1 of hoger vereist)

(Opmerking: Als je deze methode gebruikt, wordt het apparaat niet automatisch geregistreerd. In plaats daarvan moet je het handmatig aanmelden of het proces automatiseren door Auto Enrollment te gebruiken).

1. Fabrieksreset van je apparaat
2. Doorloop de installatiestappen totdat u kunt inloggen met een google-account
3. Voer "afw#apptec" in als Gebruikersnaam/Mail
4. Tik op "Volgende".
5. Uw apparaat is nu een Android Enterprise-apparaat

KNOX Inschrijving

Hier kunt u de KNOX Enrollment activeren en vindt u de informatie die u nodig hebt om een KNOX Enrollment Profile aan te maken in het KNOX Deployment Portal. U hebt een account bij het KNOX Deployment Portal nodig om dit te configureren en te gebruiken.

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

KNOX-registratie inschakelen	Activeert de KNOX-registratie. Let op: Als u KNOX Enrollment uitschakelt, werken bestaande MDM-profielen niet meer. Als u KNOX Enrollment weer inschakelt, moet u het veld "Custom JSON Data" van uw MDM-profiel bijwerken.
Automatisch ontdekken inschakelen	Wanneer een apparaat zichzelf registreert via "KNOX Enrollment" zal het systeem proberen het toe te wijzen aan een gebruiker op basis van de informatie die is ingesteld in de Whitelist Serial / IMEI ("Algemene instellingen" > "Android-configuratie" > "Automatische registratie").

1. Meld u aan bij de Samsung KNOX Mobile Enrollment Portal https://eukme.samsungknox.com/itadmin
2. Ga naar "MDM-profielen".
3. Klik op "Toevoegen".
4. Kies "Server URI niet vereist voor mijn MDM" en klik op "Volgende".
5. Maak nu een profiel aan met de informatie die wordt weergegeven in de beheerconsole

Dit KNOX Enrollment Profile kan nu rechtstreeks door Samsung op het toestel worden geïnstalleerd als je de toestellen rechtstreeks van Samsung koopt.

U kunt ook de KNOX Deployment App downloaden, inloggen met uw KNOX Deployment Account en het KNOX Enrollment Profile via NFC naar andere apparaten sturen.

Als het apparaat een KNOX Enrollment Profile heeft geïnstalleerd, zal het onze App downloaden en het apparaat registreren, als het een werkende internetverbinding heeft.

De registratie van apparaten via KNOX Enrollment kan worden gevonden in "Pool -> KNOX Enrollment", of binnen de gebruiker die u hebt opgegeven in de Auto Discover.

Zero-Touch

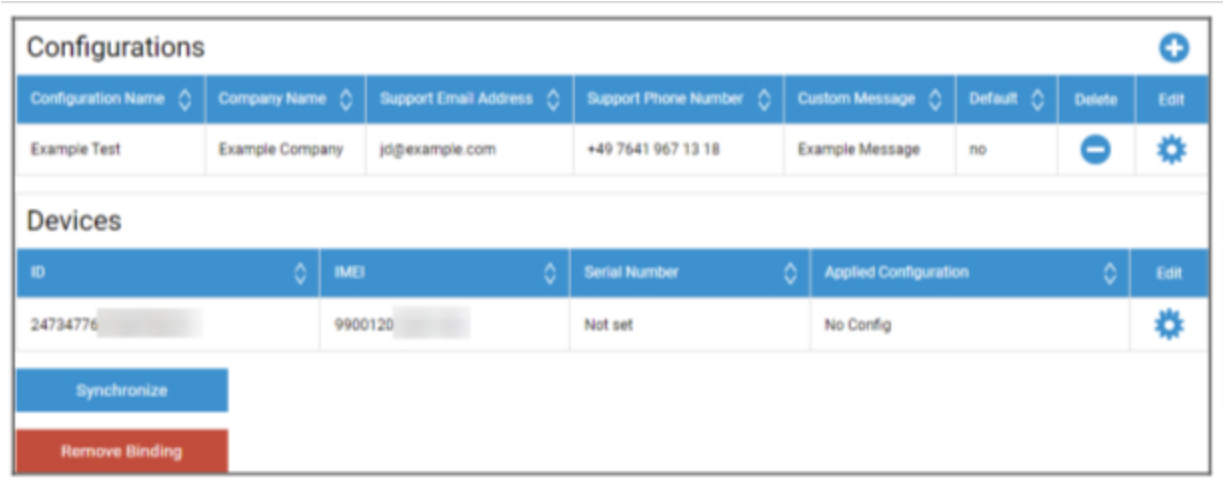
Met Zero-Touch kunt u uw apparaten eenvoudig aanmelden zonder dat u ze hoeft aan te raken of iets op het apparaat zelf hoeft te configureren. Je hoeft het alleen maar aan te zetten, de configuratie te doorlopen zoals gebruikelijk en het apparaat ontvangt volledig automatisch alle informatie over hoe het ingesteld en verbonden moet worden met de MDM.

Om Zero-Touch te kunnen gebruiken, moet u uw apparaten kopen bij een reseller die Zero-Touch ondersteunt. Dezelfde reseller maakt ook een account voor u aan in de Zero-Touch Portal. Neem contact op met uw reseller voor meer informatie over de procedure of als u problemen ondervindt bij het openen van de Zero-Touch Portal.

Klik op "Start Setup" om de setup te starten. Je wordt doorgestuurd naar een inlogpagina waar je je Google-account moet selecteren die toegang heeft tot de Zero-Touch Portal.

OPMERKING: het is mogelijk om ELKE account te selecteren. Zorg er dus voor dat je in deze stap de juiste account selecteert. Als u uw apparaten/configuraties niet ziet, hebt u waarschijnlijk de verkeerde account gebruikt.

Na het inloggen ziet het er als volgt uit:



Klik op de "+" om een configuratie toe te voegen en vul de velden in zoals weergegeven op het scherm. Als u de configuratie als standaardconfiguratie inschakelt, wordt deze automatisch toegewezen aan de nieuwe apparaten. Het aanmaken of instellen van een standaardconfiguratie wijst deze niet toe aan reeds bestaande apparaten.

Als aan een apparaat geen configuratie is toegewezen, wordt het ingesteld als een normaal apparaat en wordt er geen verbinding gemaakt met de MDM. Zorg er daarom voor dat er een configuratie is toegewezen aan uw apparaten.

Nadat je je account hebt verbonden, je apparaten zichtbaar zijn en je er een configuratie aan hebt toegewezen, kun je beginnen met het instellen van de apparaten.

Je kunt apparaten toevoegen aan de Auto Enrollment List zodat ze automatisch worden aangemeld bij een bepaalde groep of gebruiker. Als je niets configureert in de Auto Enrollment-lijst, worden apparaten ingeschreven in de Pool.

Windows Configuratie

Windows Configuratie

Hier heb je de optie om de volgende configuraties in te schakelen op je Windows 10 pc:

Directe DM-verbinding	
Initiële hersteltijd	Brengt de eerste verbindingspoging met het apparaat tot stand, deze waarde neemt exponentieel toe
Opnieuw proberen van verbinding	Geeft aan hoeveel verbindingspogingen de DM-client moet uitvoeren tijdens een verbindingsfout
Maximale slaaptijd	Geeft de maximale slaaptijd aan na een verbindingsfout
Eerste pogingen tot synchronisatie	Intervallen waarbinnen het apparaat moet communiceren met de server, na de eerste verbinding
Interval eerste nieuwe poging	Heeft betrekking op "Eerste pogingen tot synchroniseren". Hier worden de tijden in minuten weergegeven Bijvoorbeeld onder "First Sync Retries" staat de waarde "2" en onder "First Retry Interval" de waarde "4 Minutes", op deze manier communiceert het apparaat 2 keer om de 4 minuten, na de eerste verbinding.
Tweede pogingen tot synchronisatie	Intervallen waarmee het apparaat moet communiceren met de server, na het voltooien van de "First Sync Retries".
Tweede opnieuw proberen interval	Hetzelfde principe als bij "Eerste verlengingsinterval" - alleen geldt het hier voor "Tweede verlengingspogingen".
Regelmatig opnieuw synchroniseren	Intervallen, hoe vaak het apparaat in de toekomst met de server moet communiceren Standaard: "Oneindig We raden aan deze waarde niet te veranderen, want als je "10" invoert, communiceert het apparaat 10x met de server en stopt dan. De communicatie met de AppTec360-server wordt dan verbroken!
Regelmatig opnieuw proberen interval	Hetzelfde principe als bij "Eerste/Tweede terughaalinterval" - alleen worden hier de instellingen voor de toekomst toegepast.
Regelmatig opnieuw proberen interval	Hetzelfde principe als bij "Eerste/Tweede terughaalinterval" - alleen worden hier de instellingen voor de toekomst toegepast.

ContentBox

Configuratie

Hier kun je de ContentBox configureren. Je kunt bestanden voor groepen in de ContentBox plaatsen die toegankelijk zijn met de ContentBox App op het apparaat.

ContentBox inschakelen	ContentBox inschakelen. Als je deze uitschakelt als je ContentBox niet gebruikt, kun je resources besparen op OnPremise machines.
Externe ContentBox-installatie gebruiken	De ContentBox kan ook worden bediend met je eigen Nextcloud.
URL	Volledige URL van de Nextcloud-entiteit
Hoofdgebruiker	Hoofdgebruiker van het Nextcloud-account
Wachtwoord root	Rootwachtwoord van het Nextcloud-account
Standaardmachtigingen voor groepsmappen	Standaardmachtigingen voor groepsmappen, kunnen individueel worden gewijzigd per groep (in Mobile Management)
Groepsmap delen met subgroepen	Indien actief, kan elke subgroep alle mappen van de hoofdgroep lezen, kan ook individueel worden geconfigureerd voor elke groep (Mobile Management)
Rechten voor subgroepen	Rechten voor subgroepen kan individueel worden geconfigureerd voor elke groep (mobiel beheer)
Delen toestaan	Hiermee kan de gebruiker de inhoud delen via links, kan individueel worden geconfigureerd voor elke groep
Maximale bestandsgrootte bij uploaden in MB	Maximale grootte van een bestand Standaard: 512 MB Maximale configuratie: 2048
WebDAV referenties	
WebDAV URL	Je kunt de ContentBox ook openen met WebDAV. Verwijder de volgende mappen in geen geval: /apptecgroups /apptecgroups/AppTecGroup-X
Hoofdgebruiker	Naam van de hoofdgebruikers
Wachtwoord	Wachtwoord van de rootgebruikers

De synchronisatie met de ContentBox gebeurt automatisch. Je kunt echter een handmatige synchronisatie uitvoeren met "Synchroniseer ContentBox".

Bovendien kun je hier de ContentBox activeren/deactiveren op elk afzonderlijk apparaat.

Dit is alleen relevant als je de ContentBox niet aanvullend hebt gelicentieerd, dan heb je nog steeds toegang tot 25 apparaten waarmee je de ContentBox kunt testen - hier kun je dit voor de betreffende apparaten activeren.

LDAP-configuratie

LDAP-overzicht

Hier kun je een verbinding maken met je Active Directory via LDAP om gebruikers en groepen massaal te importeren. De synchronisatie moet handmatig worden uitgevoerd. Je kunt meerdere LDAP-verbindingen configureren naar verschillende systemen of met verschillende configuraties/filter.

Naam server	De weergavenaam van de server
Type	Momenteel worden alleen Active Directories ondersteund die LDAP ondersteunen
LDAP-domein	Het primaire LDAP-domein (bijv. example.com)
LDAP Host	Alleen nodig als de LDAP-host niet bereikbaar is onder het opgegeven LDAP-domein.
Haven	Leeg laten om standaardpoort te gebruiken (389 of 636 voor SSL)
Gebruikersnaam	Bijv. CN=John,OU=Users,DC=EXAMPLE,DC=COM Opmerking: De meeste systemen hebben de gebruikersnaam in deze indeling nodig en accepteren "John" niet als gebruikersnaam.
Wachtwoord	
Wachtwoord bevestigen	
Verbindingsbeveiliging	Let op: bij gebruik van SSL of TLS wordt het certificaat van de Active Directory gecontroleerd. Als dit zelfondertekend is, moet je de root-CA toevoegen aan de vertrouwensopslag van de OnPremise Machine. Als je in de Cloud zit, moet de Active Directory een vertrouwd certificaat leveren, anders werkt de verbinding alleen zonder encryptie.
Automatische synchronisatie.	Schakelt de automatische synchronisatie van de LDAP-directory in met het tijdsinterval dat is opgegeven in de algemene LDAP-instellingen.
Basis DN	Als je niet de hele map wilt synchroniseren, kun je hier een OU opgeven. Bijv. OU=AndroidUsers,OU=Users,DC=EXAMPLE,DC=COM
Lid van	Alle geïmporteerde gebruikers worden toegevoegd aan de geselecteerde groep
Alleen geactiveerde gebruikers?	Als dit is ingeschakeld, wordt het kenmerk userAccountControl in aanmerking genomen, gebruikers zonder dit kenmerk worden niet geïmporteerd.

LDAP-filter	Je kunt LDAP-filter gebruiken om te filteren welke gebruikers worden geïmporteerd
Regex filter	Je kunt een Regex-filter gebruiken om te filteren welke gebruikers worden geïmporteerd
Testaansluiting	Test de verbinding bij het opslaan van de configuratie
Mapstructuur resetten bij synchronisatie?	Als dit waar is, worden alle LDAP-vermeldingen terugverplaatst naar hun oorspronkelijke locatie in de LDAP-structuur. Aanbevolen om in te schakelen.
Verwijderde gebruikers en groepen opnieuw importeren?	Indien ingeschakeld, worden verwijderde gebruikers en groepen opnieuw aangemaakt. Aanbevolen om in te schakelen.
Verwijderen synchroniseren?	Indien ingeschakeld, worden groepen en gebruikers verwijderd wanneer ze worden verwijderd op de LDAP-server. Ook apparaten van verwijderde gebruikers worden verwijderd.

Onder de lijst van je LDAP-configuraties kun je de periode definiëren waarin het systeem automatisch synchroniseert. Gebruikt alleen de LDAP-configuraties voor automatische synchronisatie waarvoor de betreffende optie is geactiveerd.

App-beheer

Eigen app DB

Android

Hier kun je de Android Apps uploaden die je bedrijf heeft ontwikkeld en ze later distribueren in Mobile Management in apparaat- of groepsprofielen.

Houd er rekening mee dat we adviseren om op deze manier alleen Apps te distribueren die niet beschikbaar zijn in de Google Play Store.

Klik op de "+" om de APK van een App die je wilt uploaden te uploaden. Momenteel wordt alleen het APK-formaat ondersteund.

De uploadlimiet op OnPremise Appliances kan worden verhoogd in Stap 3 van de Appliance Configuratie. Als u de uploadlimiet op Cloud wilt verhogen, neem dan contact op met de support voor meer informatie.

Houd er rekening mee dat APK's meestal iets kleiner zijn dan hun inhoud. Het is mogelijk dat een upload hierdoor mislukt, omdat de APK tijdens het proces wordt uitgepakt. Het is bijvoorbeeld mogelijk dat een APK van 95 MB mislukt bij een uploadlimiet van 100 MB. Verhoog in dit geval de uploadlimiet zoals hierboven vermeld.

We adviseren ook om de APK eerst handmatig naar een testapparaat te verplaatsen (bijvoorbeeld via USB) en te proberen deze handmatig te installeren met de Bestanden-app van het apparaat. Als dit om wat voor reden dan ook niet werkt, zal het ook niet lukken via MDM.

Doel bijwerken

Met de functie "Doel bijwerken" kun je kiezen welke versie van een app moet worden geïnstalleerd of naar welke versie een app moet worden bijgewerkt als je "Up-to-date houden" voor een app hebt geactiveerd.

Als je geen updatetarget hebt geselecteerd, wordt de hoogste versie gebruikt.

Houd er rekening mee dat Android apps niet kan downgraden. Houd er ook rekening mee dat de "Versiecode" bepaalt of een versie hoger, lager of hetzelfde is. Zorg er dus voor dat je deze versie correct verhoogt in je app wanneer je een update bouwt.

iOS

Hier kun je de iOS Apps die je hebt ontwikkeld uploaden en later distribueren in Mobile Management in je apparaat- of groepsprofiel.

Klik op de "+" om de IPA te uploaden van een App die je wilt uploaden. Vanaf nu wordt alleen het IPA-formaat ondersteund.

De uploadlimiet op OnPremise Appliances kan worden verhoogd in Stap 3 van de Appliance Configuratie. Als u de uploadlimiet op Cloud wilt verhogen, neem dan contact op met de support voor meer informatie.

Doel bijwerken

Met de functie "Doel bijwerken" kun je kiezen welke versie van een app moet worden geïnstalleerd of naar welke versie een app moet worden bijgewerkt als je "Up-to-date houden" voor een app hebt geactiveerd.

Als je geen updatetarget hebt geselecteerd, wordt de hoogste versie gebruikt.

MacOS

Hier kun je de MacOS Apps die je hebt ontwikkeld uploaden en later distribueren in Mobile Management in je apparaat- of groepsprofiel.

Klik op de "+" om de PKG van een App die je wilt uploaden te uploaden. Vanaf nu wordt alleen het PKG-formaat ondersteund.

De uploadlimiet op OnPremise Appliances kan worden verhoogd in Stap 3 van de Appliance Configuratie. Als u de uploadlimiet op Cloud wilt verhogen, neem dan contact op met de support voor meer informatie.

Doel bijwerken

Met de functie "Doel bijwerken" kun je kiezen welke versie van een app moet worden geïnstalleerd of naar welke versie een app moet worden bijgewerkt als je "Up-to-date houden" voor een app hebt geactiveerd.

Als je geen updatetarget hebt geselecteerd, wordt de hoogste versie gebruikt.

Windows 10

Hier kun je de Windows 10 Apps uploaden en later distribueren in Mobile Management in je apparaat- of groepsprofiel.

Klik op de "+" om de APPX, APPXBUNDLE of MSI van een App die je wilt uploaden te uploaden. Vanaf nu wordt alleen het APPX, APPXBUNDLE of MSI formaat ondersteund.

Je kunt ook afhankelijkheden uploaden en definiëren voor een App, die automatisch worden gedistribueerd en geïnstalleerd voordat de gewenste App wordt geïnstalleerd.

De uploadlimiet op OnPremise Appliances kan worden verhoogd in Stap 3 van de Appliance Configuratie. Als u de uploadlimiet op Cloud wilt verhogen, neem dan contact op met de support voor meer informatie.

Doel bijwerken

Met de functie "Doel bijwerken" kun je kiezen welke versie van een app moet worden geïnstalleerd of naar welke versie een app moet worden bijgewerkt als je "Up-to-date houden" voor een app hebt geactiveerd.

Als je geen updatetarget hebt geselecteerd, wordt de hoogste versie gebruikt.

Win32-pakket (.exe)

Je kunt ook .exe-bestanden/installateurs naar je apparaten distribueren.

Naam verpakking	De naam die wordt weergegeven in de MDM
Beschrijving	Beschrijving weergegeven in de MDM
Pakketbestand	Alleen .zip-bestanden zijn toegestaan. Plaats de bestanden die je wilt implementeren in dit zipbestand.
Inzetcontext	**Systeem**: Het installatiecommando wordt uitgevoerd met systeemrechten, wat hoger is dan "Gebruiker". Ook wanneer "System" wordt gebruikt, heeft het proces geen UI, dus het zal stil zijn en het gebruikersprofiel, bijvoorbeeld omgevingsvariabelen zoals %AppDat%, is niet toegankelijk. **User**: Het installatiecommando heeft toegang tot het gebruikersprofiel en kan indien nodig UI weergeven. Opmerking: Sommige processen werken maar in één context. Als een software zichzelf bijvoorbeeld installeert in AppData, zal het alleen werken als "Gebruiker" wordt geselecteerd.
Opdracht installeren	De opdracht die wordt gebruikt om het programma te installeren. Bijvoorbeeld het installatiecommando voor een zipbestand met "setup.exe" in de root, dat de parameter "/s" ondersteunt voor een stille installatie, zou het installatiecommando "setup.exe /s" zijn. Houd er rekening mee dat verschillende software verschillende parameters kan hebben.
Opdracht verwijderen	De opdracht die moet worden uitgevoerd om de software via MDM te verwijderen. Meestal wijst dit naar het verwijderprogramma. Bijvoorbeeld "C:\Program Files\ExampleSoftware\uninstall.exe".
Vereisten	
Opmerking: De software kan alleen worden geïnstalleerd als aan alle vereisten is voldaan. Anders wordt de software niet geïnstalleerd. Sommige velden kunnen verplicht zijn. Als er voor een vereiste geen waarde is ingesteld, wordt de vereiste genegeerd.	
OS-architectuur	OS-architectuur
Minimale OS-versie	Minimale OS-versie
Minimale vrije schijfruimte (MB)	Minimale vrije schijfruimte (MB)
Min fysiek geheugen (MB)	Min fysiek geheugen (MB)
Minimaal aantal logische processors	Minimaal aantal logische processors

Min CPU-snelheid (MHz)	Min CPU-snelheid (MHz)
Aanvullende vereisten	Je kunt hier ook handmatig regels definiëren of een script uploaden om extra vereiste controles uit te voeren als je dat wilt.
Detectieregels	
Detectiemethode	Hier kun je definiëren hoe wordt gedetecteerd of de app is geïnstalleerd op het apparaat. Installeeropdrachten worden alleen uitgevoerd als deze regels detecteren dat de app NIET is geïnstalleerd. Deïnstalleeropdrachten worden alleen uitgevoerd als deze regels detecteren dat de app niet is geïnstalleerd. **Regels handmatig definiëren**: Hiermee kun je handmatig een of meer regels definiëren om bijvoorbeeld te controleren of een bepaald bestand, map, MSI of registersleutel aanwezig is. Als alle opgegeven detectieregels waar zijn, wordt de app als aanwezig beschouwd. **Script gebruiken**: Upload je eigen script met je eigen controles. Als het script "$TRUE" retourneert, wordt de app als aanwezig beschouwd.
Detectieregels	

App-instellingen

Instellingen iOS-app

Hier kun je de standaardinstellingen definiëren voor het toevoegen van een app aan de verplichte apps of enterprise app store.

Opmerking: Hiermee wordt alleen ingesteld wat standaard is geselecteerd bij het toevoegen van apps. Bestaande instellingen voor apps die al zijn toegevoegd in de verplichte apps of enterprise app store worden hierdoor NIET gewijzigd.

Blijf op de hoogte	Houdt de app automatisch up-to-date. Houd er rekening mee dat het tot 7 dagen na het uitkomen van een update kan duren voordat de app is bijgewerkt.
Inhalen wanneer onbeheerd	Als een app al is geïnstalleerd als onbeheerd (door de gebruiker), wordt de app ingehaald en beheerd door de MDM.
App verwijderen wanneer MDM-profiel wordt verwijderd	Verwijdert de app wanneer de MDM wordt verwijderd.
Voorkom back-up van de app-gegevens	Voorkomt de back-up van de app-gegevens.

Instellingen Android-app

Hier kun je de standaardinstellingen definiëren voor het toevoegen van een app aan de verplichte apps of enterprise app store.

Opmerking: Hiermee wordt alleen ingesteld wat standaard is geselecteerd bij het toevoegen. Dit wijzigt NIET de instellingen voor apps die al zijn toegevoegd in de verplichte apps of enterprise app store.

Blijf op de hoogte	Houdt de app automatisch up-to-date. Alleen beschikbaar voor InHouse Apps.
Gecontroleerde update voor AppTec360 EMM-client	Indien ingeschakeld kunnen Admins het updatedoel voor de AppTec360 EMM Client specificeren. Een lijst van alle beschikbare versies van de AppTec360 EMM Client wordt getoond in "Algemene Instellingen" → "App Management" → "In-House App DB" → "Android".

Apps van derden

Android

Hier kun je je activeringscode voor Ikarus instellen.

Stel dit in op "Gebruik activeringscode" en voer hier je activeringscode in.

Opmerking: Nadat je de code hebt ingevoerd en opgeslagen, is de code nog niet toegevoegd aan het profiel dat naar het apparaat wordt verzonden. Je moet een wijziging uitvoeren in je profiel om de code toe te voegen aan het profiel. Wijzig bijvoorbeeld een schakelaar in het profiel van Uit → Aan → Uit - Opslaan → Nu toewijzen.

iOS

Hier kunt u uw SecurePIM licentie invoeren. Na het invoeren van de licentie drukt u op "Wijzigingen opslaan" en kunt u de SecurePIM opties gebruiken.

VPP / KNOX Premium

Met Apples Volume Purchase Program (VPP) kun je eenvoudig betaalde en gratis Apps distribueren naar je apparaten. Dit is een aanrader omdat je geen Apple ID nodig hebt op de apparaten, gebruikers de installatie niet hoeven te bevestigen (onder toezicht), gebruikers het wachtwoord van de Apple ID niet hoeven in te voeren en je eenvoudig betaalde Apps kunt distribueren zonder ze op elk apparaat opnieuw te kopen.

Om VPP te gebruiken, moet je je registreren in de Apple Business Manager.

VPP-licenties

Hier krijg je een overzicht van je VPP Apps, hoeveel licenties er worden gebruikt en hoeveel er nog beschikbaar zijn.

Als je op het wiel klikt, kun je zien aan welke apparaten een licentie is toegewezen en wat de status van deze toewijzing is.

Als je op klikt, wordt de VPP Cache vernieuwd en worden de licenties die zijn toegewezen in de MDM vergeleken met de licenties die zijn toegewezen aan Apples kant. Dit kan in sommige gevallen licentieproblemen oplossen.

VPP Penning

Hier kun je je VPP-token uploaden, die je kunt vinden in de Apple Business Manager onder Instellingen → Apps & Boeken. Je kunt meerdere VPP-tokens uploaden.

Je kunt een Token vernieuwen door simpelweg een nieuw Token te downloaden in de Apple Business Manager, op het "Bewerk" wiel te klikken en het nieuwe Token te uploaden.

De "VPP Mode" bepaalt hoe de licentietoewijzing wordt afgehandeld. Afhankelijk van je scenario moet je verschillende modi gebruiken:

"Apparaat gebaseerd" moet worden gebruikt bij het registreren van de apparaten via QR Code, Link, Apple Configurator of DEP.

"Gebaseerd op gebruiker" is vereist als de apparaten zijn geregistreerd met de Gebruikersregistratie of als Gedeelde iPad.

Als u "Geautomatiseerd licentiebeheer" inschakelt, krijgen gebruikers die van de ene groep naar de andere worden verplaatst automatisch Apple VPP-licenties toegewezen op basis van het groepsprofiel waarnaar ze worden verplaatst.

Bestaande Apple VPP-licenties van de groep waarvan ze zijn verhuisd, worden niet ingetrokken.

Nieuwe gebruikers die aan een groep worden toegevoegd, krijgen automatisch Apple VPP-licenties toegewezen op basis van het respectievelijke groepsprofiel.

KNOX Premium sleutel

Hier kunt u uw KNOX Premium Key invoeren om de Samsung KNOX Container te gebruiken.

Houd er rekening mee dat dit niet langer wordt ondersteund sinds Android 10. Gebruik in plaats daarvan de Android Enterprise Container.

App Store-instellingen

Regio & Taal

Hier kunt u de standaard Taal en Regio instellen voor de App Search in het App Management.

Houd er rekening mee dat de instelling voor iTunes ook bepaalt hoe het systeem informatie over bepaalde apps verzamelt. Als u Apps in uw lijsten tegenkomt die op een vreemde manier worden weergegeven (bijvoorbeeld een ontbrekend pictogram), hebt u misschien een regio ingesteld waar de specifieke App niet beschikbaar is.

AE Play Store

Hier vind je alle opties voor de Play Store voor Android Enterprise Devices om Apps goed te keuren, eigen Apps te uploaden naar de Play Store of je eigen Web Apps te maken.

Goedgekeurde apps

Hier krijgt u een overzicht van alle Apps die u hebt goedgekeurd.

Apps uit de Play Store

Dit laadt een iFrame met de Play Store. Zoek een App die je wilt, klik erop en keur hem goed. Tijdens het goedkeuren van de App kun je ook instellen dat de goedkeuring wordt ingetrokken als de vereiste machtigingen veranderen. We raden aan om deze instellingen standaard te laten bij het goedkeuren van Apps.

Nadat een App is goedgekeurd, kun je deze toevoegen aan je profielen.

De knop "Goedkeuren" verandert na het goedkeuren in "Goedkeuring intrekken", zodat je de Apps altijd kunt verwijderen als je ze niet meer nodig hebt.

Privé toepassingen

Hier kun je je eigen App als privé App uploaden naar de Google Play Store. Hierdoor kun je de App via Googles Services distribueren en updaten. Dit heeft ook als voordeel dat je eigen Apps geïnstalleerd kunnen worden zonder bevestiging van de gebruiker, wat normaal wel nodig is.

Webtoepassingen

Hier kun je Web Apps maken, dat zijn links naar bepaalde webpagina's die kunnen worden toegewezen als Apps.

Je kunt dit ook een aangepast pictogram geven en verder definiëren hoe het precies wordt weergegeven.

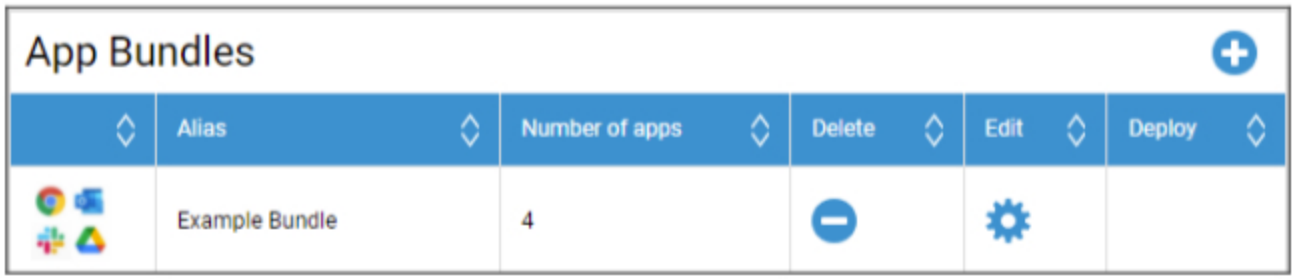
Winkelindeling

De Store-indeling bepaalt hoe apps worden weergegeven in de Play Store en of ze überhaupt worden weergegeven.

Houd er rekening mee dat als je apps in de Play Store wilt weergeven die de gebruiker handmatig kan installeren, deze hier in de lay-out moeten worden toegevoegd **EN** in het profiel aan de Enterprise Play Store. Als je een app slechts aan één van beide toevoegt, wordt deze niet weergegeven.

Bundel apps

Met App Bundles kun je groepen apps definiëren die met één klik kunnen worden toegewezen aan apparaat- of groepsprofielen.



Klik op de "+" om een nieuwe App Bundle te maken. Nadat je een App Bundle hebt gemaakt, kun je op "Bewerken" klikken om apps van verschillende bronnen aan de Bundle toe te voegen.

Een bundel kan net als elke andere app worden toegevoegd aan profielen. Als je apps toevoegt, krijg je een extra tabblad met de naam "App Bundles" waar je je bundels kunt plaatsen.

Als je een wijziging aanbrengt in een App Bundle, verschijnt er een knop in de kolom "Deploy". Hiermee kun je deze wijzigingen pushen naar alle profielen die deze bundel bevatten. Houd er dus rekening mee dat je dit handmatig moet doen na het toevoegen of verwijderen van apps in een bundel.

Afstandsbediening

TeamViewer

TeamViewer Aansluiting

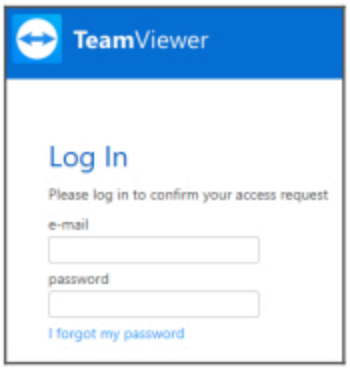
Opmerking: In de gratis proefversie van onze cloudversie kunt u geen verbinding maken met uw TeamViewer-account. In plaats daarvan wordt automatisch een gratis demo-account gekoppeld.

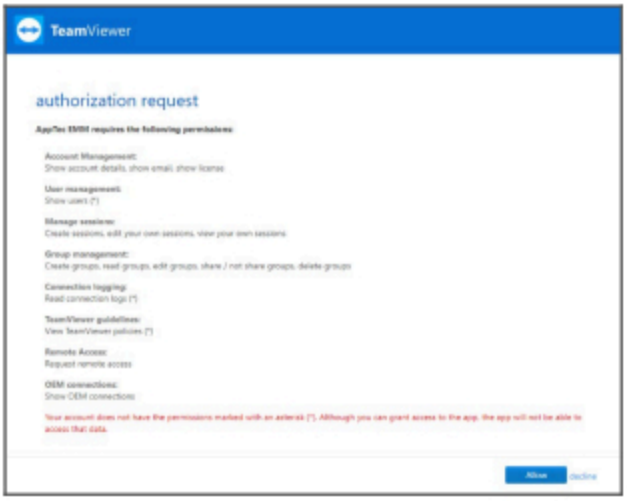
Ga naar Algemene instellingen -> Afstandsbediening -> TeamViewer. Hier kunt u uw TeamViewer-account koppelen aan de console of informatie bekijken over uw momenteel verbonden account. U kunt ook alle momenteel actieve sessies bekijken als u naar "Active Sessions" gaat.

Om je account te koppelen klik je op "Start Setup".

Als u dit doet, wordt u doorgestuurd naar een nieuwe pagina waar u moet inloggen met uw TeamViewer account.

Na het inloggen moet je AppTec360 MDM machtigen om dit account te gebruiken. Na bevestiging moet je een paar seconden wachten en is het account verbonden.


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


TeamViewer
authorization request

TeamViewer QuickSupport installeren

Voeg de app "TeamViewer QuickSupport" toe aan de verplichte apps van uw apparaatprofiel of groepsprofiel en klik op "Assign Now". Wacht tot de app is geïnstalleerd op het apparaat.

Als je toegang probeert te krijgen tot een apparaat waarop de app niet is geïnstalleerd, wordt deze geïnstalleerd of wordt er gevraagd om de app te installeren, afhankelijk van de configuratie van het apparaat.

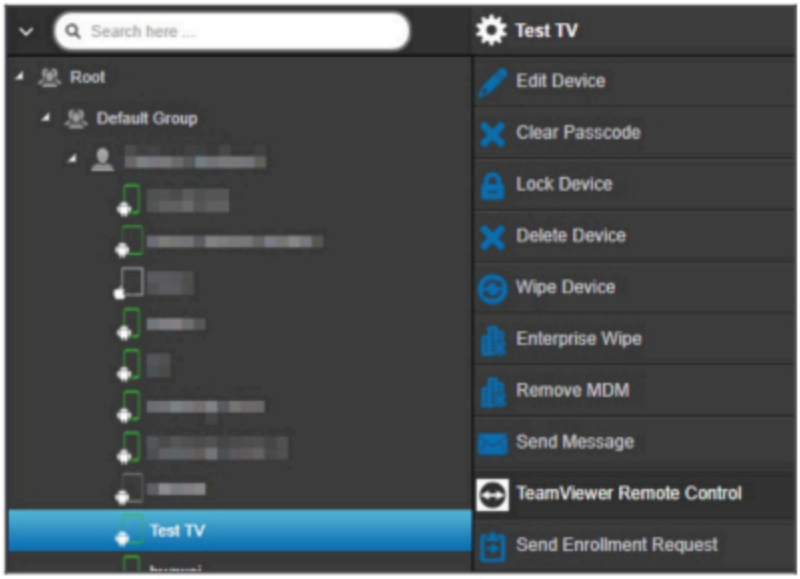
Uw apparaat op afstand bedienen

Om uw apparaat op afstand te bedienen, selecteert u het apparaat, klikt u op het wiel en kiest u "TeamViewer Remote Control".

Als er al een actieve sessie is, kun je de oude sessie gebruiken of een nieuwe aanmaken.

Bevestig dat u een nieuwe TeamViewer Sessie wilt maken.

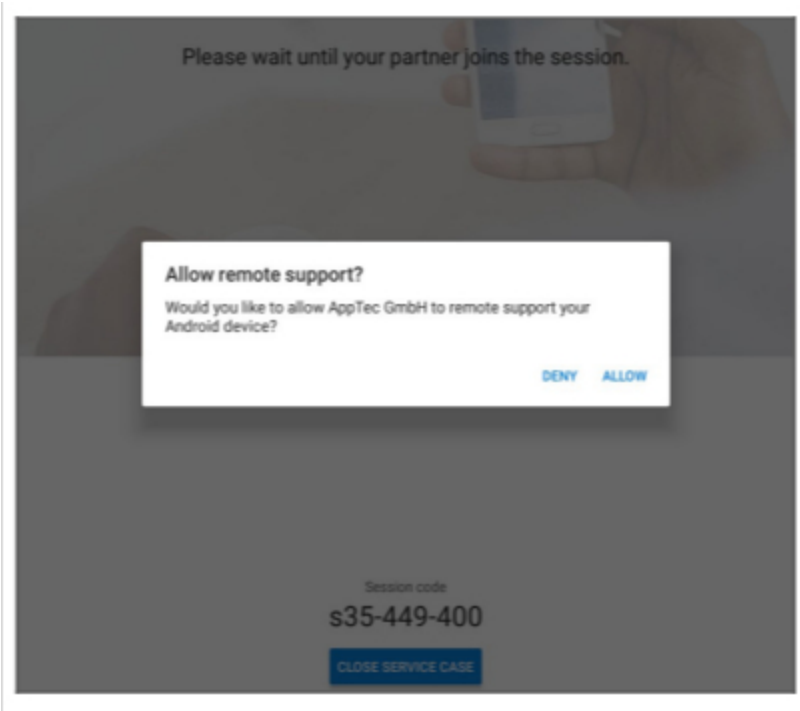
Na een paar seconden krijgt u een koppeling voor uw TeamViewer Sessie. U kunt op "Start" klikken om deze koppeling in een nieuw venster te openen.


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

Deze koppeling opent uw geïnstalleerde TeamViewer en verbindt u met uw apparaat.

Nu moet je de verbinding op het apparaat zelf bevestigen om het op afstand te kunnen bedienen.

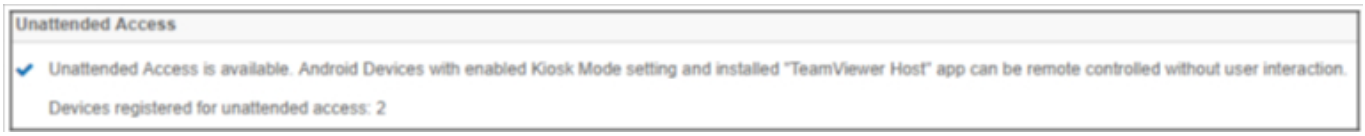


Als je iOS gebruikt krijg je een melding in de AppTec360 MDM Client. Met die link voegt het apparaat zich bij de sessie op afstand. Afhankelijk van de notificatie-instellingen van het apparaat is het mogelijk dat je geen notificatie ontvangt en de AppTec360 MDM Client handmatig moet openen.

Op sommige Android-toestellen (bijv. Samsung) is het nodig om een extra app te installeren als addon. De TeamViewer app op het apparaat zal u hierover informeren, als dit nodig is op uw apparaat.

Toegang zonder toezicht

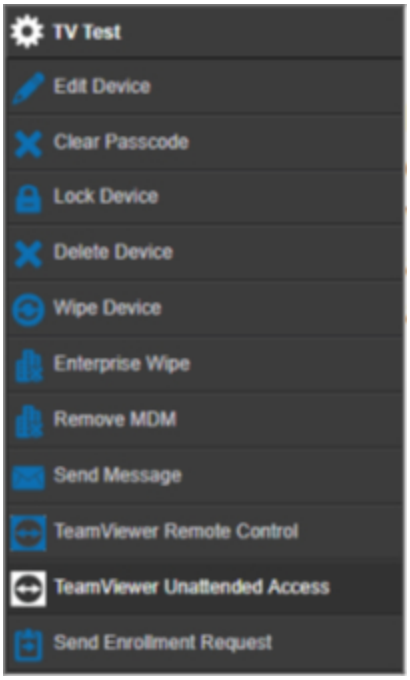
Opmerking: onbeheerde toegang is alleen mogelijk op Android-apparaten.



U kunt alleen verbinding maken met uw apparaten, zonder de verbinding op het apparaat te accepteren, als uw TeamViewer Account een "Tensor" of "Corporate" Licentie gebruikt.

Je kunt dit, na het koppelen van je account, controleren in "Algemene instellingen".

Om onbeheerde toegang te gebruiken, moet u de app "TeamViewer Host" installeren en "Enable Unattended Access" (onbeheerde toegang inschakelen) onder "Kiosk Mode & Launcher" (Kioskmodus & launcher) in uw profiel activeren. Houd er rekening mee dat dit alleen mogelijk is als u de Kiosk-modus gebruikt.



Nu kun je de onbeheerde toegang selecteren als je je apparaat selecteert en op het wiel klikt. Dit verbindt je met je apparaat zonder dat je een bevestiging op het apparaat zelf nodig hebt. Houd er rekening mee dat het even kan duren voordat je de link krijgt om toegang te krijgen tot je apparaat.

Splashtop

Als u de Splashtop-optie inschakelt, ziet u de Splashtop-configuratieopties in uw profielen.

Om Splashtop te gebruiken, moet je Splashtop Streamer (com.splashtop.streamer.csrs) instellen als verplichte app in je profiel. Daarna kun je de Splashtop-configuratie inschakelen in je profiel onder "Afstandsbediening". Als u dit inschakelt, wordt de Splashtop Streamer-app geconfigureerd. Als u Splashtop Streamer gebruikt, maar niet in combinatie met MDM, moet u dit uitschakelen.

In uw profiel onder "Afstandsbediening" moet u ook een deploy code instellen. Ga naar https://my.splashtop.com en log in op uw Splashtop-account. Klik op "Computer toevoegen" en kopieer de 12-cijferige deploy code van de resulterende pagina.

Zonder de Deploy Code is afstandsbediening NIET mogelijk.

Nadat u dit hebt gedaan, kunt u met de rechtermuisknop op uw apparaat klikken en een sessie op afstand starten door op "Splashtop afstandsbediening" te klikken.

Simkaart beheer

CSV importeren in bulk

Dit toont een overzicht van je toegewezen Simkaarten en alle informatie daarover. Dit helpt je om alle informatie, niet alleen over je apparaten maar ook over je Simkaarten in één systeem te hebben.

OPMERKING: Dit is handmatig beheer/documentatie. Het is niet mogelijk om deze gegevens automatisch van apparaten te krijgen vanwege privacy-/beveiligingsmechanismen van de besturingssystemen.

Je kunt deze lijst ook ex- en importeren als CSV.

Vervoerder & Tarief

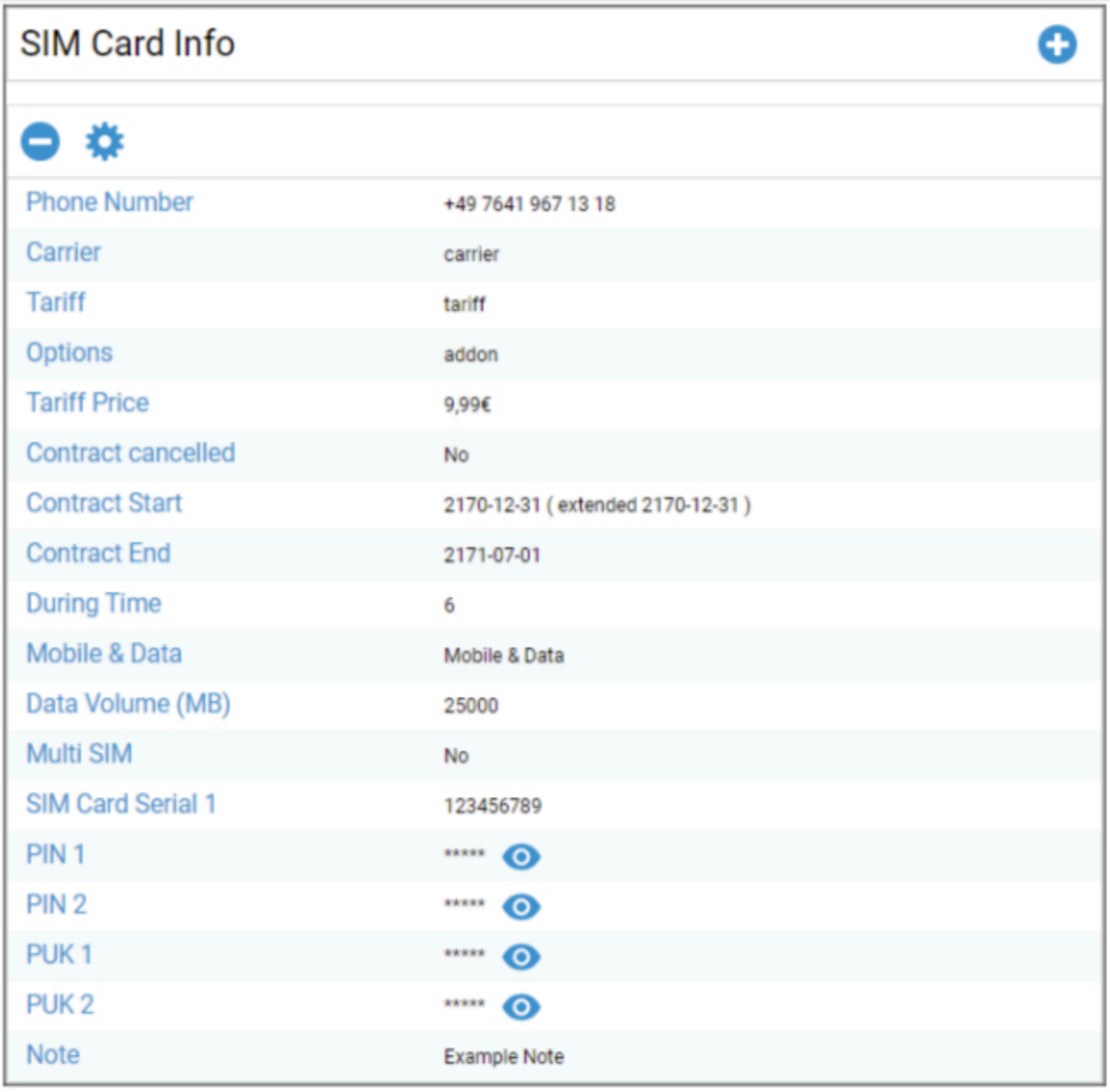
Om een simkaart toe te voegen, klik je eerst op de knop om één of meerdere carriers toe te voegen.

Klik daarna op de "+" bij "Tariefinformatie" om een tarief aan een vervoerder toe te voegen.

Optioneel kun je hieronder Add-Ons toevoegen als je zoiets hebt.

Dit bereidt alles voor wat je nodig hebt om een Simkaart toe te voegen. Simkaarten zijn momenteel toegewezen aan een Gebruiker. Ga daarom naar Mobielbeheer, selecteer een Gebruiker en ga naar "Simkaartoverzicht".

Hier zie je de Simkaarten van deze gebruikers. Als er een is, kun je deze bewerken of verwijderen. Gebruikers kunnen meerdere Simkaarten hebben.

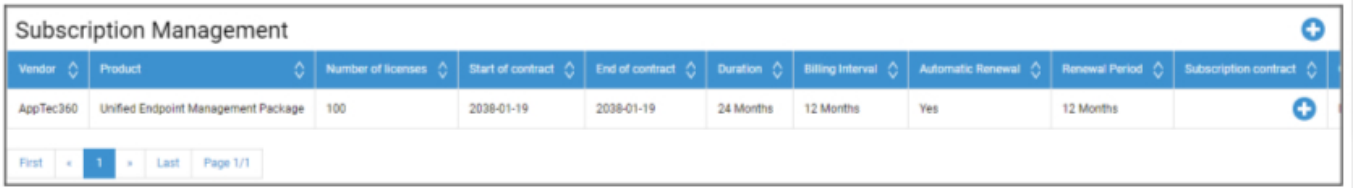


Klik op de "+" om een Simkaart toe te voegen en voeg alle benodigde informatie toe. Deze Simkaarten worden ook weergegeven in de lijst met al je Simkaarten in Algemene instellingen → Simkaartbeheer.

Abonnementenbeheer

Abonnementenbeheer

Hier kun je lopende abonnementen en hun details documenteren en ook verschillende bestanden opslaan, zoals ondertekende contracten, opzegbrieven, enz. Je kunt ook herinneringen instellen die je er per e-mail aan herinneren voordat het abonnement afloopt en misschien automatisch wordt verlengd.



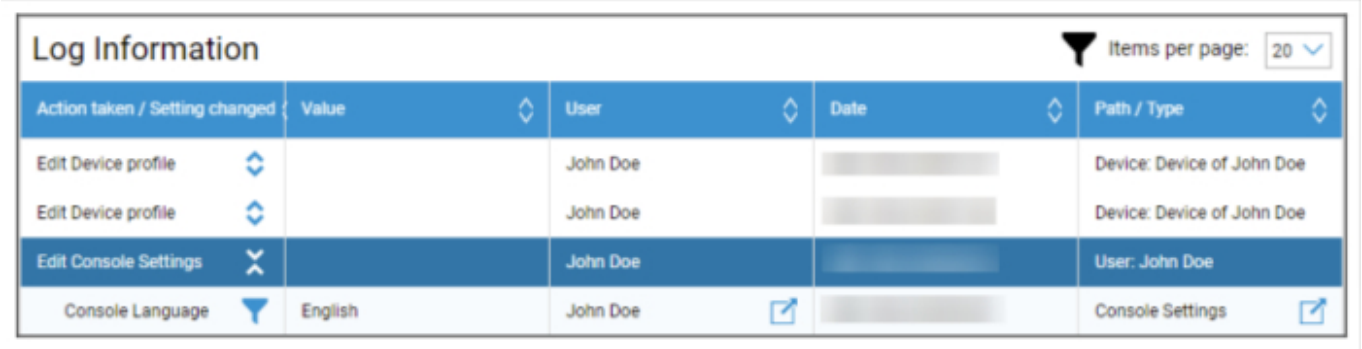
Klik op de "+" bovenaan om een abonnement toe te voegen. Je kunt zoveel abonnementen toevoegen als je wilt.

Klik op de "+" in de verschillende velden om bestanden met betrekking tot dit Abonnement te uploaden. Technisch gezien kun je elk bestandstype uploaden, maar houd er rekening mee dat niet elk bestandstype kan worden bekeken in de browser.

Algemeen controlelogboek

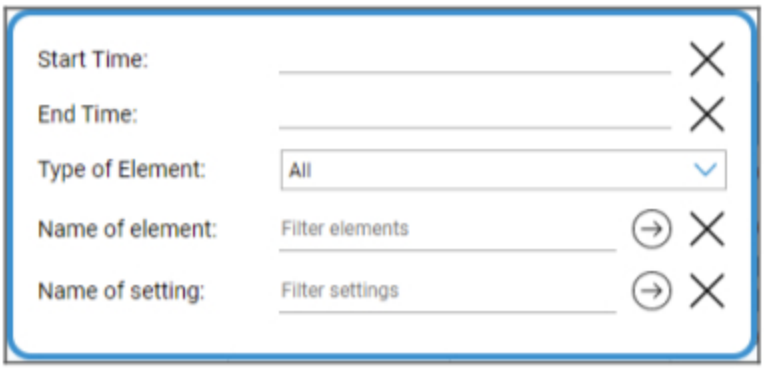
Controlelogboek

Hier heb je een algemeen Audit Log dat alle gemaakte wijzigingen laat zien. Terwijl het Audit Log bij een gebruiker of groep alleen wijzigingen laat zien voor deze gebruiker of groep, laat dit ELKE wijziging zien die waar dan ook in de console is gemaakt.



Je kunt zien wat er is gewijzigd, door wie, wanneer en waar. In sommige gevallen kun je de Entry ook uitbreiden om meer details te zien.

Het is mogelijk om op de gebruiker of op het item in "Pad / Type" te klikken om naar de locatie te gaan waar de wijziging is gemaakt.



Rechtsboven kun je ook een filter definiëren die kan helpen om bepaalde wijzigingen te vinden in een omgeving waar veel wijzigingen plaatsvinden.

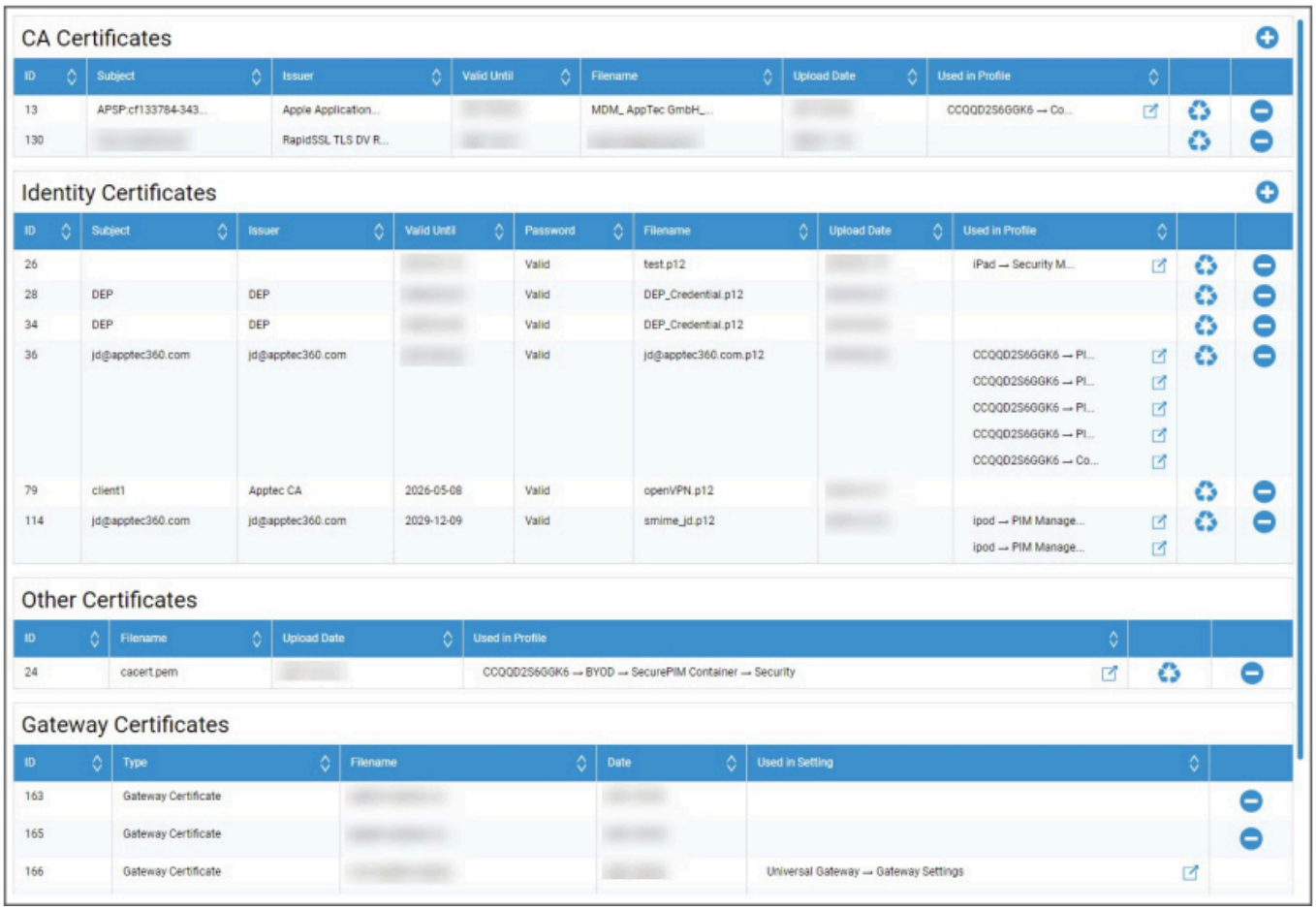
Instellingen auditlogboek

"Bewaarperiode auditlog" bepaalt hoe lang de auditlogs bewaard moeten worden voor ze gewist worden.

Beheer van certificaten

Hier krijg je een overzicht van alle certificaten die zijn geüpload en gebruikt in de Console. Dit is slechts een overzicht. De daadwerkelijke configuratie voor bijvoorbeeld Wi-Fi-certificaten wordt nog steeds gedaan in het profiel op de betreffende locatie.

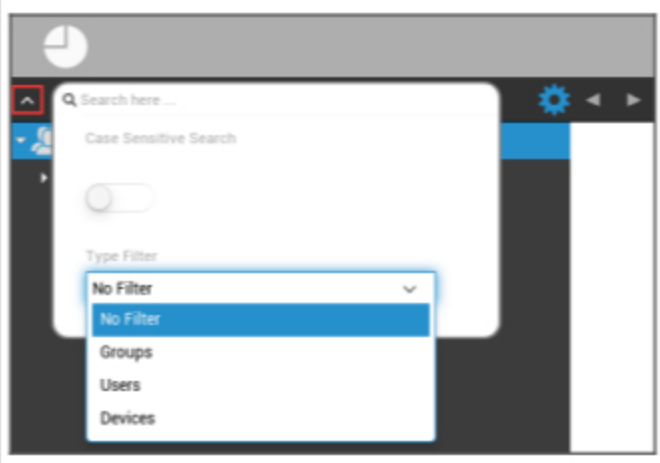
Hier kun je ook certificaten verwijderen of bijwerken, wat automatisch wordt doorgevoerd in de betreffende profielen. Klik op de info in "Gebruikt in profiel" om te zien waar een certificaat nog precies is toegewezen.



Mobiel beheer

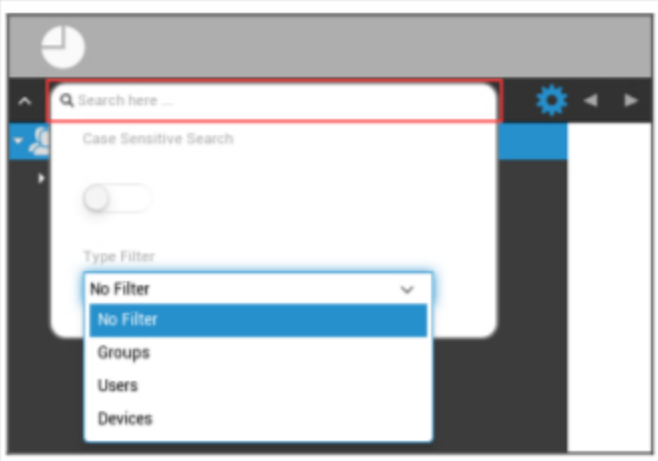
Scherm voor mobiel beheer

Apparaatfilter



Met een klik in de linkerbovenhoek van het scherm kun je verschillende filters vinden voor het weergeven van apparaten.

Zoekvenster



In het zoekvenster kun je alle apparaten en/of gebruikers met een specifiek trefwoord doorzoeken.

Opties versnelling

Nadat u op het betreffende symbool hebt geklikt, wordt een lijst met beschikbare opties weergegeven.

Deze veranderen met elk huidig venster en worden uitgelegd in de respectievelijke hoofdstukken.

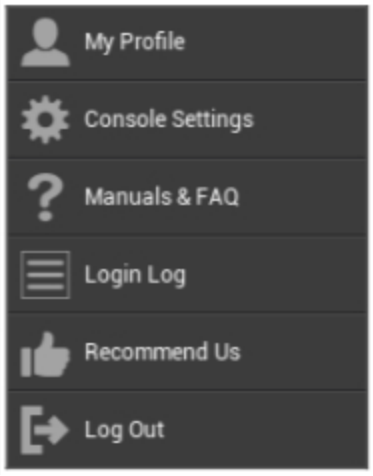
Navigatiepijlen

Als je op de pijl naar links klikt, ga je naar de vorige pagina.

Klik daarna op de pijl naar rechts om naar de pagina te gaan die je zojuist hebt verlaten.

Administratie account-instellingen

Als u op het e-mailadres klikt, zoals hierboven te zien is, wordt het volgende menu weergegeven:



Mijn profiel	De accountgegevens van de admins bewerken
Console-instellingen	Console-instellingen configureren voor het Admins-account
Handleidingen & FAQ	Bekijk de pagina "Handleidingen & FAQ" in "Algemene instellingen".
Inloggen	Toegang tot het "Login Log".
Beveel ons aan	Bekijk de pagina "Beveel ons aan" in "Algemene instellingen".
Afmelden	Afmelden bij de MDM-console

Gebruikersinformatie

Hier kun je de accountgegevens van de momenteel aangemelde beheerder bewerken.

Gebruikersnaam	Gebruikersnaam en/of e-mailadres van de account
Naam	Voornaam beheerder
Achternaam	Achternaam beheerder
Inlognaam	Beheerders inlognaam
E-mailadres	E-mailadres beheerders
Alternatief e-mailadres	Alternatief e-mailadres beheerder
Afbeelding	Profielfoto
Telefoonnummer	Telefoonnummer beheerder
Mobiel nummer	Mobiel nummer beheerder
Telefoon Uitbreiding	Telefoonuitbreiding
Locatie	Locatie
Positie	Positie in het bedrijf
Gebruikersgroep	Selecteer aan welke gebruikersgroep je de beheerdersaccount wilt toewijzen
Opmerking	Geef een reactie
Nieuw wachtwoord invoeren	Voer het wachtwoord in om het wachtwoord te wijzigen
Herhaal nieuw wachtwoord	Herhaal het nieuwe wachtwoord om te bevestigen

Merk op dat de beheerderstoegang ook als een lokale gebruikersaccount in de hiërarchiestructuur kan worden opgeslagen. Zonder de instelling van een extra beheerder, mag deze niet worden verwijderd!

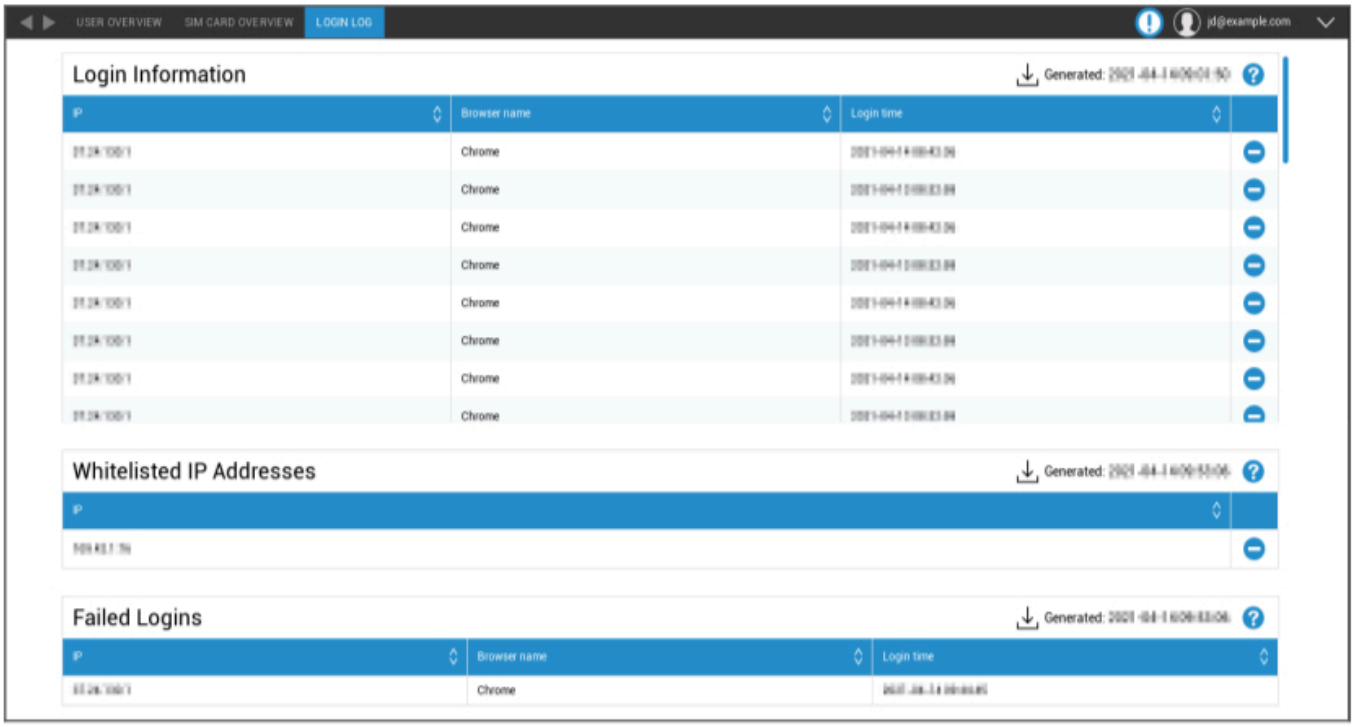
Console-instellingen

Hier kun je de volgende console-instellingen configureren voor het Admins-account:

Weergaveopties voor gebruikers in directory	Definieer hoe gebruikers in de boom moeten worden gelabeld
Weergaveopties voor directory-apparaten	Definieer hoe apparaten in de boomstructuur moeten worden gelabeld
Time-out sessie	Als de gebruiker niets doet binnen de opgegeven tijd, wordt de gebruiker uitgelogd. De standaardwaarde is 60 minuten. Log uit en log opnieuw in na het wijzigen van deze instelling.
Tijdzone	Kies de tijdzone die wordt gebruikt
Tijd Formaat	Kies hoe tijdstempels moeten worden weergegeven
Console Taal	Kies de taal waarin de console moet worden weergegeven. Engels en Duits zijn beschikbaar.
Hoofdkleur	Je kunt een kleur instellen die zal worden gebruikt als basis voor het kleurenschema van de console. Je kunt de kleurenkiezer gebruiken of een kleur invoeren in HTML HEX notatie. RGB-formatoren zoals 'roze' en 'geel' werken ook.
Opdracht opslaan	De toetsencombinatie om een opslag te activeren zonder op de "Opslaan"-knop te drukken.
Twee-factor authenticatie gebruiken	Het gebruik van twee-factor authenticatie inschakelen bij het inloggen. Na het inloggen ontvang je een e-mail met een code die je moet invoeren om in te loggen.
Time-out authenticatie met twee factoren	Stel een periode in waarin je niet wordt gevraagd om een twee-factor authenticatie na een reeds succesvolle authenticatie.
Verificatiecode verzenden via	De verificatiecode wordt naar de geselecteerde opties gestuurd. Het apparaatbericht wordt weergegeven in de AppTec360 MDM App op alle Android- en iOS-apparaten die bij jou horen.
Inlogbericht verzenden na inloggen	Als deze optie is ingeschakeld, wordt er een e-mail verzonden voor elke aanmelding vanaf een ip-adres dat niet op de witte lijst staat. De e-mail bevat informatie over het inloggen (bijv. IP, browser).

Inloggen

Hier zie je informatie over de logins van de momenteel aangemelde beheerdersaccount.



Aanmeldingsgegevens	Een lijst met de logins van de momenteel aangemelde beheerdersaccount die door de console zijn geregistreerd. Deze lijst toont al je succesvolle logins in de afgelopen 30 dagen.
IP-adressen op witte lijsten	Dit is de lijst met alle IP-adressen op de witte lijst. Als u inlogt vanaf een IP die hier wordt vermeld, krijgt u geen inlogbericht. Je kunt een IP-adres aan deze lijst toevoegen door te klikken op de knop naast een item in de lijst "Aanmeldingsgegevens" hierboven. Je kunt een IP-adres uit deze lijst verwijderen door te klikken op de knop naast een item in deze lijst of in de lijst "Aanmeldingsgegevens" hierboven.
Mislukte aanmeldingen	Dit is een lijst van alle mislukte aanmeldingspogingen in de afgelopen 30 dagen. Als je er niet in slaagt om minstens 3 keer binnen 20 minuten het juiste wachtwoord in te voeren, verschijnt er een vermelding in deze lijst. Je wordt ook via e-mail op de hoogte gebracht van mislukte aanmeldingspogingen.

Bedrijfsadministratie (Root-Node) in mobiel beheer

Wanneer je de Root-Node (eerste groep) hebt bereikt, kun je verschillende instellingen voor je bedrijf uitvoeren met betrekking tot Mobile Management.

Een subgroep maken	Een subgroep maken
Hernoem hoofdnode	Hernoemen van de Root-Node (bijv. je bedrijfsnaam)
Massa Inschrijving	Meerdere apparaten/gebruikers tegelijk aanmelden
Massa Opdracht	Een profiel toewijzen voor de respectieve groepen, met één blik
Snel app beheer	(De-)installatieverzoeken voor een toepassing naar de respectieve groepsapparaten sturen
CSV gebruiker importeren	Importeer gebruikers vanuit CSV in de respectievelijke groep

Een subgroep maken

Met "Een subgroep maken" kunt u een extra subgroep maken.

U kunt bepalen onder welke groep de subgroep moet worden toegewezen.

(Standaard wordt een nieuwe groep aangemaakt die wordt toegewezen als subgroep in het hoofdknooppunt)

Hernoem hoofdnode

Hier kunt u uw rootnaam wijzigen. Het is gebruikelijk dat in dit geval de bedrijfsnaam wordt gebruikt.

Massa Inschrijving

Met "Mass Enrollment" kun je meerdere apparaten en gebruikers aanmelden.

Je kunt direct selecteren op welke manier de gebruiker de aanmelding moet ontvangen (eMail; alternatieve eMail; SMS)

Afhankelijk van welk apparaat de gebruiker gaat ontvangen (iOS, Android, Windows Phone), kun je dat hier direct markeren.

Het onderscheid of het een smartphone of een tablet is, kan hier ook worden geconfigureerd, wat je correct moet selecteren met een vinkje.

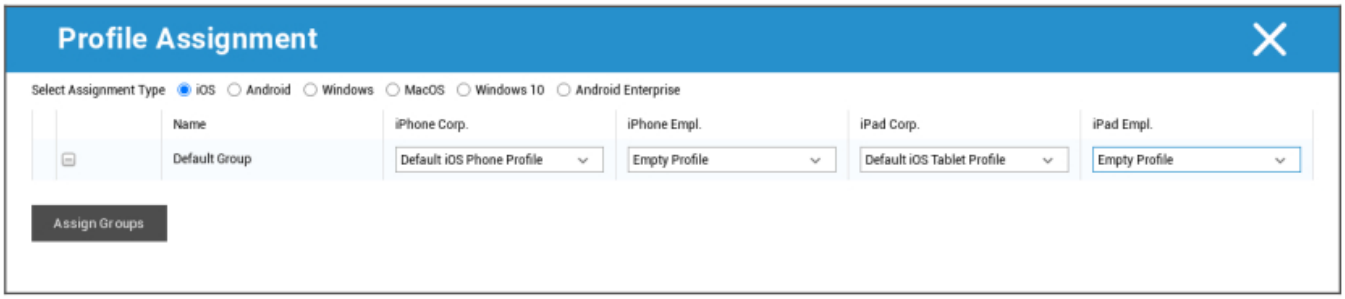
Als laatste stap kun je vaststellen of het apparaat in kwestie zakelijk of privé (BYOD) is.

Met "Exporteer als CSV" kun je de informatie exporteren als een CSV-gegevensbestand. U kunt het CSV-gegevensbestand ook importeren met "Import CSV". Het bestand moet er dan uitzien zoals in het onderstaande voorbeeld:

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

Massa Opdracht

Onder Massa-toewijzing kun je een profiel toewijzen aan alle groepen, dit is onderverdeeld in iOS - Android - Windows - MacOS - Windows 10 - Android Enterprise.

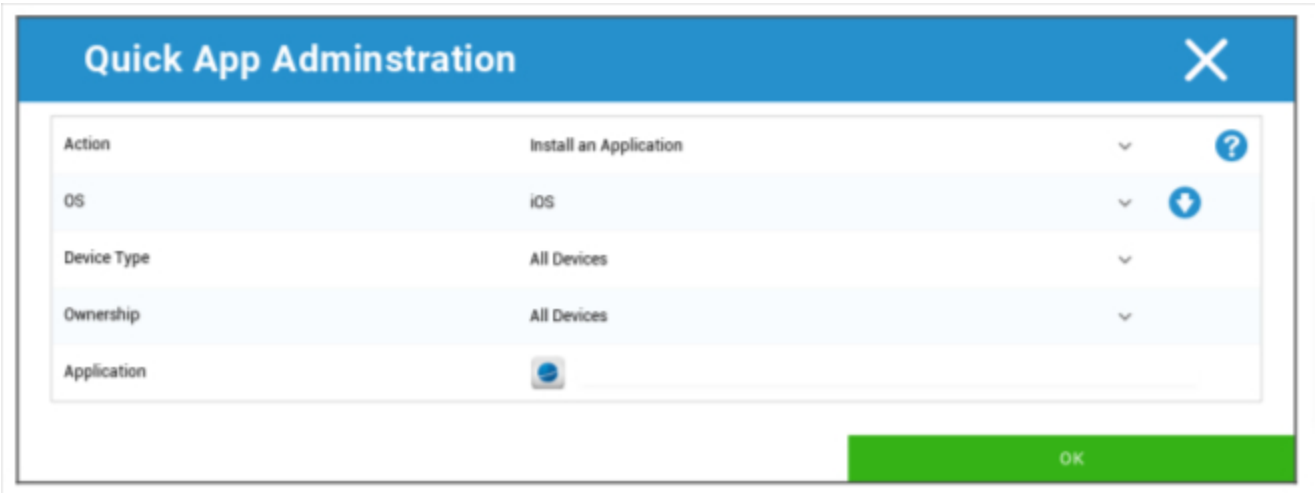


Windows - MacOS - Windows 10 - Android Onderneming

Snel app beheer

Onder Snel applicatiebeheer kun je installatie- of de-installatieverzoeken voor een bepaalde applicatie naar een OS naar keuze sturen.

Je kunt ook definiëren of het verzoek naar alle apparaattypes van het geselecteerde besturingssysteem moet worden gestuurd of alleen naar een specifiek apparaattype.



CSV gebruiker importeren

Importeer gebruikers vanuit CSV in de respectievelijke groep.

Met "CSV-sjabloon downloaden" kun je een CSV-sjabloonbestand exporteren dat je kunt invullen (of als referentie kunt gebruiken).

Je kunt ook de opties "Toon Rol Ids" en "Toon Groep Ids" als referentie gebruiken om je eigen CSV-bestand te maken.

Het CSV-bestand kan worden geüpload naar de MDM met "Upload CSV".

Als laatste stap kun je het importeren starten door op "Start Import" te klikken.

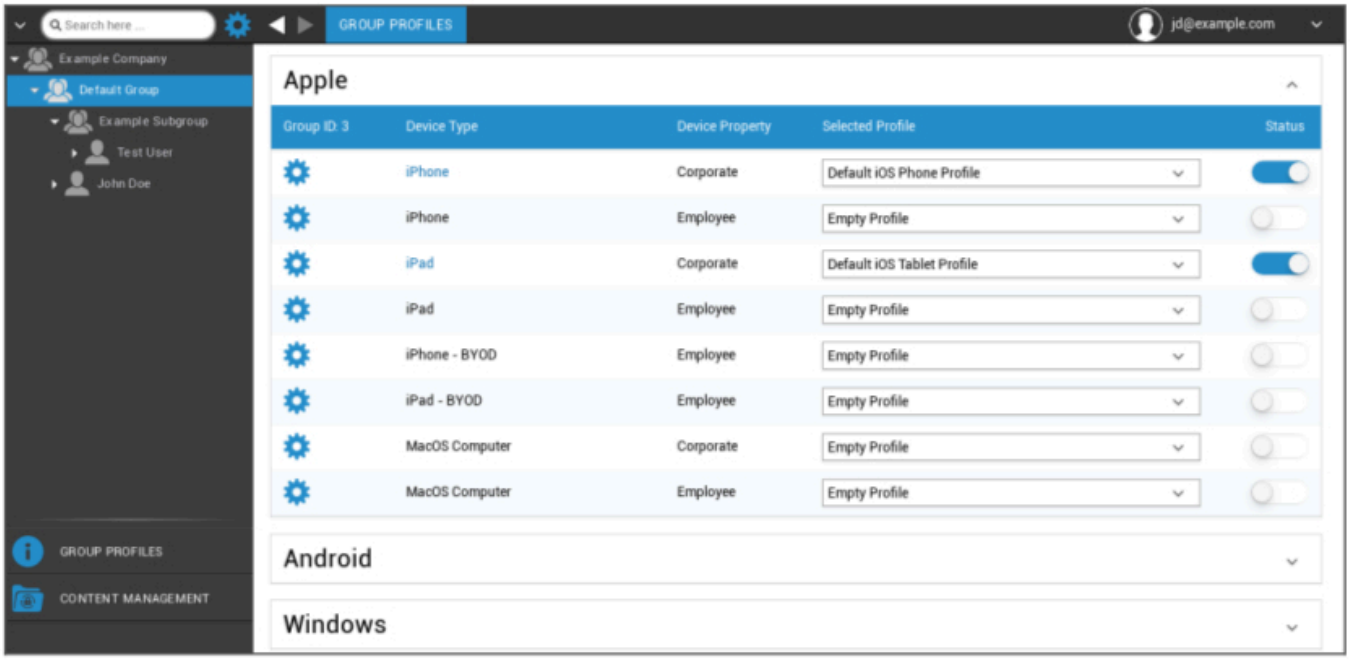
Groepsbeheer in mobiel beheer

Een klik op het overzicht toont de verschillende configuratieprofielen voor de respectieve platforms.

Eén profiel bevat alle instellingsopties die vooraf met AppTec360 kunnen worden ingesteld op het apparaat van de eindgebruiker. Op elk platform kun je profielen aanmaken voor bedrijfsapparaten (Corporate) of Bring-Your-Own-Device apparaten (Employee).

Om configuraties voor apparaatgroepen te differentiëren, bijvoorbeeld op basis van locatie of functie, is het aan te raden om meerdere subgroepen aan te maken.

Let op Profielbeheer in Mobiel beheer



Met het versnellingsmenu stel je verschillende instellingen in voor de betreffende (sub)groep.

Een subgroep maken	Subgroep maken voor de respectieve (sub)groep
Bewerk geselecteerde groep	Bewerk geselecteerde groep
Geselecteerde groep verwijderen	Geselecteerde groep verwijderen
Massale inschrijving	Veel apparaten/gebruikers tegelijk aanmelden voor het geselecteerde profiel
Massa Opdracht	Profielen toewijzen aan de groep die momenteel is geselecteerd
Een subgroep maken	Subgroep maken voor de respectieve (sub)groep

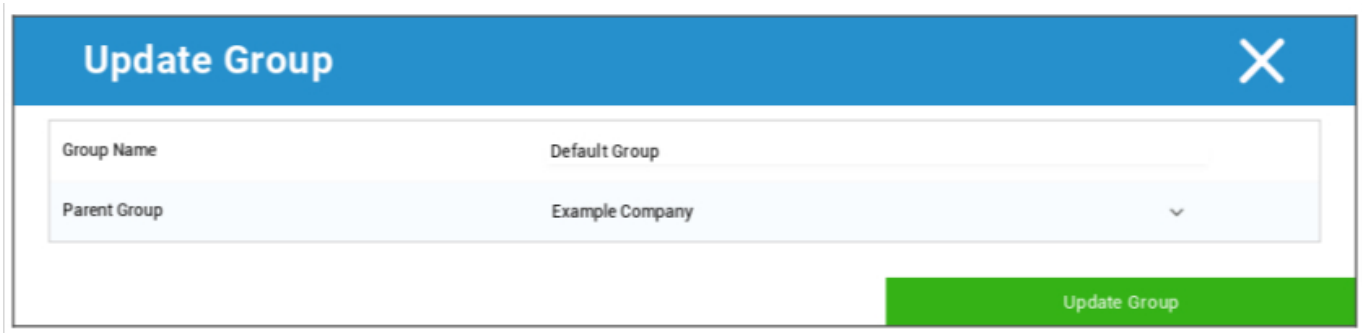
Een gebruiker maken	Maak een gebruiker voor de respectievelijke (sub)groep

Een subgroep maken

Met "Een subgroep maken" kunt u een extra subgroep maken.

Je kunt instellen aan welke groep de subgroep moet worden toegewezen (standaard wordt de subgroep toegewezen aan de groep die op dat moment is geselecteerd).

Bewerk geselecteerde groep



Hier kun je het profiel bewerken - hier zijn de volgende instellingen mogelijk:

- Groepsnaam kan worden gewijzigd
- Moedergroep kan worden gewijzigd

Geselecteerde groep verwijderen

Onder "Verwijder geselecteerde groep" worden alle gebruikers en apparaten weergegeven die in de betreffende groep zitten. Hier heb je de optie om ze te verwijderen.

Voor één gebruiker kun je de volgende verwijderopdrachten uitvoeren:

Gebruiker verwijderen	Gebruiker is verwijderd
Gebruiker naar groep verplaatsen:	Je kunt de gebruiker naar een andere groep verplaatsen (volgende kolom, bijv. "Admins)

Voor één apparaat kun je de volgende verwijderopdrachten uitvoeren:

Vegen en verwijderen	Apparaat wissen en verwijderen
Verwijderen uit systeem	Apparaat alleen uit AppTec verwijderen

Referentie: Massa Inschrijving

Referentie: Massa Opdracht

Een gebruiker maken

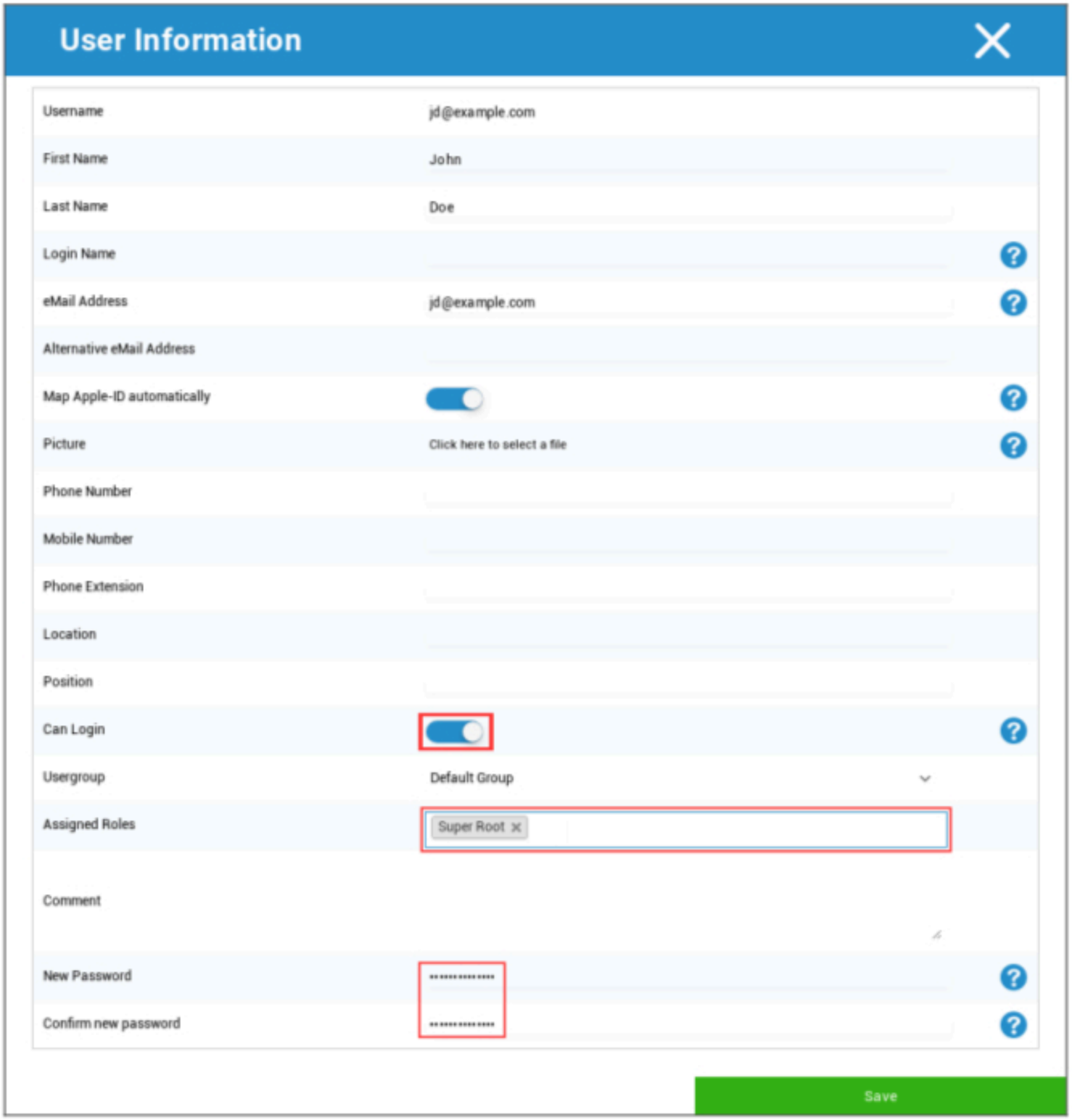
Met "Een gebruiker maken" kun je een nieuwe gebruiker toevoegen.

Een nieuwe beheerder-gebruiker aanmaken

Je kunt een gebruiker instellen als Admin-User. Hierdoor krijgt hij rechten om in te loggen op de console en gebruikers/groepen/apparaten te wijzigen.

Maak een normale Gebruiker aan of gebruik een bestaande Gebruiker. Kies de Gebruiker die je adminrechten wilt geven, klik op het wiel en kies "Gebruiker bewerken":

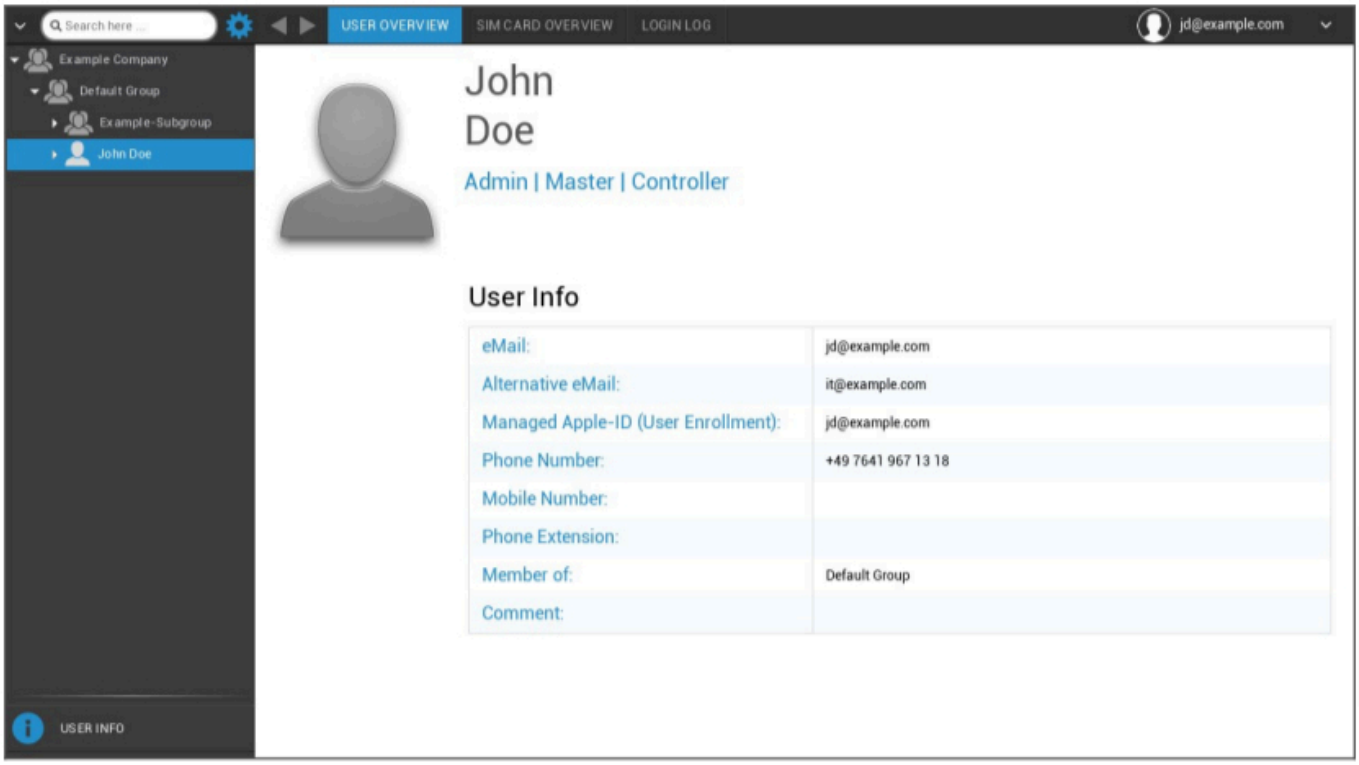
Activeer de schakelaar voor "Kan inloggen", wijs de rol "Super-Root" toe aan de gebruiker en stel een wachtwoord in.



Sla dit op en de gebruiker kan nu inloggen met de gebruikersnaam en het wachtwoord.

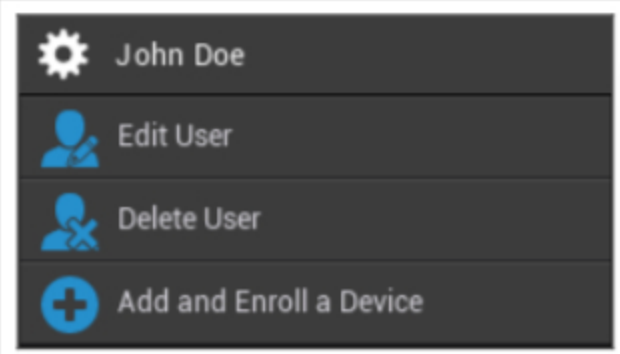
Gebruikersbeheer in mobiel beheer

Als je een bepaalde gebruiker selecteert, zie je het volgende overzicht:



U krijgt een overzicht van alle informatie die u eerder hebt ingevoerd bij "Een gebruiker maken".

Met het tandwiel dat bovenaan is geïnstalleerd, kunt u de volgende configuraties uitvoeren:



Gebruikersnaam	Gebruikersnaam van geselecteerde gebruiker
Gebruiker bewerken	Gebruikersinformatie bewerken
Gebruiker verwijderen	Gebruiker verwijderen • Verwijderen uit systeem = het apparaat wordt verwijderd uit AppTec

	• Wissen & Verwijderen = Het apparaat wordt teruggezet naar de fabrieksinstellingen en verwijderd uit AppTec
Een apparaat toevoegen en registreren	Een apparaat registreren voor de geselecteerde gebruiker

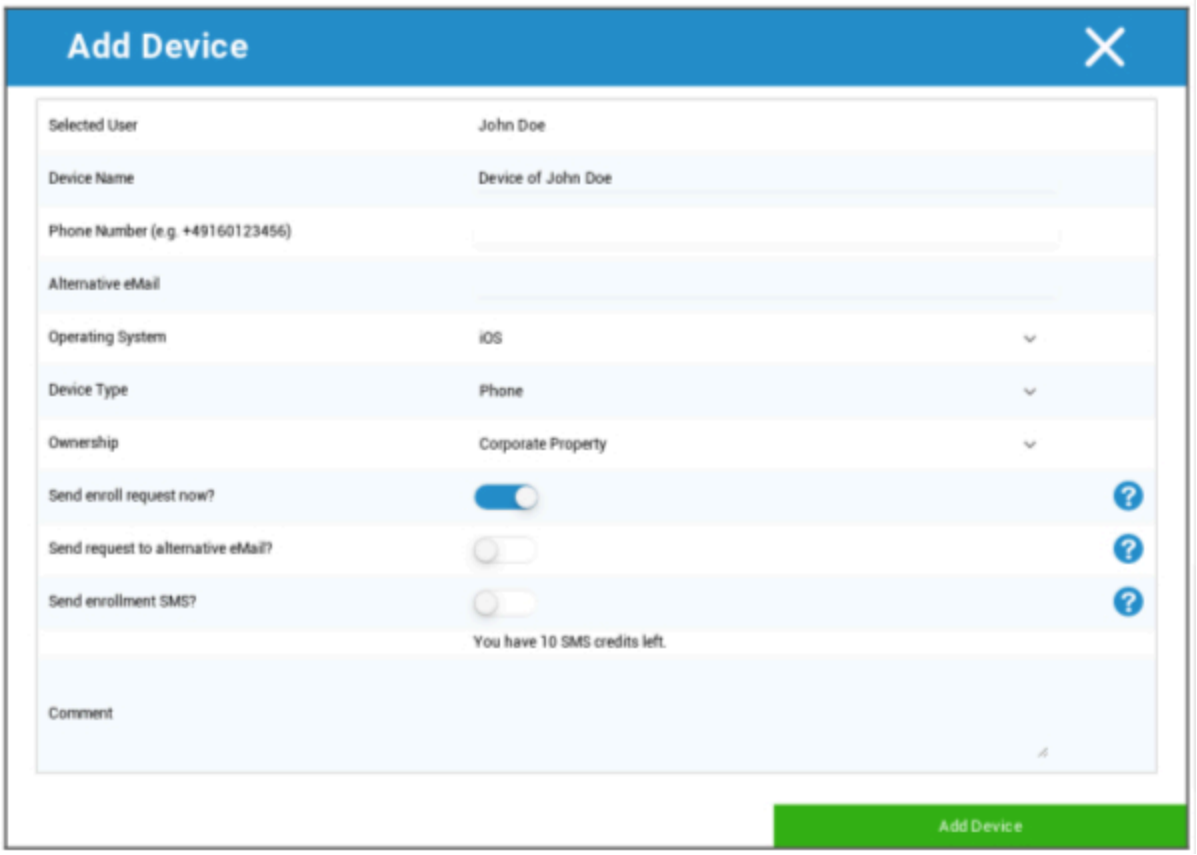
Merk op dat de beheerderstoegang ook als een lokale gebruikersaccount in de hiërarchiestructuur kan worden opgeslagen. Zonder de instelling van een extra beheerder, mag deze niet worden verwijderd!

Een apparaat toevoegen en registreren

Hier kunt u een apparaat selecteren voor het geselecteerde gebruik.

Je kunt ook rechtstreeks apparaten toevoegen aan een groep. Klik hiervoor op de groep, klik op het wiel en selecteer "Apparaat toevoegen en aanmelden".

Je zou het volgende overzicht moeten zien:



Afhankelijk van het soort apparaat dat je wilt aanmelden, moet je de volgende configuraties uitvoeren:

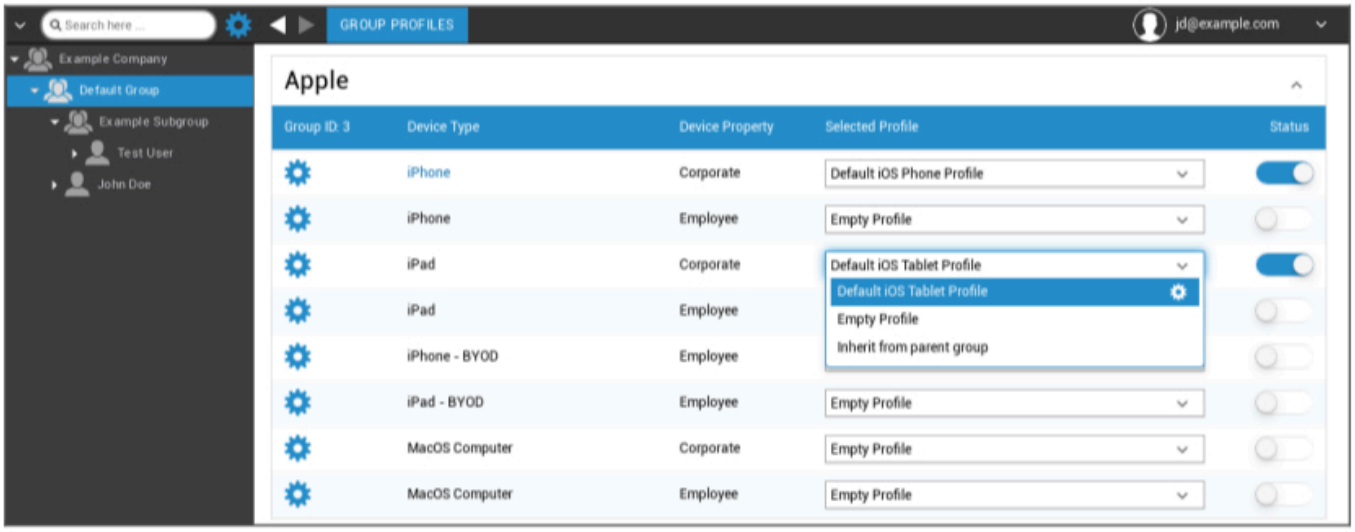
Geselecteerde gebruiker	Geselecteerde gebruiker (wordt automatisch ingevuld)
Naam apparaat	Wordt automatisch ingevuld (apparaat voor "gebruikersnaam") - kan echter worden gewijzigd
Telefoonnummer	Telefoonnummer, wordt automatisch ingevuld (zolang het is opgegeven door de gebruiker) - hier kan het echter worden toegevoegd of gewijzigd
Alternatieve e-mail	Alternatieve e-mail wordt automatisch ingevuld (zolang deze is opgegeven door de gebruiker) - hier kan deze echter worden toegevoegd of gewijzigd
Apparaateigenaar	Bedrijfseigendom = bedrijfsapparaat Werknemerseigendom = BYOD-apparaat
Kies besturingssysteem	Hier kun je kiezen uit de volgende besturingssystemen: • iOS • iOS BYOD (gebruikersregistratie) • MacOS • Android Onderneming • Android • Windows mobiel • Windows 10
Inschrijvingsverzoek verzenden?	De e-mail wordt onmiddellijk naar het hoofdmailadres gestuurd en de gebruiker wordt gevraagd zijn apparaat aan te sluiten.
Verzoek verzenden naar alternatieve eMail?	Stuur de e-mail aanvullend of uitsluitend (in het geval dat "Send enroll request?" was gedeactiveerd) naar het alternatieve e-mailadres (de e-mail is anders dan de "normale" e-mail met het verzoek tot inschrijving).
SMS voor inschrijving versturen?	Stuur een registratieverzoek via sms (het "telefoonnummer" moet worden ingevoerd)

Nadat het registratieverzoek is verzonden, wordt het apparaat meteen weergegeven (rood gemarkeerd).

Zodra het apparaat met succes is verbonden, wordt het kort daarna groen gemarkeerd en is het daarmee klaar om beperkingen, apps, enz. te ontvangen.

Profielbeheer in mobiel beheer

Nadat je op een groep hebt geklikt, krijg je een overzicht van alle te configureren apparaatplatformen en de respectievelijk toegewezen profielen.



	De configuratie voor het geselecteerde profiel uitvoeren
Type apparaat	Type en/of model apparaat
Apparaateigenschap	Eigenaar van het apparaat (Corporate = bedrijfseigendom, Employee = privéapparaat van werknemer)
Geselecteerd profiel	Geselecteerd profiel (het tandwiel opent het configuratiedialoogvenster van het profiel)
Status	Aan/Uit (het profiel is geactiveerd/gedeactiveerd)

Wanneer je de versnelling selecteert, krijg je de volgende opties:

Een profiel maken

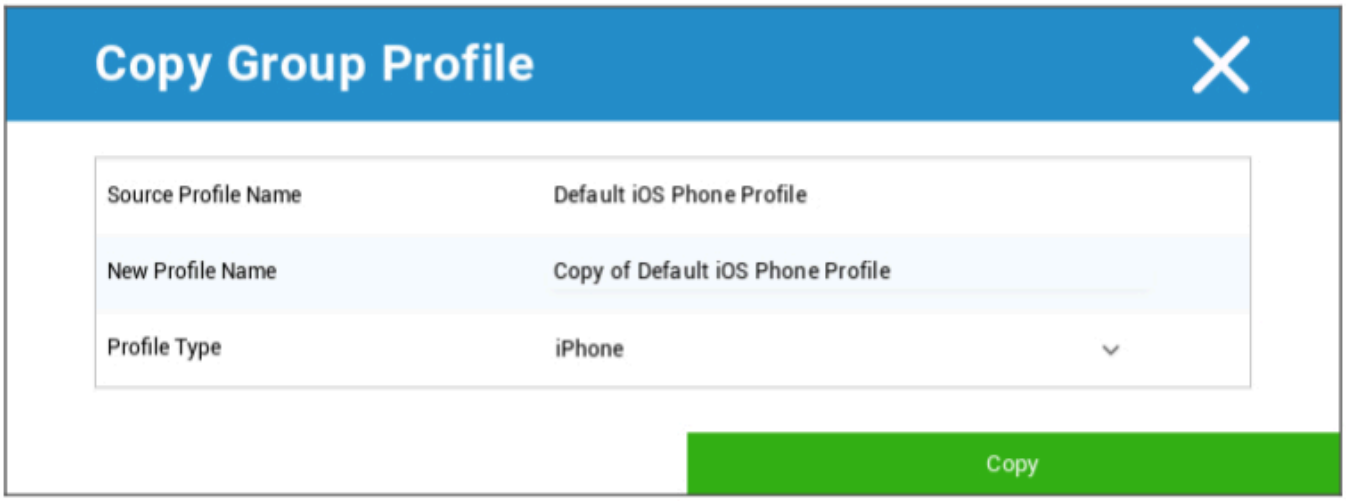
Je kunt voor elk item en/of platform een nieuw profiel aanmaken en configureren. Nadat je op dit subpunt hebt geklikt, wordt het profiel onmiddellijk aangemaakt en kun je meteen beginnen met de configuratie van de iOS, Android en Windows Phone.

Profiel bewerken

Nadat je op "Edit Profile" (Profiel bewerken) hebt geklikt, kom je bij het configuratiescherm voor het betreffende profiel, waar je de configuraties kunt instellen.

Profiel kopiëren

Met behulp van de functie "Profiel kopiëren" kunt u de instellingen/configuraties van een bestaand profiel kopiëren en toevoegen aan een nieuw profiel.

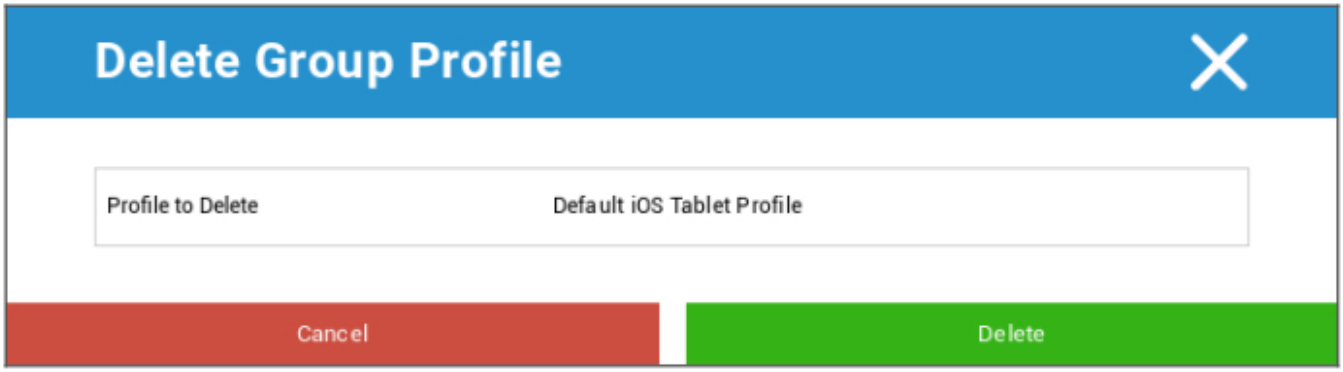


Naam bronprofiel	Naam van het profiel dat gekopieerd moet worden
Nieuwe profielnaam	Naam van het nieuwe profiel
Profiel type	Type profiel (telefoon/tablet)

Zodra je op "Kopiëren" klikt, wordt het profiel aangemaakt en kan het nu worden toegewezen aan de groep

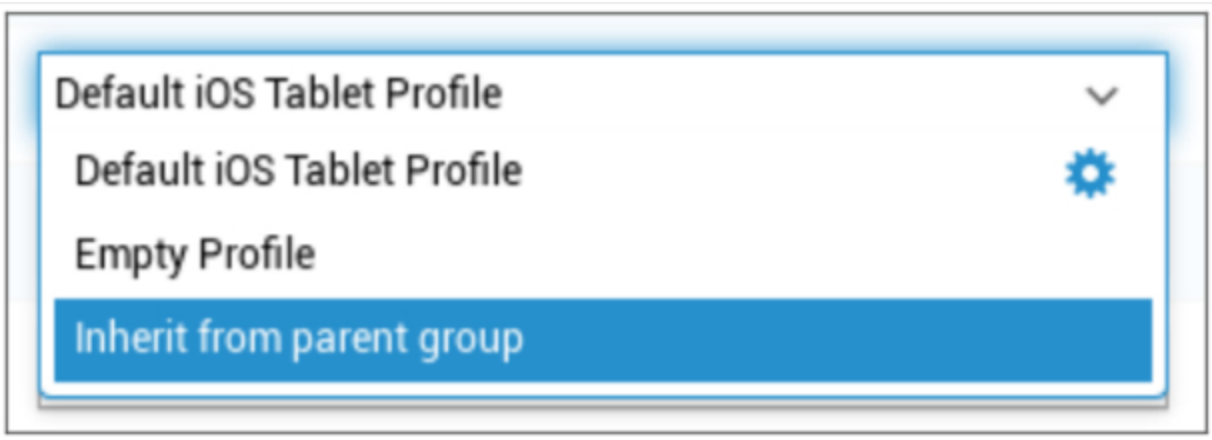
Profiel verwijderen

Hier kun je een profiel definitief verwijderen. Houd er rekening mee dat tijdens het verwijderingsproces en het volgende "Nu toewijzen"-proces voor het profiel, de configuratie zal verdwijnen op de respectieve apparaten van een betrokken groep en niet kan worden hersteld!


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

Overerving van profielen

Tijdens de selectie van de profielen is de optie "Erven van oudergroep" beschikbaar.



Als het profiel geactiveerd is, wordt het profiel van de bovenliggende groep gebruikt voor het respectievelijk geselecteerde apparaat (en het respectieve apparaattype). Merk ook op dat wijzigingen aan dit profiel mogelijk invloed hebben op meerdere groepen.

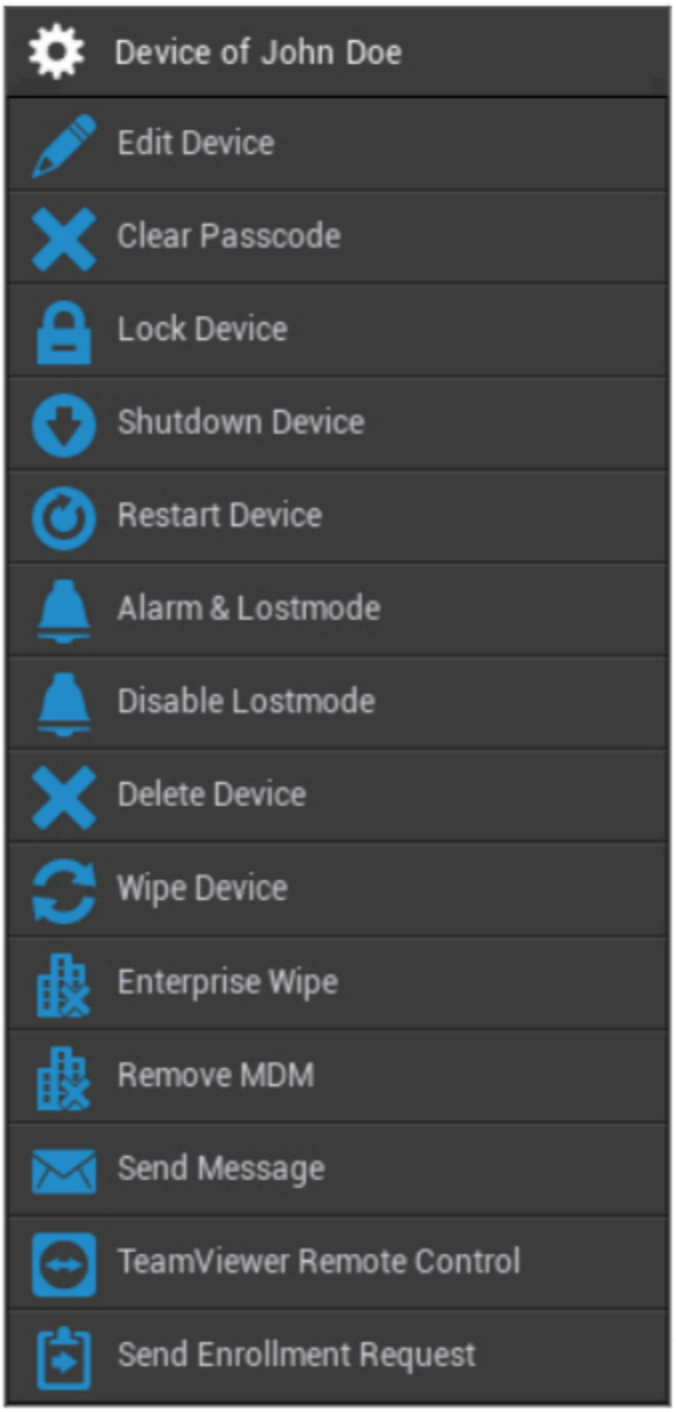
Deze configuratie wordt als standaardwaarde ingesteld wanneer een nieuwe subgroep wordt aangemaakt.

De configuratie "Empty Profile" is ook beschikbaar, wat overeenkomt met een leeg profiel, wat betekent dat er uiteindelijk geen nieuwe configuraties worden uitgevoerd op het eindgebruikersapparaat.

Apparaatbeheer in mobiel beheer

Als je een apparaat selecteert, kun je verschillende taken uitvoeren via de "versnelling". Deze zijn verschillend, afhankelijk van de OS-platforms (iOS, Android Enterprise, Android, Windows Mobile, Windows 10).

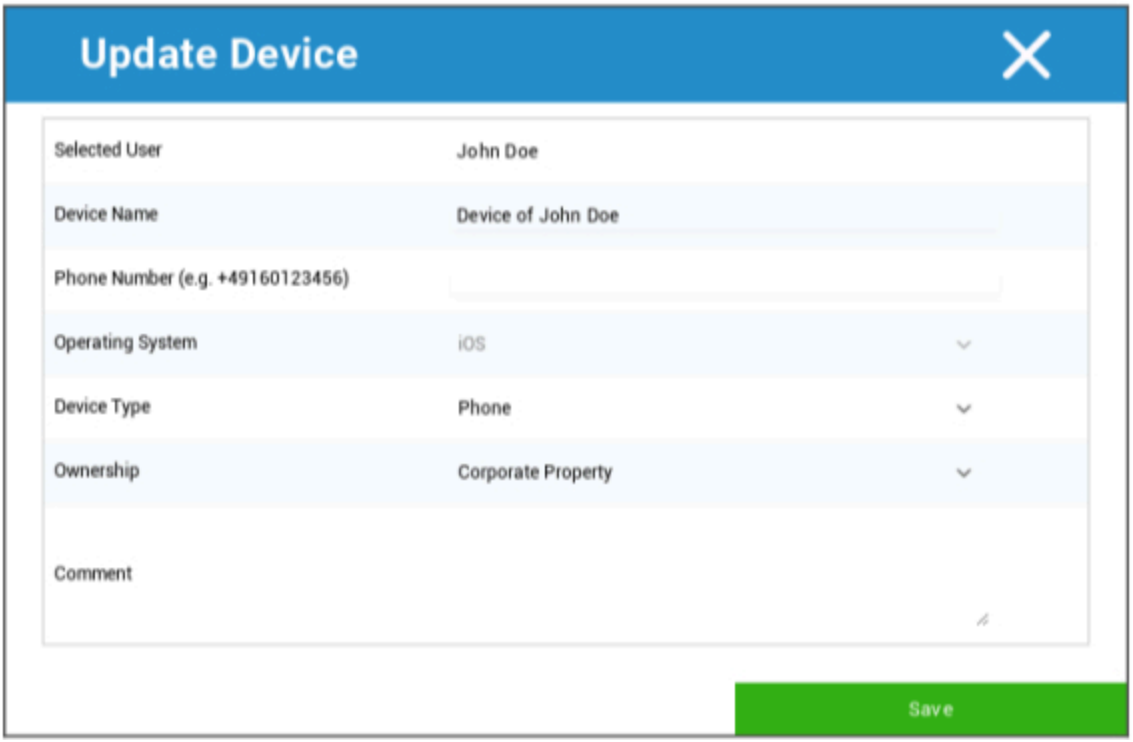
IOS



Apparaat bewerken	Apparaat bewerken
Wachtwoord wissen	Het wachtwoord van het apparaat is gewist
Apparaat vergrendelen	Apparaat vergrendelen (vergrendelscherm)
Uitschakelapparaat	Uitschakelapparaat

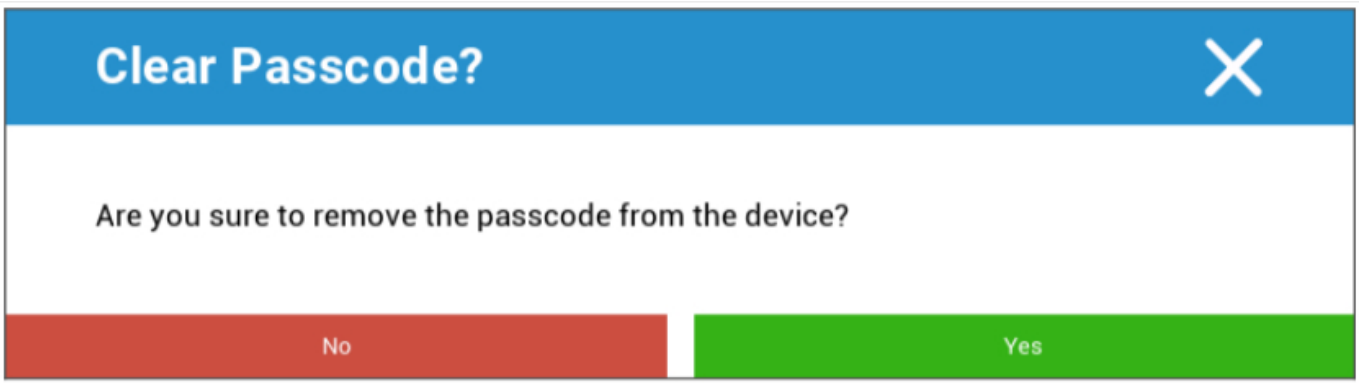
Apparaat opnieuw opstarten	Apparaat opnieuw opstarten
Alarm & Verliesmodus	Start Alarm & Verliesmodus
Verloren modus uitschakelen	Verloren modus uitschakelen
Apparaat verwijderen	Apparaat uit AppTec verwijderen
Apparaat wissen	Apparaat herstellen naar fabrieksinstellingen
Ondernemingsvegen	De informatie, apps en profielen geleverd door AppTec360 worden verwijderd (apparaat wordt losgekoppeld van MDM)
MDM verwijderen	
Verstuur bericht	Pushberichten naar het apparaat sturen Het bericht wordt weergegeven in de AppTec360 App (tabblad Bericht)
TeamViewer afstandsbediening	Sessie voor afstandsbediening starten met TeamViewer
Inschrijvingsaanvraag verzenden	(Herhaald) registratieverzoek verzenden

Apparaat bewerken



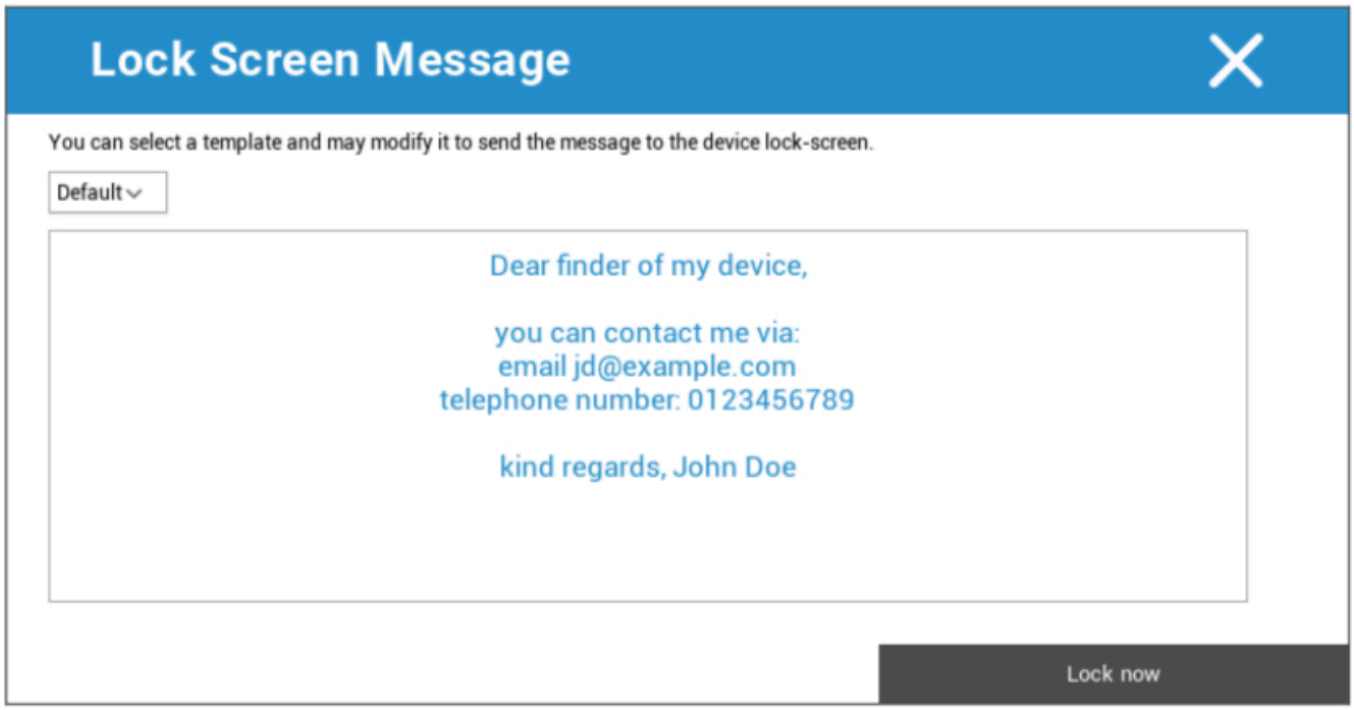
Hier kun je allerlei informatie over het apparaat bijwerken.

Wachtwoord wissen



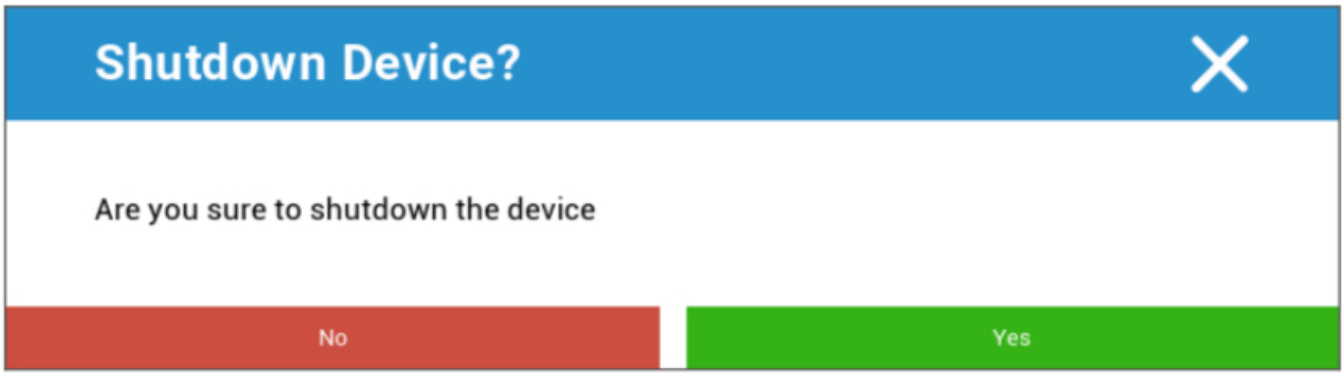
Onder "Clear Passcode" (Wachtwoord wissen) kun je op afstand het wachtwoord van het apparaat verwijderen. Vervolgens wordt de gebruiker gevraagd een nieuw wachtwoord in te voeren (afhankelijk van de richtlijnen voor het wachtwoord).

Apparaat vergrendelen



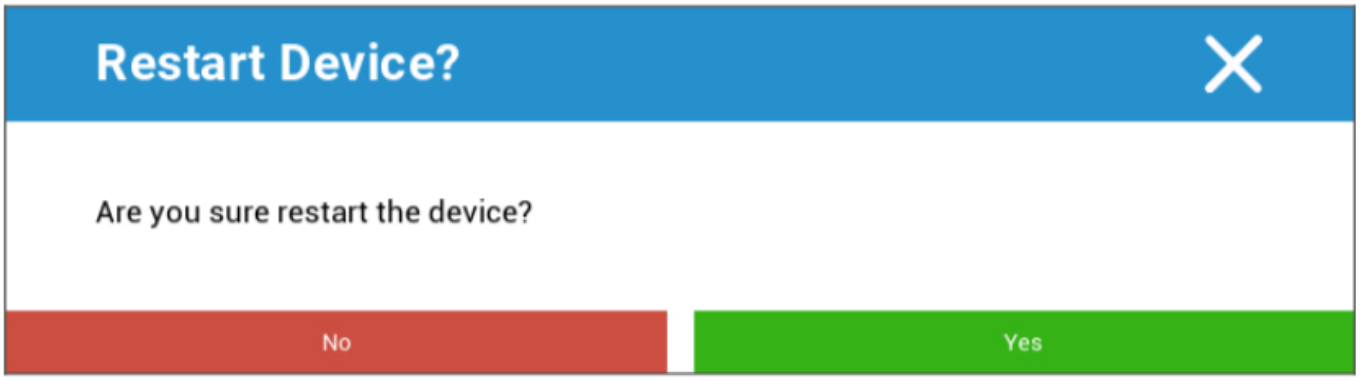
Hier wordt een vergrendelopdracht naar het eindgebruikerapparaat gestuurd (vergrendelscherm).

Uitschakelapparaat



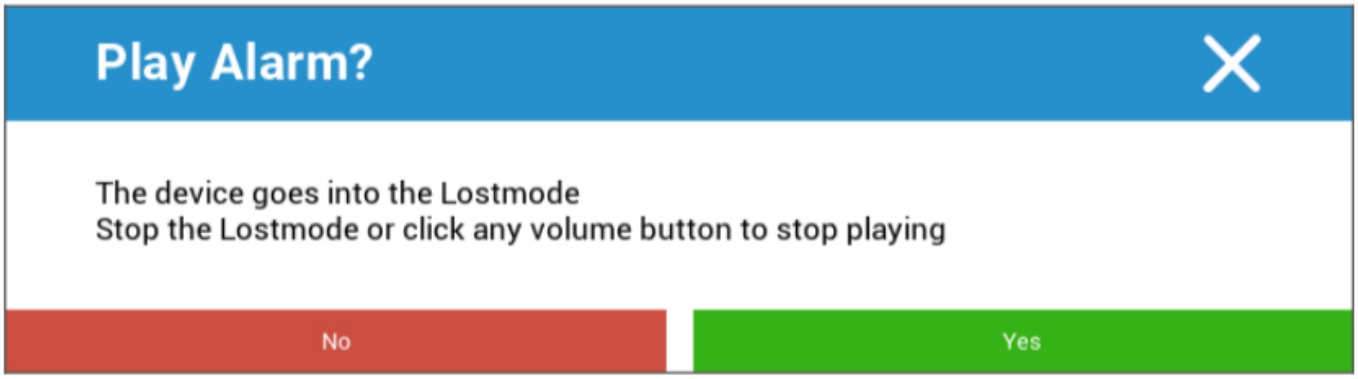
Hier wordt een afsluitcommando naar het eindgebruikerapparaat gestuurd.

Apparaat opnieuw opstarten

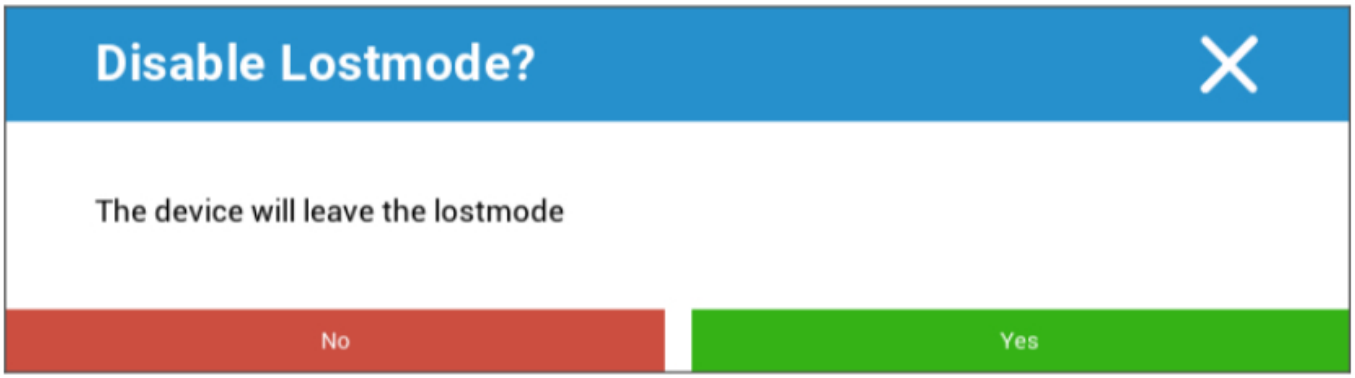


Hier wordt een herstartopdracht naar het eindgebruikerapparaat gestuurd.

Alarm & Verliesmodus | Verliesmodus uitschakelen



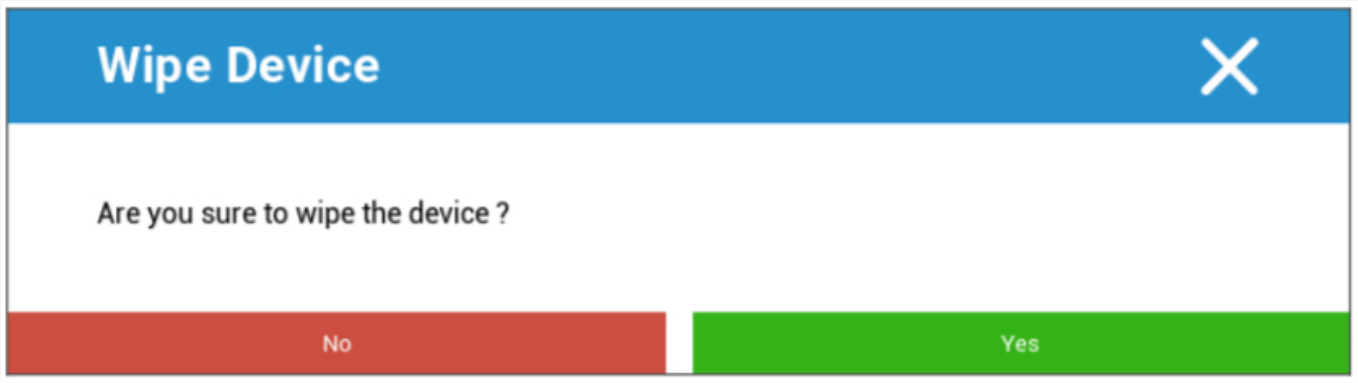
Hier kan het apparaat in de Lostmode worden gezet, waardoor het apparaat constant een alarmgeluid laat horen. De Lostmode kan worden gestopt door op een volumeknop van het apparaat te drukken of op afstand door op "Disable Lostmode" te klikken:



Apparaat verwijderen

Hier kan de verwijderopdracht worden uitgevoerd. Je kunt opnieuw beslissen of het apparaat alleen uit AppTec360 moet worden verwijderd ("Verwijderen uit systeem") of dat het apparaat uit AppTec360 moet worden verwijderd en ook moet worden teruggezet naar de fabrieksinstellingen ("Wissen & Verwijderen").

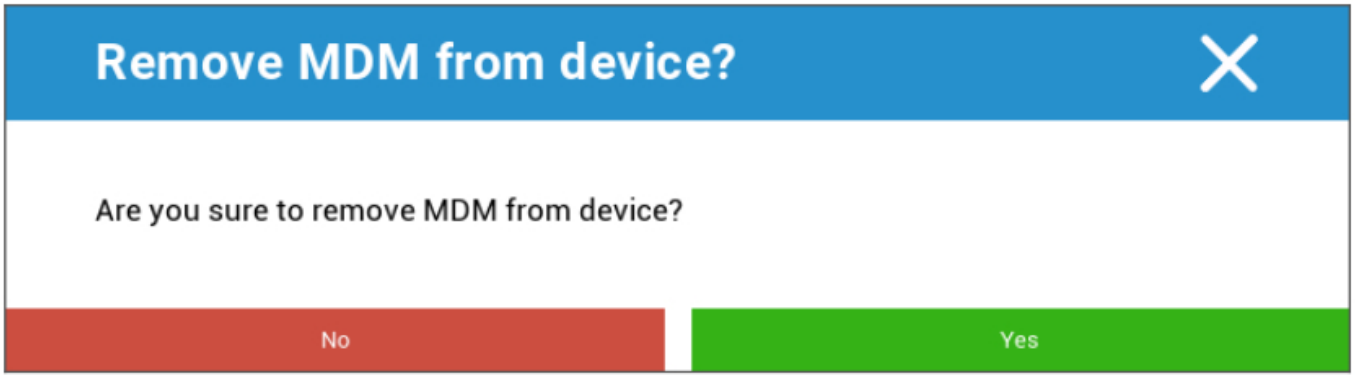
Apparaat wissen



Onder "Apparaat wissen" kun je het apparaat volledig wissen. De fabrieksinstellingen van het apparaat worden hersteld.

Wissen | MDM verwijderen

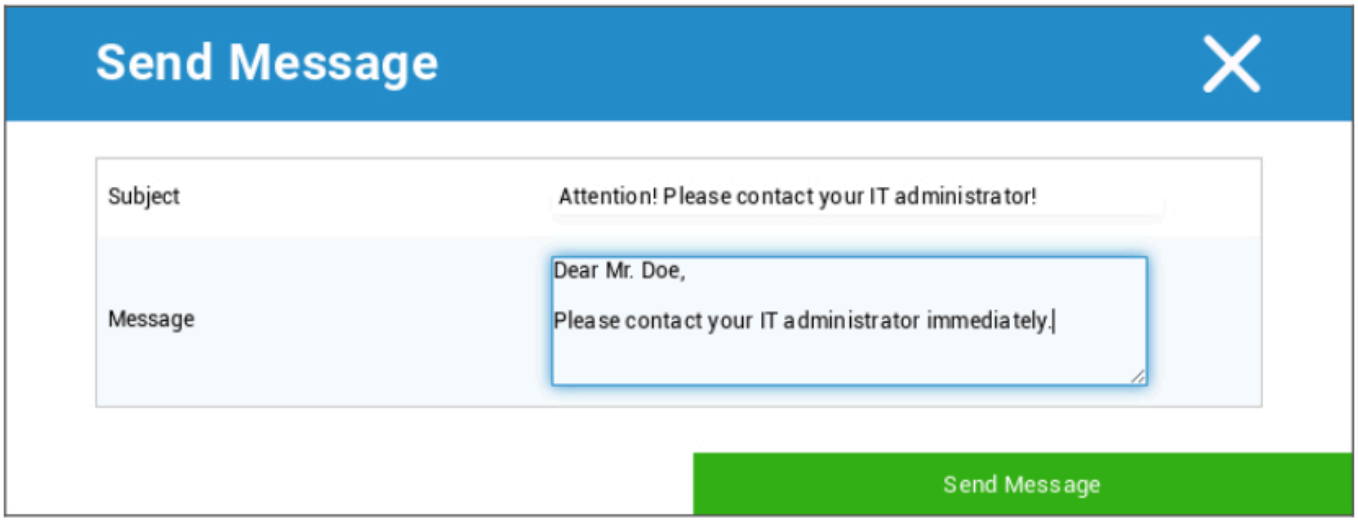
Alleen de door AppTec360 geleverde informatie, apps en profielen worden verwijderd. Op deze manier zijn de bedrijfsgegevens niet langer beschikbaar op het eindgebruikerapparaat. Het privégedeelte wordt niet aangetast en blijft op het eindgebruikerapparaat staan.



Met "MDM verwijderen" kun je het MDM-profiel op het eindgebruikersapparaat en alle andere door AppTec geleverde items verwijderen.

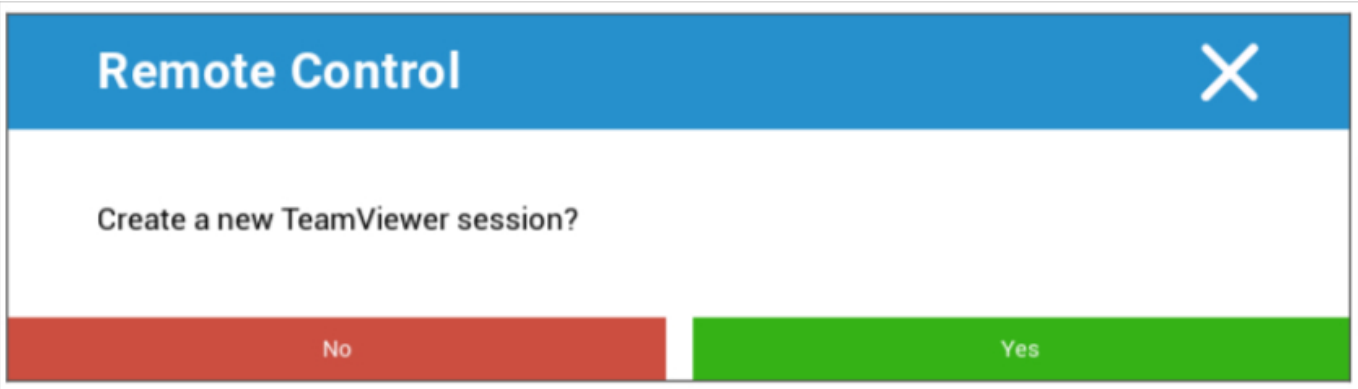
Dit commando voert dezelfde actie uit als "Enterprise Wipe".

Verstuur bericht



Hier kun je een Push notificatie naar het betreffende apparaat sturen.

TeamViewer afstandsbediening



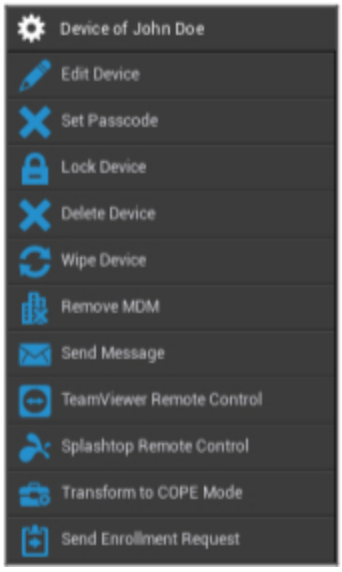
Hier kan een Teamviewer Remote Control-sessie worden gestart.

Inschrijvingsaanvraag verzenden

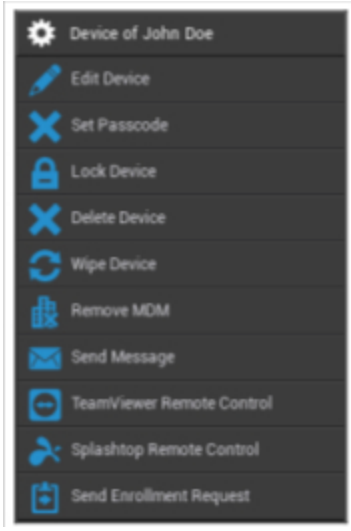
Met "Enrollment Request verzenden" kun je (nogmaals) een Enrollment Request verzenden naar de betreffende gebruiker.

Android

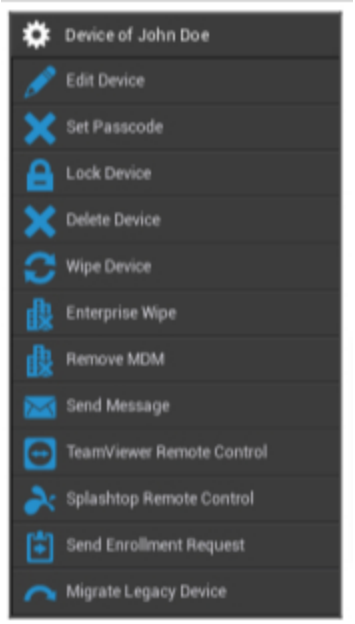
AE Volledig beheerd apparaat (Work Managed)



AE Werkprofiel (Container)



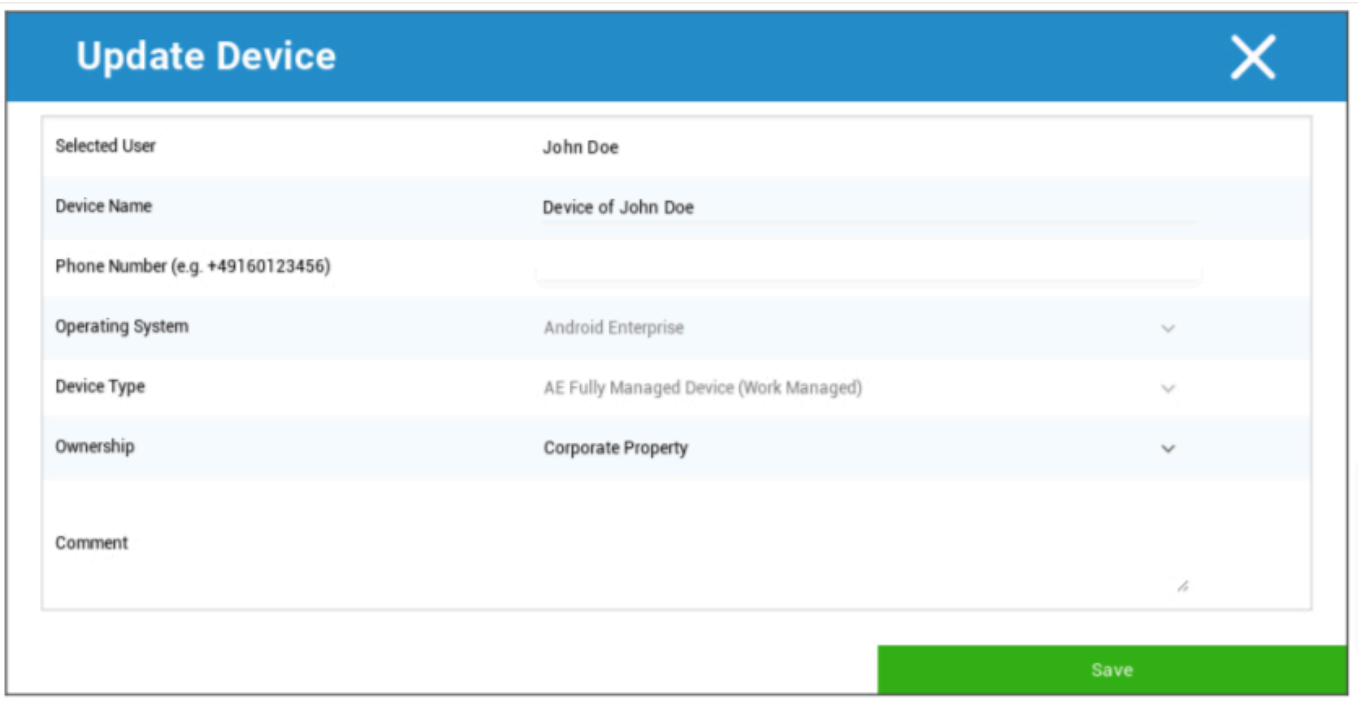
Android-telefoon | Tablet



Apparaat bewerken	Apparaatinformatie bewerken
Wachtwoord instellen	Stel het wachtwoord van het apparaat in
Apparaat vergrendelen	Apparaat vergrendelen (vergrendelscherm)
Apparaat verwijderen	Apparaat verwijderen uit AppTec
Apparaat wissen	Apparaat herstellen naar fabrieksinstellingen
Ondernemingsvegen	Informatie, Apps, Profielen die zijn aangeleverd door AppTec360 worden verwijderd (apparaat wordt losgekoppeld van MDM)
MDM verwijderen	
Verstuur bericht	Pushberichten naar het apparaat sturen Het bericht wordt weergegeven in de AppTec360 App (tabblad Bericht)
TeamViewer afstandsbediening	Start een afstandsbedieningssessie voor dit apparaat met TeamViewer
Splashtop afstandsbediening	Een afstandsbedieningssessie starten voor dit apparaat met Splashtop
Transformeren naar COPE-modus (alleen op AE apparaat met volledig beheer (Work Managed))	Maak een werkprofiel aan op dit apparaat met AE Volledig beheerd (Work Managed)
Inschrijvingsaanvraag verzenden	(Herhaald) inschrijvingsverzoek verzenden
Legacy-apparaat migreren (alleen op Android-telefoon / -tablet bij registratie met gebruik van Device Owner Mode Provisioning)	Migreer Android-telefoon-/tabletprofiel naar AE-profiel voor volledig beheerd apparaat (Work Managed)

Apparaat bewerken

Hier kun je verschillende apparaatgegevens bijwerken.



Geselecteerde gebruiker	Apparaatgebruiker
Naam apparaat	Naam apparaat
Telefoonnummer	Telefoonnummer apparaat
Besturingssysteem	Android Onderneming Android
Type apparaat	Android voor bedrijven: • AE Volledig beheerd apparaat (Work Managed) • Modus AE-werkprofiel (alleen container) • AE Volledig beheerd apparaat met werkprofiel (COPE) Android: • Telefoon • Tablet
Eigendom	Zakelijk = bedrijfseigendom

	Werknemer = eigenschap werknemer
Opmerking	Aanvullende beschrijvingen voor het apparaat

Wachtwoord wissen

Hier kun je het wachtwoord van het geselecteerde apparaat verwijderen. Op Android wordt het wachtwoord standaard ingesteld op "123456"- dit kan en moet achteraf door de gebruiker worden gewijzigd.

Apparaat vergrendelen

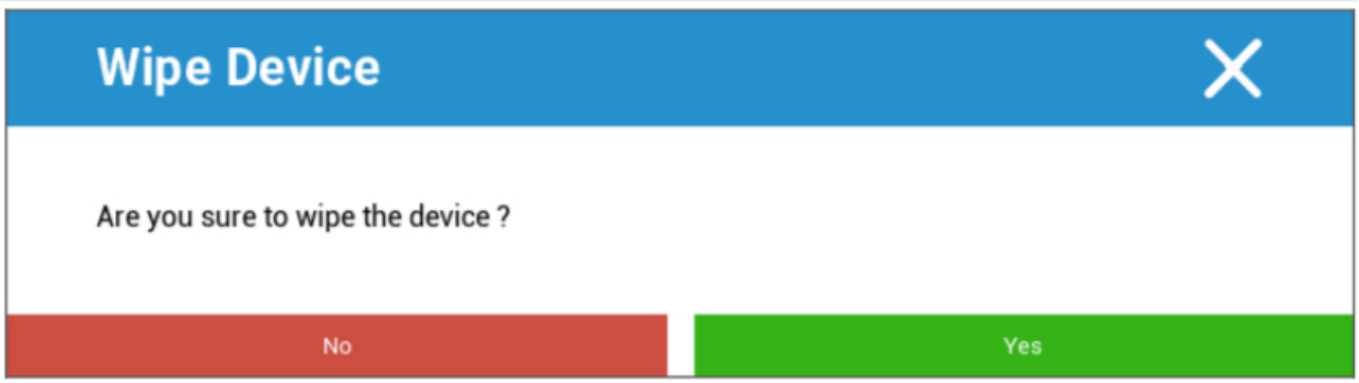
Hier wordt een opdracht om het apparaat te vergrendelen naar het apparaat gestuurd (vergrendelscherm).

Apparaat verwijderen

Hier kan een wisopdracht worden uitgevoerd. Je kunt opnieuw beslissen of het apparaat alleen uit AppTec360 moet worden verwijderd ("Verwijderen uit systeem") of dat het apparaat uit AppTec360 moet worden verwijderd en bovendien moet worden teruggezet naar de fabrieksinstellingen ("Wissen & Verwijderen").

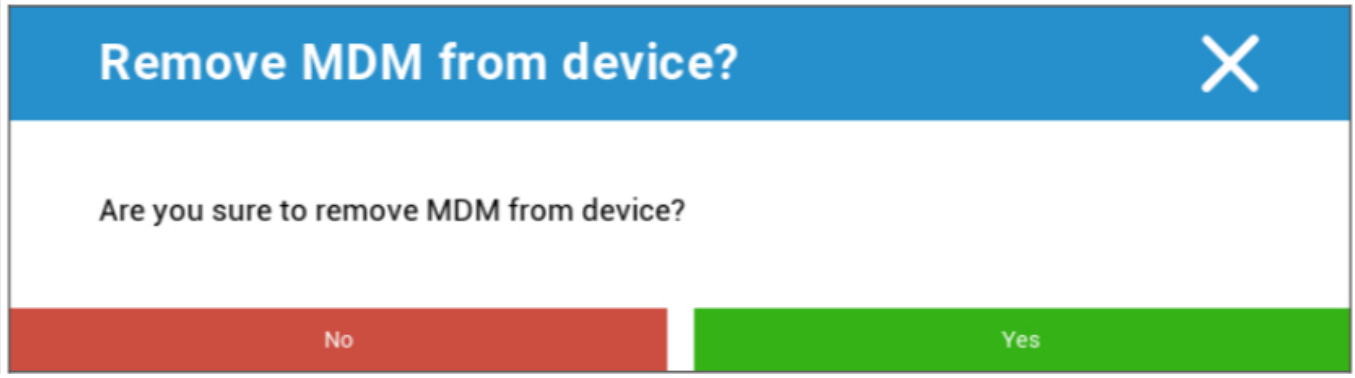
Apparaat wissen

Onder "Apparaat wissen" kun je het apparaat volledig wissen. Het apparaat wordt dan teruggezet naar de fabrieksinstellingen.



Als het apparaat een SD-kaart bevat, kun je bovendien de SD-kaart wissen. Je kunt dit doen door "Ook SD-kaart wissen? "in te stellen op "Aan".

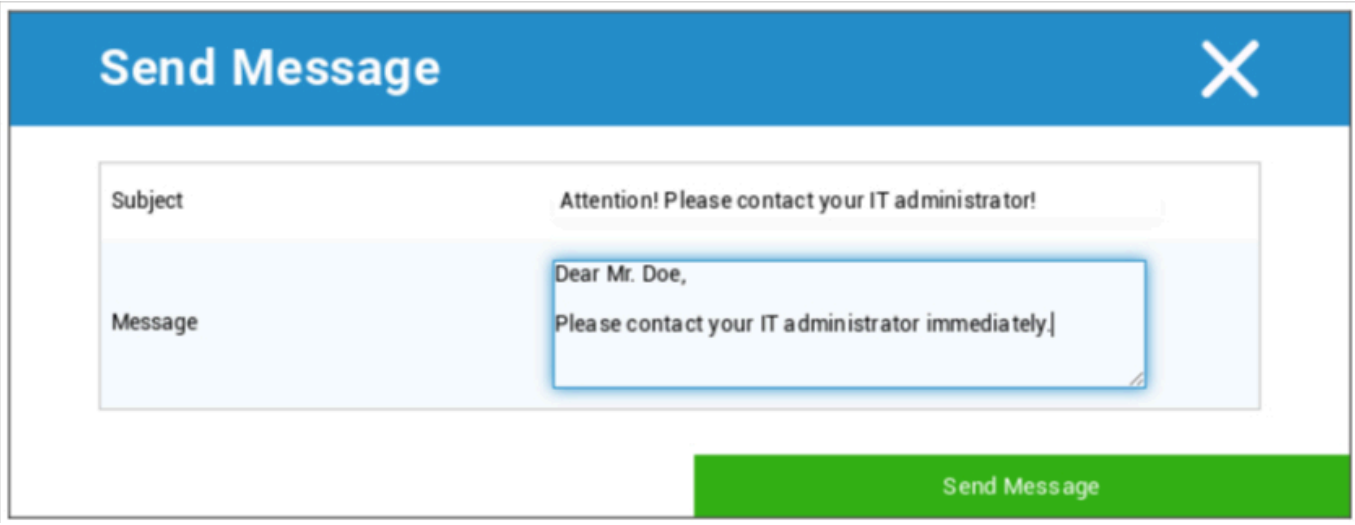
MDM verwijderen



Dit is de aanbevolen methode om een scheiding aan te brengen met MDM.

Alleen de informatie, apps en profielen geleverd door AppTec360 worden verwijderd, wat betekent dat alle bedrijfsgegevens niet langer beschikbaar zijn op het eindgebruikersapparaat. De privésfeer wordt echter niet aangetast en blijft op het apparaat van de eindgebruiker staan.

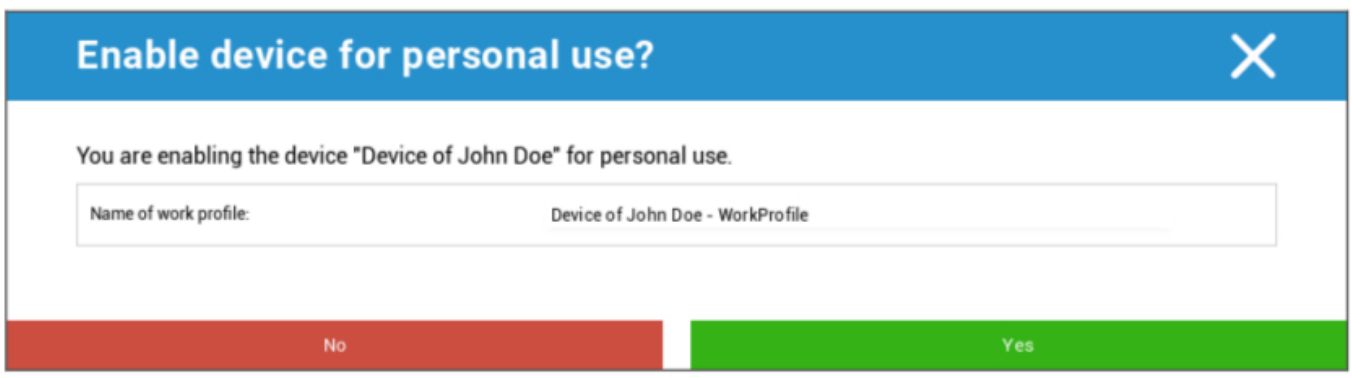
Verstuur bericht



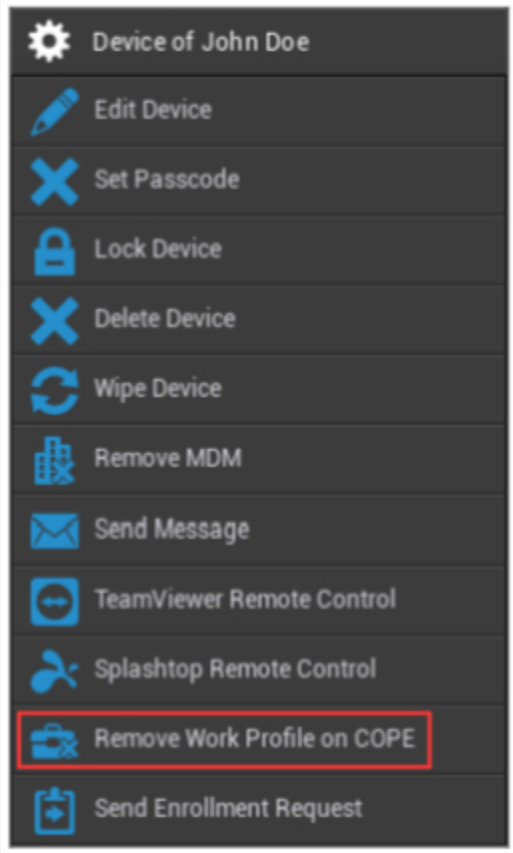
Hier kun je een pushbericht naar het betreffende eindgebruikerapparaat sturen.

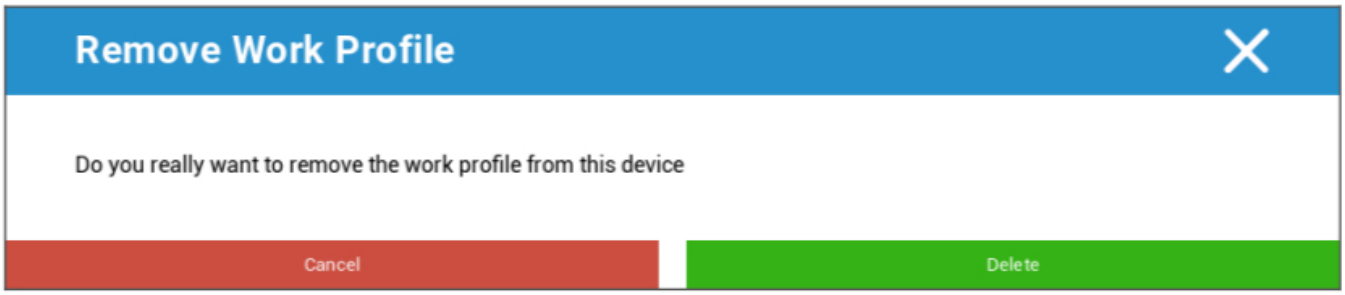
Transformeren naar COPE-modus

Maak een werkprofiel aan op dit apparaat met AE Volledig beheerd (Work Managed)



Nadat je het apparaat naar de COPE-modus hebt getransformeerd, kun je het werkprofiel verwijderen door op de tandwieloptie **Werkprofiel verwijderen op COPE te klikken:**




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

Inschrijvingsaanvraag verzenden

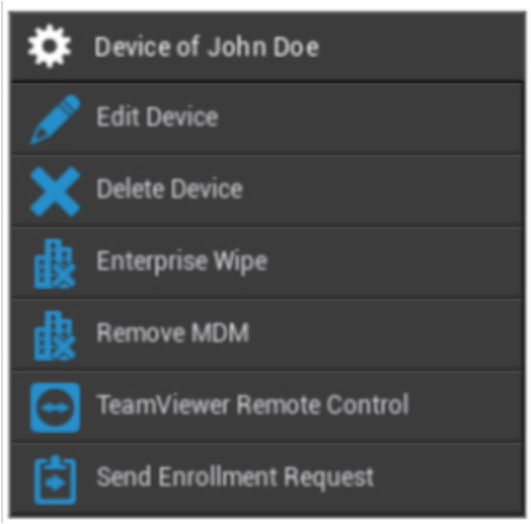
Met "Enrollment Request verzenden" kun je (nogmaals) een Enrollment Request verzenden naar de betreffende gebruiker.

Houd er rekening mee dat alleen de nieuwste Inschrijvingsaanvraag geldig is.

Legacy-apparaat migreren

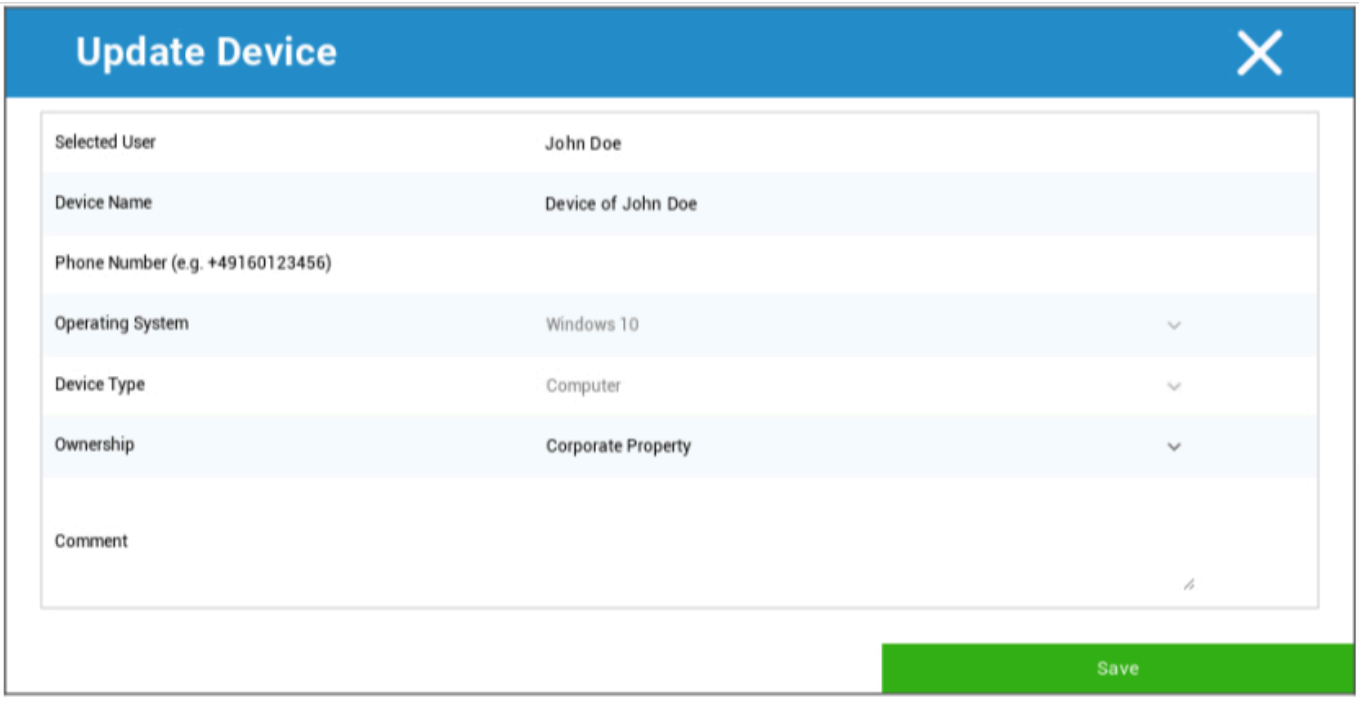
Migreer Android-telefoon-/tabletprofiel naar AE-profiel voor volledig beheerd apparaat (Work Managed)

Windows



Naam apparaat	Naam van het geselecteerde apparaat
Apparaat bewerken	Apparaat bewerken
Apparaat verwijderen	Apparaat uit AppTec verwijderen
Ondernemingsvegen	Informatie, apps en profiel verstrekt door AppTec360 worden verwijderd
MDM verwijderen	
TeamViewer afstandsbediening	Bedien het apparaat op afstand met TeamViewer
Inschrijvingsaanvraag verzenden	Registratieverzoek (opnieuw) verzenden

Apparaat bewerken

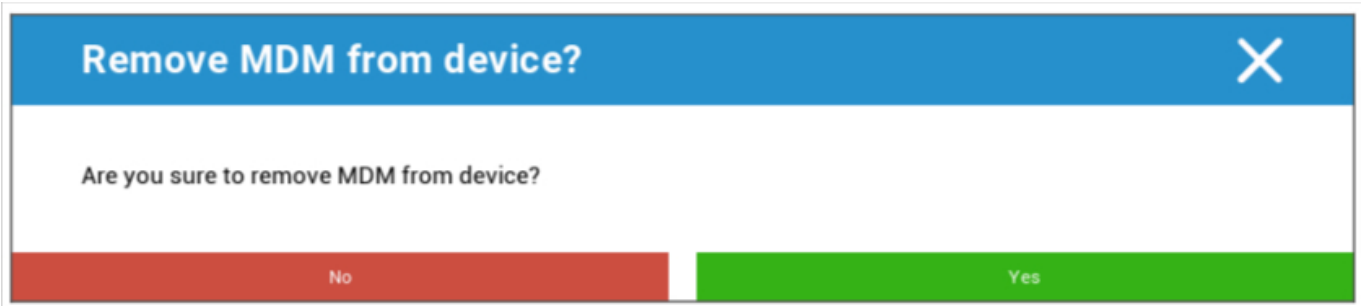


Hier kun je allerlei informatie over het apparaat bijwerken.

Apparaat verwijderen

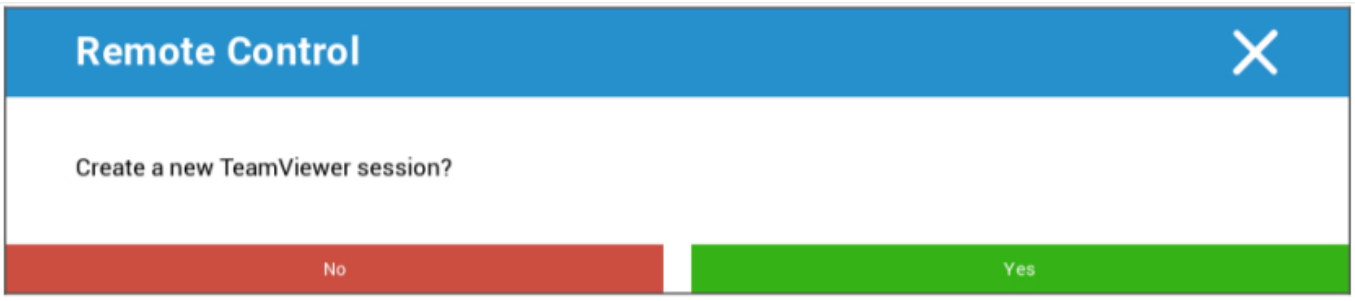
Hier kan de delete-opdracht worden uitgevoerd die alleen het apparaat uit AppTec360 verwijdert.

Wissen | MDM verwijderen



Alleen de door AppTec360 geleverde informatie, apps en profielen worden verwijderd. Op deze manier zijn de bedrijfsgegevens niet langer beschikbaar op het eindgebruikerapparaat. Het privégedeelte wordt niet aangetast en blijft op het eindgebruikerapparaat staan.

TeamViewer afstandsbediening



Hier kunt u een TeamViewer afstandsbedieningssessie starten voor dit apparaat.

Inschrijvingsaanvraag verzenden

Met "Enrollment Request verzenden" kun je (nogmaals) een Enrollment Request verzenden naar de betreffende gebruiker.

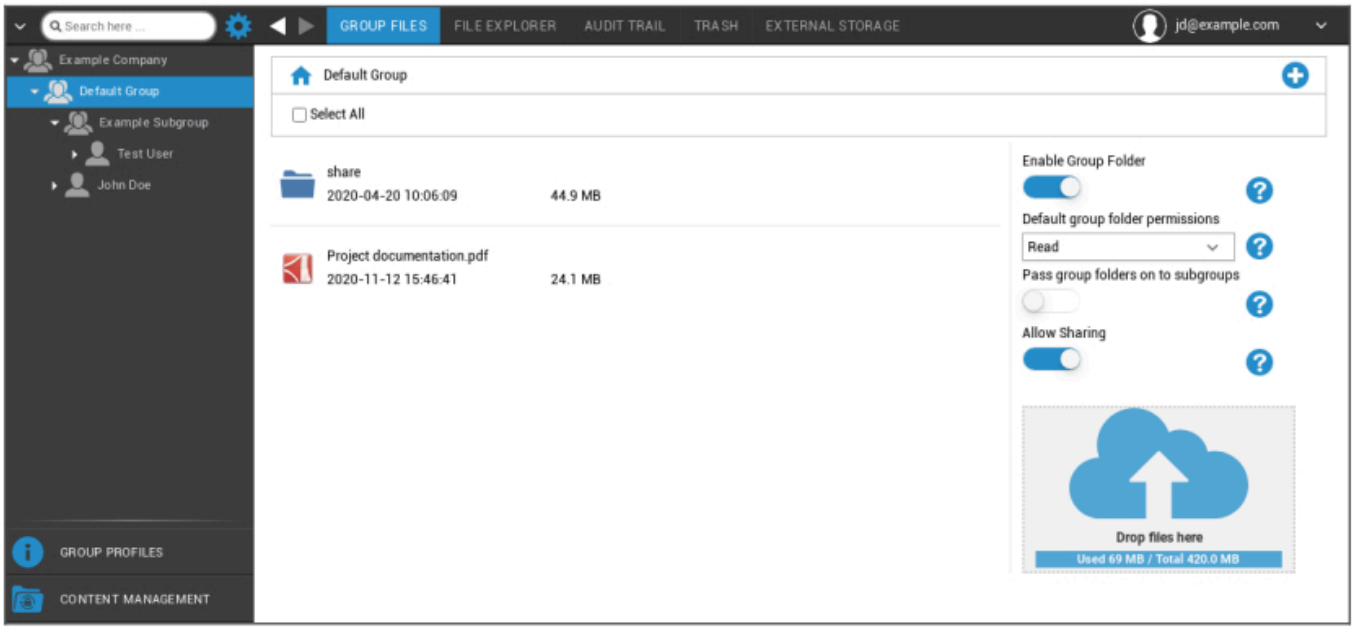
Beheer van inhoud

Als je in een groep zit, kun je AppTec's ContentBox beheren met "Contentbeheer".

Met de Content Box kun je documenten en andere bedrijfsgegevens veilig verspreiden naar de eindgebruikersapparaten.

Groepsbestanden

"Groep Bestanden" is een fundamenteel onderdeel van ContentBox. Hier kun je instellingen maken, documenten uploaden, nieuwe mappen maken, enz.



Met het symbool in de rechterbovenhoek kun je nieuwe mappen maken die worden toegewezen aan de respectieve groep met "Map toevoegen".

Met het symbool in de rechterbovenhoek kun je een nieuwe map aanmaken via "Map toevoegen", die moet worden toegewezen aan de respectieve groep.

Je kunt de map elke naam geven die je wilt.

Via "Bestanden uploaden" kun je gegevens uploaden. Hier wordt je Standaard Verkenner geopend. Je kunt deze twee acties natuurlijk in elke (sub)map uitvoeren.

Met het symbool in de linkerbovenhoek kun je terugkeren naar het hoofdmenu.

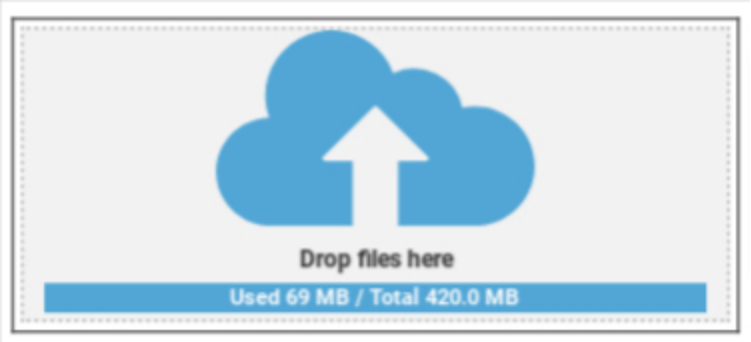
Je kunt verschillende mappen en bestanden selecteren en ze downloaden met "Downloaden" of je kunt ze wissen door op "Verwijderen" te klikken.

Je kunt ook alle bestanden en mappen selecteren en de opdrachten "Downloaden" en "Verwijderen" uitvoeren.

Als je met je muis over een map of bestand beweegt, zie je het volgende overzicht:

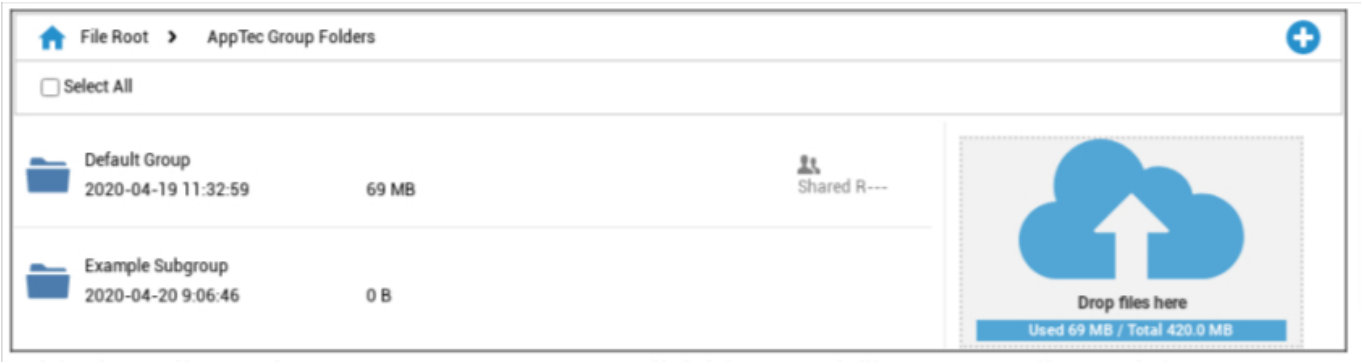
- Met "Hernoemen" kunt u de naam van de map/het bestand wijzigen
- Met "Downloaden" kunt u de map/het bestand downloaden
- Met "Verwijderen" kunt u de map/het bestand verwijderen

Groepsmap inschakelen	Indien geactiveerd, hebben alle leden van de groep toegang tot de betreffende map.
Standaardmachtigingen voor groepsmappen	Machtigingen van de gebruikers in de geselecteerde groep: Lezen = alleen lezen toegestaan Update = update-toestemming Maken = toestemming om te maken Verwijderen = toestemming verwijderen
Groepsmappen doorgeven aan subgroepen	Indien geactiveerd, hebben de respectieve subgroepen toegang tot de bovenliggende gegevensbestanden.
Rechten voor subgroepen	Machtigingen van de gebruikers in de geselecteerde subgroep: Lezen = alleen lezen toegestaan Update = update-toestemming Maken = toestemming om te maken Verwijderen = toestemming verwijderen
Delen toestaan	Indien geactiveerd, kan de gebruiker bestanden delen via een link



Om bestanden te uploaden, kun je dit veld gebruiken door een bestand via Drag & Drop naar dit venster te slepen. Je kunt ook op dit veld klikken om een bestand te selecteren en te uploaden met behulp van Internet Explorer.

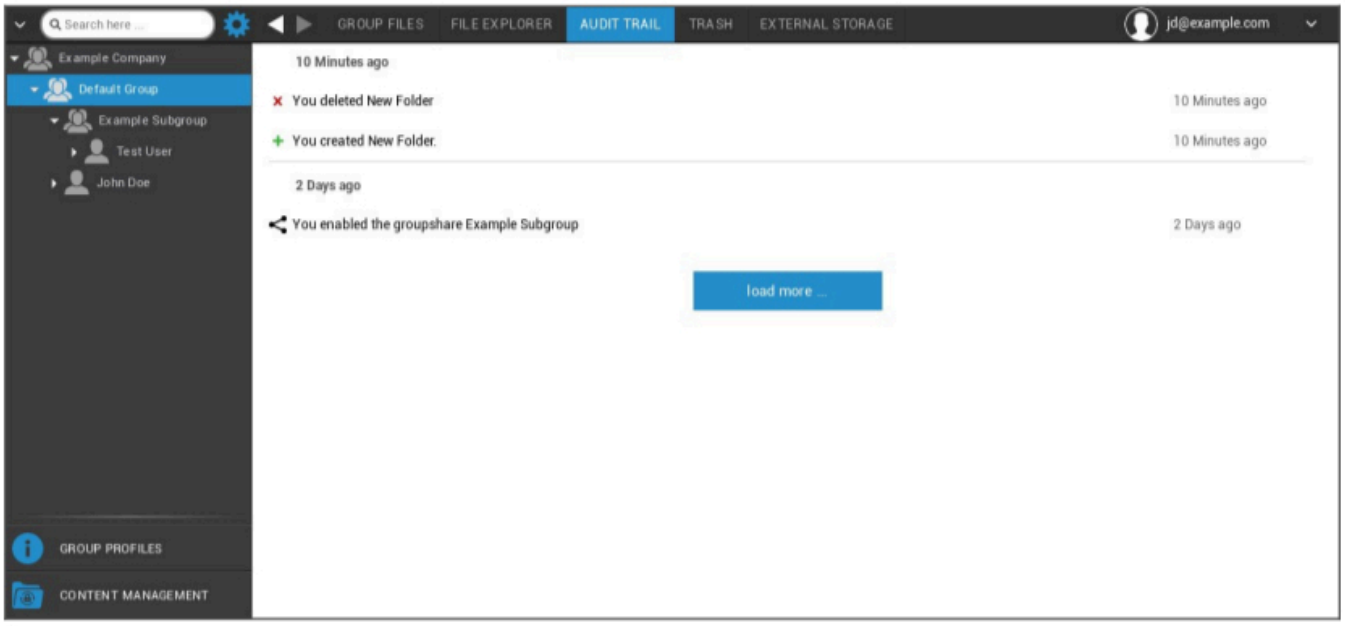
Bestandsbeheer



Met de "File Explorer" kun je alle mappen en bestanden beheren, ongeacht de groep waarin ze zijn opgeslagen.

Je vindt hier ook de instellingen en knoppen waarover je hebt geleerd in "Bestanden groeperen".

Controlespoor



In "Audit Trail" kun je in de geschiedenis zien welke gebruiker wat heeft aangemaakt, verwijderd of gedeeld. Zo kun je op elk moment vaststellen wat er met de bedrijfsgegevens is gedaan.

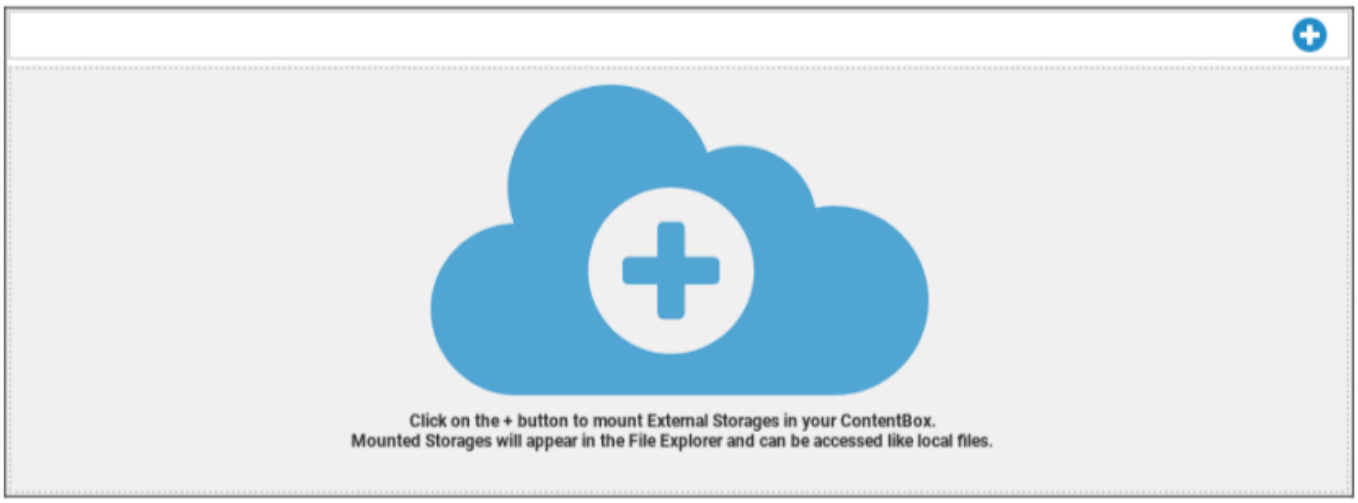
Vuilnis

Als je (per ongeluk) iets hebt verwijderd, kun je de mappen en bestanden onder "Prullenbak" zien en ze naar wens herstellen.

- Met "Undelete" kun je de gegevens/map herstellen.
- Met "Verwijderen" kun je de gegevens/map definitief verwijderen - je moet de opdracht verwijderen nog een keer bevestigen.

Houd er rekening mee dat de opslagcapaciteit die wordt gebruikt in de prullenbak, de beschikbare "Totale ruimte" vermindert - dit is een vereiste van ownCloud.

Externe opslag



Onder de kop "Externe opslag" kunt u externe opslag aansluiten.

Met het symbool kan (extra) opslag worden toegevoegd.

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

Amazon S3	
Naam weergeven	Naam weergeven
Toegangssleutel	Toegangssleutel
Geheime sleutel	Veiligheidssleutel
Emmer	Definitieve identiteit van de submap die aan u is toegewezen
Hostnaam (optioneel)	Hostnaam (optioneel)
Poort (optioneel)	Poort (optioneel)
Regio	Regio (optioneel)
SSL inschakelen	SSL inschakelen
Padstijl inschakelen	Duidelijk padadres dat aan jou is toegewezen

FTP	
Naam weergeven	Naam weergeven
Gastheer	Host-Adres
Gebruikersnaam	Gebruikersnaam
Wachtwoord	Wachtwoord
Wortel	Hoofdmenu
Beveilig ftps://	

SFTP	
Naam weergeven	Naam weergeven
Gastheer	Host-Adres
Gebruikersnaam	Gebruikersnaam
Wachtwoord	Wachtwoord
Wortel	Hoofdmenu

ownCloud	
Naam weergeven	Naam weergeven
URL	ownCloud URL
Gebruikersnaam	Gebruikersnaam
Wachtwoord	Wachtwoord
Externe submap	Standaard map
Beveilig https://	

WebDAV	
Naam weergeven	Naam weergeven
URL	WebDAV URL
Gebruikersnaam	Gebruikersnaam
Wachtwoord	Wachtwoord
Wortel	Hoofdmenu
Beveilig https://	
Windows delen	Ondersteuning voor Windows Share is binnenkort beschikbaar
SharePoint	Ondersteuning voor Microsoft SharePoint is binnenkort beschikbaar

Controlelogboek

Hier vind je een logboek waarin informatie wordt opgeslagen over acties die worden uitgevoerd in de MDM-console.

Met het filterpictogram kun je filters toepassen op de weergegeven lijst.

Met het vervolgkeuzemenu **Items per pagina**: kun je het aantal items selecteren dat op één pagina van de lijst moet worden weergegeven.

Actie ondernomen / Instelling gewijzigd	De actie die werd ondernomen / De instelling die werd gewijzigd
Waarde	De waarde van de ondernomen actie / gewijzigde instelling
Gebruiker	De naam van de gebruiker die de actie heeft uitgevoerd / de instelling heeft gewijzigd
Datum	De tijdstempel van wanneer deze actie werd ondernomen / deze instelling werd gewijzigd
Pad / Type	Het pad naar waar deze actie werd ondernomen / deze instelling werd gewijzigd

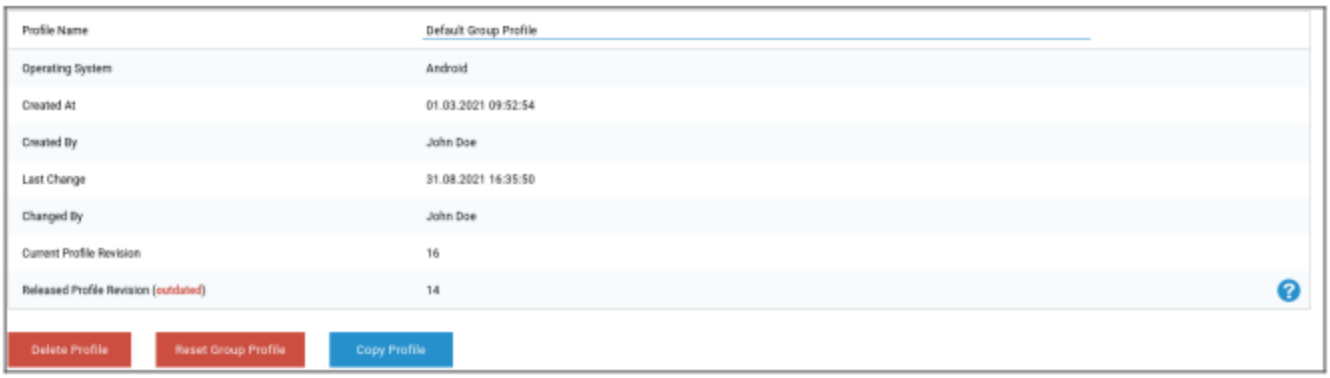
iOS-configuratie

Algemeen

Afhankelijk van of je momenteel een groep of een apparaat hebt geselecteerd, zijn het scherm en de subpunten anders - let hier goed op!

Overzicht groepsprofiel (alleen op groepsniveau)

Wanneer je een groepsprofiel opent, krijg je een snel overzicht van het profiel



Profielnaam	Naam van het profiel (kan hier worden gewijzigd)
Besturingssysteem	Besturingssysteem waar het profiel voor is
Gemaakt op	Tijd van creatie
Gemaakt door	De maker van het profiel
Laatste wijziging	Tijdstip van laatste wijziging van het profiel
Veranderd door	Account die de laatste wijzigingen heeft aangebracht
Huidige profielherziening	Revisie van opgeslagen profielstatus
Vrijgegeven profiel Revisie	Toegewezen profielrevisie ("Nu toewijzen"). Als er "(verouderd)" achter de tekst staat, betekent dit dat je het profiel hebt opgeslagen maar nog niet hebt toegewezen, zodat de apparaten nog steeds een oudere versie krijgen.

Algemene informatie

Als je direct op het apparaat bent, krijg je een kort overzicht van het geselecteerde apparaat.

Naam apparaat	Naam apparaat
Telefoonnummer	Telefoonnummer apparaat
Model	Modelnummer
Besturingssysteem	OS
Serienummer	Serienummer apparaat
Apparaateigendom	Bedrijfs- of privéapparaat Corporate = bedrijfsapparaat Werknemer = privéapparaat
Type apparaat	Type apparaat (tablet of telefoon)
Jailbroken	Als er een Jailbreak op het apparaat is
Onder toezicht	Geeft aan of dit een apparaat is dat onder toezicht staat
Conform	Als er richtlijnen zijn overtreden
Laatst gezien	Status van wanneer het apparaat voor het laatst heeft gecommuniceerd met de AppTec360 Server

Instellingen

Deze instellingen bevatten de naam van het apparaat en een voorgedefinieerde achtergrond.

Naam apparaat naar systeemnaam	De naam die wordt uitgegeven in de AppTec360 Console (in de linker hiërarchiestructuur) is dezelfde als op het betreffende eindgebruikerapparaat (te zien in de apparaatinstellingen).
Aangepaste achtergrond gebruiken (alleen apparaten onder toezicht)	Hier kun je vooraf de achtergrond definiëren die moet worden weergegeven op het apparaat van de eindgebruiker (bijv. voor een soort bedrijfsbranding voor het apparaat). Is alleen beschikbaar in de bewaakte modus!
Automatische OS-updates	Forceert OS-updates indien beschikbaar. Alleen voor DEP-apparaten in bewaakte modus.
Aangepaste lettertypen	Hier kun je aangepaste lettertypen toevoegen.
Naam	Optioneel. De door de gebruiker zichtbare naam voor het lettertype. Dit veld wordt na de installatie vervangen door de werkelijke naam van het lettertype.
Lettertype	Upload het lettertypebestand (.otf of .ttf).

Configuratie Revisie

Hier krijg je een overzicht van welk groepsprofiel is toegewezen aan het apparaat.

Als je op het groepsprofiel klikt, krijg je direct toegang tot het profiel en kun je instellingen uitvoeren.

Met het symbool kun je de toegewezen apps terugzetten naar de instellingen van het groepsprofiel.

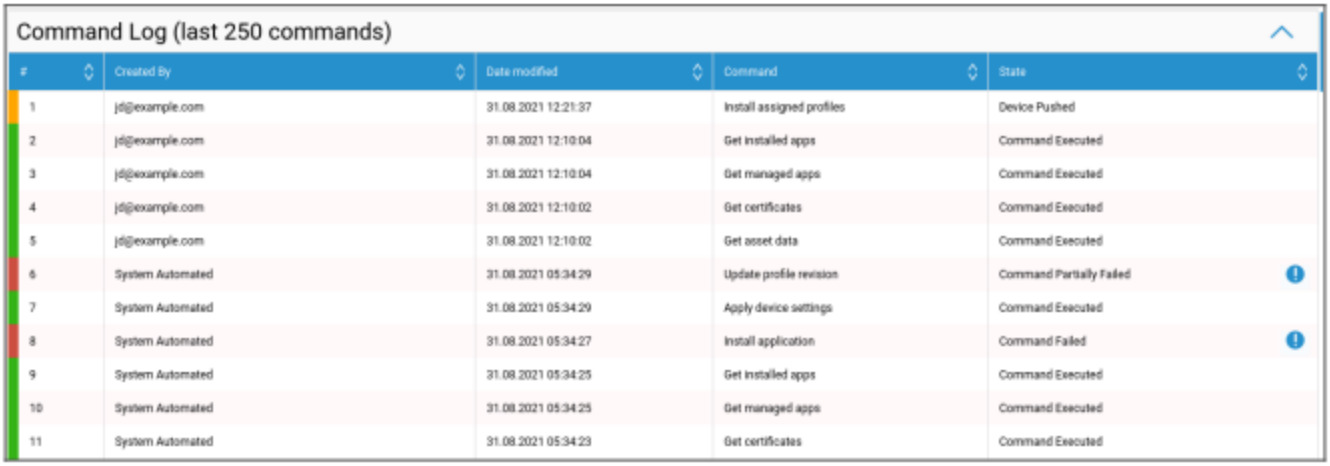
Met het symbool kun je het apparaatprofiel resetten zodat er helemaal geen instellingen zijn.

"Newer Revision available" geeft aan dat het groepsprofiel gewijzigd en opgeslagen is, maar niet toegewezen. Het groepsprofiel moet worden toegewezen met "Assign now" op groepsniveau om de wijzigingen toe te passen op de apparaten.

Apparaatlogboek (alleen op apparaatniveau)

Opdrachtlogboek

Hier kun je zien welke commando's zijn uitgegeven voor het apparaat en wat hun status is.



Commando's die zijn aangemaakt door "System Automated" worden automatisch aangemaakt door het systeem.

Mogelijke opdrachtstatussen

Apparaat ingedrukt	Er is een pushverzoek verzonden naar de pushservice (bijv. APNS) om het apparaat te vertellen terug verbinding te maken met de EMM-server.
Commando aangemaakt	De opdracht is aangemaakt in het systeem.
Opdracht verzonden	De opdracht werd naar het apparaat gestuurd nadat het verbinding had gemaakt met de server.
Opdracht uitgevoerd	De opdracht is succesvol uitgevoerd.
Opdracht mislukt	De opdracht is mislukt. *
Commando gedeeltelijk mislukt	Afhankelijk van het besturingssysteem van het apparaat kunnen sommige commando's gegroepeerd worden. Hierin zijn sommige delen van deze commandogroep mislukt. *
Opdracht uitgevoerd, uiteindelijk mislukt	Het commando werd uitgevoerd, maar misschien ook niet.
Commando verplaatst	De opdracht is opnieuw uitgevoerd door een gebruiker.
Afgedankt	De opdracht is verwijderd. Bijvoorbeeld omdat het is vervangen door een ander commando of omdat het apparaat opnieuw is aangemeld en oude commando's zijn verwijderd.

Als er een uitroepteken achter het bericht staat, kun je meer informatie krijgen door met je cursor over het pictogram te gaan.

Activabeheer (alleen op apparaatniveau)

Activabeheer (alleen op apparaatniveau)

Apparaat info

Model	Modelnummer van het apparaat
Besturingssysteem	OS
OS versie	OS-versie
Serienummer	Serienummer
UDID	Apparaat UDID
Naam apparaat	Naam apparaat
Onder toezicht	Geeft aan of het apparaat onder toezicht staat
Batterijstatus	Batterijstatus

Wi-Fi

IP-adres	IP-adres apparaat
WiFi MAC	WiFi-MAC-adres

Cellulair

Status	Status (SIM-kaart aanwezig)
Telefoonnummer	Telefoonnummer
Roaming-status	Huidige roamingstatus
Roaming (spraak/data)	Roamingstatus voor spraak/data
IP-adres	IP-adres
IMEI	IMEI-nummer
Exploitant/vervoerder	Mobiele dienstverlener
SIM-dragernetwerk	SIM-draagnetwerk
Dragerversie	Draagversie
Modem firmware	Modem firmware
Huidige MCC/MNC	Zie "SIM MCC/MNC".
SIM MCC/MNC	De mobiele landcode is een vastgestelde landidentificatie door de ITU volgens de E.212-norm, die samen met de mobiele netwerkcode (MNC) wordt gebruikt om een mobiel netwerk te identificeren (=landcode). Als je naar een ander mobiel netwerk gaat, zijn de "Current MCC/MNC" en "SIM MCC/MNC" dus verschillend.

Bluetooth

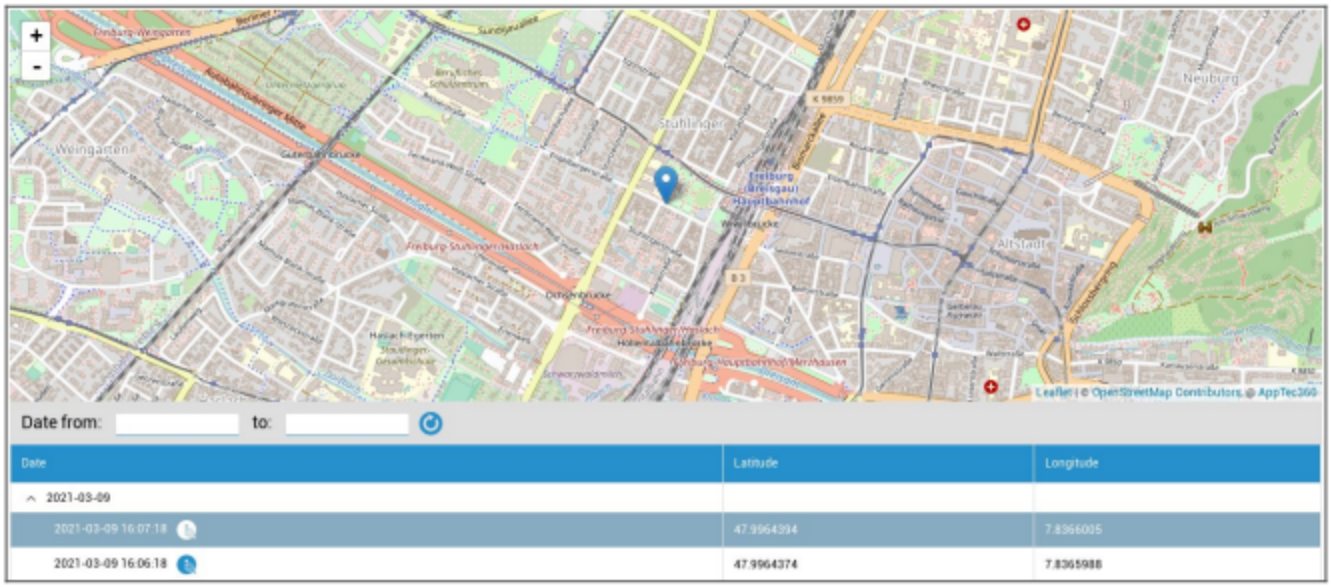
Bluetooth MAC	Bluetooth MAC-adres

Beveiligingsbeheer

Anti diefstal (alleen op apparaatniveau)

GPS-informatie (alleen op apparaatniveau)

Hier kun je de huidige/laatste locatie van het apparaat bepalen. De lokalisatie kan worden beveiligd met één of zelfs twee wachtwoorden - Zie: Algemene instellingen - Privacy - GPS-toegang



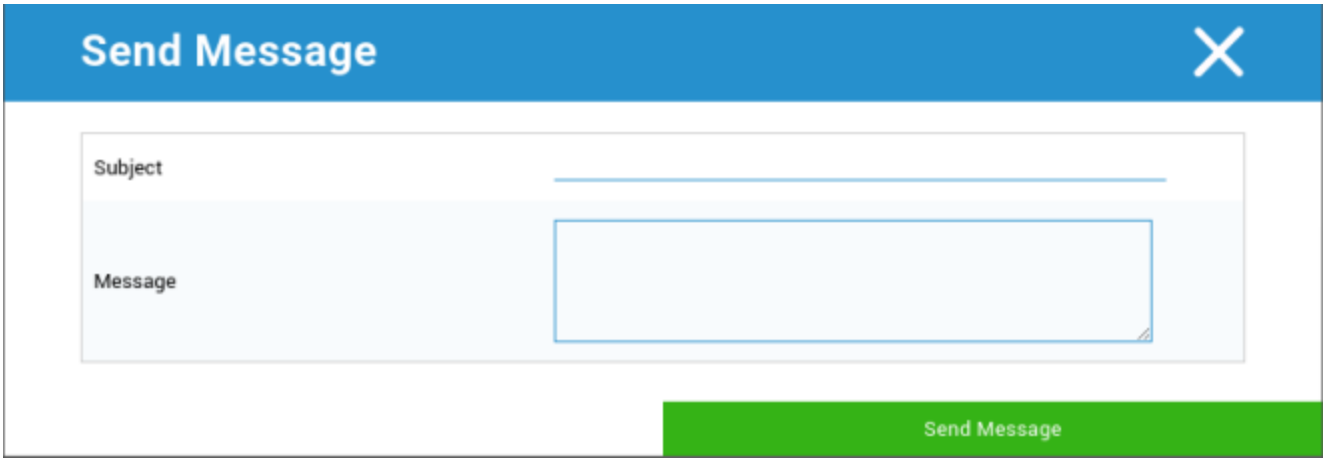
Vegen en vergrendelen (alleen op apparaatniveau)

Onder "Wissen & vergrendelen" kun je de volgende drie acties uitvoeren:

Volledig wissen	Het apparaat wordt teruggezet naar de fabrieksinstellingen (bedrijfs- en persoonlijke gegevens worden gewist)
Ondernemingsvegen	Alleen bedrijfsgegevens worden verwijderd van het apparaat van de eindgebruiker (alle apps, gegevens, enz. die werden geleverd door AppTec)
Vergrendelscherm	Schermvergrendeling is geactiveerd, het is voldoende om het apparaat te ontgrendelen met het apparaatwachtwoord/PIN
Forensische vergrendeling (alleen apparaten onder toezicht)	Als deze functie wordt geactiveerd met het symbool  , wordt het apparaat vergrendeld door een bericht weer te geven dat niet kan worden gesloten. De werknemer kan het apparaat ook niet ontgrendelen. Alleen de beheerder kan het apparaat in de console ontgrendelen met het symbool ontgrendelen  .
Activeringsslot toestaan (alleen apparaten onder toezicht)	Als deze functie is geactiveerd, wordt het apparaat vergrendeld zodra "Zoek mijn iPhone" is geactiveerd in de iCloud-instellingen.

Bericht (alleen op apparaatniveau)

In het volgende venster kun je het onderwerp en een bericht invullen en naar een eindgebruiker verzenden:



Beveiligingsconfiguratie

Wachtwoord

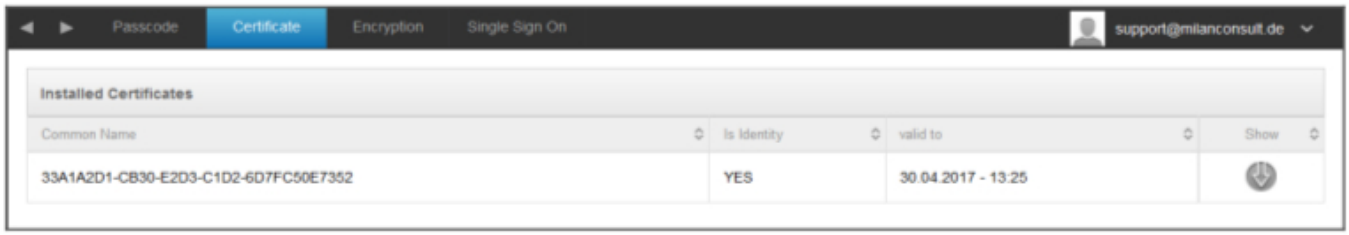
Hier stel je de instellingen voor het wachtwoord van het apparaat in

Code deactivering toegestaan	Als deze instelling geactiveerd is, wordt er niet gevraagd om een wachtwoord in te voeren. Zodra een wachtwoord is ingesteld, kan het niet worden gedeactiveerd.
Eenvoudige waarde toestaan	De gebruiker toestaan om dezelfde, escalerende en reducerende nummerreeksen te gebruiken (bijv. 1234, 1111)
Alfanumerieke waarde vereisen	Wachtwoorden moeten ten minste één letter bevatten
Minimale lengte wachtwoord	Minimale wachtwoordlengte
Minimumaantal complexe tekens	Minimaal aantal alfanumerieke symbolen in het wachtwoord
Maximale leeftijd wachtwoord	Aantal dagen waarna het wachtwoord moet worden gewijzigd
Maximale automatische vergrendeling	Maximale tijd waarna het apparaat wordt vergrendeld
Maximale respijtperiode voor apparaatvergrendeling	Tijd, waarna het apparaat naar de vergrendelde Stand-By
Maximum aantal mislukte pogingen	Bepaalt hoe vaak een wachtwoord verkeerd kan worden ingevoerd voordat het apparaat volledig wordt gewist.
Maximumleeftijd wachtwoord (1-730 dagen)	Maximale wachtwoordleeftijd
Wachtwoordgeschiedenis (1-50 wachtwoordcodes)	Het gebruik van een oud wachtwoord is toegestaan na dit nummer

Een klik op de prullenbak opent het dialoogvenster Password-Reset, waarmee een vergeten apparaatwachtwoord kan worden gewist.

Certificaat (alleen op apparaatniveau)

Geeft de certificaten weer die beschikbaar zijn op het apparaat


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

Encryptie

Opslagversleuteling vereisen	Activeer de encryptiefunctie van het geïnstalleerde apparaat

Eenmalige aanmelding

Onder het punt "Single Sign-On" kun je de Kerberos authenticatie configureren.

Hier stel je de toegangsgegevens in en de respectievelijke URL's / Apps die de Kerberos Tokens mogen gebruiken.

Beschikbaar in bewaakte modus	
Naam rekening	Naam rekening
Voornaam	Unieke identiteit waarnaar Kerberos tickets kunnen worden gedistribueerd
Realm	Je Kerberos Realm, die gebruikt moet worden (bijv. je Domein)

Met het Symbool kun je extra URL's aanmaken.

URL-patroon gebruikt om deze account te beperken	Nader te bepalen URL's waarnaar Kerberos Tickets kunnen worden gedistribueerd

Met het Symbol kunt u extra Apps maken.

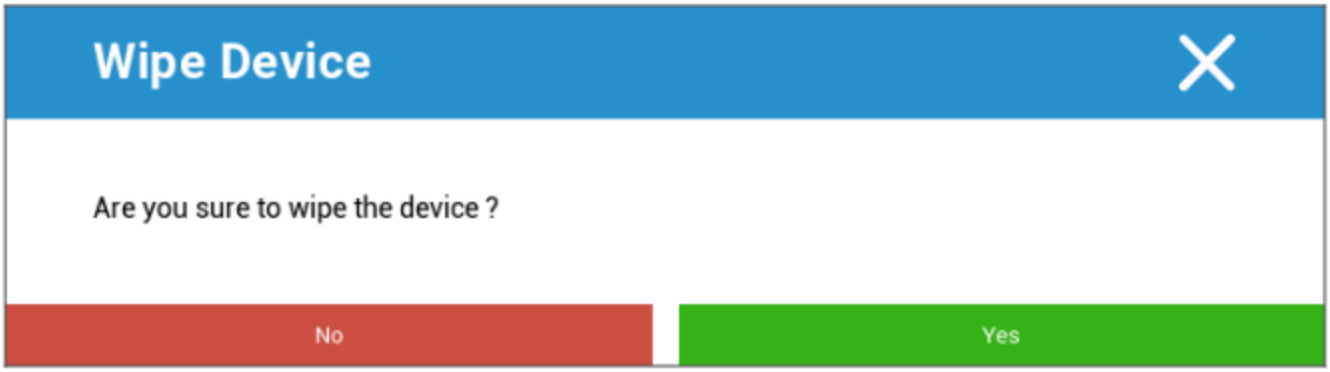
Apps om dit account te beperken	Nader te bepalen Apps, waarnaar Kerberos Tickets kunnen worden gedistribueerd

Einde levensduur (alleen op apparaatniveau)

Vegen (alleen op apparaatniveau)

Onder "Wissen" kun je het apparaat herstellen naar de fabrieksinstellingen. Hier worden de bedrijfs- en privégegevens op het eindgebruikerapparaat gewist.

Als je op het "Minus-symbool" klikt, zou je het volgende bericht moeten krijgen



Met "Ja" kunt u het wissen uitvoeren.

Onder "Wipe Report" kunnen de volgende items worden weergegeven

Gewist door	Geschiedenis van wie het afvegen heeft uitgevoerd
Datum	Datum
Status	Status (bijv. of het wissen met succes is uitgevoerd)

Beperkende instellingen

Functionaliteit van het apparaat

Hier kun je individuele functies van eindgebruikers blokkeren

Installeren van apps toestaan	Installeren van apps toestaan
Camera toestaan	Het gebruik van de camera toestaan
FaceTime toestaan	FaceTime toestaan
Schermopname toestaan	Schermopname toestaan
Automatische synchronisatie tijdens roaming toestaan	Automatische synchronisatie tijdens roaming toestaan
Siri toestaan	Siri toestaan
Spraakgestuurde nummerkeuze toestaan	Spraakgestuurde nummerkeuze toestaan
In-app aankoop toestaan	In-app aankoop toestaan
iTunes Store-wachtwoord vereisen voor alle aankopen	iTunes Store-wachtwoord vereisen voor alle aankopen
Gamen met meerdere spelers toestaan	Gamen met meerdere spelers toestaan
Het toevoegen van Game Center-vrienden toestaan	Het toevoegen van Game Center-vrienden toestaan
Openen toestaan van beheerd naar onbeheerd	Openen van inhoud in beheerde apps in onbeheerde apps toestaan
Openen van onbeheerd naar beheerd toestaan	Openen van inhoud in onbeheerde apps in beheerde apps toestaan
Vandaag bekijken in vergrendelscherm toestaan	Als deze instelling actief is, wordt de "Vandaag"-weergave weergegeven in het Berichtencentrum op het vergrendelscherm.
Bedieningscentrum toestaan in vergrendelscherm	Control Center toestaan op het vergrendelscherm
TouchID toestaan	TouchID toestaan
Over-the-air PKI-updates toestaan	Over-the-air PKI-updates toestaan

Pasboek toestaan terwijl het vergrendeld is	Pasboek toestaan terwijl apparaat is vergrendeld
Het volgen van advertenties beperken	Deze functie schakelt Ad Tracking uit (adverteerders kunnen Ad Tracking bijvoorbeeld niet gebruiken om gepersonaliseerde advertenties te verspreiden).
Handoff toestaan	Handoff toestaan
Internetresultaten in spotlight weergeven	Internetresultaten toestaan in spotlight (bijv. Bing of Wikipedia)
Wachtwoord vereist bij eerste AirPlay-koppeling	Wachtwoord vereist bij eerste AirPlay-koppeling
Force horloge polsbescherming	Indien geactiveerd, wordt de Apple Watch gedwongen om "polsbescherming" (polsherkenning) te gebruiken.
iCloud-fotobibliotheek toestaan	Staat de iCloud-fotobibliotheek toe. Als dit niet is toegestaan, worden alle foto's die niet volledig zijn gedownload van iCloud, gewist op de lokale opslag.
Beschikbaar in de bewaakte modus	
Accountwijziging toestaan	Wijziging van "mail, contactpersonen, agenda" toestaan
AirDrop toestaan	AirDrop toestaan
App Cellulaire Wijziging toestaan	Deze instelling blokkeert de instelling voor welke apps mobiele gegevens mogen gebruiken Deze instelling kan bijvoorbeeld handmatig worden ingesteld op het eindgebruikerapparaat, waarna deze beperking kan worden geactiveerd.
Siri toestaan om door gebruikers gegenereerde inhoud van het web op te vragen	Zoeken op het web op bepaalde websites wordt geblokkeerd, bijv. Wikipedia, omdat iedereen naar believen wijzigingen kan aanbrengen
Siri vloekenfilter inschakelen	Godslastering gericht aan Siri wordt gecensureerd
iBook Store toestaan	iBook Store toestaan
Erotica in iBook Store toestaan	Erotica in iBook Store toestaan
Instellingen voor Zoek mijn vrienden wijzigen toestaan	Instellingen voor Zoek mijn vrienden wijzigen toestaan
Game Center toestaan	Game Center toestaan
Host koppelen toestaan	Computer koppelen

Installatie van configuratieprofielen toestaan	Installatie van configuratieprofielen toestaan
App verwijderen toestaan	Controle apps verwijderen
iMessage toestaan	iMessage toestaan
Sta wissen van alle inhoud en instellingen toe	Het wissen van alle inhoud en instellingen toestaan
Configureren van beperkingen toestaan	Configureren van beperkingen toestaan
Podcast toestaan	Podcast toestaan
Definitie opzoeken toestaan	Definitie opzoeken toestaan
Voorspellend toetsenbord toestaan	Voorspellend toetsenbord toestaan
Automatische correctie toestaan	Automatische correctie toestaan
UI App installatie toestaan	Als deze optie is uitgeschakeld, kunnen er geen apps worden geïnstalleerd vanuit de openbare AppStore (het pictogram wordt niet meer weergegeven). Apps kunnen echter nog steeds worden geïnstalleerd via iTunes en de Configurator
Toetsenbord snelkoppelingen toestaan	Toetsenbordsnelkoppelingen toestaan als het apparaat is aangesloten op een fysiek toetsenbord
Koppeling met Apple Watch toestaan	Verbiedt een koppeling tussen het apparaat en de Apple Watch, bestaande verbindingen worden verbroken.
Wijziging van wachtwoord toestaan	Als dit niet is toegestaan, kan er geen wachtwoord voor het apparaat worden toegevoegd, gewijzigd of verwijderd.
Wijziging van devicenaam toestaan	Richtlijn om te bepalen of de apparaatnaam kan worden gewijzigd
Wijziging van achtergrond toestaan	Richtlijn om te bepalen of het behang kan worden veranderd
Automatische app downloads toestaan	Indien gedeactiveerd, wordt een gekochte app niet automatisch geïnstalleerd op andere apparaten. Geldt niet voor updates voor bestaande apps
Nieuws	Nieuws toestaan op het iOS-apparaat
Enterprise app vertrouwen toestaan	Als dit is ingesteld op false, wordt voorkomen dat zakelijke apps worden vertrouwd

iCloud

Bepaalde functies blokkeren tijdens het koppelen van iCloud

Back-up toestaan	Back-up toestaan
Document sync toestaan	Document sync toestaan
Fotostream toestaan	Fotostream toestaan
Gedeelde fotostream toestaan	Gedeelde fotostream toestaan
Cloud-sleutelhangersynchronisatie toestaan	Cloud-sleutelhangersynchronisatie toestaan
Sta beheerde apps toe om gegevens op te slaan	Sta beheerde apps toe om gegevens op te slaan
Synchronisatie van notities en hoogtepunten toestaan voor ondernemingsboeken	Synchronisatie van notities en hoogtepunten toestaan voor ondernemingsboeken
Back-up van bedrijfsboeken toestaan	Back-up van bedrijfsboeken toestaan

Veiligheid en privacy

Blokkeer deze functionaliteiten in verband met diagnostische gegevens

Diagnostische gegevens naar Apple laten sturen	Diagnostische gegevens naar Apple laten sturen
Gebruiker toestaan om niet-vertrouwde TLS-certificaten te accepteren	Gebruiker toestaan om niet-vertrouwde TLS-certificaten te accepteren
Versleutelde back-ups forceren	Versleutelde back-ups forceren

BYOD

Ingebouwde iOS-beveiliging (Container)

iOS heeft altijd een verschil kunnen maken tussen managed (zakelijk) en unmanaged (privé). Alles wat afkomstig is van het MDM systeem wordt behandeld als beheerd. Als je bijvoorbeeld een app installeert via MDM of een Exchange-account configureert, wordt dit behandeld als beheerd door iOS.

Al het andere dat handmatig wordt geconfigureerd/geïnstalleerd op het apparaat, wordt behandeld als onbeheerd. Bijvoorbeeld als de gebruiker WhatsApp zelf installeert of een Exchange-account toevoegt. Deze scheiding heeft echter nooit invloed gehad op de contactpersonen. Maar sinds iOS 11.3 (en hoger) is dit ook toegevoegd voor de contactpersonen.

Aangezien dit een basisfunctionaliteit van het besturingssysteem is, hoef je niets te installeren of een speciale container in te stellen.

Activeer de ingebouwde functie om privé en zakelijke toepassingen/informatie/bestanden te scheiden. Deze instelling schakelt ook enkele andere functies uit, die anders per ongeluk delen van deze scheiding zouden kunnen uitschakelen.

Activering

Activeer de Container-oplossingen die worden ondersteund door AppTec360

Google Divide Container inschakelen	Google Divide Container inschakelen
SecurePIM-container inschakelen	SecurePIM-container inschakelen

Als u de SecurePIM Container heeft geactiveerd, vindt u ook het volgende punt onder "Activering". Daarnaast worden er direct nog vier tabbladen geopend, die hieronder worden beschreven.

E-mailadres voor ondersteuning	E-mailadres voor ondersteuning waar een gebruiker terecht kan met problemen

SecurePIM Wachtwoord

Onder "SecurePIM Password" kunt u de richtlijnen voor de beveiligingssterkte van het wachtwoord instellen.

Time-out sessie	Hier kunt u instellen na hoeveel minuten een nieuw wachtwoord opnieuw moet worden ingevoerd als SecurePIM op de achtergrond draait.
Lengte wachtwoord	Wachtwoordlengte voor toegang tot de SecurePIM Container
Hoofdletters	Minimaal hoofdletters
Kleine letters	Minimaal kleine letters
Speciale tekens	Minimale speciale tekens
Cijfers	Minimale cijfers
Veegtoepassing	Aantal keren dat een wachtwoord verkeerd kan worden ingevoerd, voordat de SecurePIM inhoud wordt verwijderd. (De app blijft echter wel op het apparaat van de eindgebruiker staan)

SecurePIM Beveiliging

Onder "SecurePIM Security" kunt u verschillende beveiligingsinstellingen instellen.

Jailbroken apparaten detecteren	Als deze instelling is geactiveerd, wordt de toegang tot de SecurePIM Container geblokkeerd zodra het apparaat wordt gedetecteerd als jailbroken.
Veilige tekstvelden	De inhoud van de invoervelden wordt versleuteld, zodat geen informatie het OS (iOS) bereikt. Opmerking: Zolang deze instelling actief is, is autocorrectie niet langer beschikbaar.
Contactgegevens exporteren naar apparaat	Als deze instelling is geactiveerd, dan mag de gebruiker de Exchange Contacten exporteren naar het lokale apparaat. Opmerking: alleen de naam en het telefoonnummer worden geëxporteerd.
Locatie evenement tonen	Als deze instelling geactiveerd is, wordt de locatie van de komende evenementen weergegeven op de meldingsbalk
Titel evenement weergeven	Als deze instelling geactiveerd is, wordt de locatie van de titel van het komende evenement weergegeven op de meldingsbalk

VeiligePIM-browser

Hier kun je de browser van SecurePIM configureren.

Met het symbool kun je een nieuwe URL definiëren.

Met het symbool kun je een gedefinieerde URL weer verwijderen.

"Whitelisted URL's" zijn URL's die geladen kunnen worden.

"URL's op de zwarte lijst zijn URL's die niet kunnen worden geladen en daardoor worden geblokkeerd.

Merk op dat vermeldingen op de witte lijst een hogere prioriteit hebben dan vermeldingen op de zwarte lijst. Onder "Bladwijzertitel" kunt u een titel opgeven. Met "Bladwijzer-URL" kunt u URL-adressen koppelen aan de bladwijzertitel - op deze manier kunt u geïndividualiseerde bladwijzers distribueren naar de respectieve gebruikers.

Uitwisseling

Onder "Exchange" kunt u een Exchange-account configureren.

ActiveSync e-mailadres	E-mailadres van Exchange (let op de "Placeholders")
ActiveSync Exchange-login	Gebruikersnamen uitwisselen (let op de "Placeholders")
ActiveSync Uitwisselingsserver	Adres Exchange-server (FQDN)
ActiveSync Exchange-domein	Exchange-domeinadres
Gebruikerscertificaat	Gebruikerscertificaat
Certificaatgebaseerde verificatie	Gebruiker verifieert zichzelf met een certificaat
S/MIME-codering toestaan	Hiermee kan de gebruiker zijn e-mail versleutelen
S/MIME ondertekening toestaan	Hiermee kan de gebruiker zijn e-mail ondertekenen
CRL controleren	Als het actief is, wordt het privécertificaat vergeleken met de CRL (Certificate Revocation List).

Verbindingsbeheer

Wi-Fi

Serviceset Identifier (SSID)	SSID van het netwerk waarmee verbinding moet worden gemaakt
Automatisch lid worden	Automatisch lid worden activeren wanneer je lid wordt van een netwerk
Verborgen netwerk	Activeren, als het AP de SSID niet uitzendt

Proxy-instelling

Configuratie van een proxy voor elk toegangspunt

Geen		Geen volmacht vaststellen
Handmatig		Een handmatige proxy instellen
	Proxyserver URL	Adres voor toegang tot proxy-instellingen
	Haven	Stel de poort in voor de proxy
	Authenticatie	Gebruikersnaam voor de verificatie op de proxy
	Wachtwoord	Wachtwoord voor de verificatie op de proxy
Automatisch		Automatisch een proxy instellen
Proxyserver URL		URL voor toegang tot de proxy-instellingen

Type beveiliging

Beveiligingstype instellen voor het AP

WEP	
Wachtwoord	Wachtwoord voor het AP

WPA/WPA2	
Wachtwoord	Wachtwoord voor het AP

WEP Onderneming - WPA / WPA2 Onderneming - Elke Onderneming			
	Protocollen		
	TLS	Activeren/Deactiveren	
	TTLS	Activeren/Deactiveren	
	LEAP	Activeren/Deactiveren	
	PEAP	Activeren/Deactiveren	
	EAP-FAST	Activeren/Deactiveren	
	EAP-SIM	Activeren/Deactiveren	
	Gebruik PAC		Gebruik van PAC (Protected Access Controll)
	Voorziening PAC	Configuratie van voorziening PAC	
	PAC anoniem aanbieden	Anoniem verstrekken van PAC	
	Innerlijke Authenticaties	Authenticatieprotocol dat gebruikt moet worden: PAP, CHAP, MSCHAP, MSCHAPv2	
	Gebruikersnaam	Gebruikersnaam verificatie	
	Gebruik geen wachtwoord per verbinding	Gebruik geen wachtwoord per verbinding	
	Identiteitscertificaat	Verificatiecertificaat uploaden/selecteren	
	Uiterlijke identiteit	Identiteit die van buitenaf zichtbaar is	
	Vertrouwen		
	Betrouwbaar certificaat 1	Eerste vertrouwde certificaat uploaden	
	Betrouwbaar certificaat 2	Tweede vertrouwde certificaat uploaden	
	Betrouwbaar certificaat 3	Derde vertrouwde certificaat uploaden	
	Namen van certificaten voor vertrouwde servers	De namen van de verwachte servercertificaten (in een door komma's gescheiden lijst)	

Geen	Geen beveiliging instellen

VPN

Naam verbinding	Naam van het VPN-profiel

VPN-type

VPN

Al het netwerkverkeer van het apparaat wordt via een VPN-verbinding geleid.

Type aansluiting	Type VPN-verbinding tot stand brengen
IPsec (cisco)	IPsec-protocol door cisco
PPTP	PPTP-protocol
L2TP	L2TP-protocol
Cisco AnyConnect	AnyConnect-protocol
Juniper SSL	Juniper SSL-protocol
F5 SSL	F5 SSL-protocol
SonicWall mConnect	SonicWall mobiel verbinden
Aruba VIA	Aruba VIA-protocol
Aangepaste SSL	Verbinding via aangepaste SSL
OpenVPN	OpenVPN-protocol

VPN per app

Bij het openen van een bepaalde app wordt een VPN-verbinding tot stand gebracht

VPN-verbinding per app automatisch starten		VPN-verbinding per app automatisch starten
Type aansluiting		Type VPN-verbinding tot stand brengen
	Cisco AnyConnect	AnyConnect-protocol
	Juniper SSL	Juniper SSL-protocol
	F5 SSL	F5 SSL-protocol
	SonicWall mConnect	SonicWall mobiel verbinden
	Aruba VIA	Aruba VIA-protocol
	Aangepaste SSL	Verbinding via aangepaste SSL
	OpenVPN	OpenVPN-protocol

Proxy-instelling

Configuratie van een proxy voor de VPN-verbinding

Geen	Geen volmacht vaststellen
Handmatig	Handmatig een proxy aanmaken
Proxyserver URL	Adres voor toegang tot Proxy-instellingen
Haven	Stel de poort in voor de proxy
Authenticatie	Gebruikersnaam voor de verificatie bij de proxy
Wachtwoord	Wachtwoord voor de verificatie bij de proxy
Automatisch	Automatisch een proxy instellen
Proxyserver URL	URL voor toegang tot de proxy-instellingen

Plaatshouders weergeven	Toont alle beschikbare gebruikersvariabelen die AppTec360 kan gebruiken

APN

Naam toegangspunt	Naam toegangspunt
Gebruikersnaam toegangspunt	Gebruikersnaam toegangspunt
Wachtwoord toegangspunt	Wachtwoord toegangspunt
Proxyserver	Adres proxyserver
Haven	De respectieve proxy-poort

Cellulair

Dataroaming inschakelen	Dataroaming inschakelen
Spraak Roaming inschakelen	Spraak Roaming inschakelen
Hotspot inschakelen	Hotspot inschakelen

HTTP-proxy

Type volmacht	
Handmatig	Handmatig een proxy instellen
Proxyserver URL	Adres voor toegang tot de proxy-instellingen
Haven	Proxy-poort instellen
Authenticatie	Gebruikersnaam voor de verificatie bij de proxy
Wachtwoord	Wachtwoord voor de verificatie bij de proxy
Automatisch	Automatisch een proxy instellen
Proxy PAC URL	Proxy PAC URL
Directe verbinding toestaan als PAC onbereikbaar is	Directe verbinding toestaan (zonder VPN) als PAC onbereikbaar is
Proxy omzeilen om toegang te krijgen tot besloten netwerken	Proxy omzeilen om toegang te krijgen tot besloten interne netwerken

AirPrint

IP-adres	IP-adres printer
Bronnenpad	Definitief pad naar het AirPrint-apparaat

AirPlay

Naam apparaat	Naam apparaat
Wachtwoord	Wachtwoord koppelen
Whitelist	Definieer een lijst met apparaten waarmee het apparaat zichzelf exclusief kan koppelen

PIM-beheer

Exchange Actieve Synchronisatie

Naam rekening	Naam e-mailaccount
Exchange ActiveSync Host	Adres/FQDN van de server
Verplaatsing toestaan	Verplaatsen van e-mails toestaan
Alleen gebruiken in post	Interacties kunnen alleen plaatsvinden op de eigen Mail App
SSL gebruiken	SSL-codering gebruiken
Domein	Serverdomein
Gebruiker	Gebruikersnaam
E-mailadres	e-mailadres (alleen op apparaatniveau)
Wachtwoord (alleen op apparaatniveau)	Wachtwoord gebruiker
Identiteitscertificaat	Selecteer het respectieve certificaat voor verificatie op de server
Vroegere dagen van Mail to Sync	Aantal dagen tot de e-mails terug gesynchroniseerd moeten worden. Geen limiet = onbeperkt
S/MIME inschakelen	S/MIME-codering inschakelen
Certificaat ondertekenen	Het betreffende ondertekeningscertificaat uploaden
Encryptiecertificaat	Het coderingscertificaat uploaden

e-mail

POP3 / IMAP-accounts instellen op het apparaat van de eindgebruiker

Account Beschrijving	Naam van e-mailaccounts		
Type rekening	IMAP	Pad Voorvoegsel	Het padvoorvoegsel voor speciale mappen
	POP		
Gebruikersnaam	Weergavenaam gebruiker		
E-mailadres	E-mailadres gebruiker		
Verplaatsing toestaan	Verplaatsen van e-mails toestaan		
S/MIME inschakelen	S/MIME-codering inschakelen		
Certificaat ondertekenen	Het betreffende ondertekeningscertificaat uploaden		
Encryptiecertificaat	Het coderingscertificaat uploaden		

Inkomende post

Inkomende serverinstellingen

Adres mailserver	Adres mailserver
Mail server poort	Mail server poort
Gebruikersnaam	Respectieve gebruikersnaam
Type verificatie	Type verificatie
Geen	Geen verificatietype
Wachtwoord (alleen op apparaatniveau)	Wachtwoord
MDM uitdaging-antwoord	
NTLM	NTLM-authenticatie
HTTP MD5 Digest	
SSL gebruiken	Gebruik SSL, indien nodig

Uitgaande post

Instellingen uitgaande server

Adres mailserver	Adres mailserver
Mail server poort	Mail server poort
Gebruikersnaam	Respectievelijke gebruikersnaam
Type verificatie	
Geen	Geen verificatiemethode
Wachtwoord (alleen op apparaatniveau)	Wachtwoord
MDM uitdaging-antwoord	
NTLM	NTLM-authenticatie
HTTP MD5 Digest	
SSL gebruiken	Gebruik SSL, indien nodig
Uitgaand wachtwoord hetzelfde als inkomend wachtwoord	Uitgaand wachtwoord hetzelfde als inkomend wachtwoord
Alleen gebruiken in post	Activeer als alle uitgaande e-mails moeten worden verzonden via de Mail-App

CalDav

Het opzetten en distribueren van een CalDav-account configureren

Account Beschrijving	Weergavenaam van de account
Hostnaam	Hostnaam en/of IP-adres
Haven	Poort van het CalDav-account
Belangrijkste URL	Belangrijkste URL van de rekening
Gebruikersnaam	Respectieve CalDav-gebruikersnaam
Wachtwoord (alleen op apparaatniveau)	Respectievelijk CalDav-wachtwoord
SSL gebruiken	Gebruik SSL, indien nodig

Geabonneerde kalenders

Instellen en distribueren van geabonneerde kalenders

Beschrijving	Weergavenaam van de account
URL	URL van de kalenderdatabase
Gebruikersnaam	Gebruikersnaam van het kalenderabonnement
Wachtwoord (alleen op apparaatniveau)	Wachtwoord van het kalenderabonnement
SSL gebruiken	Gebruik SSL, indien nodig

LDAP

Stel in dit gebied een LDAP-verbinding in om een dynamische certificaatuitwisseling mogelijk te maken tussen het eindgebruikersapparaat en de Active Directory.

Merk op dat de geselecteerde gebruiker de respectieve leesrechten nodig heeft.

Account Beschrijving	Account Beschrijving
Gebruikersnaam account	Gebruiker voor LDAP-toegang
Wachtwoord	Wachtwoord voor LDAP-toegang
Hostnaam account	Hostnaam/IP-adres LDAP-server
SSL gebruiken	Gebruik SSL, indien nodig

In het tweede deel kun je individuele filters definiëren voor het zoeken in het LDAP-register.

Beschrijving	Toepassingsgebied	Basis zoeken
Beschrijving filter	Zoekniveau in het LDAP-register	Het individuele filter definiëren

Webbeheer

Webclips

Op deze locatie kun je bladwijzers definiëren, met links naar webpagina's, intranetportals enz. die zichtbaar zullen zijn als applicatie op het apparaat van de eindgebruiker.

Label	Naam van de verbinding op het eindgebruikersapparaat
URL	Link naar de desbetreffende website
Verwijderbaar	Indien geactiveerd, kan de gebruiker de webclip verwijderen.
Pictogram	Upload via dit dialoogvenster een logo voor de verbinding: Afmeting 180x180, png-formaat
Vooraf samengesteld pictogram	Indien geactiveerd, worden er geen extra effecten (schaduw, reflectie) weergegeven op het pictogram.
Volledig scherm	Bij het openen van webclips opent de browser op volledig scherm

Filter voor webinhoud

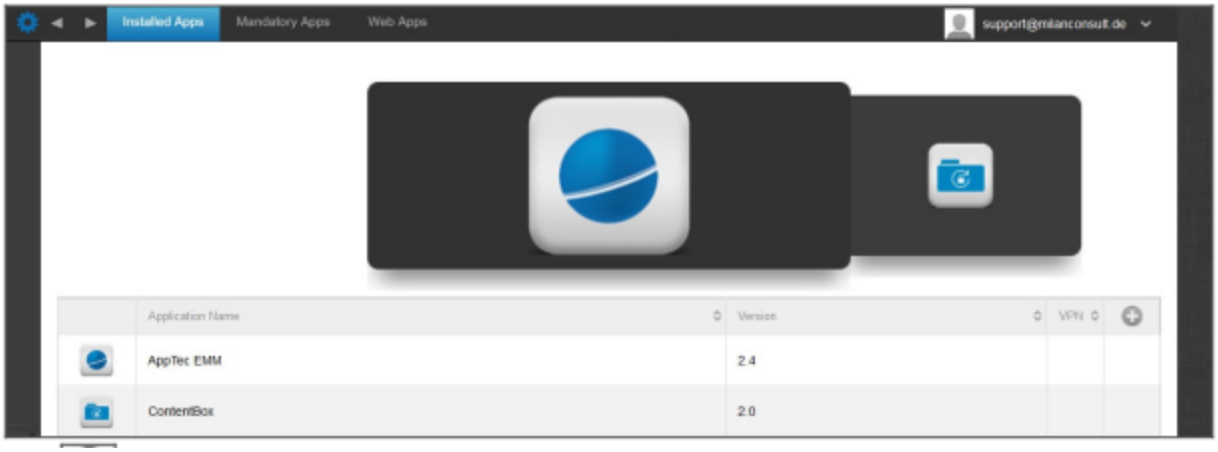
De Web Content Filter maakt het mogelijk om de toegang tot specifieke internetpagina's te beperken.

Toegestane websites	
Inhoud voor volwassenen beperken	Webfilter wordt automatisch toegepast voor inhoud voor volwassenen
Toegestane URL's	Met het + symbool voeg je toegestane pagina's toe
URL's op de zwarte lijst	Met het + symbool voeg je geblokkeerde pagina's toe
Alleen specifieke websites	Alleen specifieke inhoud kan worden weergegeven, die je kunt toevoegen met het + symbool.

App-beheer

Enterprise App Manager

Geïnstalleerde apps (alleen op apparaatniveau)



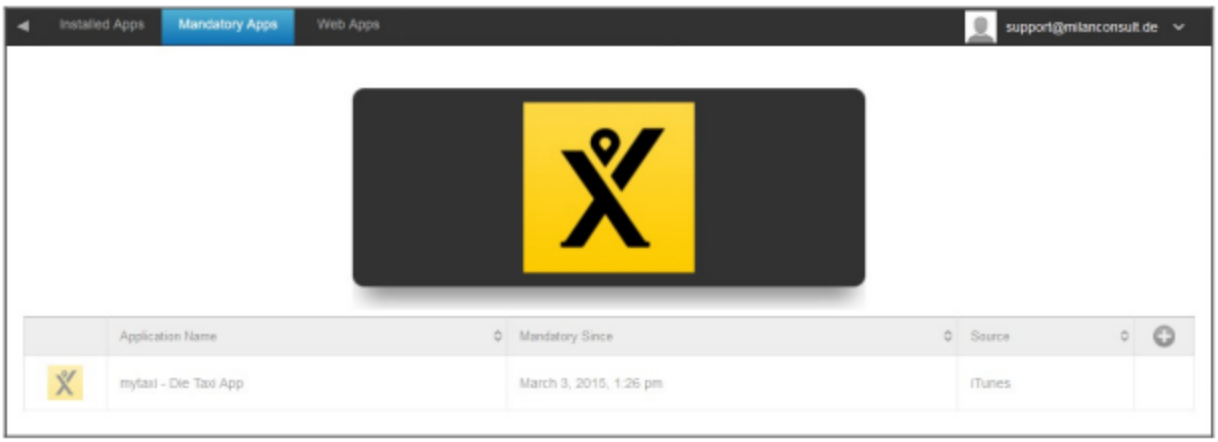
Hier ziet u de Apps die momenteel op het apparaat zijn geïnstalleerd.

Verplichte apps

Onder Verplichte Apps kunt u noodzakelijke Apps verplichten.

De gebruiker wordt er voortdurend aan herinnerd om deze app te installeren.

Via de , kan de gemandateerde App worden gedefinieerd.



Dit kan een Apple App Store App zijn, maar ook een In-House App.

Als dit een apparaat onder toezicht betreft, wordt de app automatisch geïnstalleerd.

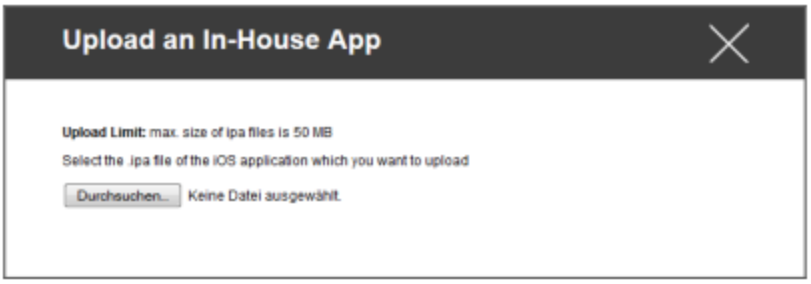
Je kunt een "Apple AppStore" app uit de openbare AppStore naar het apparaat pushen, maar ook een intern ontwikkelde in-house app.

Je kunt ook kiezen uit de categorie "iOS In-House Apps" en een In-House App kiezen die je hebt geüpload onder Algemene instellingen.

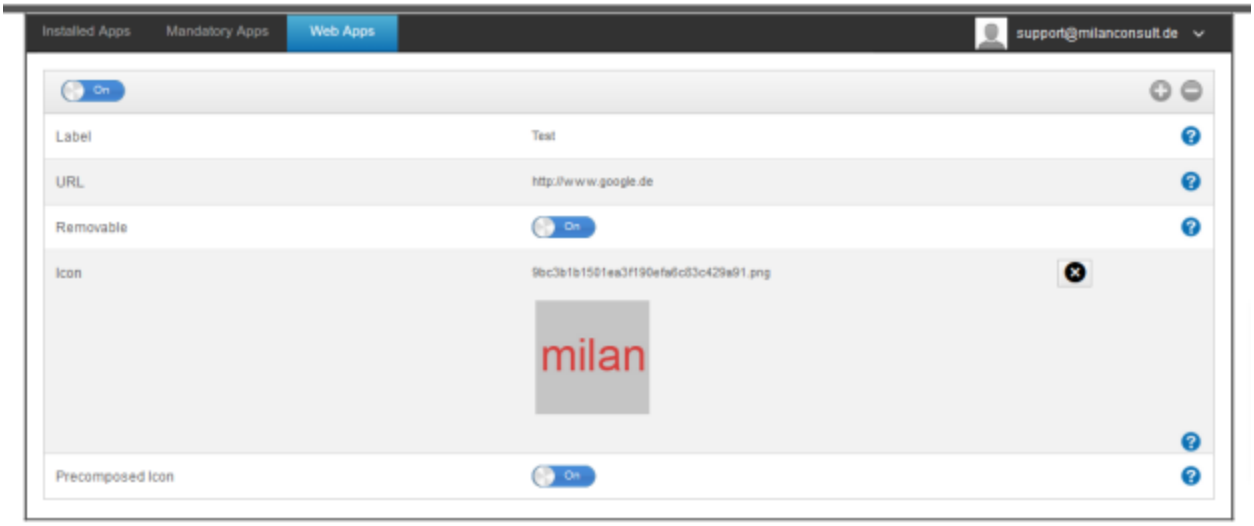
Installatie-opties

Up-to-date houden (alleen ondersteund voor VPP per apparaat)	Eens per week wordt bepaald of er een update is voor de app. Zo ja, dan wordt deze update geïnstalleerd Voor In-House Apps wordt het updatedoel dat u hebt geconfigureerd in Algemene instellingen gebruikt voor het updateproces.
Inhalen wanneer onbeheerd	Als de app al is geïnstalleerd, neemt de MDM de app over en beheert deze.
App verwijderen wanneer MDM-profiel wordt verwijderd	Als het apparaatbeheer wordt verwijderd, wordt de app verwijderd.
Back-up van app-gegevens voorkomen	Er wordt geen back-up van app-specifieke gegevens gemaakt
App-instelling	Onder "App Settings" (App-instellingen) kun je de app bepaalde waarden toewijzen aan de voorgrond (zolang de app dit ondersteunt, vraag indien nodig de ontwikkelaar van de app).

Je kunt ook direct een ipa-bestand selecteren en uploaden via "Eigen app uploaden".



Webtoepassingen



Onder het punt "Web Apps" kun je, net als bij "Web Clips", internetpagina's of intranetportals als een applicatie naar het apparaat van de eindgebruiker pushen in het gebied Webbeheer. Webapps worden standaard in volledig scherm weergegeven, wat kan worden geconfigureerd onder Webclips.

Label	Naam van de verbinding op het eindgebruikersapparaat
URL	Link naar de desbetreffende website
Verwijderbaar	Indien geactiveerd, kan de gebruiker de Webclip verwijderen.
Pictogram	Upload via dit dialoogvenster een logo voor de verbinding: Afmeting 180x180, png-formaat
Vooraf samengesteld pictogram	Indien geactiveerd, worden er geen extra effecten (schaduw, reflectie) weergegeven op het pictogram.

Beperkingen en instellingen

Apps op zwarte lijst / witte lijst

Hier kun je de apps instellen die worden geblokkeerd (of toegestaan), afhankelijk van je instellingen in "Algemene instellingen". Een klik op brengt de bekende app-zoekfunctie naar voren. Daar kun je zoeken naar de apps die je wilt toevoegen.

Merk op dat voor deze functie een apparaat onder toezicht nodig is

SysApp-beperkingen

Specifieke apps of functies van je apparaat blokkeren

Gebruik van YouTube toestaan	Gebruik van YouTube toestaan
Gebruik van iTunes Store toestaan	Gebruik van iTunes Store toestaan
Gebruik van Safari toestaan	Gebruik van Safari toestaan
Automatisch aanvullen inschakelen	Maakt automatisch invullen mogelijk
Fraude waarschuwing	Forceert de fraudewaarschuwing
JavScript inschakelen	Maakt het gebruik van JavaScript mogelijk
Pop-ups blokkeren	Blokkeert alle soorten pup-ups
Cookies toestaan	Kiezen wanneer Safari cookies accepteert

App-VPN

Via het symbool kunt u toepassingen definiëren die de geselecteerde VPN-verbinding automatisch starten bij het opstarten.

App-instellingen

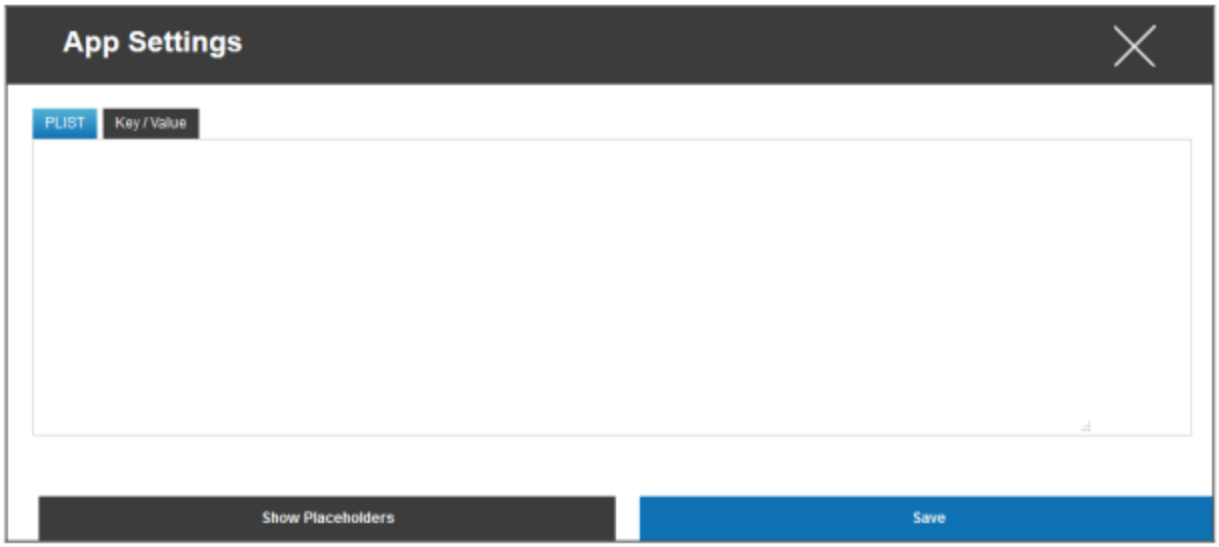
Onder "App Settings" (App-instellingen) kun je de app bepaalde waarden toewijzen aan de voorgrond (zolang de app dit ondersteunt, vraag indien nodig de ontwikkelaar van de app).

Via het symbool voeg je een (extra) app toe. Je ziet weer de bekende AppTec360 weergave van een App-Import.

Zoek hier naar de app die je wilt configureren en selecteer deze. De instellingen zijn alleen van toepassing op beheerde apps.

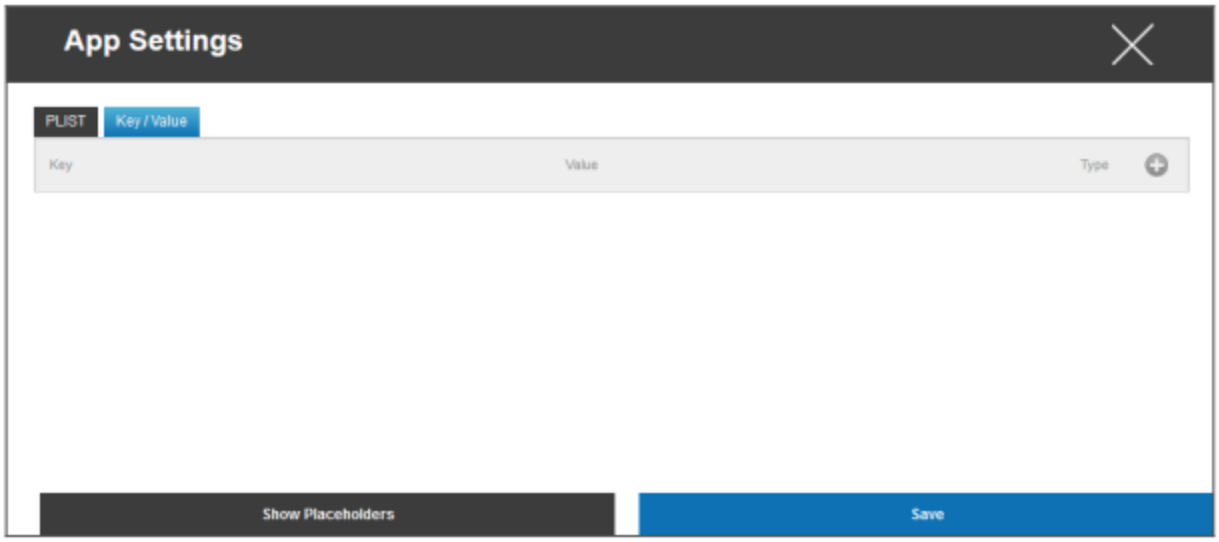
Als het importeren is gelukt, ziet u het volgende scherm:

Nu kun je met een klik op verschillende configuraties uitvoeren. Je krijgt dan het volgende overzicht:

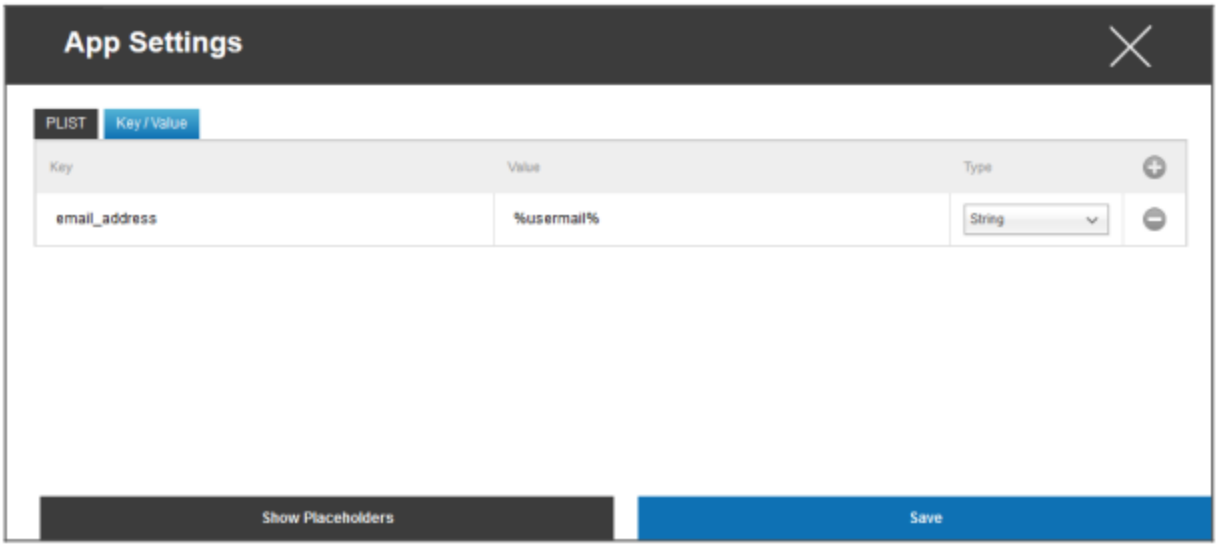


Als je al een PLIST (brontekst van de configuratie) hebt, kun je die hier toevoegen en alles opslaan met "Opslaan".

Onder "Key / Value" kunt u specifieke configuraties aan de App koppelen



Hier kun je een nieuwe sleutel en zijn waarde instellen met het symbool.



Natuurlijk staan alle plaatshouders van AppTec tot je beschikking

"Type" uitleg:

String	Tekst
Booleaans	Waar/Onwaar
Aantal	Aantal

Met het symbool kun je een app weer verwijderen.

App Store voor ondernemingen

iTunes-apps

Onder dit punt kunt u optionele Apps voor uw Gebruiker distribueren.

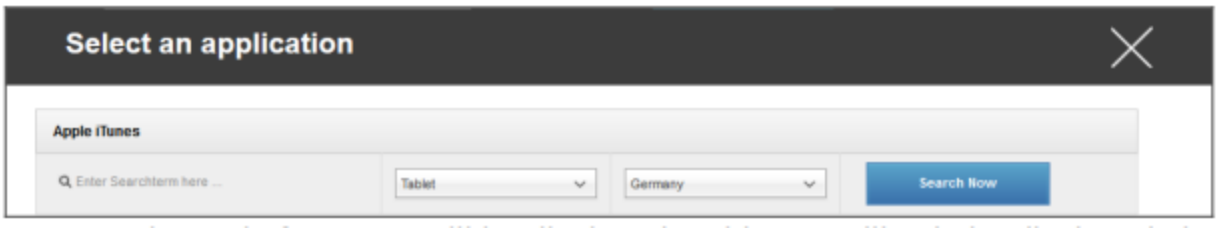
Als hier een app staat, wordt deze automatisch geïnstalleerd op het apparaat van de eindgebruiker in de AppTec360 Store.

Dit zijn gewoon links naar de officiële Apple App Store. Daarom moet elk apparaat van de eindgebruiker voorzien zijn van een Apple ID.

Op dit moment raden we aan dat elke gebruiker zijn eigen Apple ID heeft.

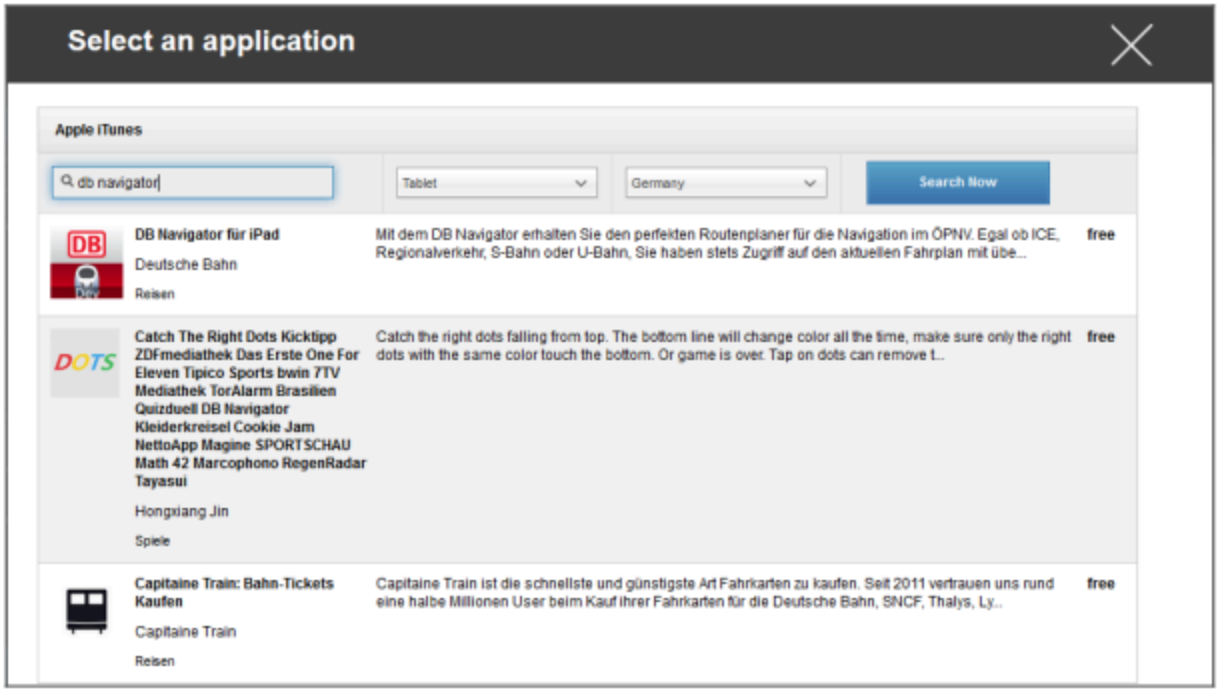
Met het symbool kunt u extra Apps toevoegen.

Daarna zou een venster met het volgende overzicht moeten openen.



Houd er rekening mee dat alleen gratis apps worden weergegeven, betaalde apps worden alleen weergegeven via VPN.

Onder "Voer hier een zoekterm in..." kun je zoeken naar een app die in de Apple App Store staat.



Als je op het pictogram of op de naam van de app klikt, wordt je opnieuw gevraagd om extra configuraties uit te voeren.

Blijf op de hoogte	Eens per week wordt bepaald of er een update is voor de app. Zo ja, dan wordt deze update geïnstalleerd
App verwijderen wanneer MDM-profiel wordt verwijderd	Als het apparaatbeheer wordt verwijderd, wordt de app verwijderd.
Back-up van app-gegevens voorkomen	Er wordt geen back-up van app-specifieke gegevens gemaakt
App-VPN	Selecteer een VPN-verbinding die wordt gestart bij het openen van de app

Na een klik op "Installeren" wordt de app toegevoegd aan de Enterprise App Store en kan vervolgens via de AppTec360 AppStore worden geïnstalleerd op het apparaat van de eindgebruiker.

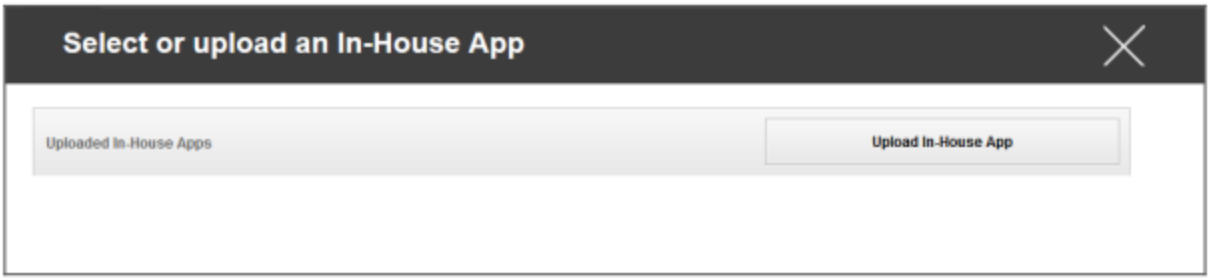
Als de App-Store Import succesvol is verlopen, krijg je het volgende overzicht te zien:

Intern

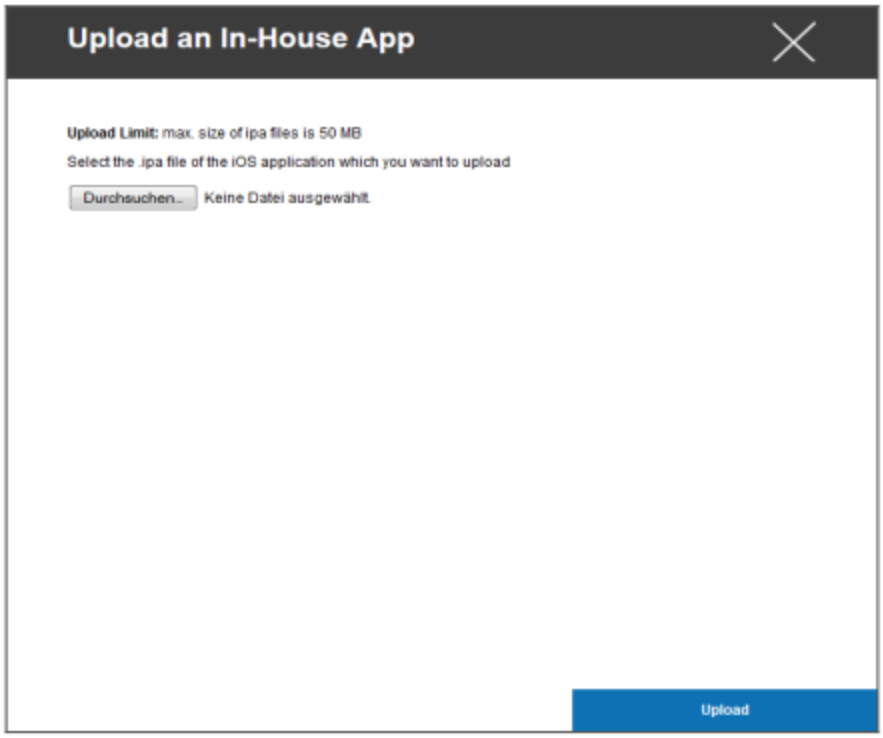
Onder het punt "In-House" kunt u intern ontwikkelde Apps uploaden en distribueren.

Met het symbool kun je extra In-House Apps distribueren.

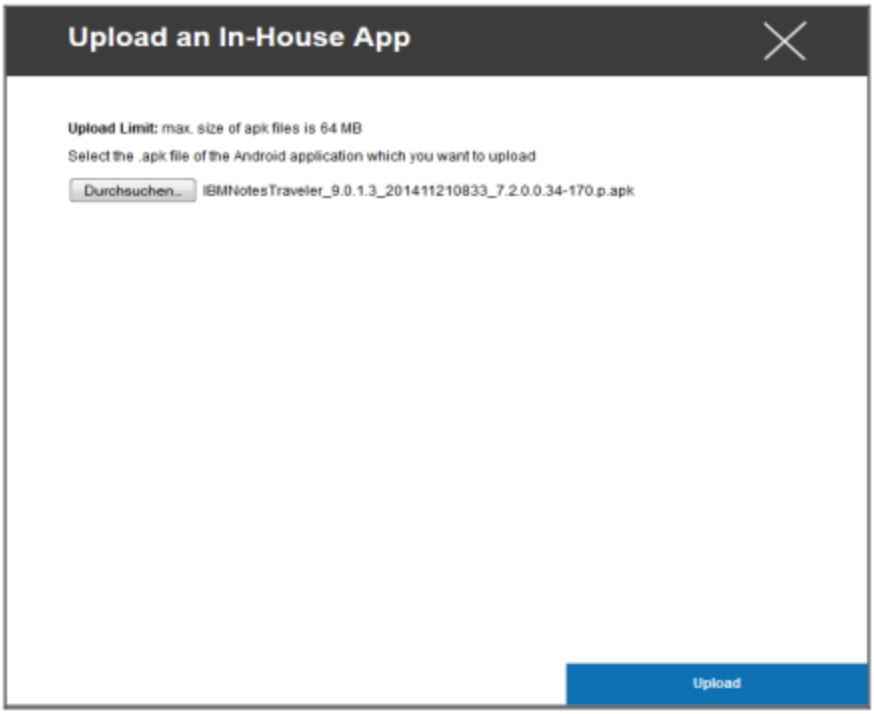
Als je nog nooit een In-House App hebt gedistribueerd, krijg je het volgende overzicht:



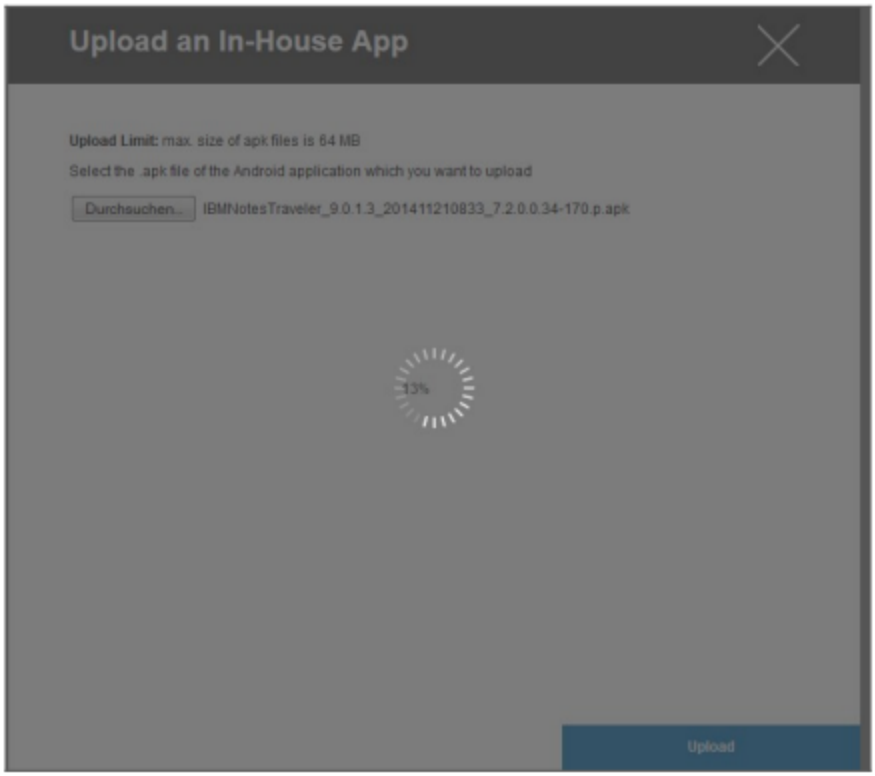
Klik hiervoor op "Upload In-House App", je krijgt dan het volgende overzicht te zien:



Selecteer nu met "Zoeken..." een .ipa-bestand en klik vervolgens op "Uploaden".



Je App wordt nu geüpload. In het midden van de cirkel kun je zien hoeveel procent van je App al is geüpload.



Als het uploaden van de In-House App succesvol is verlopen, zie je de nieuw geüploade app in je App Catalog.

De gebruiker heeft nu de mogelijkheid om deze app te bekijken en te installeren in de AppTec360 Store op het apparaat van de eindgebruiker, onder de categorie "In-House".

Omdat het hier niet gaat om een openbare Apple AppStore App, heeft de gebruiker geen opgeslagen Apple ID nodig op het apparaat van de eindgebruiker.

Kioskmodus

iOS Kioskmodus is alleen beschikbaar in modus onder toezicht

Met de Kioskmodus kun je een App of URL vooraf definiëren, zodat het mogelijk is om uitsluitend deze App/URL te draaien/bezoeken.

Bovendien kun je verschillende hardwareknoppen uitschakelen in de Kioskmodus.

Type toepassing

Pakket

Als je de app in Kioskmodus wilt starten, selecteer je "Package" onder "Application Type".

Kiosk-toepassing	Klik hier om een app te selecteren die in Kioskmodus moet worden gestart U vindt het huidige overzicht van de App Management U kunt kiezen tussen "Apple iTunes Apps" en "iOS In-House Apps".

URL

Als je een URL wilt starten in de Kioskmodus, selecteer dan "URL" onder "Type toepassing".

URL	Definieer nu het gewenste URL-adres
Beleid voor dezelfde herkomst	Als deze functie actief is, kan de gebruiker alleen surfen op de subpagina's van de vooraf gedefinieerde URL Als je bijvoorbeeld de volgende URL hebt gedefinieerd: www.mypage.com, dan kan de gebruiker surfen op www.mypage.com/subpage
URL's op witte lijsten	Hier kun je een witte lijst bijhouden, al deze URL's zijn toegestaan Maximaal 1 URL per regel Een URL moet beginnen met http:/ of https://.
URL's op de zwarte lijst	Hier kun je een zwarte lijst bijhouden, al deze URL's zijn niet toegestaan Maximaal 1 URL per regel Een URL moet beginnen met http:/ of https://.
Browser wissen na inactiviteit	Na inactiviteit wordt de browser cache geleegd.
Wachtwoord afsluiten ingeschakeld	Als u deze functie activeert, heeft de gebruiker de optie om de Kioskmodus te beëindigen met een wachtwoord dat u vooraf hebt ingesteld.
Wachtwoord afsluiten	Dit is het wachtwoord dat vooraf door u is ingesteld

Instellingen Kioskmodus

Geplande kioskmodus	Op basis van het tijdstip kun je de Kioskmodus instellen, zodat de modus automatisch wordt gestart en beëindigd op een vooraf bepaald tijdstip.
Starttijd	Starttijd
Tijd in minuten	Tijd in minuten waarna de Kioskmodus opnieuw moet worden beëindigd
Aanraking uitschakelen	Indien geactiveerd, is het aanraakscherm gedeactiveerd
Apparaatrotatie uitschakelen	Indien geactiveerd, wordt de automatische schermaanpassing uitgeschakeld.
Belsignaalschakelaar uitschakelen	Indien geactiveerd, wordt de belsignaalschakelaar vervolgens gedeactiveerd. Vanaf dat moment is het gedrag afhankelijk van de eerder ingestelde functie
Volumeknoppen uitschakelen	Indien geactiveerd, worden de volumeknoppen gedeactiveerd.
Knop Slaapwake uitschakelen	Indien geactiveerd, wordt de aan/uit-schakelaar gedeactiveerd
Automatische vergrendeling uitschakelen	Indien geactiveerd, wordt het apparaat niet op stand-by gezet.
Voice Over inschakelen	Indien geactiveerd, wordt de stemassistent geactiveerd.
Zoom inschakelen	Indien geactiveerd, wordt de zoom geactiveerd
Kleuren omkeren inschakelen	Indien geactiveerd, wordt de omgekeerde weergavemodus geactiveerd.
Assistive Touch inschakelen	Indien geactiveerd, wordt de AssistiveTouch geactiveerd
Spraakselectie inschakelen	Indien geactiveerd, wordt de spraakselectie geactiveerd
Monogeluid inschakelen	Indien geactiveerd, wordt Mono Audio geactiveerd.
VoiceOver	Indien geactiveerd, kan de gebruiker VoiceOver inschakelen.
Zoom	Indien geactiveerd, kan de gebruiker Zoom
Kleuren omkeren	Indien geactiveerd, kan de gebruiker omgekeerde kleuren inschakelen.
Assistive Touch	Indien geactiveerd, kan de gebruiker assistive touch inschakelen.

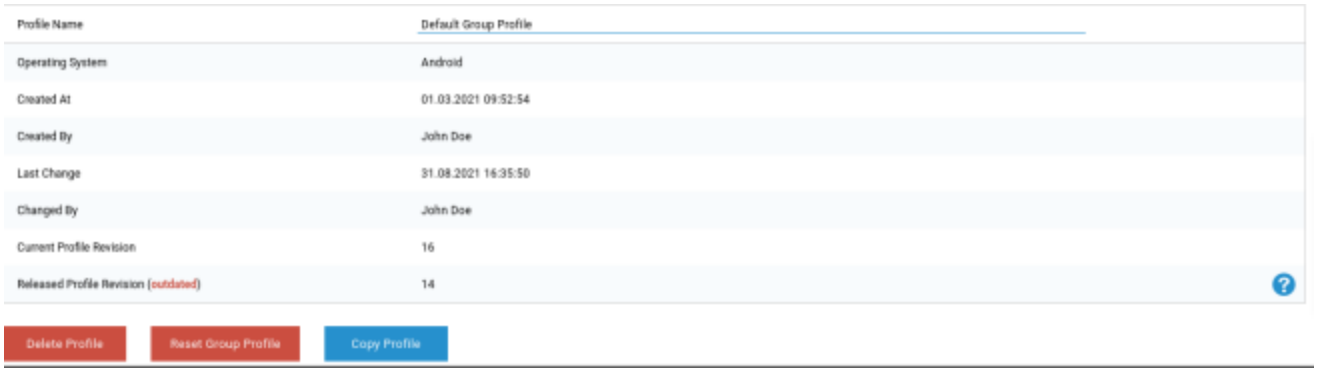
Android Enterprise – Apparaatconfiguratie volledig beheerd

Afhankelijk van of je momenteel een groepsprofiel of een apparaat hebt geselecteerd, verschillen het overzicht en de subpunten - denk hier goed over na!

Algemeen

Overzicht groepsprofiel (alleen op groepsniveau)

Wanneer je een groepsprofiel opent, krijg je een snel overzicht van het profiel.



Profielnaam	Naam van het profiel (kan hier worden gewijzigd)
Besturingssysteem	Besturingssysteem waar het profiel voor is
Gemaakt op	Tijd van creatie
Gemaakt door	De maker van het profiel
Laatste wijziging	Tijdstip van laatste wijziging van het profiel
Veranderd door	Account die de laatste wijzigingen heeft aangebracht
Huidige profielherziening	Revisie van opgeslagen profielstatus
Vrijgegeven profiel Revisie	Toegewezen profielrevisie ("Nu toewijzen"). Als er "(verouderd)" achter de tekst staat, betekent dit dat je het profiel hebt opgeslagen maar nog niet hebt toegewezen, zodat de apparaten nog steeds een oudere versie krijgen.

Apparaatoverzicht (alleen op apparaatniveau)

Als u zich op een apparaat bevindt, krijgt u een overzicht van het geselecteerde apparaat, dat het volgende bevat:

Naam apparaat	Naam apparaat
Locatie	Coördinaten locatie
Telefoonnummer	Telefoonnummer
Toegewezen verplichte apps	Aantal toegewezen verplichte apps
OS versie	OS-versie van het apparaat
Besturingssysteem	Besturingssysteem (Android Enterprise)
Serienummer	Serienummer apparaat
Apparaateigendom	Zakelijk of privéapparaat
Type apparaat	AE Work Beheerd Apparaat
Geworteld	Status, die aangeeft of het apparaat geroot is
Conform	Richtlijnconform
IP-adres	IP-adres van het apparaat
Laatst gezien	Tijdstip waarop het apparaat voor het laatst verbinding heeft gemaakt met AppTec
Laatste duw	Tijdstip waarop de laatste push naar het apparaat is verzonden.
AE Apparaat Eigenaar Modus	Ja
Gebruikerstoewijzing	De gebruiker of groep waaraan dit apparaat is toegewezen

Configuratie Revisie (alleen op apparaatniveau)

Hier krijg je een overzicht van welk groepsprofiel aan het apparaat is toegewezen.

Als je op het groepsprofiel klikt, krijg je direct toegang tot dit profiel en kun je instellingen uitvoeren.

Met dit symbool kun je de gedistribueerde apps terugzetten naar de instellingen van het groepsprofiel.

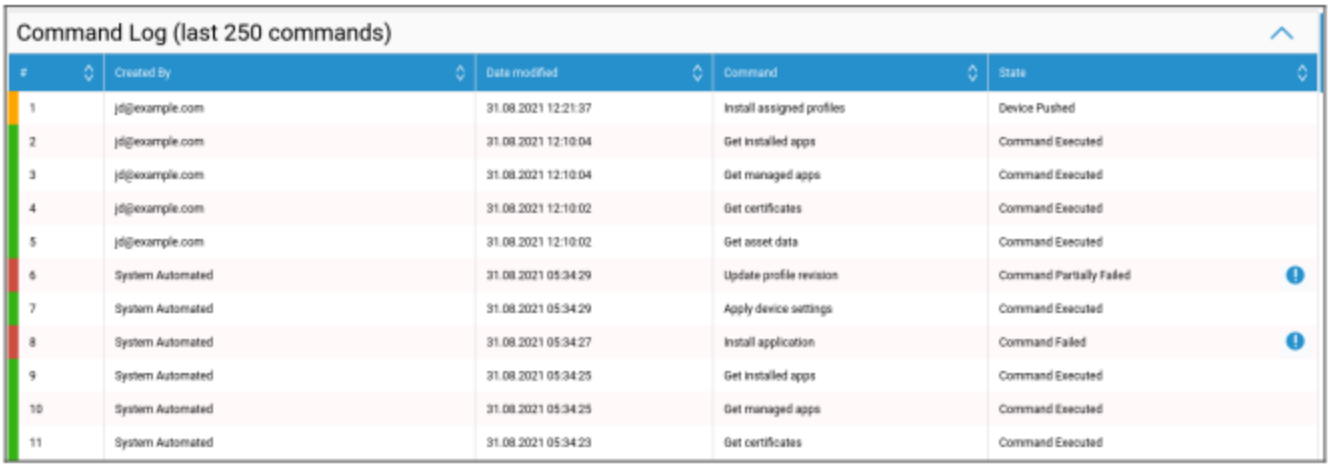
Met dit symbool kun je alle gebruikte apps terugzetten naar de instellingen van het groepsprofiel.

"Newer Revision available" geeft aan dat het groepsprofiel gewijzigd en opgeslagen is, maar niet toegewezen. Het groepsprofiel moet worden toegewezen met "Assign now" op groepsniveau om de wijzigingen toe te passen op de apparaten.

Apparaatlogboek (alleen op apparaatniveau)

Opdrachtlogboek

Hier kun je zien welke commando's zijn uitgegeven voor het apparaat en wat hun status is.



Commando's die zijn aangemaakt door "System Automated" worden automatisch aangemaakt door het systeem.

Mogelijke opdrachtstatussen

Apparaat ingedrukt	Er is een pushverzoek verzonden naar de pushservice (bijv. APNS) om het apparaat te vertellen terug verbinding te maken met de EMM-server.
Commando aangemaakt	De opdracht is aangemaakt in het systeem.
Opdracht verzonden	De opdracht werd naar het apparaat gestuurd nadat het verbinding had gemaakt met de server.
Opdracht uitgevoerd	De opdracht is succesvol uitgevoerd.
Opdracht mislukt	De opdracht is mislukt. *
Commando gedeeltelijk mislukt	Afhankelijk van het besturingssysteem van het apparaat kunnen sommige commando's gegroepeerd worden. Hierin zijn sommige delen van deze commandogroep mislukt. *
Opdracht uitgevoerd, uiteindelijk mislukt	Het commando werd uitgevoerd, maar misschien ook niet.
Commando verplaatst	De opdracht is opnieuw uitgevoerd door een gebruiker.
Afgedankt	De opdracht is verwijderd. Bijvoorbeeld omdat het is vervangen door een ander commando of omdat het apparaat opnieuw is aangemeld en oude commando's zijn verwijderd.

Als er een uitroepteken achter het bericht staat, kun je meer informatie krijgen door met je cursor over het pictogram te gaan.

Apparaatinstellingen

Configuratie klant

Hier kun je de volgende configuraties uitvoeren op je Android-toestel:

Tijd buiten naleving	De time-outlimiet voor de reactie van de gebruiker waarna de handhavingsactie wordt toegepast.
Handhavingsactie na time-out voor naleving	Handhavingsactie als een gebruiker geen acties uitvoert die leiden tot een conform apparaatstatus
Frequentie gegevensverzameling	Frequentie waarmee apparaat/GPS-informatie moet worden verzameld
Hartslagfrequentie apparaat	Interval waarin het apparaat contact moet maken met de AppTec360 Server Min. 1 minuut Max. 24 uur
Locatie-updates inschakelen	Indien geactiveerd, stuurt het apparaat locatie-updates naar de AppTec360 Server.
Locatie Update Tijd	Bepaalt met welke tijdsintervallen het apparaat locatie-updates naar AppTec360 stuurt
Gebruik Google-nauwkeurigheid voor locatie-updates	Indien geactiveerd, wordt de netwerklocatie gebruikt voor locatie-updates (als dit was uitgeschakeld onder "Beperkingen", dan heeft deze instelling geen invloed)
GPS-locatie gebruiken voor locatie-update	Indien geactiveerd, wordt de GPS gebruikt voor locatie-updates.
Neplocaties toestaan	Maakt het vervalsen van locatiegegevens via apps van derden mogelijk
Verbroken verbinding Actie	Indien ingeschakeld, kun je een actie opgeven voor het geval dat een apparaat geen verbinding krijgt met de MDM-server binnen het heartbeat-interval. Als het apparaat bijvoorbeeld een heartbeat-tijd van 5 minuten heeft, maakt het om 10:35 uur verbinding met de server. Daarna verlaat het apparaat het Wi-Fi-bereik. De volgende heartbeat om 10:40 uur zal mislukken en de opgegeven actie zal worden uitgevoerd.
Actie	De actie die ondernomen moet worden zodra een apparaat niet meer voldoet. • Lock Device = apparaat vergrendelen

	• Apparaat wissen = apparaat wordt teruggezet naar fabrieksinstellingen • Apparaat & SD-kaart wissen = het apparaat wordt teruggezet naar de fabrieksinstellingen en de opslag op de SD-kaart wordt gewist.
Drempel	U kunt een drempelwaarde van mislukte hartslagen opgeven die nodig is om de gespecificeerde actie te activeren.

Modus voor beleidshandhaving	Standaard:	Gebruikers worden regelmatig gevraagd om uitstaande acties uit te voeren
	Luie handhaving van beleid:	Gebruikers worden nooit gevraagd om openstaande acties uit te voeren. Alle openstaande acties worden getoond in de AppTec360 Client
	Agressieve beleidshandhaving:	Gebruikers worden non-stop gevraagd om uitstaande acties uit te voeren
AppTec360 Versie Slot	Indien ingeschakeld kan een versiecode voor de AppTec360 MDM Client worden opgegeven. De AppTec360-client zal alleen updaten naar de opgegeven versie. Nieuwere versies worden genegeerd. Een downgrade is NIET mogelijk.	
Versiecode	Versiecode waarop de AppTec360 MDM-client moet worden vergrendeld.	
AppTec360-melding uitschakelen	Als deze optie is uitgeschakeld, geeft AppTec360 Client geen melding weer in de meldingsbalk. Gebruikers kunnen de AppTec360-client dus afsluiten via taakbeheer. Als de AppTec360-client is afgesloten, werken verschillende functies zoals Kiosk Mode en App Black/Whitelisting niet goed. Samsung-apparaten bieden een beveiligingsmechanisme voor de AppTec360 Client. De melding is standaard uitgeschakeld op Samsung-apparaten die de KNOX API's ondersteunen. De melding moet niet worden uitgeschakeld op apparaten met Android 8.0 of hoger.	

Behang

Aangepast behang instellen	De aangepaste achtergrond inschakelen/uitschakelen
Behang	De achtergrondmodus instellen om een kleurcode of een afbeelding te gebruiken
Geef een kleur op	Geef een achtergrondkleur op als hexadecimale waarde, bijvoorbeeld #000000 voor zwart of #fffff als wit
Afbeelding instellen als achtergrond	Upload het afbeeldingsbestand dat je als achtergrond wilt gebruiken

Activabeheer (alleen op apparaatniveau)

Apparaat info

Model	Typeaanduiding apparaat
Besturingssysteem	OS
OS versie	OS-versie
Serienummer	Serienummer
Naam apparaat	Naam apparaat
Batterijstatus	Batterijstatus
Vrij / Totaal geheugen	Vrij / Totaal geheugen
Samsung Veilig	Samsung SAFE-interface, vereist voor diverse instelopties
SD-kaart beschikbaar	SD-kaart beschikbaar
SD-kaart geëmuleerd	SD-kaart geëmuleerd
SD-kaart verwijderbaar	SD-kaart verwijderbaar
SD vrij / totaal geheugen	SD vrij / totaal SD-kaartgeheugen

Wi-Fi

IP-adres	IP-adres apparaat
WiFi MAC	WiFi-MAC-adres

Cellulair

Status	Status (SIM-kaart geïnstalleerd)
Telefoonnummer	Telefoonnummer
Roaming (spraak/data)	Roaming voor spraak/data
Roaming-status	Huidige roamingstatus
IP-adres	IP-adres
Exploitant/vervoerder	Exploitant/vervoerder
Cellulaire technologie	Cellulaire technologie
IMEI	IMEI-nummer
ICCID	Dit is de ID voor de SIM-kaart, vaak ook een Smartcard of Integrated Circuit Card (ICC).
IMSI	De International Mobile Subscriber Identity (IMSI) biedt in GSM- en UMTS-mobiele netwerken een definitieve identificatie van de netwerkgebruikers. De IMSI bestaat uit maximaal 15 cijfers en wordt als volgt geconfigureerd: • Mobiele landcode (MCC), 3 cijfers • Mobiele netwerkcode (MNC), 2 of 3 cijfers • Identificatienummer mobiele abonnee (MSIN), 1-10 cijfers
Huidige MCC/MNC	Zie "SIM MCC/MNC".
SIM MCC/MNC	De mobiele landcode is een vastgestelde landidentificatie die door de ITU is ingesteld volgens de E.212-norm. Deze werkt samen met de mobiele netwerkcode (MNC) voor de identificatie van het mobiele netwerk. Dit betekent de landcode/mobiele netwerkcode van de SIM-kaart. Als je naar een ander mobiel netwerk roamt, zullen de "Current MCC/MNC" en "SIM MCC/MNC" logischerwijs verschillend zijn.

Bluetooth

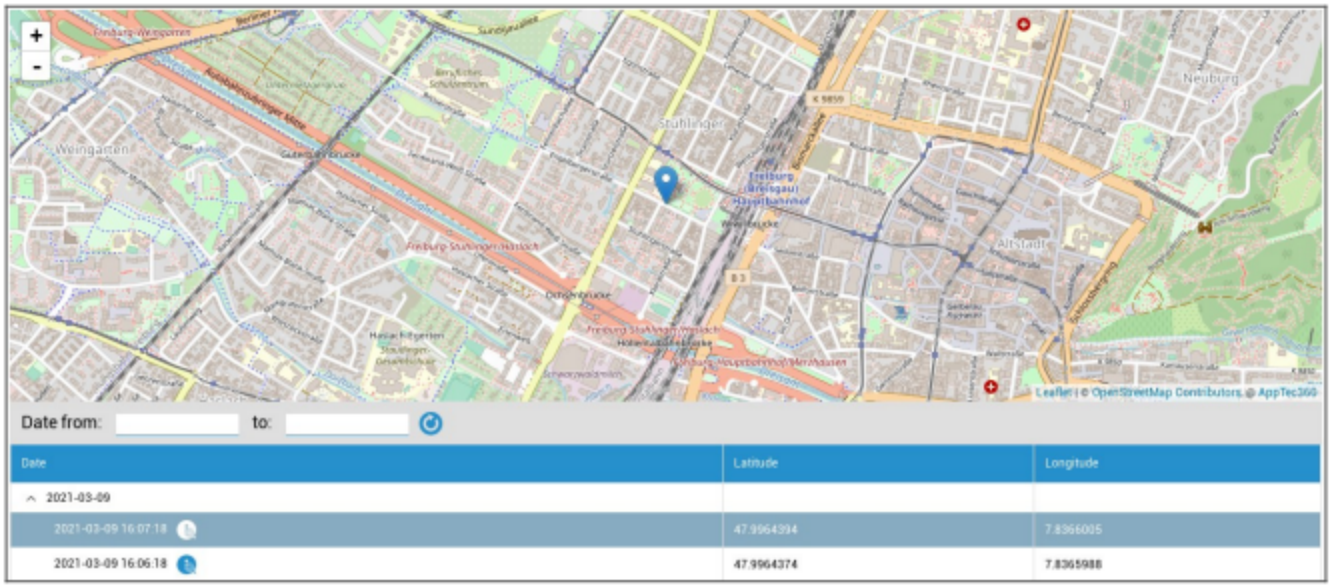
Bluetooth MAC	Bluetooth MAC-adres

Beveiligingsbeheer

Anti diefstal (alleen op apparaatniveau)

GPS-informatie (alleen op apparaatniveau)

Hier kun je de huidige/laatste locatie van het apparaat bepalen. De lokalisatie kan worden beveiligd met een of zelfs twee wachtwoorden - Zie: Algemene instellingen - Privacy - GPS-toegang



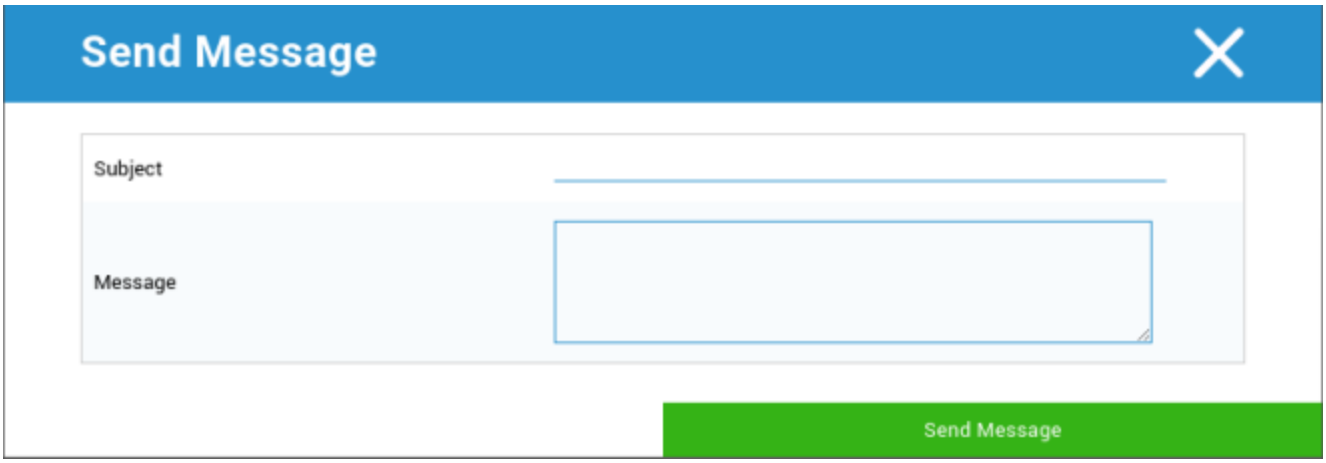
Vegen en vergrendelen (alleen op apparaatniveau)

Onder "Wissen & vergrendelen" kun je de volgende drie acties uitvoeren:

Volledig wissen	Het apparaat wordt teruggezet naar de fabrieksinstellingen (bedrijfs- en persoonlijke gegevens worden gewist)
Ondernemingsvegen	Alleen bedrijfsdata wordt verwijderd van het apparaat van de eindgebruiker (alle apps, data, etc. die zijn geleverd door AppTec360)
Vergrendelscherm	Schermvergrendeling is geactiveerd, het is voldoende om het apparaat te ontgrendelen met het apparaatwachtwoord/PIN

Bericht (alleen op apparaatniveau)

Hier kun je het onderwerp en een bericht invullen en naar een eindgebruiker sturen.



Beveiligingsconfiguratie

Toestelwachtwoord

Onder "Passcode" kunt u een wachtwoord voor het apparaat instellen, de volgende opties zijn beschikbaar

Minimale lengte wachtwoord	Bepaalt het minimum aantal symbolen dat een wachtwoord moet hebben	
Wachtwoord kwaliteit	Ongespecificeerd	Dit beleid stelt geen eisen aan het wachtwoord.
	Biometrisch zwak	Dit beleid staat laagbeveiligde biometrische herkenningstechnologie toe. Dit houdt technologieën in die de identiteit van een individu kunnen herkennen tot ongeveer een PIN-code van 3 cijfers (valse detectie is minder dan 1 op 1.000).
	Iets	Dit beleid vereist dat er een wachtwoord of patroon wordt ingesteld, maar dwingt geen specifieke regels af.
	Alfabetisch	De gebruiker moet een wachtwoord hebben ingevoerd dat ten minste alfabetische tekens (of andere symbolen) bevat.
	Alfanumeriek	De gebruiker moet een wachtwoord hebben ingevoerd dat zowel numerieke als alfabetische tekens (of andere symbolen) bevat.
	Complex	De gebruiker moet een wachtwoord hebben ingevoerd dat standaard ten minste een letter, een cijfer en een speciaal symbool bevat. Met deze wachtwoordkwaliteit kunnen wachtwoorden worden beperkt tot verschillende sets tekens, zoals ten minste een hoofdletter, enz.
Minimale lengte wachtwoord	Stel het vereiste aantal tekens in voor het wachtwoord. Je kunt bijvoorbeeld eisen dat PIN-codes of wachtwoorden minstens zes tekens bevatten.	
Minimaal aantal cijfers vereist in wachtwoord	Minimaal aantal cijfers vereist in wachtwoord	
Minimaal aantal kleine letters vereist in wachtwoord	Minimaal aantal kleine letters vereist in wachtwoord	

Minimaal hoofdletters vereist in wachtwoord	Minimaal hoofdletters vereist in wachtwoord
Minimaal aantal niet-lettertekens vereist in wachtwoord	Minimaal aantal niet-lettertekens vereist in wachtwoord
Minimaal vereiste symbolen in wachtwoord	Minimaal vereiste symbolen in wachtwoord

Vergrendeling maximale inactiviteitstijd	Maximale inactiviteit gebruiker tot tijdslot
Time-out verlopen wachtwoord	Wordt ingesteld, na welk tijdsinterval het wachtwoord verloopt en een nieuw wachtwoord moet worden ingesteld
Beperking wachtwoordgeschiedenis	Aantal eerder gebruikte wachtwoorden die niet zijn toegestaan
Maximaal aantal mislukte wachtwoordpogingen	Bepaalt hoe vaak een wachtwoord verkeerd kan worden ingevoerd voordat het apparaat volledig wordt gewist.
Biometrische verificatie toestaan	Maakt verificatie via vingerafdruk of irisscan mogelijk. Alleen voor Samsung KNOX 2.1 en hoger

AntiVirus

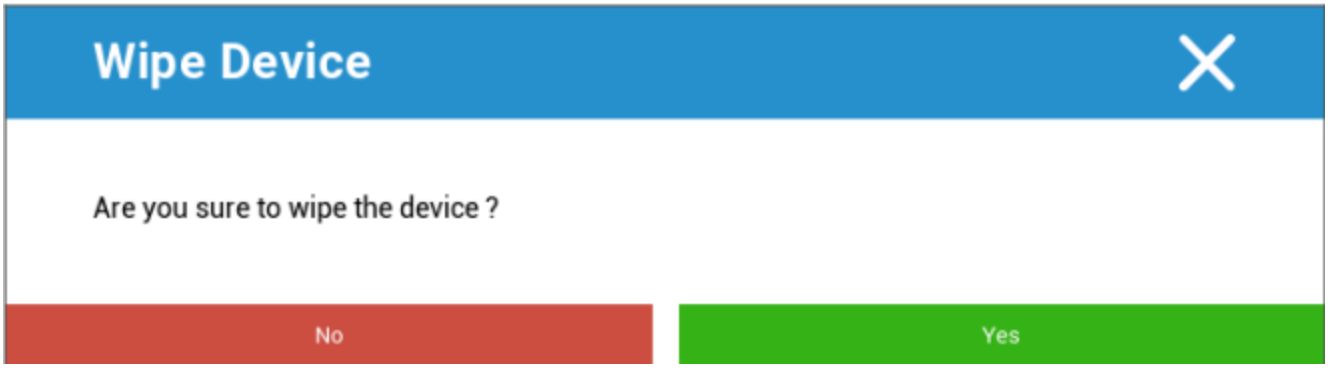
Automatisch scannen	Periodieke automatische scans inschakelen
Scaninterval	Interval voor onderzoek (Snel / Volledig)
Volledig automatisch scannen	Volledig automatische scans inschakelen
Automatische updates	Automatische updates inschakelen
Interval updatecontrole	Hoe vaak de app en de database moeten worden bijgewerkt (virussen / beschadigde code)
Bescherming van apps	Automatische app-scan inschakelen
Bescherming SD-kaart	Automatische SD-kaartscan inschakelen
Update alleen voor Wi-Fi	Als deze optie is ingeschakeld, worden updates alleen toegepast als het apparaat verbinding heeft met een Wi-Fi-netwerk.

Einde levensduur (alleen op apparaatniveau)

Vegen (alleen op apparaatniveau)

Onder "Wissen" kun je het apparaat herstellen naar de fabrieksinstellingen. Hier worden de bedrijfs- en privégegevens op het eindgebruikerapparaat gewist.

Als je op het "Minus-symbool" klikt, krijg je het volgende bericht:



Met "Ja" kunt u het wissen uitvoeren.

Onder "Wipe Report" kunnen de volgende items worden weergegeven

Gewist door	Geschiedenis van wie het afvegen heeft uitgevoerd
Datum	Datum
Status	Status (bijv. of het wissen met succes is uitgevoerd)

Beperkende instellingen

Beperkingen

Hier kunnen verschillende dingen worden beperkt en geblokkeerd.

Camera inschakelen	Gebruik van camera toestaan	
Automatische synchronisatie forceren	Op	Synchronisatie is permanent geactiveerd
	Uit	Synchronisatie is permanent gedeactiveerd
	Keuze van de gebruiker	Geselecteerd door de gebruiker
Bluetooth forceren	Op	Bluetooth is permanent geactiveerd
	Uit	Bluetooth is permanent gedeactiveerd
	Keuze van de gebruiker	Geselecteerd door de gebruiker
GPS afdwingen	Op	GPS is permanent geactiveerd
	Uit	GPS is permanent uitgeschakeld
	Keuze van de gebruiker	Geselecteerd door de gebruiker
Krachtennetwerk locatie	Op	Permanente internet-lokalisatie
	Uit	Permanente deactivering van internet-localisatie
	Keuze van de gebruiker	Geselecteerd door de gebruiker

Beveiliging		
Locatie delen niet toestaan	Geeft aan of een gebruiker geen locatie mag delen.	
Veilig opstarten niet toestaan	Geeft aan of de gebruiker het apparaat niet in veilige opstartmodus mag herstarten.	
Reset netwerk niet toestaan	Geeft aan of een gebruiker de netwerkinstellingen niet mag resetten vanuit Instellingen.	
Fabrieksreset weigeren	Geeft aan of een gebruiker het apparaat niet mag resetten.	
ADB inschakelen	Maakt verbinding met een pc mogelijk via ADB	
Toetsenbord uitschakelen	Schakelt het Toetsenbord uit	
Apparaateigenaar Info over vergrendelscherm	Stelt in welke informatie over de eigenaar van het apparaat wordt weergegeven op het vergrendelscherm.	
Handhaving	Modus Prompt gebruiker	De gebruiker wordt gevraagd de nodige acties uit te voeren.
	Modus Gesloten Container	Verberg alle apps totdat aan alle vereisten is voldaan

App-beheer	
Koppeling tussen profiel-apps toestaan	Hiermee kunnen apps in het bovenliggende profiel weblinks afhandelen vanuit het beheerde profiel.
App-bediening weigeren	Geeft aan of een gebruiker applicaties niet mag wijzigen in Instellingen of launchers.
Installatie van app weigeren	Geeft aan of een gebruiker geen applicaties mag installeren.
Apps niet verwijderen	Geeft aan of een gebruiker applicaties niet mag verwijderen.
Beleid voor runtime-toestemming	Specificeert hoe nieuwe toestemmingsaanvragen van apps zullen worden behandeld.
Onbekende bronnen toestaan	Als dit is ingeschakeld, kunnen gebruikers apps sideloaden door een .apk-bestand te installeren.

Connectiviteit	
Mobiel netwerk configureren niet toestaan	Geeft aan of een gebruiker geen mobiele netwerken mag configureren.
Tethering verbieden Configuratie	Geeft aan of een gebruiker geen Tethering & draagbare hotspots mag configureren.
VPN-configuratie niet toestaan	Geeft aan of een gebruiker geen VPN mag configureren.
Wifi configuratie weigeren	Geeft aan of een gebruiker geen WiFi-toegangspunten mag wijzigen.
Uitgaande NFC-bundel niet toestaan	Geeft aan of de gebruiker NFC niet mag gebruiken om gegevens van apps uit te stralen.
WiFi-configuratie vergrendelen	Deze instelling bepaalt of WiFi-configuraties die zijn gemaakt door een app voor apparaateigenaren moeten worden vergrendeld (dat wil zeggen, alleen kunnen worden bewerkt of verwijderd door de app voor apparaateigenaren, zelfs niet door de app Instellingen).
Dataroaming inschakelen	Activeert dataroaming

Bluetooth	
Bluetooth niet toestaan	Geeft aan of bluetooth niet is toegestaan op het apparaat. Vereist Android 8.0
Delen via Bluetooth niet toestaan	Geeft aan of uitgaande bluetooth-sharing niet is toegestaan op het apparaat. Vereist Android 8.0
Bluetooth-configuratie weigeren	Geeft aan of een gebruiker bluetooth niet mag configureren.

Accountbeheer	
Toevoeging beheerd profiel niet toestaan	Geeft aan of een gebruiker geen beheerde profielen mag toevoegen. Vereist Android 8.0
Gebruikers niet toestaan toe te voegen	Geeft aan of een gebruiker geen nieuwe gebruikers mag toevoegen.
Verwijderen beheerd profiel niet toestaan	Geeft aan of beheerde profielen van deze gebruiker kunnen worden verwijderd, behalve door de eigenaar van het profiel. Vereist Android 8.0
Accountwijziging niet toestaan	Geeft aan of een gebruiker geen accounts mag toevoegen of verwijderen, tenzij ze programmatisch zijn toegevoegd door Authenticator.

Telefonie	
Uitgaande gesprekken weigeren	Geeft aan dat de gebruiker geen uitgaande telefoongesprekken mag voeren.
SMS weigeren	Geeft aan dat de gebruiker geen SMS-berichten mag verzenden of ontvangen.

Systeem	
Venster maken niet toestaan	Geeft aan dat vensters naast app-vensters niet mogen worden gemaakt.
Gebruikerspictogram niet toestaan	Geeft aan of een gebruiker zijn icoon niet mag wijzigen.
Achtergrond niet toestaan	Gebruikersbeperking om het instellen van een achtergrond niet toe te staan.
Statusbalk uitschakelen	Het uitschakelen van de statusbalk blokkeert meldingen, snelle instellingen en andere schermoverlays waarmee je kunt ontsnappen aan een apparaat voor eenmalig gebruik.
Automatische tijd inschakelen	Stelt de tijd automatisch in.
Automatische tijdzone inschakelen	Stelt de tijdzone automatisch in.
Blijft aan als de stekker in het stopcontact zit	Het apparaat blijft actief als het op een voedingsbron is aangesloten.

Opslag	
App-verificatie uitschakelen	Geeft aan of een gebruiker de applicatieverificatie niet mag uitschakelen.
Mount fysieke media niet toestaan	Geeft aan of een gebruiker geen fysieke externe media mag aankoppelen.
Back-upservice inschakelen	Back-upservice beheert alle back-up- en herstelmechanismen op het apparaat. Als u dit op false zet, wordt voorkomen dat er een back-up of herstel van gegevens wordt gemaakt. Back-upservice is standaard uitgeschakeld. Android 8.0 vereist
USB-massaopslag inschakelen	Schakelt het gebruik van USB Mass Storage in.

Toetsenbord	
Autofill weigeren	Geeft aan of een gebruiker Autofill Services niet mag gebruiken. Vereist Android 8.0
Kopiëren en plakken tussen profielen verbieden	Specificeert of wat op het klembord van dit profiel wordt gekopieerd, in gerelateerde profielen kan worden geplakt.

Geluid	
Volume-aanpassing niet toestaan	Geeft aan of een gebruiker het mastervolume niet mag aanpassen.
Microfoon uitschakelen	Geeft aan of een gebruiker het microfoonvolume niet mag aanpassen.
Apparaat dempen	Apparaat dempen.

Beheer van certificaten

Hier kun je Trusted Certificates en Identity Certificates distribueren naar je apparaten.

Android 8 of hoger is vereist om Trusted Certificates te distribueren en Android 9 of hoger is vereist om Identity Certificates te distribueren.

Met de "+" kun je meerdere certificaten toevoegen.

Trusted Certificates moeten in PEM-formaat zijn.

Identiteitscertificaten moeten in PKCS12-formaat zijn

Verbindingsbeheer

Wifi

Voer voor deze instelling de voorconfiguratie uit van de eindgebruikersapparaten voor toegang tot interne Access
Points.

Serviceset Identifier (SSID)	SSID voor het netwerk waarmee verbinding moet worden gemaakt
Verborgen netwerk	Activeren, als het AP de SSID niet uitzendt

Type beveiliging

Het beveiligingstype van het AP vaststellen

WEP

Wachtwoord	Wachtwoord voor het AP

WPA/WPA2

Wachtwoord	Wachtwoord voor het AP

802.1x EAP

EAP-Methode

PWD	Identiteit	Identiteit
	Wachtwoord	Wachtwoord

PEAP	Fase 2 Authenticatieprotocol	geen	Geen aanvullend protocol
		MSCHAPV2	MSCHAPV2-protocol
		GTC	GTC-protocol
	CA-certificaat	CA-certificaat	
	Identiteit	Identiteit	
	Anonieme identiteit	Anonieme identiteit	
	Wachtwoord	Wachtwoord	

TTLS	Fase 2 Authenticatieprotocol	geen	Geen aanvullend protocol
		PAP	PAP-protocol
		MSCHAP	MSCHAP-protocol
		MSCHAPV2	MSCHAPV2-protocol
		GTC	GTC-protocol
	CA-certificaat	CA-certificaat	
	Identiteit	Identiteit	
	Anonieme identiteit	Anonieme identiteit	
	Wachtwoord	Wachtwoord	

TLS	CA-certificaat	CA-certificaat
	Identiteit	Identiteit
	Wachtwoord	Wachtwoord

VPN

Naam verbinding	Naam van de VPN-verbinding

VPN-type

VPN

VPN-client

AppTec360 VPN-client	
Configuratie gateway	Selecteer de VPN-configuratie van de gateway (zie **Algemene instellingen > Universele gateway > VPN-instellingen**)
Altijd aan VPN	Native Lockdown inschakelen
AppTec360 vergrendeling inschakelen	AppTec360 vergrendeling inschakelen

Ingebouwd (alleen beschikbaar op Samsung-apparaten)			
Type aansluiting	PPTP	Server	Server
		PPTP-codering inschakelen	PPTP-codering inschakelen
	L2TP / IPSec PSK	Server	Server
		Vooraf gedeelde IPSec-sleutel	Vooraf gedeelde IPSec-sleutel
		L2TP-geheim inschakelen	L2TP-geheim inschakelen
		L2TP-geheim	L2TP-geheim
	IPSec XAuth PSK	Server	Server
		IPSec-identificatiecode	IPSec-identificatiecode
		Vooraf gedeelde IPSec-sleutel	Vooraf gedeelde IPSec-sleutel
DNS domeinen zoeken	DNS domeinen zoeken		
Expertinstellingen	DNS-servers	DNS-servers	
	Routes doorsturen	Routes doorsturen	

Open VPN		
Server	Server	
OpenVPN-profiel	OpenVPN-profiel	
OpenVPN-app	OpenVPN voor Android (aanbevolen)	
	OpenVPN verbinden	
Expertinstellingen	DNS-servers	DNS-servers
	Routes doorsturen	Routes doorsturen

Samsung / Sterke Zwaan			
Type aansluiting	PPTP	Server	Server
		Gebruikersnaam	Gebruikersnaam
		Wachtwoord	Wachtwoord
		PPTP-codering inschakelen	PPTP-codering inschakelen
	L2TP / IPSec PSK	Server	Server
		Vooraf gedeelde IPSec-sleutel	Vooraf gedeelde IPSec-sleutel
		Gebruikersnaam	Gebruikersnaam
		Wachtwoord	Wachtwoord
		L2TP-geheim inschakelen	L2TP-geheim
	IPSec XAuth PSK	Server	Server
		IPSec-identificatiecode	IPSec-identificatiecode
		Vooraf gedeelde IPSec-sleutel	Vooraf gedeelde IPSec-sleutel
		Gebruikersnaam	Gebruikersnaam
		Wachtwoord	Wachtwoord
Expertinstellingen	DNS-servers	DNS-servers	
	Routes doorsturen	Routes doorsturen	

Cisco elke verbinding		
Server	Server	
Certificaatmodus	Uitgeschakeld	Uitgeschakeld
	Automatisch	Automatisch
Expertinstellingen	DNS-servers	DNS-servers
	Routes doorsturen	Routes doorsturen

VPN per app

VPN-client

AppTec360 VPN-client		
Configuratie gateway	Selecteer de VPN-configuratie van de gateway (zie **Algemene instellingen > Universele gateway > VPN-instellingen**)	
VPN-apps	VPN-apps	
Altijd aan VPN	Native Lockdown inschakelen	Altijd aan VPN
AppTec360 vergrendeling inschakelen	AppTec360 vergrendeling inschakelen	

Samsung / Sterke Zwaan			
Type aansluiting	PPTP	Server	Server
		VPN-apps	VPN-apps
		Gebruikersnaam	Gebruikersnaam
		Wachtwoord	Wachtwoord
		PPTP-codering inschakelen	PPTP-codering inschakelen
	L2TP / IPSec PSK	Server	Server
		VPN-apps	VPN-apps
		Vooraf gedeelde IPSec-sleutel	Vooraf gedeelde IPSec-sleutel
		Gebruikersnaam	Gebruikersnaam
		Wachtwoord	Wachtwoord
		L2TP-geheim inschakelen	L2TP-geheim
	IPSec XAuth PSK	Server	Server
		VPN-apps	VPN-apps
		IPSec-identificatiecode	IPSec-identificatiecode
		Vooraf gedeelde IPSec-sleutel	Vooraf gedeelde IPSec-sleutel
		Gebruikersnaam	Gebruikersnaam
		Wachtwoord	Wachtwoord
Expertinstellingen	DNS-servers	DNS-servers	
	Routes doorsturen	Routes doorsturen	

Beperkingen

Hier kun je de beperkingen instellen met betrekking tot het verbindingsbeheer.

Dataroaming toestaan	Sta mobiele data toe tijdens roaming
Gegevensroaming forceren	Indien geactiveerd, wordt roaming voor mobiele data permanent geactiveerd (niet aanbevolen!) Deze instelling overschrijft de instelling "Sta dataroaming toe"!
De volgende instellingen zijn alleen beschikbaar op SAFE 2.x of hoger	
Alleen noodoproepen toestaan	Alleen noodoproepen toestaan
WiFi toestaan	WiFi toestaan
Minimumbeveiligingsniveau WiFi-netwerk	Minimumbeveiligingsniveau WiFi-netwerk Open = alle soorten WiFi zijn toegestaan
Verbied gebruiker om WiFi-netwerken toe te voegen	De gebruiker mag niet zelf een WiFi-netwerk toevoegen Deze instelling is alleen mogelijk als er een WiFi-profiel is gedefinieerd onder "Verbindingsbeheer".
SMS & MMS toestaan	Alles = alle SMS- en MMS-verkeer is toegestaan Alleen inkomende SMS = alleen inkomende SMS-berichten zijn toegestaan Alleen uitgaande SMS = alleen uitgaande SMS-berichten zijn toegestaan Geen = Geen SMS- / MMS-verkeer toegestaan
Synchronisatie toestaan tijdens roaming	Synchronisatie toestaan tijdens roaming Aan = geactiveerd Uit = gedeactiveerd Keuze van de gebruiker = keuze van de gebruiker
Spraak Roaming toestaan	Spraak Roaming toestaan Aan = geactiveerd Uit = gedeactiveerd Keuze van de gebruiker = keuze van de gebruiker
Systeem http proxyserver gebruiken	Het gebruik van een HTTP-proxyserver, dat wordt aangeboden door de systeeminstellingen in instellingen, is afhankelijk van het verbonden netwerk (WiFi of APN).

PIM-beheer

Gmail Uitwisseling

Info: Deze Configuratie wordt toegepast op de Gmail-app. Je moet dus Gmail goedkeuren en installeren.

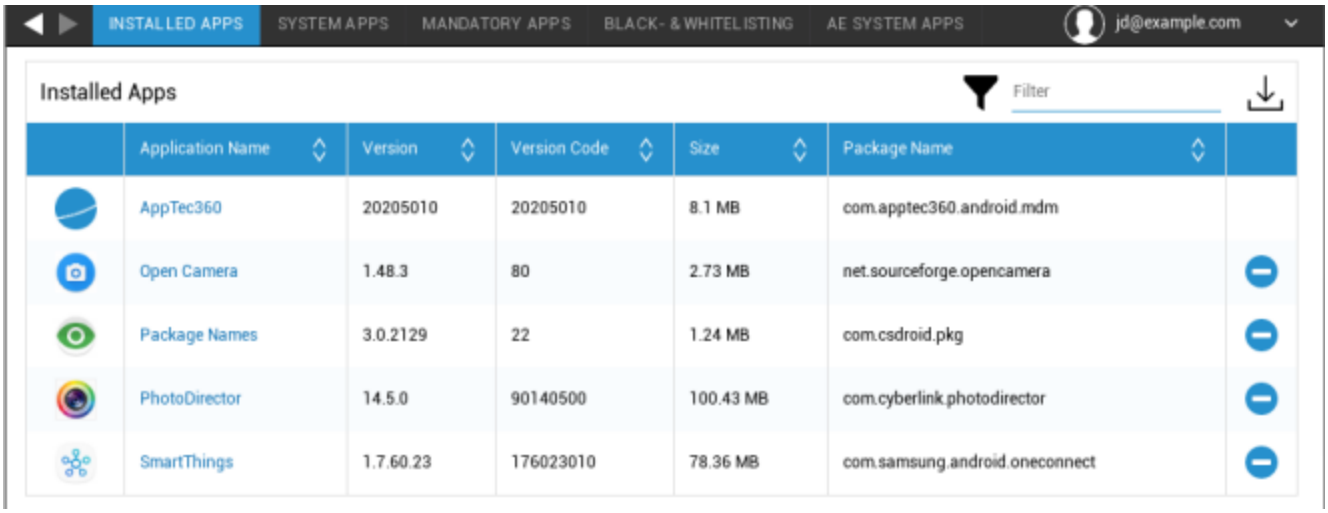
E-mailadres	Het e-mailadres van de opgegeven gebruiker Let op de "Plaatshouders", die je kunt gebruiken om met referenties te werken en die je niet handmatig op elk apparaat hoeft te wijzigen. Met een klik kun je ze zelf bekijken
Server hostnaam	Serveradres van uw Exchange-servers
Inlognaam	De aanmeldingsnaam voor het betreffende eindgebruikersapparaat, let ook op de "Placeholders here
Handtekening	Er kan een handtekening worden toegevoegd (Tip: Sommige apparaten vereisen HTML-opmaak voor de handtekening)
Aantal vorige dagen om te synchroniseren	Aantal dagen dat bepaalt wanneer e-mails worden teruggesynchroniseerd
Apparaat-ID	Een string die die EAS DeviceID bevat. Dit is een onderdeel van het EAS-protocol en wordt in verschillende omgevingen gebruikt.
Gebruik SSL (Secure Sockets Layer)	Gebruik een SSL-verbinding
Accepteer alle certificaten	Alle certificaten worden geaccepteerd. Selecteer deze optie als uw Exchange Server gebruikmaakt van een zelfondertekend certificaat.

App-beheer

Enterprise App Manager

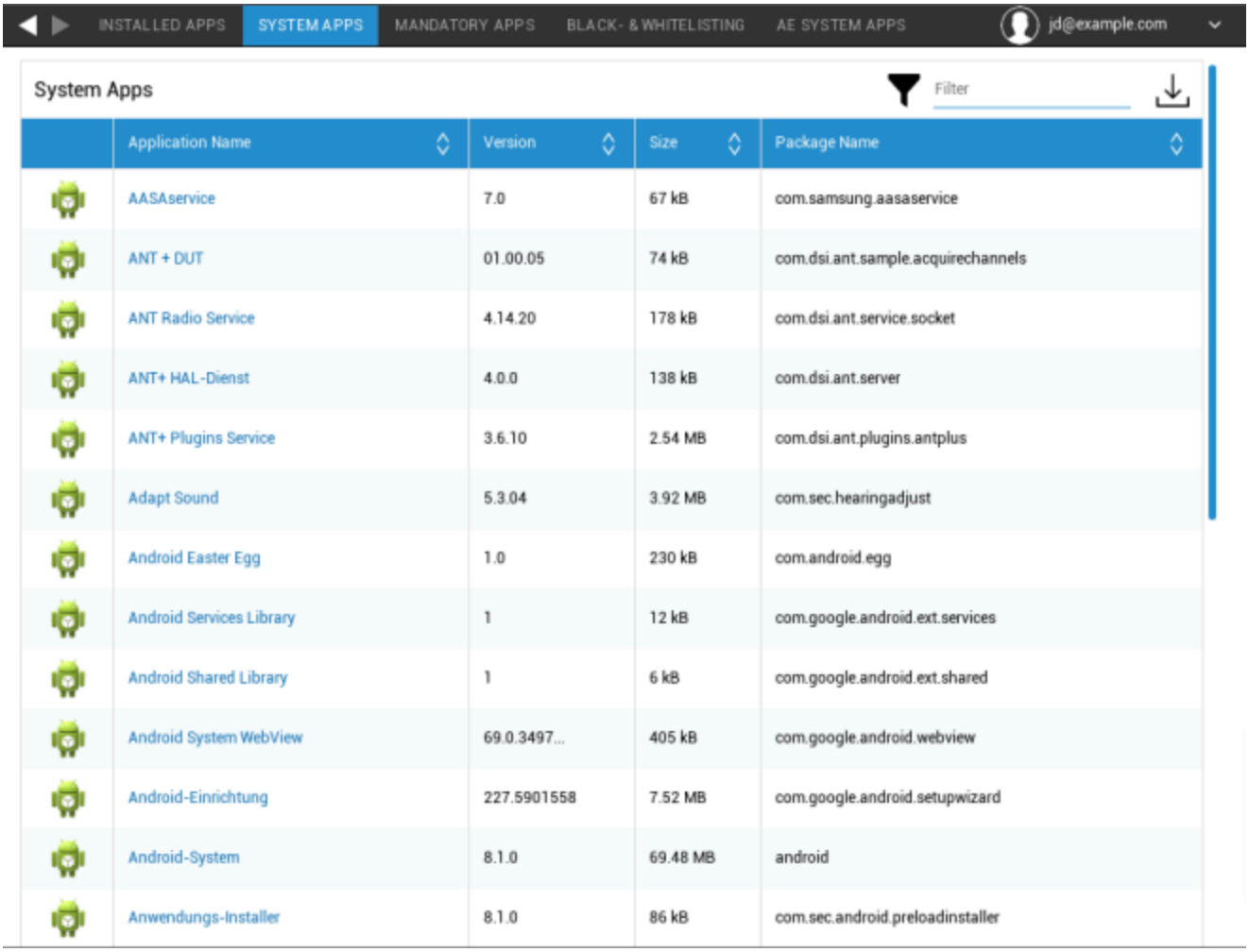
Geïnstalleerde apps (alleen op apparaatniveau)

Hier worden alle apps weergegeven die momenteel zijn geïnstalleerd op het eindgebruikerapparaat.



Systeemapps (alleen op apparaatniveau)

Onder "System Apps" worden alle apps en services weergegeven die al door de fabrikant van het apparaat op het eindapparaat zijn geïnstalleerd.

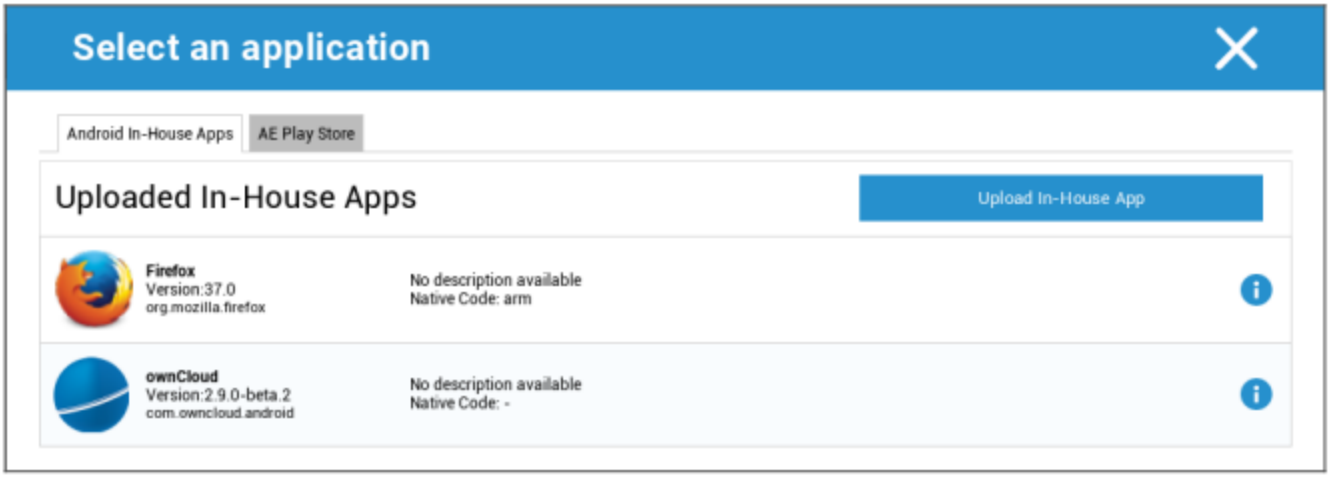


Verplichte apps

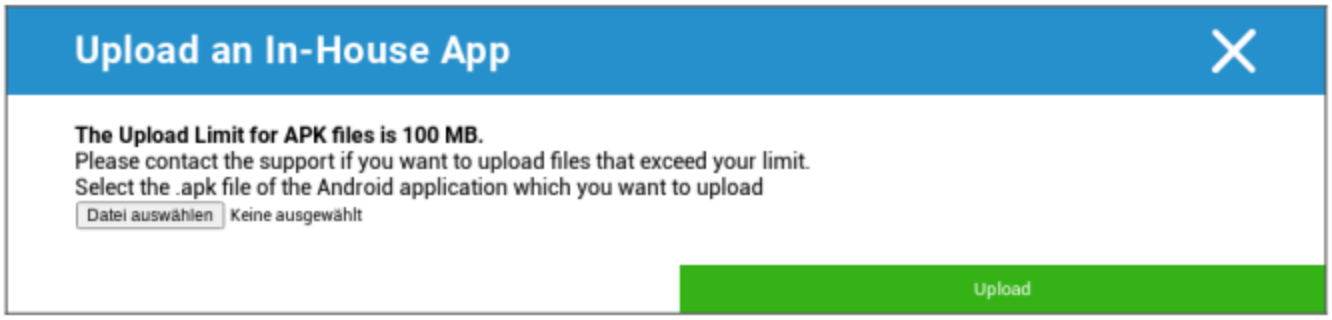
Onder de Verplichte apps kun je de verplichte apps instellen. De gebruiker wordt voortdurend gevraagd om deze aangewezen app te installeren.

Via de , kan de verplichte app worden gedefinieerd.

Dit kan een In-House App zijn uit de "Android In-House Apps", die je hebt geüpload in Algemene Instellingen.

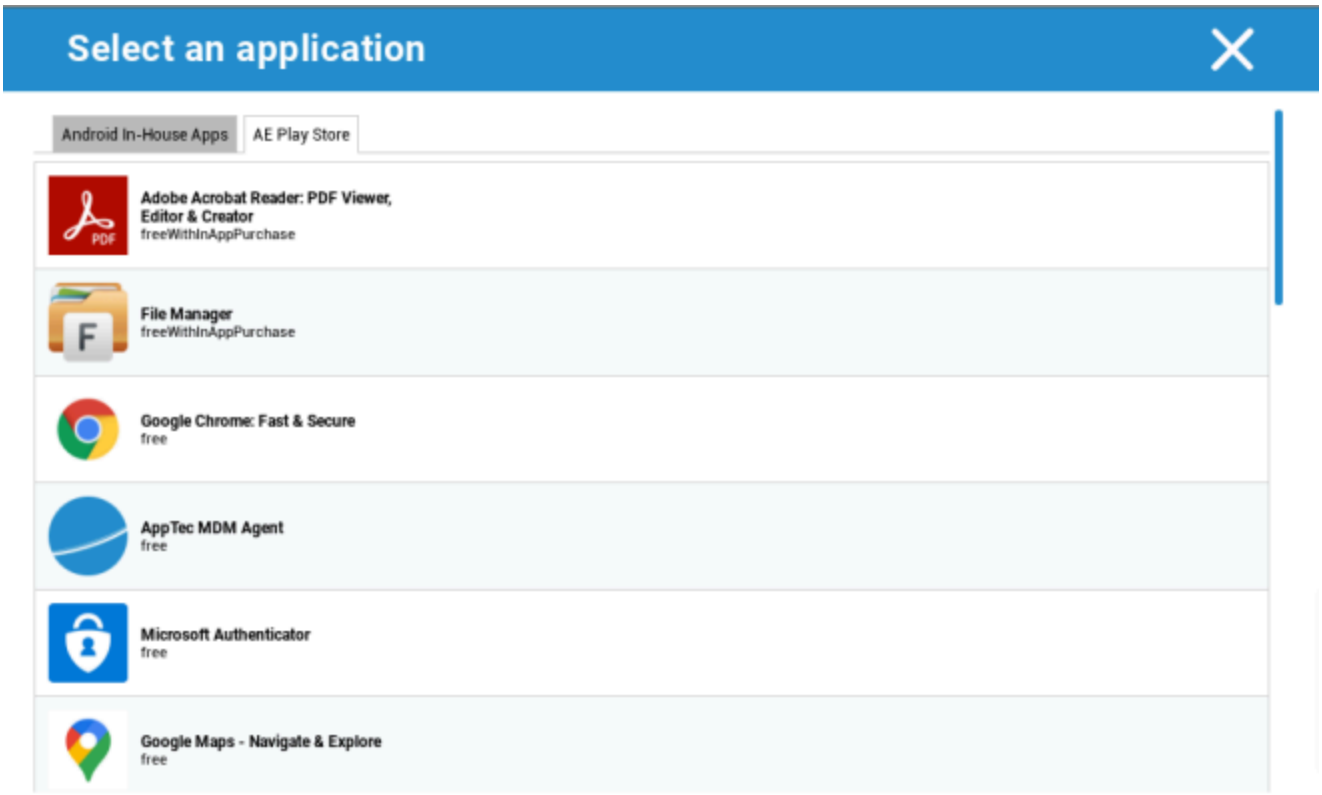


Je kunt ook direct een apk-bestand selecteren en uploaden met "Eigen app uploaden".



Als je een In-House App installeert, heb je de mogelijkheid om "Up-to-date houden" te activeren. Als dit is geactiveerd en je hebt een nieuwere versie gedefinieerd in de In-House App DB, dan wordt de app bijgewerkt op het apparaat.

Of het kan een "AE Play Store"-app zijn uit de Google Work Play Store.



Alleen goedgekeurde "AE Play Store Apps" worden op dit tabblad weergegeven.

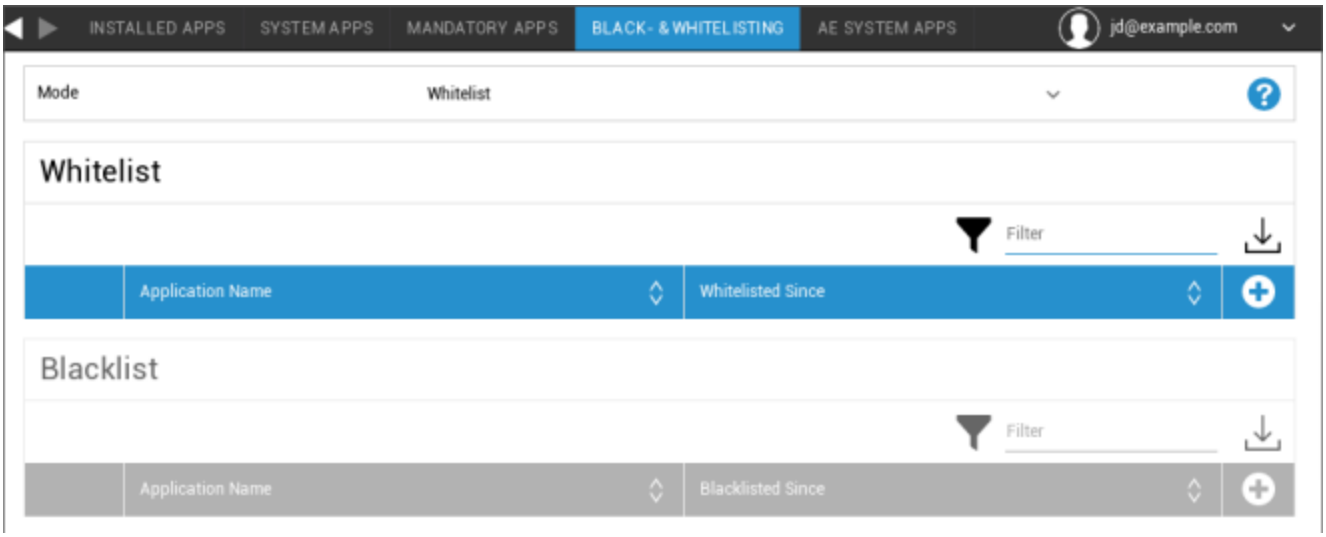
Om een "AE Play Store App" goed te keuren, gaat u naar "Algemene instellingen" > "Appbeheer" > "AE Play".

Store" en voeg een app toe via de knop die je doorverwijst naar het tabblad "Play Store Apps" (of je kunt rechtstreeks naar het tabblad "Play Store Apps" gaan).

In het tabblad "Play Store Apps" kun je naar apps zoeken. Als je op een app klikt, opent de app-pagina en hier kun je de app goedkeuren door op "Goedkeuren" te klikken.

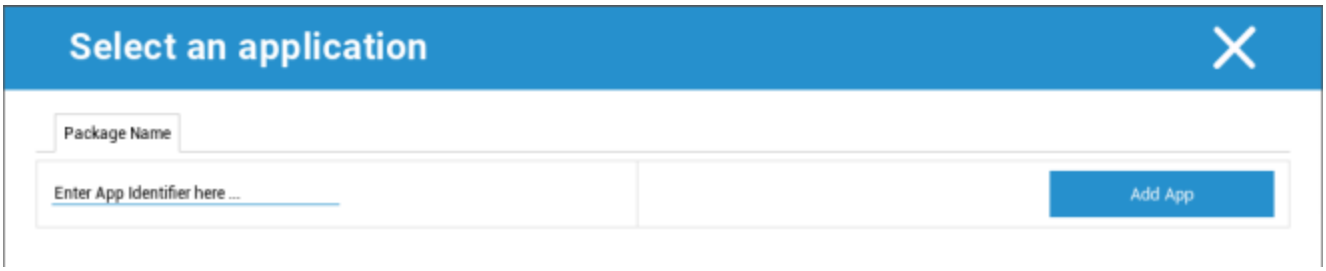
Zwarte lijsten en witte lijsten

Onder "Black- & Whitelisting" kun je kiezen tussen de modus "Whitelist" en de modus "Blacklist".



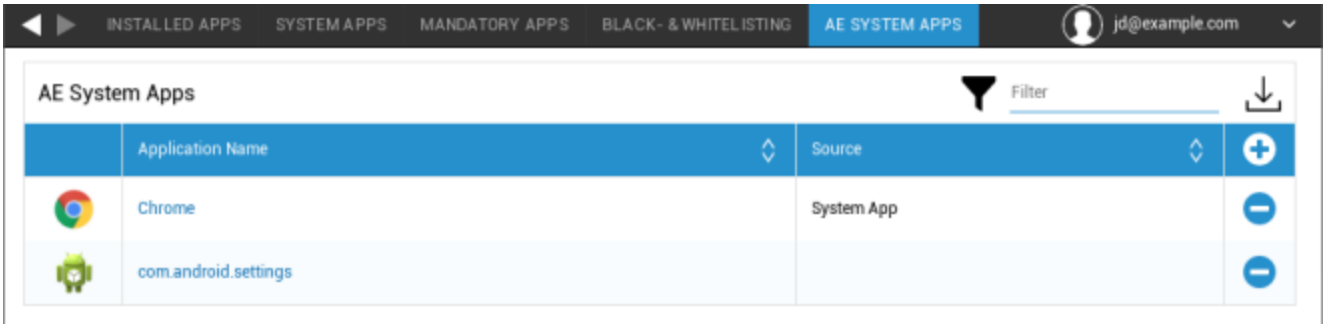
Whitelist	Alleen apps en services die aan de lijst zijn toegevoegd, kunnen op het eindgebruikerapparaat worden geïnstalleerd. Als deze al vooraf zijn geïnstalleerd op het eindgebruikerapparaat, worden ze geactiveerd en ingesteld, zodat de gebruiker ze kan uitvoeren.
	Alle andere apps die niet aan de lijst zijn toegevoegd, kunnen niet op het eindgebruikerapparaat worden geïnstalleerd. Als deze al vooraf zijn geïnstalleerd op het eindgebruikerapparaat, worden ze gedeactiveerd en ingesteld, zodat de gebruiker ze niet kan uitvoeren.
Zwarte lijst	Apps en services die aan de lijst zijn toegevoegd, kunnen niet op het eindgebruikerapparaat worden geïnstalleerd. Als deze al vooraf zijn geïnstalleerd op het eindgebruikerapparaat, worden ze gedeactiveerd en ingesteld, zodat de gebruiker ze niet kan uitvoeren.
	Alle andere apps die niet aan de lijst zijn toegevoegd, kunnen op het eindgebruikerapparaat worden geïnstalleerd. Als deze al vooraf zijn geïnstalleerd op het eindgebruikerapparaat, worden ze geactiveerd en ingesteld, zodat de gebruiker ze kan uitvoeren.

Via de , voegt u extra apps of services toe aan de momenteel gebruikte lijst.
Via de , voegt u extra apps of services toe aan de momenteel inactieve lijst.
U kunt een "Packagename" definiëren:

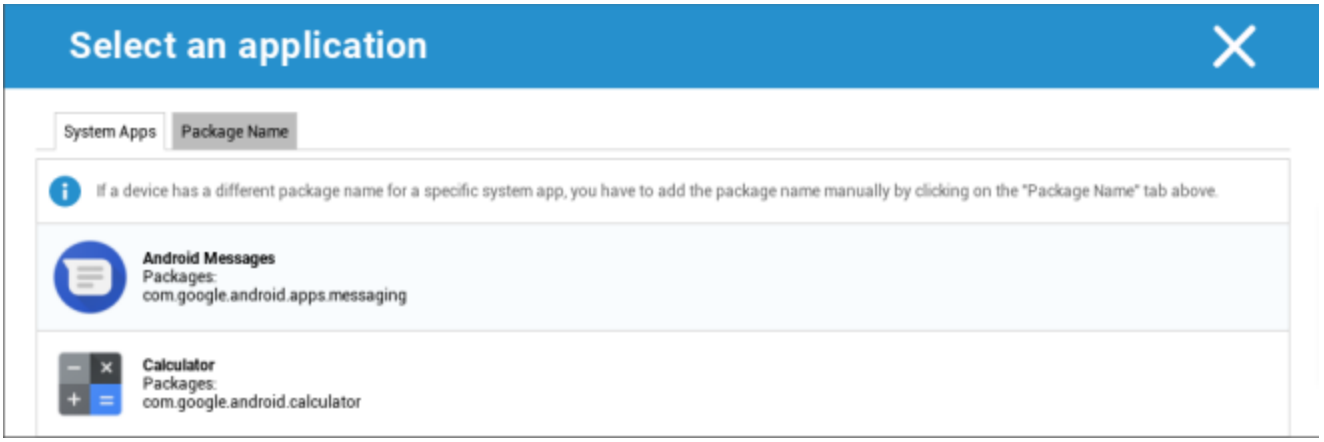

Select an application
Package Name
Enter App Identifier here ...
Add App

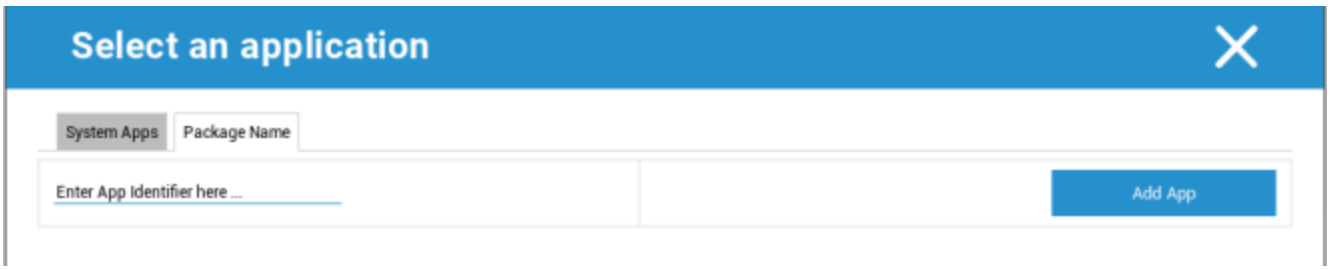
AE-systeemapps

Hier kun je een lijst definiëren met specifieke systeemapps die moeten worden geactiveerd op de apparaten.



Als je op de knop klikt, kun je kiezen uit een lijst met mogelijke systeemapps van Google of direct de pakketnaam invoeren van een systeemapp die moet worden geactiveerd.





Houd er rekening mee dat de systeem-apps in de lijst van Google alleen apps zijn die systeem-apps kunnen zijn, maar niet per se systeem-apps hoeven te zijn op je apparaten.

Deze lijst heeft echter alleen betrekking op apps die al vooraf zijn geïnstalleerd.

Het toevoegen van apps die niet vooraf op uw apparaten zijn geïnstalleerd, heeft geen invloed op uw apparaten, ongeacht of de app uit de door Google geleverde lijst komt of de pakketnaam van de app rechtstreeks wordt ingevoerd.

Beperkingen en instellingen

App Beheer Instellingen

Hier kun je het gedrag van het apparaat met betrekking tot app-updates configureren.

Controlefrequentie bijwerken	Geef aan met welk interval de AppTec360 Client naar app-updates zoekt. De standaardwaarde is 24 uur.
Wi-Fi-drempel	Apps die groter zijn dan de opgegeven grootte worden via Wi-Fi gedownload. Als "Alleen Wi-Fi" is geselecteerd, worden alle apps via Wi-Fi gedownload.

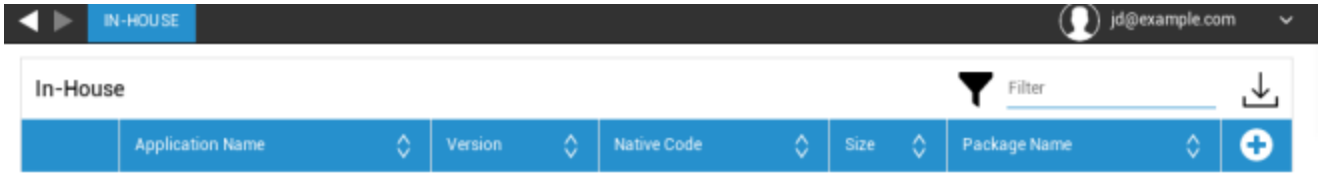
App Store voor ondernemingen

Intern

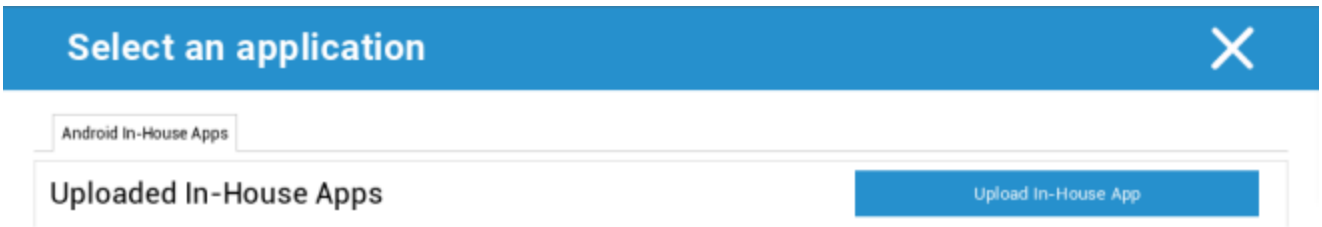
Onder het punt "In-House" kun je intern ontwikkelde apps uploaden en distribueren.

Met het symbool kun je extra In-House Apps distribueren.

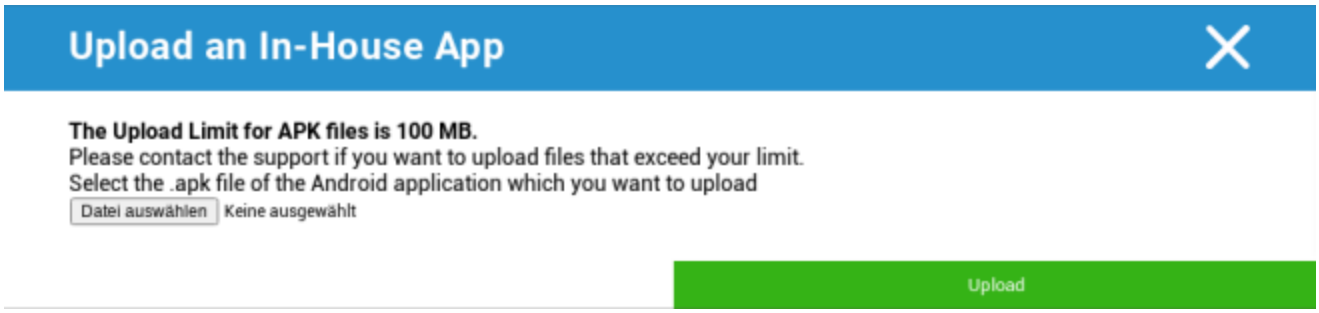
Als je een In-House App installeert, heb je de mogelijkheid om "Up-to-date houden" te activeren. Als dit activeert en je hebt een nieuwere versie gedefinieerd in de In-House App DB, dan wordt de app bijgewerkt op het apparaat.



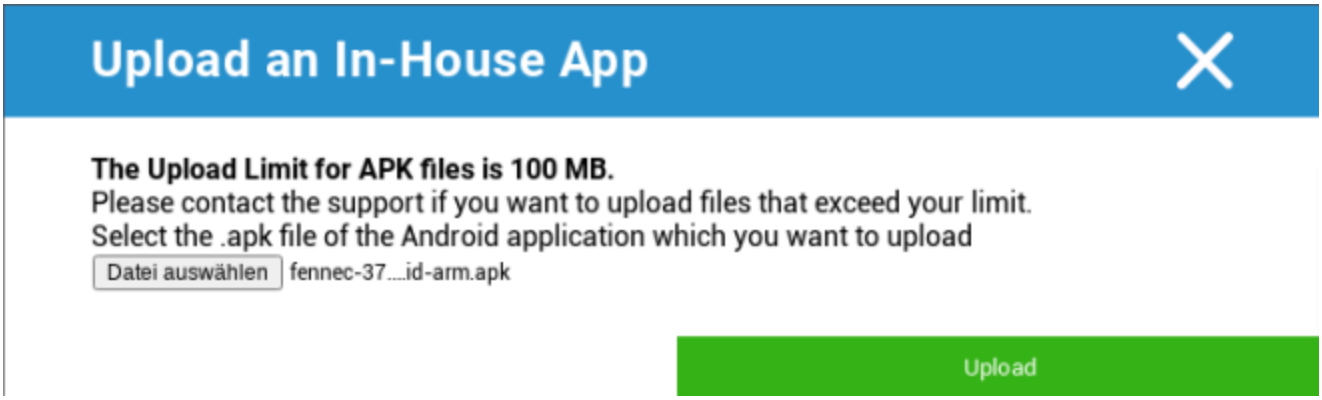
Als je geen In-House Apps hebt gedistribueerd, ontvang je het volgende overzicht:



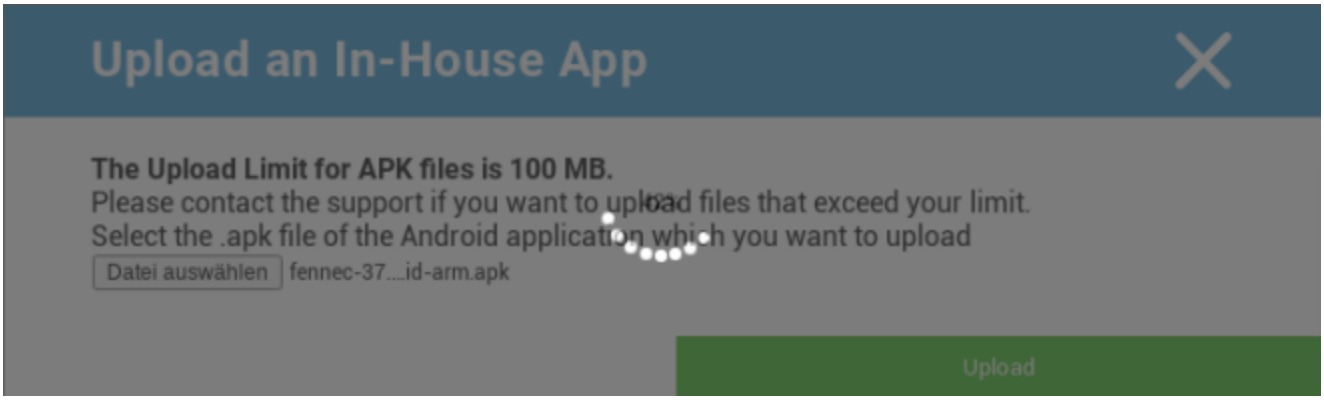
Klik hiervoor op "Upload In-House App", je krijgt dan het volgende overzicht te zien:



Kies nu met "Zoeken..." een .apk-bestand en klik vervolgens op "Uploaden".



Je app wordt nu geüpload. In het midden van de cirkel zie je een percentage-indicator, die aangeeft hoeveel van je app al is geüpload.



Als het uploaden van je In-House App is gelukt, kun je de geüploade app terugvinden in je App Catalogus.

De gebruiker heeft nu de mogelijkheid om deze app te zien en te installeren in de AppTec360 Store op het eindgebruiker
apparaat, onder de categorie "In-House".

Omdat het hier niet om een Google PlayStore App gaat, heeft de gebruiker geen opgeslagen Google ID nodig op zijn eindgebruiker.

Play Store voor bedrijven

AE Play Store

Hier kunt u Apps toevoegen aan de Android Enterprise Playstore. Houd er rekening mee dat u Apps moet goedkeuren met uw AE Administrator Account voordat u ze kunt toevoegen.

Zie voor het goedkeuren van een app de instructies in Verplichte apps.

Kioskmodus & Launcher

Kioskmodus

Met de Kioskmodus kun je een app of URL vooraf definiëren. Dan zal het uitsluitend mogelijk zijn om deze app en/of URL uit te voeren/te bezoeken.

Op dezelfde manier kunnen verschillende hardwareknoppen gedeactiveerd worden in de verschillende Kioskmodi.

Automatisch starten	Start automatisch de Kiosk-modus zodra het profiel het eindgebruikersapparaat bereikt
Geplande kioskmodus?	Je kunt een tijd plannen voor de Kioskmodus, deze zal dan automatisch starten en eindigen op een door jou ingestelde tijd.
Starttijd	Starttijd
Tijd in minuten	Tijd in minuten waarna de Kioskmodus weer moet eindigen

Type toepassing

Enkele app	Als je de app in de Kioskmodus wilt starten, selecteer dan Package" onder "Application Type".
Kiosk-toepassing	Klik hier om een app te selecteren die moet worden gestart in Kioskmodus U vindt het gebruikelijke App Management overzicht U kunt kiezen tussen een "Google Play Store", "Android In-House Apps" en een "Pakketnaam".

Type toepassing

URL	Als je een URL wilt starten in de Kioskmodus, selecteer dan "URL" onder "Type toepassing". Definieer vervolgens het gewenste URL-adres
Browser wissen na inactiviteit	Hier kunt u een tijdsinterval in minuten instellen waarna de Kioskmodus opnieuw moet worden gestart.
Webcache en cookies wissen	Als u deze functie activeert, zal na een herstart van de Kioskmodus de webcache (cookies en afbeeldingen in het cachegeheugen) worden gewist.
Beleid voor dezelfde herkomst	Als deze functie actief is, dan kan de gebruiker alleen surfen op de subpagina's van een gedefinieerde URL Je hebt bijvoorbeeld de volgende URL gedefinieerd:www.mypage.com Dan kan de gebruiker surfen op: www.mypage.com/subpage
URL's op witte lijsten	Hier kun je een witte lijst bijhouden, al deze URL's zijn toegestaan Maximaal 1 URL per regel Een URL moet beginnen met http:/ of https://.
URL's op de zwarte lijst	Hier kun je een zwarte lijst bijhouden, al deze URL's zijn niet toegestaan Maximaal 1 URL per regel Een URL moet beginnen met http:/ of https://.
Schermoriëntatie	Deze instelling heeft betrekking op de schermaanpassingen Automatisch = automatisch Staand = verticaal formaat Landschap = liggende modus

Meerdere apps	Als je de "Multi App" Kiosk Mode selecteert, wordt het gebruik van de AppTec360 Launcher afgedwongen.
Apps	Toepassing: Selecteer een Playstore of een eigen app als Kiosk-toepassing. Het is ook mogelijk om een packagenaam in te voeren. De geselecteerde Kiosk-applicatie moet geïnstalleerd zijn op het apparaat. Vergeet niet om de Kiosk Application als verplicht in te stellen. Snelkoppeling op Homescreen: Als deze optie is ingesteld op "Aan" wordt er een snelkoppeling op het beginscherm gemaakt. Als dit is ingesteld op "Uit" wordt de app nog steeds weergegeven in de app-lijst.

Wachtwoord afsluiten ingeschakeld	Als u deze functie activeert, is het mogelijk voor de gebruiker om de Kiosk-modus te beëindigen met een wachtwoord dat u vooraf hebt ingesteld.
Wachtwoord afsluiten	Dit is het wachtwoord dat vooraf door u is ingesteld
Statusbalk automatisch samenvouwen	Als deze optie is ingeschakeld, wordt de Statusbalk automatisch ingeklapt. Met deze optie kunnen gebruikers de informatie op de Statusbalk zien, maar hebben ze geen toegang tot de functies ervan.
Statusbalk uitschakelen	De statusbalk bevat meldingen, snelkoppelingen en informatie. Alleen beschikbaar voor Samsung-apparaten met SAFE 4.0 of hoger.
Volumetoetsen uitschakelen	Volumetoetsen uitschakelen (alleen beschikbaar op Samsung-apparaten met SAFE 3.0 of hoger)
Aan/uit-schakelaar uitschakelen	Aan/uit-schakelaar uitschakelen (alleen beschikbaar op Samsung-apparaten met SAFE 3.0 of hoger)
Home-knop uitschakelen	Home-knop uitschakelen. Als deze functie is geactiveerd, kan de Kiosk-modus alleen in de AppTec360 Console worden beëindigd. (alleen beschikbaar op Samsung-apparaten met SAFE 3.0 of hoger)
Navigatiebalk uitschakelen	Hiermee kun je de navigatiebalk (Terug / Menu) uitschakelen. Als deze functie is geactiveerd, kan de Kiosk-modus alleen in de AppTec360 Console worden beëindigd. (alleen beschikbaar op Samsung-apparaten met SAFE 3.0 of hoger)

AppTec360 Launcher

AppTec360 Launcher inschakelen	Aan: Schakelt de AppTec360 Launcher in. De gebruiker moet deze eenmalig instellen als standaard Launcher. Opmerking: Als de Kiosk-modus is ingeschakeld en de Kiosk-modus is ingesteld op "Multi App", wordt het gebruik van AppTec360 launcher afgedwongen.
Grote pictogrammen	Aan: Toont een grotere versie van de app-pictogrammen in de Launcher
AppTec360-pictogram verbergen	Aan: Verbergt de AppTec360 App volledig
AppTec360-winkelpictogram verbergen	Aan: Verbergt de AppTec360 Enterprise AppStore volledig

AppTec360-instellingen

AppTec360 Instellingen App inschakelen	De AppTec360 Settings App biedt controle over WiFi- en Bluetooth-verbindingen.
Instellingen inschakelen in meerdere apps Kioskmodus	Indien ingeschakeld, hebben gebruikers toegang tot de AppTec360 Settings App terwijl de Multi App Kiosk Mode actief is.

Afstandsbediening

Splashtop

Om een afstandsbedieningssessie voor uw apparaat te starten, moet de app "Splashtop Streamer" op het apparaat worden geïnstalleerd door de app toe te voegen aan **App Management** → **Enterprise App Manager** → **Verplichte apps**.

Configureer daarna de volgende instellingen voor Splashtop:

Splashtop inschakelen	Als AppTec360 deze optie inschakelt, wordt de Splashtop-app zo geconfigureerd dat bediening op afstand mogelijk is.
Code implementeren	Ga naar https://my.splashtop.com en log in op uw Splashtop-account. Klik op "Computer toevoegen" en kopieer de 12-cijferige inzetcode van de resulterende pagina.
Aangepaste implementatiegateway instellen?	Gateway implementeren
Gateway domein / host implementeren	Gateway implementeren
Certificaatverificatie	Certificaatverificatie

Vervolgens kun je de optie Splashtop afstandsbediening gebruiken in het contextmenu (tandwiel naast de zoekbalk wanneer het apparaat is geselecteerd of klik met de rechtermuisknop op het apparaat in de boomstructuur) om de afstandsbedieningssessie te starten.

TeamViewer

Om een afstandsbedieningssessie voor uw apparaat te starten, moet de app "TeamViewer QuickSupport" op het apparaat worden geïnstalleerd door de app toe te voegen aan **App Management** → **Enterprise App Manager** → **Verplichte apps**.

Vervolgens kunt u de optie **TeamViewer afstandsbediening** gebruiken in het contextmenu (tandwiel naast de zoekbalk wanneer het apparaat is geselecteerd of klik met de rechtermuisknop op het apparaat in de boomstructuur) om de afstandsbedieningssessie te starten.

Beheer van inhoud

ContentBox

Hier kun je de ContentBox activeren.

Zodra je "Enable ContentBox" op "On" zet, wordt er automatisch een aparte ContentBox App geïnstalleerd
op het eindgebruiker apparaat.

Veilige browser

Hier kun je instellingen configureren voor de AppTec360 Secure Browser.

Zodra je het onderdeel "Veilige browser" inschakelt op "Aan", wordt er automatisch een aparte Browser App
geïnstalleerd op het apparaat van de eindgebruiker.

Wachtwoord nodig	Eis dat de gebruiker een wachtwoord instelt en gebruikt om toegang te krijgen tot de browser.
Minimaal vereiste wachtwoordlengte	Stel het vereiste aantal tekens in voor het wachtwoord
Vereiste wachtwoordkwaliteit	Stel de vereiste wachtwoordkwaliteit in
Beperk downloads / Open in	
Uploads beperken	
Whitelist uploaden	Een lijst met URL's waarvoor uploaden altijd wordt toegestaan.
Kopiëren toestaan	Sta het kopiëren, knippen of delen van tekst binnen de webpagina's toe.
Schermopname toestaan	Het maken van schermafbeeldingen toestaan.
Frequentie gegevensopschoning	Selecteer met welke frequentie ALLE gebruikersgegevens (geschiedenis, cache enz.) automatisch moeten worden verwijderd.
Bladwijzers voor bedrijven	De bladwijzers worden weergegeven in de map "Bedrijfsbladwijzers" in de bladwijzers van de browser. Ze kunnen niet bewerkt worden door de gebruiker.
Adresbalk verbergen	
Whitelisting in browser (zonder Universal Gateway)	Schakelt client-side URL whitelisting in. • Bladwijzers van bedrijven worden altijd gewist • Alleen ondersteund voor 100 URL's • Gebruik de Universal Gateway voor onbeperkt Black- en Whitelisting
URL's op witte lijsten	Een lijst met toegestane URL's.
Black- en whitelisting op basis van gateways	Blacklisting heeft de volgende vereisten:

	• Een werkende AppTec360 Universal Gateway ("Algemene instellingen" → "Universal Gateway") • Een werkende VPN-configuratie met een opgegeven DNS-server ("Algemene instellingen" → "Universele gateway" → "VPN-instellingen") • Een Blacklist-configuratie ("Algemene instellingen" → "Universal Gateway" → "Domein Blacklist") • Een geldige VPN-verbinding in het profiel ("Verbindingsbeheer" → "VPN")

Extra API

Samsung KNOX

Beperkingen

SD-kaart toestaan	
SD-kaart schrijven toestaan	
Schermopname toestaan	
Klembord toestaan	
Back-up maken van instellingen en app-gegevens in Google Cloud	
Instellingen herstellen vanuit Google Cloud bij het opnieuw installeren van een app	
USB-debugging toestaan	
Google Crash Rapport toestaan	
Fabrieksreset toestaan	
OTA-upgrade toestaan	
USB-hostopslag toestaan	Als dit is ingeschakeld, kan een gebruiker een pen drive (draagbare USB-opslag), externe HD of Secure Digital (SD) kaartlezer aansluiten en wordt deze als een opslagstation op het apparaat gemount.
USB-mediaspeler toestaan (MTP, PTP)	
Microfoon toestaan	Schakelt de microfoon uit voor toepassingen van derden
NFC (Near Field Communication) toestaan	
Onbekende bronnen toestaan (APK Sideloading)	Als deze optie is ingeschakeld, is side-loading van apps (APK-bestanden) toegestaan. Zodra deze instelling is uitgeschakeld, moet de gebruiker deze handmatig inschakelen wanneer je de installatie van APK's van onbekende bronnen opnieuw toestaat.
Gebruiker aanmaken toestaan	Als deze optie is ingeschakeld, mogen gebruikers meerdere accounts aanmaken op het apparaat, bijvoorbeeld gastaccounts.

E-mail

E-mailadres	
Inkomend serverprotocol	
Inkomend serveradres	
Inkomende serverpoort	
Inlognaam/gebruikersnaam van inkomende server	
Inkomend serverwachtwoord	
Inkomende server gebruikt SSL	
Inkomende server gebruikt TLS	
Inkomende server accepteert alle certificaten	
Uitgaand serverprotocol	
Uitgaand serveradres	
Uitgaande serverpoort	
Uitgaande server gebruikt extra referenties	Als dit is uitgeschakeld, gebruikt het systeem de inkomende aanmeldgegevens ook voor de uitgaande server.
Uitgaande server login/gebruikersnaam	
Uitgaand serverwachtwoord	
Uitgaande server gebruikt SSL	
Uitgaande server gebruikt TLS	
Uitgaande server accepteert alle certificaten	
Handtekening instellen	
Handtekening	Opmerking: Voor sommige apparaten moet de handtekening in HTML-formaat gespecificeerd worden.
Gebruiker op de hoogte stellen bij ontvangst van nieuwe e-mail	

Uitwisseling

E-mailadres	
Server hostnaam	De hostnaam van de Exchange Server
Inlognaam	De gebruikersnaam die wordt gebruikt om in te loggen op de Exchange Server
Domein	Als een ACL-gatewayconfiguratie is ingeschakeld en het veld Domein niet leeg is, zal de AppTec360 Universal Gateway het apparaat authenticeren met de volgende naam "Domeinnaam".
Wachtwoord	
Aantal vorige dagen om te synchroniseren	
Frequentie om eMail te synchroniseren	
Synchroniseren tijdens roaming	
Handtekening instellen	
Handtekening	Opmerking: Voor sommige apparaten moet de handtekening in HTML-formaat gespecificeerd worden.
Standaard account	
Gebruik SSL (Secure Sockets Layer)	
Gebruik TLS (Transport Layer Security)	
Accepteer alle certificaten	

APN

APN Weergavenaam	
Naam toegangspunt	Naam van het APN
Uitgaand serverprotocol	
MCC - Mobiele landcode	Leeg laten om mmc van geïnstalleerde SIM te gebruiken
MNC - Mobiele netwerkcode	Leeg laten om mnc van geïnstalleerde SIM te gebruiken
Serveradres	
Poortnummer server	
Proxy-adres server	
MMS server adres	Leeg laten voor standaard
MMS poortnummer	Leeg laten voor standaard
MMS proxy-adres	Leeg laten voor standaard
Gebruikersnaam	
Wachtwoord	
Type toegangspunt	Geaccepteerde types zijn "default", "mms", "supl".
	Als nul of leeg wordt doorgegeven, wordt standaard "default,supl,mms" gebruikt.
	Laat leeg voor standaard.
Voorkeur APN	

Bluetooth

Apparaatontdekking via Bluetooth toestaan	
Bluetooth-koppeling toestaan	
Bluetooth-headsetapparaten toestaan	
Bluetooth-handsfree-apparaten toestaan	
Bluetooth A2DP-apparaten toestaan	A2DP, Advanced Audio Distribution Profile maakt audiostreaming tussen apparaten mogelijk
Uitgaande gesprekken toestaan	
Gegevensoverdracht via Bluetooth toestaan	
Bluetooth-tethering toestaan	
Verbinding met computer via Bluetooth toestaan	

Aansluiting

Alleen noodoproepen toestaanWi-Fi toestaan	
Minimumbeveiligingsniveau Wi-Fi-netwerk	
Verbied gebruiker om Wi-Fi-netwerken toe te voegen	Deze beperking kan alleen worden geactiveerd als er ten minste één actief Wi-Fi-profiel is gedefinieerd onder Verbindingsbeheer.
SMS & MMS toestaan	
Synchronisatie toestaan tijdens roaming	
Spraak Roaming toestaan	

Android Enterprise – Volledig beheerd apparaat met werkprofiel (COPE)

Algemene uitleg van COPE

COPE is een afkorting voor **Corporate Owned Personally Enabled**.

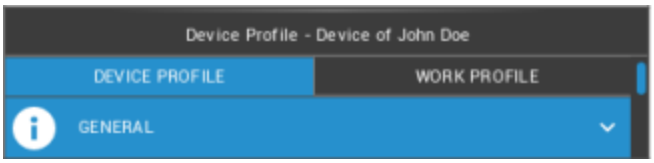
Met de COPE-modus kan een Android-apparaat worden geregistreerd als een **Android Enterprise - Fully Managed Device** met geïntegreerd **Android Enterprise - Container-profiel**.

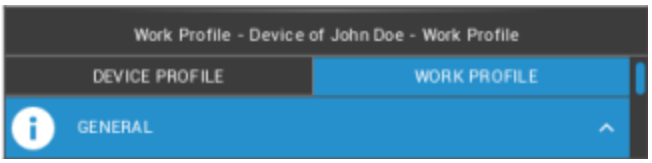
Dit kan ofwel een Android-apparaat zijn dat al is ingeschreven als een **Android Enterprise - Fully Managed Device** en waarop de **Android Enterprise - Container** extra is ingesteld, of een nieuw ingeschreven Android-apparaat dat direct is ingeschreven als een **Android Enterprise - Fully Managed Device** samen met de **Android Enterprise - Container** erop.

De COPE-modus is alleen beschikbaar voor apparaten met Android 8, 9 en 10.

Configuratie van profielen voor COPE-apparaten

Aangezien er geen configuratieprofiel is voor de COPE-modus zelf, is de configuratie van **Android Enterprise - Volledig beheerd apparaat** en **Android Enterprise - Container** gescheiden in twee profielen binnen het COPE-profiel. Het is mogelijk om te schakelen tussen de twee profielen voor de configuratie van elk profiel door te klikken op de respectieve knop aan de linkerkant van de console:





Beide profielen kunnen geconfigureerd worden zoals beschreven voor elk individueel profiel:

Android Enterprise - Volledig beheerd apparaat

Android Onderneming - Container

Terugkeren naar AE Volledig beheerd apparaat

Het **Android Enterprise - Container** profiel kan worden verwijderd zoals beschreven in **Mobile Management**.

Door het Container profiel te verwijderen, wordt het COPE profiel getransformeerd naar een **Android Enterprise - Fully Managed Device** profiel.

Android Enterprise – Containerconfiguratie

Afhankelijk van of je momenteel een groepsprofiel of een apparaat hebt geselecteerd, verschillen het overzicht en de subpunten - denk hier goed over na!

Algemeen

Profieloverzicht (alleen op profielniveau)

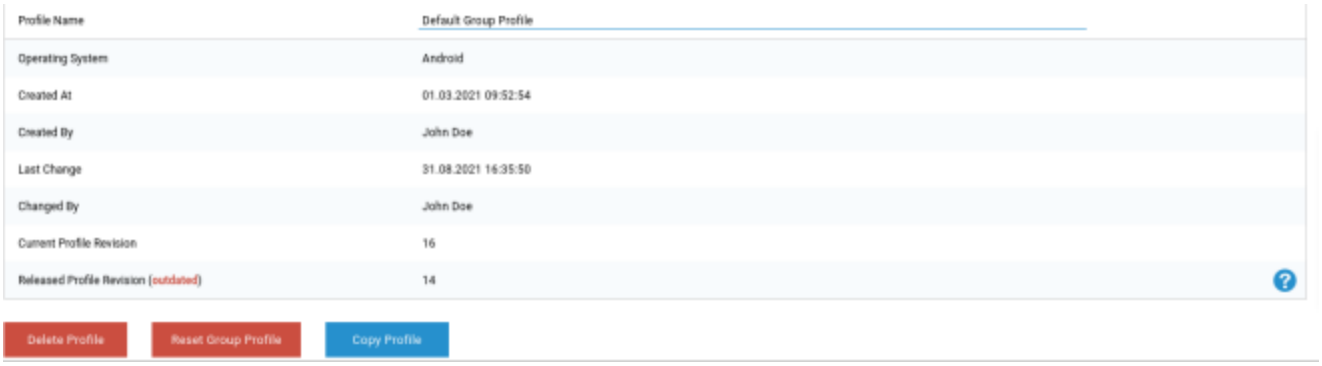
Als je in een profiel zit, krijg je een kort overzicht van het profiel, met naam, OS, aanmaakdatum, auteur, enz.

Profielnaam	Profielnaam - kan hier direct worden hernoemd
Besturingssysteem	Geldig OS voor het profiel
Gemaakt op	Aanmaakdatum
Gemaakt door	Gemaakt door
Laatste wijziging	Laatste wijzigingsdatum
Veranderd door	De gebruiker die de laatste wijzigingen in dit profiel heeft uitgevoerd
Huidige profielherziening	Aantal keren dat het profiel al is bijgewerkt
Vrijgegeven profiel Revisie	Aantal keren dat het profiel al is bijgewerkt en er apparaten aan zijn toegewezen

Profiel verwijderen	Profiel verwijderen
Groepsprofiel opnieuw instellen	Groepsprofiel opnieuw instellen
Profiel kopiëren	Profiel kopiëren

Overzicht groepsprofiel (alleen op groepsniveau)

Wanneer je een groepsprofiel opent, krijg je een snel overzicht van het profiel.



Profielnaam	Naam van het profiel (kan hier worden gewijzigd)
Besturingssysteem	Besturingssysteem waar het profiel voor is
Gemaakt op	Tijd van creatie
Gemaakt door	De maker van het profiel
Laatste wijziging	Tijdstip van laatste wijziging van het profiel
Veranderd door	Account die de laatste wijzigingen heeft aangebracht
Huidige profielherziening	Revisie van opgeslagen profielstatus
Vrijgegeven profiel Revisie	Toegewezen profielrevisie ("Nu toewijzen"). Als er "(verouderd)" achter de tekst staat, betekent dit dat je het profiel hebt opgeslagen maar nog niet hebt toegewezen, zodat de apparaten nog steeds een oudere versie krijgen.

Apparaatoverzicht (alleen op apparaatniveau)

Als u zich op een apparaat bevindt, krijgt u een overzicht van het geselecteerde apparaat, dat het volgende bevat:

Naam apparaat	Naam apparaat
Locatie	Coördinaten locatie
Telefoonnummer	Telefoonnummer
Toegewezen verplichte apps	Aantal toegewezen verplichte apps
OS versie	OS-versie van het apparaat
Besturingssysteem	Besturingssysteem (Android Enterprise)
Serienummer	Serienummer apparaat
Apparaateigendom	Zakelijk of privéapparaat
Type apparaat	AE Work Beheerd Apparaat
Geworteld	Status, die aangeeft of het apparaat geroot is
Conform	Richtlijnconform
IP-adres	IP-adres van het apparaat
Laatst gezien	Tijdstip waarop het apparaat voor het laatst verbinding heeft gemaakt met AppTec
Laatste duw	Tijdstip waarop de laatste push naar het apparaat is verzonden.
Gebruikerstoewijzing	De gebruiker of groep waaraan dit apparaat is toegewezen

Configuratie Revisie

Hier krijg je een overzicht van welk groepsprofiel aan het apparaat is toegewezen.

Als je op het groepsprofiel klikt, krijg je direct toegang tot dit profiel en kun je instellingen uitvoeren.

Met dit symbool kun je de gedistribueerde apps terugzetten naar de instellingen van het groepsprofiel.

Met dit symbool kun je alle gebruikte apps terugzetten naar de instellingen van het groepsprofiel.

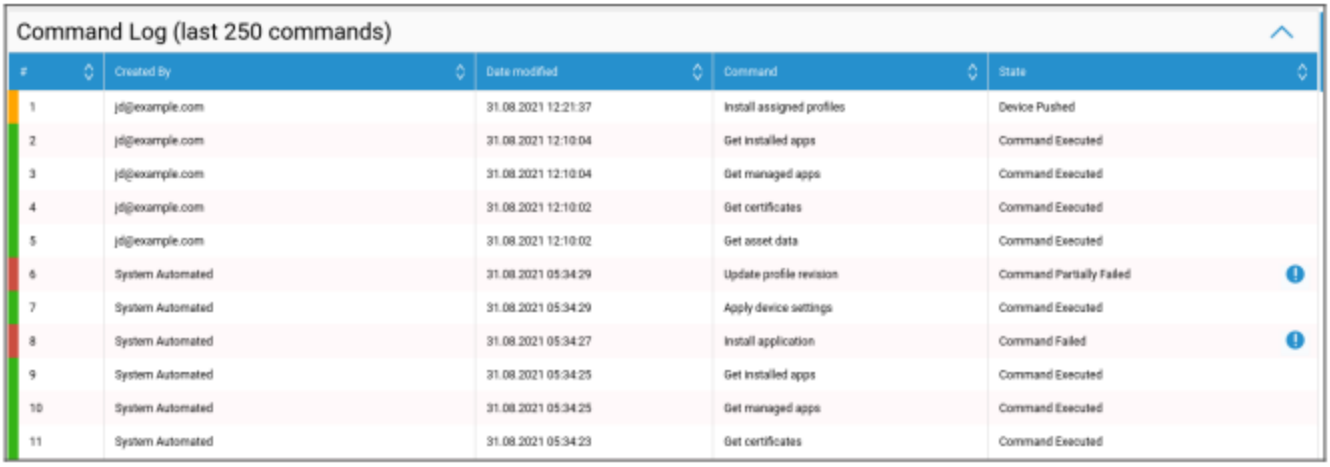
"Newer Revision available" geeft aan dat het groepsprofiel gewijzigd en opgeslagen is, maar niet toegewezen. Het groepsprofiel moet worden toegewezen met "Assign now" op groepsniveau om de wijzigingen toe te passen op de apparaten.

Apparaatlogboek (alleen op apparaatniveau)

Hier krijg je verschillende apparaatlogboeken te zien. Indien nodig kun je hier direct de oorzaak van een fout achterhalen.

Opdrachtlogboek

Hier kun je zien welke commando's zijn uitgegeven voor het apparaat en wat hun status is.



Mogelijke opdrachtstatussen

Apparaat ingedrukt	Er is een pushverzoek verzonden naar de pushservice (bijv. APNS) om het apparaat te vertellen terug verbinding te maken met de EMM-server.
Commando aangemaakt	De opdracht is aangemaakt in het systeem.
Opdracht verzonden	De opdracht werd naar het apparaat gestuurd nadat het verbinding had gemaakt met de server.
Opdracht uitgevoerd	De opdracht is succesvol uitgevoerd.
Opdracht mislukt	De opdracht is mislukt. *
Commando gedeeltelijk mislukt	Afhankelijk van het besturingssysteem van het apparaat kunnen sommige commando's gegroepeerd worden. Hierin zijn sommige delen van deze commandogroep mislukt. *
Opdracht uitgevoerd, uiteindelijk mislukt	Het commando werd uitgevoerd, maar misschien ook niet.
Commando verplaatst	De opdracht is opnieuw uitgevoerd door een gebruiker.
Afgedankt	De opdracht is verwijderd. Bijvoorbeeld omdat het is vervangen door een ander commando of omdat het apparaat opnieuw is aangemeld en oude commando's zijn verwijderd.

*Als er een uitroepteken achter het bericht staat, kun je meer informatie krijgen door met je cursor over het pictogram te gaan.

Apparaatinstellingen

Configuratie klant

Hier kun je de volgende configuraties uitvoeren op je Android-toestel:

Tijd buiten naleving	De time-outlimiet voor de reactie van de gebruiker waarna de handhavingsactie wordt toegepast.
Handhavingsactie na time-out voor naleving	Handhavingsactie als een gebruiker geen acties uitvoert die leiden tot een conform apparaatstatus
Frequentie gegevensverzameling	Frequentie waarmee apparaat/GPS-informatie moet worden verzameld
Hartslagfrequentie apparaat	Interval waarin het apparaat contact moet opnemen met de AppTec Server Min. 1 minuut Max. 24 uur
Locatie-updates inschakelen	Indien geactiveerd stuurt het apparaat locatie-updates naar de AppTec Server.
Locatie Update Tijd	Bepaalt in welke tijdsintervallen het apparaat locatie-updates naar AppTec stuurt
Gebruik Google-nauwkeurigheid voor locatie-updates	Indien geactiveerd, wordt de netwerklocatie gebruikt voor locatie-updates (als dit was uitgeschakeld onder "Beperkingen", dan heeft deze instelling geen invloed)
GPS-locatie gebruiken voor locatie-update	Indien geactiveerd, wordt de GPS gebruikt voor locatie-updates.
Neplocaties toestaan	Maakt het vervalsen van locatiegegevens via apps van derden mogelijk
Verbroken verbinding Actie	Indien ingeschakeld, kun je een actie opgeven voor het geval dat een apparaat geen verbinding krijgt met de MDM-server binnen het heartbeat-interval. Als het apparaat bijvoorbeeld een heartbeat-tijd van 5 minuten heeft, maakt het om 10:35 uur verbinding met de server. Daarna verlaat het apparaat het Wi-Fi-bereik. De volgende heartbeat om 10:40 uur zal mislukken en de opgegeven actie zal worden uitgevoerd.
Actie	De actie die ondernomen moet worden zodra een apparaat niet meer voldoet. • Lock Apparaat = apparaat vergrendelen

	• Apparaat wissen = apparaat wordt teruggezet naar fabrieksinstellingen • Apparaat & SD-kaart wissen = het apparaat wordt teruggezet naar de fabrieksinstellingen en de opslag op de SD-kaart wordt gewist.
Drempel	U kunt een drempelwaarde van mislukte hartslagen opgeven die nodig is om de opgegeven actie te activeren.

Modus voor beleidshandhaving	Standaard:	Gebruikers worden regelmatig gevraagd om uitstaande acties uit te voeren
	Luie handhaving van beleid:	Gebruikers zullen nooit gevraagd worden om openstaande acties uit te voeren. Alle openstaande acties worden getoond in de AppTec Client
	Agressieve beleidshandhaving:	Gebruikers worden non-stop gevraagd om uitstaande acties uit te voeren
AppTec Versie Slot	Als deze optie is ingeschakeld, kan een versiecode voor de AppTec app worden opgegeven. De AppTec client zal alleen updaten naar de gespecificeerde versie. Nieuwere versies worden genegeerd. Een downgrade is NIET mogelijk.	
Versiecode	Versiecode waarop de AppTec app moet worden vergrendeld.	
AppTec-melding uitschakelen	Als deze optie is uitgeschakeld, toont AppTec Client geen melding in de meldingsbalk. Gebruikers kunnen de AppTec client dus afsluiten via het taakbeheer. Als de AppTec client gesloten is, zullen verschillende functies zoals Kiosk Mode en App Black/Whitelisting niet goed werken. Samsung-apparaten bieden een beveiligingsmechanisme voor de AppTec Client. De melding is standaard uitgeschakeld op Samsung-apparaten die de KNOX API's ondersteunen. De melding moet niet worden uitgeschakeld op apparaten met Android 8.0 of hoger.	

Behang

Aangepast behang instellen	De aangepaste achtergrond inschakelen/uitschakelen
Behang	De achtergrondmodus instellen om een kleurcode of een afbeelding te gebruiken
Geef een kleur op	Geef een achtergrondkleur op als hexadecimale waarde, bijvoorbeeld #000000 voor zwart of #fffff als wit
Afbeelding instellen als achtergrond	Upload het afbeeldingsbestand dat je als achtergrond wilt gebruiken

Activabeheer (alleen op apparaatniveau)

Apparaat info

Model	Typeaanduiding apparaat
Besturingssysteem	OS
OS versie	OS-versie
Serienummer	Serienummer
Naam apparaat	Naam apparaat
Batterijstatus	Batterijstatus
Vrij / Totaal geheugen	Vrij / Totaal geheugen
Samsung Veilig	Samsung SAFE-interface, vereist voor diverse instelopties
SD-kaart beschikbaar	SD-kaart beschikbaar
SD-kaart geëmuleerd	SD-kaart geëmuleerd
SD-kaart verwijderbaar	SD-kaart verwijderbaar
SD vrij / totaal geheugen	SD vrij / totaal SD-kaartgeheugen

Wi-Fi

IP-adres	IP-adres apparaat
WiFi MAC	WiFi-MAC-adres

Cellulair

Status	Status (SIM-kaart geïnstalleerd)
Telefoonnummer	Telefoonnummer
Roaming (spraak/data)	Roaming voor spraak/data
Roaming-status	Huidige roamingstatus
IP-adres	IP-adres
Exploitant/vervoerder	Exploitant/vervoerder
Cellulaire technologie	Cellulaire technologie
IMEI	IMEI-nummer
ICCID	Dit is de ID voor de SIM-kaart, vaak ook een Smartcard of Integrated Circuit Card (ICC).
IMSI	De International Mobile Subscriber Identity (IMSI) biedt in GSM- en UMTS-mobiele netwerken een definitieve identificatie van de netwerkgebruikers. De IMSI bestaat uit maximaal 15 cijfers en wordt als volgt geconfigureerd: • Mobiele landcode (MCC), 3 cijfers • Mobiele netwerkcode (MNC), 2 of 3 cijfers • Identificatienummer mobiele abonnee (MSIN), 1-10 cijfers
Huidige MCC/MNC	Zie "SIM MCC/MNC".
SIM MCC/MNC	De mobiele landcode is een vastgestelde landidentificatie die door de ITU is ingesteld volgens de E.212-norm. Deze werkt samen met de mobiele netwerkcode (MNC) voor de identificatie van het mobiele netwerk. Dit betekent de landcode/mobiele netwerkcode van de SIM-kaart. Als je naar een ander mobiel netwerk roamt, zullen de "Current MCC/MNC" en "SIM MCC/MNC" logischerwijs verschillend zijn.

Bluetooth

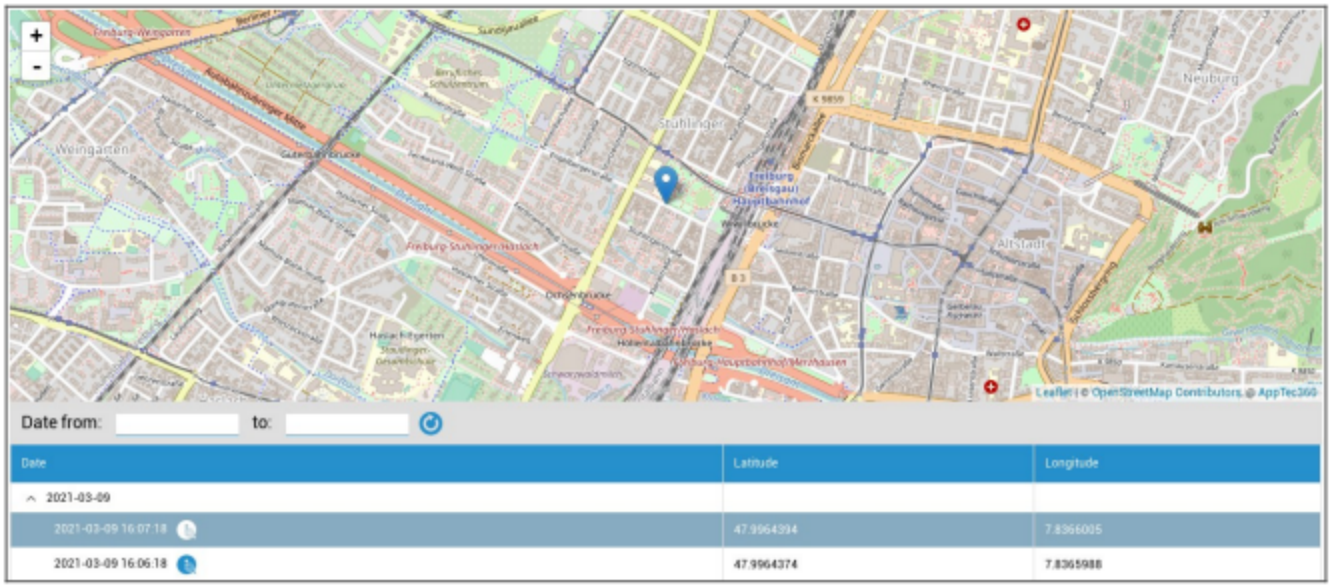
Bluetooth MAC	Bluetooth MAC-adres

Beveiligingsbeheer

Anti diefstal (alleen op apparaatniveau)

GPS-informatie (alleen op apparaatniveau)

Hier kun je de huidige/laatste locatie van het apparaat bepalen. De lokalisatie kan worden beveiligd met een of zelfs twee wachtwoorden - Zie: Algemene instellingen - Privacy - GPS-toegang



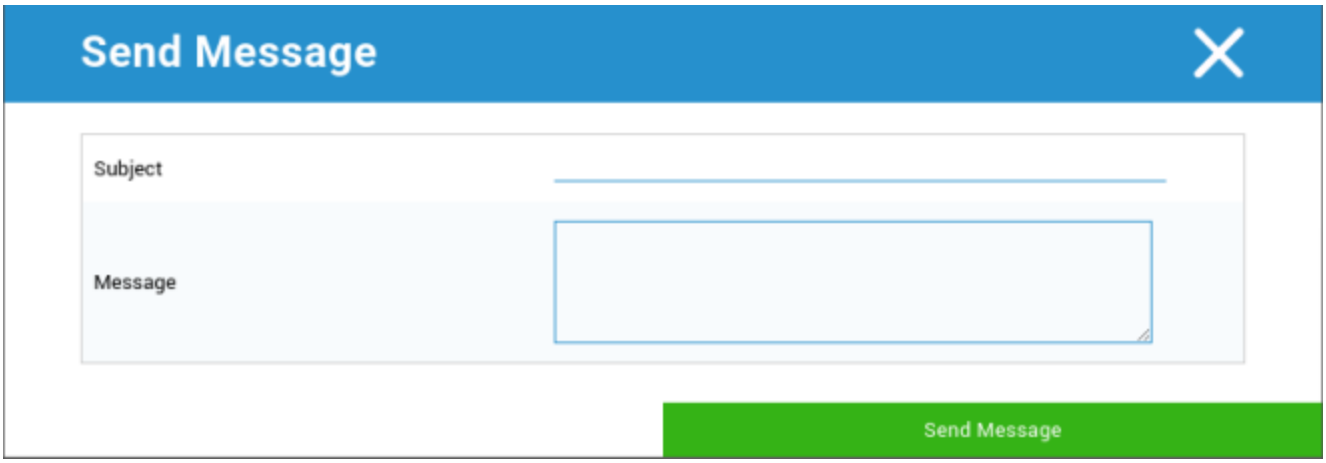
Vegen en vergrendelen (alleen op apparaatniveau)

Onder "Wissen & vergrendelen" kun je de volgende drie acties uitvoeren:

Volledig wissen	Het apparaat wordt teruggezet naar de fabrieksinstellingen (zowel bedrijfs- als persoonlijke gegevens worden gewist). Werkt alleen voor uitgebreid werkprofiel
Ondernemingsvegen	Alleen bedrijfsgegevens worden verwijderd van het apparaat van de eindgebruiker (alle apps, gegevens, enz. die werden geleverd door AppTec)
Vergrendelscherm	Schermvergrendeling is geactiveerd, het is voldoende om het apparaat te ontgrendelen met het apparaatwachtwoord/PIN

Bericht (alleen op apparaatniveau)

Hier kun je het onderwerp en een bericht invullen en naar een eindgebruiker sturen



Beveiligingsconfiguratie

Toestelwachtwoord

Onder "Passcode" kunt u een wachtwoord voor het apparaat instellen, de volgende opties zijn beschikbaar

Minimale lengte wachtwoord	Bepaalt het minimum aantal symbolen dat een wachtwoord moet hebben	
Wachtwoord kwaliteit	Ongespecificeerd	Dit beleid stelt geen eisen aan het wachtwoord.
	Biometrisch zwak	Dit beleid staat laagbeveiligde biometrische herkenningstechnologie toe. Dit houdt technologieën in die de identiteit van een individu kunnen herkennen tot ongeveer een PIN-code van 3 cijfers (valse detectie is minder dan 1 op 1.000).
	Iets	Dit beleid vereist dat er een wachtwoord of patroon wordt ingesteld, maar dwingt geen specifieke regels af.
	Alfabetisch	De gebruiker moet een wachtwoord hebben ingevoerd dat ten minste alfabetische tekens (of andere symbolen) bevat.
	Alfanumeriek	De gebruiker moet een wachtwoord hebben ingevoerd dat zowel numerieke als alfabetische tekens (of andere symbolen) bevat.
	Complex	De gebruiker moet een wachtwoord hebben ingevoerd dat standaard ten minste een letter, een cijfer en een speciaal symbool bevat. Met deze wachtwoordkwaliteit kunnen wachtwoorden worden beperkt tot verschillende sets tekens, zoals ten minste een hoofdletter, enz.
Minimale lengte wachtwoord	Stel het vereiste aantal tekens in voor het wachtwoord. Je kunt bijvoorbeeld eisen dat PIN-codes of wachtwoorden minstens zes tekens bevatten.	
Minimaal aantal cijfers vereist in wachtwoord	Minimaal aantal cijfers vereist in wachtwoord	
Minimaal aantal kleine letters vereist in wachtwoord	Minimaal aantal kleine letters vereist in wachtwoord	

Minimaal hoofdletters vereist in wachtwoord	Minimaal hoofdletters vereist in wachtwoord
Minimaal aantal niet-lettertekens vereist in wachtwoord	Minimaal aantal niet-lettertekens vereist in wachtwoord
Minimaal vereiste symbolen in wachtwoord	Minimaal vereiste symbolen in wachtwoord

Vergrendeling maximale inactiviteitstijd	Maximale inactiviteit gebruiker tot tijdslot
Time-out verlopen wachtwoord	Wordt ingesteld, na welk tijdsinterval het wachtwoord verloopt en een nieuw wachtwoord moet worden ingesteld
Beperking wachtwoordgeschiedenis	Aantal eerder gebruikte wachtwoorden die niet zijn toegestaan
Maximaal aantal mislukte wachtwoordpogingen	Bepaalt hoe vaak een wachtwoord verkeerd kan worden ingevoerd voordat het apparaat volledig wordt gewist.
Biometrische verificatie toestaan	Maakt verificatie via vingerafdruk of irisscan mogelijk. Alleen voor Samsung KNOX 2.1 en hoger

Container Wachtwoord

Onder "Passcode" kunt u een wachtwoord voor de container instellen, de volgende instellingsopties zijn
beschikbaar voor u

Minimale lengte wachtwoord	Bepaalt het minimum aantal symbolen dat een wachtwoord moet hebben	
Wachtwoord kwaliteit	Ongespecificeerd	Dit beleid stelt geen eisen aan het wachtwoord.
	Biometrisch zwak	Dit beleid staat laagbeveiligde biometrische herkenningstechnologie toe. Dit houdt technologieën in die de identiteit van een individu kunnen herkennen tot ongeveer een PIN-code van 3 cijfers (valse detectie is minder dan 1 op 1.000).
	Iets	Dit beleid vereist dat er een wachtwoord of patroon wordt ingesteld, maar dwingt geen specifieke regels af.
	Alfabetisch	De gebruiker moet een wachtwoord hebben ingevoerd dat ten minste alfabetische tekens (of andere symbolen) bevat.
	Alfanumeriek	De gebruiker moet een wachtwoord hebben ingevoerd dat zowel numerieke als alfabetische tekens (of andere symbolen) bevat.
	Complex	De gebruiker moet een wachtwoord hebben ingevoerd dat standaard ten minste een letter, een cijfer en een speciaal symbool bevat. Met deze wachtwoordkwaliteit kunnen wachtwoorden worden beperkt tot verschillende sets tekens, zoals ten minste een hoofdletter, enz.
Minimale lengte wachtwoord	Stel het vereiste aantal tekens in voor het wachtwoord. Je kunt bijvoorbeeld eisen dat PIN-codes of wachtwoorden minstens zes tekens bevatten.	
Minimaal aantal cijfers vereist in wachtwoord	Minimaal aantal cijfers vereist in wachtwoord	
Minimaal aantal kleine letters vereist in wachtwoord	Minimaal aantal kleine letters vereist in wachtwoord	
Minimaal hoofdletters vereist	Minimaal hoofdletters vereist in wachtwoord	

in wachtwoord	
Minimaal aantal niet-lettertekens vereist in wachtwoord	Minimaal aantal niet-lettertekens vereist in wachtwoord
Minimaal vereiste symbolen in wachtwoord	Minimaal vereiste symbolen in wachtwoord

Vergrendeling maximale inactiviteitstijd	Maximale inactiviteit gebruiker tot tijdslot
Time-out verlopen wachtwoord	Wordt ingesteld, na welk tijdsinterval het wachtwoord verloopt en een nieuw wachtwoord moet worden ingesteld
Beperking wachtwoordgeschiedenis	Aantal eerder gebruikte wachtwoorden die niet zijn toegestaan
Maximaal aantal mislukte wachtwoordpogingen	Bepaalt hoe vaak een wachtwoord verkeerd kan worden ingevoerd voordat het apparaat volledig wordt gewist.

AntiVirus

Automatisch scannen	Periodieke automatische scans inschakelen
Scaninterval	Interval voor onderzoek (Snel / Volledig)
Volledig automatisch scannen	Volledig automatische scans inschakelen
Automatische updates	Automatische updates inschakelen
Interval updatecontrole	Hoe vaak de app en de database moeten worden bijgewerkt (virussen / beschadigde code)
Bescherming van apps	Automatische app-scan inschakelen
Bescherming SD-kaart	Automatische SD-kaartscan inschakelen
Update alleen voor Wi-Fi	Als deze optie is ingeschakeld, worden updates alleen toegepast als het apparaat verbinding heeft met een Wi-Fi-netwerk.

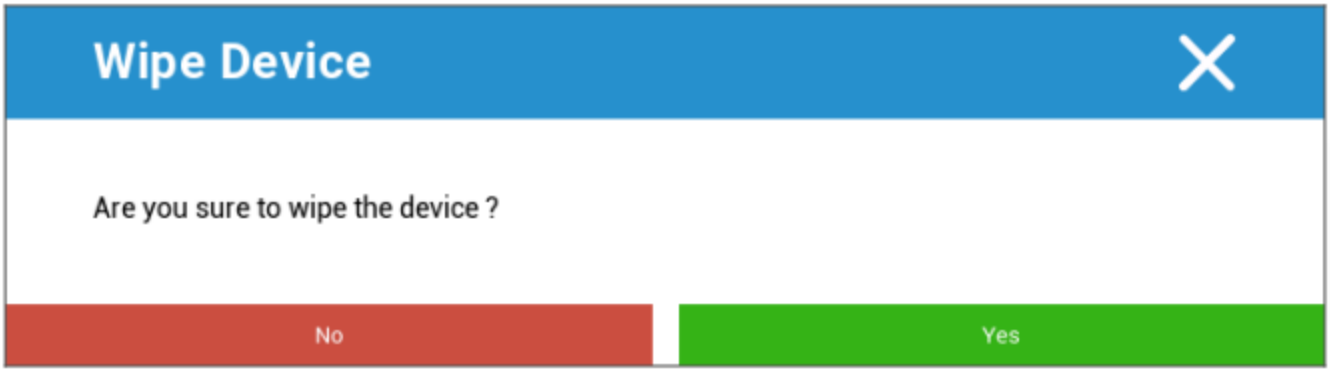
Einde levensduur (alleen op apparaatniveau)

Vegen (alleen op apparaatniveau)

Onder "Wissen" kunt u de fabrieksinstellingen van het apparaat herstellen (alleen bij uitgebreid werkprofiel).

Hier worden zowel de bedrijfsgegevens als de privégegevens verwijderd op het apparaat van de eindgebruiker.

Als je op het "Minus-symbool" klikt, krijg je het volgende bericht:



Met "Ja" kunt u het wissen uitvoeren.

Onder "Wipe Report" kunnen de volgende items worden weergegeven

Gewist door	Geschiedenis van wie het afvegen heeft uitgevoerd
Datum	Datum
Status	Status (bijv. of het wissen met succes is uitgevoerd)

Beperkende instellingen

Beperkingen

Hier kunnen verschillende dingen worden beperkt en geblokkeerd.

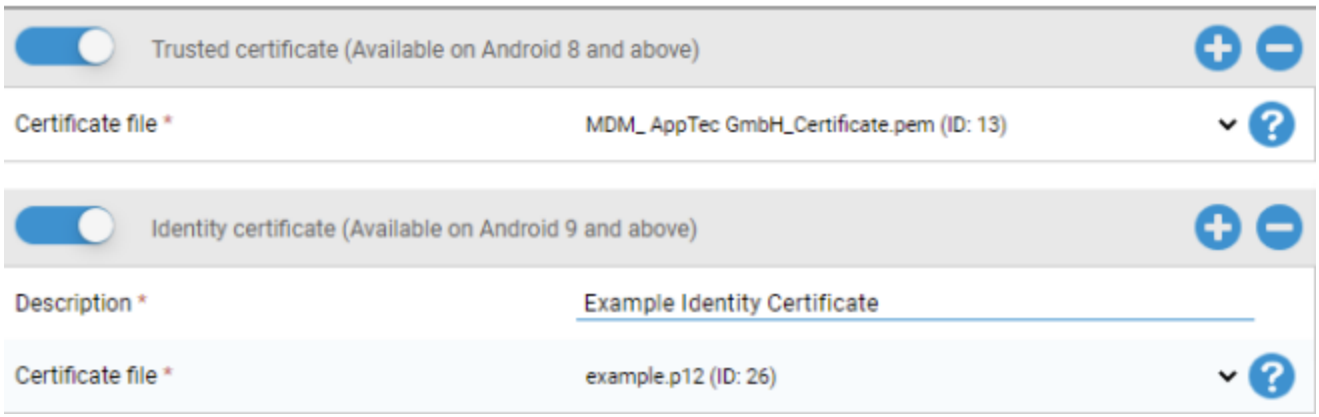
Handhaving	Mode Prompt User - Gebruiker wordt gevraagd om de nodige acties uit te voeren. Mode Lock-Down Container - Verberg alle apps totdat aan alle vereisten is voldaan
Beleid voor runtime-toestemming	Gebruiker vragen om nieuwe rechten Verleen altijd nieuwe toestemmingsaanvragen Weiger nieuwe toestemmingsaanvragen altijd Waarschuwing: Sommige apps hebben problemen met het herkennen van de machtigingen als deze automatisch worden ingesteld. Als je altijd rechten toekent en problemen ondervindt met apps die zeggen dat rechten ontbreken, stel dit dan in op "prompt user" en installeer de app opnieuw.
Uitgaand klembord toestaan	Kopiëren en plakken van binnen de container naar buiten is mogelijk
Resolutie voor beller-ID toestaan	Toont de naam voor een inkomend gesprek op basis van contacten in de container
Oplossing contact zoeken toestaan	Maakt het mogelijk om naar namen te zoeken in de containercontacten bij het bellen
Delen van Bluetooth-contacten toestaan	Biedt toegang tot containercontact in een auto
Uitgaande NFC-bundel niet toestaan	Schakelt NFC voor de container uit
Onbekende bronnen toestaan	Als dit is ingeschakeld, kunnen gebruikers apps sideloaden door een .apk-bestand te installeren.
USB-debugging toestaan	Als deze optie is ingeschakeld, kunnen gebruikers USB Debugging inschakelen.
Accountwijziging niet toestaan	Staat het aanmaken, verwijderen en wijzigen van accounts in de container niet toe Houd er rekening mee dat sommige apps accounts moeten maken of wijzigen om naar verwachting te werken

Beperkingen werkprofiel. Alleen beschikbaar op Android 11-apparaten en hoger, met uitgebreid werkprofiel	
Camera niet toestaan	Geeft aan of de camera niet is toegestaan in het werkprofiel.
Bluetooth niet toestaan	Specificeert of bluetooth niet is toegestaan in het werkprofiel.
Bescherming tegen fabrieksreset inschakelen	Activeer dit om de beveiliging tegen fabrieksresetten van Android op te heffen naar de Google-account die u hebt gedefinieerd in "Algemene instellingen" → "Android-configuratie" → "Android Enterprise" → "Bescherming tegen fabrieksresetten" Als dit is ingeschakeld en u reset het apparaat, moet u de geconfigureerde Google-account opgeven om het apparaat opnieuw in te stellen.
Controle OS-update	Schakel dit in om het updategedrag in te stellen op automatisch, windowed of uitgesteld.
Beleid bijwerken	Automatisch: Installeer automatisch zodra er een update beschikbaar is. Venster: Installeer automatisch binnen een dagelijks onderhoudsvenster. Hiermee worden ook Play-apps geconfigureerd om binnen het venster te worden bijgewerkt. Dit wordt sterk aanbevolen voor kiosktoestellen omdat dit de enige manier is waarop apps die permanent op de voorgrond zijn vastgepind, kunnen worden bijgewerkt door Play. Uitstellen: Stel automatische installatie uit tot maximaal 30 dagen.

Beperkingen persoonlijk profiel. Alleen beschikbaar op Android 11-apparaten en hoger, met uitgebreid werkprofiel	
Camera niet toestaan	Geeft aan of de camera niet is toegestaan in het persoonlijke profiel.
Bluetooth niet toestaan	Specificeert of bluetooth niet is toegestaan in het persoonlijke profiel.
Onbekende bronnen toestaan	Als dit is ingeschakeld, kunnen gebruikers van werkprofielen apps sideloaden door een .apk-bestand te installeren.

Beheer van certificaten

Hier kunt u Trusted Certificates en Identity Certificates distribueren naar uw apparaten. Android 8 of hoger is vereist om Trusted Certificates te distribueren en Android 9 of hoger is vereist om Identity Certificates te distribueren.



Met de "+" kun je meerdere certificaten toevoegen.

Trusted Certificates moeten in PEM-formaat zijn.

Identiteitscertificaten moeten in PKCS12-formaat zijn.

Verbindingsbeheer

Wifi

Voer voor deze instelling de voorconfiguratie uit van de eindgebruikersapparaten voor toegang tot interne Access
Points.

Serviceset Identifier (SSID)	SSID voor het netwerk waarmee verbinding moet worden gemaakt
Verborgen netwerk	Activeren, als het AP de SSID niet uitzendt

Type beveiliging

Het beveiligingstype van het AP vaststellen

WEP

Wachtwoord	Wachtwoord voor het AP

WPA/WPA2

Wachtwoord	Wachtwoord voor het AP

802.1x EAP

EAP-Methode

PWD	Identiteit	Identiteit
	Wachtwoord	Wachtwoord

PEAP	Fase 2 Authenticatieprotocol	geen	Geen aanvullend protocol
		MSCHAPV2	MSCHAPV2-protocol
		GTC	GTC-protocol
	CA-certificaat	CA-certificaat	
	Identiteit	Identiteit	
	Anonieme identiteit	Anonieme identiteit	
	Wachtwoord	Wachtwoord	

TTLS	Fase 2 Authenticatieprotocol	geen	Geen aanvullend protocol
		PAP	PAP-protocol
		MSCHAP	MSCHAP-protocol
		MSCHAPV2	MSCHAPV2-protocol
		GTC	GTC-protocol
	CA-certificaat	CA-certificaat	
	Identiteit	Identiteit	
	Anonieme identiteit	Anonieme identiteit	
	Wachtwoord	Wachtwoord	

TLS	CA-certificaat	CA-certificaat
	Identiteit	Identiteit
	Wachtwoord	Wachtwoord

VPN

Naam verbinding	Naam van de VPN-verbinding

VPN-type

VPN

VPN-client

AppTec VPN-client	
Configuratie gateway	Selecteer de VPN-configuratie van de gateway (zie **Algemene instellingen > Universele gateway > VPN-instellingen**)
Altijd aan VPN	Native Lockdown inschakelen
AppTec Lockdown inschakelen	AppTec Lockdown inschakelen

Ingebouwd (alleen beschikbaar op Samsung-apparaten)			
Type aansluiting	PPTP	Server	Server
		PPTP-codering inschakelen	PPTP-codering inschakelen
	L2TP / IPSec PSK	Server	Server
		Vooraf gedeelde IPSec-sleutel	Vooraf gedeelde IPSec-sleutel
		L2TP-geheim inschakelen	L2TP-geheim inschakelen
		L2TP-geheim	L2TP-geheim
	IPSec XAuth PSK	Server	Server
		IPSec-identificatiecode	IPSec-identificatiecode
		Vooraf gedeelde IPSec-sleutel	Vooraf gedeelde IPSec-sleutel
DNS domeinen zoeken	DNS domeinen zoeken		
Expertinstellingen	DNS-servers	DNS-servers	
	Routes doorsturen	Routes doorsturen	

Open VPN		
Server	Server	
OpenVPN-profiel	OpenVPN-profiel	
OpenVPN-app	OpenVPN voor Android (aanbevolen)	
	OpenVPN verbinden	
Expertinstellingen	DNS-servers	DNS-servers
	Routes doorsturen	Routes doorsturen

Samsung / Sterke Zwaan			
Type aansluiting	PPTP	Server	Server
		Gebruikersnaam	Gebruikersnaam
		Wachtwoord	Wachtwoord
		PPTP-codering inschakelen	PPTP-codering inschakelen
	L2TP / IPSec PSK	Server	Server
		Vooraf gedeelde IPSec-sleutel	Vooraf gedeelde IPSec-sleutel
		Gebruikersnaam	Gebruikersnaam
		Wachtwoord	Wachtwoord
		L2TP-geheim inschakelen	L2TP-geheim
	IPSec XAuth PSK	Server	Server
		IPSec-identificatiecode	IPSec-identificatiecode
		Vooraf gedeelde IPSec-sleutel	Vooraf gedeelde IPSec-sleutel
		Gebruikersnaam	Gebruikersnaam
		Wachtwoord	Wachtwoord
Expertinstellingen	DNS-servers	DNS-servers	
	Routes doorsturen	Routes doorsturen	

Cisco elke verbinding		
Server	Server	
Certificaatmodus	Uitgeschakeld	Uitgeschakeld
	Automatisch	Automatisch
Expertinstellingen	DNS-servers	DNS-servers
	Routes doorsturen	Routes doorsturen

VPN per app

VPN-client

AppTec VPN-client		
Configuratie gateway	Selecteer de VPN-configuratie van de gateway (zie **Algemene instellingen > Universele gateway > VPN-instellingen**)	
VPN-apps	VPN-apps	
Altijd aan VPN	Native Lockdown inschakelen	Altijd aan VPN
AppTec Lockdown inschakelen	AppTec Lockdown inschakelen	

Samsung / Sterke Zwaan			
Type aansluiting	PPTP	Server	Server
		VPN-apps	VPN-apps
		Gebruikersnaam	Gebruikersnaam
		Wachtwoord	Wachtwoord
		PPTP-codering inschakelen	PPTP-codering inschakelen
	L2TP / IPSec PSK	Server	Server
		VPN-apps	VPN-apps
		Vooraf gedeelde IPSec-sleutel	Vooraf gedeelde IPSec-sleutel
		Gebruikersnaam	Gebruikersnaam
		Wachtwoord	Wachtwoord
		L2TP-geheim inschakelen	L2TP-geheim
	IPSec XAuth PSK	Server	Server
		VPN-apps	VPN-apps
		IPSec-identificatiecode	IPSec-identificatiecode
		Vooraf gedeelde IPSec-sleutel	Vooraf gedeelde IPSec-sleutel
		Gebruikersnaam	Gebruikersnaam
		Wachtwoord	Wachtwoord
Expertinstellingen	DNS-servers	DNS-servers	
	Routes doorsturen	Routes doorsturen	

Beperkingen

Hier kunt u de beperkingen instellen met betrekking tot het verbindingsbeheer

Dataroaming toestaan	Sta mobiele data toe tijdens roaming
Gegevensroaming forceren	Indien geactiveerd, wordt roaming voor mobiele data permanent geactiveerd (niet aanbevolen!) Deze instelling overschrijft de instelling "Sta dataroaming toe"!
Systeem http proxyserver gebruiken	Het gebruik van een HTTP-proxyserver, dat wordt aangeboden door de systeeminstellingen in instellingen, is afhankelijk van het verbonden netwerk (WiFi of APN).

PIM-beheer

Gmail Uitwisseling

Info: Deze Configuratie wordt toegepast op de Gmail-app. Je moet dus Gmail goedkeuren en installeren.

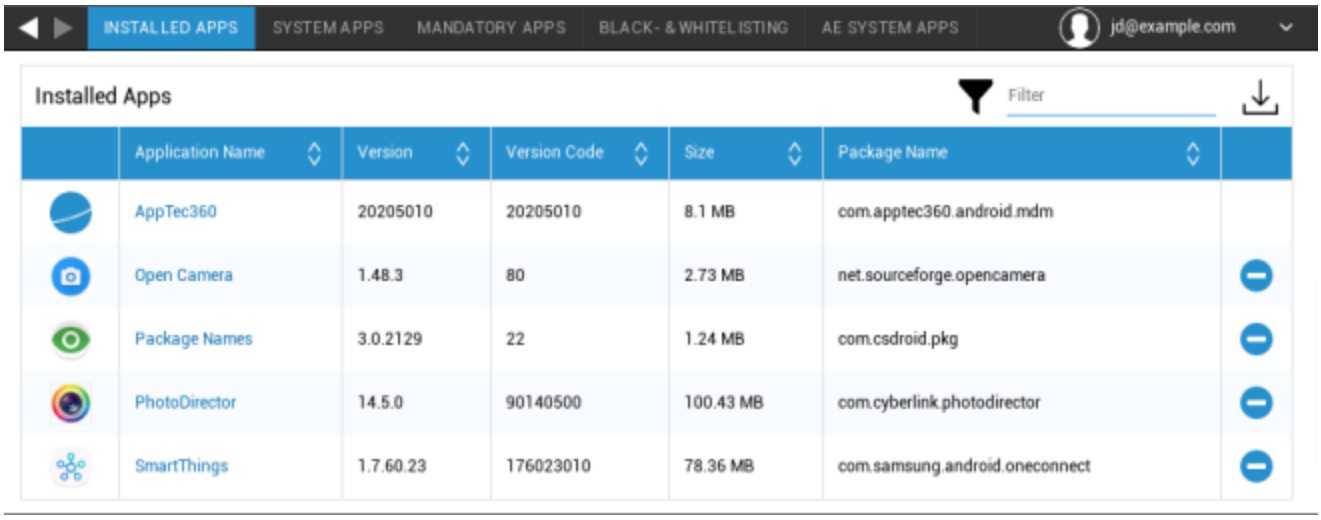
E-mailadres	Het e-mailadres van de opgegeven gebruiker Let op de "Plaatshouders", die je kunt gebruiken om met referenties te werken en die je niet handmatig op elk apparaat hoeft te wijzigen. Met een klik kun je ze zelf bekijken
Server hostnaam	Serveradres van uw Exchange-servers
Inlognaam	De aanmeldingsnaam voor het betreffende eindgebruikersapparaat, let ook op de "Placeholders here
Handtekening	Er kan een handtekening worden toegevoegd (Tip: Sommige apparaten vereisen HTML-opmaak voor de handtekening)
Aantal vorige dagen om te synchroniseren	Aantal dagen dat bepaalt wanneer e-mails worden teruggesynchroniseerd
Apparaat-ID	Een string die die EAS DeviceID bevat. Dit is een onderdeel van het EAS-protocol en wordt in verschillende omgevingen gebruikt.
Gebruik SSL (Secure Sockets Layer)	Gebruik een SSL-verbinding
Accepteer alle certificaten	Alle certificaten worden geaccepteerd. Selecteer deze optie als uw Exchange Server gebruikmaakt van een zelfondertekend certificaat.
Onbeheerde accounts toestaan	Sta gebruikers toe een ander Exchange-account toe te voegen of te verwijderen dan het account dat is opgegeven in deze beheerde configuratie. Als deze instelling is ingeschakeld, kun je niet voorkomen dat gebruikers andere Exchange-accounts toevoegen aan Gmail. Je kunt ook geen controle uitoefenen op het delen van gegevens tussen andere apps en Exchange-accounts die door gebruikers zijn toegevoegd. Deze instelling moet alleen worden ingeschakeld als je gebruikers meer dan één werkaccount van Exchange moeten onderhouden in Gmail.
Klantcertificaat	Clientcertificaat. Alleen vereist als uw mailserver verwacht dat dit aanwezig is.

App-beheer

Enterprise App Manager

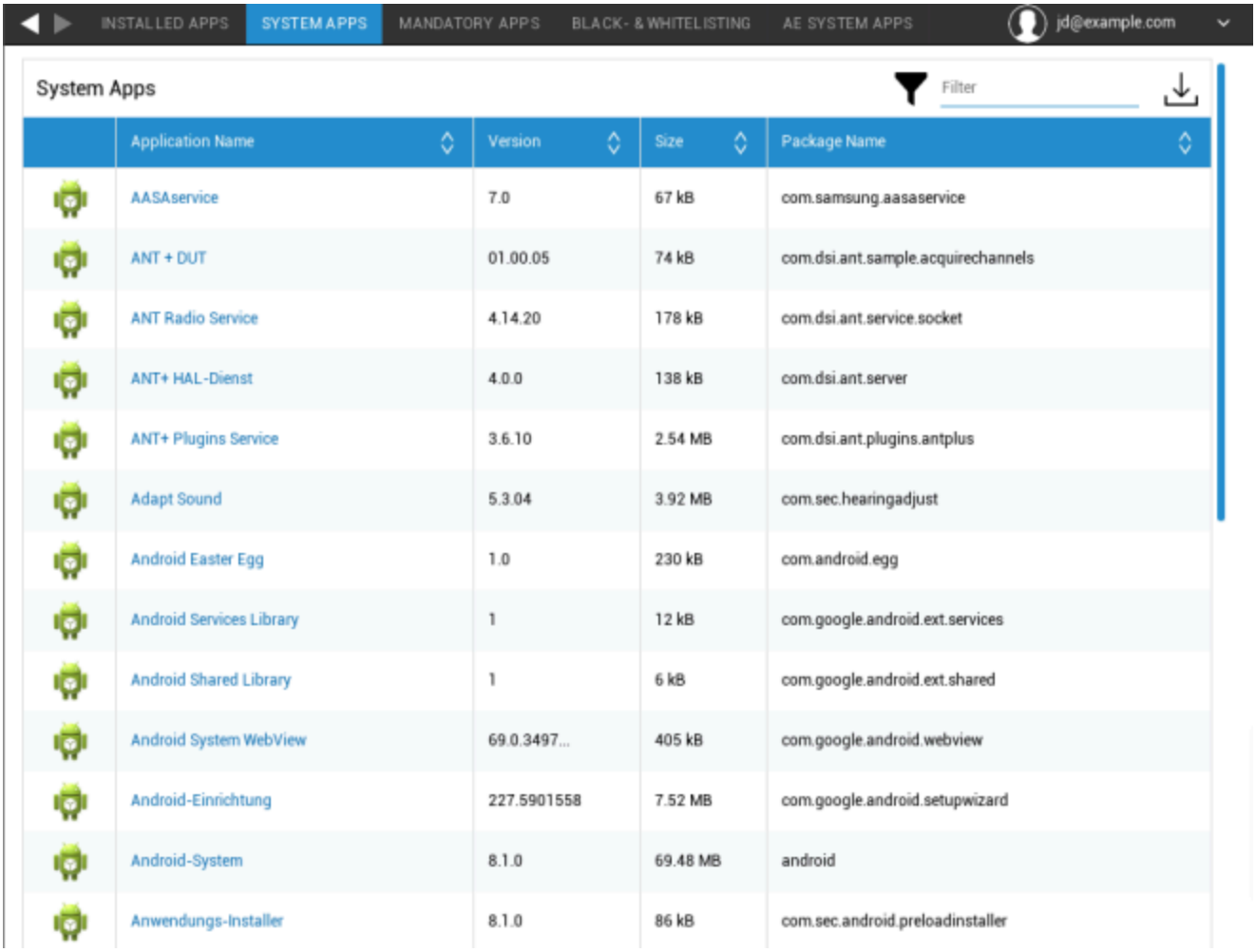
Geïnstalleerde apps (alleen op apparaatniveau)

Hier worden alle apps weergegeven die momenteel in de container zijn geïnstalleerd.



Systeemapps (alleen op apparaatniveau)

Onder "System Apps" worden alle apps en services weergegeven die al door de fabrikant van het apparaat op het eindapparaat zijn geïnstalleerd.

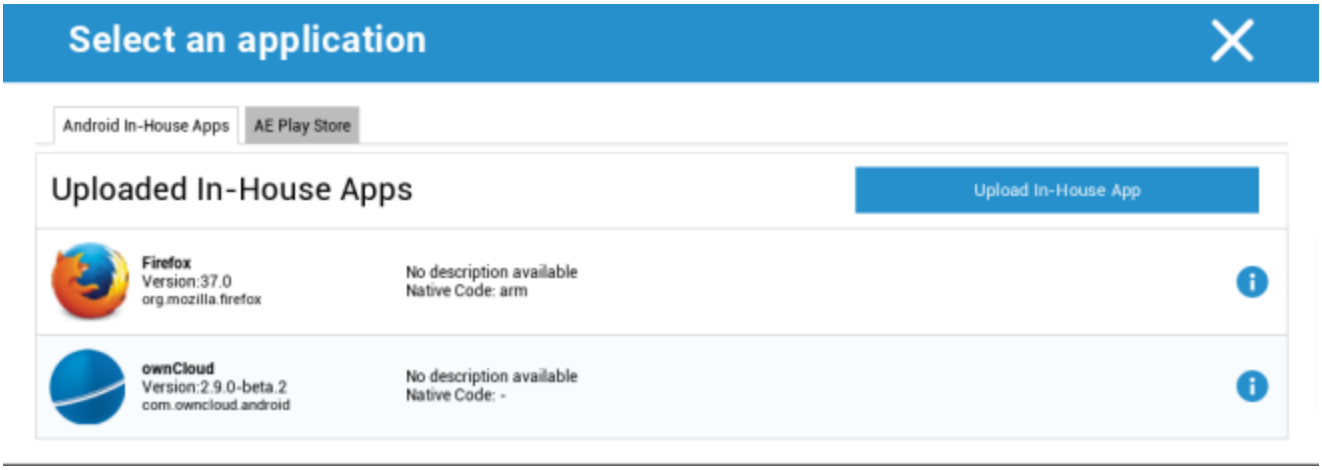


Verplichte apps

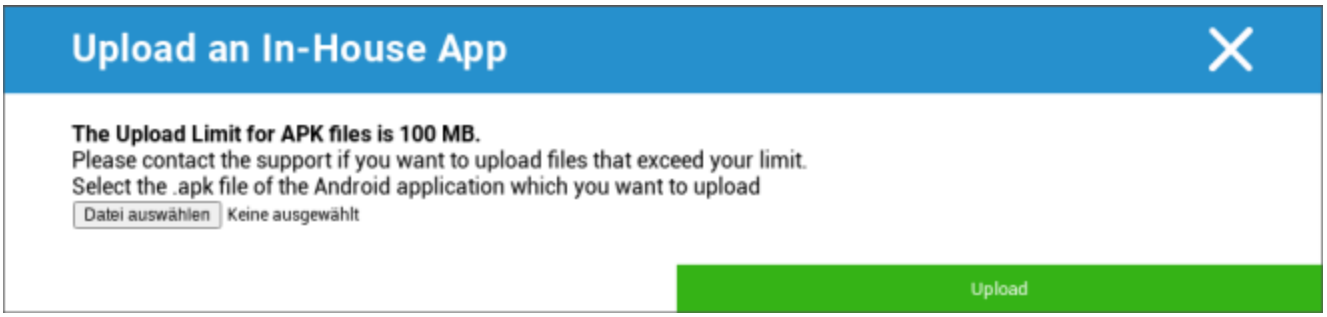
Onder de Verplichte apps kunt u de verplichte apps instellen. Als het een InHouse app is, wordt de gebruiker voortdurend gevraagd deze app te installeren. Play Store-apps worden automatisch geïnstalleerd.

Via de , kan de verplichte app worden gedefinieerd.

Dit kan een In-House App zijn uit de "Android In-House Apps", die je hebt geüpload in Algemene Instellingen.

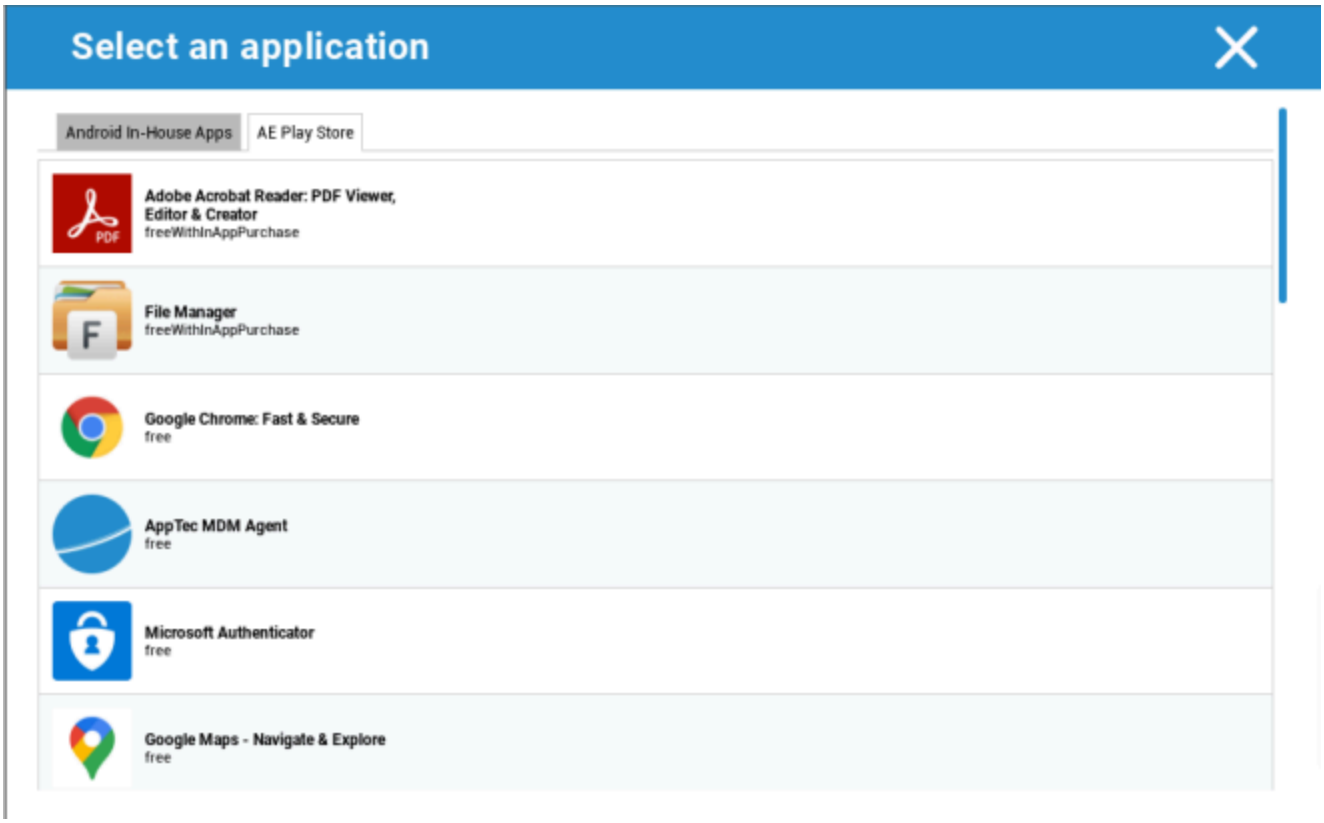


Je kunt ook direct een apk-bestand selecteren en uploaden met "Eigen app uploaden".



Als je een In-House App installeert, heb je de mogelijkheid om "Up-to-date houden" te activeren. Als dit is geactiveerd en je hebt een nieuwere versie gedefinieerd in de In-House App DB, dan wordt de app bijgewerkt op het apparaat.

Of het kan een "AE Play Store"-app zijn uit de Google Work Play Store.



Alleen goedgekeurde "AE Play Store Apps" worden op dit tabblad weergegeven.

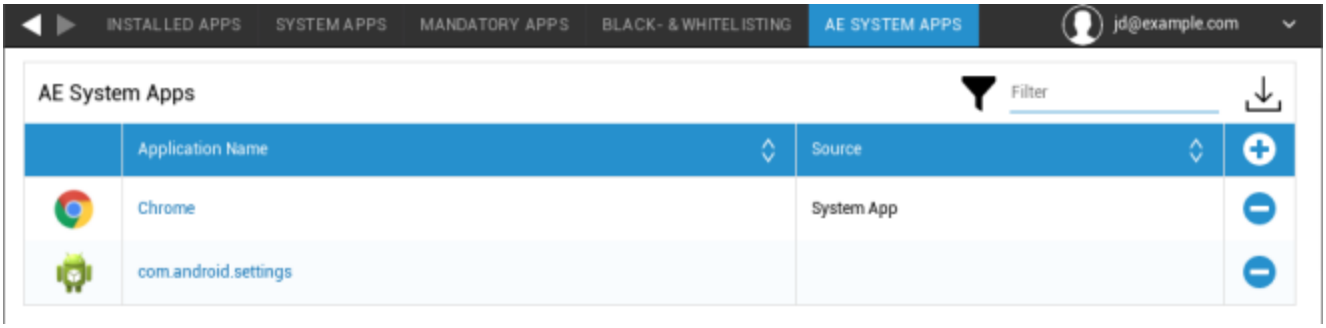
Om een "AE Play Store App" goed te keuren, gaat u naar "Algemene instellingen" > "Appbeheer" > "AE Play".

Store" en voeg een app toe via de knop die je doorverwijst naar het tabblad "Play Store Apps" (of je kunt direct naar het tabblad "Play Store Apps" gaan).

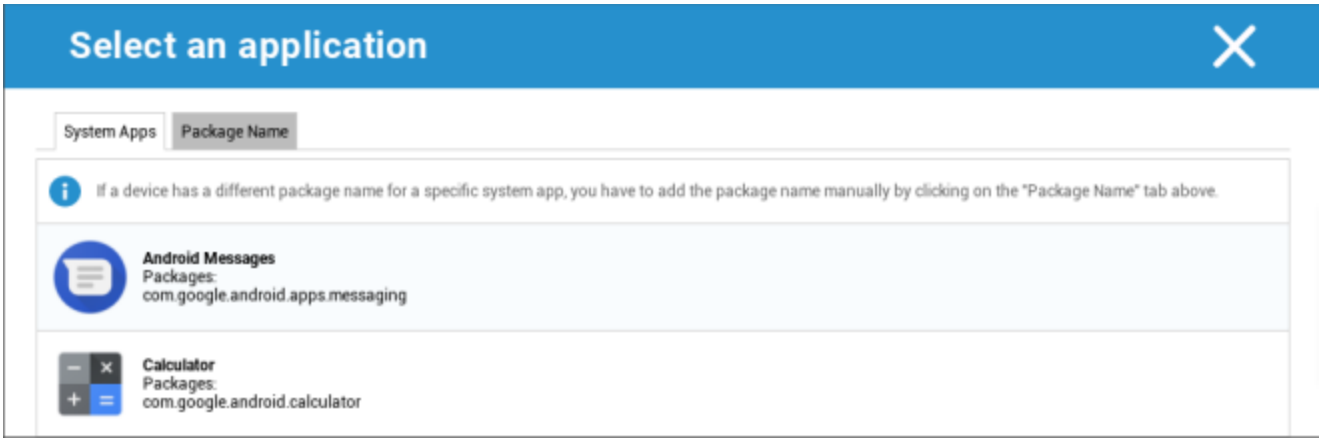
In het tabblad "Play Store Apps" kun je naar apps zoeken. Als je op een app klikt, wordt de app-pagina geopend en hier kun je de app goedkeuren door op "Goedkeuren" te klikken.

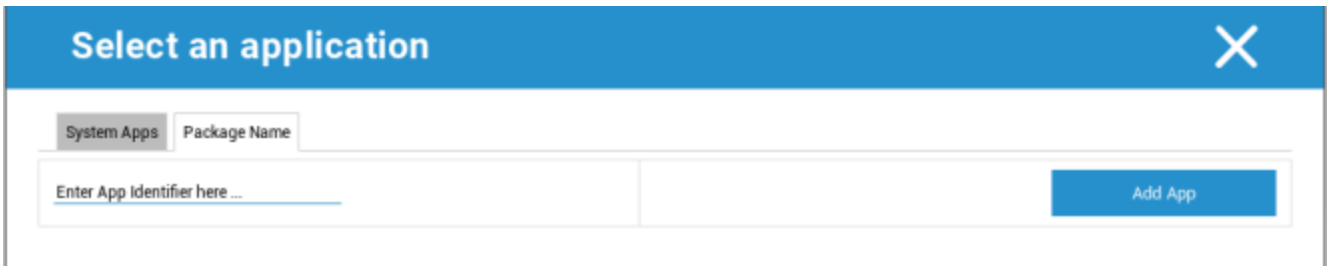
AE-systeemapps

Hier kun je een lijst definiëren met specifieke systeemapps die moeten worden geactiveerd op de apparaten.



Als je op de knop klikt, kun je kiezen uit een lijst met mogelijke systeemapps van Google of direct de pakketnaam invoeren van een systeemapp die moet worden geactiveerd.





Houd er rekening mee dat de systeem-apps in de lijst van Google alleen apps zijn die systeem-apps kunnen zijn, maar niet per se systeem-apps hoeven te zijn op je apparaten.

Deze lijst heeft echter alleen betrekking op apps die al vooraf zijn geïnstalleerd.

Het toevoegen van apps die niet vooraf op uw apparaten zijn geïnstalleerd, heeft geen invloed op uw apparaten, ongeacht of de app uit de door Google geleverde lijst komt of de pakketnaam van de app rechtstreeks wordt ingevoerd.

Beperkingen en instellingen

App Beheer Instellingen

Hier kun je het gedrag van het apparaat met betrekking tot app-updates configureren.

Controlefrequentie bijwerken	Geef aan met welk interval de AppTec Client naar app-updates moet zoeken. De standaardwaarde is 24 uur.
Wi-Fi-drempel	Apps die groter zijn dan de opgegeven grootte worden via Wi-Fi gedownload. Als "Alleen Wi-Fi" is geselecteerd, worden alle apps via Wi-Fi gedownload.

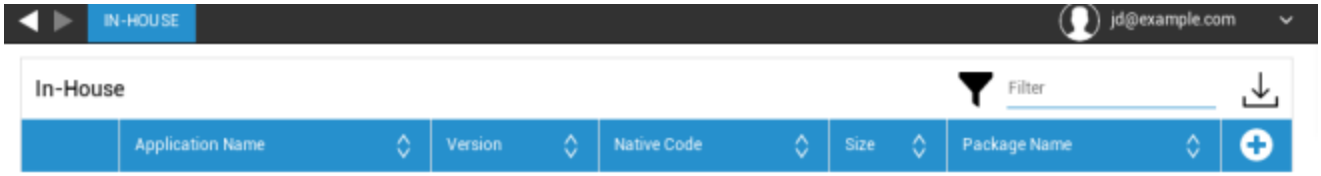
App Store voor ondernemingen

Intern

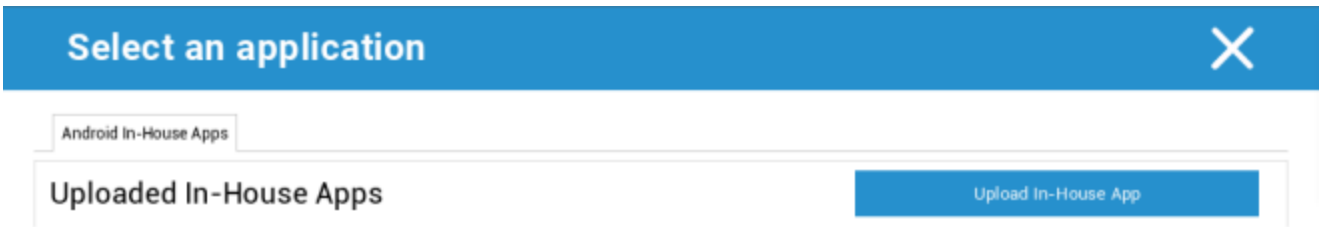
Onder het punt "In-House" kun je intern ontwikkelde apps uploaden en distribueren.

Met het symbool kun je extra In-House Apps distribueren.

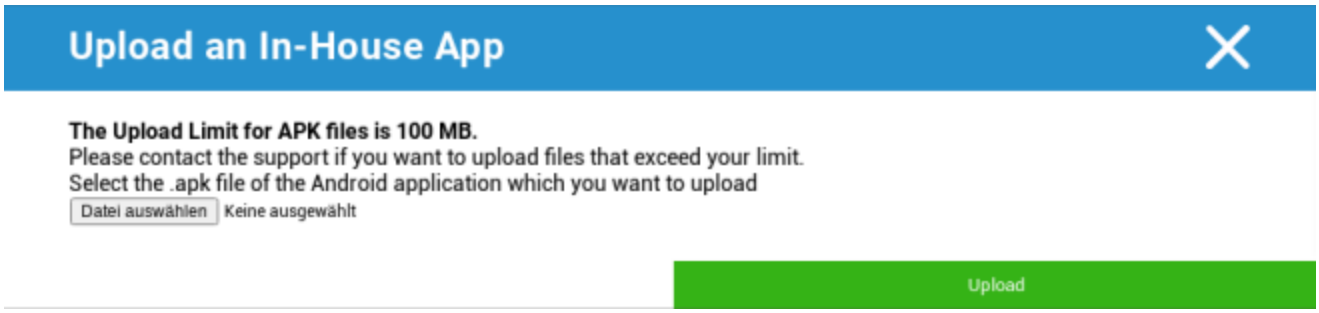
Als je een In-House App installeert, heb je de mogelijkheid om "Up-to-date houden" te activeren. Als dit is geactiveerd en je hebt een nieuwere versie gedefinieerd in de In-House App DB, dan wordt de app bijgewerkt op het apparaat.



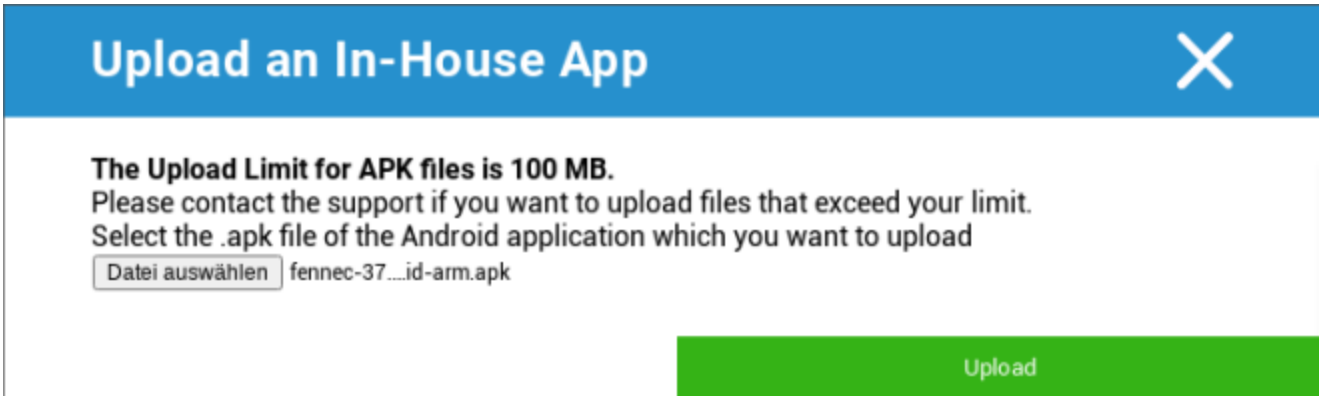
Als je geen In-House Apps hebt gedistribueerd, ontvang je het volgende overzicht:



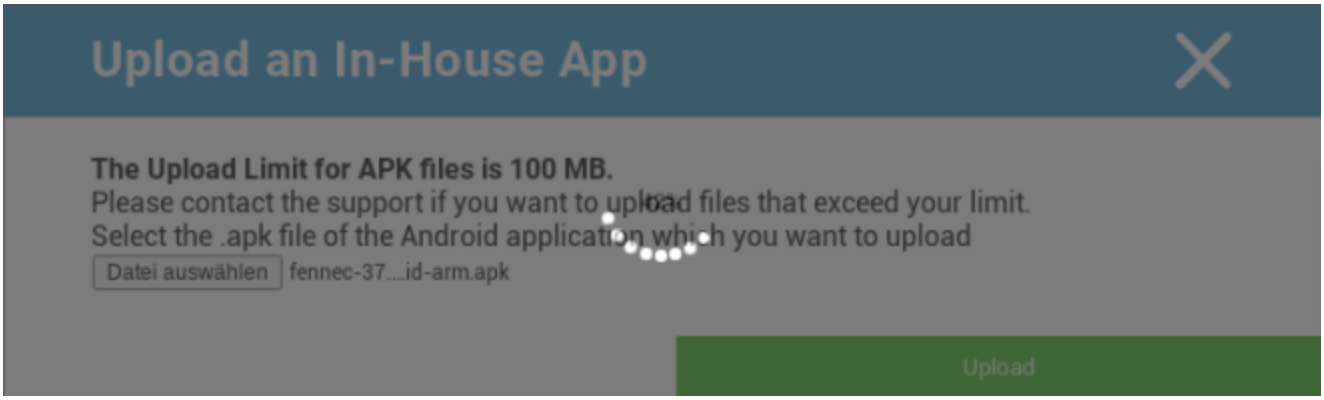
Klik hiervoor op "Upload In-House App", je krijgt dan het volgende overzicht te zien:



Kies nu met "Zoeken..." een .apk-bestand en klik vervolgens op "Uploaden".



Je app wordt nu geüpload. In het midden van de cirkel zie je een percentage-indicator die aangeeft hoeveel van je app al is geüpload.



Als het uploaden van je In-House App is gelukt, kun je de geüploade app terugvinden in je App Catalog.

De gebruiker heeft nu de mogelijkheid om deze app te bekijken en te installeren in de AppTec Store op het apparaat van de eindgebruiker, onder de categorie "In-House".

Omdat het hier niet om een Google PlayStore App gaat, heeft de gebruiker geen opgeslagen Google ID nodig op zijn eindgebruiker.

Play Store voor bedrijven

AE Play Store

Hier kunt u Apps toevoegen aan de Android Enterprise Playstore. Houd er rekening mee dat u Apps moet goedkeuren met uw AE Administrator Account voordat u ze kunt toevoegen.

Zie voor het goedkeuren van een app de instructies in Verplichte apps.

Beheer van inhoud

ContentBox

Hier kun je de ContentBox activeren.

Zodra je "Enable ContentBox" op "On" zet, wordt er automatisch een aparte ContentBox App geïnstalleerd op het apparaat van de eindgebruiker.

Veilige browser

Hier kun je instellingen configureren voor de AppTec Secure Browser.

Zodra je het onderdeel "Veilige browser" inschakelt op "Aan", wordt er automatisch een aparte Browser App geïnstalleerd op het apparaat van de eindgebruiker.

Wachtwoord nodig	Eis dat de gebruiker een wachtwoord instelt en gebruikt om toegang te krijgen tot de browser.
Minimaal vereiste wachtwoordlengte	Stel het vereiste aantal tekens in voor het wachtwoord
Vereiste wachtwoordkwaliteit	Stel de vereiste wachtwoordkwaliteit in
Beperk downloads / Open in	
Uploads beperken	
Whitelist uploaden	Een lijst met URL's waarvoor uploaden altijd wordt toegestaan.
Kopiëren toestaan	Sta het kopiëren, knippen of delen van tekst binnen de webpagina's toe.
Schermopname toestaan	Het maken van schermafbeeldingen toestaan.
Frequentie gegevensopschoning	Selecteer met welke frequentie ALLE gebruikersgegevens (geschiedenis, cache enz.) automatisch moeten worden verwijderd.
Bladwijzers voor bedrijven	De bladwijzers worden weergegeven in de map "Bedrijfsbladwijzers" in de bladwijzers van de browser. Ze kunnen niet bewerkt worden door de gebruiker.
Adresbalk verbergen	
Whitelisting in browser (zonder Universal Gateway)	Schakelt client-side URL whitelisting in. • Bladwijzers van bedrijven worden altijd gewist • Alleen ondersteund voor 100 URL's • Gebruik de Universal Gateway voor onbeperkt Black- en Whitelisting
URL's op witte lijsten	Een lijst met toegestane URL's.
Black- en whitelisting op basis van gateways	Blacklisting heeft de volgende vereisten: • Een werkende AppTec Universal Gateway ("Algemene instellingen" → "Universal Gateway")

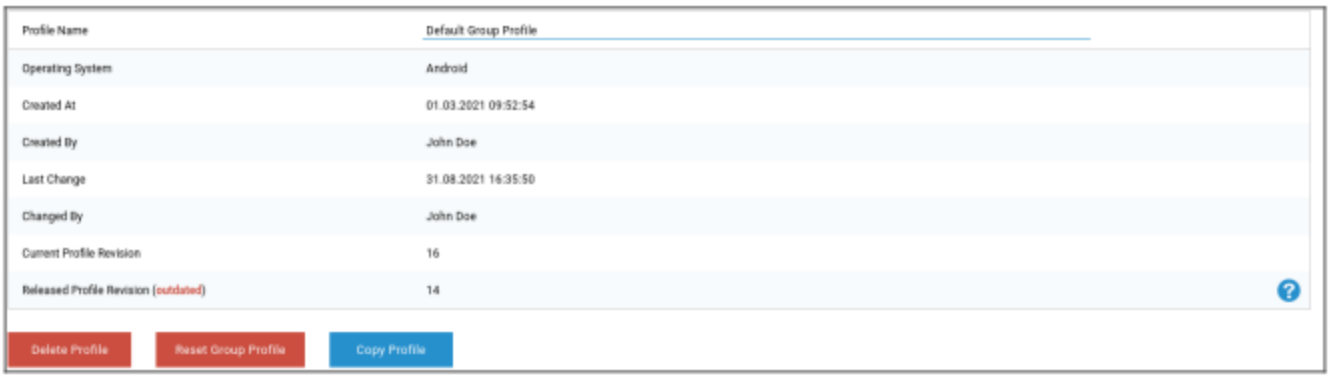
	• Een werkende VPN-configuratie met een opgegeven DNS-server ("Algemene instellingen" → "Universele gateway" → "VPN-instellingen") • Een Blacklist-configuratie ("Algemene instellingen" → "Universal Gateway" → "Domein Blacklist") • Een geldige VPN-verbinding in het profiel ("Verbindingsbeheer" → "VPN")

Android-configuratie

Algemeen

Overzicht groepsprofiel (alleen op groepsniveau)

Wanneer je een groepsprofiel opent, krijg je een snel overzicht van het profiel.



Profielnaam	Naam van het profiel (kan hier worden gewijzigd)
Besturingssysteem	Besturingssysteem waar het profiel voor is
Gemaakt op	Tijd van creatie
Gemaakt door	De maker van het profiel
Laatste wijziging	Tijdstip van laatste wijziging van het profiel
Veranderd door	Account die de laatste wijzigingen heeft aangebracht
Huidige profielherziening	Revisie van opgeslagen profielstatus
Vrijgegeven profiel Revisie	Toegewezen profielrevisie ("Nu toewijzen"). Als er "(verouderd)" achter de tekst staat, betekent dit dat je het profiel hebt opgeslagen maar nog niet hebt toegewezen, zodat de apparaten nog steeds een oudere versie krijgen.

Apparaatoverzicht (alleen op apparaatniveau)

Als u zich op een apparaat bevindt, krijgt u een overzicht van het geselecteerde apparaat, dat het volgende bevat:

Naam apparaat	Naam apparaat
Laatst bekende locatie	De laatst bekende GPS-coördinaten
Telefoonnummer	Telefoonnummer
Toegewezen verplichte apps	Het aantal toegewezen verplichte apps
OS versie	OS-versie van het apparaat
Besturingssysteem	Besturingssysteem (Android / iOS / Windows Phone)
Serienummer	Serienummer apparaat
Apparaateigendom	Zakelijk of privéapparaat
Type apparaat	Telefoon of tablet
Geworteld	Status, die aangeeft of het apparaat geroot is
Conform	Richtlijnconform
IP-adres	IP-adres
Laatst gezien	Tijdstip waarop het apparaat voor het laatst verbinding heeft gemaakt met AppTec
Laatste duw	Tijdstip waarop de server een push naar het apparaat heeft gestuurd
Gebruikerstoewijzing	Een dropdown om het apparaat aan een andere gebruiker toe te wijzen

Configuratie Revisie (alleen op apparaatniveau)

Hier krijg je een overzicht van welk groepsprofiel aan het apparaat is toegewezen.

Als je op het groepsprofiel klikt, krijg je direct toegang tot het profiel en kun je instellingen uitvoeren.

Met het symbool kun je de toegewezen apps terugzetten naar de instellingen van het groepsprofiel.

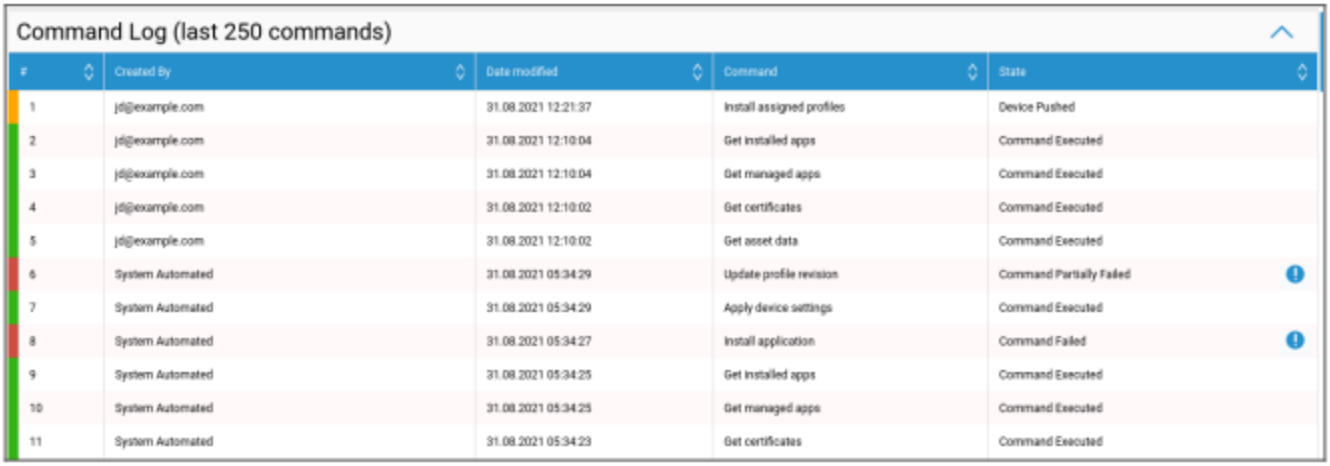
Met het symbool kun je het apparaatprofiel resetten zodat er helemaal geen instellingen zijn.

"Newer Revision available" geeft aan dat het groepsprofiel gewijzigd en opgeslagen is, maar niet toegewezen. Het groepsprofiel moet worden toegewezen met "Assign now" op groepsniveau om de wijzigingen toe te passen op de apparaten.

Apparaatlogboek (alleen op apparaatniveau)

Opdrachtlogboek

Hier kun je zien welke commando's zijn uitgegeven voor het apparaat en wat hun status is.



Commando's die zijn aangemaakt door "System Automated" worden automatisch aangemaakt door het systeem.

Mogelijke opdrachtstatussen

Apparaat ingedrukt	Er is een pushverzoek verzonden naar de pushservice (bijv. APNS) om het apparaat te vertellen terug verbinding te maken met de EMM-server.
Commando aangemaakt	De opdracht is aangemaakt in het systeem.
Opdracht verzonden	De opdracht werd naar het apparaat gestuurd nadat het verbinding had gemaakt met de server.
Opdracht uitgevoerd	De opdracht is succesvol uitgevoerd.
Opdracht mislukt	De opdracht is mislukt. *
Commando gedeeltelijk mislukt	Afhankelijk van het besturingssysteem van het apparaat kunnen sommige commando's gegroepeerd worden. Hierin zijn sommige delen van deze commandogroep mislukt. *
Opdracht uitgevoerd, uiteindelijk mislukt	Het commando werd uitgevoerd, maar misschien ook niet.
Commando verplaatst	De opdracht is opnieuw uitgevoerd door een gebruiker.
Afgedankt	De opdracht is verwijderd. Bijvoorbeeld omdat het is vervangen door een ander commando of omdat het apparaat opnieuw is aangemeld en oude commando's zijn verwijderd.

*Als er een uitroepteken achter het bericht staat, kun je meer informatie krijgen door met je cursor over het pictogram te gaan.

Apparaatinstellingen

Configuratie klant

Hier kun je de volgende configuraties uitvoeren op je Android-toestel:

Waarschuwingsbericht na uitschakelen apparaatbeheer	Opgericht waarschuwingsbericht na uitschakelen apparaatbeheer
Tijd buiten naleving	Tijdslimiet waarna "Handhavingsactie na conformiteit" wordt uitgevoerd als het apparaat niet conform is. Min. 1 minuut Max. 24 uur
Handhavingsactie na time-out voor naleving	De actie die ondernomen moet worden zodra een apparaat niet meer voldoet. • niets doen = geen actie • Lock Device = apparaat vergrendelen • Apparaat wissen = apparaat wordt teruggezet naar fabrieksinstellingen
Frequentie gegevensverzameling	Frequentie waarmee apparaat/GPS-informatie moet worden verzameld
Hartslagfrequentie apparaat	Interval waarin het apparaat contact moet maken met de AppTec360 Server Min. 1 minuut Max. 24 uur
Locatie-updates inschakelen	Indien geactiveerd, stuurt het apparaat locatie-updates naar de AppTec360 Server.
Locatie Update Tijd	Bepaalt in welke tijdsintervallen het apparaat locatie-updates naar AppTec stuurt
Gebruik Google-nauwkeurigheid voor locatie-updates	Als deze optie is geactiveerd, wordt de Google-locatienauwkeurigheid (voorheen bekend als netwerklocatie) gebruikt voor locatie-updates (als deze optie is uitgeschakeld onder "Beperkingen", heeft deze instelling geen invloed).
GPS-locatie gebruiken voor locatie-update	Indien geactiveerd, wordt de GPS gebruikt voor locatie-updates.

Neplocaties toestaan	Maakt het vervalsen van locatiegegevens via apps van derden mogelijk
Verbroken verbinding Actie	Hiermee kunt u een bepaalde actie instellen die wordt uitgevoerd nadat een bepaald aantal hartslagen is gefaald
Modus voor beleidshandhaving	Bepaalt hoe agressief de AppTec360 Client de gebruiker vraagt om bepaalde acties uit te voeren die gebruikersinvoer vereisen. Interval (standaard) = vraag in intervallen, zodat de gebruiker dit een tijdje op de achtergrond kan zetten. Geen waarschuwing = geen pop-up voor een vereiste interactie. Je moet de AppTec360 Client handmatig openen om te controleren of er een vereiste actie is. Constante waarschuwing = De gebruiker kan alleen de vereiste actie uitvoeren. De AppTec360 Client forceert zichzelf op de voorgrond als de gebruiker hem probeert te vermijden.
AppTec360 Versie Slot	Hiermee kun je een versie van de AppTec360 Client definiëren die de maximale versie is waarnaar de client zichzelf bijwerkt.

Behang

Hier kun je een aangepaste achtergrond definiëren.

Met "Geef een kleur op" kun je een kleur in hexadecimaal formaat definiëren (bijv. #000000). Alleen hexadecimale waarden zijn toegestaan.

Met "Afbeelding instellen als achtergrond" kun je een afbeelding uploaden. Houd er rekening mee dat verschillende apparaten met verschillende launchers en OS-versies anders werken. Er is geen algemene richtlijn voor grootte en verhouding, omdat dit afhangt van het apparaat.

Gebruik JPG (of JPEG) of PNG voor het bestandsformaat.

Activabeheer (alleen op apparaatniveau)

Vermogensbeheer

Apparaat info

Model	**Typeaanduiding apparaat**
Besturingssysteem	OS
OS versie	OS-versie
AE Ondersteuning	Ondersteuning voor Android Enterprise (Container en volledig beheerd)
Serienummer	Serienummer
Naam apparaat	Naam apparaat
Batterijstatus	Batterijstatus
Vrij / Totaal geheugen	Vrij / Totaal geheugen
Samsung KNOX	Samsung KNOX API-niveau
SD-kaart beschikbaar	SD-kaart beschikbaar
SD-kaart geëmuleerd	SD-kaart geëmuleerd
SD-kaart verwijderbaar	SD-kaart verwijderbaar
SD vrij / totaal geheugen	SD vrij / totaal SD-kaartgeheugen

Wi-Fi

IP-adres	IP-adres apparaat
WiFi MAC	WiFi-MAC-adres

Cellulair

Status	Status (SIM-kaart geïnstalleerd)
Telefoonnummer	Telefoonnummer
Roaming (spraak/data)	Roaming voor spraak/data
Roaming-status	Huidige roamingstatus
IP-adres	IP-adres
Exploitant/vervoerder	Exploitant/vervoerder
Cellulaire technologie	Cellulaire technologie
IMEI	IMEI-nummer
ICCID	Dit is de ID voor de SIM-kaart, vaak ook een Smartcard of Integrated Circuit Card (ICC).
IMSI	De International Mobile Subscriber Identity (IMSI) biedt in GSM- en UMTS-mobiele netwerken een definitieve identificatie van de netwerkgebruikers. De IMSI bestaat uit maximaal 15 cijfers en wordt als volgt geconfigureerd: • Mobiele landcode (MCC), 3 cijfers • Mobiele netwerkcode (MNC), 2 of 3 cijfers • Identificatienummer mobiele abonnee (MSIN), 1-10 cijfers
Huidige MCC/MNC	Zie "SIM MCC/MNC".
SIM MCC/MNC	De mobiele landcode is een vastgestelde landidentificatie die door de ITU is ingesteld volgens de E.212-norm. Deze werkt samen met de mobiele netwerkcode (MNC) voor de identificatie van het mobiele netwerk. Dit betekent de landcode/mobiele netwerkcode van de SIM-kaart. Als je naar een ander mobiel netwerk roamt, zullen de "Current MCC/MNC" en "SIM MCC/MNC" logischerwijs verschillend zijn.

Bluetooth

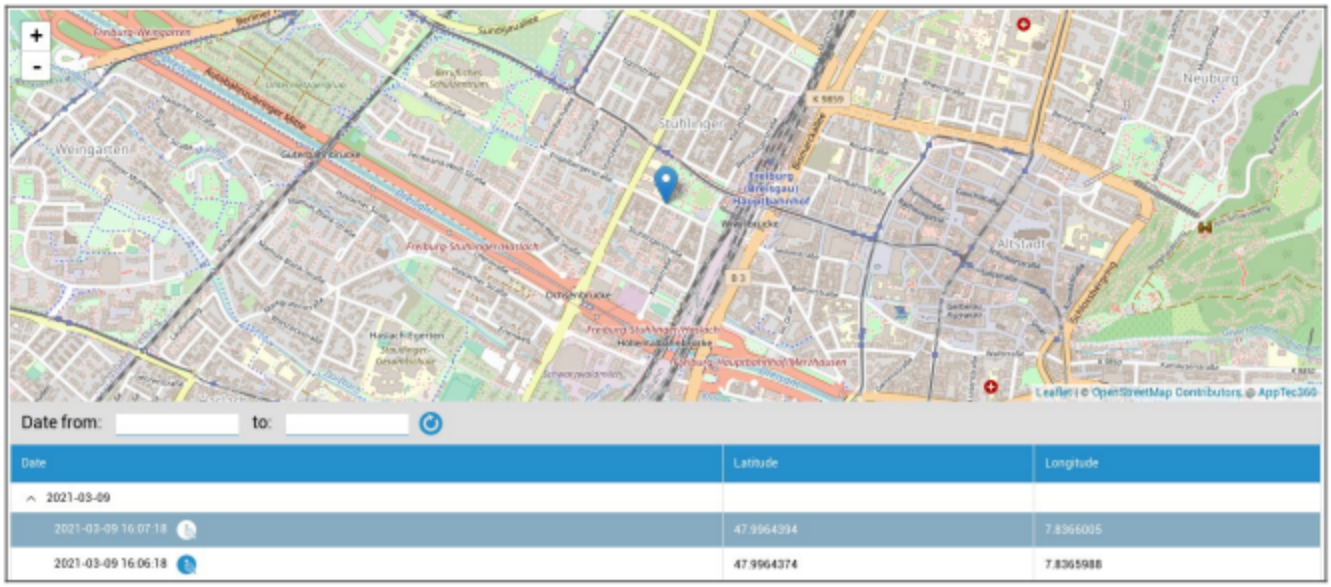
Bluetooth MAC	Bluetooth MAC-adres

Beveiligingsbeheer

Anti diefstal (alleen op apparaatniveau)

GPS-informatie (alleen op apparaatniveau)

Hier kun je de huidige/laatste locatie van het apparaat bepalen. De lokalisatie kan worden beveiligd met een of zelfs twee wachtwoorden - Zie: Algemene instellingen - Privacy - GPS-toegang



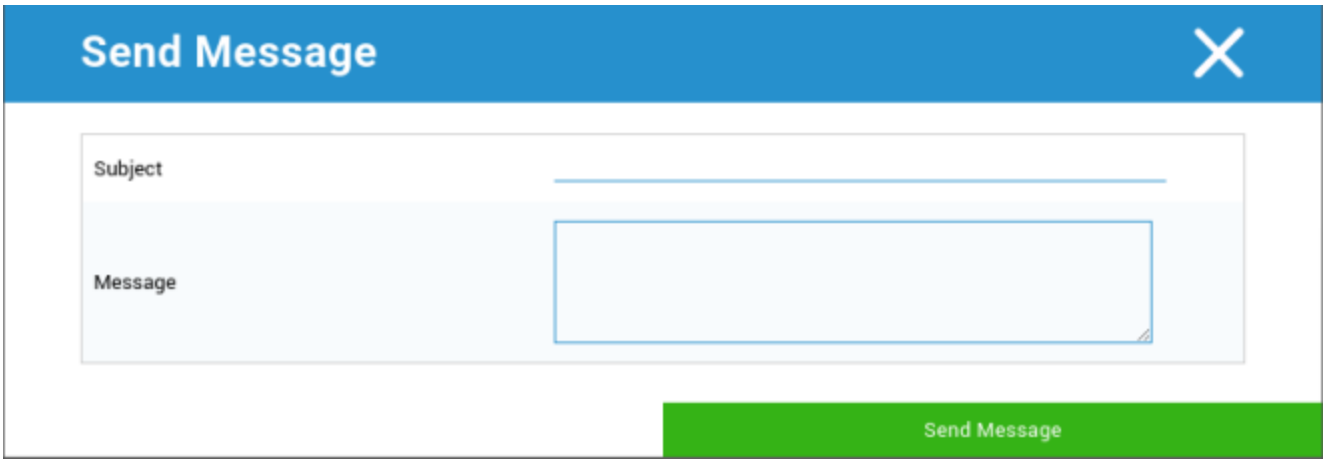
Vegen en vergrendelen (alleen op apparaatniveau)

Onder "Wissen & vergrendelen" kun je de volgende drie acties uitvoeren:

Volledig wissen	Het apparaat wordt teruggezet naar de fabrieksinstellingen (bedrijfs- en persoonlijke gegevens worden gewist)
Ondernemingsvegen	Alleen bedrijfsdata wordt verwijderd van het apparaat van de eindgebruiker (alle apps, data, etc. die zijn geleverd door AppTec360)
Vergrendelscherm	Schermvergrendeling is geactiveerd, het is voldoende om het apparaat te ontgrendelen met het apparaatwachtwoord/PIN

Bericht (alleen op apparaatniveau)

Je kunt het onderwerp en een bericht invullen en naar een eindgebruiker sturen. Dit bericht wordt weergegeven in de AppTec360 Client.



Beveiligingsconfiguratie

Wachtwoord

Onder "Passcode" kunt u een wachtwoord voor het apparaat instellen, de volgende opties zijn beschikbaar

Minimale lengte wachtwoord	Bepaalt het minimum aantal symbolen dat een wachtwoord moet hebben
Wachtwoord kwaliteit	Wachtwoordsterkte Unspecified = niet gespecificeerd Elk wachtwoord is ok = elk wachtwoord is acceptabel ten minste numerieke tekens = moet ten minste numerieke tekens bevatten minstens complexe tekens = moet minstens speciale tekens bevatten ten minste alfanumerieke tekens = moet ten minste alfanumerieke tekens bevatten ten minste alfabetische tekens = moet ten minste alfabetische tekens bevatten
Vergrendeling maximale inactiviteitstijd	Maximale time-out scherm. Dit configureert alleen de maximale waarde die door de gebruiker kan worden geselecteerd.
Minimaal aantal kleine letters vereist in wachtwoord	Minimaal aantal kleine letters vereist in wachtwoord
Minimaal hoofdletters vereist in wachtwoord	Minimaal hoofdletters vereist in wachtwoord
Minimaal aantal niet-lettertekens vereist in wachtwoord	Minimaal aantal niet-lettertekens vereist in wachtwoord
Minimaal aantal cijfers vereist in wachtwoord	Minimaal aantal cijfers vereist in wachtwoord
Minimaal vereiste symbolen in wachtwoord	Minimaal vereiste symbolen in wachtwoord
Time-out verlopen wachtwoord	Wordt ingesteld, na welk tijdsinterval het wachtwoord verloopt en een nieuw wachtwoord moet worden ingesteld
Beperking wachtwoordgeschiedenis	Aantal eerder gebruikte wachtwoorden die niet zijn toegestaan
Maximaal aantal mislukte wachtwoordpogingen	Bepaalt hoe vaak een wachtwoord verkeerd kan worden ingevoerd voordat het apparaat volledig wordt gewist.

Encryptie

Op dit punt kun je het interne apparaatgeheugen en het geheugen van de SD-kaart versleutelen.

Opslagversleuteling vereisen	Als deze instelling geactiveerd is, wordt het geheugen van het apparaat gecodeerd, zolang het apparaat deze functionaliteit ondersteunt. Zodra het geheugen van het apparaat voor de eerste keer is versleuteld, is het niet meer mogelijk om het te ontsleutelen. Het wachtwoordbeleid wordt ook automatisch omgeschakeld naar 6 alfanumerieke symbolen
SD-kaartcodering vereisen	Deze instelling is alleen van toepassing op Samsung-apparaten! Als deze instelling is geactiveerd, kan de externe SD-kaart worden gecodeerd en kan deze alleen handmatig worden gedecodeerd op het eindgebruikerapparaat. Het wachtwoordbeleid wordt ook automatisch omgeschakeld naar 6 alfanumerieke symbolen

AntiVirus

Als u AntiVirus inschakelt, wordt Ikarus op de apparaten geïnstalleerd. Houd er rekening mee dat hiervoor een aparte licentie nodig is die kan worden ingevoerd in Algemene instellingen → Appbeheer → Apps van derden.

Automatisch scannen	Definieert of Ikarus al dan niet automatisch scant en hoe vaak het deze scan uitvoert. Als je "Volledig automatisch scannen" inschakelt, wordt een volledige scan uitgevoerd. Anders wordt een snelle scan uitgevoerd
Automatische updates	Schakelt automatische updates van de virusdatabase in en stelt in hoe vaak dit gebeurt
Bescherming van apps	Schakelt het scannen van apps in naast het gewone scannen, dat alleen bestanden scant.
Bescherming SD-kaart	Schakelt SD-kaartbeveiliging in. Zonder dit is de scan beperkt tot de lokale opslag.
Update alleen voor Wi-Fi	Beperkt update tot Wi-Fi

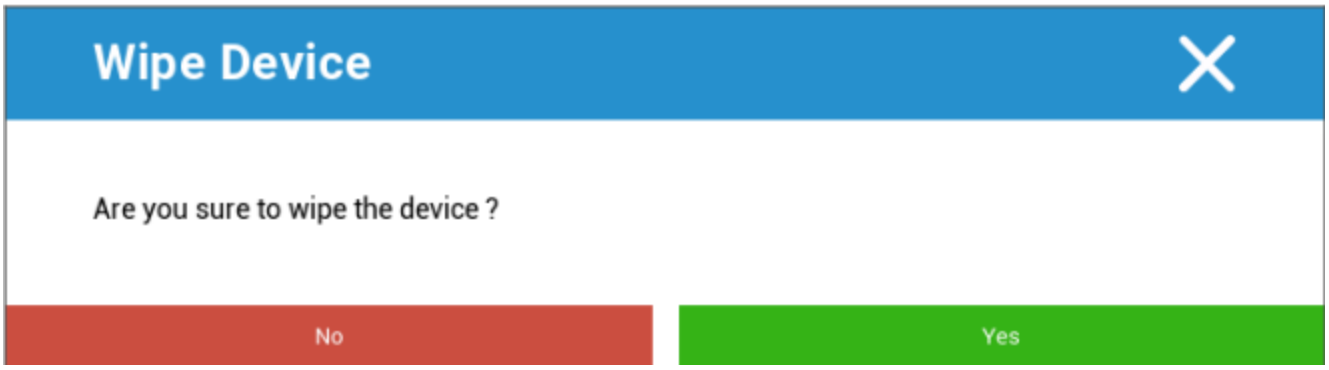
Einde levensduur (alleen op apparaatniveau)

Vegen (alleen op apparaatniveau)

Onder "Wissen" kun je het apparaat herstellen naar de fabrieksinstellingen. Hier worden de bedrijfs- en privégegevens op het eindgebruikerapparaat gewist.

Als je op het "Minus-symbool" klikt, zou je het volgende bericht moeten krijgen

Ook SD-kaart wissen?	Het geheugen van de SD-kaart wordt ook gewist



Met "Ja" kunt u het wissen uitvoeren.

Onder "Wipe Report" kunnen de volgende items worden weergegeven

Gewist door	Geschiedenis van wie het afvegen heeft uitgevoerd
Datum	Datum
Status	Status (bijv. of het wissen met succes is uitgevoerd)

Beperkende instellingen

Beperkingen

Hier kunnen verschillende dingen worden beperkt en geblokkeerd.

Camera inschakelen	Gebruik van camera toestaan
Automatische synchronisatie forceren	Heeft betrekking op "Sync"-interface Aan = synchronisatie is permanent geactiveerd Uit = synchronisatie is permanent uitgeschakeld Keuze van de gebruiker = geselecteerd door de gebruiker
Bluetooth forceren	Aan = Bluetooth is permanent geactiveerd Uit = Bluetooth is permanent uitgeschakeld Keuze van de gebruiker = geselecteerd door de gebruiker
GPS afdwingen	Aan = GPS is permanent geactiveerd Uit = GPS is permanent uitgeschakeld Keuze van de gebruiker = geselecteerd door de gebruiker
Google Locatienauwkeurigheid afdwingen	Aan = permanente internet-lokalisatie Uit = permanente deactivering van internet-lokalisatie Keuze van de gebruiker = geselecteerd door de gebruiker

Voor Samsung-apparaten met de KNOX 1.0-interface of hoger zijn de volgende instellingsopties beschikbaar.

SD-kaart toestaan	SD-kaart toestaan
SD-kaart schrijven toestaan	Schrijven" op de SD-kaart toestaan
Schermopname toestaan	Schermopname toestaan
Klembord toestaan	Klembord toestaan
Back-up maken van instellingen en app-gegevens in Google Cloud	Uit = Google Backup uitschakelen Aan = Google Backup activeren Keuze van de gebruiker = geselecteerd door de gebruiker
USB-debugging toestaan	USB Debugging toestaan (wordt bijvoorbeeld gebruikt voor het maken van apparaatlogs (ADB))
Google Crash Rapport toestaan	Toestaan dat Google Crash Report wordt verzonden vanuit de apps
Fabrieksreset toestaan	Hiermee kan de gebruiker de fabrieksinstellingen van het apparaat herstellen
OTA-upgrade toestaan	Over-The-Air" updates toestaan
USB-hostopslag toestaan	Indien geactiveerd, kan een USB-geheugen, in de vorm van een HD of een SD-kaartlezer, worden aangesloten.
USB-mediaspeler toestaan (MTP, PTP)	USB-mediaspeler toestaan (MTP, PTP)
Microfoon toestaan	Aan = microfoon toestaan voor apps van derden Uit = microfoon blokkeren voor apps van derden Keuze van de gebruiker = gebruikers kunnen kiezen of de app van derden toegang heeft tot de microfoon
NFC (Near Field Communication) toestaan	NFC toestaan
Onbekende bronnen toestaan (APK Sideloading)	Als deze optie is ingeschakeld, is side-loading van apps (APK-bestanden) toegestaan. Zodra deze instelling is uitgeschakeld, moet de gebruiker deze handmatig inschakelen wanneer je de installatie van APK's van onbekende bronnen opnieuw toestaat.
Gebruiker aanmaken toestaan	Meerdere gebruikers aanmaken

AE Apparaateigenaar

(Apparaat moet in Android Enterprise Device Owner Mode staan) Het wordt aanbevolen om de apparaten aan te maken als "Android Enterprise"-apparaat en niet als "Android"-apparaat.

Beveiliging	
Locatie delen niet toestaan	Geeft aan of een gebruiker geen locatie mag delen.
Veilig opstarten niet toestaan	Geeft aan of de gebruiker het apparaat niet in veilige opstartmodus mag herstarten.
Reset netwerk niet toestaan	Geeft aan of een gebruiker de netwerkinstellingen niet mag resetten vanuit Instellingen.
Fabrieksreset weigeren	Geeft aan of een gebruiker het apparaat niet mag resetten.
ADB inschakelen	Maakt verbinding met een pc mogelijk via ADB
Toetsenbord uitschakelen	Schakelt het Toetsenbord uit
Apparaateigenaar Info over vergrendelscherm	Stelt in welke informatie over de eigenaar van het apparaat wordt weergegeven op het vergrendelscherm.
Handhaving	Mode Prompt User - Gebruiker wordt gevraagd om de nodige acties uit te voeren. Mode Lock-Down Container - Verberg alle apps totdat aan alle vereisten is voldaan

App-beheer	
Koppeling tussen profiel-apps toestaan	Hiermee kunnen apps in het bovenliggende profiel weblinks afhandelen vanuit het beheerde profiel.
App-bediening weigeren	Geeft aan of een gebruiker applicaties niet mag wijzigen in Instellingen of launchers.
Installatie van app weigeren	Geeft aan of een gebruiker geen applicaties mag installeren.
Apps niet verwijderen	Geeft aan of een gebruiker applicaties niet mag verwijderen.
Beleid voor runtime-toestemming	Specificeert hoe nieuwe toestemmingsaanvragen van apps zullen worden behandeld.
Onbekende bronnen toestaan	Als dit is ingeschakeld, kunnen gebruikers apps sideloaden door een .apk-bestand te installeren.

Connectiviteit	
Mobiel netwerk configureren niet toestaan	Geeft aan of een gebruiker geen mobiele netwerken mag configureren.
Tethering verbieden Configuratie	Geeft aan of een gebruiker geen Tethering & draagbare hotspots mag configureren.
VPN-configuratie niet toestaan	Geeft aan of een gebruiker geen VPN mag configureren.
Wifi configuratie weigeren	Geeft aan of een gebruiker geen WiFi-toegangspunten mag wijzigen.
Uitgaande NFC-bundel niet toestaan	Geeft aan of de gebruiker NFC niet mag gebruiken om gegevens van apps uit te stralen.
WiFi-configuratie vergrendelen	Deze instelling bepaalt of WiFi-configuraties die zijn gemaakt door een app voor apparaateigenaren moeten worden vergrendeld (dat wil zeggen, alleen kunnen worden bewerkt of verwijderd door de app voor apparaateigenaren, zelfs niet door de app Instellingen).
Dataroaming inschakelen	Activeert dataroaming

Bluetooth	
Bluetooth niet toestaan	Geeft aan of bluetooth niet is toegestaan op het apparaat. Vereist Android 8.0
Delen via Bluetooth niet toestaan	Geeft aan of uitgaande bluetooth-sharing niet is toegestaan op het apparaat. Vereist Android 8.0
Bluetooth-configuratie weigeren	Geeft aan of een gebruiker bluetooth niet mag configureren.

Accountbeheer	
Toevoeging beheerd profiel niet toestaan	Geeft aan of een gebruiker geen beheerde profielen mag toevoegen. Vereist Android 8.0
Gebruikers niet toestaan toe te voegen	Geeft aan of een gebruiker geen nieuwe gebruikers mag toevoegen.
Verwijderen beheerd profiel niet toestaan	Geeft aan of beheerde profielen van deze gebruiker kunnen worden verwijderd, behalve door de eigenaar van het profiel. Vereist Android 8.0
Accountwijziging niet toestaan	Geeft aan of een gebruiker geen accounts mag toevoegen of verwijderen, tenzij ze programmatisch zijn toegevoegd door Authenticator.

Telefonie	
Uitgaande gesprekken weigeren	Geeft aan dat de gebruiker geen uitgaande telefoongesprekken mag voeren.
SMS weigeren	Geeft aan dat de gebruiker geen SMS-berichten mag verzenden of ontvangen.

Systeem	
Venster maken niet toestaan	Geeft aan dat vensters naast app-vensters niet mogen worden gemaakt.
Gebruikerspictogram niet toestaan	Geeft aan of een gebruiker zijn icoon niet mag wijzigen.
Achtergrond niet toestaan	Gebruikersbeperking om het instellen van een achtergrond niet toe te staan.
Statusbalk uitschakelen	Het uitschakelen van de statusbalk blokkeert meldingen, snelle instellingen en andere schermoverlays waarmee je kunt ontsnappen aan een apparaat voor eenmalig gebruik.
Automatische tijd inschakelen	Stelt de tijd automatisch in.
Automatische tijdzone inschakelen	Stelt de tijdzone automatisch in.
Blijft aan als de stekker in het stopcontact zit	Het apparaat blijft actief als het op een voedingsbron is aangesloten.

Opslag	
App-verificatie uitschakelen	Geeft aan of een gebruiker de applicatieverificatie niet mag uitschakelen.
Mount fysieke media niet toestaan	Geeft aan of een gebruiker geen fysieke externe media mag aankoppelen.
Back-upservice inschakelen	Back-upservice beheert alle back-up- en herstelmechanismen op het apparaat. Als u dit op false zet, wordt voorkomen dat er een back-up of herstel van gegevens wordt gemaakt. Back-upservice is standaard uitgeschakeld. Android 8.0 vereist
USB-massaopslag inschakelen	Schakelt het gebruik van USB Mass Storage in.

Toetsenbord	
Autofill weigeren	Geeft aan of een gebruiker Autofill Services niet mag gebruiken. Vereist Android 8.0
Kopiëren en plakken tussen profielen verbieden	Specificeert of wat op het klembord van dit profiel wordt gekopieerd, in gerelateerde profielen kan worden geplakt.

Geluid	
Volume-aanpassing niet toestaan	Geeft aan of een gebruiker het mastervolume niet mag aanpassen.
Microfoon uitschakelen	Geeft aan of een gebruiker het microfoonvolume niet mag aanpassen.
Apparaat dempen	Apparaat dempen.

Beleid voor systeemupdates	
OS-updates beheren	Schakel dit in om het updategedrag in te stellen op automatisch, windowed of uitgesteld.

BYOD-container

Android Onderneming

Android Onderneming

Android Enterprise inschakelen	Android Enterprise (AE) inschakelen. AE wordt ondersteund vanaf Android 5.1 en hoger.
Handhaving	Mode Prompt User - Gebruiker wordt gevraagd om de nodige acties uit te voeren. Mode Lock-Down Container - Verberg alle apps totdat aan alle vereisten is voldaan
Beleid voor runtime-toestemming	Gebruiker vragen om nieuwe rechten Verleen altijd nieuwe toestemmingsaanvragen Weiger nieuwe toestemmingsaanvragen altijd Waarschuwing: Sommige apps hebben problemen met het herkennen van de machtigingen als deze automatisch worden ingesteld. Als je altijd rechten toekent en problemen ondervindt met apps die zeggen dat rechten ontbreken, stel dit dan in op "prompt user" en installeer de app opnieuw.
Uitgaand klembord toestaan	Kopiëren en plakken van binnen de container naar buiten is mogelijk
Resolutie voor beller-ID toestaan	Toont de naam voor een inkomend gesprek op basis van contacten in de container
Oplossing contact zoeken toestaan	Maakt het mogelijk om naar namen te zoeken in de containercontacten bij het bellen
Delen van Bluetooth-contacten toestaan	Biedt toegang tot containercontact in een auto
Uitgaande NFC-bundel niet toestaan	Schakelt NFC voor de container uit
Onbekende bronnen toestaan	Als dit is ingeschakeld, kunnen gebruikers apps sideloaden door een .apk-bestand te installeren.
USB-debugging toestaan	Als deze optie is ingeschakeld, kunnen gebruikers USB Debugging inschakelen.
Accountwijziging niet toestaan	Staat het aanmaken, verwijderen en wijzigen van accounts in de container niet toe

	Houd er rekening mee dat sommige apps accounts moeten maken of wijzigen om naar verwachting te werken

Gmail Uitwisseling

Hiermee kunt u Gmail configureren in de container. Houd er rekening mee dat het inschakelen van deze configuratie de app niet automatisch installeert. Je moet deze app nog steeds toevoegen als verplichte app.

E-mailadres	E-mailadres
Server hostnaam	Server hostnaam
Inlognaam	Inlognaam
Handtekening	Handtekening
Aantal vorige dagen om te synchroniseren	Aantal vorige dagen om te synchroniseren.
Apparaat-ID	EAS Identifier. Laat dit leeg als uw omgeving dit niet vereist
Gebruik SSL (Secure Sockets Layer)	Schakelt het gebruik van SSL in. Als u dit uitschakelt, kan de beveiliging afnemen
Accepteer alle certificaten	Accepteert alle certificaten. Als u dit inschakelt, kan dit de beveiliging verlagen
Onbeheerde accounts toestaan	Hiermee kan de gebruiker extra accounts toevoegen
Klantcertificaat	Clientcertificaat uploaden als uw Exchange-server dit vereist

AE-systeemapps

Hier kun je System Apps inschakelen voor de Android Enterprise Container. Houd er rekening mee dat de gespecificeerde app in de opslag van het systeem moet staan, anders gebeurt er niets.

Container Wachtwoord

Alleen voor Android 7.0 of hoger

Hiermee kunt u een specifiek wachtwoord instellen voor de container.

Minimale lengte wachtwoord	Bepaalt het minimum aantal symbolen dat een wachtwoord moet hebben
Wachtwoord kwaliteit	Wachtwoordsterkte Unspecified = niet gespecificeerd Elk wachtwoord is ok = elk wachtwoord is acceptabel ten minste numerieke tekens = moet ten minste numerieke tekens bevatten minstens complexe tekens = moet minstens speciale tekens bevatten ten minste alfanumerieke tekens = moet ten minste alfanumerieke tekens bevatten ten minste alfabetische tekens = moet ten minste alfabetische tekens bevatten
Vergrendeling maximale inactiviteitstijd	Maximale tijd tot de container wordt vergrendeld. Dit configureert alleen de maximale waarde die door de gebruiker kan worden geselecteerd.
Minimaal aantal kleine letters vereist in wachtwoord	Minimaal aantal kleine letters vereist in wachtwoord
Minimaal hoofdletters vereist in wachtwoord	Minimaal hoofdletters vereist in wachtwoord
Minimaal aantal niet-lettertekens vereist in wachtwoord	Minimaal aantal niet-lettertekens vereist in wachtwoord
Minimaal aantal cijfers vereist in wachtwoord	Minimaal aantal cijfers vereist in wachtwoord
Minimaal vereiste symbolen in wachtwoord	Minimaal vereiste symbolen in wachtwoord
Time-out verlopen wachtwoord	Wordt ingesteld, na welk tijdsinterval het wachtwoord verloopt en een nieuw wachtwoord moet worden ingesteld
Beperking wachtwoordgeschiedenis	Aantal eerder gebruikte wachtwoorden die niet zijn toegestaan
Maximaal aantal mislukte wachtwoordpogingen	Bepaalt hoe vaak een wachtwoord verkeerd kan worden ingevoerd voordat de container wordt verwijderd

Samsung KNOX

Activering

Hier kun je de Samsung KNOX-container inschakelen. Houd er rekening mee dat deze niet langer wordt ondersteund door Samsung op Android 10 of hoger. De Android Enterprise Container gebruiken op Android 10 of hoger

Knox-toegangscode

Stel de richtlijnen op die betrekking hebben op de instellingen van het wachtwoord van het apparaat

Minimale lengte wachtwoord	Bepaalt hoeveel symbolen het wachtwoord moet hebben
Wachtwoord kwaliteit	Wachtwoordsterkte Elk wachtwoord is goed = Elk wachtwoord is goed Minimaal numerieke tekens = er moeten minimaal numerieke tekens aanwezig zijn Minimaal complexe tekens = er moeten minimaal speciale tekens aanwezig zijn Minimaal alfanumerieke tekens = er moeten minimaal alfanumerieke tekens aanwezig zijn Minimaal alfabetische tekens = er moeten minimaal alfabetische tekens aanwezig zijn
Minimaal aantal complexe tekens vereist	Er moeten minimaal complexe tekens aanwezig zijn
Maximale time-out inactiviteit	Maximale time-out voor inactiviteit van de gebruiker, voor toetsenbordvergrendeling
Vingerafdrukverificatie toestaan	Verificatie via vingerafdruk toestaan
Irisverificatie toestaan	Verificatie met irisherkenning toestaan
Maximumleeftijd wachtwoord	Bepaalt na welke tijd het wachtwoord verloopt en een nieuw wachtwoord moet worden uitgegeven
Opgeslagen wachtwoordgeschiedenis	Aantal voormalige wachtwoorden die niet zijn toegestaan
Maximaal aantal mislukte wachtwoordpogingen	Bepaalt hoe vaak het wachtwoord verkeerd mag worden ingevoerd voordat het apparaat volledig wordt gewist.

Knox Beveiliging

Beperk specifieke apparaatfunctionaliteiten

Camera inschakelen	Het gebruik van de camera toestaan

Samsung KNOX App Store toestaan	Het gebruik van de Samsung KNOX App Store toestaan
Google Play-services toestaan	Google Play-services toestaan
Browser toestaan	Het gebruik van de native browser toestaan
Screenshots toestaan	Het maken van schermafbeeldingen toestaan
Contact importeren toestaan	Indien geactiveerd, is toegang tot apparaatcontacten via de KNOX-container toegestaan.
Contactexport toestaan	Indien geactiveerd, is toegang tot KNOX-contacten vanaf het apparaat toegestaan.
Kalender importeren toestaan	Indien geactiveerd, is de toegang tot de apparaatkalender vanuit de KNOX-container toegestaan.
Kalender exporteren toestaan	Indien geactiveerd, is toegang tot de KNOX-kalender vanaf het apparaat toegestaan.
Niet-beveiligd toetsenbord toestaan	Het gebruik van een niet-beveiligd toetsenblok toestaan
Bestanden importeren inschakelen	Bestanden importeren in de KNOX-container inschakelen
Bestandsexport inschakelen	Bestandsexport van de KNOX-container inschakelen

Knox Uitwisseling

Hier kunt u het Exchange-profiel voor de KNOX-container configureren.

E-mailadres	Het e-mailadres van de opgegeven gebruiker Let op de "Plaatshouders", die je kunt gebruiken om met referenties te werken en die je niet handmatig op elk apparaat hoeft te wijzigen. Met een klik op **Toon plaatshouders** kun je ze zelf weergeven
Server hostnaam	Serveradres van uw Exchange-servers
Inlognaam	De aanmeldingsnaam voor het betreffende eindgebruikersapparaat, let ook op de "Placeholders" hier
Domein	Domeinadres
Wachtwoord (alleen op apparaatniveau)	Optioneel kan een individueel apparaat worden voorzien van een wachtwoord. Als dit leeg blijft, wordt de gebruiker gevraagd om zijn Exchange-wachtwoord in te voeren.
Aantal vorige dagen om te synchroniseren	Aantal dagen dat bepaalt wanneer e-mails worden teruggesynchroniseerd
Handtekening	Er kan een handtekening worden toegevoegd
Standaard account	Stelt vast dat dit e-mailaccount het standaardaccount is
Gebruik SSL (Secure Sockets Layer)	Gebruik een SSL-verbinding
Gebruik TLS (Transport Layer Security)	Gebruik een TLS-verbinding
Accepteer alle certificaten	Alle certificaten worden geaccepteerd. Selecteer deze optie als uw Exchange Server gebruikmaakt van een zelfondertekend certificaat.

Knox e-mail

E-mailadres	Het e-mailadres van de opgegeven gebruiker Let op de "Plaatshouders", die je kunt gebruiken om met referenties te werken en die je niet handmatig op elk apparaat hoeft te wijzigen. Met een klik op **Toon plaatshouders** kun je ze zelf weergeven
Inkomend serverprotocol	Inkomend serverprotocol IMAP of POP
Inkomend serveradres	Inkomend serveradres
Inkomende serverpoort	Inkomende serverpoort
Inlognaam/gebruikersnaam van inkomende server	Inlognaam/gebruikersnaam van inkomende server
Inkomend serverwachtwoord	Inkomend serverwachtwoord
Inkomende server gebruikt SSL	Inkomende server gebruikt SSL
Inkomende server gebruikt TLS	Inkomende server gebruikt TLS
Inkomende server accepteert alle certificaten	Inkomende server accepteert alle soorten certificaten
Uitgaand serverprotocol	Uitgaand serverprotocol SMTP
Uitgaande serverpoort	Uitgaande serverpoort
Uitgaande server gebruikt extra referenties	Extra aanmeldingsgegevens voor de uitgaande server. Als dit is ingesteld op "uit", worden de instellingen voor de inkomende server gebruikt.
Uitgaande server login/gebruikersnaam	Uitgaande server login/gebruikersnaam
Uitgaand serverwachtwoord	Uitgaand serverwachtwoord
Uitgaande server gebruikt SSL	Uitgaande server gebruikt SSL
Uitgaande server gebruikt TLS	Uitgaande server gebruikt TLS
Uitgaande server accepteert alle certificaten	Uitgaande server accepteert alle soorten certificaten
Handtekening	Hier kan een handtekening worden toegevoegd
Gebruiker op de hoogte stellen bij ontvangst van nieuwe e-mail	Gebruiker op de hoogte stellen bij ontvangst van nieuwe e-mail

Knox-apps

Stel hier apps op die u wilt distribueren naar de eindgebruikersapparaten. Deze zullen dan beschikbaar zijn in de KNOX-Container. Om een app toe te voegen, gaat u te werk zoals in het menu Verplichte apps

Naam toepassing	Naam toepassing
Verplicht Sinds	Tijdstip waarop de app werd toegevoegd
Bron	App bron (Play Store | In-house)

Door op het symbool te klikken, kan de betreffende app weer worden verwijderd.

Verbindingsbeheer

Wifi

Voer voor deze instelling de voorconfiguratie uit van de eindgebruikersapparaten voor toegang tot interne toegangspunten

Serviceset Identifier (SSID)	SSID voor het netwerk waarmee verbinding moet worden gemaakt
Verborgen netwerk	Activeren, als het AP de SSID niet uitzendt
Type beveiliging	Het beveiligingstype van het AP vaststellen

Type beveiliging

WEP

Wachtwoord	Wachtwoord voor het AP

WPA/WPA2

Wachtwoord	Wachtwoord voor het AP

802.1x EAP

EAP-Methode	

PWD	Identiteit	Identiteit

	Wachtwoord	Wachtwoord

PEAP	Fase 2 Authenticatieprotocol	geen	Geen aanvullend protocol
		MSCHAPV2	MSCHAPV2-protocol
		GTC	GTC-protocol
	CA-certificaat	CA-certificaat	
	Identiteit	Identiteit	
	Anonieme identiteit	Anonieme identiteit	
	Wachtwoord	Wachtwoord	

EAP-Methode	

TTLS	Fase 2 Authenticatieprotocol	geen	Geen aanvullend protocol
		PAP	PAP-protocol
		MSCHAP	MSCHAP-protocol
		MSCHAPV2	MSCHAPV2-protocol
		GTC	GTC-protocol
	CA-certificaat	CA-certificaat	
	Identiteit	Identiteit	
	Anonieme identiteit	Anonieme identiteit	
	Wachtwoord	Wachtwoord	

TLS	CA-certificaat	CA-certificaat
	Identiteit	Identiteit
	Wachtwoord	Wachtwoord

VPN

Type aansluiting	**Type VPN-verbinding tot stand brengen**

Als u "Per-App VPN" als VPN Type selecteert, zullen de beschikbare VPN-clients veranderen. Per-App VPN beperkt het VPN tot bepaalde apps en start de VPN-verbinding automatisch als een specifieke app wordt gestart.

AppTec360 VPN-client	Gebruikt de AppTec360 VPN Client in combinatie met de Universal Gateway
Naam verbinding	Naam VPN-verbinding
Configuratie gateway	Selecteer de VPN-configuratie van de Universal Gateway
Altijd VPN aan	Forceert dat het VPN altijd actief is, zodat al het verkeer via het VPN gaat.
Native Lockdown inschakelen	Blokkeert alle netwerken wanneer het apparaat niet verbonden is met het VPN. Gebruik dit voorzichtig omdat dit kan leiden tot een volledig verbroken verbinding als het niet goed geconfigureerd is. Alleen voor Android Enterprise op Android 7 of hoger
AppTec360 vergrendeling inschakelen	Blokkeert het gebruik van alle apps totdat de VPN-verbinding is gestart

Cisco AnyConnect	
Naam verbinding	Naam VPN-verbinding
Server	Adres server
Certificaatmodus	Uitgeschakeld = gedeactiveerd Automatisch = automatisch

L2TP (alleen KNOX)	Alleen beschikbaar op Samsung-apparaten
Naam verbinding	Naam verbinding
Server	Adres server
L2TP-geheim inschakelen	
DNS domeinen zoeken	DNS-zoekdomeinen

Type aansluiting	**Type VPN-verbinding tot stand brengen**

PPTP (alleen KNOX)	Alleen beschikbaar op Samsung-apparaten
Naam verbinding	Naam VPN-verbinding
Server	Adres server
Encryptie inschakelen	Encryptie inschakelen
DNS domeinen zoeken	DNS-zoekdomeinen

L2TP / IPSec PSK (alleen KNOX)	Alleen beschikbaar op Samsung-apparaten
Naam verbinding	Naam VPN-verbinding
Server	Adres server
Vooraf gedeelde IPSec-sleutel	Vooraf gedeelde sleutel voor verificatie
L2TP-geheim inschakelen	
L2TP-geheim	
DNS domeinen zoeken	DNS-zoekdomeinen

IPSec XAuth PSK (alleen KNOX)	Alleen beschikbaar op Samsung-apparaten
Naam verbinding	Naam VPN-verbinding
Server	Adres server
IPSec-identificatiecode	Gebruikersnaam voor de verbinding
Vooraf gedeelde IPSec-sleutel	Wachtwoord voor de verbinding
DNS domeinen zoeken	DNS-zoekdomeinen

OpenVPN	

Naam verbinding	Naam verbinding
OpenVPN-profiel	Hier is waar de inhoud van het .ovpn bestand zal worden gekopieerd
OpenVPN-app	Er zijn twee verschillende apps voor het gebruik van OpenVPN Wij raden de app "OpenVPN voor Android" aan. Maar als alternatief kan de app "OpenVPN Connect" worden gebruikt.

Beperkingen

Hier kun je de beperkingen instellen met betrekking tot het verbindingsbeheer.

Dataroaming toestaan	Sta mobiele data toe tijdens roaming
Gegevensroaming forceren	Indien geactiveerd, wordt roaming voor mobiele data permanent geactiveerd (niet aanbevolen!) Deze instelling overschrijft de instelling "Sta dataroaming toe"!
De volgende instellingen zijn alleen beschikbaar op Samsung KNOX 2.0 of hoger	
Alleen noodoproepen toestaan	Alleen noodoproepen toestaan
WiFi toestaan	WiFi toestaan
Minimumbeveiligingsniveau WiFi-netwerk	Minimumbeveiligingsniveau WiFi-netwerk Open = alle soorten WiFi zijn toegestaan
Verbied gebruiker om WiFi-netwerken toe te voegen	De gebruiker mag niet zelf een WiFi-netwerk toevoegen Deze instelling is alleen mogelijk als er een WiFi-profiel is gedefinieerd onder "Verbindingsbeheer".
SMS & MMS toestaan	Alles = alle SMS- en MMS-verkeer is toegestaan Alleen inkomende SMS = alleen inkomende SMS-berichten zijn toegestaan Alleen uitgaande SMS = alleen uitgaande SMS-berichten zijn toegestaan Geen = Geen SMS- / MMS-verkeer toegestaan
Synchronisatie toestaan tijdens roaming	Synchronisatie toestaan tijdens roaming Aan = geactiveerd Uit = gedeactiveerd Keuze van de gebruiker = keuze van de gebruiker
Spraak Roaming toestaan	Spraak Roaming toestaan Aan = geactiveerd Uit = gedeactiveerd Keuze van de gebruiker = keuze van de gebruiker
Systeem http proxyserver gebruiken	Het gebruik van een HTTP-proxyserver, dat wordt aangeboden door de systeeminstellingen in instellingen, is afhankelijk van het verbonden netwerk (WiFi of APN).

APN

De volgende instellingen zijn alleen beschikbaar op Samsung SAFE 2.0 of hoger!

APN Weergavenaam	APN Weergavenaam	
Naam toegangspunt	Naam APN	
Uitgaand serverprotocol	Niet ingesteld	
	Geen	
	PAP	PAP-protocol
	CHAP	CHAP-protocol
	PAP of CHAP	Het PAP- of CHAP-protocol
MCC - Mobiele landcode	Laat dit veld leeg als de MCC van de geplaatste SIM-kaart moet worden gebruikt.	
MNC - Mobiele netwerkcode	Laat dit veld leeg als de MCC van de geplaatste SIM-kaart moet worden gebruikt.	
Adres server	Adres server	
Poortnummer server	Poortnummer server	
Proxy-adres server	Proxy-adres server	
MMS server adres	MMS-serveradres, voor standaard leeg laten	
MMS poortnummer	MMS poortnummer	
MMS proxy-adres	MMS proxy-adres	
Gebruikersnaam	Gebruikersnaam	
Wachtwoord	Wachtwoord	
Type toegangspunt	Toegestane types zijn: "default", "mms", "supl". Als dit veld leeg blijft, wordt "default,supl,mms" gebruikt.	
Voorkeur APN	APN heeft de voorkeur	

Bluetooth

Hier kunnen verschillende Bluetooth-instellingen worden uitgevoerd.

De volgende instellingen zijn alleen beschikbaar op Samsung KNOX 1.0 of hoger!

Apparaatontdekking via Bluetooth toestaan	Apparaatontdekking via Bluetooth toestaan
Bluetooth-koppeling toestaan	Bluetooth-koppeling toestaan
Bluetooth-headsetapparaten toestaan	Bluetooth-headsetapparaten toestaan
Bluetooth-handsfree-apparaten toestaan	Bluetooth-handsfree-apparaten toestaan
Bluetooth A2DP-apparaten toestaan	Bluetooth A2DP audiostreaming tussen apparaten toestaan
Uitgaande gesprekken toestaan	Uitgaande gesprekken viaBT toestaan
Gegevensoverdracht via Bluetooth toestaan	Gegevensoverdracht via Bluetooth toestaan
Bluetooth-tethering toestaan	Hiermee kan het apparaat als modem worden gebruikt (Bluetooth-internetverbinding)
Verbinding met computer via Bluetooth toestaan	Verbinding met computer via Bluetooth toestaan

PIM-beheer

Uitwisseling

Alleen beschikbaar voor Samsung KNOX 1.0 of hoger!

E-mailadres	Het e-mailadres van de opgegeven gebruiker Let op de "Plaatshouders", die je kunt gebruiken om met referenties te werken en die je niet handmatig op elk apparaat hoeft te wijzigen. Met een klik op **Toon plaatshouders** kun je ze zelf weergeven
Server hostnaam	Serveradres van uw Exchange-servers
Inlognaam	De aanmeldingsnaam voor het betreffende eindgebruikersapparaat, let ook op de "Placeholders here
Domein	Domeinadres
Wachtwoord (alleen op apparaatniveau)	Optioneel kan een individueel apparaat worden voorzien van een wachtwoord. Als dit leeg blijft, wordt de gebruiker gevraagd om zijn Exchange-wachtwoord in te voeren.
Aantal vorige dagen om te synchroniseren	Aantal dagen dat bepaalt wanneer e-mails worden teruggesynchroniseerd
Handtekening	Er kan een handtekening worden toegevoegd (Tip: Sommige apparaten vereisen HTML-opmaak voor de handtekening)
Standaard account	Stelt vast dat dit e-mailaccount het standaardaccount is
Gebruik SSL (Secure Sockets Layer)	Gebruik een SSL-verbinding
Gebruik TLS (Transport Layer Security)	Gebruik een TLS-verbinding
Accepteer alle certificaten	Alle certificaten worden geaccepteerd. Selecteer deze optie als uw Exchange Server gebruikmaakt van een zelfondertekend certificaat.

e-mail

Hier kun je IMAP- en POP-accounts distribueren naar de respectievelijke eindgebruikersapparaten.

De volgende instellingen zijn alleen beschikbaar op Samsung KNOX 1.0 of hoger!		
E-mailadres	Het e-mailadres van de opgegeven gebruiker Let op de "Plaatshouders", die je kunt gebruiken om met referenties te werken en die je niet handmatig op elk apparaat hoeft te wijzigen. Met een klik op **Toon plaatshouders** kun je ze zelf weergeven	
Inkomend serverprotocol	Inkomend serverprotocol	IMAP of POP
Inkomend serveradres	Inkomend serveradres	
Inkomende serverpoort	Inkomende serverpoort	
Inlognaam/gebruikersnaam van inkomende server	Inlognaam/gebruikersnaam van inkomende server	
Inkomend serverwachtwoord (alleen op apparaatniveau)	Inkomend serverwachtwoord (alleen op apparaatniveau)	
Inkomende server gebruikt SSL	Inkomende server gebruikt SSL	
Inkomende server gebruikt TLS	Inkomende server gebruikt TLS	
Inkomende server accepteert alle certificaten	Inkomende server accepteert alle soorten certificaten	
Uitgaand serverprotocol	Uitgaand serverprotocol	SMTP
Uitgaande serverpoort	Uitgaande serverpoort	
Uitgaande server gebruikt extra referenties	Extra referenties voor de uitgaande server. Als dit is ingesteld op "uit", dan worden de instellingen voor de inkomende server gebruikt.	
Uitgaande server login/gebruikersnaam	Uitgaande server login/gebruikersnaam	
Uitgaand serverwachtwoord (alleen op apparaatniveau)	Uitgaand serverwachtwoord	
Uitgaande server gebruikt SSL	Uitgaande server gebruikt SSL	
Uitgaande server gebruikt TLS	Uitgaande server gebruikt TLS	

Uitgaande server accepteert alle certificaten	Uitgaande server accepteert alle soorten certificaten
Handtekening	Hier kan een handtekening worden toegevoegd (Tip: Sommige apparaten vereisen HTML-opmaak voor de handtekening)
Gebruiker op de hoogte stellen bij ontvangst van nieuwe e-mail	Stelt gebruiker op de hoogte bij ontvangst van nieuwe e-mail

AE Gmail Uitwisseling

Info: Deze Configuratie wordt toegepast op de Gmail-app. Je moet dus Gmail goedkeuren en installeren.

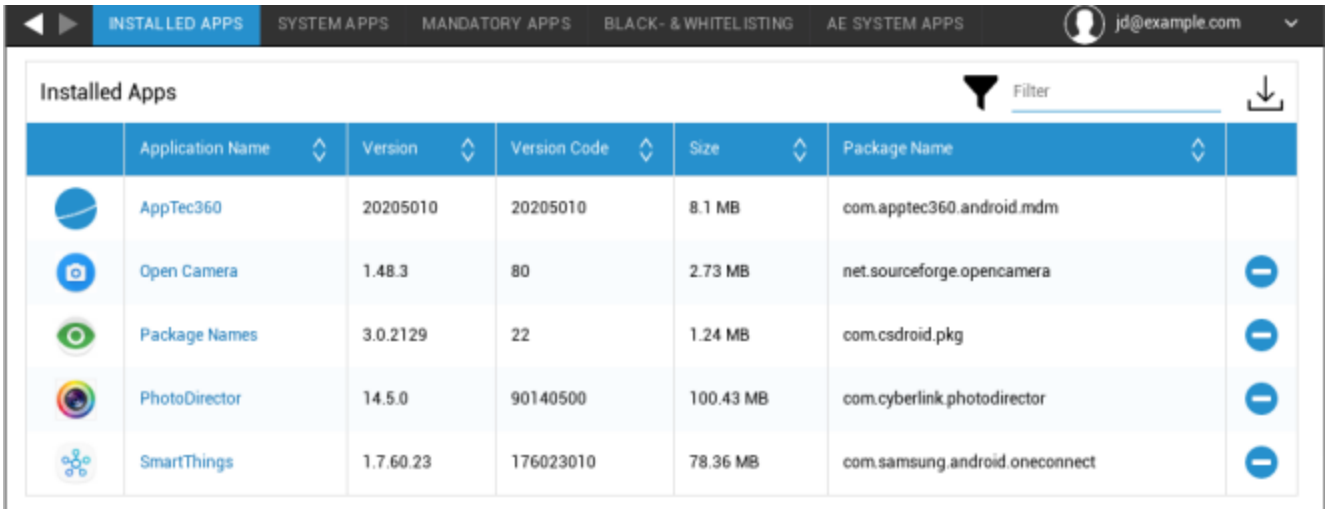
E-mailadres	Het e-mailadres van de opgegeven gebruiker Let op de "Plaatshouders", die je kunt gebruiken om met referenties te werken en die je niet handmatig op elk apparaat hoeft te wijzigen. Met een klik op Toon plaatshouders kun je ze zelf weergeven
Server hostnaam	Serveradres van uw Exchange-servers
Inlognaam	De aanmeldingsnaam voor het betreffende eindgebruikersapparaat, let ook op de "Placeholders here
Handtekening	Er kan een handtekening worden toegevoegd (Tip: Sommige apparaten vereisen HTML-opmaak voor de handtekening)
Aantal vorige dagen om te synchroniseren	Aantal dagen dat bepaalt wanneer e-mails worden teruggesynchroniseerd
Apparaat-ID	EAS Identifier. Laat dit leeg als uw omgeving dit niet vereist
Gebruik SSL (Secure Sockets Layer)	Gebruik een SSL-verbinding
Accepteer alle certificaten	Alle certificaten worden geaccepteerd. Selecteer deze optie als uw Exchange Server een zelfondertekend certificaat gebruikt.
Onbeheerde accounts toestaan	Hiermee kan de gebruiker extra accounts toevoegen
Klantcertificaat	Clientcertificaat uploaden als uw Exchange-server dit vereist

App-beheer

Enterprise App Manager

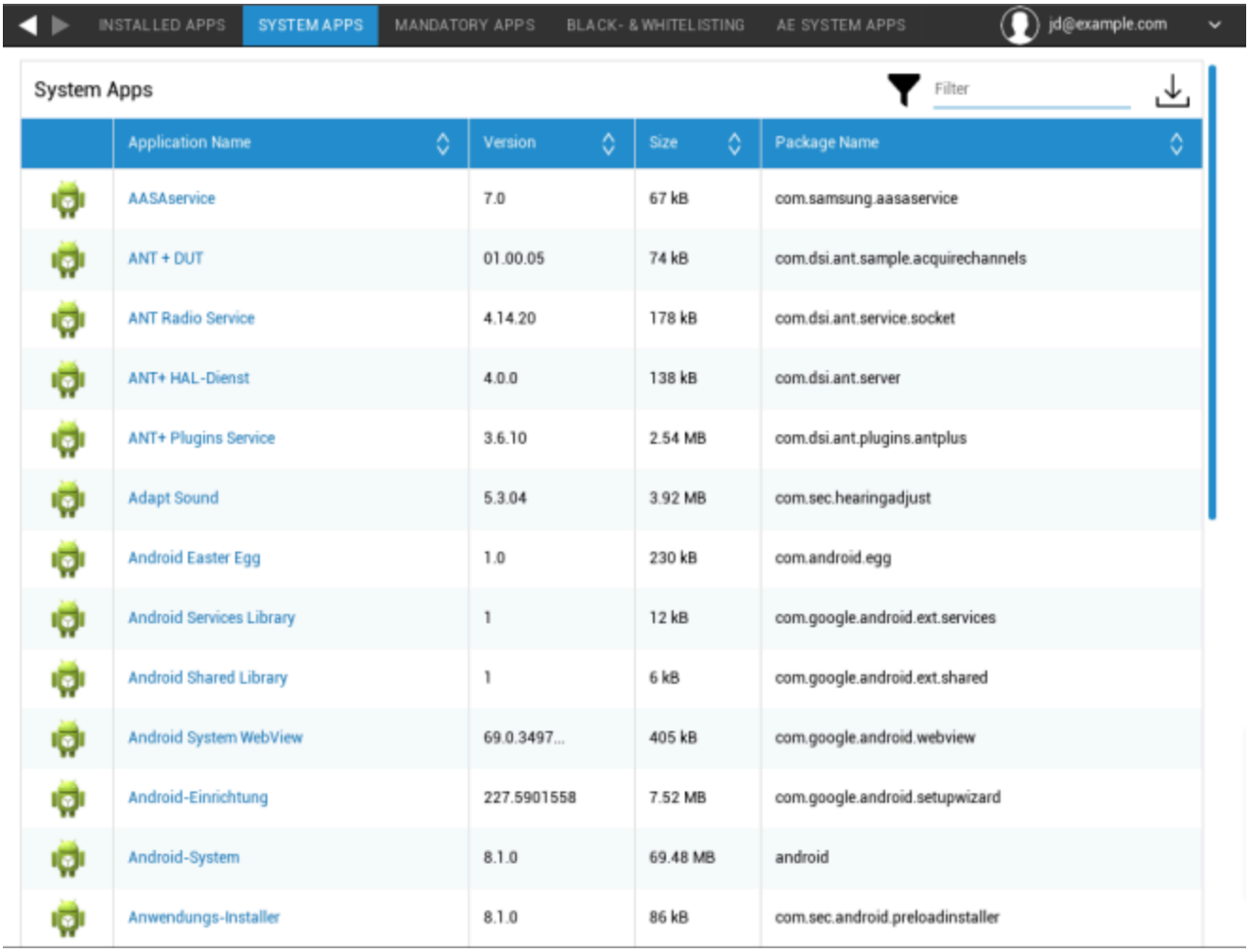
Geïnstalleerde apps (alleen op apparaatniveau)

Hier worden alle Apps weergegeven die momenteel op het eindgebruikerapparaat zijn geïnstalleerd.


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

Systeemapps (alleen op apparaatniveau)

Onder "System Apps" worden alle vooraf geïnstalleerde systemen weergegeven met hun pakketnaam en versie.



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

Verplichte apps

In Verplichte apps kun je aangeven welke apps op het apparaat geïnstalleerd moeten worden. Afhankelijk van de configuratie en het apparaat wordt de app automatisch geïnstalleerd of wordt de gebruiker gevraagd de app te installeren.

Houd er rekening mee dat het wordt aanbevolen om Android Enterprise te gebruiken voor eenvoudig app-beheer.

De scenario's staan hieronder:

Normale Play Store-apps

Voor het installeren van een Playstore App is altijd interactie van de gebruiker nodig. Daarnaast moet er een Google-account worden geconfigureerd op het apparaat.

InHouse app installatie

Op Samsung-apparaten worden deze apps geruisloos geïnstalleerd. De enige uitzondering is de container, waar de gebruiker de installatie moet bevestigen.

In elk ander scenario moet de gebruiker de installatie van de app bevestigen.

Android Play Store-apps voor bedrijven

Deze Apps worden altijd geruisloos geïnstalleerd, zonder interactie van de gebruiker.

Om een verplichte app toe te voegen, klikt u op de "+" en selecteert u de gewenste app uit de lijst. Houd er rekening mee dat u geen apps kunt installeren vanuit het tabblad "Google Play Store" als het apparaat is geconfigureerd met Android Enterprise als volledig beheerd of als container.

Als u Android Enterprise gebruikt, selecteert u de apps uit het gedeelte "AE Play Store". Om apps hier beschikbaar te maken, bevestigt u ze in de Google Enterprise Play Store door naar Algemene instellingen → AE Play Store → Play Store Apps te gaan.

Als je een verplichte app verwijdert, wordt deze ook van het apparaat verwijderd.

Je kunt op de naam van een app klikken in de verplichte app-lijst en naar het tabblad "configuratie" gaan om een app te configureren. Dit vereist het gebruik van Android Enterprise en de app moet dit ondersteunen. Daarom zijn de beschikbare opties afhankelijk van de geselecteerde app.

AE-systeemapps

Hier kun je System Apps inschakelen voor Android Enterprise-apparaten. Houd er rekening mee dat de opgegeven app in de opslag van het systeem moet staan, anders gebeurt er niets. 296

Beperkingen en instellingen

Zwarte lijsten en witte lijsten

Hier kun je een zwarte of witte lijst definiëren. Alle apps op de zwarte lijst worden geblokkeerd. Alle apps die niet op de witte lijst staan, worden geblokkeerd. Een lege zwarte lijst blokkeert niets, terwijl een lege witte lijst alles blokkeert*.

**Alle verplichte apps en apps uit de Enterprise App Store worden automatisch in de witte lijst opgenomen. U hoeft ze niet handmatig toe te voegen*

Als je op de "+" klikt, kun je zoeken naar een app die je wilt toevoegen aan je zwarte of witte lijst of handmatig een pakketnaam invoeren.

Beperkingen voor systeemtoepassingen

Onder "Sys App Restrictions" kun je naar wens onder andere voorgeïnstalleerde apps en services blokkeren.

Browser uitschakelen	Standaardbrowser uitschakelen
Kalender uitschakelen	Eigen kalender uitschakelen
Rekenmachine uitschakelen	Rekenmachine uitschakelen
Browser Chrome uitschakelen	Chrome-browser uitschakelen
Klok uitschakelen	Klok uitschakelen
Contacten uitschakelen	Contacten uitschakelen
Dialer uitschakelen	Native dialer uitschakelen
E-mail uitschakelen	E-mail uitschakelen
Uitwisseling uitschakelen	Exchange-accounts uitschakelen
Facebook uitschakelen	Facebook-app uitschakelen
Galerij uitschakelen	Native galerij-app uitschakelen
Gmail uitschakelen	Gmail uitschakelen
Google Boeken uitschakelen	Google Boeken uitschakelen
Google Play Kiosk uitschakelen	Google Play Kiosk uitschakelen
Google Maps uitschakelen	Google Maps uitschakelen
Google Muziek uitschakelen	Google Muziek uitschakelen
Google Films uitschakelen	Google Films uitschakelen
Google Play Store uitschakelen	Google Play Store (openbare App Store) uitschakelen
Google Plus uitschakelen	Google Plus uitschakelen
Google-zoekopdracht uitschakelen	Google-zoekopdracht uitschakelen
Google Talk / Google Hangouts uitschakelen	Google Talk / Google Hangouts uitschakelen
Muziekspeler uitschakelen	Muziekspeler-app uitschakelen
Instellingen uitschakelen	Apparaatinstellingen uitschakelen
Sim Toolkit uitschakelen	Sim Toolkit-diensten uitschakelen
SMS / MMS uitschakelen	SMS / MMS uitschakelen
Straatweergave uitschakelen	Street View-diensten uitschakelen
Youtube uitschakelen	Youtube uitschakelen

Samsung-apps

Onder "Samsung Apps" kunt u extra instellingen en/of beperkingen voor Samsung-apparaten definiëren.

AllShare Play / Samsung Link uitschakelen	AllShare Play / Samsung Link uitschakelen
ChatON uitschakelen	ChatON uitschakelen
Gamehub uitschakelen	Gamehub uitschakelen
Groepsweergave uitschakelen	Groepsweergave uitschakelen
Help uitschakelen	Samsung Help uitschakelen
KNOX uitschakelen	Samsung KNOX-container uitschakelen
Memo uitschakelen	Spraakmemo uitschakelen
Mijn bestanden uitschakelen	Mijn bestanden uitschakelen
Optische lezer uitschakelen	Optische lezer uitschakelen
Polaris Office uitschakelen	Polaris Office uitschakelen
Readers Hub / Samsung boeken uitschakelen	Readers Hub / Samsung boeken uitschakelen
S Memo uitschakelen	Samsung Memo app uitschakelen
S Vertaler uitschakelen	Samsung Translator-app uitschakelen
S Voice uitschakelen	S Spraakassistent uitschakelen
Samsung-apps uitschakelen	Samsung App Store uitschakelen
Samsung Hub uitschakelen	Samsung-entertainmentwinkels uitschakelen
Videospeler uitschakelen	Videospeler uitschakelen
Stemrecorder uitschakelen	Stemrecorder uitschakelen
WatchON uitschakelen	WatchON uitschakelen (simuleert een afstandsbediening)

Huawei Apps

Onder "Huawei Apps" kunt u extra instellingen en/of beperkingen op het Huawei apparaat instellen.

DLNA uitschakelen	DLNA uitschakelen
App-installer uitschakelen	App-installer uitschakelen
Bestandsbeheer uitschakelen	Bestandsbeheer uitschakelen
Back-upbeheer uitschakelen	Back-upbeheer uitschakelen
Systeemupdater uitschakelen	Systeemupdater uitschakelen
Gereedschapskist uitschakelen	Gereedschapskist uitschakelen
Weer uitschakelen	Weer uitschakelen
FM-radio uitschakelen	FM-radio uitschakelen

App Beheer Instellingen

Hier kunt u het update gedrag van InHouse Apps definiëren.

Update Check Frequency bepaalt hoe vaak de AppTec360 App zoekt naar updates voor InHouse apps. Zodra een nieuwe versie is gedetecteerd, wordt deze gedownload en geïnstalleerd.

Wi-Fi Threshold definieert of het downloaden moet worden beperkt tot Wi-Fi-verbindingen als de app groter is dan de door jou geconfigureerde Threshold. Als de app kleiner is of als je geen drempel instelt, wordt de app zowel via Wi-Fi als via een mobiel netwerk gedownload.

App Store voor ondernemingen

Houd er rekening mee dat apps die hier worden toegevoegd (Enterprise App Store) NIET automatisch op het apparaat worden geïnstalleerd. De gebruiker moet de Enterprise App Store openen op het apparaat en de app handmatig installeren.

Als u automatisch apps wilt installeren op het apparaat, ga dan naar "App Management" → "Enterprise App Manager" → "Verplichte apps" en voeg daar de gewenste apps toe.

Onder dit punt kunt u optionele Apps distribueren onder uw gebruikers.

Playstore

Klik op de "+" om een Play Store-app toe te voegen aan de store. Als je Android Enterprise gebruikt, ga dan naar "App Management Enterprise Play Store". Houd er ook rekening mee dat er een Google-account moet worden geconfigureerd op → het apparaat om de hier gedefinieerde apps te installeren.

Intern

Onder het punt "In-House" kun je intern ontwikkelde apps uploaden en distribueren.

Klik op de "+" om een InHouse app toe te voegen aan de enterprise app store die vervolgens door de gebruiker geïnstalleerd kan worden. In dit dialoogvenster kun je ook een nieuwe InHouse app uploaden.

Play Store voor bedrijven

Houd er rekening mee dat apps die hier worden toegevoegd (Enterprise Play Store) NIET automatisch op het apparaat worden geïnstalleerd. De gebruiker moet de Play Store op het apparaat openen en de app handmatig installeren.

Als u automatisch apps wilt installeren op het apparaat, ga dan naar "App Management" → "Enterprise App Manager" → "Verplichte apps" en voeg daar de gewenste apps toe.

Onder dit punt kunt u optionele Apps distribueren onder uw gebruikers.

Hier kun je Apps toevoegen aan de Android Enterprise Playstore. Houd er rekening mee dat u Apps moet goedkeuren in Algemene Instellingen → AE Play Store → Play Store Apps. Deze Apps worden toegevoegd aan de normale Google Play Store.

Houd er ook rekening mee dat je eerst een lay-out met apps moet definiëren in Algemene instellingen → App-beheer → AE Play Store → Store-indeling.

Apps moeten in een Lay-out staan voordat je ze aan de winkel kunt toevoegen.

Kioskmodus & Launcher

Kioskmodus

Met de Kioskmodus kun je een app of URL vooraf definiëren. Dan zal het uitsluitend mogelijk zijn om deze app en/of URL uit te voeren/te bezoeken.

Op dezelfde manier kunnen verschillende hardwareknoppen gedeactiveerd worden in de verschillende Kioskmodi.

Automatisch starten	Start automatisch de Kiosk-modus zodra het profiel het eindgebruikersapparaat bereikt
Geplande kioskmodus?	Je kunt een tijd plannen voor de Kioskmodus, deze zal dan automatisch starten en eindigen op een door jou ingestelde tijd.
Starttijd	Starttijd
Tijd in minuten	Tijd in minuten waarna de Kioskmodus weer moet eindigen

Type toepassing

Enkele app	Als je de app in de Kioskmodus wilt starten, selecteer dan Package" onder "Application Type".
Kiosk-toepassing	Klik hier om een app te selecteren die moet worden gestart in Kioskmodus U vindt het gebruikelijke App Management overzicht U kunt kiezen tussen een "Google Play Store", "Android In-House Apps" en een "Pakketnaam".

Type toepassing

URL	Als je een URL wilt starten in de Kioskmodus, selecteer dan "URL" onder "Type toepassing". Definieer vervolgens het gewenste URL-adres
Browser wissen na inactiviteit	Hier kunt u een tijdsinterval in minuten instellen waarna de Kioskmodus opnieuw moet worden gestart.
Webcache en cookies wissen	Als u deze functie activeert, zal na een herstart van de Kioskmodus de webcache (cookies en afbeeldingen in het cachegeheugen) worden gewist.
Beleid voor dezelfde herkomst	Als deze functie actief is, dan kan de gebruiker alleen surfen op de subpagina's van een gedefinieerde URL Je hebt bijvoorbeeld de volgende URL gedefinieerd:www.mypage.com Dan kan de gebruiker surfen op: www.mypage.com/subpage
URL's op witte lijsten	Hier kun je een witte lijst bijhouden, al deze URL's zijn toegestaan Maximaal 1 URL per regel Een URL moet beginnen met http:/ of https://.
URL's op de zwarte lijst	Hier kun je een zwarte lijst bijhouden, al deze URL's zijn niet toegestaan Maximaal 1 URL per regel Een URL moet beginnen met http:/ of https://.
Schermoriëntatie	Deze instelling heeft betrekking op de schermaanpassingen Automatisch = automatisch Staand = verticaal formaat Landschap = liggende modus

Meerdere apps	Als je de "Multi App" Kiosk Mode selecteert, wordt het gebruik van de AppTec360 Launcher afgedwongen.
Apps	Toepassing: Selecteer een Playstore of een eigen app als Kiosk-toepassing. Het is ook mogelijk om een packagenaam in te voeren. De geselecteerde Kiosk-applicatie moet geïnstalleerd zijn op het apparaat. Vergeet niet om de Kiosk Application als verplicht in te stellen. Snelkoppeling op Homescreen: Als deze optie is ingesteld op "Aan" wordt er een snelkoppeling op het beginscherm gemaakt. Als dit is ingesteld op "Uit" wordt de app nog steeds weergegeven in de app-lijst.

Wachtwoord afsluiten ingeschakeld	Als u deze functie activeert, is het mogelijk voor de gebruiker om de Kiosk-modus te beëindigen met een wachtwoord dat u vooraf hebt ingesteld.
Wachtwoord afsluiten	Dit is het wachtwoord dat vooraf door u is ingesteld
Statusbalk automatisch samenvouwen	Als deze optie is ingeschakeld, wordt de Statusbalk automatisch ingeklapt. Met deze optie kunnen gebruikers de informatie op de Statusbalk zien, maar hebben ze geen toegang tot de functies ervan.
Statusbalk uitschakelen	De statusbalk bevat meldingen, snelkoppelingen en informatie. Alleen beschikbaar voor Samsung-apparaten met KNOX 1.0 of hoger.
Volumetoetsen uitschakelen	Volumetoetsen uitschakelen (alleen beschikbaar op Samsung-apparaten met KNOX 1.0 of hoger)
Aan/uit-schakelaar uitschakelen	Aan/uit-schakelaar uitschakelen (alleen beschikbaar op Samsung-apparaten met KNOX 1.0 of hoger)
Home-knop uitschakelen	Home-knop uitschakelen. Als deze functie is geactiveerd, kan de Kiosk-modus alleen in de AppTec360 Console worden beëindigd. (alleen beschikbaar op Samsung-apparaten met KNOX 1.0 of hoger)
Navigatiebalk uitschakelen	Hiermee kun je de navigatiebalk (Terug / Menu) uitschakelen. Als deze functie is geactiveerd, kan de Kiosk-modus alleen in de AppTec360 Console worden beëindigd. (alleen beschikbaar op Samsung-apparaten met KNOX 1.0 of hoger)

App Update-instellingen	
App-updates toestaan	Gebruikers worden gevraagd om app-updates uit te voeren, zelfs als de Kioskmodus actief is. Op apparaten met Samsung KNOX worden apps stil bijgewerkt.
Venster bijwerken	Stel een interval in waarbinnen gebruikers worden gevraagd om app-updates te installeren.

TeamViewer	
Toegang zonder toezicht inschakelen	Indien ingeschakeld, kunnen beheerders het apparaat op afstand bedienen zonder interactie van de gebruiker. De app TeamViewer Host moet geïnstalleerd zijn op het apparaat.

AppTec360 Launcher

AppTec360 Launcher inschakelen	Aan: Schakelt de AppTec360 Launcher in. De gebruiker moet deze eenmalig instellen als standaard Launcher. Opmerking: Als de Kiosk-modus is ingeschakeld en de Kiosk-modus is ingesteld op "Multi App", wordt het gebruik van AppTec360 launcher afgedwongen.
Grote pictogrammen	Aan: Toont een grotere versie van de app-pictogrammen in de Launcher
AppTec360-pictogram verbergen	Aan: Verbergt de AppTec360 App volledig
AppTec360-winkelpictogram verbergen	Aan: Verbergt de AppTec360 Enterprise AppStore volledig

AppTec360-instellingen

AppTec360 Instellingen App inschakelen	De AppTec360 Settings App biedt controle over WiFi- en Bluetooth-verbindingen.
Instellingen inschakelen in meerdere apps Kioskmodus	Indien ingeschakeld, hebben gebruikers toegang tot de AppTec360 Settings App terwijl de Multi App Kiosk Mode actief is.

Afstandsbediening

Splashtop

Toont de huidige status van de Splashtop-instelling. Hier ziet u de stappen die u moet uitvoeren om op afstand toegang te krijgen tot het apparaat via Splashtop. Hier moet u ook uw deploy code invoeren die u van de Splashtop-website kunt krijgen. De deploy code is nodig om verbinding te maken met het apparaat.

Teamviewer

Toont de huidige status van de Teamviewer Setup. Hier zie je de stappen die je moet uitvoeren om op afstand toegang te krijgen tot het apparaat via Teamviewer.

Beheer van inhoud

Inhoudsvak

Hier kun je de Contentbox inschakelen voor dit apparaat. Eenmaal geactiveerd, wordt de Contentbox App geïnstalleerd op het apparaat.

Veilige browser

Hier kun je de Veilige browser inschakelen voor dit apparaat. Eenmaal geactiveerd wordt de Secure Browser App geïnstalleerd op het toestel. Deze browser kan worden geconfigureerd om een webbrowser op het apparaat aan te bieden die beperkt is tot uw behoeften.

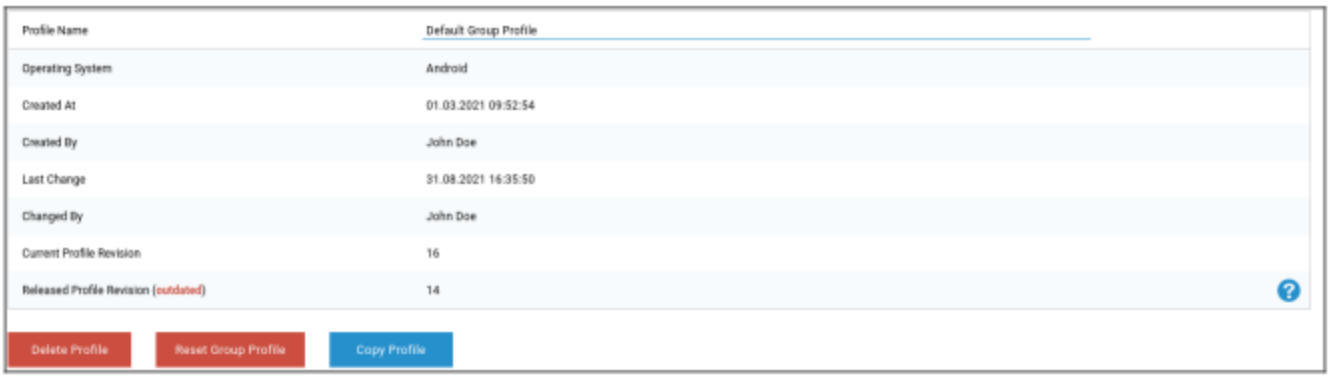
Wachtwoord nodig	Eis dat de gebruiker een wachtwoord instelt en gebruikt om toegang te krijgen tot de browser.
Beperk downloads / Open in	Blokkeert downloads van websites
Uploads beperken	Beperkt uploaden tot bepaalde URL's. Geef geen URL op om de upload volledig te blokkeren
Kopiëren toestaan	Sta het kopiëren, knippen of delen van tekst binnen de webpagina's toe.
Schermopname toestaan	Het maken van schermafbeeldingen toestaan.
Frequentie gegevensopschoning	Selecteer met welke frequentie ALLE gebruikersgegevens (geschiedenis, cache enz.) automatisch moeten worden verwijderd.
Bladwijzers voor bedrijven	De bladwijzers worden weergegeven in de map "Bedrijfsbladwijzers" in de bladwijzers van de browser. Ze kunnen niet worden bewerkt door de gebruiker.
Adresbalk verbergen	Verbergt de adresbalk zodat de gebruiker de URL die hij bezoekt niet ziet
Whitelisting in browser (zonder Universal Gateway)	Maakt client-side URL-whitelisting mogelijk. - Bedrijfsbladwijzers worden altijd gewhitelist - Ondersteund voor slechts 100 URL's - Gebruik de Universal Gateway voor onbeperkte zwarte en witte lijsten
Black- en whitelisting op basis van gateways	Blacklisting heeft de volgende vereisten: - Een werkende AppTec360 Universal Gateway ("Algemene instellingen" → "Universal Gateway") - Een werkende VPN-configuratie met een opgegeven DNS-server ("Algemene instellingen" → "Universal Gateway" → "VPN-instellingen") - Een Blacklist-configuratie ("Algemene instellingen" → "Universal Gateway" → "Domein Blacklist") - Een geldige VPN-verbinding in het profiel ("Verbindingsbeheer" → "VPN")

Configuratie Windows 10 PC

Algemeen

Overzicht groepsprofiel (alleen op groepsniveau)

Wanneer je een groepsprofiel opent, krijg je een snel overzicht van het profiel.



Profielnaam	Naam van het profiel (kan hier worden gewijzigd)
Besturingssysteem	Besturingssysteem waar het profiel voor is
Gemaakt op	Tijd van creatie
Gemaakt door	De maker van het profiel
Laatste wijziging	Tijdstip van laatste wijziging van het profiel
Veranderd door	Account die de laatste wijzigingen heeft aangebracht
Huidige profielherziening	Revisie van opgeslagen profielstatus
Vrijgegeven profiel Revisie	Toegewezen profielrevisie ("Nu toewijzen"). Als er "(verouderd)" achter de tekst staat, betekent dit dat je het profiel hebt opgeslagen maar nog niet hebt toegewezen, zodat de apparaten nog steeds een oudere versie krijgen.

Apparaatoverzicht (alleen op apparaatniveau)

Het samengevatte overzicht van het apparaat, dat het volgende bevat:

PC-naam	Naam van de pc
Klant	De apparaten Windows type
Laatst bekende locatie	De lengte- en breedtegraad van de laatst bekende locatie van het apparaat
Toegewezen verplichte apps	Aantal verplichte apps toegewezen aan het apparaat
PC UID	UID van de pc
OS Editie	Toont uw Windows-editie
OS versie	Momenteel geïnstalleerde Windows-versie
OS bouwen	Huidige Windows-versie
Besturingssysteem	Momenteel geïnstalleerd besturingssysteem
Serienummer	Serienummer van het apparaat
Apparaateigendom	Het geconfigureerde eigenaarschapstype
Type apparaat	Het type apparaat
Geworteld	Geeft aan of het apparaat geroot is
Conform	Geeft aan of het apparaat voldoet
Laatst gezien	Datum en tijd waarop wijzigingen zijn aangebracht in het profiel
Gebruikerstoewijzing	Geeft de gebruiker of groep weer waaraan dit apparaat momenteel is toegewezen. Je kunt het apparaat verplaatsen door een andere gebruiker of groep te selecteren in de vervolgkeuzelijst.

Instellingen

Automatisch bijwerken toestaan	Automatische os-updates toestaan of weigeren.

Configuratie Revisie (alleen op apparaatniveau)

Hier krijg je een overzicht van welk groepsprofiel aan het apparaat is toegewezen.

Als je op het groepsprofiel klikt, krijg je direct toegang tot het profiel en kun je instellingen uitvoeren.

Met het symbool kun je de toegewezen apps terugzetten naar de instellingen van het groepsprofiel.

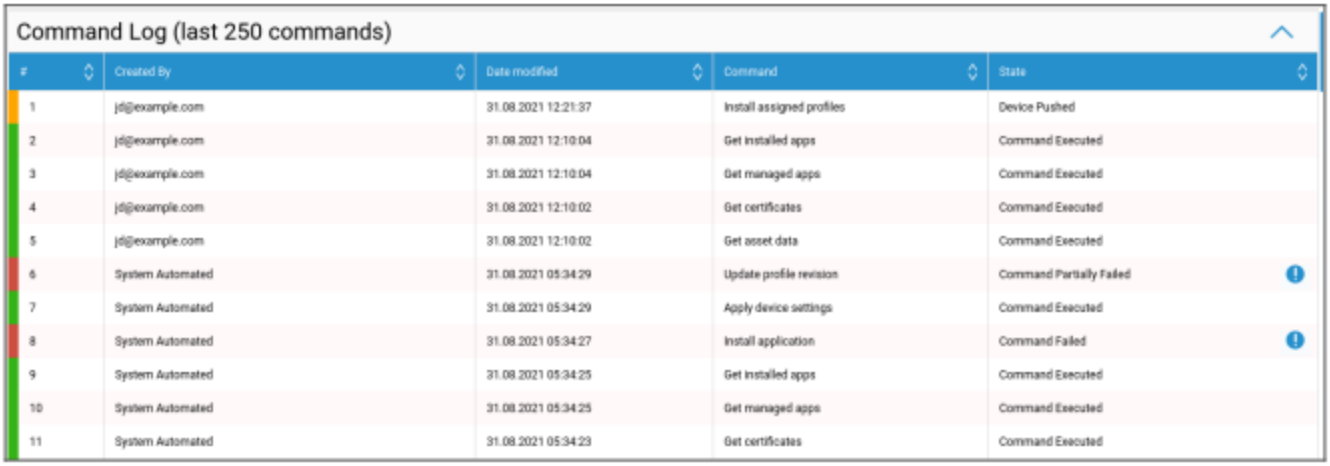
Met het symbool kun je het apparaatprofiel resetten zodat er helemaal geen instellingen zijn.

"Newer Revision available" geeft aan dat het groepsprofiel gewijzigd en opgeslagen is, maar niet toegewezen. Het groepsprofiel moet worden toegewezen met "Assign now" op groepsniveau om de wijzigingen toe te passen op de apparaten.

Apparaatlogboek (alleen op apparaatniveau)

Opdrachtlogboek

Hier kun je zien welke commando's zijn uitgegeven voor het apparaat en wat hun status is.



Commando's die zijn aangemaakt door "System Automated" worden automatisch aangemaakt door het systeem.

Mogelijke opdrachtstatussen

Apparaat ingedrukt	Er is een pushverzoek verzonden naar de pushservice (bijv. APNS) om het apparaat te vertellen terug verbinding te maken met de EMM-server.
Commando aangemaakt	De opdracht is aangemaakt in het systeem.
Opdracht verzonden	De opdracht werd naar het apparaat gestuurd nadat het verbinding had gemaakt met de server.
Opdracht uitgevoerd	De opdracht is succesvol uitgevoerd.
Opdracht mislukt	De opdracht is mislukt. *
Commando gedeeltelijk mislukt	Afhankelijk van het besturingssysteem van het apparaat kunnen sommige commando's gegroepeerd worden. Hierin zijn sommige delen van deze commandogroep mislukt. *
Opdracht uitgevoerd, uiteindelijk mislukt	Het commando werd uitgevoerd, maar misschien ook niet.
Commando verplaatst	De opdracht is opnieuw uitgevoerd door een gebruiker.
Afgedankt	De opdracht is verwijderd. Bijvoorbeeld omdat het is vervangen door een ander commando of omdat het apparaat opnieuw is aangemeld en oude commando's zijn verwijderd.

*Als er een uitroepteken achter het bericht staat, kun je meer informatie krijgen door met je cursor over het pictogram te gaan.

Activabeheer (alleen op apparaatniveau)

Apparaat info

Fabrikant	Fabrikant van het apparaat
Model	Apparaatmodel
Modelnummer	Modelnummer
Besturingssysteem	Besturingssysteem
OS versie	OS-versie
Serienummer	Serienummer
ExchangeID	ExchangeID
Totaal RAM	Totaal RAM
Resolutie	Resolutie weergeven
Telefoon Taal	Taal apparaat
Firmwareversie	Firmwareversie
DM-clientversie	Versie apparaatbeheerclient
Hardwareversie	Apparaathardwareversie
CPU-architectuur	CPU-architectuur (processortype)

Cellulair

SIM-dragernetwerk	Carrier-netwerk
Telefoonnummer	Telefoonnummer
Roaming-status	Roaming-status
IMEI	IMEI
IMSI	IMSI
Modem firmware	Modem firmware

Synchronisatie-info

Directe DM-verbinding	Het apparaat moet onmiddellijk een verbinding maken met AppTec
Initiële hersteltijd	Initiële hersteltijd voor deze eerste verbinding
Opnieuw proberen van verbinding	Aantal nieuwe verbindingspogingen na een verbroken verbinding van de Connection Manager of een fout op WinInet-niveau
Maximale slaaptijd	Maximale slaaptijd na fout bij pakketverzending
Eerste pogingen tot synchronisatie	Tijd voor de eerste fase na de inschrijving
Interval eerste nieuwe poging	Tijd voor de eerste fase na de inschrijving
Tweede pogingen tot synchronisatie	Tijd voor de tweede fase na de inschrijving
Tweede opnieuw proberen interval	Tijd voor de tweede fase na de inschrijving
Regelmatig opnieuw synchroniseren	Tijd voor de extra stappen na de inschrijving
Regelmatig opnieuw proberen interval	Tijd voor de extra stappen na de inschrijving

Beveiligingsbeheer

Anti diefstal (alleen op apparaatniveau)

GPS-informatie (alleen op apparaatniveau)

Hier kun je de huidige/laatste locatie van het apparaat bepalen. De lokalisatie kan worden beveiligd met een of zelfs twee wachtwoorden - Zie: "Algemene instellingen" > "Privacy" > "GPS-toegang".

GPS-instellingen

GPS-tracering inschakelen	Regelmatige synchronisatie van GPS-informatie inschakelen.
Volginterval	Het synchronisatie-interval van de GPS-informatie instellen.

Beveiligingsconfiguratie

Wachtwoord

Minimale lengte wachtwoord	Minimale lengte wachtwoord	
Wachtwoord Samenstelling	Bepaalt het aantal specifieke tekens dat het wachtwoord moet bevatten Deze bestaan uit hoofdletters, kleine letters, cijfers en speciale symbolen	
Wachtwoord kwaliteit	Hier kunt u de wachtwoordkwaliteit instellen	
	Alfanumeriek	Alleen cijfers en letters
	Numeriek	Alleen getallen
	Numeriek of alfanumeriek	Cijfers of cijfers en letters
Maximale inactiviteitstijd Slot	Aantal minuten van inactiviteit van de gebruiker op het apparaat, waarna het apparaat wordt vergrendeld. Na deze tijd moet de gebruiker het apparaat ontgrendelen door het wachtwoord van het apparaat in te voeren.	
Verlopen wachtwoord	Stel de tijd in tot een nieuw wachtwoord moet worden ingesteld	
Beperking wachtwoordgeschiedenis	Aantal eerder gebruikte wachtwoorden die niet zijn toegestaan	
Maximum aantal mislukte wachtwoordpogingen	Aantal keren dat het wachtwoord verkeerd kan worden ingevoerd, voordat het apparaat volledig wordt gewist	

Antivirus

Antivirusinstellingen - scanconfiguratie instellen	
Type scan	Selecteert of een snelle of volledige scan moet worden uitgevoerd
Start scan instellen	Selecteert het tijdstip van de dag waarop Windows Defender het scannen start.
Scanfrequentie	Selecteert de dag waarop de scan van Windows Defender moet worden uitgevoerd
Frequentie handtekeningupdates	Specificeert het interval in uren dat wordt gebruikt om te controleren op handtekeningen

Type te scannen bestanden configureren	
Scannen van archiefbestanden toestaan	Het scannen van archieven (zoals .zip) toestaan of niet toestaan wanneer ze worden geopend.
Scannen van scripts toestaan	Hiermee wordt de functionaliteit voor Windows Defender Script Scannen in- of uitgeschakeld.
Scannen van e-mails toestaan	Het scannen van e-mails toestaan of weigeren.
Scannen van netwerkbestanden toestaan	Het scannen van netwerkbestanden toestaan of niet toestaan.
Volledig scannen van gemapte netwerkstations toestaan	Scannen van gemapte netwerkstations toestaan of niet toestaan (alleen ingeschakeld als volledige scan is ingeschakeld).
Controle bidirectioneel scannen	Bepaalt welke sets bestanden moeten worden gemonitord.
Volledig scannen van verwisselbare schijven toestaan	Volledig scannen van verwisselbare stations toestaan of niet toestaan. Alleen tijdens volledige scan wordt gestart.

Type bestanden dat moet worden uitgesloten van de scan	
Bestandstypen negeren voor scannen	Definieer een reeks bestandstype-extensies. Elke bestandsextensie voor elk veld.
Mappaden negeren	Definieer een reeks mappaden om ze niet te scannen. Eén pad per veld. Voorbeelden: "C:\Example", "C:\Windows" of "C:\Users".
Processen uitsluiten van scan	Bestanden die zijn geopend door specifieke processen uitsluiten van Microsoft Defender Antivirusscans. . Eén pad per veld. Voorbeelden: C:\myFile.exe", "C:\Windows\myProcess.exe", "C:\myScript.bat".

Extra instellingen	
Realtime bewaking toestaan	De functionaliteit Windows Defender Realtime Monitoring toestaan of weigeren
Gedragsmonitoring toestaan	De functionaliteit van Windows Gedragsmonitoring toestaan of weigeren
Cloudbescherming toestaan	Toestaan of niet toestaan dat Windows Defender informatie naar Microsoft stuurt over elk probleem dat het vindt. Microsoft zal deze informatie analyseren, meer te weten komen over het probleem dat van invloed is op het apparaat en verbeterde oplossingen aanbieden.
	Gedrag bij het verzenden van monsters
Windows Defender IOAV-bescherming toestaan	Windows Defender IOAV-bescherming toestaan of weigeren
Toegang verlenen tot de Defenders "Toegangsbeveiliging" UI	
Gemiddelde CPU-belastingsfactor	Geeft de gemiddelde CPU-belastingsfactor weer voor de scan van Windows Defender (in procenten)

Afhandeling van malware	
Lage ernst	U kunt voor elk ernstniveau definiëren hoe het apparaat omgaat met malware. Beschikbare opties zijn: • Schoon • Quarantaine • Verwijder • Sta toe. • Door gebruiker gedefinieerd • Blok
Matig ernstig	
Zeer ernstig	
Ernstig	
Dagen om opgeschoonde malware te behouden	Tijdsperiode in dagen dat bestanden/items in quarantaine worden bewaard op het systeem. De standaardwaarde is 0, waardoor items in quarantaine blijven en niet automatisch worden verwijderd. De maximale waarde is 90.

Beveiligingscentrum

Windows Beveiligingscentrum - Instellingen voor Windows Beveiliging	
UI voor virus- en bedreigingsbeveiliging uitschakelen	
Verberg Ransomware Data Herstel UI	
Accountbeveiliging UI uitschakelen	
UI Firewall en netwerkbeveiliging uitschakelen	
UI voor besturingselementen voor apps en browsers uitschakelen	
Wijzigingen in Exploitbeveiliging niet toestaan	Gebruiker niet toestaan wijzigingen aan te brengen in instellingen voor Exploitbeveiliging
UI voor apparaatbeveiliging uitschakelen	
TPM-problemen verbergen	Instellingen voor probleemoplossing TPM verbergen
Knop TPM wissen uitschakelen	
UI voor apparaatprestaties en gezondheid uitschakelen	
UI voor gezinsopties uitschakelen	

Toasts aanpassen	
Aangepaste ondersteuningsinfo inschakelen	Inschakelen om aangepaste contactgegevens voor ondersteuning voor je bedrijf weer te geven rechtsonder in de app van het beveiligingscentrum.
E-mailadres	Stel het e-mailadres van het bedrijf in
Bedrijfsnaam	Bedrijfsnaam instellen
Telefoon bedrijf	Bedrijfstelefoon instellen
URL Help	Stel de help-URL van het bedrijf in

Extra instellingen	
Meldingen uitschakelen	De weergave van meldingen van Windows Defender Beveiligingscentrum uitschakelen.
Verberg TPM firmware update aanbevelingen	Verberg de aanbeveling om de TPM-firmware bij te werken wanneer een kwetsbare firmware wordt gedetecteerd.
Bedrijfsnaam en contactopties weergeven	Geef je bedrijfsnaam en contactopties weer in een contactkaart in Windows Defender Beveiligingscentrum.
Secure Boot verbergen	Verberg het gebied Security Boot.
Gebied voor beveiligingsmeldingen verbergen	Windows Beveiligingskennisgeving gebied controle verbergen.

Firewall configureren

Firewall configureren - Globale instellingen	
Negeer authenticatieset	Negeer de volledige authenticatieset als ze niet alle in de set gespecificeerde authenticatiesuites ondersteunen
Type pakketwachtrij	Specificeert hoe het schalen voor de software aan de ontvangstzijde is ingeschakeld voor zowel de versleutelde ontvangst als het vrijmaken van het doorstuurpad voor het IPsec tunnel gateway scenario.
Stateful FTP-filtering uitschakelen	Als het is uitgeschakeld, zal het geen stateful File Transfer Protocol (FTP) filtering uitvoeren om secundaire verbindingen toe te staan.
Beveiligingsassociatie inactieve tijd	Dit veld configureert de inactieve tijd van de beveiligingsassociatie, in seconden. Beveiligingsassociaties worden verwijderd nadat er geen netwerkverkeer is gezien gedurende deze gespecificeerde periode.
Vooraf gedeelde sleutelcodering	De codering van de vooraf gedeelde sleutel instellen
IPSec-uitzonderingen	Internet Protocol uitzonderingen configureren
Controle van de certificatenlijst	

Firewallprofielen (domeinprofiel / privéprofiel / openbaar profiel)	
Firewall inschakelen voor dit profiel	
Meldingen uitschakelen	Schakel het weergeven van een melding aan de gebruiker uit wanneer een applicatie geblokkeerd is om op een poort te luisteren.
Unicast-reacties op multicast-uitzendingen blokkeren	
Geautoriseerde applicatiefirewallregels afdwingen	Als dit niet wordt afgedwongen, worden geautoriseerde applicatiefirewallregels in de lokale opslag genegeerd en niet afgedwongen.
Globale poort-firewallregels afdwingen	Als dit niet is afgedwongen, worden de regels van de globale poort-firewall in de lokale opslag genegeerd en niet afgedwongen. De instelling heeft alleen betekenis als deze is ingesteld of opgesomd in de Group Policy store of als deze is opgesomd vanuit de GroupPolicyRSoPStore
Firewallregels afdwingen	Als dit niet wordt afgedwongen, worden firewallregels van de lokale opslag genegeerd en niet afgedwongen
Verbindingsbeveiligingsregels afdwingen	Als dit niet wordt afgedwongen, worden de verbindingsbeveiligingsregels van de lokale winkel genegeerd en niet afgedwongen.
Standaard uitgaande actie	De actie die de firewall standaard uitvoert op uitgaande verbindingen
Standaard inkomende actie	De actie die de firewall standaard uitvoert op inkomende verbindingen
Stealth-modus uitschakelen	Stealth modus is een mechanisme in Windows Firewall dat helpt voorkomen dat kwaadwillende gebruikers informatie ontdekken over netwerkcomputers en de services die ze uitvoeren.
Het voorkomen van reageren op ongevraagd verkeer uitschakelen	Indien uitgeschakeld, mogen de regels van de stealth modus van de firewall niet verhinderen dat de hostcomputer reageert op ongevraagd netwerkverkeer als dat verkeer beveiligd is door IPsec.

Firewall-regels

Firewall-regels	
Naam	Naam van de regel
Beschrijving	Beschrijving van de regel
Actie	Specificeer of deze regel het verkeer zal blokkeren of toestaan. Houd er rekening mee dat de optie Blokkeren ook het verkeer tussen de MDM-server en het Apparaat kan blokkeren (afhankelijk van de rest van de configuratie).
Richting	
Edge traversal inschakelen (alleen beschikbaar wanneer **Richting** is ingesteld op **inkomend verkeer**)	Geeft aan dat specifiek inkomend verkeer door NAT's en andere randapparaten mag tunnelen met behulp van de Teredo tunneling technologie.

Programma's & diensten	
Definieer toepassingen, alle andere	Als dit niet is ingeschakeld, worden alle aanvragen in aanmerking genomen.
Naam pakketfamilie	De pakketnaam waarop de regel van toepassing is.
Bestandspad van de toepassing	De volledige toepassing zoals C:\WindowsSystem\Notepad.exe waarop de regel van toepassing is
Volledig gekwalificeerde binaire naam	De Fully Qualified Binary Name waarop de regel van toepassing is. Een FQBN is een string in de volgende vorm: {UitgeverProductBenaming,Versie}
Servicenaam	Voer de naam van een service in (bijvoorbeeld "EventLog"). Je kunt een lijst met servicenamen opvragen met Powershell door het commando "Get-Service" uit te voeren.

Protocollen en poorten				
Protocol	Het protocol dat door de regel wordt gebruikt.			
	Beschikbare waarden: - Elke - Aangepast - HOPORT - ICMPv4 - IGMP - TCP - UDP - IPv6 - IPv6-route - IPv6-sleuf - GRE - ICMPv6 - IPv6-NoNxt - IPv6-opties - VRRP - PGM - L2TP	Wanneer ingesteld op Aangepast	Voer een protocolnummer in tussen 0 en 255	Het protocolnummer
		Wanneer ingesteld op TCP of UDP	Geef lokale poorten op, anders worden ze allemaal gebruikt	Lokale poorten die de regel zal gebruiken, bereikpoorten zijn ook toegestaan
			Lokale haven	Enkele poort of een reeks poorten. Bijv. 100-120,200,300-320.
			Geef poorten op afstand op, anders worden ze allemaal gebruikt	Remote poorten die de regel zal gebruiken, bereikpoorten zijn ook toegestaan
			Externe poort	Enkele poort of een reeks poorten. Bijv. 100-120,200,300-320.

Toepassingsgebied	
Geef lokale IP's op, anders elk IP	Set lokale IP's, het kan ook een reeks IP's zijn gescheiden door -.
Lokaal IP-adres	Set van afzonderlijke IP's of een reeks IP's gescheiden door -
IP's op afstand opgeven, anders elk IP op afstand	Geef een reeks IP's op afstand op, het kan ook een reeks IP's zijn, gescheiden door "-".
IP-adres op afstand	Geef afzonderlijke IP's of een bereik van IP's op
Tokens	Tokens die samen met Remote Addresses kunnen worden ingesteld. Tokens Intranet, RmtIntranet en Ply2Renders worden ondersteund in Windows 10, versie 1809 en hoger.

Geavanceerde instellingen	
Geef profielen op, anders worden ze allemaal gebruikt	Als deze optie is uitgeschakeld, worden alle profielen gebruikt

Domein	Domein Profiel
Privé	Privé profiel
Openbaar	Publiek profiel
Geef interfaces op, anders worden ze allemaal gebruikt	Indien uitgeschakeld worden alle interfaces gebruikt
Lokaal netwerk	Interface lokaal netwerk
Toegang op afstand	Interface voor externe toegang
Draadloze	Draadloze interface

Plaatselijke schooldirecteuren	
Geautoriseerde lokale gebruikers toevoegen	Sta toe om een lijst van lokale gebruikers toe te voegen die deze regel zullen gebruiken
Geautoriseerde gebruikers	Lijst van geautoriseerde lokale gebruikers voor deze regel. De gebruiker moet in SDDL-formaat (Security Description Definition language) zijn, bijvoorbeeld PC_NAME\USERNAME. Dit veld moet niet worden gevuld als een servicenaam is ingesteld om deze regel te gebruiken.

Beperkende instellingen

Functionaliteit van het apparaat

SD-kaart toestaan	Het gebruik van een SD-kaart toestaan
Camera toestaan	Het gebruik van de camera toestaan
Locatieservice toestaan	Sta de locatiedienst van het apparaat toe
Sideloading van apps toestaan	Installatie van apps van onbekende bronnen toestaan
Modus Ontwikkelaar toestaan	Ontwikkelmodus mogelijk
Mobiele dataroaming toestaan	Mobiel dataroamen toestaan
Cortana toestaan	Stemassistent Cortana toestaan
Zoeken toestaan om locatie te gebruiken	Laat zoeken op locatie toe
Toevoegen van niet-Microsoft e-mailaccount toestaan	Geef aan of de gebruiker e-mailaccounts mag toevoegen die niet van MSA zijn.
Microsoft-accountverbinding toestaan	Geef aan of het gebruik van MSA-accounts voor niet-e-mailgerelateerde verbindingsverificatie en -diensten is toegestaan.
Mijn instellingen synchroniseren toestaan	Instellingen synchroniseren over het hele apparaat
Beschermde bedrijfsdomeinnamen	Geeft de domeinnamen van de onderneming op, gescheiden door ";".
Gebruiker toestaan om systeemherstel uit te schakelen	Hiermee kan de gebruiker Systeemherstel uitschakelen. **WAARSCHUWING!** Deze functie mag alleen worden gebruikt op apparaten die eigendom zijn van of geleverd worden door het bedrijf of de organisatie of op een apparaat dat eigendom is van de gebruiker en waarbij de gebruiker toestaat dat het apparaat volledig wordt beheerd door het bedrijf. Als je deze beleidsinstelling uitschakelt, wordt Systeemherstel uitgeschakeld en is de Wizard Systeemherstel niet toegankelijk. De optie om Systeemherstel te configureren of een herstelpunt aan te maken via Systeembeveiliging is ook uitgeschakeld.

Gebruiker uitschrijven toestaan	Hiermee kan de gebruiker het bedrijfsgedeelte van het apparaat verwijderen en daarmee de verbinding met de AppTec360-servers verbreken. Als dit gebeurt, kan het apparaat niet meer worden beheerd. **WAARSCHUWING!** Deze functie mag alleen gebruikt worden op apparaten die eigendom zijn van of geleverd worden door de onderneming of organisatie of op een apparaat dat eigendom is van de gebruiker en waarbij de gebruiker toestaat dat het apparaat volledig beheerd wordt door de onderneming. Als je deze beleidsinstelling uitschakelt, kunnen gebruikers geen MDM-registraties verwijderen. Geef aan of de gebruiker het werkplekaccount mag verwijderen via het werkplekbedieningspaneel. De MDM-server kan het account altijd op afstand verwijderen.

BitLocker

BitLocker configuratie

Algemene instellingen	
Apparaatversleuteling vereisen	Gebruikers vragen om apparaatversleuteling in te schakelen.Afhankelijk van de Windows-editie en systeemconfiguratie kunnen gebruikers worden gevraagd: - Om te bevestigen dat encryptie van een andere provider niet is ingeschakeld. - BitLocker Drive Encryption uitschakelen en BitLocker vervolgens weer inschakelen.
Encryptiemethoden	
Encryptiemethode voor besturingssysteemstations	
Encryptiemethode voor vaste gegevensstations	
Encryptiemethode voor verwijderbare gegevensstations	
Waarschuwing over schijfversleuteling door derden uitschakelen	Schakel de waarschuwingsmelding uit over een schijfcoderingsservice van derden die op het apparaat wordt gebruikt. Vanaf Windows 10, versie 1803, wordt deze instelling alleen ondersteund voor Azure Active Directory verbonden apparaten.
Codering toestaan terwijl niet-beheerder is ingelogd	Alleen ondersteund voor Azure Active Directory verbonden apparaten

AppTec360 Uitbreidingen	
Stille encryptie	Indien geselecteerd samen met "Apparaatversleuteling vereisen", zal de AppTec360 Management Service automatische stille versleuteling van de apparaatstations uitvoeren.
Automatisch gebruikersgegevens genereren	De versleutelde OS-schijf wordt beschermd met automatisch gegenereerde gebruikersgegevens. Ofwel een TPM PIN, wanneer een TPM beschikbaar is, of een 6-cijferig tekstueel wachtwoord. De gegenereerde referenties worden naar het e-mailadres gestuurd dat voor het opgegeven apparaat is geregistreerd. Als deze optie uitgeschakeld is, is de enige mogelijke bescherming voor stille encryptie het gebruik van TPM. In dat geval zal voor apparaten zonder TPM de stille encryptie mislukken.
Vaste schijven coderen	Alle beschikbare vaste gegevensstations worden ook versleuteld en beveiligd met "Automatische ontgrendeling" met behulp van een sleutel die is opgeslagen op het OS-station.

OS schijfinstellingen	
Extra verificatie vereisen bij het opstarten	Met deze instelling kunt u instellen of BitLocker elke keer dat de computer opstart een verificatie vereist. Deze instelling wordt toegepast tijdens het instellen van BitLocker. Als u deze instelling inschakelt, kunnen gebruikers geavanceerde opstartopties configureren in de installatiewizard van BitLocker.
BitLocker blokkeren zonder een compatibele TPM	
Alleen TPM	
TPM en PIN	
TPM en sleutel	
TPM, sleutel en PIN	Als u het gebruik van een PIN en een USB-flashstation (sleutel) verplicht wilt stellen, moet de gebruiker BitLocker instellen met het opdrachtregelprogramma "manage-bde" in plaats van met de installatiewizard van BitLocker Drive Encryption.

Minimale PIN-lengte vereist

	Minimale tekens

Bericht en URL voor herstel vóór het opstarten configureren	Configureer het volledige herstelbericht of vervang de bestaande URL die wordt weergegeven op het scherm voor herstel van de opstartsleutel wanneer het OS-station is vergrendeld. Opmerking: Niet alle tekens en talen worden ondersteund in pre-boot. Het wordt ten zeerste aangeraden om te testen of de tekens die je gebruikt correct verschijnen op het pre-boot herstelscherm.
	Optie voor herstelberichten vóór het opstarten
	Aangepast herstelbericht
	Aangepaste herstel-URL

Opties voor herstel van OS-schijven		Met deze instelling kunt u bepalen hoe BitLocker-beveiligde stations van het besturingssysteem worden hersteld als de vereiste referenties ontbreken. Deze instelling wordt toegepast tijdens het instellen van BitLocker. Standaard is een gegevensherstelagent op basis van een certificaat toegestaan, kunnen de herstelopties door de gebruiker worden opgegeven, inclusief het herstelwachtwoord en de herstelsleutel, en wordt van de herstelinformatie geen back-up gemaakt op AD DS.
	Agent voor gegevensherstel op basis van blokcertificaten	Geef aan of een gegevensherstelagent kan worden gebruikt met schijven van het besturingssysteem die met BitLocker zijn beveiligd. Voordat een gegevensherstelagent kan worden gebruikt, moet deze worden toegevoegd vanuit het item Public Key Policies in de Group Policy Management Console of de Local Group Policy Editor. Raadpleeg de implementatiehandleiding voor BitLocker-schijfversleuteling op Microsoft TechNet voor meer informatie over het toevoegen van agents voor gegevensherstel.
	Instellingen BitLocker herstelwachtwoord	
	Instellingen BitLocker herstelsleutel	
	BitLocker herstelinformatie opslaan in Active Directory Domain Services	
	AD DS BitLocker-opslagconfiguratie voor herstel	Het opslaan van het sleutelpakket ondersteunt het herstellen van gegevens van een schijf die fysiek beschadigd is.
	Opslag van herstelgegevens in AD DS vereisen	Voorkom dat gebruikers BitLocker inschakelen, tenzij de computer is aangesloten op het domein en

Vaste schijfinstellingen	
Herstelopties voor vaste schijven	Met deze instelling kunt u bepalen hoe vaste schijven met BitLocker-bescherming worden hersteld als de vereiste referenties ontbreken. Deze instelling wordt toegepast tijdens het instellen van BitLocker. Standaard is een gegevensherstelagent op basis van een certificaat toegestaan, kunnen de herstelopties door de gebruiker worden opgegeven, inclusief het herstelwachtwoord en de herstelsleutel, en wordt van de herstelinformatie geen back-up gemaakt op AD DS.
Agent voor gegevensherstel op basis van blokcertificaten	
Instellingen BitLocker herstelwachtwoord	
Instellingen BitLocker herstelsleutel	
BitLocker-herstelgegevens opslaan in Active Directory Domain Services	
AD DS BitLocker-opslagconfiguratie voor herstel	Het opslaan van het sleutelpakket ondersteunt het herstellen van gegevens van een schijf die fysiek beschadigd is.
Opslag van herstelgegevens in AD DS vereisen	Voorkom dat gebruikers BitLocker inschakelen, tenzij de computer is verbonden met het domein en de back-up van BitLocker-herstelinformatie naar AD DS is geslaagd. Opmerking: Het herstelwachtwoord wordt automatisch gegenereerd.
Schrijftoegang tot onbeveiligde vaste schijven weigeren	

Instellingen verwisselbare schijf	
Schrijftoegang tot onbeveiligde verwisselbare schijven weigeren	Schrijftoegang weigeren tot verwisselbare gegevensstations die niet door Bitlocker zijn beveiligd. Opmerking: Als "Verwisselbare schijven: Schrijftoegang weigeren" is ingeschakeld in het groepsbeleid, wordt deze beleidsinstelling genegeerd.
Schrijftoegang weigeren tot apparaten die in een andere organisatie zijn geconfigureerd	Alleen schijven met identificatievelden die overeenkomen met de identificatievelden van de computer krijgen schrijftoegang. Deze velden worden gedefinieerd door de groepsbeleidsinstelling "Provide the unique identifiers for your organization".

BitLocker staat

Hier ziet u de huidige status van met BitLocker versleutelde schijven

C [OS Drive]
Coderingsstatus
Gecodeerd (%)
Beschermingsstatus
Encryptiemethode
Sleutelbeschermers
Herstel wachtwoord

Met een klik op de knop "Herstelwachtwoord draaien" kun je het BitLocker herstelwachtwoord draaien.

Beheer van certificaten

Certificatenlijst

Hier is een lijst met certificaten die zijn geïnstalleerd op het apparaat dat wordt weergegeven.

Certificaatconfiguratie

Hier kunt u certificaten configureren en instellen hoe ze op het apparaat worden geïnstalleerd.

Betrouwbaar certificaat	
Beschrijving	Beschrijving certificaat
Toepassingsgebied	Toepassingsgebied certificaat: Huidige gebruiker vs apparaat
Certificaat opslaan	"Niet-vertrouwde certificaten" is alleen beschikbaar vanaf Windows 10, versie 1803
Certificaatbestand	Een PKCS#1-bestand uploaden

Identiteitscertificaat			
Beschrijving	Beschrijving certificaat		
Toepassingsgebied	Toepassingsgebied certificaat: Huidige gebruiker vs apparaat		
Belangrijke locatie	De Sleutelopslag Provider om de privésleutel in te installeren.		
		TPM. Mislukt als geen TPM aanwezig is	
	TPM. Als er geen TPM aanwezig is, terugvallen op Software KSP		
	Aanbieder van softwaresleutelopslag		Markeer privésleutel als exporteerbaar
	Windows Hello voor bedrijven	Naam container	Geeft de containernaam op van Windows Hello for Business (voorheen bekend als Microsoft Passport for Work).
		PIN-prompt tekst	Hiermee geeft u de aangepaste tekst op die moet worden weergegeven op de Windows Hello for Business PIN-prompt tijdens de registratie van het certificaat.
Geloofsbrief	Een PKCS#12-bestand uploaden		

SCEP

Beschrijving	Beschrijving SCEP-server	
Toepassingsgebied	Implementatiebereik certificaat: Huidig apparaat vs gebruiker	
URL's voor SCEP-servers	Een of meer servers die certificaten uitgeven via SCEP	
Onderwerp	Weergave van een X.500-naam. Bijvoorbeeld "C=US, O=Microsoft Corporation, CN=foo, 1.2.5.3=bar".	
Onderwerp alternatieve namen	Type	E-mailadres
		DNS
		URI
		Voornaam gebruiker (UPN)
CA Vingerafdruk	De SHA1-vingerafdruk van het certificaat van de certificeringsinstantie. E.g. 31:8F:1E:78:5C:D5:12:9F:7E:3B:AD:F3:1C:C0:19:03:96:43:A9:E5	
Geldigheidsperiode eenheden	Dagen, maanden of jaren	
Geldigheidsperiode		
Uitdaging	Gebruikt als vooraf gedeeld geheim voor automatische registratie	
Herhalingen	Het aantal keren dat het apparaat opnieuw moet proberen als de server een PENDING antwoord stuurt. De standaardwaarde is 5. De maximumwaarde is 30.	
Vertraging bij opnieuw proberen	Aantal minuten dat moet worden gewacht voordat opnieuw wordt geprobeerd. De standaardwaarde is 5. De minimumwaarde is 1.	
Sleutelgrootte	Sleutelgrootte in bits	
Hash-algoritme	Familie hash-algoritmen	
Sleutelgebruik	De uitbreiding sleutelgebruik definieert het doel (bv. vercijfering, handtekening) van de sleutel in het certificaat. Ten minste één van de opties "Digitale handtekening" of "Sleutelvercijfering" moet worden geselecteerd.	
Uitgebreid sleutelgebruik	Specificeert uitgebreid sleutelgebruik.afhankelijk van de configuratie van de SCEP-server. Specificeer de lijst met corresponderende OID's, bijv. 1.3.6.1.5.5.7.3.2 (Klantauthenticatie)	
Belangrijke locatie	De Sleutelopslag Provider om de privésleutel in te installeren.	
		TPM. Mislukt als geen TPM aanwezig is

	TPM. Als er geen TPM aanwezig is, terugvallen op Software KSP			
	Aanbieder van softwaresleutelopslag			
	Windows Hello voor bedrijven	Naam container	Geeft de containernaam op van Windows Hello for Business (voorheen bekend als Microsoft Passport for Work).	
		PIN-prompt tekst	Hiermee geeft u de aangepaste tekst op die moet worden weergegeven op de Windows Hello for Business PIN-prompt tijdens de registratie van het certificaat.	

Verbindingsbeheer

Wifi

Voer bij deze instelling de voorconfiguratie uit van de eindgebruikersapparaten voor toegang tot interne toegangspunten

Service Set Identifier (SSID)	SSID van het netwerk waarmee de verbinding tot stand wordt gebracht
Automatisch lid worden	Automatisch lid worden van het netwerk activeren
Verborgen netwerk	Activeren, als het AP de SSID niet uitzendt

Type beveiliging

AP-beveiligingstype instellen

WEP Open Systeem	
Wachtwoord	Wachtwoord voor het AP

WPA PSK	
Wachtwoord	Wachtwoord voor het AP

WPA EAP	
Type verificatie	Authenticatietype, alleen mogelijk met "PEAP-MSCAHPv2".
Snel opnieuw verbinden	Apparaten kunnen wisselen tussen Access Points zonder zich opnieuw te hoeven authenticeren
Toegang voor gasten	De gebruiker heeft geen account en moet zich daarom registreren als gast
Quarantainecontroles	De client moet NAP (Network Access Protection)-controles uitvoeren en de resultaten delen met het systeem, dat vervolgens beslist of de client verbinding kan maken.
Cryptobinding vereisen	Authenticatie is alleen mogelijk via Crypto Binding
Servervalidatie	De client controleert of het servercertificaat geldig is. Als dit het geval is, wordt een verbinding tot stand gebracht
Certificaten aanvragen	Hiermee kan de gebruiker niet-vertrouwde certificaten accepteren
Servernamen	Biedt de optie om de naam van de RADIUS-server weer te geven, die de netwerkverificatie en -autorisatie biedt.

WPA2-PSK	
Wachtwoord	AP wachtwoord

WPA2 EAP	
Type verificatie	Authenticatietype, alleen mogelijk met "PEAP-MSCAHPv2".
Snel opnieuw verbinden	
Toegang voor gasten	
Quarantainecontroles	Activeert de netwerktoegangsbeveiliging NAP
Cryptobinding vereisen	Authenticatie is alleen mogelijk via Crypto Binding
Servervalidatie	
Certificaten aanvragen	Vraagt om een gevalideerd servercertificaat, naam of een rootcertificaatauthenticatie (CA)
Servernamen	Lijst met servers die door de apparaten moeten worden vertrouwd
Geen	Geen gevestigde beveiliging
Proxyserver gebruiken	Gebruik van een proxyserver
Serveradres	Adres proxyserver
Serverpoort	Serverpoort van proxyserver

Proxyserver gebruiken

Gebruik van proxyserver inschakelen.

Serveradres	Proxyserveradres dat door dit netwerk wordt gebruikt.
Serverpoort	De poort van de proxyserver die door dit netwerk wordt gebruikt.

Wifi beperkingen

Hier kun je verschillende Wifi-restricties instellen.

WiFi toestaan	WiFi toestaan/weigeren
Delen via internet toestaan	Gebruik van een hotspot toestaan
Automatisch verbinding maken met WiFi-gevoelige hotspots toestaan	Automatisch verbinding maken met WiFi-gevoelige hotspots toestaan
Handmatige WiFi-configuratie toestaan	De gebruiker toestaan verbinding te maken met WiFi-netwerken die niet door AppTec zijn gedefinieerd
WLAN Scanfrequentie	Stelt het WLAN-Scan interval in. Hier verhoogt een hogere waarde het vermogen om WIFI-netwerken te herkennen.

VPN

Voer hier de juiste instellingen uit om VPN-verbindingen te configureren

Naam verbinding	Aangegeven verbindingsnaam		
Type VPN	Een Per-App VPN verbinding wordt gebruikt om het verkeer van bepaalde Apps te beveiligen.		
	VPN	Altijd aan	Hierdoor wordt het VPN automatisch verbonden bij het aanmelden en blijft het verbonden totdat de gebruiker de verbinding handmatig verbreekt.
	VPN per app	VPN-apps	Apps definiëren die deze VPN-verbinding gebruiken
		Vergrendeling per app	Per-App Lockdown zorgt ervoor dat de geselecteerde apps alleen verbinding hebben via deze VPN-verbinding. Deze functie is afhankelijk van Windows Defender Firewall.
	WIP-profiel	WIP-domein voor deze verbinding	Enterprise ID, die nodig is om dit VPN-profiel te verbinden met een Windows Information Protection (WIP)-beleid

Type aansluiting

AppTec360 VPN	
Voor "AppTec360 VPN" is het vereist dat app Sideloading is toegestaan. Schakel "Allow App Sideloading" in onder "Security Management" → "Restriction Settings" → "Device Functionality".	
Configuratie gateway	Om een VPN-verbinding met blacklisting te configureren, selecteert u een VPN-configuratie met een opgegeven DNS-server. U kunt een VPN-configuratie instellen onder "Algemene instellingen" → "Universele gateway" → "VPN-instellingen".

IKEv2		
Servers	Lijst van VPN-servers	
Apparaat tunnel	Verbinding inschakelen voordat gebruiker inlogt.	
Authenticatiemethode	EAP	EAP XML
	Machinecertificaten	
Encryptie-algoritme		
Algoritme voor integriteitscontrole		
Diffie-Hellman groep		
Algoritme voor versleuteling		
Algoritme voor authenticatietransformatie		
Perfect forward secrecy (PFS) groep		

PPTP		
Servers	Lijst van VPN-servers	
Authenticatiemethode	EAP	EAP XML

L2TP		
Servers	Lijst van VPN-servers	
Authenticatiemethode	EAP	EAP XML
Encryptie-algoritme		
Algoritme voor integriteitscontrole		
Diffie-Hellman groep		
Algoritme voor versleuteling		
Algoritme voor authenticatietransformatie		
Perfect forward secrecy (PFS) groep		

Automatisch		
Servers	Lijst van VPN-servers	
Authenticatiemethode	EAP	EAP XML

Algemene VPN-configuraties

Inloggegevens onthouden bij elke aanmelding	
IP-adressen registreren bij interne DNS	
Regels voor filteren van netwerkverkeer	Beperk de VPN-verbinding tot de gedefinieerde set regels.
DNS suffix zoeklijst	DNS suffixen om toe te voegen aan de DNS-zoeklijst voor het routeren van korte namen.
NRPT-regels (Name Resolution Policy Table)	Name Resolution Policy Table (NRPT) regels definiëren hoe het DNS namen omzet wanneer ze verbonden zijn met het VPN.
Detectie van vertrouwde netwerken	Lijst met DNS suffixen om het vertrouwde netwerk te identificeren.
Gesplitste tunneling	Split tunneling betekent dat verkeer over gelijk welke interface kan gaan zoals bepaald door de networking stack.
Gesplitste tunnelroutes	Lijst van routes die toegevoegd moeten worden aan de routeringstabel voor de VPN interface.
Proxy instellen	Configureert de proxy voor dit netwerk
Volmacht Adres	Proxyserveradres als een volledig gekwalificeerde hostnaam of een IP-adres.
Haven	Proxyserverpoort.
Proxy auto-config URL	URL om automatisch de proxy-instellingen op te halen.

VPN-beperkingen

Hier kunt u verschillende VPN-beperkingen definiëren.

VPN-instellingen toestaan	Deze richtlijn staat de gebruiker toe de VPN-instellingen te deactiveren en te wijzigen.
VPN over mobiel toestaan	Staat het apparaat toe/verbiedt het om een VPN-verbinding tot stand te brengen als het apparaat mobiele data gebruikt.
VPN roaming over mobiel toestaan	Staat het apparaat toe/verbiedt het om een VPN-verbinding tot stand te brengen als het apparaat aan het roamen is

Bluetooth

Hier kun je instellen of Bluetooth moet worden toegestaan/uitgesloten.

Bluetooth toestaan	Bluetooth in-/uitschakelen

PIM-beheer

Exchange Actieve Synchronisatie

Instellen van de ActiveSync-account op het eindgebruikerapparaat

Naam rekening	Naam e-mailaccount
Server hostnaam	Serveradres/FQDN
Domeinnaam	Serverdomein
E-mailadres	E-mailadres
Gebruikersnaam	Gebruikersnaam
Wachtwoord gebruiker	Optioneel kun je hier al een wachtwoord aan de gebruiker koppelen
SSL gebruiken	SSL-verbinding gebruiken
Synchronisatie-interval	Hier kan het synchronisatie-interval worden ingesteld Handmatige synchronisatie = De gebruiker moet zijn e-mails downloaden en een handmatige synchronisatie uitvoeren.
Leeftijd filter	Tijdsduur tot de e-mails gesynchroniseerd moeten worden Geen filter = onbeperkt
Log Niveau	Vaststelling van de logboekniveaus voor ActiveSync-verkeer
E-mail synchroniseren	Geactiveerd = e-mails worden gesynchroniseerd
Contacten synchroniseren	Geactiveerd = contacten worden gesynchroniseerd
Kalender synchroniseren	Geactiveerd = kalender is gesynchroniseerd
Taken synchroniseren	Geactiveerd = taken zijn gesynchroniseerd

e-mail

POP3/IMAP4-accounts aanmaken op het apparaat van de eindgebruiker.

Account Beschrijving	Naam e-mailaccount
Naam afzender	Weergegeven afzendernaam
Domeinnaam	Domeinnaam voor het e-mailaccount
E-mailadres	E-mailadres gebruiker
Gebruikersnaam	Gebruikersnaam
Wachtwoord gebruiker	Optioneel kun je hier al een wachtwoord aan de gebruiker koppelen
Alternatieve uitgaande servergegevens	Hier kan worden gedefinieerd of er andere referenties nodig zijn voor de uitgaande server
Uitgaande domeinnaam	Uitgaande domeinnaam
Uitgaande server gebruikersnaam	Uitgaande server gebruikersnaam
Uitgaand serverwachtwoord	Uitgaand serverwachtwoord
E-mail Protocol	POP3 of IMAP4 kan worden gebruikt als protocol.
Hostnaam inkomende mailserver	Inkomende mailserver hostnaam
SSL gebruiken voor inkomende e-mails	SSL gebruiken voor inkomende e-mails
Hostnaam uitgaande mailserver	Hostnaam uitgaande mailserver
SSL gebruiken voor uitgaande e-mails	SSL gebruiken voor uitgaande e-mails
Uitgaande serververificatie	Een uitgaande serververificatie is vereist
Synchronisatie-interval	Hier kan het synchronisatie-interval worden ingesteld Handmatige synchronisatie = De gebruiker moet zijn e-mails downloaden en een handmatige synchronisatie uitvoeren.
Leeftijd filter	Tijdsduur tot de e-mails gesynchroniseerd moeten worden Geen filter = onbeperkt

App-beheer

Enterprise App Manager

Geïnstalleerde apps

Hier is een lijst van de apps die momenteel zijn geïnstalleerd op het apparaat dat wordt weergegeven.

Verplichte apps

Hier kun je een lijst configureren van apps die verplicht zijn op het apparaat.

Deze lijst wordt elke keer gecontroleerd als het apparaat verbinding maakt met de MDM en installeert alle apps op deze lijst die toevallig niet geïnstalleerd zijn op het apparaat, ongeacht of de app verwijderd is of nooit eerder geïnstalleerd is.

Je kunt Windows 10 In-House Apps uploaden en ze vervolgens toevoegen aan deze lijst of je kunt Microsoft Office configuraties toevoegen die vooraf moeten worden geconfigureerd in "Algemene instellingen" > "Appbeheer" > "Microsoft Office".

Beperkingen voor systeemtoepassingen

Inbox-apps
Wekkers en klok toestaan
Rekenmachine toestaan
Camera toestaan
Contactondersteuning toestaan
Cortana toestaan
Bestandsbeheer toestaan
Aan de slag
Sta Groove Muziek toe
Kaarten toestaan
Berichten toestaan
Microsoft Edge toestaan
Films en tv toestaan
Geld toestaan
Nieuws
OneDrive toestaan
OneNote toestaan
Outlook Agenda en Mail toestaan
Mensen toestaan
Telefoon toestaan
Foto's toestaan
Powerpoint toestaan
Instellingen toestaan
Skype toestaan
Sport toestaan
Toestaan Winkel
Voice Recorder toestaan
Portemonnee toestaan
Weer toestaan

Windows Feedback Hub toestaan
Word toestaan
Xbox toestaan

Pagina's instellen
Accounts Werkplek toestaan
Geavanceerde info toestaan
Apps toestaan in de hoek
Blokkeren en filteren toestaan
Kleurprofiel toestaan
Rijmodus toestaan
E-mail en accounts toestaan
Equalizer toestaan
Toetsenbord toestaan
Navigatiebalk toestaan
Sta netwerk vliegtuigmodus toe
Delen via het netwerk toestaan
Netwerkservices toestaan
Netwerk Wi-Fi toestaan
Bluetooth voor pc-systeem toestaan
Uw apparaat beoordelen toestaan
Herstel bijwerken toestaan
Delen toestaan
Start toestaan
Tijd Taal
Tijd Regio
Windows standaard vergrendelscherm toestaan
Werk of school account toestaan

Zwarte lijsten en witte lijsten

Onder "Black- & Whitelisting" kun je kiezen tussen de modus "Whitelist" en de modus "Blacklist".

Whitelist	Alleen apps en services die aan de lijst zijn toegevoegd, kunnen op het eindgebruikerapparaat worden geïnstalleerd. Als deze al vooraf zijn geïnstalleerd op het eindgebruikerapparaat, worden ze geactiveerd en ingesteld, zodat de gebruiker ze kan uitvoeren.
	Alle andere apps die niet aan de lijst zijn toegevoegd, kunnen niet op het eindgebruikerapparaat worden geïnstalleerd. Als deze al vooraf zijn geïnstalleerd op het eindgebruikerapparaat, worden ze gedeactiveerd en ingesteld, zodat de gebruiker ze niet kan uitvoeren.
Zwarte lijst	Apps en services die aan de lijst zijn toegevoegd, kunnen niet op het eindgebruikerapparaat worden geïnstalleerd. Als deze al vooraf zijn geïnstalleerd op het eindgebruikerapparaat, worden ze gedeactiveerd en ingesteld, zodat de gebruiker ze niet kan uitvoeren.
	Alle andere apps die niet aan de lijst zijn toegevoegd, kunnen op het eindgebruikerapparaat worden geïnstalleerd. Als deze al vooraf zijn geïnstalleerd op het eindgebruikerapparaat, worden ze geactiveerd en ingesteld, zodat de gebruiker ze kan uitvoeren.

Via de , voeg je extra apps of diensten toe aan de lijst die momenteel wordt gebruikt.

Via de , kunt u extra apps of services toevoegen aan de momenteel inactieve lijst.

Je kunt een app toevoegen vanuit de "Windows App Store" of direct een "App Identifier" invoeren om toe te voegen aan de zwarte of witte lijst.

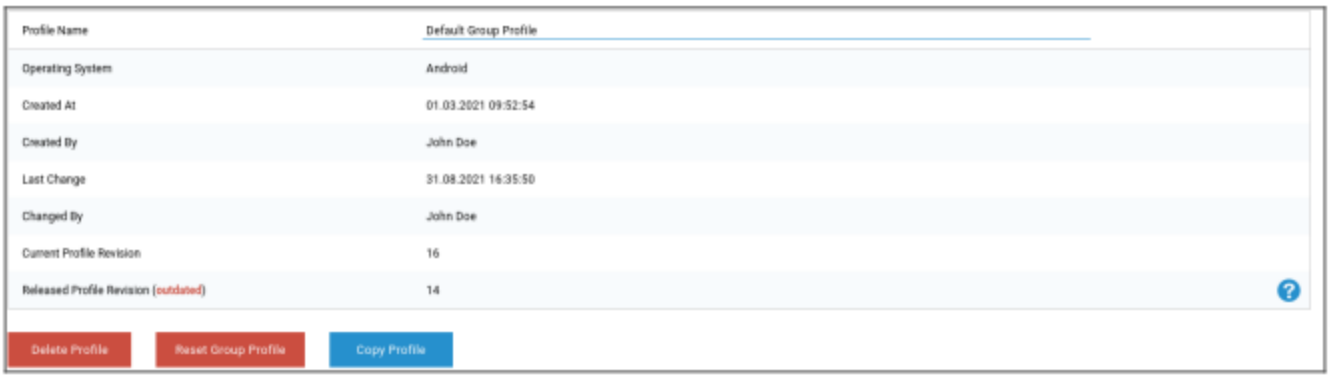
MacOS-configuratie

Afhankelijk van of je een profiel of een apparaat hebt geselecteerd, zijn het scherm en de subpunten anders - let hier goed op!

Algemeen

Overzicht groepsprofiel (alleen op groepsniveau)

Wanneer je een groepsprofiel opent, krijg je een snel overzicht van het profiel.



Profielnaam	Naam van het profiel (kan hier worden gewijzigd)
Besturingssysteem	Besturingssysteem waar het profiel voor is
Gemaakt op	Tijd van creatie
Gemaakt door	De maker van het profiel
Laatste wijziging	Tijdstip van laatste wijziging van het profiel
Veranderd door	Account die de laatste wijzigingen heeft aangebracht
Huidige profielherziening	Revisie van opgeslagen profielstatus
Vrijgegeven profiel Revisie	Toegewezen profielrevisie ("Nu toewijzen"). Als er "(verouderd)" achter de tekst staat, betekent dit dat je het profiel hebt opgeslagen maar nog niet hebt toegewezen, zodat de apparaten nog steeds een oudere versie krijgen.

Apparaatoverzicht (alleen op apparaatniveau)

Een beknopt overzicht van het apparaat.

Naam apparaat	Naam apparaat
Model	Model
Besturingssysteem	Besturingssysteem
Serienummer	Serienummer van het apparaat
Apparaateigendom	Het geconfigureerde eigenaarschapstype
Type apparaat	Het type apparaat
Conform	Geeft aan of het apparaat voldoet
IP-adres	Het IP-adres vanwaar het apparaat verbinding heeft met de server
Laatst gezien	Tijd van de laatste verbinding vanaf het apparaat
Laatste duw	Tijdstip van de laatste push die naar het apparaat is verzonden
Opdracht	Hier kunt u het apparaat verplaatsen naar een andere gebruiker of groep

Configuratie Revisie (alleen op apparaatniveau)

Hier krijg je een overzicht van welk groepsprofiel aan het apparaat is toegewezen.

Als je op het groepsprofiel klikt, krijg je direct toegang tot het profiel en kun je instellingen uitvoeren.

Met het symbool kun je de toegewezen apps terugzetten naar de instellingen van het groepsprofiel.

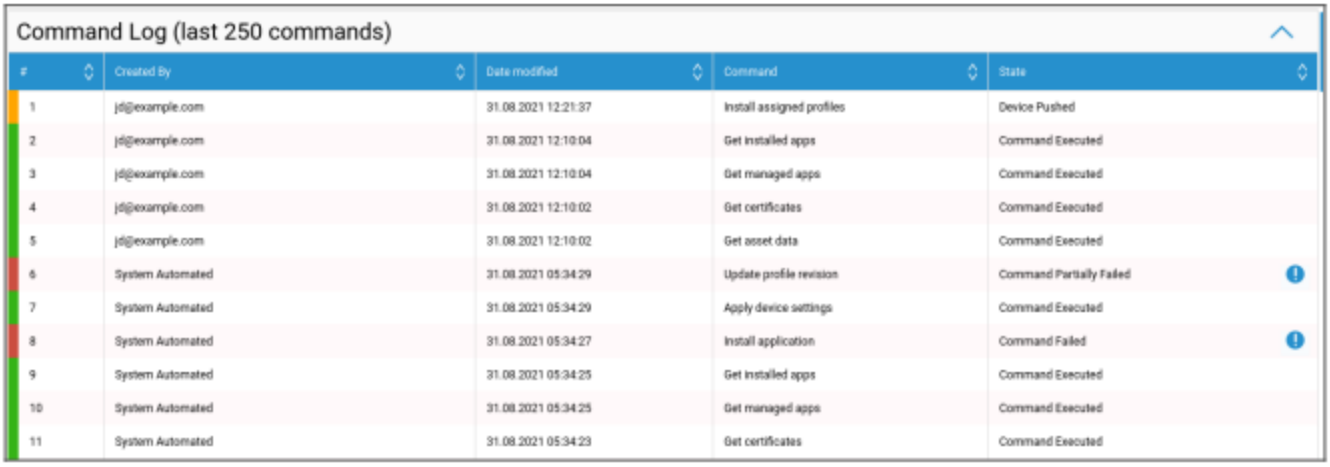
Met het symbool kun je het apparaatprofiel resetten zodat er helemaal geen instellingen zijn.

"Newer Revision available" geeft aan dat het groepsprofiel gewijzigd en opgeslagen is, maar niet toegewezen. Het groepsprofiel moet worden toegewezen met "Assign now" op groepsniveau om de wijzigingen toe te passen op de apparaten.

Apparaatlogboek (alleen op apparaatniveau)

Opdrachtlogboek

Hier kun je zien welke commando's zijn uitgegeven voor het apparaat en wat hun status is.



Commando's die zijn aangemaakt door "System Automated" worden automatisch aangemaakt door het systeem.

Mogelijke opdrachtstatussen

Apparaat ingedrukt	Er is een pushverzoek verzonden naar de pushservice (bijv. APNS) om het apparaat te vertellen terug verbinding te maken met de EMM-server.
Commando aangemaakt	De opdracht is aangemaakt in het systeem.
Opdracht verzonden	De opdracht werd naar het apparaat gestuurd nadat het verbinding had gemaakt met de server.
Opdracht uitgevoerd	De opdracht is succesvol uitgevoerd.
Opdracht mislukt	De opdracht is mislukt. *
Commando gedeeltelijk mislukt	Afhankelijk van het besturingssysteem van het apparaat kunnen sommige commando's gegroepeerd worden. Hierin zijn sommige delen van deze commandogroep mislukt. *
Opdracht uitgevoerd, uiteindelijk mislukt	Het commando werd uitgevoerd, maar misschien ook niet.
Commando verplaatst	De opdracht is opnieuw uitgevoerd door een gebruiker.
Afgedankt	De opdracht is verwijderd. Bijvoorbeeld omdat het is vervangen door een ander commando of omdat het apparaat opnieuw is aangemeld en oude commando's zijn verwijderd.

*Als er een uitroepteken achter het bericht staat, kun je meer informatie krijgen door met je cursor over het pictogram te gaan.

Activabeheer (alleen op apparaatniveau)

Apparaat info

Modelnummer	Modelnummer
Hostnaam	Hostnaam
Lokale hostnaam	Lokale hostnaam
Besturingssysteem	Besturingssysteem
OS versie	OS-versie
UDID	UDID
Vrij / Totaal geheugen	Vrij / Totaal geheugen

WiFi

IP-adres	IP-adres
WiFi MAC	WiFi MAC

Cellulair

Telefoonnummer	Telefoonnummer
Roaming-status	Roaming-status
Roaming (spraak/data)	Roaming (spraak/data)
IP-adres	IP-adres
Exploitant/vervoerder	Exploitant/vervoerder
SIM-dragernetwerk	Carrier-netwerk
Dragerversie	Dragerversie
ICCID	ICCID
Huidige MCC/MNC	Huidige MCC/MNC
SIM MCC/MNC	SIM MCC/MNC

Bluetooth

Bluetooth MAC	Bluetooth MAC

Updatebeheer (alleen op apparaatniveau)

Info bijwerken

Dit tabblad toont informatie over de instellingen voor systeemupdates op het apparaat.

Autocheck ingeschakeld	Als het systeem automatisch op updates controleert.
Automatische app-update ingeschakeld	Als het systeem app-updates automatisch installeert.
Automatische OS-updates ingeschakeld	Als het systeem os-updates automatisch installeert.
Automatische beveiligingsupdates ingeschakeld	Als het systeem automatisch beveiligingsupdates installeert.
App Update downloaden op de achtergrond ingeschakeld	Als het systeem app-updates downloadt op de achtergrond.
Catalogus URL	De URL naar de software-updatecatalogus die de client gebruikt.
Is standaard catalogus	Als "ja", dan is Catalog de standaard catalogus.
Periodieke controle uitvoeren	Als "ja", start dan een nieuwe scan.
Vorige scandatum	De datum van de laatste software-updatescan.
Vorig scanresultaat	De resultaatcode van de laatste software-updatescan.

Beveiligingsbeheer

Anti diefstal

Vegen en vergrendelen

Volledig wissen	Een opdracht verzenden om het apparaat te resetten
Ondernemingsvegen	Verwijder de MDM van het apparaat en verwijder alle MDM-gegevens (zoals accounts en apps).
Vergrendelscherm	Laat het apparaat terugkeren naar het vergrendelscherm

Beveiligingsconfiguratie

Wachtwoord

Code deactivering toegestaan	Bepaalt of de gebruiker gedwongen wordt om een pincode in te stellen. Door deze waarde in te stellen (en geen andere) wordt de gebruiker gedwongen om een wachtwoord in te voeren, zonder een lengte of kwaliteit op te leggen.
Eenvoudige waarde toestaan	De gebruiker toestaan om dezelfde, escalerende en reducerende nummerreeksen te gebruiken (bijv. 1234, 1111)
Alfanumerieke waarde vereisen	Wachtwoorden moeten ten minste één letter bevatten
Minimale lengte wachtwoord	Minimale wachtwoordlengte
Minimumaantal complexe tekens	Minimaal aantal alfanumerieke symbolen in het wachtwoord
Maximale leeftijd wachtwoord	Aantal dagen waarna het wachtwoord moet worden gewijzigd
Maximale automatische vergrendeling	Maximale tijd waarna het apparaat wordt vergrendeld
Maximale respijtperiode voor apparaatvergrendeling	De tijd dat het apparaat kan worden vergrendeld zonder te vragen om het wachtwoord bij het ontgrendelen
Maximumleeftijd wachtwoord (1-730 dagen, of geen)	Dagen waarna de wachtwoordcode moet worden gewijzigd
Wachtwoordgeschiedenis (1-50 wachtwoordcodes, of geen)	Aantal unieke wachtwoorden voor hergebruik

Certificaat

PKCS#1	
Beschrijving	Voer een beschrijving in voor het certificaat
Geloofsbrief	Een pkcs1-bestand uploaden

PKCS#12	
Beschrijving	Voer een beschrijving in voor het certificaat
Geloofsbrief	Upload een pkcs12-bestand

Beperkende instellingen

Functionaliteit van het apparaat

Camera toestaan	Het gebruik van de camera toestaan
Game Center toestaan	Als dit niet het geval is, wordt Game Center uitgeschakeld en wordt het pictogram verwijderd van het beginscherm.
Gamen met meerdere spelers toestaan	Als deze optie onwaar is, wordt multiplayergamen verboden.
Het toevoegen van Game Center-vrienden toestaan	Indien false, verbiedt deze optie het toevoegen van vrienden aan Game Center.
iCloud-fotobibliotheek toestaan	Indien ingesteld op false, wordt iCloud Photo Library uitgeschakeld. Foto's die niet volledig zijn gedownload van iCloud Photo Library naar het apparaat, worden verwijderd uit de lokale opslag.
Touch ID toestaan	Als deze optie onwaar is, wordt voorkomen dat Touch ID een apparaat ontgrendelt.

iCloud

Bepaalde functies blokkeren tijdens het koppelen van iCloud

Document sync toestaan	Document sync toestaan
Synchronisatie van iCloud-sleutelhanger toestaan	Synchronisatie van iCloud-sleutelhanger toestaan
iCloud notities toestaan	Indien false, sluit MacOS iCloud Notes-diensten uit.
iCloud BTMM toestaan	Indien false, schakelt MacOS Back to My Mac iCloud-service uit.
iCloud FMM toestaan	Indien false, schakelt MacOS Zoek mijn Mac iCloud-service uit.
iCloud bladwijzers toestaan	Indien false, wordt de synchronisatie van MacOS iCloud-bladwijzers uitgeschakeld.
iCloud Mail toestaan	Indien false, worden de iCloud-diensten van MacOS Mail uitgeschakeld.
iCloud Agenda toestaan	Indien false, worden MacOS Cloud iCloud-diensten niet toegestaan.

Herinneringen via iCloud toestaan	Indien false, worden iCloud Herinneringsservices uitgeschakeld.
iCloud Adresboek toestaan	Indien false, worden MacOS iCloud Adresboekservices uitgeschakeld.

Mediabeheer

Uitwerpen bij afmelden	Alle verwisselbare media uitwerpen bij afmelden
Netwerk toestaan	Toegang verlenen voor netwerkmedia
Interne schijf toestaan	Toegang voor interne schijf toestaan.
Verificatie vereisen	Authenticatie vereist voor het gebruik van deze media
Alleen lezen	De gebruiker kan alleen gegevens lezen van de media
Externe schijf toestaan	Toegang voor externe schijf toestaan.
Verificatie vereisen	Authenticatie vereist voor het gebruik van deze media
Alleen lezen	De gebruiker kan alleen gegevens lezen van de media
Gebruik van schijfafbeeldingen toestaan	Toegang verlenen voor afbeeldingen.
Verificatie vereisen	Authenticatie vereist voor het gebruik van deze media
Alleen lezen	De gebruiker kan alleen gegevens lezen van de media
Gebruik van DVD-RAM's toestaan	Toegang voor DVD-RAM-schijf toestaan.
Verificatie vereisen	Authenticatie vereist voor het gebruik van deze media
Alleen lezen	De gebruiker kan alleen gegevens lezen van de media
Gebruik van DVD's toestaan	Toegang voor DVD-schijf toestaan.
Verificatie vereisen	Authenticatie vereist voor het gebruik van deze media
Gebruik van CD's toestaan	Toegang voor CD-schijf toestaan.
Verificatie vereisen	Authenticatie vereist voor het gebruik van deze media

Verbindingsbeheer

Wi-Fi

Hier kunt u Wi-Fi-verbindingen toevoegen en configureren

Service Set Identifier (SSID)	SSID van het netwerk waarmee de verbinding tot stand wordt gebracht
Automatisch lid worden	Automatisch lid worden voor het netwerk inschakelen
Verborgen netwerk	Inschakelen, als het AP het SSID niet uitzendt
Proxy-instelling	Configuratie van een proxy voor elk toegangspunt
Geen	Gebruik geen proxyserver
Handmatig	Een handmatige proxy instellen
Proxyserver URL	Adres voor toegang tot proxy-instellingen
Haven	Stel de poort in voor de proxy
Authenticatie	Gebruikersnaam voor de verificatie op de proxy
Wachtwoord	Wachtwoord voor de verificatie op de proxy
Automatisch	Automatisch een proxy instellen
Proxyserver URL	URL voor het proxy-instellingenbestand
Type beveiliging	Beveiligingstype instellen voor het AP
WEP	
Wachtwoord	Wachtwoord voor het AP
WPA/WPA2	
Wachtwoord	Wachtwoord voor het AP
WEP Onderneming - WPA / WPA2 Onderneming / Elke onderneming	Zie tabel Fout: Verwijzingsbron hieronder niet gevonden
Geen	Geen beveiliging instellen
Willekeurige MAC-adressen uitschakelen	Schakelt de randomisatie van MAC-adressen voor dat Wi-Fi-netwerk uit terwijl het verbonden is met het netwerk. Dit toont ook een privacywaarschuwing in

	Instellingen die aangeeft dat het netwerk verminderde privacybescherming heeft.

Wi-Fi configuratie voor bedrijven

Opmerking: Alleen beschikbaar als "Beveiligingstype" is ingesteld op een Bedrijfstype.

Protocollen	Authenticatieprotocol ondersteund op doelnetwerk
TLS	Gebruik in-/uitschakelen
TTLS	Gebruik in-/uitschakelen
Innerlijke Authenticaties	Authenticatieprotocol dat moet worden gebruikt: PAP, CHAP, MSCHAP, MSCHAPv2
LEAP	Gebruik in-/uitschakelen
PEAP	Gebruik in-/uitschakelen
EAP-FAST	Gebruik in-/uitschakelen
EAP-SIM	Gebruik in-/uitschakelen
Gebruik PAC	Gebruik van PAC (beschermde toegangscontrole)
Voorziening PAC	Configuratie van voorziening PAC
PAC anoniem aanbieden	Anoniem verstrekken van PAC
Authenticatie	
Gebruikersnaam	Gebruikersnaam verificatie
Gebruik geen Per aansluiting Wachtwoord	Gebruik geen wachtwoord per verbinding
Wachtwoord	Het te gebruiken wachtwoord
Identiteitscertificaat	Verificatiecertificaat uploaden/selecteren
Uiterlijke identiteit	Identiteit die van buitenaf zichtbaar is
Vertrouwen	
Betrouwbaar certificaat 1	Eerste vertrouwde certificaat uploaden
Betrouwbaar certificaat 2	Tweede vertrouwde certificaat uploaden

Betrouwbaar certificaat 3	Derde vertrouwde certificaat uploaden
Vertrouwde server Certificaatnamen	De namen van de verwachte servercertificaten (in een door komma's gescheiden lijst)

VPN

Afhankelijk van het geselecteerde verbindingstype kunnen verschillende velden zichtbaar zijn.

Naam verbinding	Naam van het VPN-profiel
VPN-type	
VPN	Al het netwerkverkeer van het apparaat wordt via een VPN-verbinding geleid.
Type aansluiting	Type VPN-verbinding tot stand brengen
IPsec (cisco)	IPsec-protocol door cisco
L2TP	L2TP-protocol
Aangepaste SSL	Verbinding via aangepaste SSL
IKEv2	IKEv2-protocol
Proxy-instelling	Configuratie van een proxy voor de VPN-verbinding
Geen	Geen volmacht vaststellen
Handmatig	Handmatig een proxy aanmaken
Proxyserver URL	Adres voor toegang tot Proxy-instellingen
Haven	Stel de poort in voor de proxy
Authenticatie	Gebruikersnaam voor de verificatie bij de proxy
Wachtwoord	Wachtwoord voor de verificatie bij de proxy
Automatisch	Automatisch een proxy instellen
Proxyserver URL	URL voor toegang tot de proxy-instellingen

HTTP-proxy

Type volmacht	
Handmatig	Handmatig een proxy instellen
Proxyserver URL	Adres voor toegang tot de proxy-instellingen
Haven	Proxy-poort instellen
Authenticatie	Gebruikersnaam voor de verificatie bij de proxy
Wachtwoord	Wachtwoord voor de verificatie bij de proxy
Automatisch	Automatisch een proxy instellen
Proxy PAC URL	Proxy PAC URL
Directe verbinding toestaan als PAC onbereikbaar is	Directe verbinding toestaan (zonder VPN) als PAC onbereikbaar is
Proxy omzeilen om toegang te krijgen tot besloten netwerken	Proxy omzeilen om toegang te krijgen tot besloten interne netwerken

AirPrint

IP-adres	IP-adres printer
Bronnenpad	Definitief pad naar het AirPrint-apparaat

AirPlay

Naam apparaat	Naam apparaat
Wachtwoord	Wachtwoord koppelen
Whitelist	Definieer een lijst met apparaten waarmee het apparaat zichzelf exclusief kan koppelen

PIM-beheer

Exchange Actieve Synchronisatie

Naam rekening	Naam van de rekening.
E-mailadres	Het adres van de account (bijv. max@company.com)
Server hostnaam	Interne hostnaam
Inlognaam	"Domain" en "Login Name" moeten leeg zijn om het apparaat om een gebruiker te laten vragen.
Domein	"Domain" en "Login Name" moeten leeg zijn om het apparaat om een gebruiker te laten vragen. Als een ACL-gatewayconfiguratie is ingeschakeld en het veld Domein niet leeg is, zal de AppTec360 Universal Gateway het apparaat authenticeren met de volgende naam "Domeinnaam".
Wachtwoord	Het wachtwoord voor de account (bijv. secretUserPassword)
Vroegere dagen van Mail to Sync	Het aantal afgelopen dagen van mail om te synchroniseren
SSL gebruiken	SSL gebruiken voor interne Exchange-host
Geavanceerde optie	Geavanceerde opties weergeven
Serverpoort	Interne poort
Serverpad	Intern pad
Externe hostnaam	Externe host
Externe poort	Externe poort
Extern pad	Extern pad
SSL gebruiken voor extern Uitwisselingshost	SSL gebruiken voor externe Exchange-host

e-mail

POP3 / IMAP-accounts instellen op het apparaat van de eindgebruiker

Account Beschrijving	Naam van e-mailaccounts
Type rekening	
IMAP	
Pad Voorvoegsel	Het padvoorvoegsel voor speciale mappen
POP	
Gebruikersnaam	Weergavenaam gebruiker
E-mailadres	E-mailadres gebruiker

Inkomende post	Inkomende serverinstellingen
Adres mailserver	Adres mailserver
Mail server poort	Mail server poort
Gebruikersnaam	Respectieve gebruikersnaam
Type verificatie	Type verificatie
Geen	Geen verificatietype
Wachtwoord (alleen op apparaatniveau)	Wachtwoord
MDM uitdaging-antwoord	
NTLM	NTLM-authenticatie
HTTP MD5 Digest	
SSL gebruiken	Gebruik SSL, indien nodig

Uitgaande post	Instellingen uitgaande server
Adres mailserver	Adres mailserver
Mail server poort	Mail server poort
Gebruikersnaam	Respectievelijke gebruikersnaam
Type verificatie	
Geen	Geen verificatiemethode
Wachtwoord (alleen op apparaatniveau)	Wachtwoord
MDM uitdaging-antwoord	
NTLM	NTLM-authenticatie
HTTP MD5 Digest	
SSL gebruiken	Gebruik SSL, indien nodig
Uitgaand wachtwoord hetzelfde als inkomend wachtwoord	Uitgaand wachtwoord hetzelfde als inkomend wachtwoord
Alleen gebruiken in post	Activeer als alle uitgaande e-mails moeten worden verzonden via de Mail-App

CalDav

Het opzetten en distribueren van een CalDav-account configureren

Account Beschrijving	Weergavenaam van de account
Hostnaam	Hostnaam en/of IP-adres
Haven	Poort van het CalDav-account
Belangrijkste URL	Belangrijkste URL van de rekening
Gebruikersnaam	Respectieve CalDav-gebruikersnaam
Wachtwoord (alleen op apparaatniveau)	Respectievelijk CalDav-wachtwoord
SSL gebruiken	Gebruik SSL, indien nodig

CardDav

Configureer de instelling en distributie van een CardDav Account

Account Beschrijving	Weergavenaam van de account
Hostnaam	Hostnaam en/of IP-adres
Haven	Poort van de CardDav-account
Belangrijkste URL	Belangrijkste URL van de rekening
Gebruikersnaam	Respectieve CardDav-gebruikersnaam
Wachtwoord (alleen op apparaatniveau)	Respectievelijk CardDav-wachtwoord
SSL gebruiken	Gebruik SSL, indien nodig

LDAP

Stel in dit gebied een LDAP-verbinding in om een dynamische certificaatuitwisseling mogelijk te maken tussen het eindgebruikersapparaat en de Active Directory.

Merk op dat de geselecteerde gebruiker de respectieve leesrechten nodig heeft.

Account Beschrijving	Account Beschrijving
Gebruikersnaam account	Gebruiker voor LDAP-toegang
Wachtwoord	Wachtwoord voor LDAP-toegang
Hostnaam account	Hostnaam/IP-adres LDAP-server
SSL gebruiken	Gebruik SSL, indien nodig

In het tweede deel kun je individuele filters definiëren voor het zoeken in het LDAP-register.

Beschrijving	Toepassingsgebied	Basis zoeken
Beschrijving filter	Zoekniveau in het LDAP-register	Het individuele filter definiëren

Dashboard en rapportage

Dashboard-instellingen

Hier kun je zien welke dashboards er zijn, ze bewerken of nieuwe aanmaken. Elk Dashboard heeft zijn eigen set weer te geven gegevens en grafiekconfiguratie.

Dashboard Instellingen Controle

Openbaar	Hiermee wordt het Dashboard openbaar gemaakt, zodat andere gebruikers het Dashboard kunnen zien. De gebruikers moeten natuurlijk kunnen inloggen en Dashboards kunnen bekijken. Als "Openbaar" niet is geactiveerd, kan alleen de maker het Dashboard zien.
Standaard	Stelt het Dashboard in als standaard, zodat het automatisch wordt geopend de volgende keer dat je de Dashboard-weergave opent.
	Het dashboard en de bijbehorende grafieken weergeven
	Het dashboard verwijderen
	Dashboardnaam en -instellingen bewerken
	Maak een kopie van het dashboard
	Een compleet nieuw dashboard toevoegen

Dashboardweergave

Hiermee worden de gegevens en grafieken van het geselecteerde Dashboard getoond en kun je deze ook wijzigen.

Dashboardbediening

	Hiermee kunt u definiëren welke gegevens worden getoond in het Dashboard, hoeveel gegevens worden getoond en in welke grootte deze gegevens worden getoond.
	Brengt je terug naar het dashboardoverzicht
	Stelt het momenteel geopende Dashboard terug op de standaardwaarde
	Slaat alle wijzigingen op die je hebt aangebracht in het momenteel geopende Dashboard (bijvoorbeeld welke gegevens je wilt weergeven)
	Grafiektype wijzigen in zuilgrafiek
	Grafiektype wijzigen in cirkeldiagram
	Verander grafiektype in donutgrafiek
	Verander kaarttype in polaire gebiedskaart
	Sorteervolgorde wijzigen

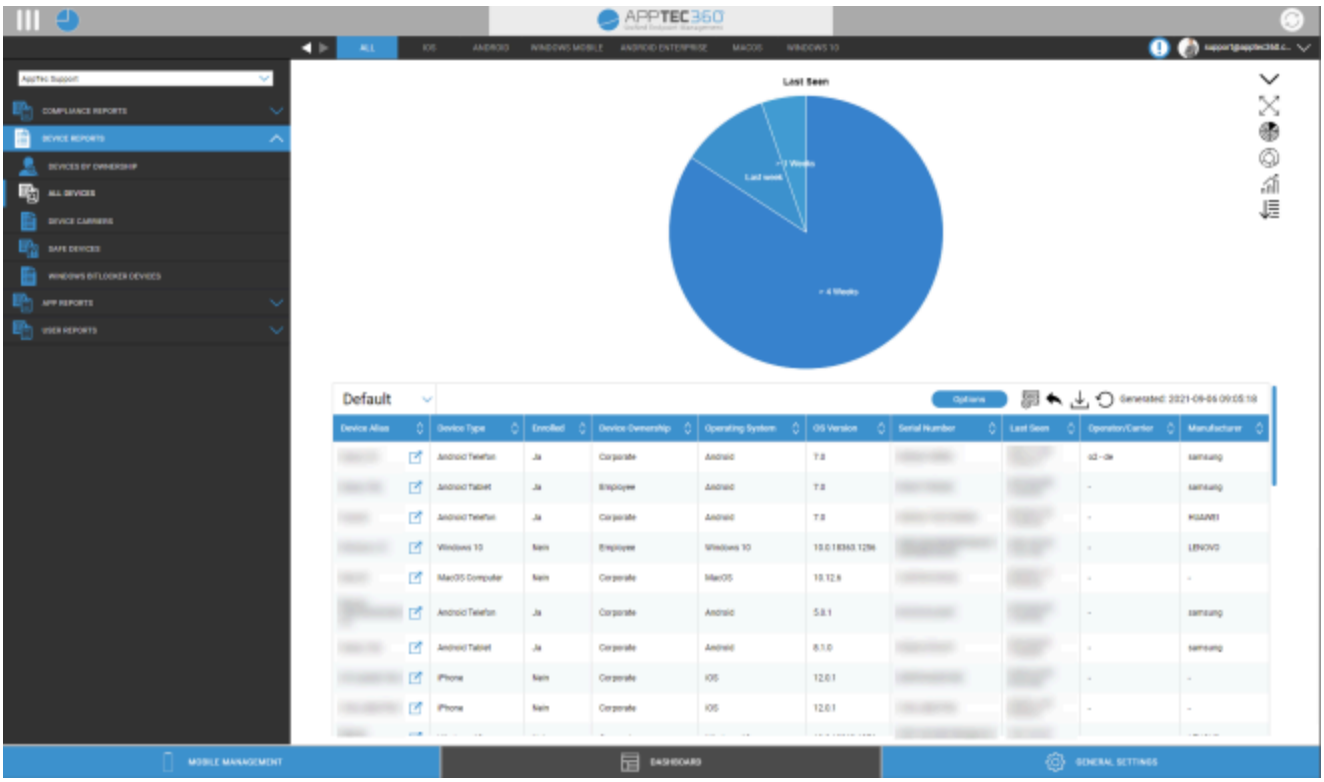
Uitgebreide rapportage

De "Uitgebreide rapportage" biedt gedetailleerde overzichten en grafieken over apparaat- en gebruikersinformatie.

Er zijn een paar standaardrapporten, maar ze kunnen allemaal handmatig worden gewijzigd om gegevens toe te voegen of te verwijderen.

Houd er rekening mee dat je alleen handmatig kunt wijzigen welke gegevens worden weergegeven. De geselecteerde rapportcategorie bepaalt op welke gegevens dit gebaseerd is. Je zult bijvoorbeeld nooit Android-apparaten kunnen zien in het iOS-rapport in Apparaatrapporten Alle apparaten iOS

Linksboven kun je de gegevens van de rapportage beperken tot een bepaalde groep (en al zijn subgroepen). Standaard is dit ingesteld op je hoofdnode, dus er wordt rekening gehouden met ALLE apparaten en gebruikers.



Uitgebreide rapportagecontrole

In elk overzicht kun je de volgende functies gebruiken om het rapport naar wens aan te passen:

	Verberg grafiek (Als grafiek wordt getoond)
	Toon grafiek (Als grafiek verborgen is)
	Grafiek uitvouwen (Als de grafiek is samengevouwen)
	Grafiek samenvouwen (Als de grafiek is uitgebreid)
	Grafiektype wijzigen in zuilgrafiek
	Grafiektype wijzigen in cirkeldiagram
	Verander grafiektype in donutgrafiek
	Verander kaarttype in polaire gebiedskaart
	Sorteervolgorde wijzigen
	Wijzig de volgende onderdelen van het weergegeven overzicht: • Kolommen toevoegen/verwijderen • Geef de volgorde op waarin de kolommen worden weergegeven • Toon/verberg de grafiek boven de tabel • Selecteer de kolom die wordt gebruikt voor de grafiek • De gegevens van je tabel filteren
	Open de setupmanager om verschillende rapporten op te slaan en te laden
	Stelt het huidig geopende rapport terug op standaard
	Het huidige rapport exporteren als .csv-bestand
	Gegevens opnieuw genereren en het huidige rapport opnieuw laden

Je vindt een lijst met alle standaardrapporten op de volgende pagina's.

Rapporten over naleving

Apparaten met wortels

Overzicht van de apparaten die geroot/gejailbreakt zijn.

Standaard kolommen van dit rapport:

Alias apparaat
Apparaateigenaar
E-mail
Besturingssysteem
Telefoonnummer
Laatst gezien
Fabrikant

Roaming-apparaten

Overzicht van alle apparaten die roamen

Standaard kolommen van dit rapport:

Alias apparaat
Apparaateigenaar
E-mail
Type apparaat
Besturingssysteem
Telefoonnummer
Laatst gezien

Apparaten met roaming

Overzicht van alle apparaten die roaming hebben geactiveerd, maar niet noodzakelijk momenteel aan het roamen zijn.

Standaard kolommen van dit rapport:

Alias apparaat
Apparaateigenaar
E-mail
Type apparaat
Besturingssysteem
Telefoonnummer
Laatst gezien

Apparaten onder toezicht

Overzicht van alle apparaten die onder toezicht staan in de bewaakte modus (alleen iOS)

Standaard kolommen van dit rapport:

Alias apparaat
Apparaateigenaar
E-mail
Type apparaat
Laatst gezien

Inactieve apparaten

Overzicht van alle apparaten die de afgelopen 7 dagen geen verbinding hebben gemaakt met de server

Standaard kolommen van dit rapport:

Alias apparaat
Apparaateigenaar
E-mail
Type apparaat
Besturingssysteem
Laatst gezien

Apparaatrapporten

Apparaten naar eigendom

Hier kun je zien hoeveel apparaten momenteel zijn ingezet als bedrijfsapparaten (corporate devices) en werknemersapparaten (private devices).

Standaard kolommen van dit rapport:

Alias apparaat
Apparaateigenaar
Type apparaat
Apparaateigendom
Besturingssysteem

Alle apparaten

Hier zie je een overzicht van alle apparaten met de belangrijkste informatie.

Standaard kolommen van dit rapport:

Alias apparaat
Type apparaat
Ingeschreven
Apparaateigendom
Besturingssysteem
OS versie
Serienummer
Laatst gezien
Exploitant/vervoerder
Fabrikant

Apparaatdragers

Hier zie je een overzicht van de provider.

Standaard kolommen van dit rapport:

Alias apparaat
Apparaateigenaar
E-mail
Besturingssysteem
OS versie
Exploitant/vervoerder

SAFE-apparaten

Hier zie je een overzicht van welke apparaten SAFE Version gebruiken.

Omdat het overzicht en/of SAFE alleen beschikbaar is voor Samsung-apparaten, zie je onder dit punt niet de gebruikelijke tabbladen.

Standaard kolommen van dit rapport:

Alias apparaat
Apparaateigenaar
E-mail
Type apparaat
Laatst gezien
SAFE-versie

Windows BitLocker-apparaten

Hier zie je een overzicht van de Windows-apparaten die BitLocker gebruiken.

Standaard kolommen van dit rapport:

Alias apparaat
Apparaateigenaar
E-mail

BitLocker staat

App rapporten

Hier krijg je verschillende overzichten met betrekking tot apps. In al deze rapporten kun je op een item klikken om verder te zien welke versies op de apparaten zijn geïnstalleerd en hoe vaak. In deze weergave kun je weer op een specifieke versie klikken om te zien op welke apparaten deze specifieke versie is geïnstalleerd.

Opmerking: Het kan even duren voordat het systeem actuele informatie van het apparaat ontvangt. Bovendien worden de rapporten niet elke minuut bijgewerkt. Je moet misschien even geduld hebben om de huidige status te zien als je net een nieuwe app of versie hebt toegewezen. Als je het rapport handmatig opnieuw laadt, worden de meest recente gegevens getoond.

Geïnstalleerde apps

Hier krijg je een overzicht van alle geïnstalleerde apps.

Standaard kolommen van dit rapport:

Naam	Naam van de app en/of service
Identificatiecode	Definitieve app/service-ID
Totaal aantal	Hoe vaak deze app / service is geïnstalleerd op de apparaten van de eindgebruiker

Meest geïnstalleerde apps

Hier krijg je een overzicht van de apps die het meest zijn geïnstalleerd.

Standaard kolommen van dit rapport:

Naam	Naam van de app en/of service
Identificatiecode	Definitieve app/service-ID
Totaal aantal	Hoe vaak deze app / service is geïnstalleerd op de apparaten van de eindgebruiker

Verplichte apps

Hier krijg je een overzicht van verplichte (mandatory required) apps.

Standaard kolommen van dit rapport:

Naam	Naam van de app en/of service
Identificatiecode	Definitieve app/service-ID
App Bron	Om welke AppStore het gaat: • Google PlayStore (Android) • iTunes AppStore (iOS)
OS	Besturingssysteem

Apps op de zwarte lijst

Hier krijg je een overzicht van alle gedefinieerde apps op de zwarte lijst.

Standaard kolommen van dit rapport:

Naam	Naam van de app en/of service
Identificatiecode	Definitieve app/service-ID
App Bron	Om welke AppStore het gaat: • Google PlayStore (Android) • iTunes AppStore (iOS)
OS	Besturingssysteem

Rapporten van gebruikers

Tarief

Hier krijg je een overzicht van de telefoontarieven en simkaarten van je gebruikers.

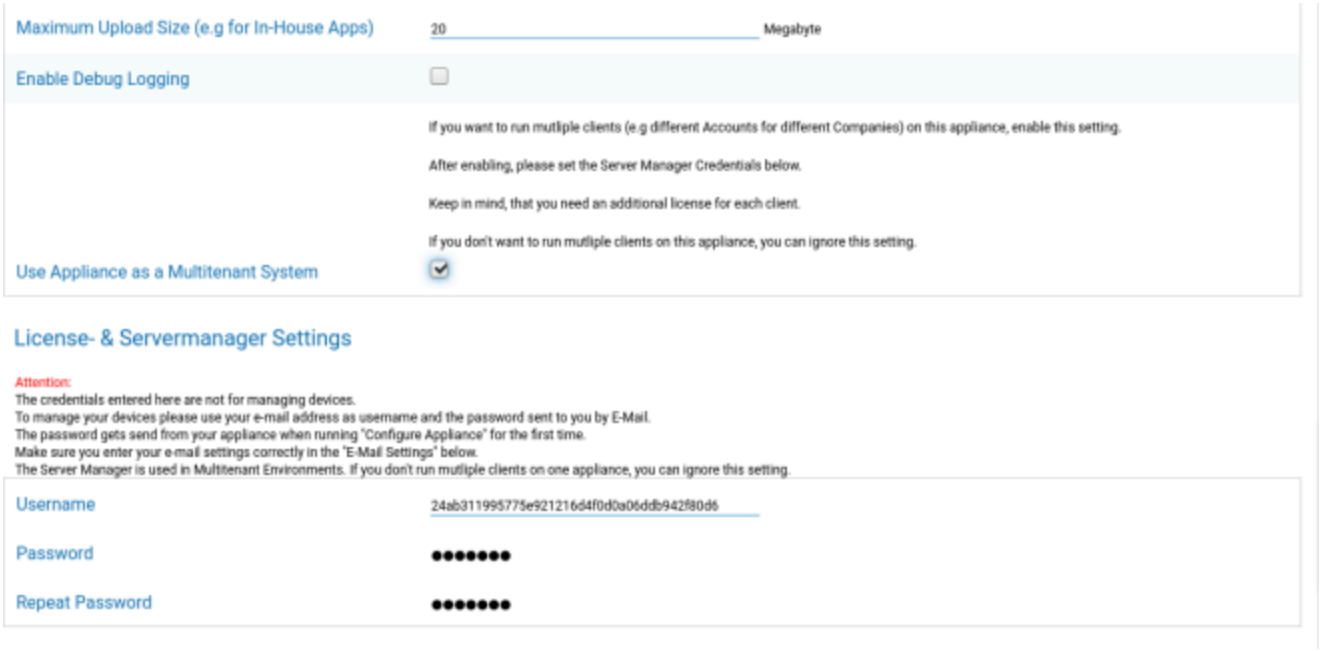
Standaard kolommen van dit rapport:

E-mail
Naam
telefoonnummer
drager
tarief
optie
prijs
contractgeannuleerd
contractStart
tijdensTijd
mobileAndData
dataVolume
multiSIM
type
simCardSerial1
simCardSerial2
simCardSerial3
pin1
pin2
puk1
puk2
noot

Beheer van meerdere huurders

De AppTec360 EMM kan meerdere afzonderlijke tenants hosten, elk met hun eigen gebruikers en groepen, machtigingen en globale instellingen.

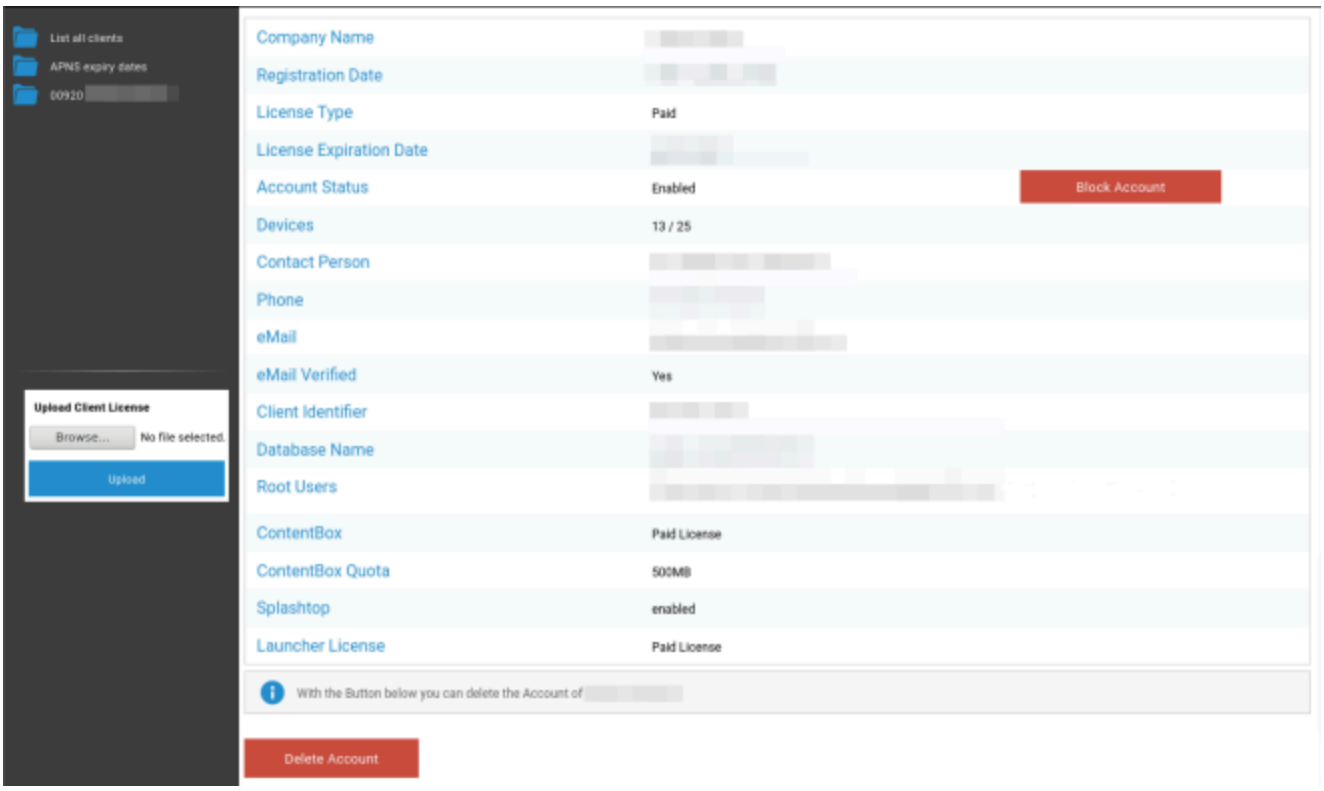
Om Multitenant mogelijkheden in te schakelen, moet je het inschakelen in de configuratie interface van de Appliance in "Stap Drie - Server Instellingen".



Stel in het nieuwe menu een gebruikersnaam en een wachtwoord in voor de Servermanager. Sla de instellingen op en voer "Configure Appliance" uit in "Stap Vijf - Licentieovereenkomst" om de instelling toe te passen.

Als de configuratie klaar is, kun je nu inloggen met de ingestelde referenties via de normale Mobile Management interface.

Na het inloggen zie je de volgende weergave.



Links zie je alle huurders (in dit geval slechts één met id 920) en rechts de informatie over deze klant. Je hebt ook de optie om de toegang tot de account te blokkeren en om de client te verwijderen (LET OP: hierdoor worden alle gegevens met betrekking tot die client verwijderd).

Aan de linkerkant kun je een nieuwe klantlicentie uploaden. Dit kan een licentie-update zijn voor een bestaande klant of een nieuwe licentie waarmee automatisch een nieuwe klant wordt aangemaakt. Wanneer een nieuwe client wordt aangemaakt, wordt automatisch een e-mail met het inlogwachtwoord verzonden naar het e-mailadres waarvoor de licentie is uitgegeven.

Om een nieuwe of bijgewerkte clientlicentie aan te schaffen (bijvoorbeeld als je meer apparaatlicenties nodig hebt), neem je contact op met je verkoopvertegenwoordiger.

Extra weergaven

Lijst van alle klanten

Toont een overzicht van alle clients in het systeem.

Klant-ID	Klant-ID
Identificatiecode	Klant
Database	Database
Bedrijfsnaam	Bedrijfsnaam
e-mail	Contactpersoon e-mail
Geverifieerd	Of de e-mail van de contactpersoon is geverifieerd of niet
Land	Land
Apparaten	Aantal geregistreerde apparaten
Registratiedatum	Tijdstip van de licentietoewijzing
Laatste aanmelding	Laatste login admin account
Licentie	Weergavetype licentie (gratis|betaald)
CB licentie	ContentBox licentietype (gratis|betaald)
Status	Huidige status AppTec-Client
Verlopen	Geeft weer of de licentie is verlopen
iOS	Aantal iOS-apparaten
Android	Aantal Android-apparaten
Windows mobiel	Aantal Windows Mobile apparaten
MacOS	Aantal MacOS-apparaten
Windows 10	Aantal Windows 10-apparaten
Android Onderneming	Aantal Android-apparaten voor bedrijven
IOS BYOD (Gebruikersregistratie)	Aantal IOS BYOD-apparaten (gebruikersregistratie)
IoT	Aantal IoT-apparaten

Vervaldata APNS

Toont een overzicht van alle vervaldata van APNS-certificaten van alle clients.

Klant-ID	Klant-ID
Bedrijfsnaam	Bedrijfsnaam
Vervaldatum	Vervaldatum voor het Apple APNS-certificaat
Info	Informatie over de vervaldatum

Neem contact op met

Nog meer vragen? Neem dan contact met ons op onder:

Voor algemene technische vragen

support@apptec360.com

+41 61 511 3210

Voor vragen over de installatie van een virtueel apparaat

consulting@apptec360.com

+41 61 511 3214

Disclaimer