AppTec360 Enterprise Mobile Manager & ContentBox

Administration Manual | Version 5.0 (202110)

Table of Contents

- General Overview
  - Introduction to AppTec360
  - Supported Device Operating Systems
  - Supported LDAP Directories
  - Explanation of the “Supervised-Mode” on Apple Devices
    - Available in the Supervised-Mode
    - Activate the supervised mode
    - Adding a device to the DEP
  - Explanation of Android Enterprise
    - What is Android Enterprise?
    - What are the requirements to use Android Enterprise?.
    - What are the available modes with Android Enterprise?
    - How can I assign apps to Android Enterprise devices?
  - Upload your own Apps to the Google Play Store
- Requirements and Installation
  - Requirements
    - System requirements
    - License key
    - IP-Address and DNS Resolution
    - SSL-Certificate
    - SMTP Server
    - Firewall Rules
  - Security Updates
    - Default Passwords of the Virtual Appliance
  - Configuration of the Virtual Appliance
    - Preparation
      - Configure from external host
    - Step One – Appliance License
    - Step Two – SSL Certificate
      - Automatic

- Custom
- Step Three – Server Settings
- Step Four – MySQL Setup
- Step Five – License Agreement
- Troubleshooting
- Security Recommendations

General Settings

Account Overview

- Account Information
  - Overview
  - Bug Report
  - Feature Request

Global Configuration

- eMail Settings
- eMail Templates
- SMS Enrollment

Privacy

- GPS Access

Role Based Access

- Role Management
- Role Assignments
  - Assignment of a role
- API Access
  - Access AppTec360 REST API
  - General Rules
  - Request example
  - Queries
  - Example Code in Python3

Apple Configuration

- APNS Certificate
  - Step 1
  - Step 2
  - Step 3
- Managed Access

- User Enrollment
- Shared iPad
- DEP
- Configurator & URL
  - Pool Enrollment URL's
  - MDM Profile – Apple Configurator

Android Configuration

- Android Configuration
- Auto Enrollment
- Android Enterprise
  - First Method: Android Enterprise Account (Google Account)
  - Second Method: G-Suite Account
  - Factory Reset Protection
- AE Enrollment
  - Method 1: QR Code Enrollment
  - Method 2: NFC Enrollment
  - Method 3: Google Account
- KNOX Enrollment
- Zero-Touch

Windows Configuration

- Windows Configuration

ContentBox

- Configuration

LDAP Configuration

- LDAP Overview

App Management

- In-House App DB
  - Android
  - iOS
  - MacOS
  - Windows 10
- App Settings
  - iOS App Settings
  - Android App Settings

- Third Party Apps
  - Android
  - iOS
- VPP / KNOX Premium
  - VPP Licenses
  - VPP Token
  - KNOX Premium Key
- App Store Settings
  - Region & Language
- AE Play Store
  - Approved Apps
  - Play Store Apps
  - Private Apps
  - Web Apps
  - Store Layout
- App Bundle

Remote Control

- TeamViewer
  - TeamViewer Connector
  - Install TeamViewer QuickSupport
  - Remote Control your device
  - Unattended Access
- Splashtop

Sim Card Management

- CSV Bulk Import
- Carrier & Tariff

Subscription Management

- Subscription Management

General Audit Log

- Audit Log
- Audit Log Settings

Certificate Management

Mobile Management

Mobile Management Screen

- Device filter
- Search window
- Options gear
- Navigation arrows

Administration account-settings

- User Information
- Console Settings
- Login Log

Corporate administration (Root-Node) in Mobile Management

- Create a Subgroup
- Rename Root Node
- Mass Enrollment
- Mass Assignment
- Quick App Administration
- CSV User Import

Group Management in Mobile Management

- Create a Subgroup
- Edit selected Group
- Delete selected Group
- Create a User
  - Create a new Admin-User

User Management in Mobile Management

- Add and enroll a Device

Profile Management in Mobile Management

- Create a profile
- Edit Profile
- Copy Profile
- Delete Profile
- Inheriting of Profiles

Device Management in Mobile Management

- IOS
  - Edit Device
  - Clear Passcode
  - Lock Device

- Shutdown Device
- Restart Device
- Alarm & Lostmode | Disable Lostmode
- Delete Device
- Wipe Device
- Enterprise Wipe | Remove MDM
- Send Message
- TeamViewer Remote Control
- Send Enrollment Request

Android

- Edit Device
- Clear Passcode
- Lock Device
- Delete Device
- Wipe Device
- Remove MDM
- Send Message
- Transform to COPE Mode
- Send Enrollment Request
- Migrate Legacy Device

Windows

- Edit Device
- Delete Device
- Enterprise Wipe | Remove MDM
- TeamViewer Remote Control
- Send Enrollment Request

Content Management

- Group Files
- File Explorer
- Audit Trail
- Trash
- External Storage

Audit Log

iOS Configuration

- General
  - Group profile overview (only on group level)
  - General Information
  - Settings
  - Config Revision
  - Device Log (only on device level)
    - Command Log
    - Possible command statuses
- Asset Management (only on device level)
  - Asset Management (only on device level)
    - Device Info
    - Wi-Fi
    - Cellular
    - Bluetooth
- Security Management
  - Anti Theft (only on device level)
    - GPS Information (only on device level)
    - Wipe & Lock (only on device level)
    - Message (only on device level)
  - Security Configuration
    - Passcode
    - Certificate (only on device level)
    - Encryption
    - Single Sign-On
  - End of Life (only on device level)
    - Wipe (only on device level)
  - Restriction Settings
    - Device Functionality
    - iCloud
    - Security and Privacy
- BYOD
  - Built-In iOS Security (Container)
    - Activation
    - SecurePIM Password

- SecurePIM Security
- SecurePIM Browser
- Exchange

Connection Management

- Wi-Fi
  - Proxy Setup
  - Security Type
- VPN
  - VPN Type
    - VPN
    - Per-App VPN
  - Proxy Setup
- APN
- Cellular
- HTTP Proxy
- AirPrint
- AirPlay

PIM Management

- Exchange Active Sync
- eMail
  - Incoming Mail
  - Outgoing Mail
- CalDav
- Subscribed Calendars
- LDAP

Web Management

- Webclips
- Web Content Filter

App Management

- Enterprise App Manager
  - Installed Apps (only on device level)
  - Mandatory Apps
    - Installation-options
  - Web Apps

- Restriction & Settings
  - Blacklisted / Whitelisted Apps
  - SysApp Restrictions
  - App-VPN
  - App Settings
- Enterprise App Store
  - iTunes Apps
  - In-House
- Kiosk Mode
  - Application Type
    - Package
    - URL
  - Kiosk Mode Settings

Android Enterprise – Fully Managed Device Configuration

General

- Group profile overview (only on group level)
- Device Overview (only on device level)
- Config Revision (only on device level)
- Device Log (only on device level)
  - Command Log
  - Possible command statuses
- Device Settings
  - Client Configuration
  - Wallpaper

Asset Management (only on device level)

- Device Info
  - Wi-Fi
- Cellular
- Bluetooth

Security Management

- Anti Theft (only on device level)
  - GPS Information (only on device level)
  - Wipe & Lock (only on device level)
  - Message (only on device level)

- Security Configuration
  - Device Passcode
  - AntiVirus
- End of Life (only on device level)
  - Wipe (only on device level)
- Restriction Settings
  - Restrictions
- Certificate Management

Connection Management

- Wifi
  - Security Type
    - WEP
    - WPA/WPA2
    - 802.1x EAP
- VPN
  - VPN Type
    - VPN
    - Per-App VPN
- Restrictions

PIM Management

- Gmail Exchange

App Management

- Enterprise App Manager
  - Installed Apps (only on device level)
  - System Apps (only on device level)
  - Mandatory Apps
  - Black- & Whitelisting
  - AE System Apps
- Restrictions & Settings
  - App Management Settings
- Enterprise App Store
  - In-House
- Enterprise Play Store
  - AE Play Store
- Kiosk Mode & Launcher

- Kiosk Mode
- AppTec360 Launcher
- AppTec360 Settings

Remote Control

- Splashtop
- TeamViewer

Content Management

- ContentBox
- Secure Browser

Additional API

- Samsung KNOX
  - Restrictions
  - Email
  - Exchange
  - APN
  - Bluetooth
  - Connection

Android Enterprise – Fully Managed Device with-Work Profile (COPE)

General Explanation of COPE

Configuration of Profiles for COPE Devices

Reverting to AE Fully Managed Device

Android Enterprise – Container Configuration

General

- Profile Overview (only on profile level)
- Group profile overview (only on group level)
- Device Overview (only on device level)
- Config Revision
- Device Log (only on device level)
  - Command Log
  - Possible command statuses
- Device Settings
  - Client Configuration

- Wallpaper
- Asset Management (only on device level)
  - Device Info
    - Wi-Fi
  - Cellular
  - Bluetooth
- Security Management
  - Anti Theft (only on device level)
    - GPS Information (only on device level)
    - Wipe & Lock (only on device level)
    - Message (only on device level)
  - Security Configuration
    - Device Passcode
    - Container Passcode
    - AntiVirus
  - End of Life (only on device level)
    - Wipe (only on device level)
  - Restriction Settings
    - Restrictions
  - Certificate Management
- Connection Management
  - Wifi
    - Security Type
      - WEP
      - WPA/WPA2
      - 802.1x EAP
  - VPN
    - VPN Type
      - VPN
      - Per-App VPN
  - Restrictions
- PIM Management
  - Gmail Exchange
- App Management
  - Enterprise App Manager

- Installed Apps (only on device level)
- System Apps (only on device level)
- Mandatory Apps
- AE System Apps
- Restrictions & Settings
  - App Management Settings
- Enterprise App Store
  - In-House
- Enterprise Play Store
  - AE Play Store

Content Management

- ContentBox
- Secure Browser

Android Configuration

General

- Group profile overview (only on group level)
  - Device Overview (only on device level)
- Config Revision (only on device level)
- Device Log (only on device level)
  - Command Log
  - Possible command statuses
- Device Settings
  - Client Configuration
  - Wallpaper

Asset Management (only on device level)

- Asset Management
  - Device Info
  - Wi-Fi
  - Cellular
  - Bluetooth

Security Management

- Anti Theft (only on device level)
  - GPS Information (only on device level)
  - Wipe & Lock (only on device level)

- Message (only on device level)
- Security Configuration
  - Passcode
  - Encryption
  - AntiVirus
- End of Life (only on device level)
  - Wipe (only on device level)
- Restriction Settings
  - Restrictions
  - AE Device Owner

BYOD Container

- Android Enterprise
  - Android Enterprise
  - Gmail Exchange
  - AE System Apps
  - Container Passcode
- Samsung KNOX
  - Activation
  - Knox Passcode
  - Knox Security
  - Knox Exchange
  - Knox eMail
  - Knox Apps

Connection Management

- Wifi
  - Security Type
    - WEP
    - WPA/WPA2
    - 802.1x EAP
- VPN
- Restrictions
- APN
- Bluetooth

PIM Management

- Exchange

- eMail
- AE Gmail Exchange

App Management

- Enterprise App Manager
  - Installed Apps (only on device level)
  - System Apps (only on device level)
  - Mandatory Apps
  - AE System Apps
- Restrictions & Settings
  - Black- & Whitelisting
  - Sys App Restrictions
    - Samsung Apps
    - Huawei Apps
  - App Management Settings
- Enterprise App Store
  - Playstore
  - In-House
- Enterprise Play Store
- Kiosk Mode & Launcher
  - Kiosk Mode
  - AppTec360 Launcher
  - AppTec360 Settings

Remote Control

- Splashtop
- Teamviewer

Content Management

- Contentbox
- Secure Browser

Configuration Windows 10 PC

General

- Group profile overview (only on group level)
- Device Overview (only on device level)
- Settings
- Config Revision (only on device level)

- Device Log (only on device level)
  - Command Log
  - Possible command statuses
- Asset Management (only on device level)
  - Device Info
  - Cellular
  - Synchronization Info
- Security Management
  - Anti Theft (only on device level)
    - GPS Information (only on device level)
    - GPS Settings
  - Security Configuration
    - Passcode
    - Antivirus
    - Security Center
    - Firewall Configuration
    - Firewall Rules
  - Restriction Settings
    - Device Functionality
  - BitLocker
    - BitLocker Configuration
    - BitLocker State
  - Certificate Management
    - Certificate List
    - Certificate Configuration
    - SCEP
- Connection Management
  - Wifi
    - Security Type
    - Use Proxy Server
  - Wifi Restrictions
  - VPN
    - Connection type
    - Generic VPN Configurations
  - VPN Restrictions
  - Bluetooth
- PIM Management

- Exchange Active Sync
- eMail
- App Management
  - Enterprise App Manager
    - Installed Apps
    - Mandatory Apps
    - Sys App Restrictions
    - Black- & Whitelisting

MacOS Configuration

General

- Group profile overview (only on group level)
- Device Overview (only on device level)
- Config Revision (only on device level)
- Device Log (only on device level)
  - Command Log
  - Possible command statuses

Asset Management (only on device level)

- Device Info
- WiFi
- Cellular
- Bluetooth

Update Management (only on device level)

- Update Info

Security Management

- Anti Theft
  - Wipe & Lock
- Security Configuration
  - Passcode
  - Certificate
- Restriction Settings
  - Device Functionality
  - iCloud
  - Media Management

Connection Management

- Wi-Fi
  - Enterprise Wi-Fi Configuration
- VPN
- HTTP Proxy
- AirPrint
- AirPlay

PIM Management

- Exchange Active Sync
- eMail
- CalDav
- CardDav
- LDAP

Dashboard & Reporting

Dashboard Settings

Dashboard View

Extended Reporting

- Compliance Reports
  - Rooted Devices
  - Roaming Devices
  - Roaming Enabled Devices
  - Supervised Devices
  - Inactive Devices
- Device Reports
  - Devices by Ownership
  - All Devices
  - Device Carriers
  - SAFE Devices
  - Windows BitLocker Devices
- App Reports
  - Installed Apps
  - Most Installed Apps
  - Mandatory Apps
  - Blacklisted Apps
- User Reports

- Tariff
- Multitenant Management
  - Additional views
    - List all clients
    - APNS expiry dates
- Contact
  - For general technical questions
  - For questions related to the installation of a virtual appliance
- Disclaimer

General Overview

Introduction to AppTec360

AppTec's Enterprise-Mobile-Management-Solution offers the option to manage and configure all mobile devices with its intuitive management console. In this scenario, the EMM server can either run in your own surroundings or you can utilize our cloud based solution.

Even on the topic of a central installation of corporate applications on to smartphones, you have come to the right place. With the Enterprise Mobile Manager, you can distribute corporate applications and documents onto devices within seconds or block undesirable applications with white/blacklisting.

The usage of private devices in companies poses a new challenge for securing smartphones and tablets. Due to the fact that employees want to use their smartphones more and more, ITadministrators must protect a large number of different types of devices. We will help you with securing all devices and the sensitive data that is stored on them and manage them from an intuitive console.

Supported Device Operating Systems

AppTec360 offers support for iOS, Android and Windows devices. Please note that the functions capacity of the mentioned platforms can be different from one OS to another.

- Apple iOS 11.0 or higher*
- Apple macOS 10.11 or higher
- Google Android 4.4 or higher** on the Cloud Version
- Google Android 4.1 or higher** on the OnPrem Version
- MS Windows 10 or higher*** (Desktop-Computer, Notebook and Tablet)

**Please note that devices with iOS 10 or earlier cannot be enrolled due to drastic changes made by apple in the enrollment process.*

***Devices can be connected and configured even if they use a version that is no longer supported by the manufacturer. Please note that there may be features that require a certain Android Version. In support cases, we follow the official support of the manufacturer. In case of problems or bugs caused by an outdated version that is no longer supported by the manufacturer, we reserve the right to offer only limited support.*

****Home Version of Windows are not supported due to limitations of the Operating System. We highly recommend using an OS version which is still supported by the manufacturer. Not only for compatibility but also for security reasons. Therefore we recommend iOS 12 or higher and Android 9 or higher.*

Supported LDAP Directories

- Microsoft Active Directory
- Open LDAP

Up-To-Date Information on “Supported Device Operating Systems” and “Supported LDAP Directories” can be found here:

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

Explanation of the “Supervised-Mode” on Apple Devices

The Supervised-Mode represents an expanded interface for iOS devices.

On the respectively configured device, additional limitations, as they pertain to the functionality of the end user device, can be applied. These are also contained in the administration handbook and are so marked with a banner.

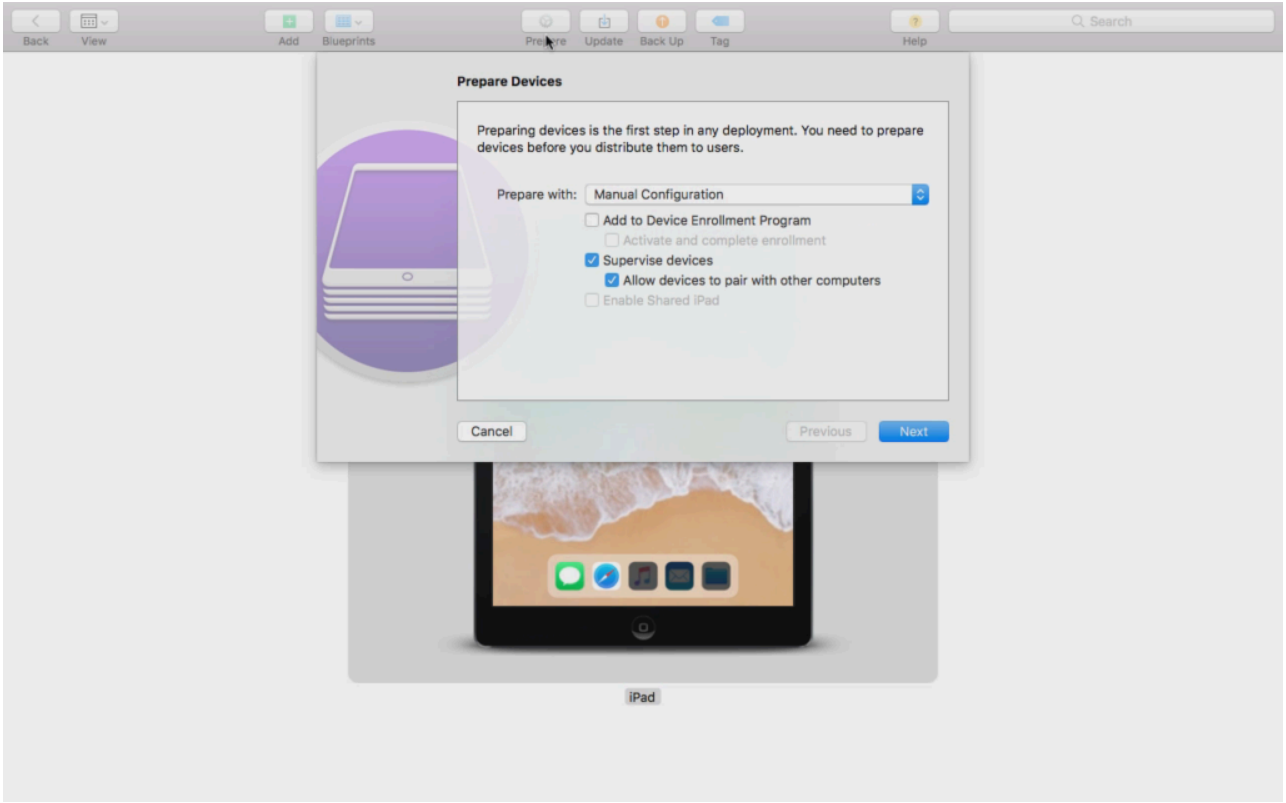
Available in the Supervised-Mode

The “Supervised-Mode” can be activated with the “Apple Configurator” program. The Apple Configurator can set the default settings on new iOS devices as a configuration-tool (via the USB interface).

The tool can not only install configuration profiles, but also apps. It is free of charge, but does require a Mac computer.

Activate the supervised mode

1. Open the Apple Configurator



2. Click on the device and choose „Prepare“
3. Choose „Manual Configuration“ and „Supervise devices“
4. Click on „Next“
5. (Optional) Now you can add a MDM Server where the device will be enrolled. The link for this can be found in „General Settings – iOS Configuration – Configurator & URL“ Choose your Organization or create a new one
6. Choose your Organization or create a new one
7. Choose which steps should be skipped in the initial setup and click on „Next“ (CAUTION: Proceeding will delete your device!)

Now your device will be put in supervised mode. This can take some minutes. After it is done, the device will reboot.

Now you device is supervised!

Adding a device to the DEP

You can also add devices to the DEP (Device Enrollment Programm) using the Apple Configurator, if your devices are on iOS 11 or higher.

More Information about DEP: https://www.apple.com/business/dep/

Follow the same steps like you would supervise a device and additionally check “Add to Device Enrollment Programm“. You will be asked for your DEP login data if you never before logged into DEP with the Apple Configurator.

After the Process is completed, the device can be found in the DEP Server “Devices Added by Apple Configurator 2”. You can now use this Server and connect it to the management console or transfer the device to an already existing server.

You now successfully added a device to the DEP!

Explanation of Android Enterprise

What is Android Enterprise?

Android Enterprise offers a better control of work devices that are managed with an MDM. This allows administrators to either have full control over their android devices or separate the company data from private data on container devices. Additionally Android Enterprise allows an easier enrollment of the devices and an easy app distribution.

What are the requirements to use Android Enterprise?.

Android Enterprise can be used for free by everyone. You only need to connect a google account to the MDM to enable all Android Enterprise features. More about this can be found in the Android Enterprise section.

Android Enterprise can be used on devices with Android 5.1 or higher, with the exception of Enhanced Work Profile (see below). We recommend at least Android 7 or higher for an easier enrollment or Android 11 to make use of all available features.

What are the available modes with Android Enterprise?

There are 3 different modes to use when using Android Enterprise.

AE Fully Managed Device (Work Managed): A fully managed device that is only used for work. This allows the administrator full control over the device. This does not allow a private use of the device. To enroll devices in this mode, devices have to be reset and enrolled with a QR Code (see AE Enrollment) or enrolled via Knox Enrollment or Zero Touch.

AE BYOD Container: The BYOD (bring your own device) Container allows users to access company data on their private phone in a separate container. In this mode, private apps are not able to see company data and apps and vice versa. To enroll devices in this mode, the AppTec app has to be downloaded and a QR Code can be scanned. Create a device in the console and select “AE Container (BYOD & Enahnced Work Profile)” as device type. Click on the QR Code on the newly generated device to get the QR Code and set the first switch to “Legacy & BYOD”.

AE Enhanced Work Profile: (requires Android 11 or higher) While the above mentioned BYOD Container brings company data on a private device, the Enhanced Work Profile does the same but for a company owned device. It creates the same container, but gives the administrator a bit more control over the device, so the user cannot simply remove the MDM from the device. Create a device in the console and select “AE Container (BYOD & Enahnced Work Profile)” as device type. Click on the QR Code on the newly generated device to get the QR Code and set the first switch to “Enhanced Work

Profile". This QR Code can be scanned after resetting the device and tapping 6 times on the screen as explained in Method 1 in AE Enrollment.

How can I assign apps to Android Enterprise devices?

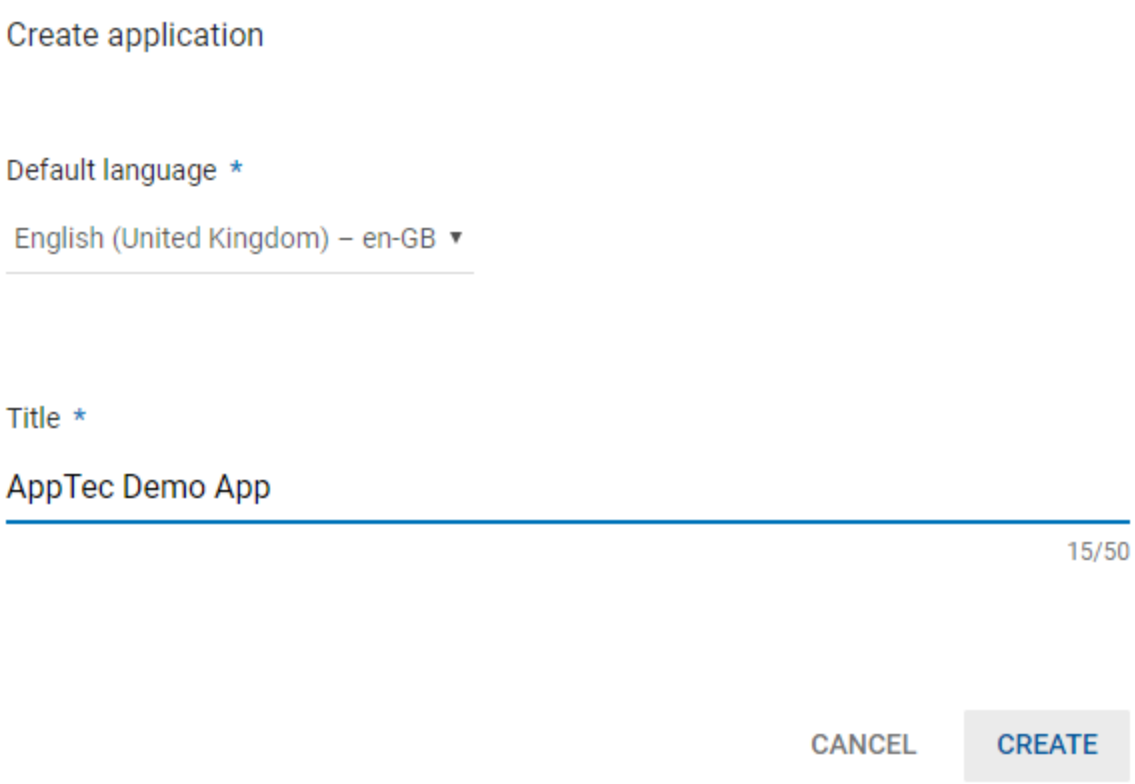
First you have to approve the Apps you want to use in General Settings → App Management → AE Play Store → Play Store Apps. After approving an app you can assign them to the mandatory app list → of your profile by clicking on the "+" and selecting the app from the "AE Play Store" tab. This will download and install the app automatically. There is no google account on the device required and the user does not have to confirm or allow this.

Upload your own Apps to the Google Play Store

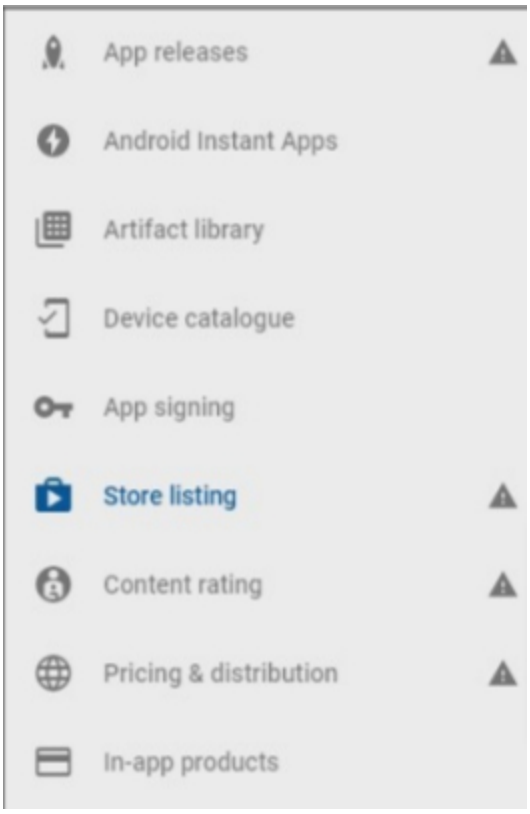
It is possible to upload your Inhouse Apps to the Google Play Store. This way you can benefit from different advantages like the update mechanism of the Play Store.

To do so, you need a Google Developer Account. Log in using the Google Play Console (https://play.google.com/apps/publish)

Click on „Create Application". Choose your default language and the title of the app.



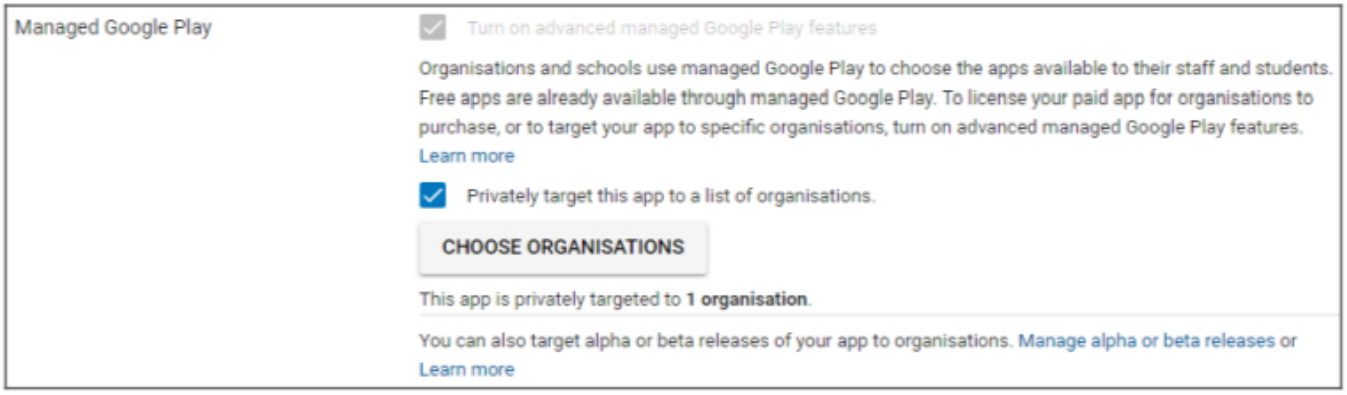
On the following Page you will be asked to enter different details about your app.



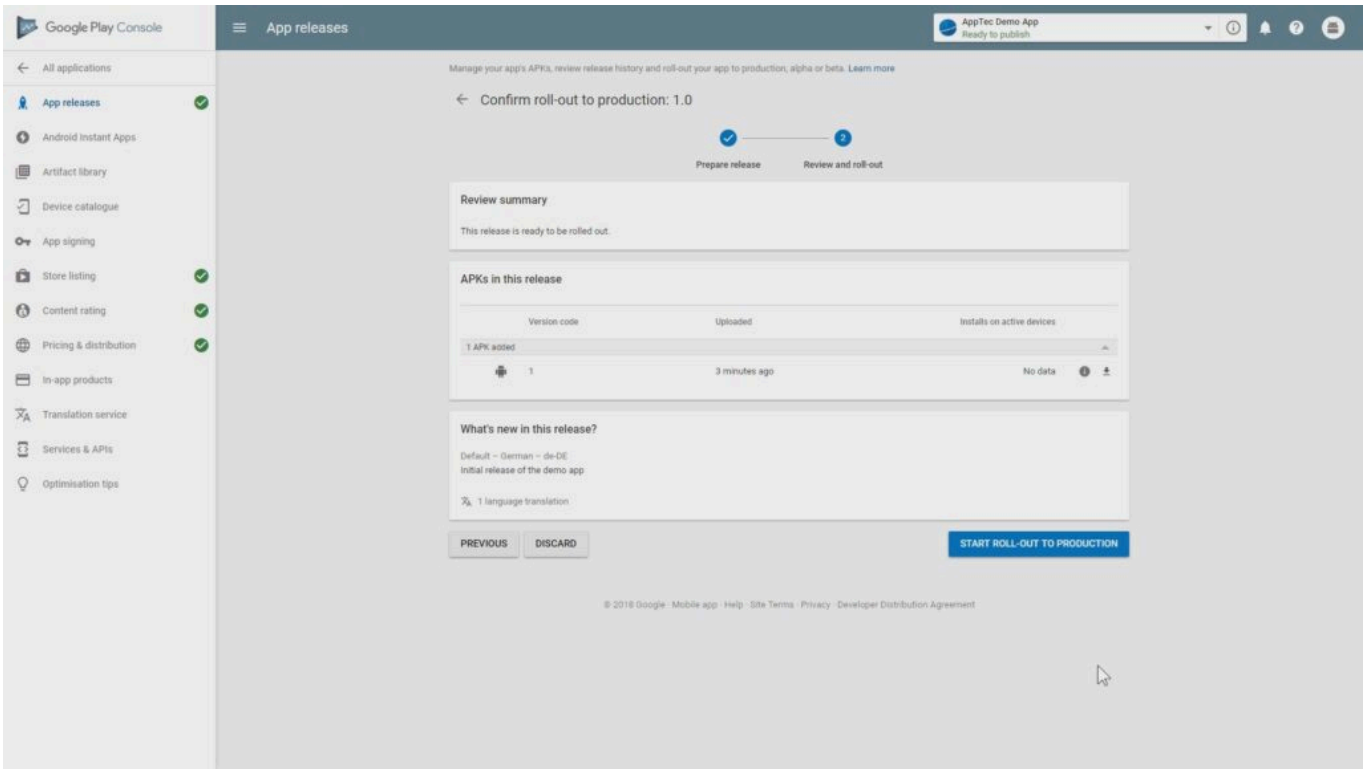
After you entered all the details, you will see different hint symbols at the left side.

Hover over them to see which steps are left and follow these in any order you like.

Note: Get sure to check the two checkboxes at „Managed Google Play“ under „Pricing & Distribution“. Otherwise the app will be public and can be accessed by everyone. Also get sure to choose the countrie for distribution.



Atfer you completed every step, you can go to „App releases“. Click on “Review” and “Start Roll-Out to Production” to finalize your draft and publish the app.



It my take some time until the app is available in the Play Store. After the process is finished, you can search your app in the Play for Work store and approve it. After that you can simply assign the app to devices using the EMM console just like you do it with other apps.

Requirements and Installation

Requirements

System requirements

The virtual appliance is available in the Open Virtualization Format (VMWare, VirtualBox, Citrix Xen Server) and as compressed .vhdx (Hyper-V) file*.

*Note: The machine has to be created with Generation 1 when using Hyper-V.

The virtual disk has a target size of 20GB and the machine requires 4 GB of RAM.

The appliance is based on Debian 9 64bit

Upgrade the imported machine to the newest compatibility (e.g. in VMWare) and make sure the machine OS type is set correctly in your hypervisor.

License key

In order to successfully activate and install the server, you will need a valid license file. You can obtain one from AppTec360 direct and/or from your respective reseller.

IP-Address and DNS Resolution

The AppTec360 appliance hast be reachable by the device using the hostname that the license is issued for.

To enroll Windows 10 devices you also need to set up an additional subdomain in the form of “enterpriseenrollment.”, pointing to the appliance.

SSL-Certificate

As all connections to and from the devices have to be secured using SSL, you need a valid certificate for the hostname issued by a Certificate Authority that is trusted by the device. The private key for the certificate has to be uploaded without a password protection. In most cases an intermediate certificate for the CA is required for the devices to recognize the server certificate.

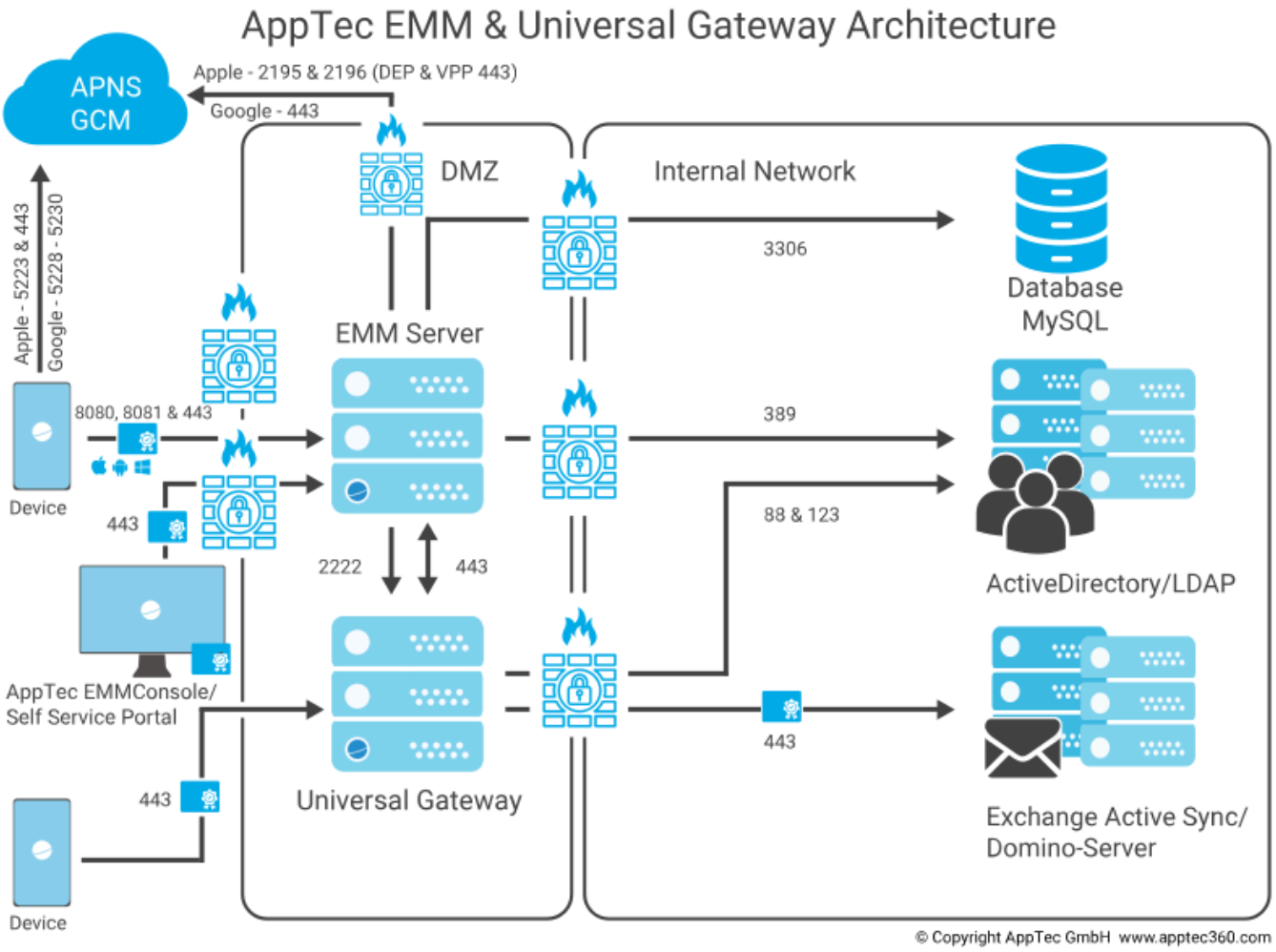
Windows 10 devices will require a specific certificate for your enterpriseenrollment subdomain.

Starting with appliance version 202104 you can also use Let's Encrypt certificates, which get generated automatically (described in Step Two – SSL Certificate).

SMTP Server

An e-mail server and/or an email-relay is required, to allow the AppTec360 EMM to send e-mails (e.g. for device registration and account validation).

Firewall Rules



This diagram shows which connection is needed depending on what services you want to use.

For a more detailed description see the table on the next page.

Any (external/Devices)	→	**AppTec360 Appliance / emmconsole.com**
Ports	443	Management, Enterprise AppStore & Windows Phone Communication
	8080	Android & iOS Communication
	80	Certificate creation and renewal with Let´s Encrypt.
Any (Devices)	→	**Any (external)**
Ports	5223, 443	Apple Push Service, has to be reachable without proxy, 443 as Fallback, see https://support.apple.com/en-us/HT203609
	5228-5230	Android Push Service (FCM), has to be reachable without proxy
AppTec360 Appliance	→	**Domain Controller**
Ports	389, (LDAPS 636)	User synchronization with LDAP
AppTec360 Appliance	→	**Any**
Port	443	Used for the Android Push Service (GCM) AppStore / Play Store search
AppTec360 Appliance	→	**emmconsole.com**
Ports	443	AppTec360 Appliance Updates, APNS certificate generation
AppTec360 Appliance	→	**Apple Network (17.0.0.0/8)**
Ports	2195, 2196	Apple Push Service & Feedback Service
	443	DEP & VPP

Security Updates

The Debian operating system should be updated regularly to get the newest security fixes. However make sure you don't upgrade to a newer major version of Debian manually. When the AppTec360 EMM is compatible to a newer major version we will add a way to upgrade in a appliance update.

Default Passwords of the Virtual Appliance

Login User (Root login is disabled. Use "sudo" for administration tasks)

apptec

Login Password

apptec

MySQL Root User

root

MySQL Root Password

apptec

MySQL Default User

AppTec

MySQL Default User Password

AppTec

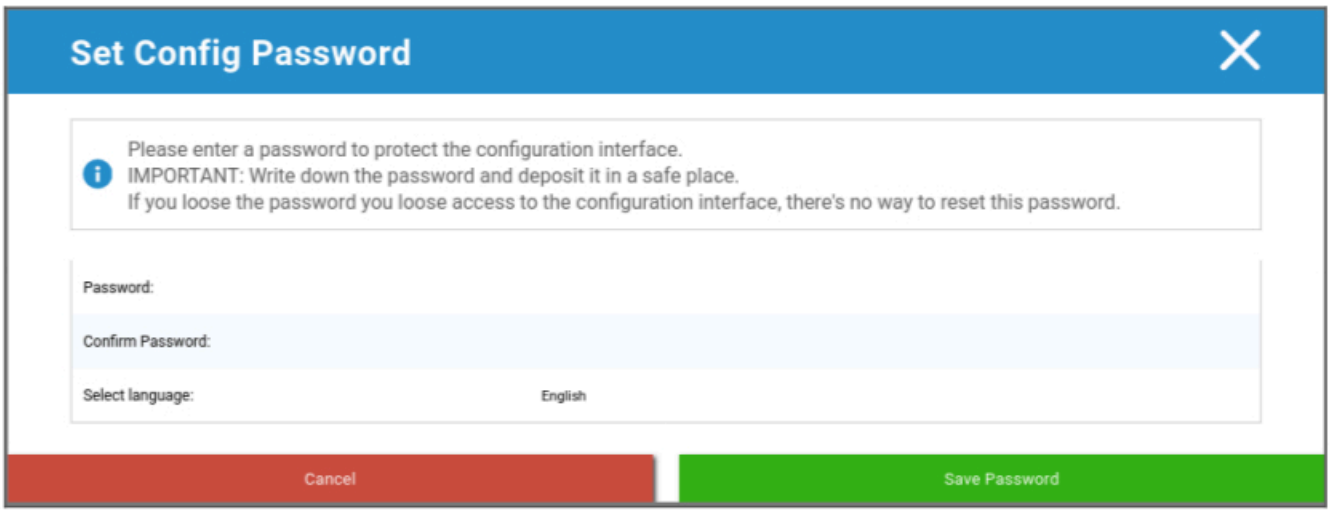
Configuration of the Virtual Appliance

Important: Before you begin with the configuration of the Virtual Appliance the display resolution should be set to at least 1280 x 800 pixels.

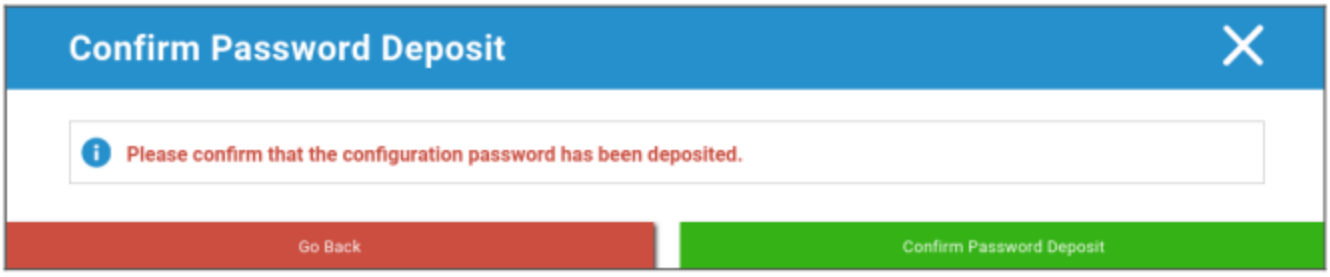
After longing in to the Appliance, Firefox should automatically get started and display the configuration interface.

Preparation

First you need to supply a password for the configuration interface. This password is used to encrypt all information and files entered in the configuration interface. Here you can also set the language the interface should be displayed in (can be changed later).

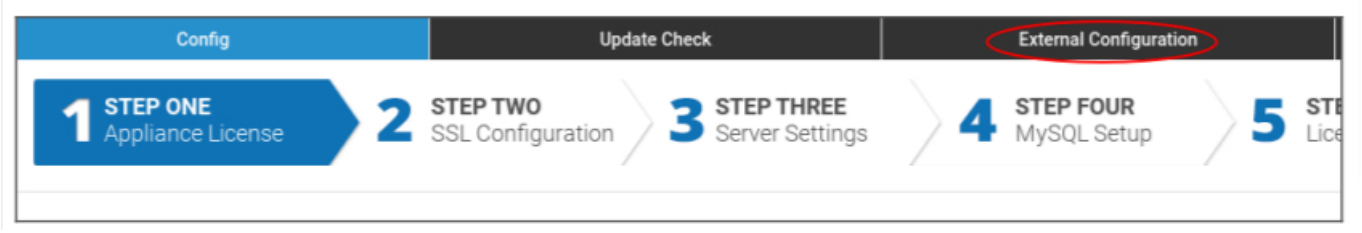


The password can only be reset by AppTec360 Support, so make sure you deposit it in a safe place and confirm the upcoming popup.



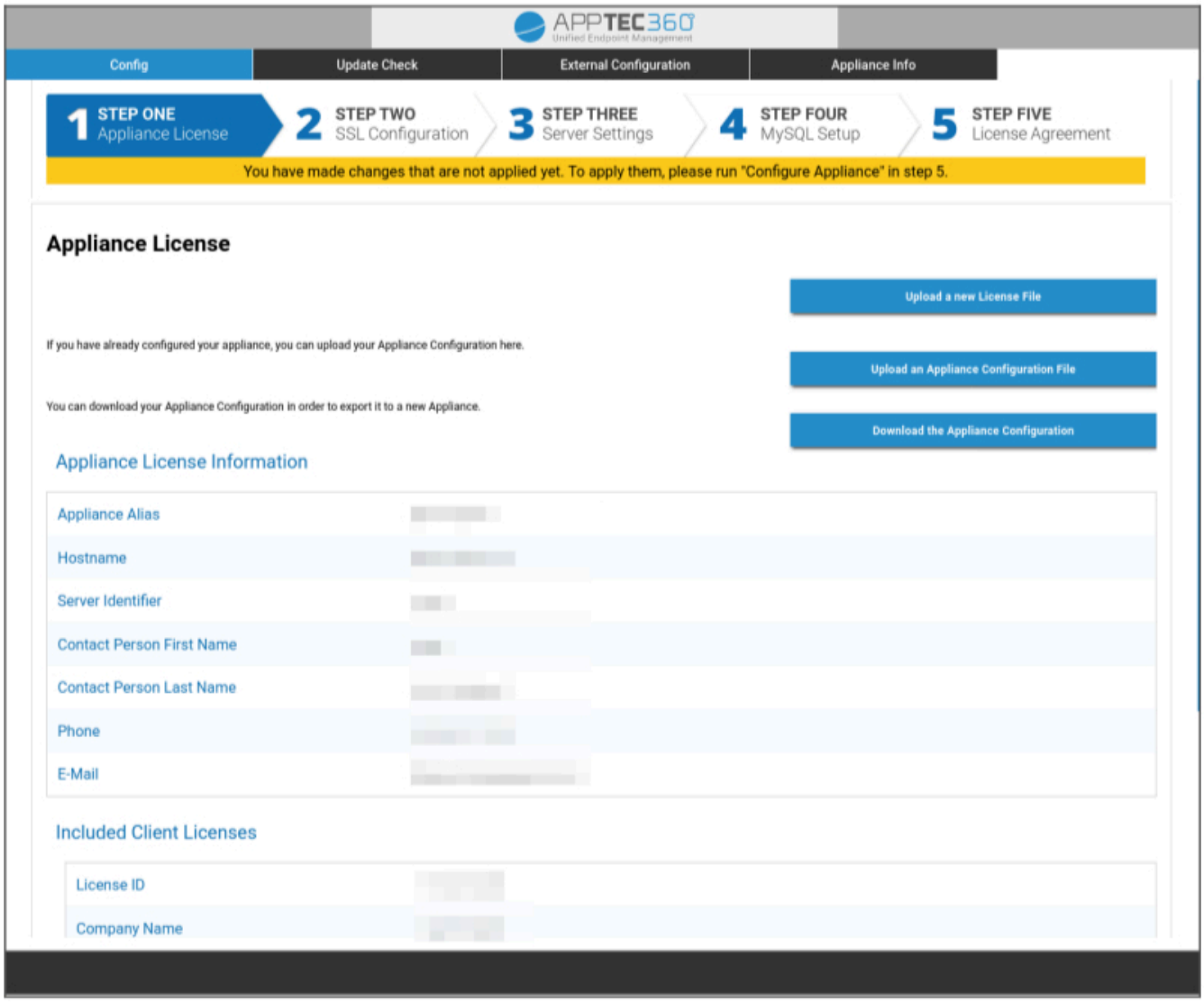
Configure from external host

To ease the setup process, you can make the configuration page accessible from remote. To do so, follow the steps in “Configure from external host”.



Step One – Appliance License

1. Please upload the license file that you have received from AppTec.
2. If the license file has been uploaded successfully, you can see the appliance license information like in the screenshot below.



Step Two – SSL Certificate

You can either use the automatic certificate setup using Let's Encrypt or provide the certificates yourself (see SSL-Certificate for more information).

Automatic

The certificate will be automatically generated using the Let's Encrypt service.

The AppTec360 EMM uses the HTTP-01 challenge for validation of the domain which means that the HTTP port has to be open from the internet for the first request of a certificate. Subsequent renewal requests can be validated via HTTPS.

Switch the radio buttons to "Automatic (Let's Encrypt)" and press "SAVE VALUES". The certificate will be automatically requested when applying the configuration in Step Five – License Agreement. The certificate will be automatically renewed if necessary and you will receive an e-mail if the certificate is about to expire (which implies that the renewal might have failed).

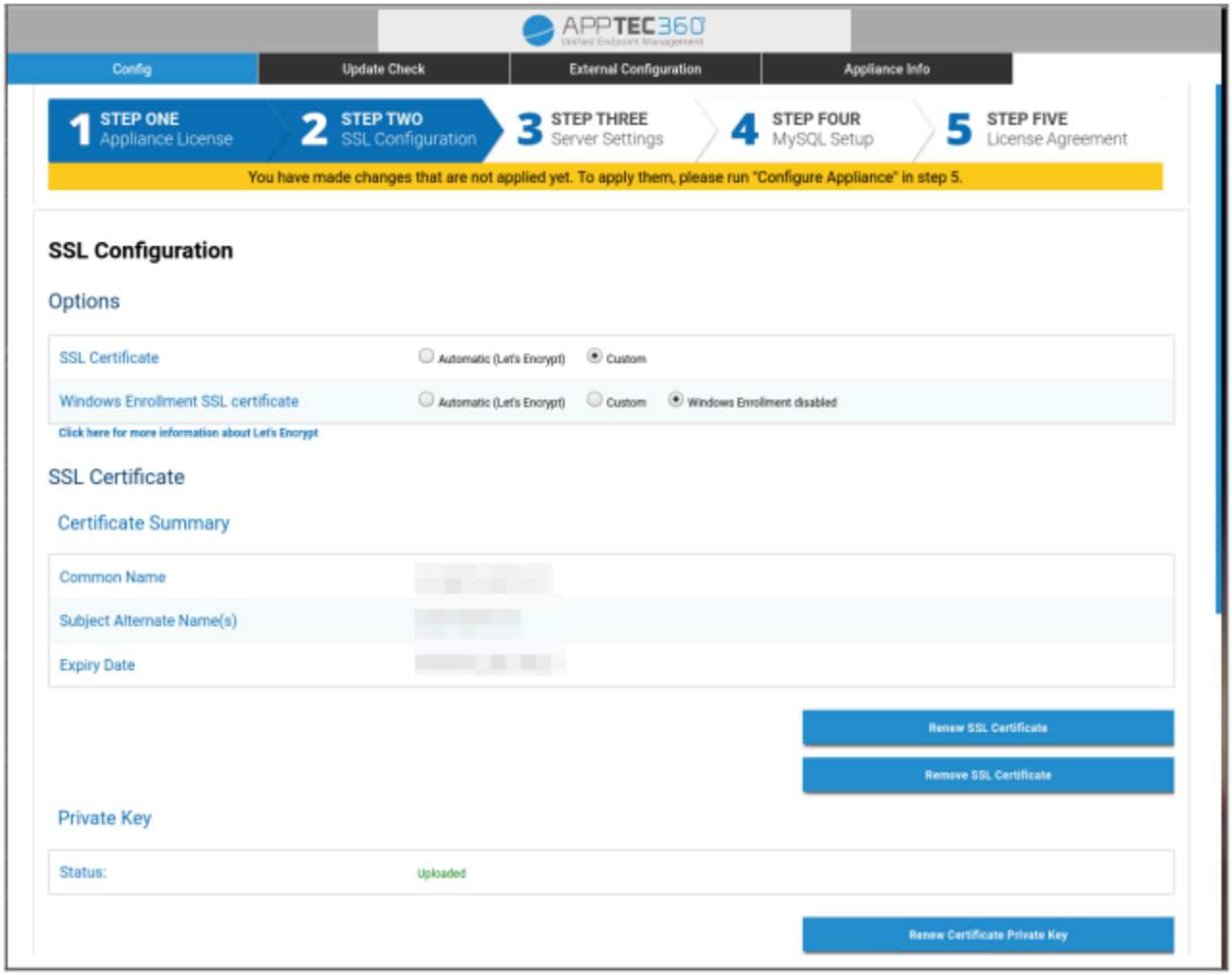
Custom

1. Upload the SSL-Certificate for your licensed hostname. You can see the hostname in Step One – Appliance License.

2. Please also upload the private key for the certificate and if necessary the intermediate certificate.

Important: The key must not be password protected. If it is, please remove the password before uploading.

Hint: If you also want to use Windows 10 devices you have to enable “Windows Enrollment SSL certificate” and upload the certificate, private key and intermediate certificate for your subdomain (described in IP-Address and DNS Resolution) upload at the bottom of the page.



Step Three – Server Settings

1. Please enter a global support e-mail address. This address will be used in e-mails to your users so they know who to contact in case of any issues in regards to their device.
2. Supply E-Mail Settings to be used by the system to send e-mails. The settings will be used to send e-mails to the user and also to send Bug Reports and Feature Requests to “support@apptec360.com”. After saving your e-mail settings you need to verify them by clicking on “Test E-Mail Configuration” and following the instructions.

Step Four – MySQL Setup

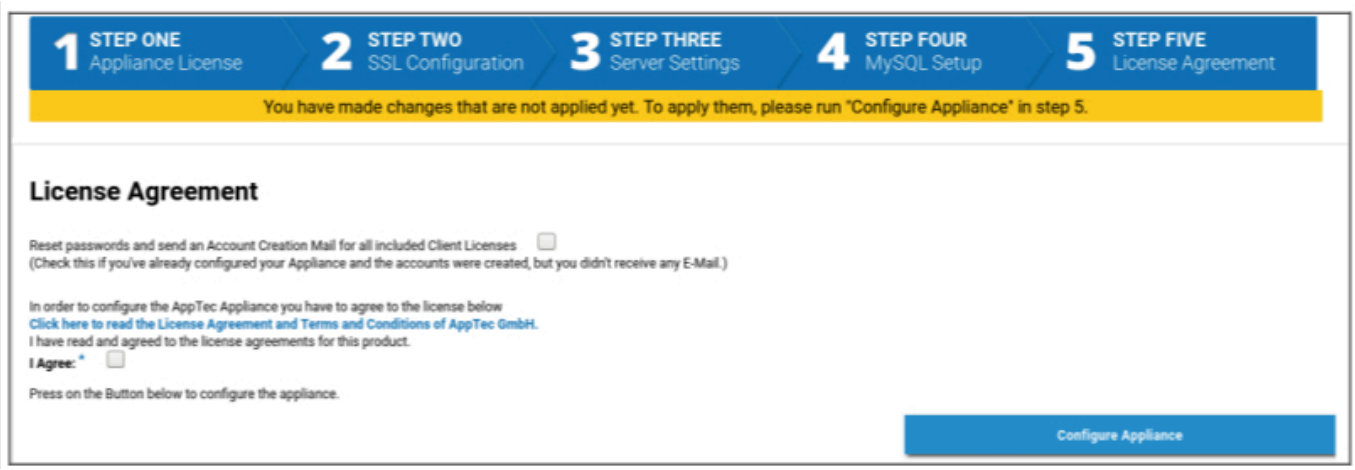
1. If you want to use the internal database you can skip this step. Otherwise you can enter the connection information for your external database server.


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)

Step Five – License Agreement

1. Please make to read the license agreement.
2. Check “I Agree” and press the “Configure Appliance” button, to apply the settings.

Hint: You will need to run “Configure Appliance” every time you change settings in the 5 steps to apply the settings.



Congratulations!

You have finished the configuration of the virtual appliance.

An e-mail including your password was send to the address that you’ve provided for the license (visible at “Included Client Licenses” in Step One – Appliance License).

You are now able to login into the console using this password and the e-mail address you’ve received it on.

To login into the console, please enter the hostname of the console into the address bar of your browser.

You can find the hostname of your appliance in Step One – Appliance License.

Troubleshooting

1. You did not receive an e-mail when configuring the appliance in Step Five – License Agreement:

Make sure your e-mail settings in Step Three – Server Settings are correct. To resend the password check “Reset passwords and send an Account Creation Mail for all included Client Licenses” in Step Five – License Agreement before running “Configure Appliance” again.

2. You’ve received an error in regards to Let’s Encrypt during the configuration in Step Five – License Agreement:

Make sure the appliance is reachable by its domain name on port 80. Let’s encrypt also writes a log to “/var/log/letsencrypt” which might help with further troubleshooting.

Security Recommendations

It's recommended to perform the following steps to secure your AppTec360 appliance.

This is not a full set of instructions, it's just a recommendation for a basic configuration.

- Change the password for the AppTec360 user
- Change the password for MySQL users “root”and “AppTec” and update Step Four – MySQL Setup accordingly
- Change the default SSH server port
- Block port 80 in your console and disallow incoming HTTP traffic, only use HTTPS. Once configured, an external configuration over HTTPS is possible too.
- Restrict access to the management interface to certain Ips only at the bottom of Step Three – Server Settings
- Configure the firewall

General Settings

Account Overview

Account Information

Overview

Here, you can see an overview of your AppTec360 account.

Company Name	Your company name
Creation Date	Creation date of your account
License Type	Paid = paid license Free = unpaid license Note: Accounts on an OnPremise Appliance will always be shown as paid for technical reasons
Client Identifier	Identifier of your account (This is NOT your customer number)
License Expiration Date	Expiration date of your AppTec360 license
ContentBox License	Free = free license for 25 devices Paid = paid license for x devices
Launcher	Shows whether or not you can use the custom launcher for Android
Devices	Number of currently used / total licenses
Contact Person	Provided contact person
Phone	Provided telephone number
eMail*	Provided email address
Root User	Root Users which are able to login
Software Version	Current Software Version

**Note: The email address shown here is the one you entered to register the Account. Based on this a user will be created in the user/device tree and can be modified. Editing this user will change the email address you have to use to login but not the information in the account overview*.

Bug Report

A bug report can be sent directly to support to report issues or bugs and includes information and logs about your account and setup.

Subject	The subject of the bug report. Include a ticket number if you want to add this to an existing support ticket.
Expected Behavior	Describe in detail what you did and what you expected to happen
Actual Behavior	Describe in detail what exactly happen. Please quote error messages EXACTLY. It also helps if you add screenshots to the attachment.
At what time did you experience the issue?	Please give a precise time when you got a specific error message/problem. In best case include seconds too, e.g. 18:55:27
Can the issue be replicated? If yes, how (in detail)?	Describe how you can reproduce the issue in detail.
Has this feature worked previously as you expected? If yes, until when?	Leave empty if you do not know.
Were there any specific changes made to the system before this issue appeared? If yes, what changes (in detail)?	Always mention what your last change or action was before the issue appeared, even if you think it is irrelevant.
If Applicable: Which device models and OS versions are affected?	Please always name the exact OS Version (e.g. iOS 14.7.1 or Android 11)
If Applicable: What is the public IP address or/and Serialnumber of the Device?	Name at least one, even if all devices are affected.
Include logfiles	Check this to send the logfile with the bugreport. This is recommended to do.
Fetch current VPP state from Apple and include to bugreport	Includes information about VPP License Assignments. Only activate this if you are asked to do so by support or if your problem is about VPP.
Attachment	Attach any file that could be useful (e.g. Screenshots of an error message)

Feature Request

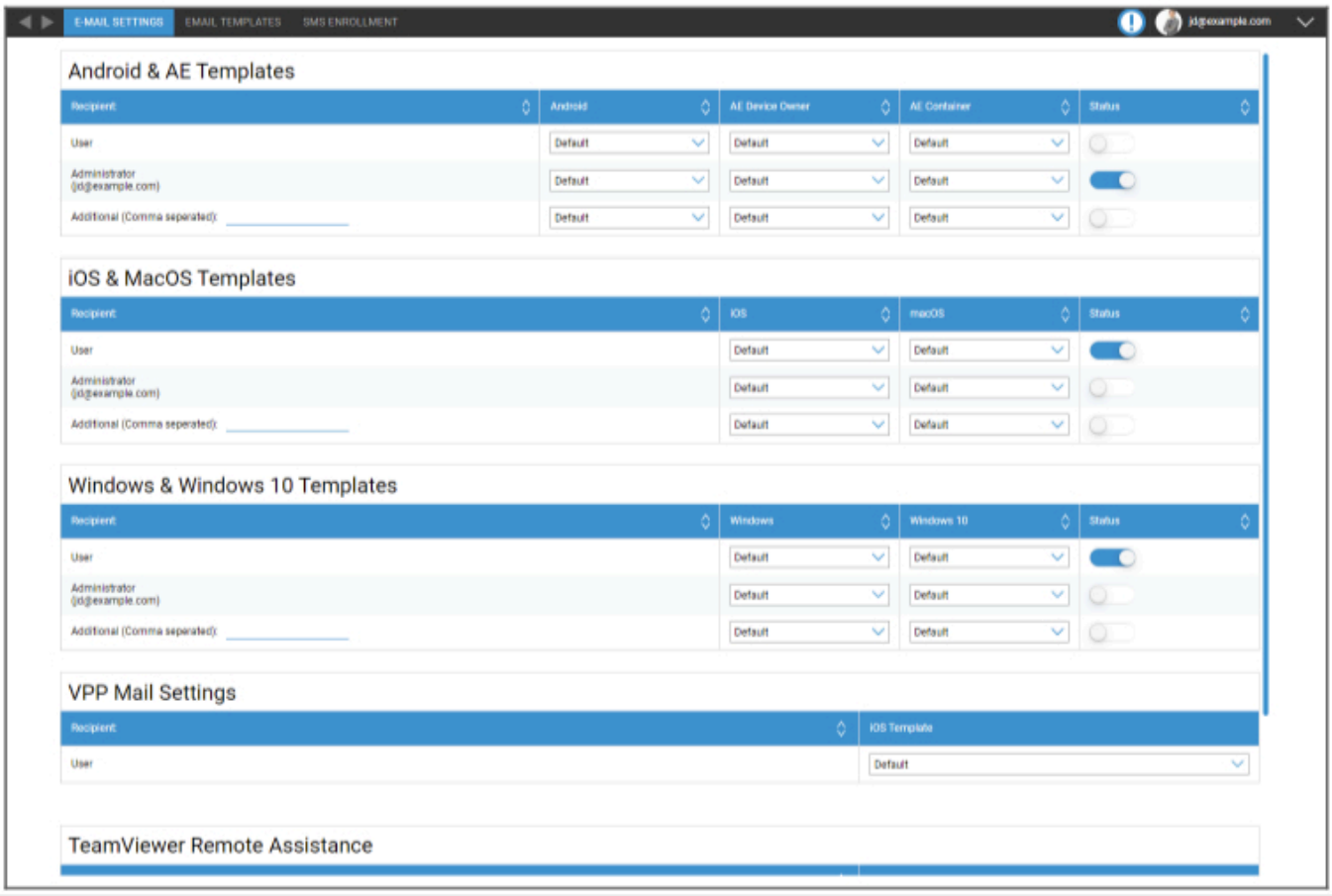
A feature request can be sent directly to support. This can contain a request for a specific feature or an improvement for

Summary	A brief synopsis of your problem
Description	A detailed description of your problem, please be as specific as possible
Attachment	Attach files to the bug report

Global Configuration

eMail Settings

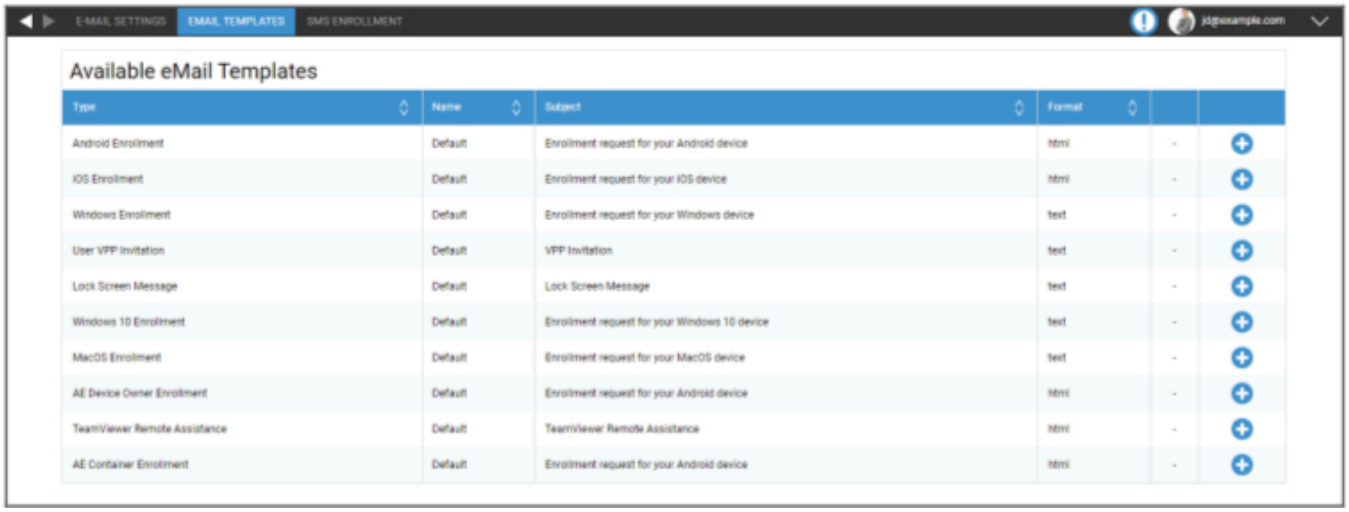
Here you can define who gets a mail when an enrollment request is generated and which text template is used for that mail.



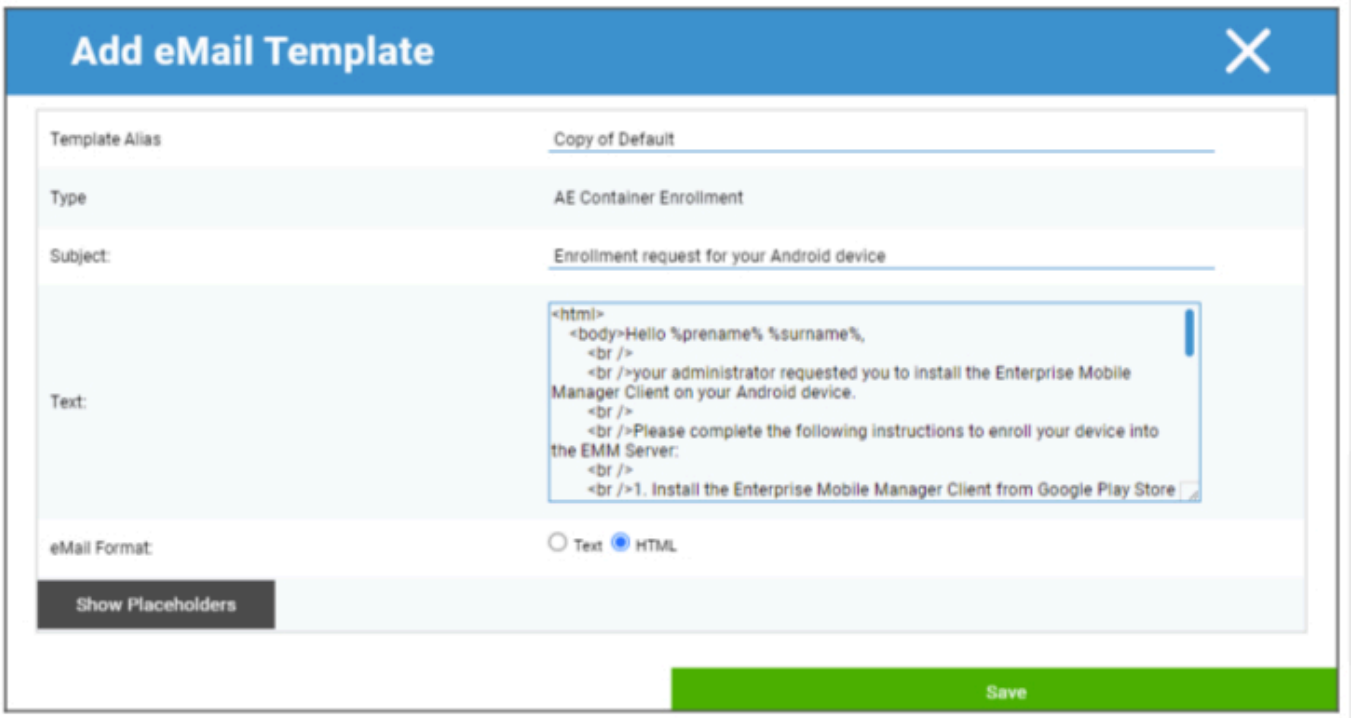
eMail Templates

Here you can generate and edit your templates for different scenarios. These can be in normal text form or in HTML. With HTML you can better control the formatting of your text.

The default templates cannot be edited or erased.



You can also use Placeholders as variable which will be automatically replaced. Click on “Show Placeholders” while editing to see available Placeholders. Different Categories have different Placeholder.



SMS Enrollment

Here you can de/activate the SMS Enrollment process.

(Default: deactivated)

You will also see a display, indicating how many SMS Credits are still available.

SMS Credits need to be purchased seperately.

Privacy

GPS Access

Here you can protect the GPS View for every device with 1 or 2 passwords (four eyes principle). You will be prompted to enter your password(s) every time you try to access the location of a device.

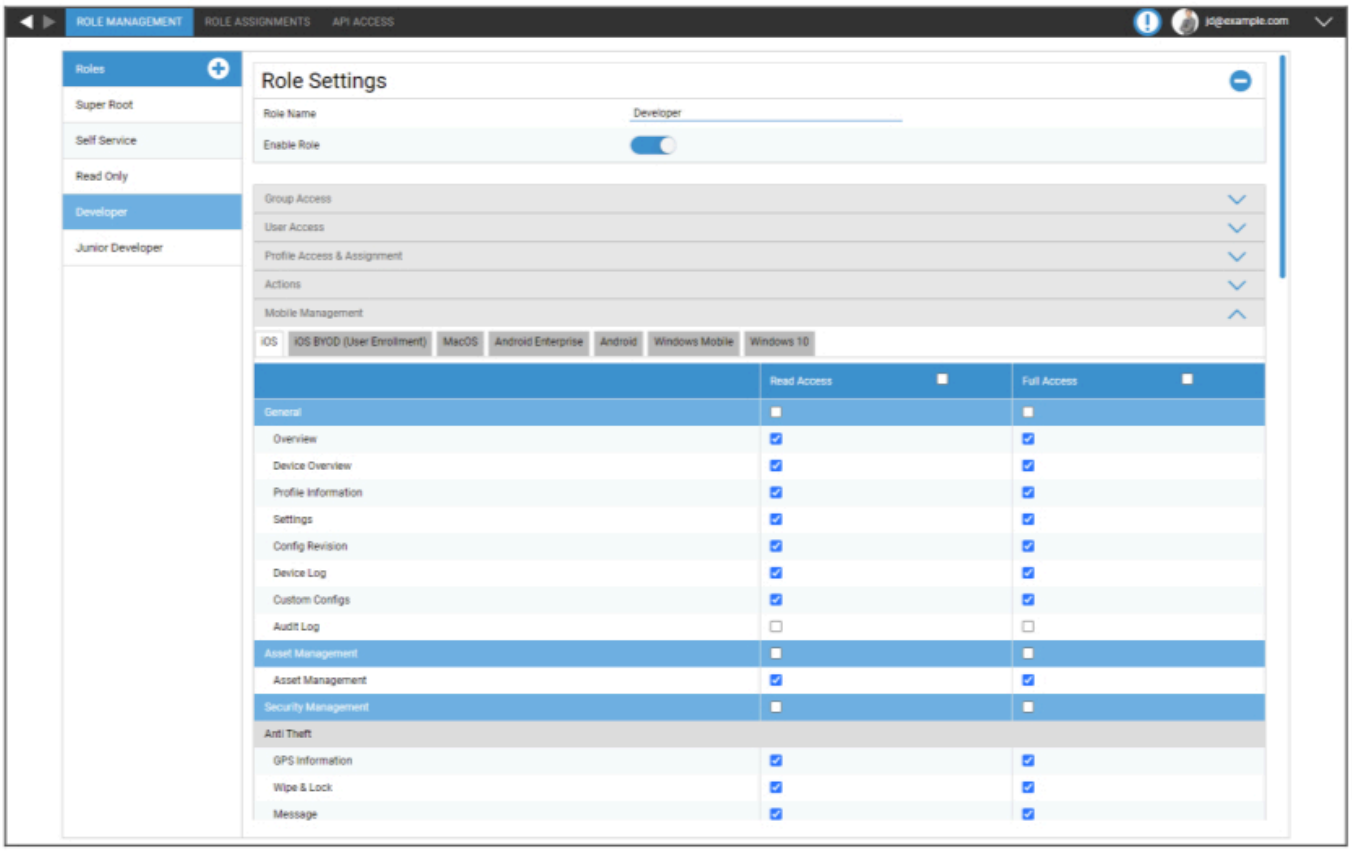
Restrict access to GPS Settings	Off = function is turned off and no password is required for localizing
	On = function is turned on and a password is required for localizing
Protection Method	Use one password = use one password for localizing
	Use two passwords = use two passwords for localizing
Enter Password (1)	Enter chosen password
Repeat Password (1)	Re-enter chosen password
optional: Enter Password 2	Enter 2nd chosen password
optional: Repeat Password 2	Re-enter 2nd chosen password

Note: After setting your passcode(s), you have to enter it once more before it is completely enabled.

Role Based Access

Role Management

The Roles define what a user can see and do when he logs into the management console. This allows your to create users which can log in but have limited functionality.



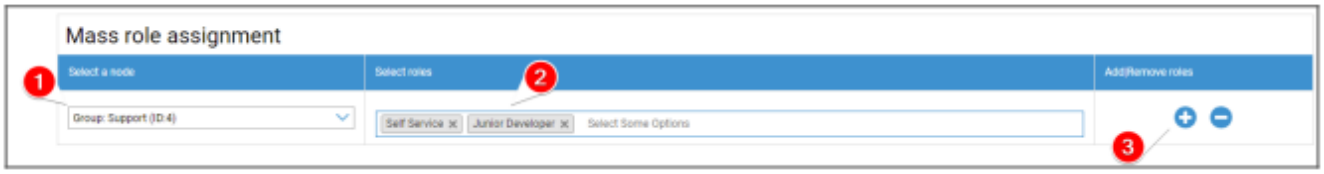
The Super Root Role is a default Role which always is able to see and change everything. It cannot be changed or deleted. The Self Service Role is only able to see its own user and devices. You can combine Self Service and a custom role to e.g. allow users to login and enroll devices on their own and only for their user.

Custom Roles can manually be enabled or disabled. New Roles are disabled by default. Users with a disabled role work like they do not have the role. This allows you to e.g. temporarily restrict a given role from their actions.

All Permissions are split between “Read Access” and “Full Access”. Giving a Role Read Access allows them to see the specific part of the console. Giving them Full Access allows the Role to see and change the specific part of the console.

Role Assignments

Here you get an overview of all users which have a role and see which one they have. You can also assign a role to users or whole groups here:

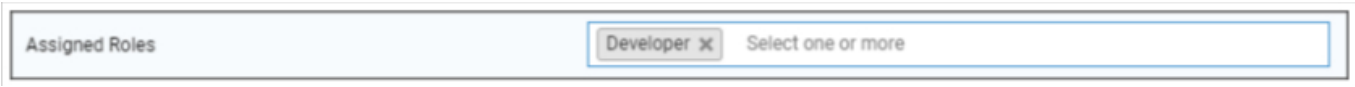


1. Select for which group or user you want to add or remove roles. You can either select a single user or select a group. When selecting a group, your change will affect all users within that group and all users of sub groups withing the selected group.
2. Select which role you want to add or remove. You can select one or multiple roles.
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. Save to finish the process. Users which previously had no role and “Can Login” disabled will automatically receive a mail with a link to set a password.

Below the Mass role assignment you can find the overview over the assigned roles. You can also manually change roles there for specific users.

Assignment of a role

To assign a role to a user, you have to go to the Mobile Management, where you find the tree of your groups, users and devices. Edit the user to assign a role. Alternatively you can use the above mentioned method for only single users as well.



API Access

Access AppTec360 REST API

The AppTec360 REST API requires an authentication token (API key) and a private key which have to be generated in the Managment Console.

To do so login into the AppTec360 EMM and go to

General Settings → Role Based Access → API Access and add a new Key.

You have to select a user whose permissions will apply to the API key.

The private key can only be downloaded once. After the download has started the key will be deleted, and the "Download" button disappears.

If you lose your private key you have to generate a new API key.

General Rules

- The REST API is available below the base URL:

/public/external/api

- All requests have to be send via POST.
- The REST API only supports requests via HTTPS.
- Requests must contain the following Headers:

Header Name	Header Value	Description
Content-type	application/json	fixed
auth	123...xyz	API Key from the "API Access" Tab
signature	Base64 encoded signature	Signature of the payload generated with the private Key from the "API Access" Tab

- The request body must be a json encoded object which must contain the following values:

Field	Field Example Value	Description
api	v2/device/listdevices	Name of the API
time	1529662725	Unix Timestamp (UTC) of the client machine. The maximum allowed time difference between the client and the server is 30 minutes.

- On success the API returns the requested data (see the Queries below) and an HTTP status code 200.
- If an error occurs, the HTTP status code will be between 4xx and 5xx depending on error and the response object will contain an array with the key “errors”, which contains a list of human readable error messages.
- If there is no matching data for a device an empty array will be returned.
- If a device Id does not exist it’s return data will be null.

Request example

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]}}

Queries

List all devices

Functionality: Returns a list of all devices containing the Device ID, IMEI and Serial
API URI: v2/device/listdevices
Mandatory Parameters: none
Optional Parameters: none

Example Request Body


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


Example Response Body


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

Get list of (GPS) positions

Functionality: Returns a list of all stored position log entries for device ids
API URI: v2/device/listposition
Mandatory Parameters: “ids” – Array of Device IDs
Optional Parameters: none

Example Request Body


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


Example 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":[],
]
}
```

Get asset map

Functionality:
Returns a list of all stored possible assets to be requested using Get any asset data.
You can either use the human readable form or the asset tag to request the data.
API URI: v2/device/getassetmap
Mandatory Parameters: none
Optional Parameters: none

Example Request Body

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

Example Response Body

This response was shortened for readability.

{
"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": []
}

Get any asset data

Functionality: Returns a list of requested asset data for device ids
API URI: v2/device/getassetdata
Mandatory Parameters: “ids” – Array of Device IDs
Optional Parameters:
“assetkeys” – Asset data keys to return. If not specified all available asset data will be returned. You can get a list of asset keys using Get asset map.

Example Request Body


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


Example Response Body


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

Example Code 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 Configuration

APNS Certificate

Here you can upload an APNS Certificate. This is required to manage iOS and MacOS devices.

Note: The APNS Certificate is only valid for one year. This has to be renewed before it expires. The Renewal process is identical to the creation (see below) and takes only a few short minutes.

Should you forget to renew this in time, you cannot make changes to your already enrolled devices **and you have to enroll all the devices again**.

Step 1

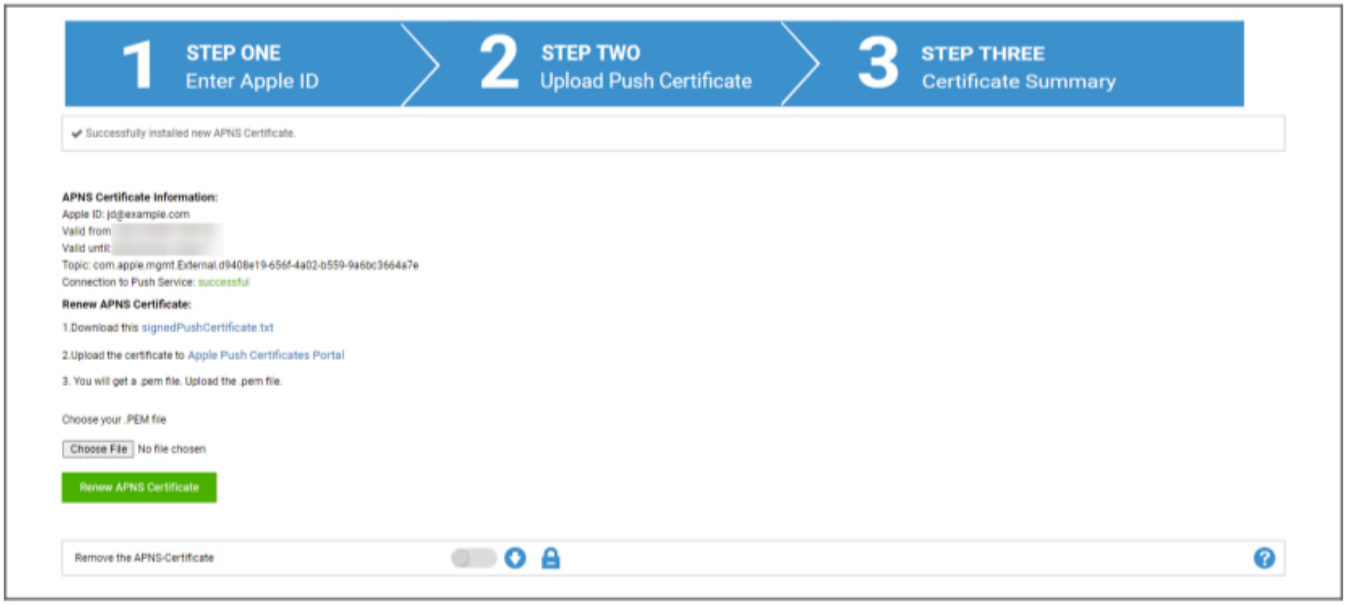
- First, enter your Apple ID you want to use to create the APNS Certificate.

Note: This Apple ID is only used for the APNS Certificate creation. This Apple ID has nothing to do with the devices and the devices will not know about this Apple ID. Additionally you also need access to this Apple ID to renew the APNS Certificate. Therefore it is recommended to use some generic Apple ID and document the login data. A Reminder is sent to the used Mail Address of the Apple ID before the APNS Certificate expires.

- Click on “Next Step” to proceed.
- (optional) You can also recover the previously deleted APNS Certificate if you deleted it by accident

Step 2

- Download the signedPushCertificate.txt
- Go to https://identity.apple.com/pushcert/ and login with the Apple ID from Step 1
- Click on “Create a Certificate”
- (optional) enter a Note. This can be helpful if you manage multiple tenants to easily identify them.
- Click on “Choose File” to select the previously downloaded signedPushCertificate.txt
- Click on “Upload”.
- You will now see the confirmation that you created an APNS Certificate.
- Click on “Download” and save it.
- Go back to the management console.
- Click on “Choose File” and select the APNS Certificate you want to upload.
- Click on “Upload”



Step 3

You now have successfully setup the APNS Certificate and can now manage iOS and MacOS devices.

In Step 3 you will see an overview of your currently used APNS Certificate.

Also you have the Option to renew the APNS Certificate by following the steps shown on screen. Keep in mind to renew this before it expires.

When renewing the APNS Certificate, keep in mind to login with the Apple ID shown in Step 3 and also to renew the previously used certificate and NOT create a new one. You will see the “topic” of the APNS Certificate in Step 3 and when clicking on the “i” in the Apple Push Certificate Portal. This is the unique ID which identifies the Certificate. This will help you to identify the correct and renew the correct one.

When you get “Error: The Push Certificate has a different topic!” while renewing, this means that you did renew another Certificate or created a new one.

If you want to upload a new Certificate, e.g. if you cannot access the previously used Apple ID any more, you first have delete the currently uploaded Certificate.

Anyhow deleting the APNS Certificate means that you can no longer make changes for the currently enrolled devices until you enroll them again. So get sure that you are prepared for this and only remove the Certificate if there is no other way.

Managed Access

Here you can enable User-Enrollment for iOS Devices and Shared iPad for iOS Devices.

User Enrollment

'User Enrollment' enables a special mode for BYOD devices.

For each user a managed Apple-ID has to be created in the Apple Business Portal.

During the enrollment process the users will be asked for their Apple-ID credentials.

'User Enrollment' guarantees maximum safety for the user as it allows only a limited set of settings and restrictions to be configured by the MDM.

Managed Domain:

The Domain used to map the user's e-mail address to their managed Apple-ID (must be in the format: '@appleid.company.com').E.g john.doe@example.com will be mapped to john.doe@appleid.company.com

Check the Apple Business Manager to see your Managed Domain

Shared iPad

A shared iPad is a DEP device configured with a special DEP Profile.

This allows multiple users to login into the device using their managed Apple-ID.

The managed Apple-ID has to be created in the Apple Business Portal or the Apple School Manager.

Users, who log into a shared iPad are asked for their managed Apple-ID credentials.

Managed Domain:

The Domain used to map the user's e-mail address to their managed Apple-ID (must be in the format: '@appleid.company.com').E.g john.doe@example.com will be mapped to john.doe@appleid.company.com

Check the Apple Business Manager to see your Managed Domain

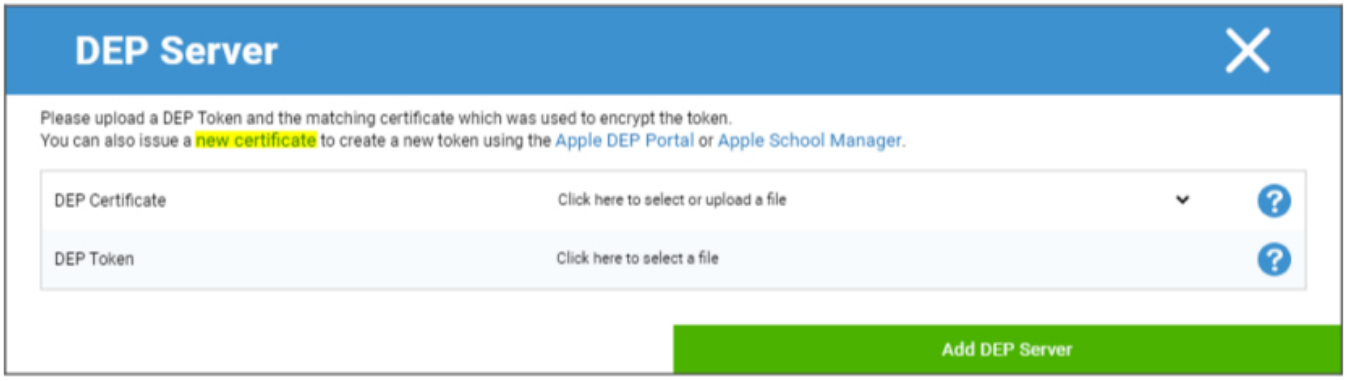
DEP

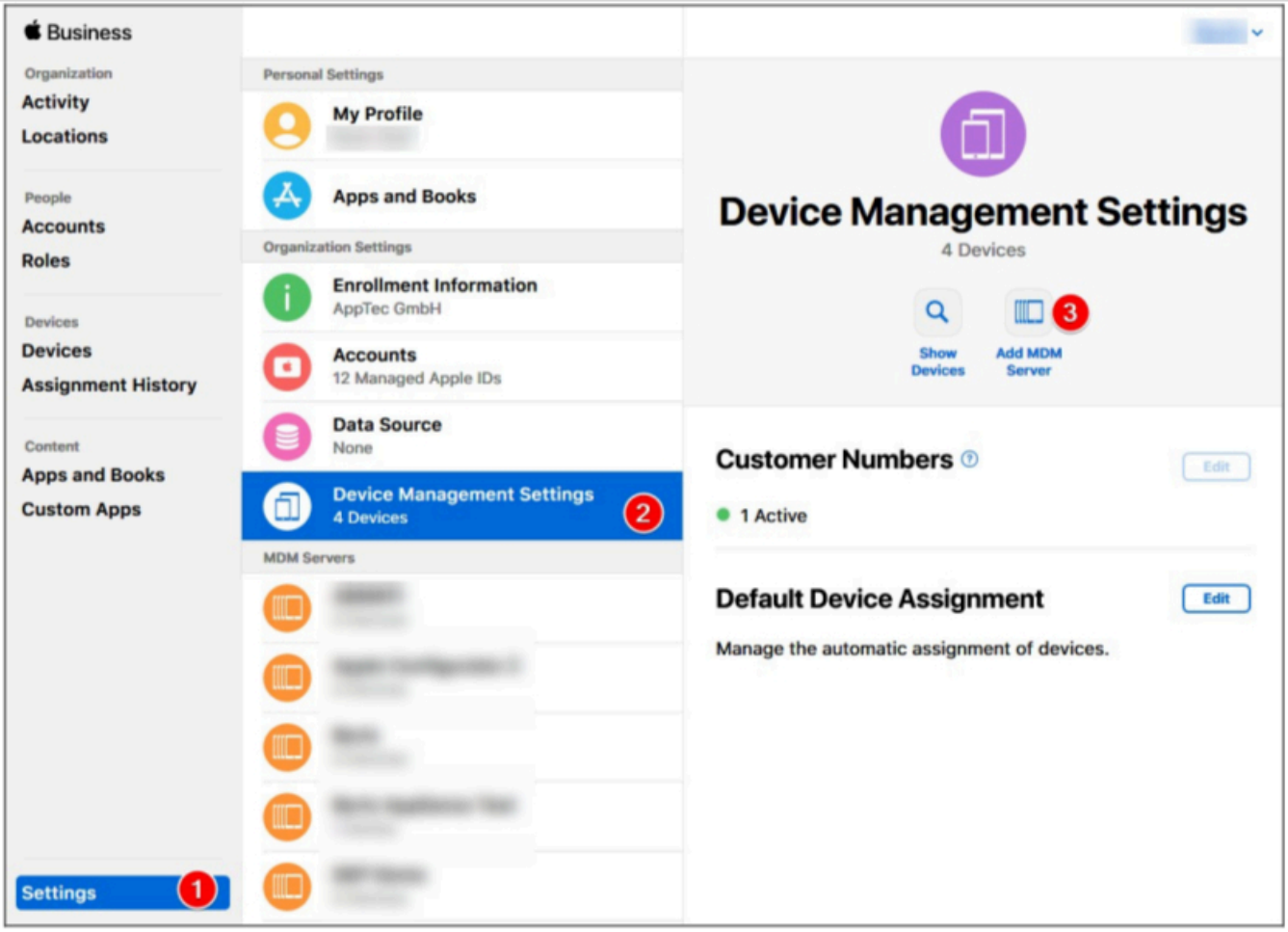
DEP (Device Enrollment Program) allows you to easily enroll devices into the MDM. When using DEP, the devices will be automatically connected to the MDM when setting up the device. You can also skip almost all of the setup steps which are usually mandatory on iOS.

Keep in mind that you need to buy the devices from a reseller who supports DEP. For more information, contact your reseller or Apple.

More Information about DEP: https://www.apple.com/business/dep/

Click on the “+” to add a DEP Token. In the Popup, click on “new certificate” in the text (marked yellow in the image below). This will generate and download a DEP certificate. Afterwards go to the Apple Business Manager (https://business.apple.com/) or Apple School Manager (https://school.apple.com/).

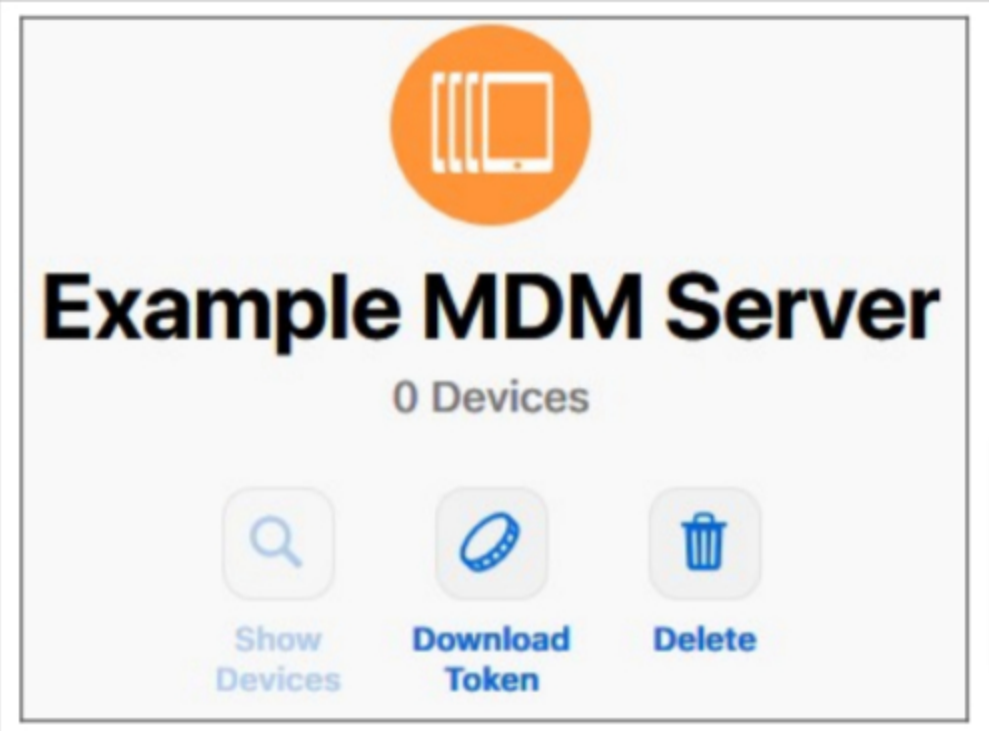




In the Apple Business Manager, follow the steps as shown in the image above. Settings → Device Management Settings → Add MDM Server.

Give the Server any name you want and upload the previously downloaded DEP Certificate under MDM Server Settings → Upload Public Key and click on “Save”.

You will now have the option “Download Token”. Click on this and save it. The Token is only valid for 1 year. But just clicking “Download Token” again, will give you a new one, which makes renewing the token very easy.



You can now go back to the MDM, where you previously downloaded the DEP Certificate. If you did not close the tab, the popup for adding a DEP Server should still be opened and the DEP Certificate should already be selected. You can now upload your Token in the field “DEP Token” and click on DEP Server.

In the column “**Devices**” you will see the amount of devices that are assigned to this DEP Server. Devices added to this DEP server will be automatically created in the DEP Pool in the Mobile Management.

You can click on this number to get an overview over all your DEP devices and their status.

Note: Depending on your workflow or configuration in the Business Manager it may be possible that you have to manually assign these devices to the DEP Server. You can also set a default DEP Server in the Apple Business Manager for new devices.

In the column “**Profiles**” you see the Amount of DEP Profiles you have. You can also click on this number to see details about your DEP Profiles and you are able to delete old/unused profiles here. It is currently not possible to change these. If you want to make a change, you have to create a new one.

In the column “**Last Synchronization**” you can manually sync the DEP Server (e.g. if you just added a new device to DEP) and see the date of the last successful Sync.

In the column “**Auto Profile**” you can set a DEP profile as an automatic default. This profile will be assigned automatically to new devices. If you do not set an Auto Profile, you have to manually assign a profile to new devices each time.

In the column “**Add Profile**” you can add a new DEP profile. The device will receive this at the beginning of the device setup. The DEP profile defines how the device is set up and which setup steps will be skipped.

Note: after a device is enrolled, these settings can only be changed by performing a factory reset and enrolling the device with a new profile. This is especially relevant for “**Removable**” and “**Allow pairing**”. In case of “**Allow pairing**” it is recommended to turn this on, since this can be disabled via MDM restrictions, but it cannot be enabled again if its disabled in the DEP profile.

In the column “**Edit**” you can upload a new token, e.g. when renewing the Token.

Configurator & URL

Pool Enrollment URL’s

Here you can create an enrollment URL and an enrollment QR Code which is valid a set amount of enrollment and until a set date. This allows you to enroll multiple devices which only one link or QR code.

Devices enrolled with this URL or QR Code will be in the Pool in the Mobile Management and you have to manually assign them to a group or user afterwards.

Note: this is only for manual enrollment. Do not use this URL if you enroll the devices via Apple Configurator

MDM Profile – Apple Configurator

Here you can get the URL you need when enrolling devices via Apple Configurator. While preparing devices with the Apple Configurator you can add the devices to the MDM in the same process. The Apple Configurator requires this URL for this.

Devices added via Apple Configurator will be in the Pool in the Mobile Management and you have to manually assign them to a group or user afterwards.

You will also find a .mobileconfig file here which can be used to enroll the devices via Apple Configurator. Anyhow using the URL is recommonded.

Android Configuration

Android Configuration

Uninstall Protection	If this function is activated, the user cannot deactivate the device administrator, without entering the password set by the MDM Administrator. The password is set during enrollment, so devices have to be re-enrolled to update the password. There are two options for removing the device administrators: 1. Manually on the device ◦ Open EMM App on the device ◦ Switch to the Status tab ◦ Tap on “Uninstall Protection” ◦ Enter the password You can use the Revision to get the correct password from the “Password History” in the console. ◦ Scroll down and tap the newly added point,“Tap to uninstall AppTec360 MDM App“ (you have 20 seconds to perform this task) ◦ Confirm the dialogue “Uninstall AppTec360 MDM App“ with “ok“. This will unenroll the device from the console. ◦ To remove the App from the device confirm the dialogue “AppTec360 MDM will be uninstalled“ with “UNINSTALL“ 2. the automatic (Console) ◦ Select the Device in the console ◦ Click on the blue gear icon and select “Enterprise Wipe” Note: Only available with Android 4.x and lower versions or on devices with the KNOX API (Samsung devices)
Uninstall Password (Revision x)	The established password, with which the user can remove the device administrator Revision x = counter, how often the password has already been changed It is important which password the user needs, because it is possible that the device

	has not communicated with the AppTec360 Server and therefore the newest password has not been transmitted yet
Password History	When you click on the blue button (“Show History“), you are able to view the previously established passwords
Extended Uninstall Protection	This Option offers protection against non-SAFE devices As long as this setting is activated, it is not possible to easily deactivate the device administrator
Prompt the user to uninstall blocked Apps?	If possible, blocked Apps will not only be blocked but also uninstalled automatically. The user will be prompted to uninstall blocked Apps if no automatic uninstall is possible.
Intelligent System App Blocking	If Whitelisting is enabled, the Android MDM Client blocks all user installed Apps. Enable this setting to block all launchable System Apps in Whitelisting mode.

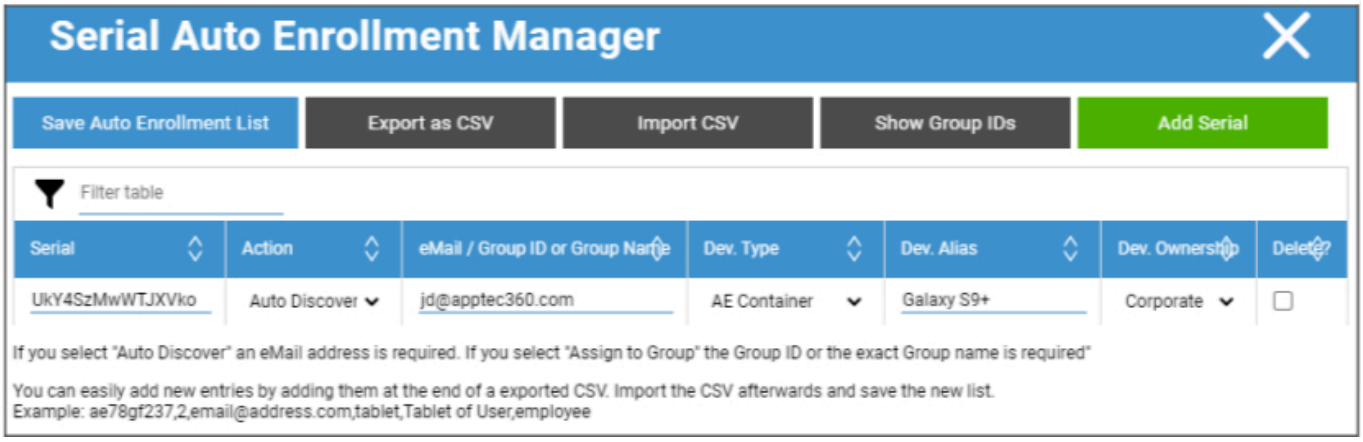
Auto Enrollment

Here you can enable the Auto Enrollment feature to enroll your devices automatically when the AppTec360 MDM Client is opened on the device.

Important: This enrollment method is deprecated and no longer works on Android 10 or higher. Anyhow when using Android 7 or higher you should enroll devices as Android Enterprise fully managed anyways. If you want to use the Android Enterprise BYOD container and you are on Android 10 or higher, you have to manually enroll the device via credentials, QR Code or SMS. Anyways, the Auto Enrollment List is still used to automate the enrollment process for e.g. AE Enrollment, Knox Enrollment, etc.

Anyways, the Auto Enrollment List is still used to automate the enrollment process for e.g. AE Enrollment, Knox Enrollment, etc.

By either clicking on “Serial Manager” or “IMEI Manager” you can add the Serial or IMEI of your devices respectively. It is not required to do both for you devices, only one is enough.



Action defines if the devices will be enrolled into the pool, a user or a group.

You are also able to export and import a .csv file and filter your entries by keywords.

Android Enterprise

Here you can setup Android Enterprise. This is necessary to use all Android Enterprise features.

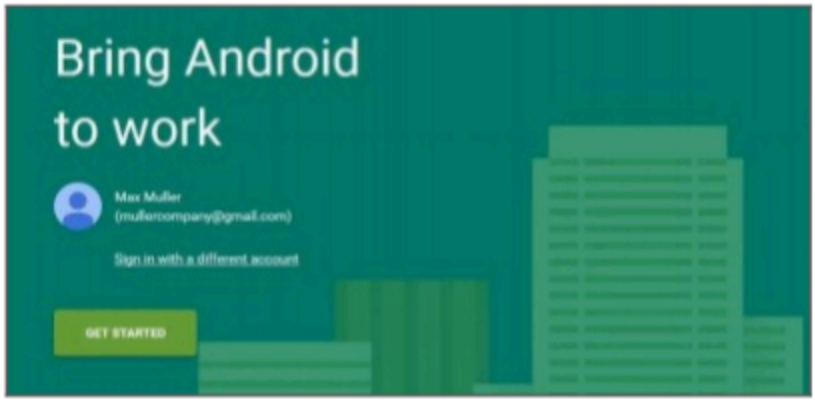
First Method: Android Enterprise Account (Google Account)

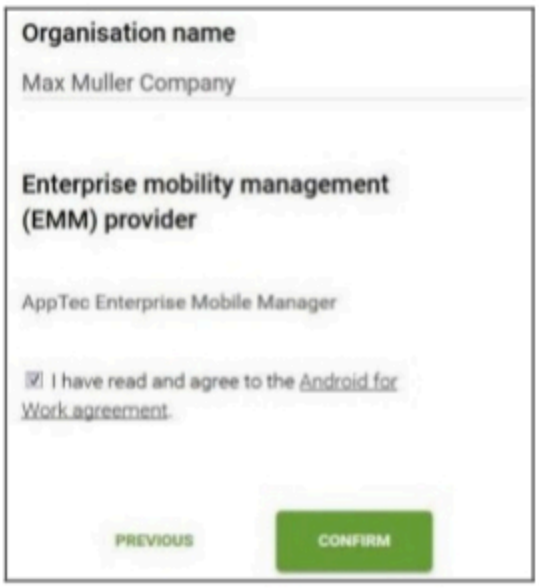
First press “Prepare Setup”, than after a short moment there should be the button “Start Setup”.

This will bring you to the Google’s Android Enterprise Setup Page.

Login with the Google Account you want to use, if you are not already logged in and press “Get started”.

Now you can enter the name of your company. After doing so, check the checkbox and press “Confirm”





In the last step you can complete your registration and should return to the console. If everything worked it should look like this:

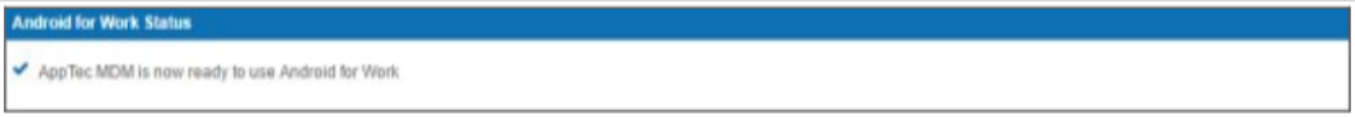
Now you can start configuring your Android Enterprise Container.

Second Method: G-Suite Account

Press “Use G-Suite” and login to your Google Admin Account. There you go to “Security” -> “Show more” -> “Manage EMM provider for Android” and generate a Token. Note: If you do not see the Android Enterprise Settings in your G-Suite Account, you have to go to “Get more apps and services” and add the Android device management. Now enter the Token and your primary Domain in our console and click on “Save Changes”. When you are done, click on “Use Android Enterprise Account”.

Now you should see the “Create Service Account” Button. Click on it. This process can take a few moments.

If everything worked, it should look like this:



Now you can start configuring your Android Enterprise Container.

Factory Reset Protection

With the Factory Reset Protection you can bind your device to a google account of your choice, which also overrides any existing binding to a google account. To use Factory Reset Protection, you have to set it up here first and activate it in your profiles afterwards.

To set up the Factory Reset Protection, click on “FRP Setup” and follow the instructions on screen.

NOTE: Carefully read and perform the steps. We recommend doing this in a new incognito browser window to avoid automatically login into the wrong google Account. You can completely lock out yourself out of the device, if you should enter a wrong ID or loose access to the used Google Account!

AE Enrollment

Here you can activate the Android Enterprise Ernollment. Using this Method will enrolle your Devices into the Android Enterprise Device Owner Mode. In this mode you will have the full control over the device.

Enable AE Enrollment	Activates the AE Enrollment Caution: If you disable AE Enrollment, existing QR Codes and already configured NFC programmer devices will stop working. If you enable AE Enrollment again, you'll have to resend NFC push configurations / generate new QR codes.
Enable Auto Discover	When a device enrolls itself via "AE Enrollment" the system will try to assign it to an user based on the information set in the Serial / IMEI Whitelist ("General Settings" > "Android Configuration" > "Auto Enrollment").
Block Unknown Devices	Only devices that have been whitelisted in the Serial / IMEI Whitelist ("General Settings" > "Android Configuration" > "Auto Enrollment") are allowed to enoll.

Note on Method 1 & 2: „Welcome Screen“ refers to the first screen you see after the factory reset. This can look different depending on the android version and/or device model you are using.

Method 1: QR Code Enrollment

(requires Android 7.0 or higher) We recommend to always use this method if you are running Android 7 or higher.

1. Factory reset the device
2. Generate the QR Code for the Enrollment using one of the two following methods:
    - Click in „General Settings -> Android Configuration -> AE Enrollment“ on „Generate QR Code“. Choose if you wish to skip the storage encryption and/or all system apps should be removed.
    - (alternatively) Choose an existing Device. In the „Device Overview“ click on the QR Code displayed there. Choose if you wish to skip the storage encryption and/or all system apps should be removed.
3. Now tap 6 times on the Welcome Screen of your device. This should start the QR Enrollment Mode.
4. Now connect to a wireless network and wait a short time until the QR code reader is installed
5. Now scan the QR code
6. That’s it. Your device is now enrolled in the Android Enterprise Device Mode.
    - a. If you used the QR Code in „General Settings“ you can find your device in „Pool -> AE Device Owner Devices“. (Hint: It is possible that you have to reload the site to see the

devices). If you checked “Enable Auto Discover” you will find it within your Auto Discover user.

- If you used the QR code of an existing device profile, the device will be enrolled into this profile.

Method 2: NFC Enrollment

(requires NFC and Android 6.0 or higher)

Preparation: Enter your WiFi information in „General Settings -> Android Configuration -> AE Enrollment -> Data for NFC provisioning“. Now use „NFC Device“ to search for the device that will become the programmer. This device will be used to send the enrollment information to the other devices via NFC.

1. Factory Reset your device
2. Open the NFC pairing app from AppTec360 on your programmer
3. Choose if you wish to skip the storage encryption and/or all system apps should be removed.
4. Hold both devices back to back
5. Now the Android Enterprise Enrollment should stark
6. You now find your device in the console
    - a. In the pool, if you have not configured Auto Discover
    - b. Within the user, you configured for the Auto Discover
    - c. Hint: It is possible that you have to reload the site to see the devices

Method 3: Google Account

(requires Android 5.1 or higher)

(Note: If you are using this method, the device will not be automatically enrolled. Instead you have to enroll it manually or automate the process by using Auto Enrollment.)

1. Factory Reset your device
2. Go through the setup steps until you can login with a google account
3. Enter „afw#apptec“ as Username/Mail
4. Tap on “Next”
5. Your device is now an Android Enterprise Device

KNOX Enrollment

Here you can activate the KNOX Enrollment and find the information you need to create a KNOX Enrollment Profile in the KNOX Deployment Portal. You need an Account at the KNOX Deployment Portal to configure and use this.

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

Enable KNOX Enrollment	Activates the KNOX Enrollment. Caution: If you disable KNOX Enrollment, existing MDM profiles will stop working. If you enable KNOX Enrollment again, you'll have to update the "Custom JSON Data" field of your MDM Profile
Enable Auto Discover	When a device enrolls itself via "KNOX Enrollment" the system will try to assign it to an user based on the information set in the Serial / IMEI Whitelist ("General Settings" > "Android Configuration" > "Auto Enrollment").

1. Log into the Samsung KNOX Mobile Enrollment Portal https://eukme.samsungknox.com/itadmin
2. Go to „MDM Profiles“
3. Click on "Add"
4. Choose "Server URI not required for my MDM" and click on "Next"
5. Now create a profile with the information shown in the management console

Now this KNOX Enrollment Profile can be directly installed on the device by Samsung if you acquire the devices from Samsung directly.

Alternatively you can download the KNOX Deployment App, login with your KNOX Deployment Account and send the KNOX Enrollment Profile via NFC to other devices.

If the device has a KNOX Enrollment Profile installed, it will download our App and enroll the device, if it has a working internet connection.

Devices enrollment via KNOX Enrollment can be found in „Pool -> KNOX Enrollment“, or within the user you specified in the Auto Discover.

Zero-Touch

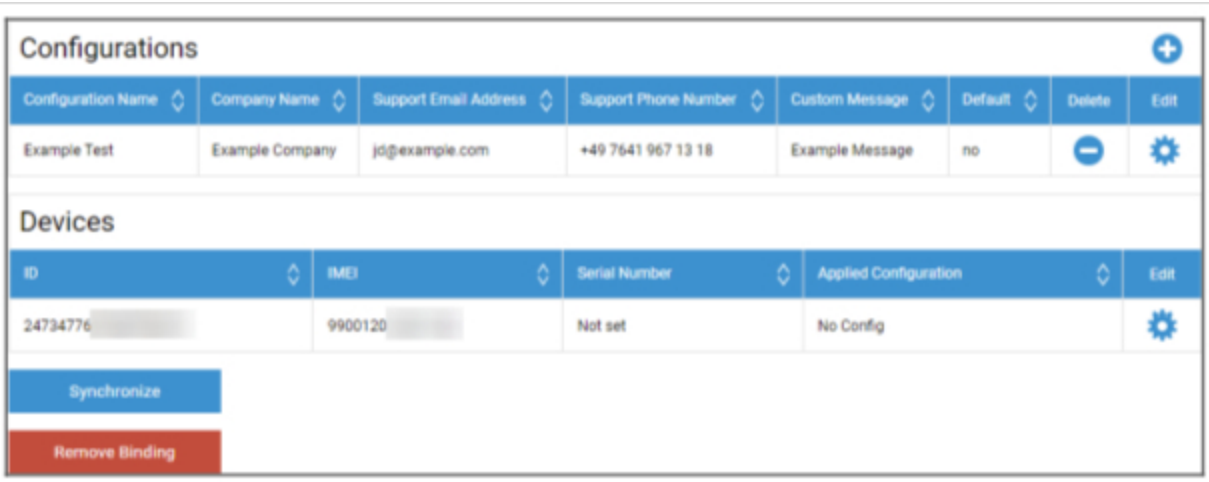
With Zero-Touch you can easily enroll your devices without the need of touching them or configure anything on the device itself. You just have to turn it on, proceed through the configuration as normal and the device will receive all information on how to setup and connect to the MDM completely automatically.

To use Zero-Touch you have to buy your devices from a Reseller which supports Zero-Touch. The same Reseller is also creating an Account for you in the Zero-Touch Portal. Contact your Reseller to get more info about the procedure or if you have problems when accessing the Zero-Touch Portal.

Click on “Start Setup” to start the setup. You will be redirected to a login page where you have to select your Google Account which has access to the Zero-Touch Portal.

NOTE: It is possible to select ANY Account. So get sure to select the correct Account in this step. If you do not see your devices/configurations, you high likely used the wrong Account.

After completing the login, it will look like this:



Click on the “+” to add a Configuration and fill out the fields as presented on the screen. If you enable the Configuration as default Configuration, it will be assigned to the new devices automatically. Creating or setting a default configuration does not assign it to already existing devices.

If a device has no Configuration assigned, it will setup as a normal device and not connect to the MDM. Therefore get sure that your devices have a Configuration assigned.

After you connected your Account, your devices are visible and you have a Configuration assigned to them, you can start setting up the devices.

You can add the devices to the Auto Enrollment List so they will get enrolled into a specified group or user automatically. If you did not configure anything in the Auto Enrollment list, devices will be enrolled

into the Pool.

Windows Configuration

Windows Configuration

Here you have the option to enable the following configurations on your Windows 10 PC:

Instant DM Connection	
Initial Retry Time	Establishes the first connection attempt to the device, this value increases exponentially
Connection Retries	Indicates how many connection attempts the DM-client should perform, during a connection error
Maximum Sleep Time	Indicates the maximum sleep time after a connection error
First Sync Retries	Intervals, at which the device is to communicate with the server, after the first connection
First Retry Interval	Relates to “First Sync Retries“ Here the times are listed in minutes For example under “First Sync Retries“ the value “2“ is listed and under “First Retry Interval“ the value “4 Minutes“ is listed, this way the device communicates 2 times every 4 minutes, after the first connection
Second Sync Retries	Intervals, at which the device should communicate with the server, after completing the “First Sync Retries“
Second Retry Interval	Same principle as for “First Retry Interval“ – just that here, it applies to “Second Sync Retries“
Regular Sync Retries	Intervals, of how often the device should communicate with the server in the future Default: “Infinite“ We recommend not changing this value, because if you enter “10“, the device will communicate with the server 10x and then stop Therefore, the communication with the AppTec360 server is disconnected!
Regular Retry Interval	Same principle as for “First/Second Retry Interval“ – just that here, it applies the settings for the future
Regular Retry Interval	Same principle as for “First/Second Retry Interval“ – just that here, it applies the settings for the future

ContentBox

Configuration

Here you can configure the ContentBox. You can place files for groups in the ContentBox which can be access with the ContentBox App on the device.

Enable ContentBox	Enable ContentBox. Disabling this if you do not use the ContentBox, can save resources on OnPremise machines.
Use external ContentBox installation	The ContentBox can also be operated with your own Nextcloud.
URL	Complete URL of the Nextcloud entity
Root User	Root User of the Nextcloud Account
Root Password	Root password of the Nextcloud Account
Default group folder permissions	Default group folder permissions, can be individually modified by group (in Mobile Management)
Share group folder with subgroups	If active, each subgroup can read all of the main group's folders, can also be individually configured for each group (Mobile Management)
Permissions for subgroups	Permissions for subgroups can be individually configured for each group (Mobile Management)
Allow sharing	Allows the user to share the content via Links, can be individually configured for each group
Maximum File Upload Size in MB	Maximum size of a file Standard: 512 MB Maximum configuration: 2048
WebDAV Credentials	
WebDAV URL	You can also open the ContentBox with WebDAV. Please do not delete the following folders, under any circumstances: /apptecgroups /apptecgroups/AppTecGroup-X
Root User	Name of the Root Users
Password	Password of the Root Users

The synchronization with the ContentBox occurs automatically. You can, however, perform a manual synchronization with “Synchronize ContentBox“.

Additionally, here you can activate/deactivate the ContentBox on each individual device.

This is only relevant, if you have not additionally licensed the ContentBox, then you still have access to 25 devices with which you can test the ContentBox – here you can activate this for the respective devices.

LDAP Configuration

LDAP Overview

Here you can establish a connection to your Active Directory via LDAP to mass import users and groups. The sync has to be performed manually. You can configure multiple LDAP connections to different systems or with different configurations/filter.

Server Name	The Display Name of the Server
Type	Currently only Active Directories which support LDAP are supported
LDAP Domain	The primary LDAP Domain (e.g. example.com)
LDAP Host	Only necessary if the LDAP host is not reachable under the given LDAP Domain.
Port	Leave empty to use Standard Port (389 or 636 for SSL)
Username	E.g. CN=John,OU=Users,DC=EXAMPLE,DC=COM Note: Most systems require the username in this format and do not accept “John” as Username
Password	
Confirm Password	
Connection Security	Note: when using SSL or TLS, the certificate of the Active Directory will be checked. If this is self-signed you have to add the root CA to the trust storage of the OnPremise Machine. If you are on Cloud the Active Directory has to provide a trusted certificate or the connection will only work with no Encryption
Automatic Sync.	Enables the automatic synchronization of the LDAP directory in the time interval specified in the general LDAP settings.
Base DN	If you don't want to synchronize the whole directory, you can specify an OU here.E.g. OU=AndroidUsers,OU=Users,DC=EXAMPLE,DC=COM
Member of	All imported users will be added to the selected group
Only activated users?	When enabled, the attribute userAccountControl will be considered, users without that attribute won't be imported.
LDAP Filter	You can use LDAP Filter to filter which Users get imported
Regex Filter	You can use Regex Filter to filter which Users get imported
Test Connection	Tests the connection when saving the configuration
Reset directory	If true all LDAP entries will be moved back to their original location in the LDAP tree. Recommended to be enabled.

structure on sync?	
Re-import deleted users and groups?	When enabled, users and groups that have been deleted will be recreated. Recommended to be enabled.
Sync deletions?	When enabled, groups and users will be deleted when they are deleted on the LDAP server. Also devices of deleted users will be deleted.

Below the list of your LDAP Configurations you can define the period in which the system sync automatically. Only uses the LDAP Configurations for automatic sync which have the according option activated.

App Management

In-House App DB

Android

Here you can upload the Android Apps that your company has developed and distribute them later in Mobile Management in device or group profiles.

Please be aware that we advice to only distribute Apps this way, which are not available in the Google Play Store.

Click on the “+” to upload the APK of an App you want to upload. Only the APK format is currently supported.

The upload limit on OnPremise Appliances can be increased in Step 3 of the Appliance Configuration. If you would like to increase the Upload Limit on Cloud, please contact the support for more information.

Be aware that usually APKs are a bit smaller than their content. It is possible that an upload fails due to this, since the APK is unpacked in the process. E.g. it is possible that a 95MB APK fails with an 100MB upload limit. In this case, increase the upload limit as mentioned above.

We also advice to first manually move the APK to one test device (e.g. via USB) and try to install it manually with the Files app of the device. If this does not work for any reason, it will also fail via MDM.

Update Target

With the „Update Target“ feature you can choose which version of an app should be installed or to which version an app should be updated if you activated „Keep up to date“ for an app.

If you have not selected an Update Target, the highest version will be used.

Keep in mind that Android cannot downgrade apps. Also be aware that the “Version Code” determines whether or not a version is higher, lower or the same. So get sure to correctly increase this version in your app when building an update.

iOS

Here you can upload the iOS Apps that you developed and distribute them later in Mobile Management in your device or group profile.

Click on the “+” to upload the IPA of an App you want to upload. Only the IPA format is supported as of now.

The upload limit on OnPremise Appliances can be increased in Step 3 of the Appliance Configuration. If you would like to increase the Upload Limit on Cloud, please contact the support for more information.

Update Target

With the „Update Target“ feature you can choose which version of an app should be installed or to which version an app should be updated if you activated „Keep up to date“ for an app.

If you have not selected an Update Target, the highest version will be used.

MacOS

Here you can upload the MacOS Apps that you developed and distribute them later in Mobile Management in your device or group profile.

Click on the “+” to upload the PKG of an App you want to upload. Only the PKG format is supported as of now.

The upload limit on OnPremise Appliances can be increased in Step 3 of the Appliance Configuration. If you would like to increase the Upload Limit on Cloud, please contact the support for more information.

Update Target

With the function „Update Target“ you can choose which version of an app should be installed or to which version an app should be updated if you activated „Keep up to date“ for an app.

If you have not selected an Update Target, the highest version will be used.

Windows 10

Here you can upload the Windows 10 Apps and distribute them later in Mobile Management in your device or group profile.

Click on the “+” to upload the APPX, APPXBUNDLE or MSI of an App you want to upload. Only the APPX, APPXBUNDLE or MSI format is supported as of now.

You can also upload and define Dependencies for an App, which will be automatically distributed and installed before installing the desired App.

The upload limit on OnPremise Appliances can be increased in Step 3 of the Appliance Configuration. If you would like to increase the Upload Limit on Cloud, please contact the support for more information.

Update Target

With the function „Update Target“ you can choose which version of an app should be installed or to which version an app should be updated if you activated „Keep up to date“ for an app.

If you have not selected an Update Target, the highest version will be used.

Win32 Package (.exe)

You can also distribute .exe files/installers to your devices.

Package name	The name which will be displayed in the MDM
Description	Description shown in the MDM
Package file	Only .zip files are allowed. Place the files you want to deploy in this zip file.
Deployment context	**System**: The install command runs with system privileges which is higher than "User". Also when using "System" the process has no UI, so it will be silent and the user profile, e.g. environment variables like %AppDat%, is not accessible. **User**: The install command has access to the user profile and it can display UI if necessary. Note: Some processes may only be working in one context. E.g. if a software installs itself into AppData, it will only work when selecting "User"
Install command	The command used to install the program. For example the install command for a zip file containing “setup.exe” in its root, which supports the parameter "/s" for a silent installation the Install command would be "setup.exe /s". Be aware that different software may have different parameters.
Uninstall command	The command to run to uninstall the software via MDM. Usually this points to the uninstaller. For example "C:\Program Files\ExampleSoftware\uninstall.exe".
Requirements	
Note: All of the set requirements have to be fulfilled for the software to install. Otherwise it will not be installed. Some fields may be mandatory. If no value is set for a requirement, the requirement will be ignored.	
OS architecture	OS architecture
Min OS Version	Min OS Version
Min free disk space (MB)	Min free disk space (MB)
Min physical memory (MB)	Min physical memory (MB)
Min number of logical processors	Min number of logical processors
Min CPU Speed (MHz)	Min CPU Speed (MHz)
Additional Requirements	You can also manually define rules or upload a script here to perform additional requirement checks if you want to.
Detection Rules	

Detection method	Here you can define how to detect whether the app is installed on the device. Install commands will only be run when these rules detect that the app is NOT installed. Uninstall commands only run when these rules detect that the app is not installed. **Manually define rules**: Lets you manually define one or more rules to check for example if a certain file, folder, MSI or registry key being present. If all of the given detection rules are true, the app will be considered present. **Use script**: Upload your own script with your own checks. If the script returns "$TRUE", the app will be considered present.
Detection rules	

App Settings

iOS App Settings

Here you can define the default settings for adding an app to the mandatory apps or enterprise app store.

Note: This only sets what is selected by default when adding apps. This does NOT change existing settings for apps which are already added in the mandatory apps or enterprise app store.

Keep up to date	Automatically keeps the app up to date. Please be aware that it can take up to 7 days after an update is released until the app is updated.
Overtake when unmanaged	If an App is already installed as unmanaged (by the user) the app will be overtaken and managed by the MDM.
Remove app when MDM profile is removed	Uninstalls the App when the MDM is removed.
Prevent backup of the app data	Prevents the backup of the app data.

Android App Settings

Here you can define the default settings for adding an app to the mandatory apps or enterprise app store.

Note: This only sets what is selected by default when adding. This does NOT change the settings for apps which are already added in the mandatory apps or enterprise app store.

Keep up to date	Automatically keeps the app up to date. Only available for InHouse Apps.
Controlled AppTec360 EMM Client Update	If enabled, Admins can specify the update target for the AppTec360 EMM Client. A list of all available versions of the AppTec360 EMM Client will be shown in "General Settings" → "App Management" → "In-House App DB" → "Android".

Third Party Apps

Android

Here you can set your Activation Code for Ikarus.

Set this to “Use Activation Code” and enter your Activation Code here.

Note: After entering the Code and saving, the Code is not yet added to the profile which gets sent to the device. You have to perform any change in your profile for the code to be added to the profile. E.g. change any Switch in the Profile from off → on → off – Save → Assign now.

iOS

Here you can enter your SecurePIM License. After entering the license, press „Save Changes“ and you can use the SecurePIM options.

VPP / KNOX Premium

Apples Volume Purchase Program (VPP) allows you to easily distribute paid and free Apps to your devices. This is highly recommended since you do not need an Apple ID on the devices, users do not have to confirm the installation (supervised), users will not have to enter the password of the Apple ID and you can easily distribute paid Apps without buying them on every Device again.

To use VPP you have to register in the Apple Business Manager.

VPP Licenses

Here you can get an overview over your VPP Apps, how many Licenses are used and how many are available.

Clicking the Wheel will let you see which devices have a License assigned and what the Status of this Assignment is.

Clicking on the refreshes the VPP Cache which compares the Licenses assigned in the MDM with the Licenses assigned on Apples side. This can resolve License Problems in some cases.

VPP Token

Here you can upload the your VPP Token, which can be found in the Apple Business Manager in Settings → Apps & Books. You can upload multiple VPP Tokens.

You can renew a Token by simply downloading a new one in the Apple Business Manager, click on the “Edit” Wheel and upload the new one.

The “VPP Mode” decides how the License Assignment is handled. Depending on your scenario, you have to use different modes:

“Device based” has to be used when enrolling the devices via QR Code, Link, Apple Configurator or DEP.

“User based” is required if the Devices are enrolled with the User Enrollment or as Shared iPad.

If you enable “Automated License Management“, users that are moved from one group to another will automatically be assigned Apple VPP licenses based on the group profile that they are moved too.

Existing Apple VPP licenses from the group they have moved from will not be revoked.

New users added to a group will automatically be assigned Apple VPP Licenses based on the respective group profile.

KNOX Premium Key

Here you can enter your KNOX Premium Key to use the Samsung KNOX Container.

Please be aware that this is no longer supported since Android 10. Use the Android Enterprise Container instead.

App Store Settings

Region & Language

Here you can set the default Language and Region for the App Search in the App Management.

Please be aware that the setting for iTunes also defines how the system grabs information about certain apps. If you encounter Apps in your lists which are displayed in a weird way (e.g. missing icon) you maybe have set a region where the specific App is not available.

AE Play Store

Here you can find all the Options for the Play Store for Android Enterprise Devices to approve Apps, upload own Apps to the Play Store or create your own Web Apps.

Approved Apps

Here you can get an Overview over all the Apps you have approved.

Play Store Apps

This will load an iFrame showing the Play Store. Search for any App you want, click on it and approve it. While approving the App you can also define that the approval gets revoked if the permissions required change. We recommend leaving these settings default when approving Apps.

After an App has been approved, you can add it to your profiles.

The “Approve” button will change to “Revoke approval” after approving it, so you can always remove the Apps if you do not need them anymore.

Private Apps

Here you can upload your own App as a private App to the Google Play Store. This allows you to distribute the App through Googles Services and update it through them. This also has the benefit that your own Apps can be installed without user confirmation which normally is necessary.

Web Apps

Here you can create Web Apps, which are links to certain Web Pages that can be assigned like Apps.

You can also give this a custom Icon and further define how exactly it is displayed.

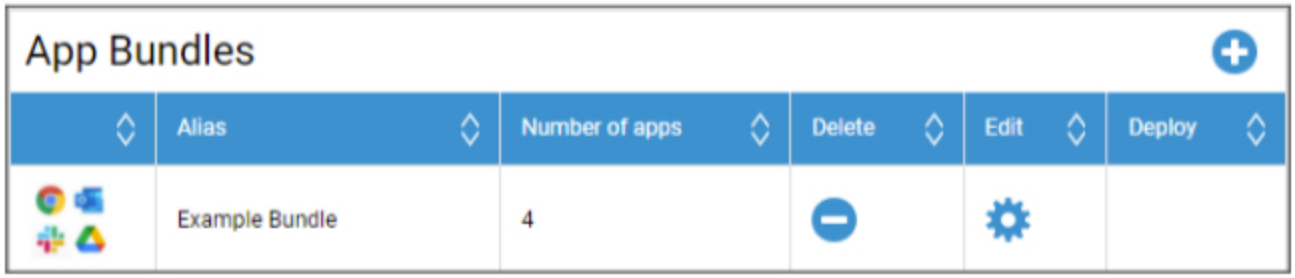
Store Layout

The Store Layout defines how Apps are displayed in the Play Store or if they are displayed at all.

Keep in mind, if you want to show Apps in the Play Store for the user to manually install, these have to be added here in the Layout **AND** in the profile to the Enterprise Play Store. If you add an App to only one of them, it will not be displayed.

App Bundle

With App Bundles you can define groups of apps which can be assigned to device or group profiles with one click.



Click on the “+” to create a new App Bundle. After creating an App Bundle, you can click on “Edit” to add apps from various Sources to the Bundle.

A Bundle can be added to profiles like every other Apps. When adding apps you will have an extra Tab named “App Bundles” where you have your Bundles.

If you make any change to an App Bundle a Button in the column “Deploy” will appear. This will let you push these changes to all profiles containing this Bundle. So keep in mind that you have to manually do this after adding or removing apps in a Bundle.

Remote Control

TeamViewer

TeamViewer Connector

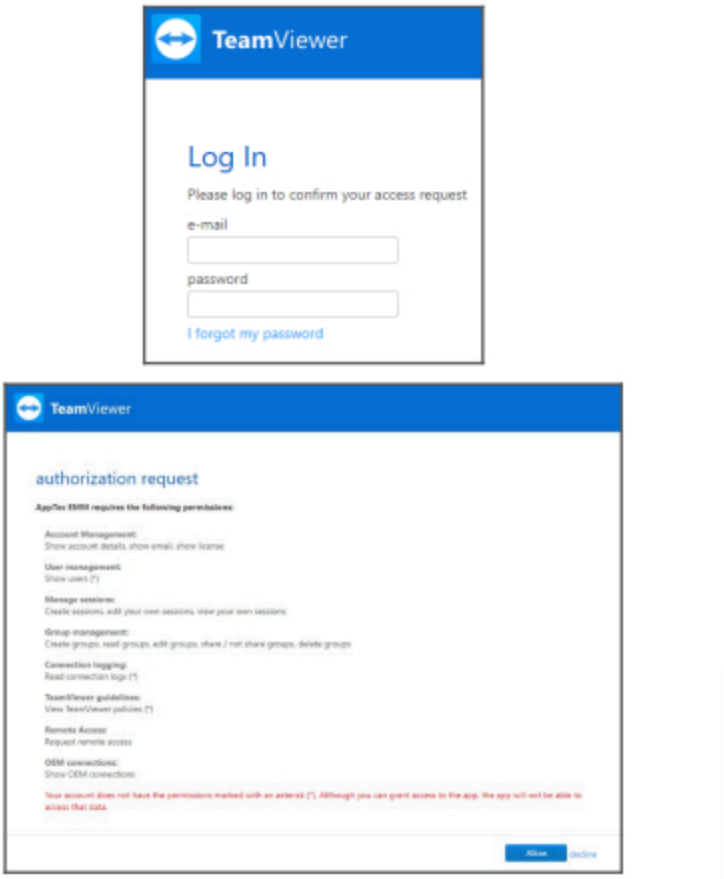
Note: In the free trial on our cloud version you are not able to connect your TeamViewer account. You will have a free demo account linked automatically instead.

Go to General Settings -> Remote Control -> TeamViewer. Here you can link your TeamViewer Account with the console or see information about your currently connected account. Also you are able to view all currently active sessions if you go to “Active Sessions”.

To link your account click on “Start Setup”.

Doing so will forward you to a new page where you have to login with your TeamViewer account.

After logging in, you have authorize the AppTec360 MDM to use this account. After confirming this, you have to wait a few seconds and the Account is connected.


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

Install TeamViewer QuickSupport

Add the app “TeamViewer QuickSupport” to the mandatory apps of your your device profile or group profile and click on “Assign Now”. Wait until the App is installed on the device.

If you try to access a device on which the app is not installed, it will be installed or the asked will be asked to install it, depending on the device configuration.

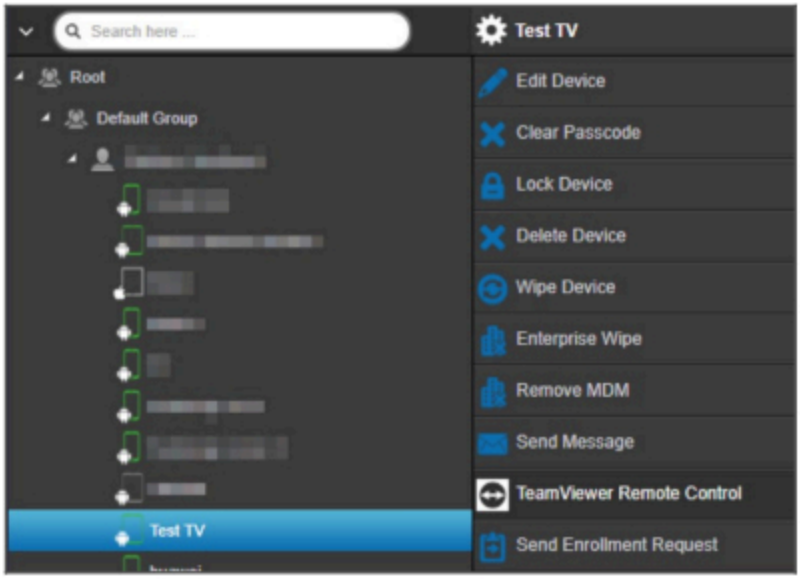
Remote Control your device

To remote control your device, select the device, click on the wheel and choose “TeamViewer Remote Control”

If there is already an active session, you can either use the old session or create a new one.

Confirm that you want to create a new TeamViewer Session.

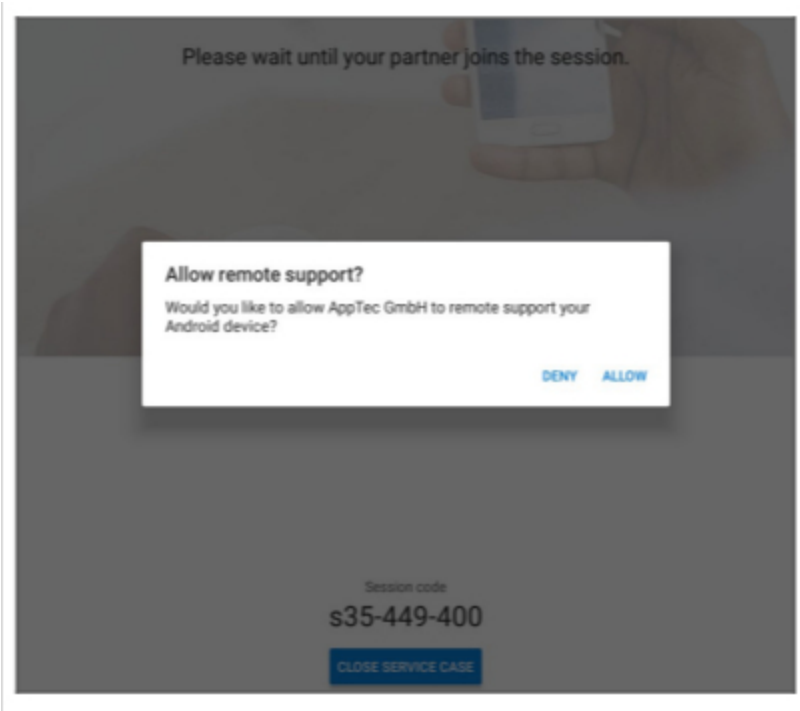
After a few seconds you will get a link for your TeamViewer Session. You can click on “Start” to open this link in a new window.


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

This link will open your installed TeamViewer and connect you to your device.

Now you have to confirm the connection on the device itself to remote control it.

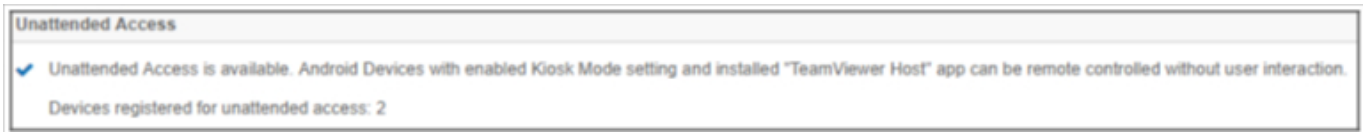


If you are using iOS you will get a message in the AppTec360 MDM Client. With that link the device will join the remote session. Depending on the notification settings of the device it is possible that you will not receive a notification and have to open the AppTec360 MDM Client manually.

On some Android devices (e.g. Samsung) it is required to install an additional app as addon. The TeamViewer app on the device will inform you about that, if this is necessary on your device.

Unattended Access

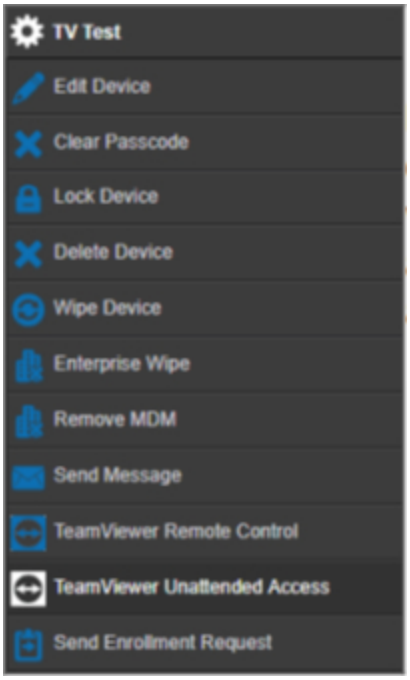
Note: Unattended Access is only possible on Android devices.



You can only connect to your devices, without accepting the connection on the device, if your TeamViewer Account is using a „Tensor“ or „Corporate” License.

You can check this, after linking your account, in „General Settings“

To use the unattended access, you have to install the app „TeamViewer Host“ and activate „Enable Unattended Access“ under „Kiosk Mode & Launcher“ in your profile. Please be aware that this is only possible if you are using the Kiosk Mode.



Now you are able to select the unattended access if you select your device and click on the wheel. This will connect you to your device without any need of confirmation on the device itself. Please be aware that it can take some moments until you get the Link to access your device.

Splashtop

If you enable the Splashtop option, you see the Splashtop configuration options in your profiles.

To use Splashtop, you have to set the Splashtop Streamer (com.splashtop.streamer.csrs) as mandatory app in your profile. Afterwards you can enable the Splashtop Configuration in your profile in “Remote Control”. Enabling this will configure the Splashtop Streamer app. If you are using Splashtop Streamer but not in combination with the MDM, you should leave this off.

In your profile under “Remote Control” you also have to set a deploy code. Go to https://my.splashtop.com and login into your Splashtop account. Click on "Add Computer" and copy the 12 digit deploy code from the resulting page.

Without the Deploy Code remote control is NOT possible.

After doing so, you can right click your device and start a remote Session by clicking on “Splashtop Remote Control”

Sim Card Management

CSV Bulk Import

This shows an overview over your assigned Sim Cards and all information about them. This helps you having all the information, not only about your devices but also about your Sim Cards in one system.

NOTE: This is a manual management/documentation. It is not possible to get this data automatically from devices due to privacy/security mechanisms of the operating systems.

You can also ex- and import this list as CSV.

Carrier & Tariff

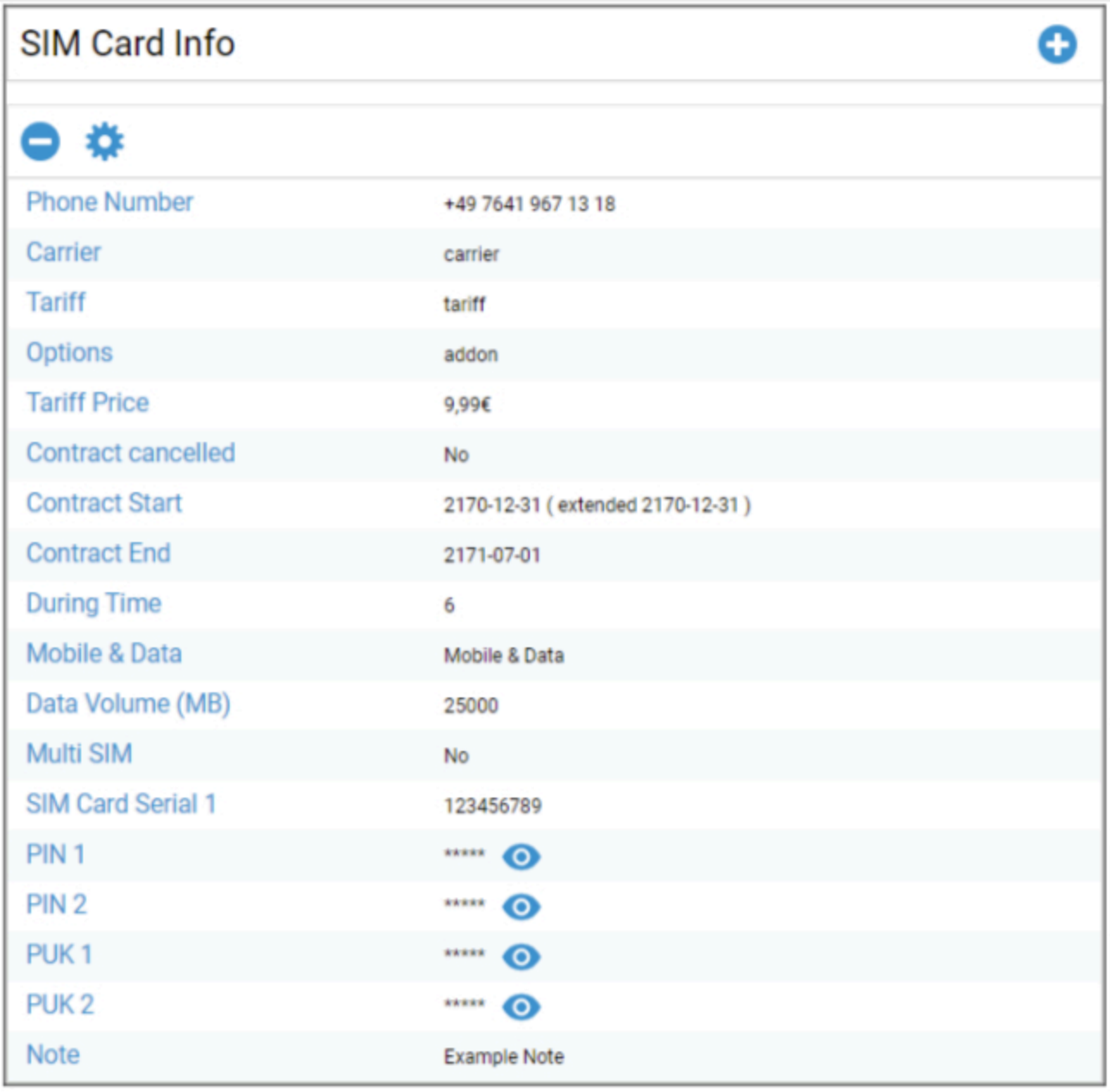
To add a Sim card, first click on the Button to add one or multiple carrier.

Afterwards click on the “+” on “Tariff Information” to add a Tariff to a carrier.

Optionally you can add optional Add-Ons below if you have something like this.

This prepared everything you need to add an actual Sim Card. Sim Cards are currently assigned to a User. Therefore go to the Mobile Management, select a User and go to “Sim Card Overview.

Here you see the Sim Cards of this users. If there is one, you can edit or remove it. Users can have multiple Sim Cards.

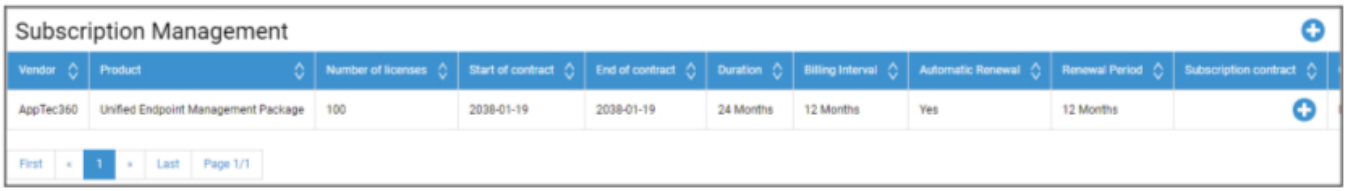


Click on the “+” to add a Sim Card and add all the Info you need. These Sim Cards will also be listed in the list of all your Sim Cards in General Settings → Sim Card Management.

Subscription Management

Subscription Management

Here you can document running subscriptions, their details and also store different files, e.g. signed contract, Letter of termination, etc. You can also set up reminders that remind you per mail before the subscription ends and maybe extends automatically.



Click on the “+” at the top to add a subscription. You can add as many subscriptions as you want.

Click on the “+” in the different fields to upload files regarding this Subscription. You can technically upload any file type but be aware that not every file type can be previewed in the browser.

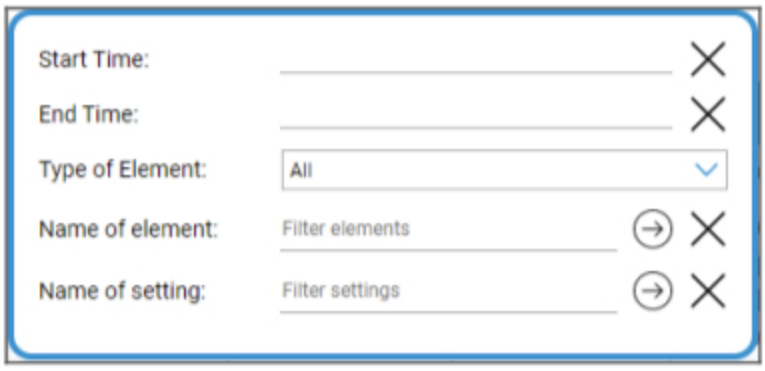
General Audit Log

Audit Log

Here you have a general Audit Log which shows all changes made. While the Audit Log in a user or group only shows changes according to this user or group, this shows EVERY change made anywhere in the console.

You can see what has been changed, by who, when and where. In some cases you can also extend the Entry to see further details.

It is possible to click on the user or on the entry in “Path / Type” to get to the location where the change has been made.



On the top right you are also able to define a filter which can help to find certain changes in an environment where many changes are happening.

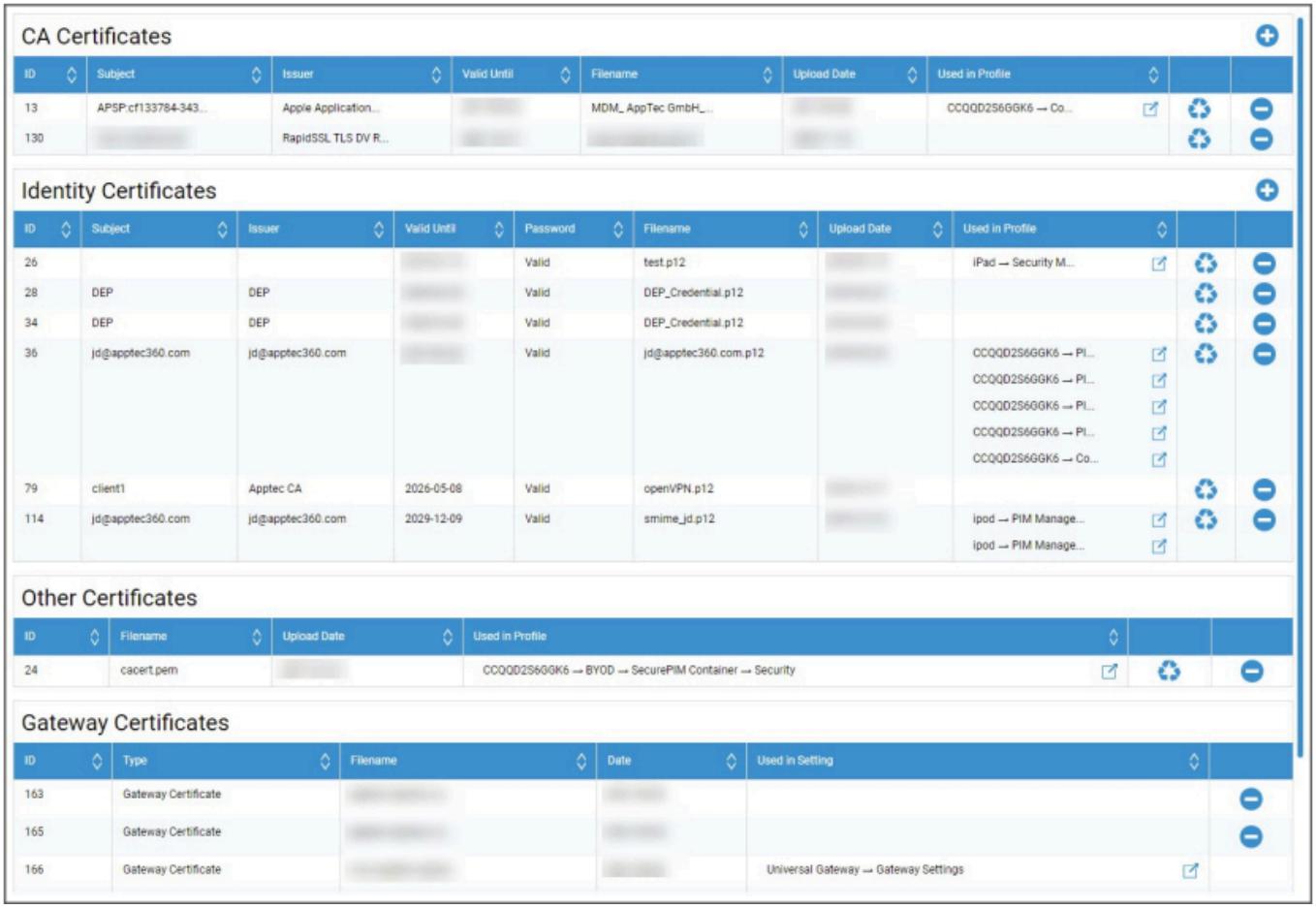
Audit Log Settings

“Audit Log Retention Period” defines how long the Audit Logs should be retained before deletion.

Certificate Management

Here you will get an overview over all certificates uploaded and used in the Console. This is only an overview. The actual configuration for e.g. Wi-Fi certificates is still done in the profile at the corresponding location.

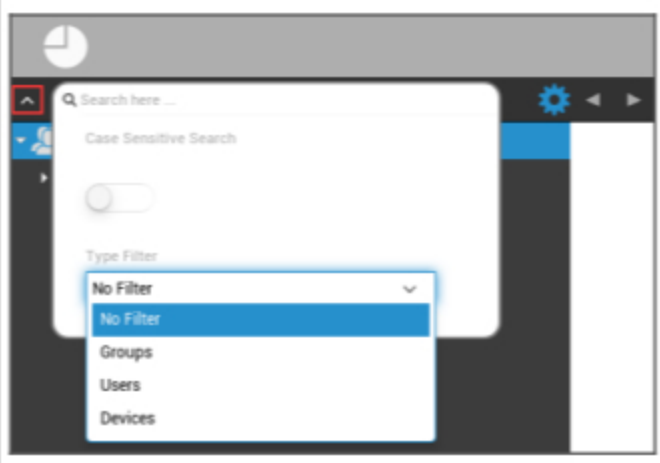
Here you can also remove or update certificates, which will automatically be reflected in the affected profiles. Click on the info in “Used in Profile” to see where exactly any certificate is still assigned.



Mobile Management

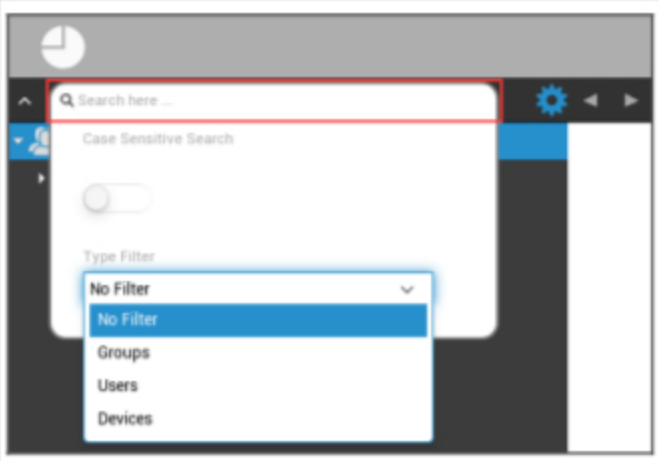
Mobile Management Screen

Device filter



With a click in the upper left hand corner of the screen, you can find a variety of filters for the display of devices.

Search window



The search window allows you to search all devices and/or users with a specific keyword.

Options gear

After clicking on the respective symbol, a list of options that are available to you, is displayed.

These change with every current window and are explained in the respective chapters.

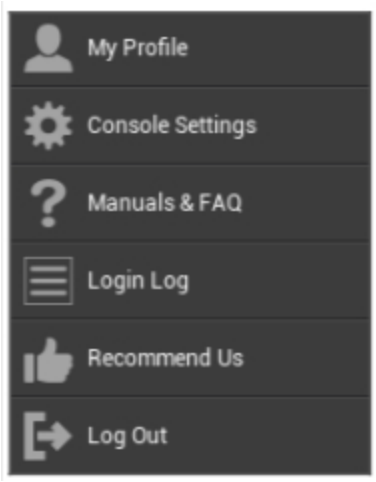
Navigation arrows

With a click on the left arrow, you will be taken to the previous page.

Afterwards, with a click on the right arrow, you will be taken to the page that you just left.

Administration account-settings

Clicking on the email address as seen above displays the following menu:



My Profile	Edit the admins account details
Console Settings	Configure console settings for the Admins account
Manuals & FAQ	View the „Manuals & FAQ“ page in „General Settings“
Login Log	Access the „Login Log“
Recommend Us	View the „Recommend Us“ page in „General Settings“
Log Out	Log out of the MDM console

User Information

Here you can edit the account details of the currently logged in admin.

Username	User name and/or email address of the account
Name	Administrators first name
Last Name	Administrators last name
Login Name	Administrators login name
eMail Address	Administrators email address
Alternative eMail address	Administrators alternate email address
Picture	Profile picture
Phone Number	Administrators phone number
Mobile Number	Administrators mobile number
Phone Extension	Phone extension
Location	Location
Position	Position in the company
Usergroup	Select to which user group you want to assign the admin account
Comment	Enter a comment
Enter new password	Enter the password for a change in password
Repeat new password	Repeat the new password to confirm

Please note, that the administration access can also be filed as a local user account in the hierarchy structure. Without the establishment of an additional administrator, this one should not be deleted!

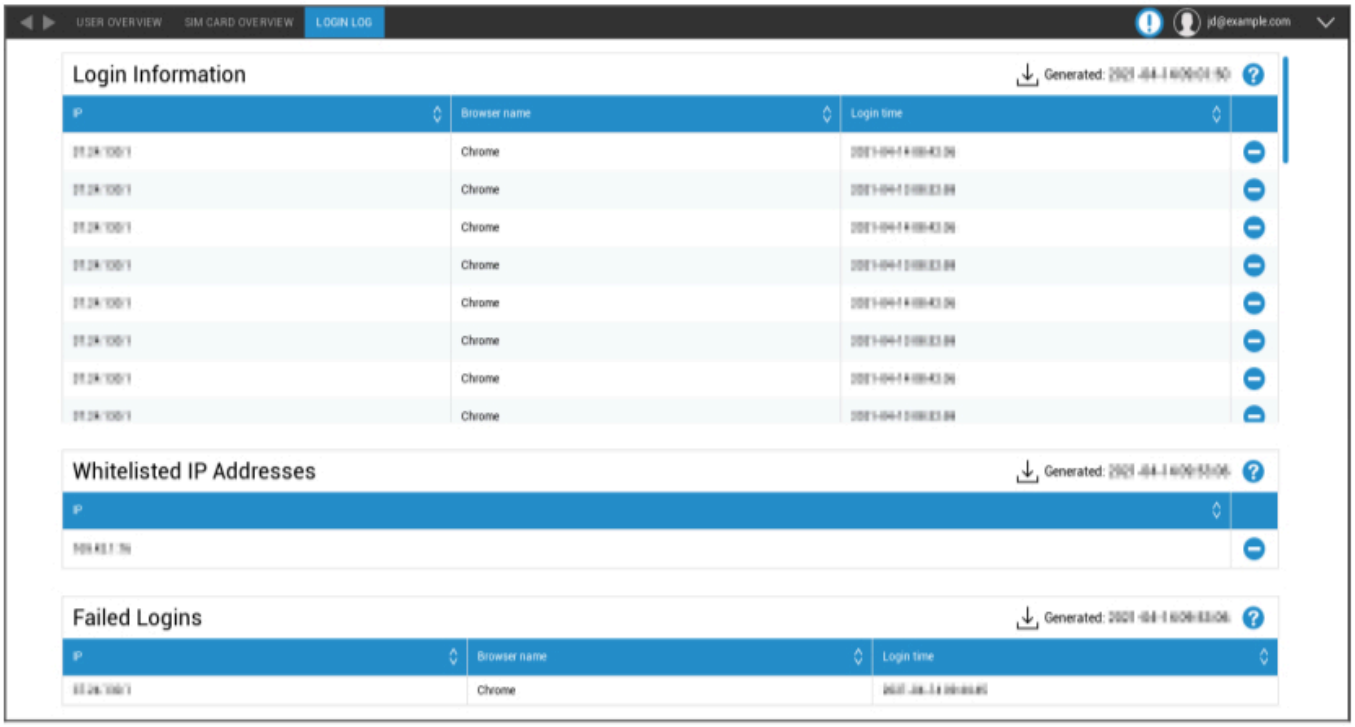
Console Settings

Here you can configure the following console settings for the Admins account:

Directory User Display Options	Define how users should be labeled in the tree
Directory Device Display Options	Define how devices should be labeled in the tree
Session Timeout	If the user doesn't do anything in the specified time, the user will be logged out. The default value is 60 minutes. Please logout and log on again after changing this setting.
Timezone	Choose the time zone that is used
Time Format	Choose how timestamps should be displayed
Console Language	Choose the language in which the console should be displayed. English and German are available.
Main Color	You can set a color which will be used as base for the color scheme of the console. You can either use the color picker, or enter a color in HTML HEX notation. RGB formators like 'pink', 'yellow' work aswell.
Save Command	The key combination to trigger a save without pressing the "Save"-button.
Use Two-Factor Authentication	Enable the use of two-factor authentication when logging in. You will recieve an email upon login with a code that you'll have to enter to log in.
Two-Factor Authentication Timeout	Set a time period during which you will be not asked for a two-factor authentication after an already successful authentication.
Send Verification Code via	The verification code will be sent to the options selected. The device message will be shown in the AppTec360 MDM App on all Android and iOS devices that belong to you.
Send login message after login	If enabled an email will be sent for every login from an ip address that isn't whitelisted. The email contains information about the login (e.g. IP, Browser).

Login Log

Here you can see information regarding the logins of the currently logged in admin account.



Login Information	A list containing the logins of the currently logged in admin account that was recorded by the console. This list shows all your successful logins in the last 30 days.
Whitelisted IP Addresses	This is the list of all of your whitelisted IP addresses. If you login from an IP which is listed here you will not get the login message. You can add an IP address to this list by clicking on the button next to an entry in the „Login Information“ list above. You can remove an IP address from this list by clicking on the button next to an entry in this list or in the „Login Information“ list above.
Failed Logins	This is a list of all of the failed login attempts in the last 30 days. If you failed to enter the correct password at least 3 times in 20 minutes an entry will appear in this list. You will also be informed about failed login attempts via email.

Corporate administration (Root-Node) in Mobile Management

When you have reached the Root-Node (first group), you can perform a variety of settings for you company, in regards to Mobile Management.

Create a Subgroup	Create a subgroup
Rename Root Node	Renaming of the Root-Node (ex. your company name)
Mass Enrollment	Enroll multiple devices /users at the same time
Mass Assignment	Assign a profile for the respective groups, with one look
Quick App Administration	Send (Un-)Installation requests for an application to the respective groups devices
CSV User Import	Import Users from CSV into the respective group

Create a Subgroup

With “Create a Subgroup” you can create an additional subgroup.

You can establish under which group the subgroup should be assigned.

(By default, a new group is created that is assigned as a subgroup in the root-node)

Rename Root Node

Here you can rename your root-name. It is common, that the company name is used in this instance.

Mass Enrollment

With “Mass Enrollment“ you can enroll multiple devices and users.

You can select directly in what manner the user should receive the enrollment (eMail; alternative eMail; SMS)

Depending on which device the user is going to receive (iOS, Android, Windows Phone), you can directly mark that here.

The distinction of whether it is a Smartphone or a Tablet, can also be configured here, which you will have to select correctly, with a check mark.

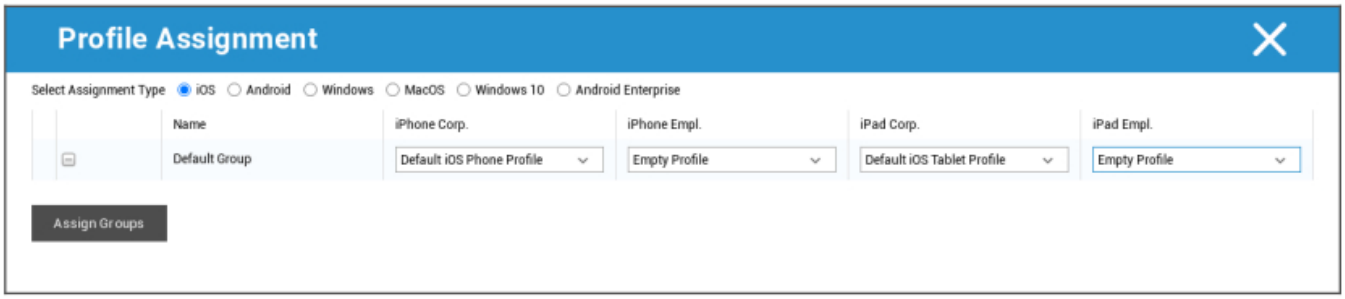
As a final step, you can establish whether the respective device is corporate or private (BYOD).

With the “Export as CSV“, you can export the Information as a CSV data file. In return, you can also import the CSV data file with “Import CSV“, the file should look like the example below:

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

Mass Assignment

Under Mass Assignment you can assign a profile to all groups, this is divided into iOS – Android – Windows – MacOS – Windows 10 – Android Enterprise

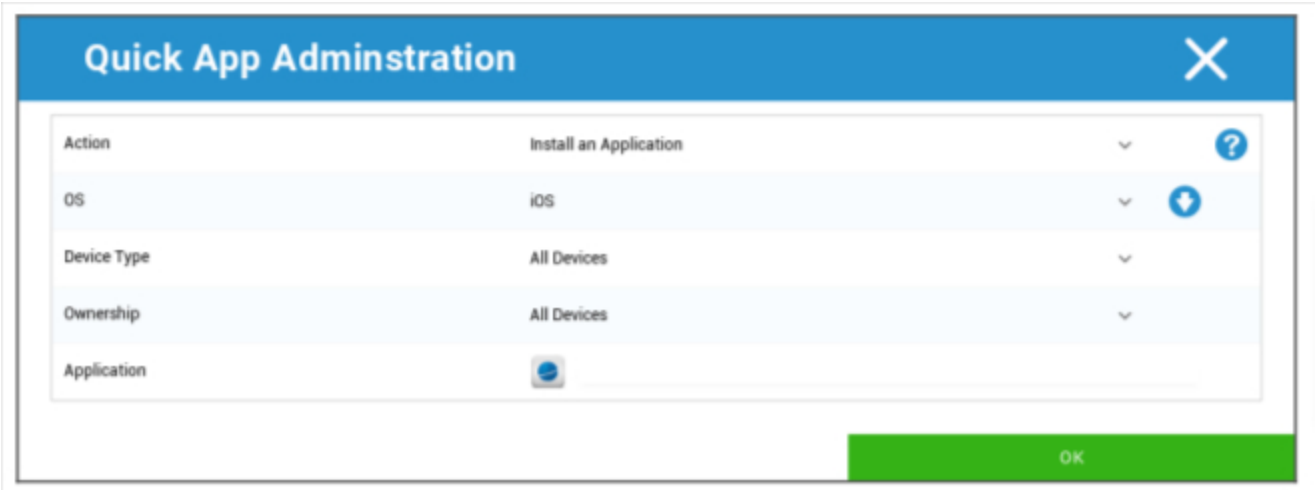


Windows – MacOS – Windows 10 – Android Enterprise

Quick App Administration

Under Quick App Administration you can send Installation or Uninstallation requests for a specified application to an OS of your choice.

You also can define whether the request should be sent to all device types of the selected OS or only to a specific device type.



CSV User Import

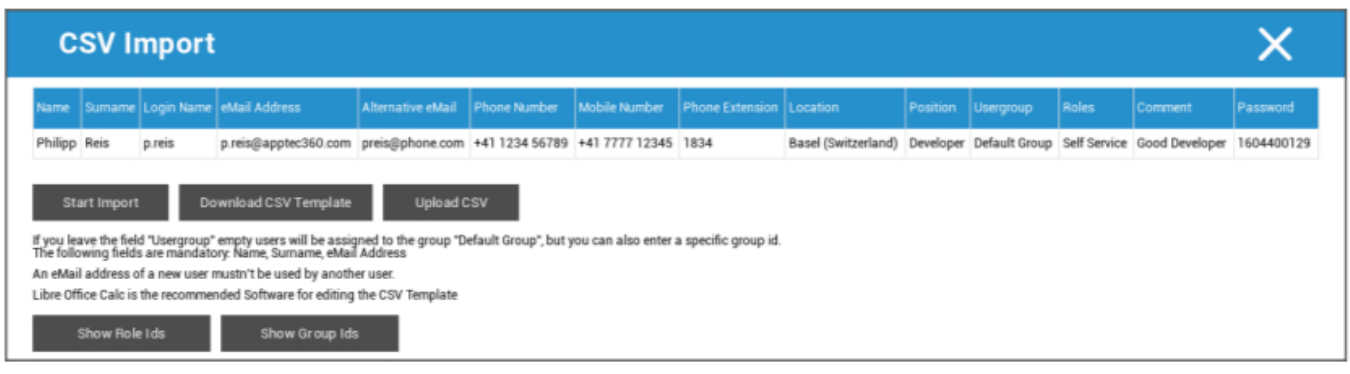
Import Users from CSV into the respective group.

With “Download CSV Template“, you can export a CSV template file, which can be filled in (or it can be used as reference).

You can also use the Options “Show Role Ids“ and “Show Group Ids“ as reference to create your own CSV file.

The CSV file can be uploaded to the MDM with “Upload CSV“.

As a final step, you can start the Import by clicking on “Start Import“.



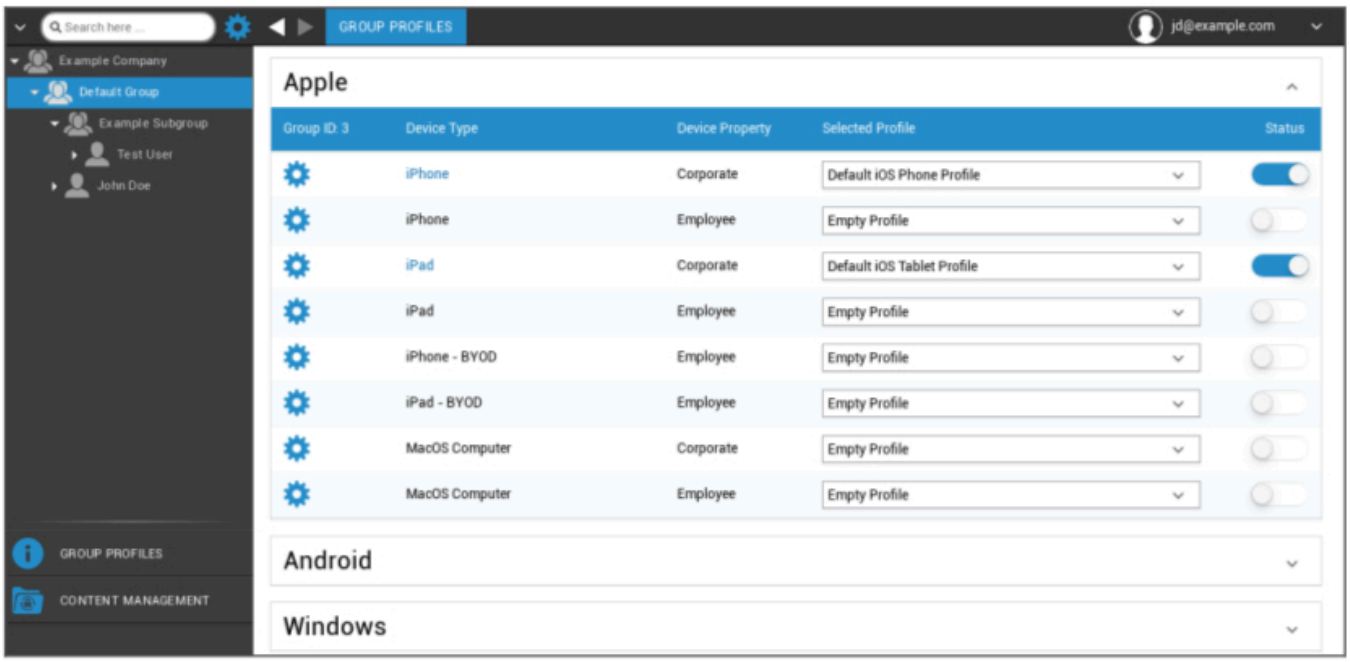
Group Management in Mobile Management

One click on the overview displays the different configuration profiles for the respective platforms.

One profile contains all settings options that can be established with AppTec360 in advance on the end user device. On each platform you can create profiles for corporate devices (Corporate) or Bring-Your-Own-Device devices (Employee).

In order to differentiate configurations for device groups, for example based on location or function, it is advised that several subgroups are created.

Please note the Profile Management in Mobile Management



With the gear menu you set up a variety of settings for the respective (sub)group.

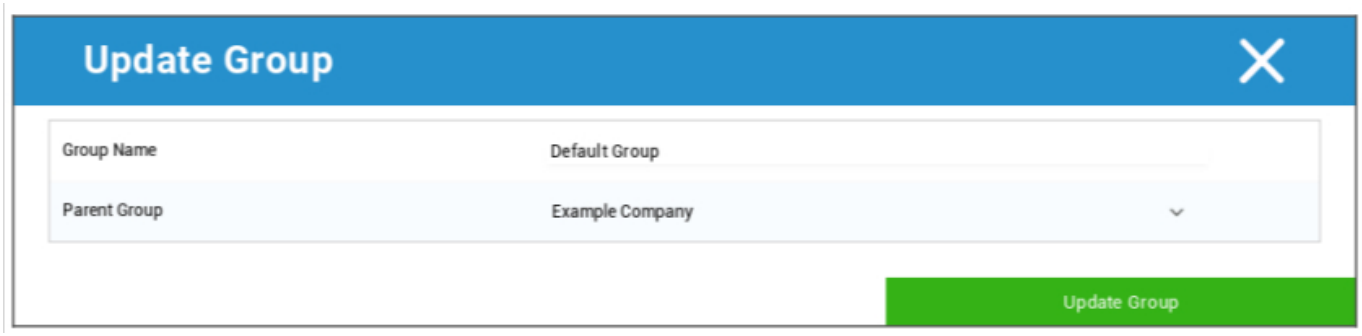
Create a Subgroup	Create subgroup for the respective (sub)group
Edit selected Group	Edit selected group
Delete selected Group	Delete selected group
Mass enrollment	Enroll many devices / users at once for the selected profile
Mass Assignment	Assign profiles to the group that is currently selected
Create a Subgroup	Create subgroup for the respective (sub)group
Create a User	Create a user for the respective (sub)group

Create a Subgroup

With “Create a Subgroup”, you can create an additional subgroup.

You can establish under which group the subgroup is to be assigned (as a default, the subgroup is assigned to the group that is currently selected).

Edit selected Group



Here you can edit the profile – here, the following settings are possible:

- Group name can be changed
- Parent group can be changed

Delete selected Group

Under “delete selected Group“ all the users and devices are listed for you that are in the respective group. Here, you have the option to delete them.

For one user you can perform the following delete commands:

Delete User	User is deleted
Move User To Group:	You can move the user to another group (following column, ex. “Admins)

For one device you can perform the following delete commands:

Wipe & Delete	Wipe and delete device
Delete from System	Remove device only from AppTec

Reference: Mass Enrollment

Reference: Mass Assignment

Create a User

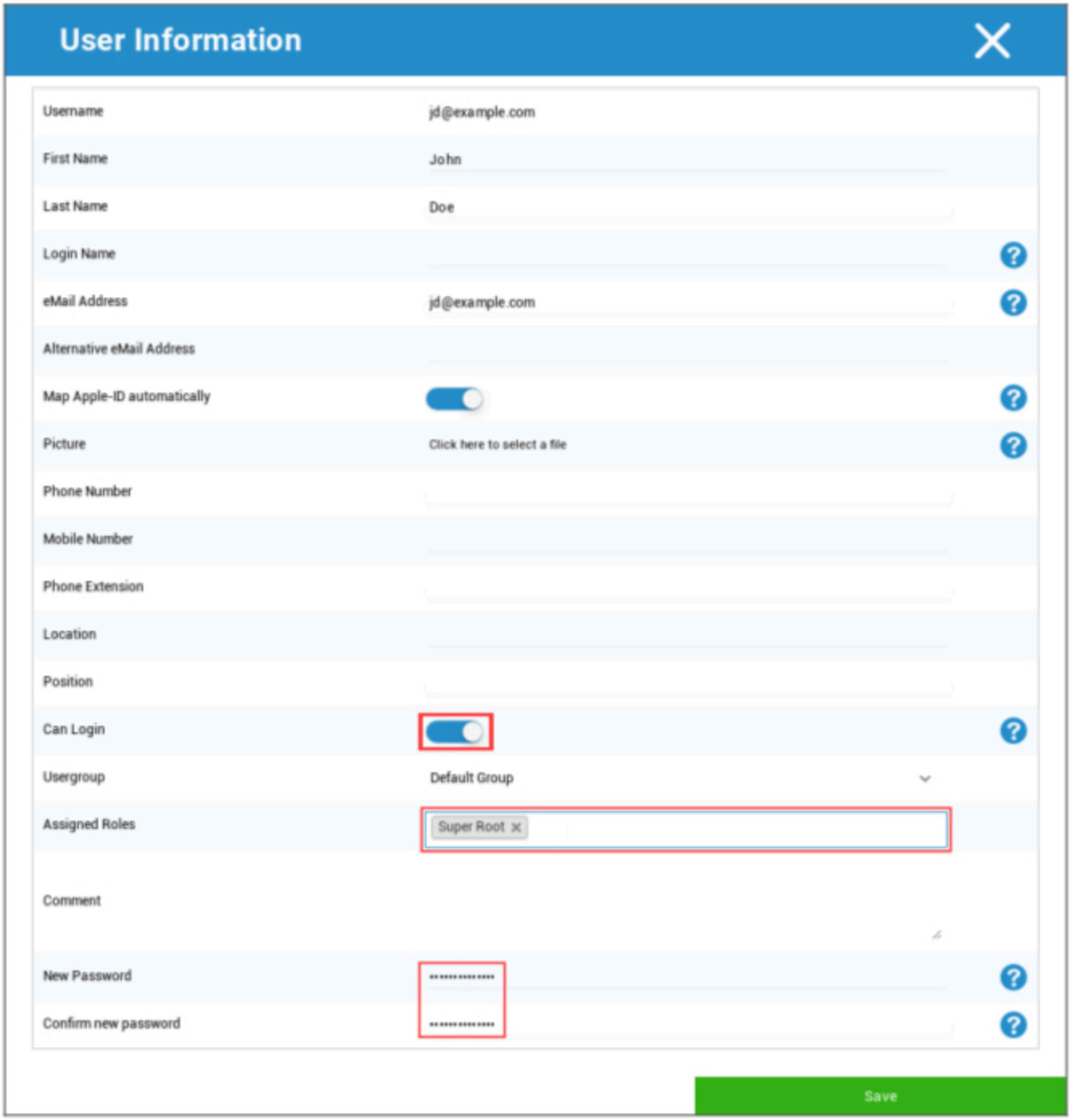
With “Create a User“, you can add a new user.

Create a new Admin-User

You can set a User as Admin-User. Doing so will give him the permissions to login into the console and also change users/groups/devices.

Create a normal User or use an existing User. Choose the User you want to give admin permissions, click on the wheel and choose “Edit User”:

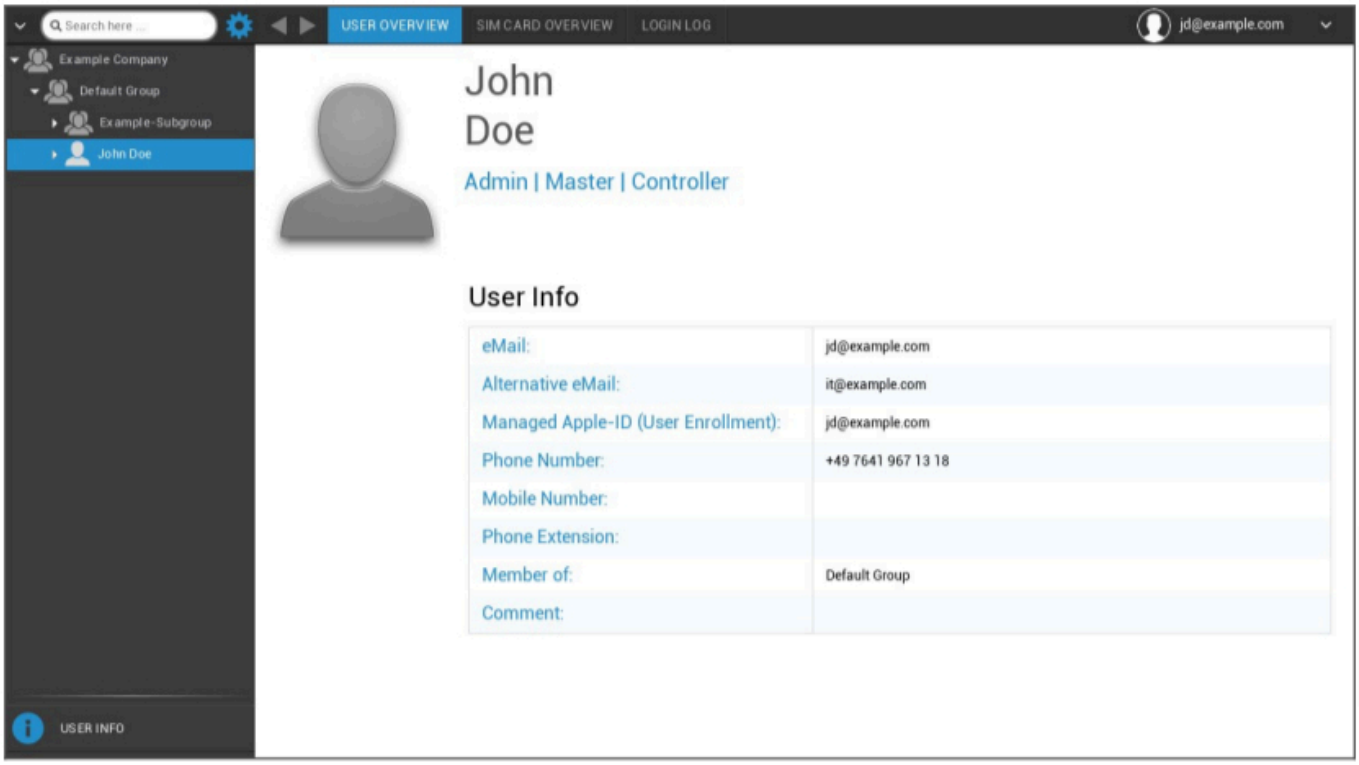
Activate the switch for “Can Login”, assign the “Super-Root” role to the user and set a password.



Save this and the user can now login with the username and password.

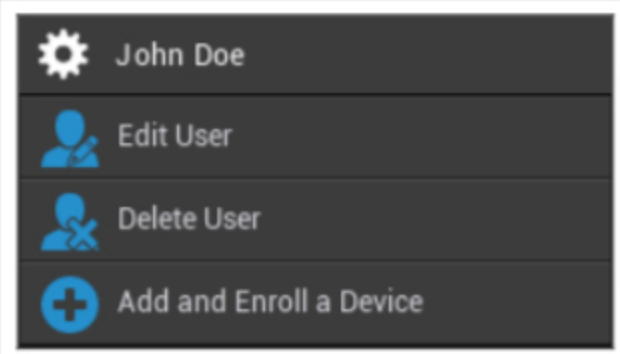
User Management in Mobile Management

When you select a certain user, you will see the following overview:



You will receive an overview of all the information that you entered earlier in “Create a User“.

With the gear that is installed at the top, you can perform the following configurations:



User Name	User Name of selected User
Edit User	Edit user-information
Delete user	Delete user • Delete from System = The device will be removed from AppTec

	• Wipe & Delete = The device will be restored to the factory settings and removed from AppTec
Add and enroll a Device	Enroll a device for the selected user

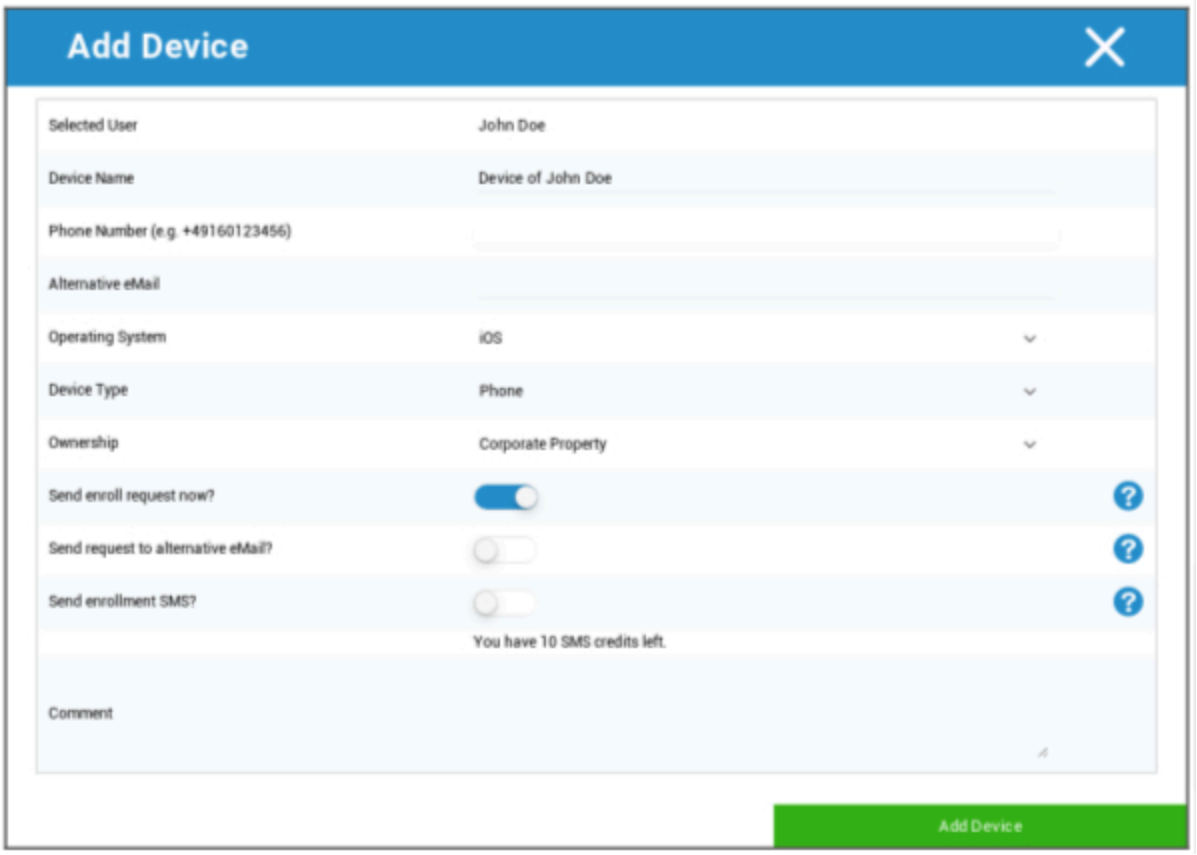
Please note, that the administration access can also be filed as a local user account in the hierarchy structure. Without the establishment of an additional administrator, this one should not be deleted!

Add and enroll a Device

Here you can select a device for the selected use.

Alternatively you can enroll devices into a group directly. To do so, click on the group, click on the wheel and select “Add and enroll a Device”.

You should see the following overview:



Depending on what sort of device you want to enroll, you must perform the following configurations:

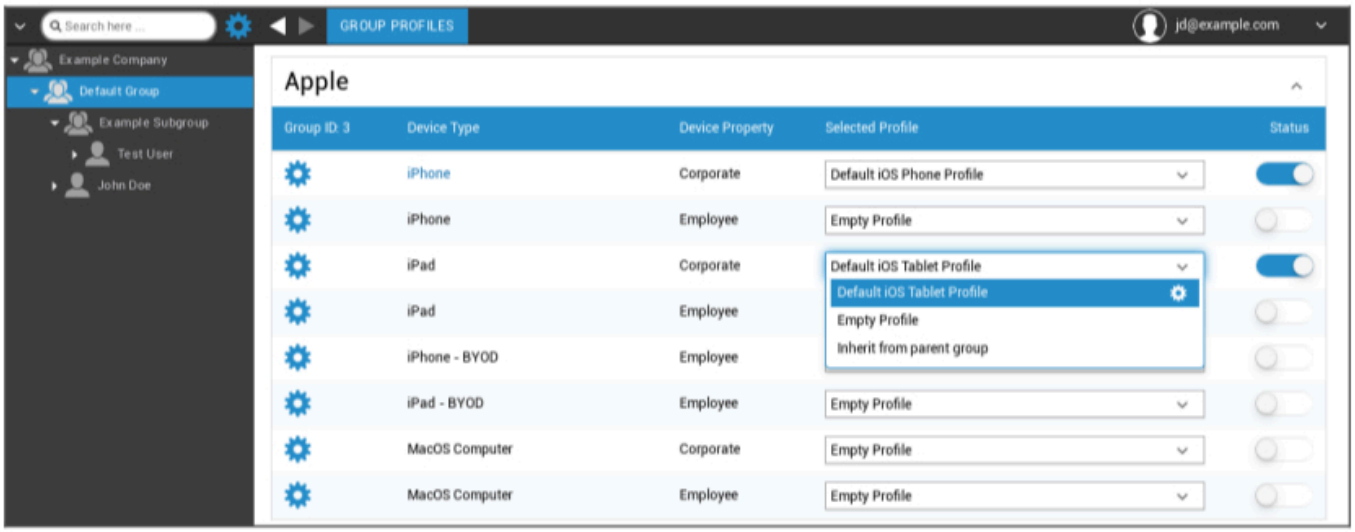
Selected User	Selected user (will be filled in automatically)
Device Name	Will be filled in automatically (device for “user's name“) – can, however, be changed
Phone Number	Telephone number, will be filled in automatically (as long as it was provided by the user) – here, however, it can be added or changed
Alternative eMail	Alternate email, will be filled in automatically (as long as it was provided by the user) – here, however, it can be added or changed
Device Owner	Corporate Property = corporate device Employee Property = BYOD device
Choose operation System	Here, you can choose between the following operating systems: • iOS • iOS BYOD (User Enrollment) • MacOS • Android Enterprise • Android • Windows Mobile • Windows 10
Send enroll request?	The email is sent immediately to the main email address and the user is prompted to connect their device
Send request to alternative eMail?	Send the email additionally or exclusively (in case “Send enroll request?“ was deactivated) to the alternate email address (email is different from the “normal“ enroll Request email)
Send enrollment SMS?	Send an enrollment request via SMS (the “Phone Number“ must be entered)

After the Enrollment Request has been sent, the device will be displayed (marked red) right away.

As soon as the device has been connected successfully, the device will be marked green shortly thereafter and is thereby ready to receive restrictions, apps, etc.

Profile Management in Mobile Management

After clicking on a group, you will receive an overview of all of the device platforms that are to be configured and the respectively assigned profiles.



	Perform the configuration for the selected profile
Device Type	Device type and/or model
Device Property	Device's owner (Corporate = corporate property, Employee = private employee device)
Selected Profile	Selected profile (the gear opens the profile's configuration dialogue)
Status	On/Off (the profile is activated/deactivated)

When you select the gear, you will receive the following options:

Create a profile

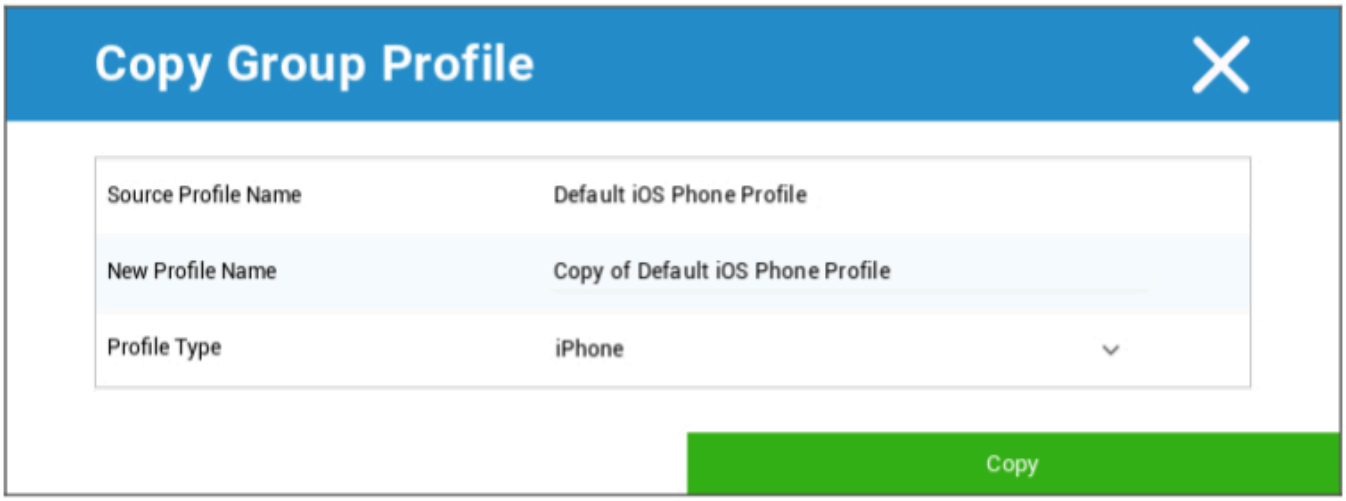
You can create and configure a new profile for each entry and/or platform. After clicking on this sub point, the profile will be created immediately and you can start with the configuration of the iOS, Android und Windows Phone right away.

Edit Profile

After clicking on “Edit Profile“, you will reach the configuration display for the respective profile, where you can set the configurations.

Copy Profile

With the aid of the “Copy Profile“ function, you can copy the set-ups/configurations from an already existing profile and add them to a new profile.

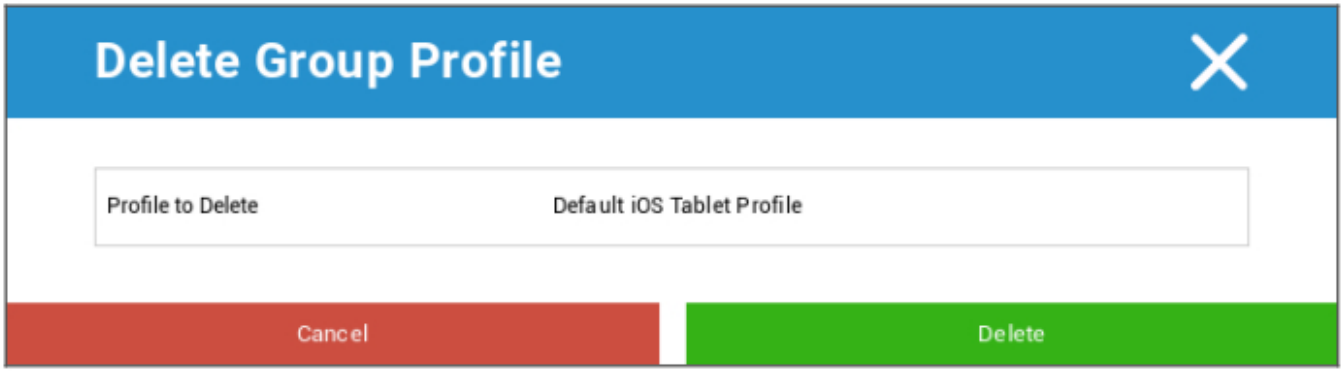


Source Profile Name	Name of the profile that is to be copied
New Profile Name	Name of the new profile
Profile Type	Profile type (Phone/Tablet)

Once you click on “Copy“, the profile will be created and can now be assigned to the group

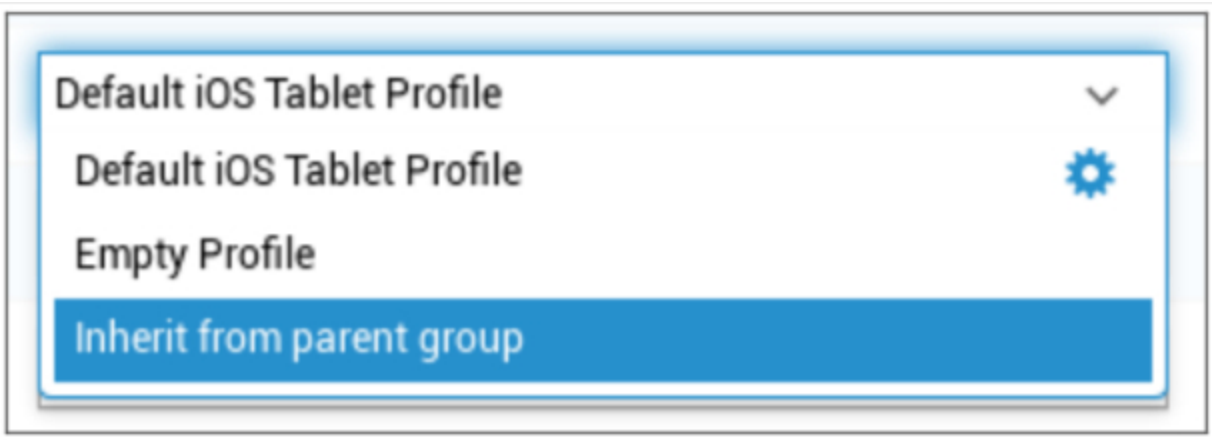
Delete Profile

Here you can permanently delete a profile. Please note, that during the deleting process and the following “Assign Now“ process for the profile, the configuration will disappear on the respective devices of an affected group and cannot be recovered!


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

Inheriting of Profiles

During the selection of the profiles, the option “Inherit from parent group“ is available.



When the profile is activated, then the profile of the parent group will be used for the respectively selected device (and respective device type). Please note also, that changes to this profile could possibly affect numerous groups.

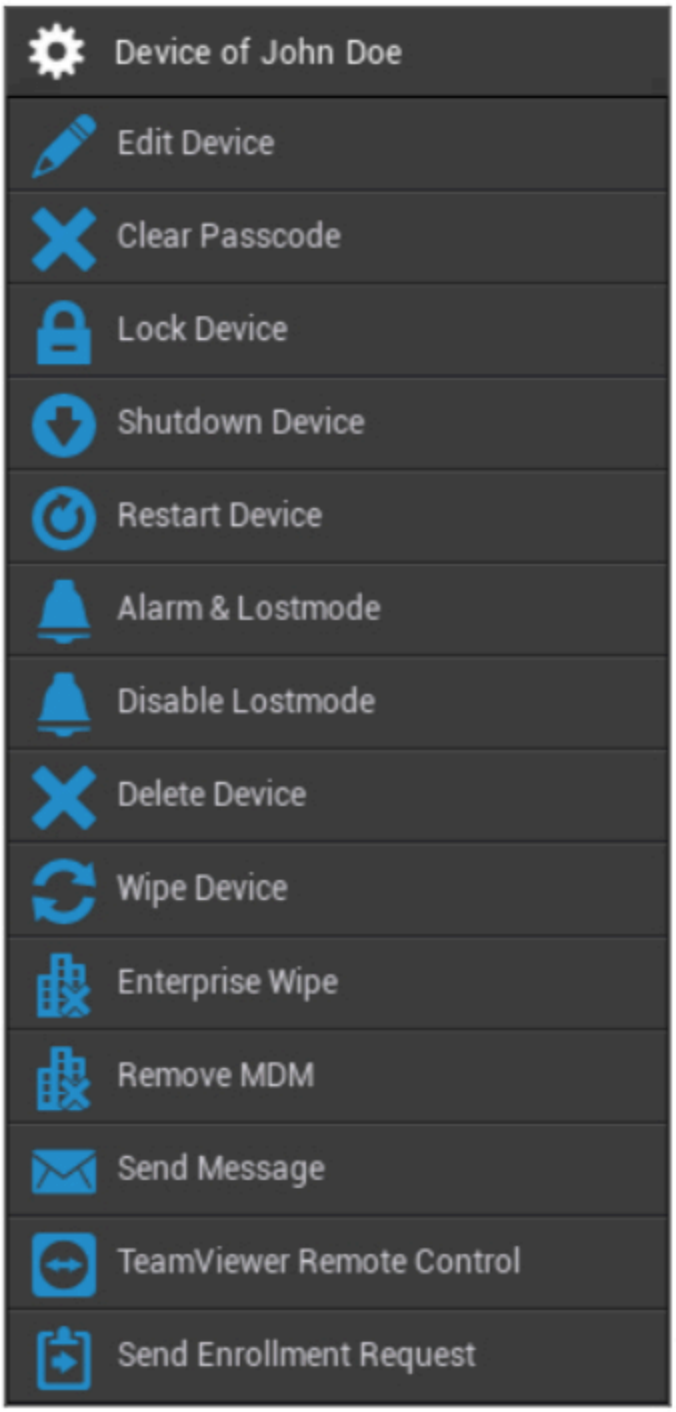
This configuration is set as the default value, when a new subgroup is created.

The configuration “Empty Profile“ is also available, which corresponds to an empty profile, meaning that in the end no new configurations will be performed on the end user device.

Device Management in Mobile Management

When you select a device, you can perform a variety of tasks via the “gear”. These are different, depending on the OS platforms (iOS, Android Enterprise, Android, Windows Mobile, Windows 10).

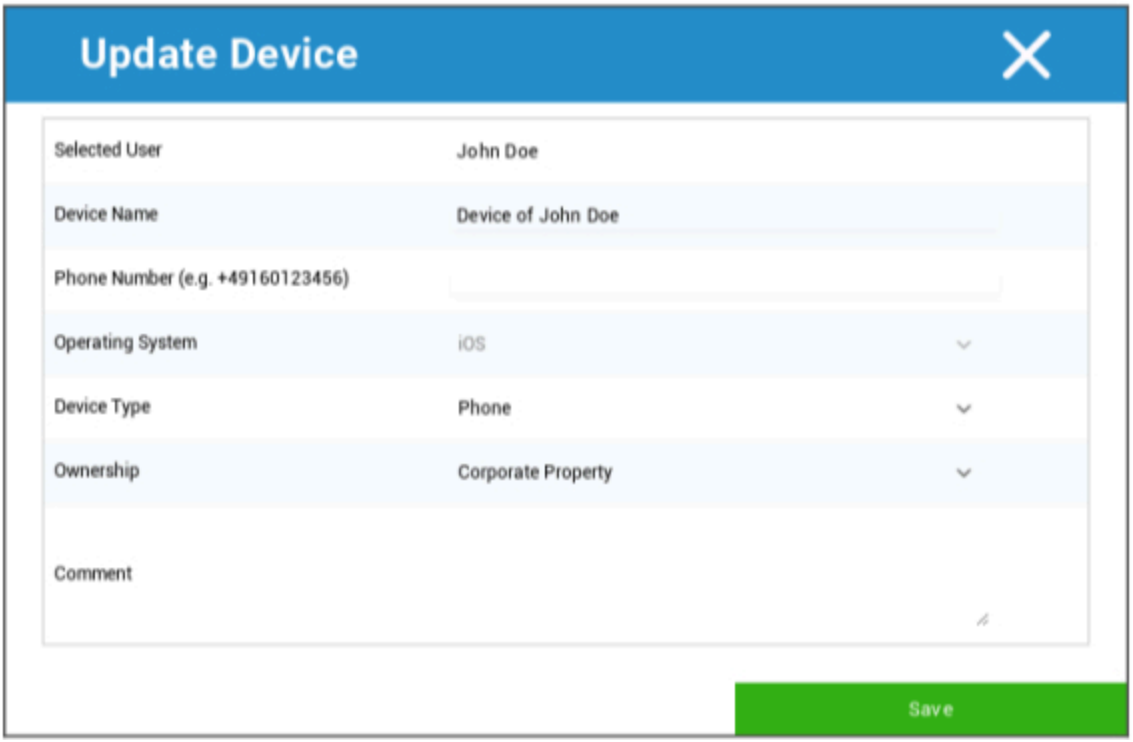
IOS



Edit Device	Edit device
Clear Passcode	The device passcode is erased
Lock Device	Lock device (lock screen)
Shutdown Device	Shutdown device

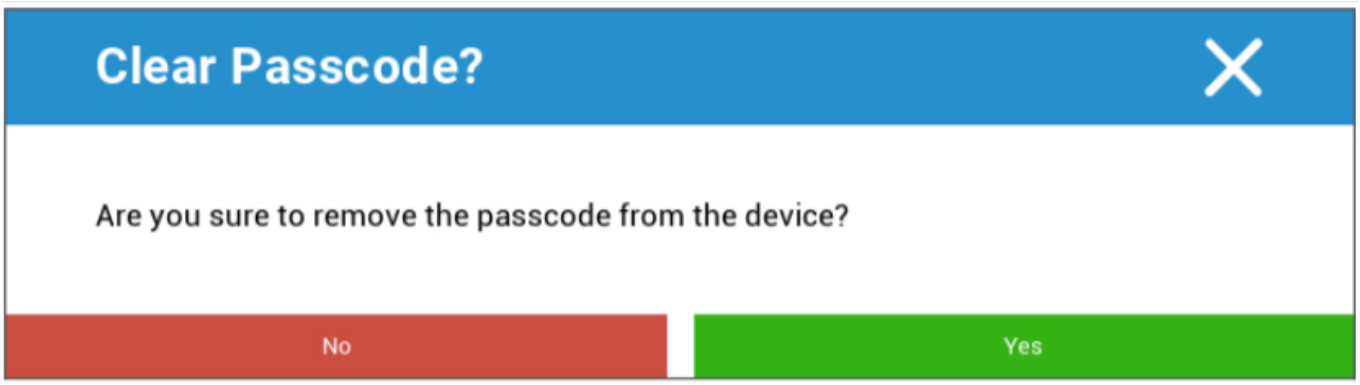
Restart Device	Restart device
Alarm & Lostmode	Start Alarm & Lostmode
Disable Lostmode	Disable Lostmode
Delete Device	Remove device from AppTec
Wipe Device	Restore device to factory settings
Enterprise Wipe	The information, apps and profiles provided by AppTec360 are deleted (device is separated from MDM)
Remove MDM	
Send Message	Send Push Notifications to the device Message will be displayed in the AppTec360 App (Message Tab)
TeamViewer Remote Control	Start Remote Control Session using TeamViewer
Send Enrollment Request	Send (repeated) Enrollment request

Edit Device



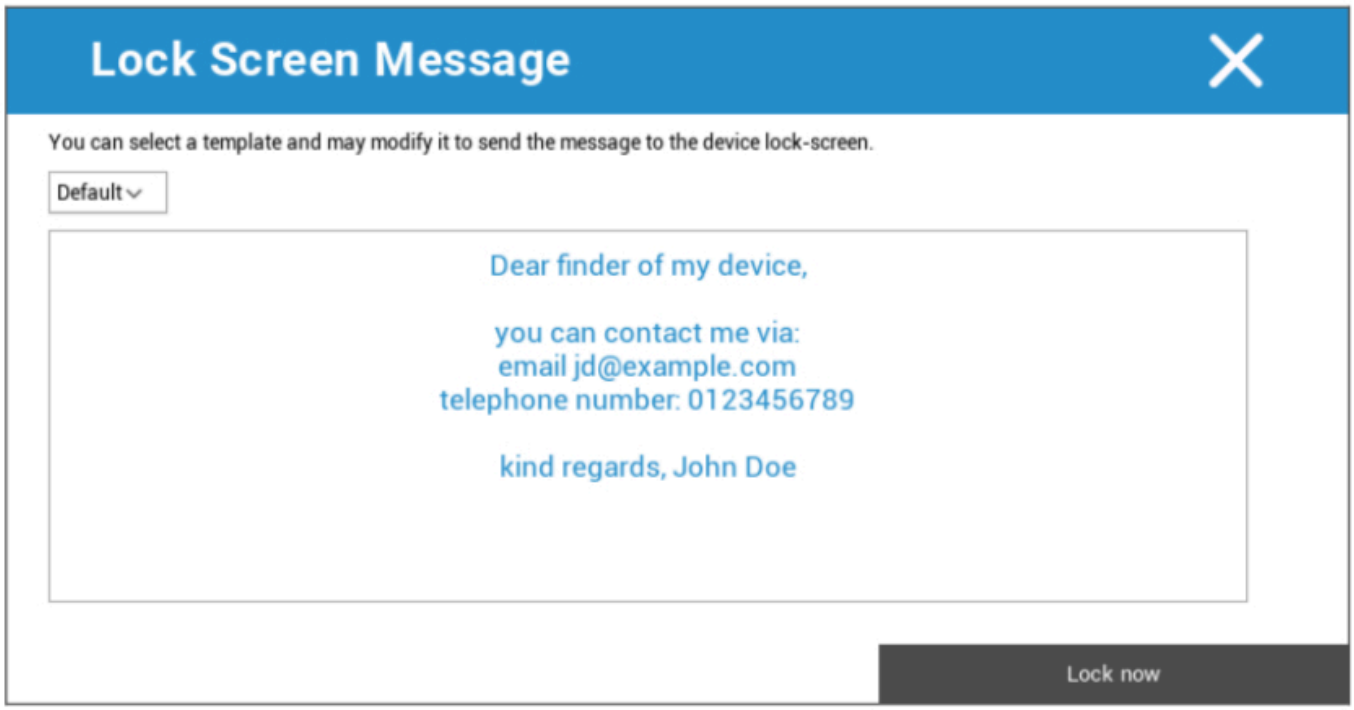
Here you can update a variety of information on the device.

Clear Passcode



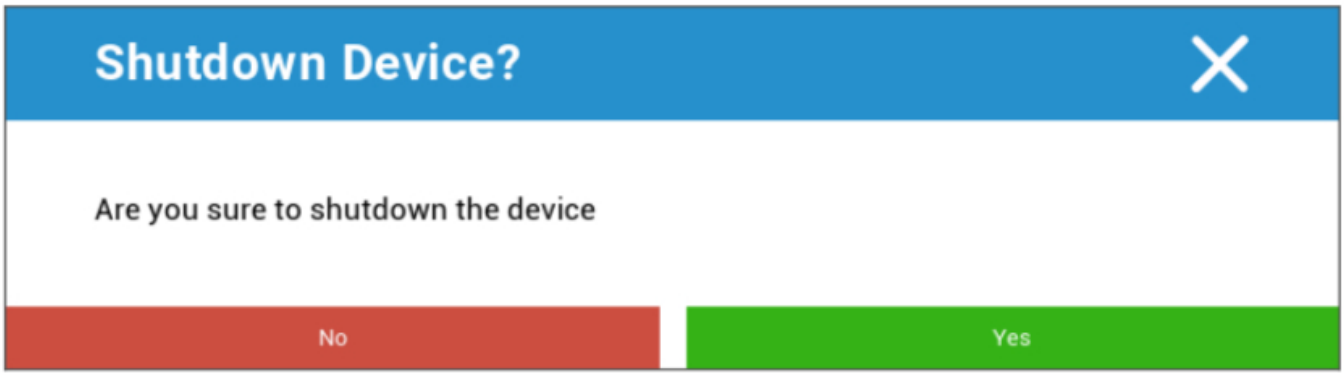
Under “Clear Passcode“ you can remotely remove the passcode from the device. Subsequently, the user will be prompted to issue a new password (depending on Passcode guidelines).

Lock Device



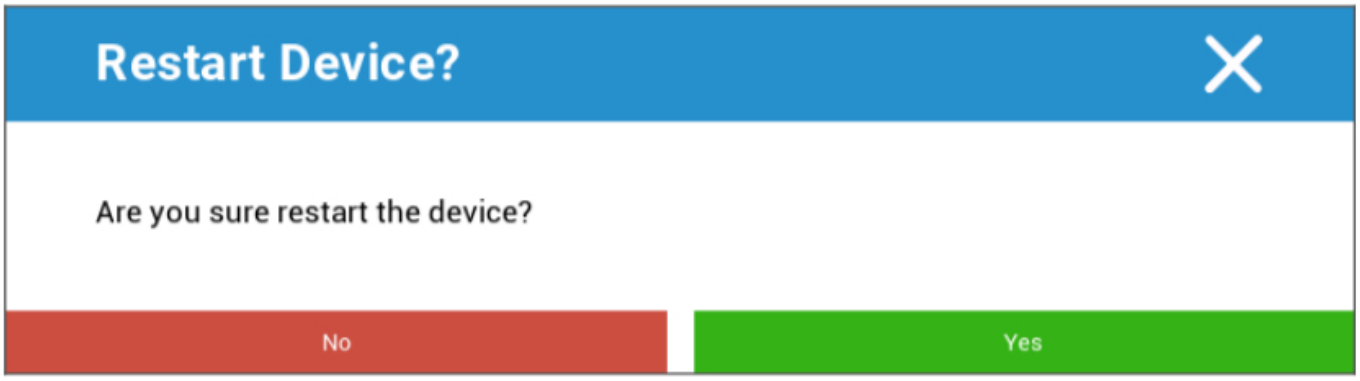
Here a lock command is sent to the end user device (lock screen).

Shutdown Device



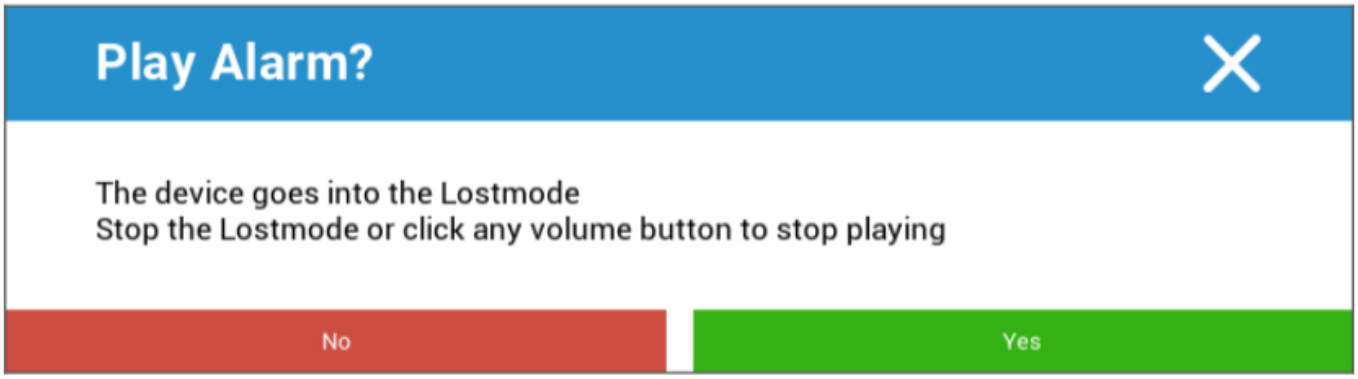
Here a shutdown command is sent to the end user device.

Restart Device

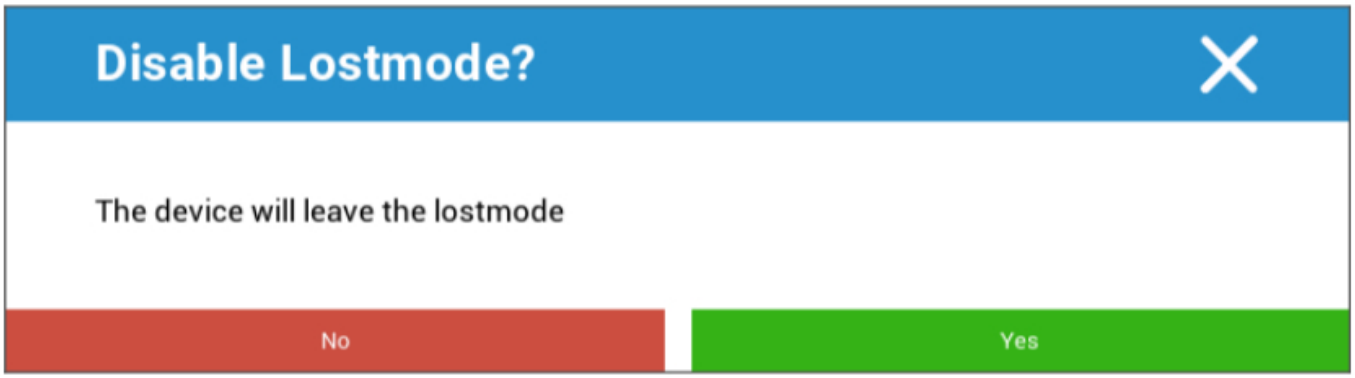


Here a restart command is sent to the end user device.

Alarm & Lostmode | Disable Lostmode



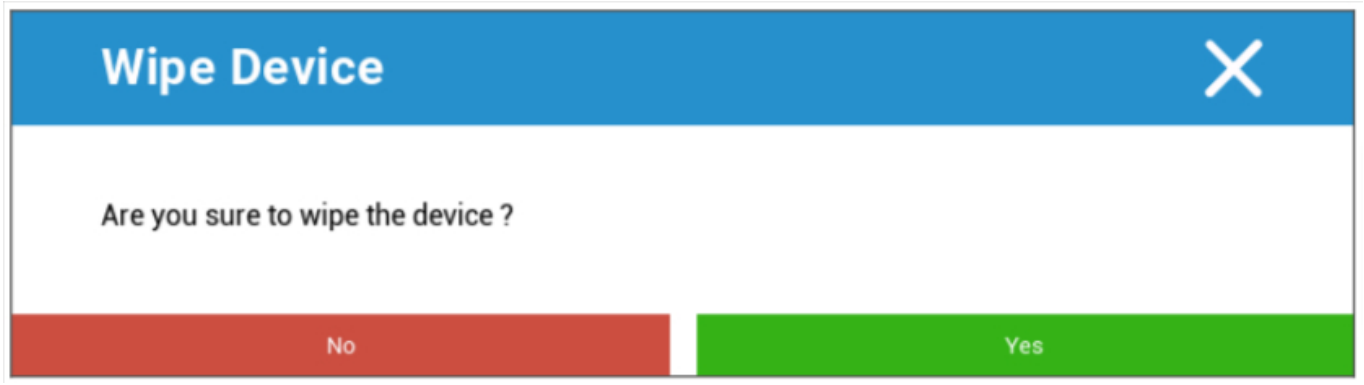
Here the device can be set into the Lostmode, which sets the device to be constantly playing an Alarm sound. The Lostmode can be stopped by pressing any volume button of the device or remotely by clicking on “Disable Lostmode“:



Delete Device

Here the delete command can be performed. You can once again decide, if the device should only be removed from AppTec360 (“Delete from System“) or, if the device should be removed from AppTec360 and also be restored to its factory setting (“Wipe & Delete).

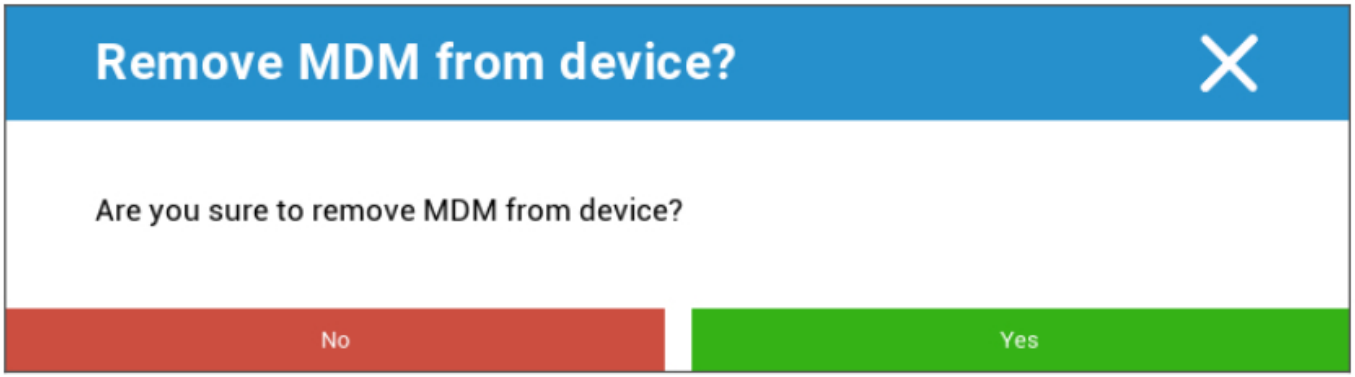
Wipe Device



Under “Wipe Device“ you can perform a complete wipe of the device. The device will be restored to its factory settings.

Enterprise Wipe | Remove MDM

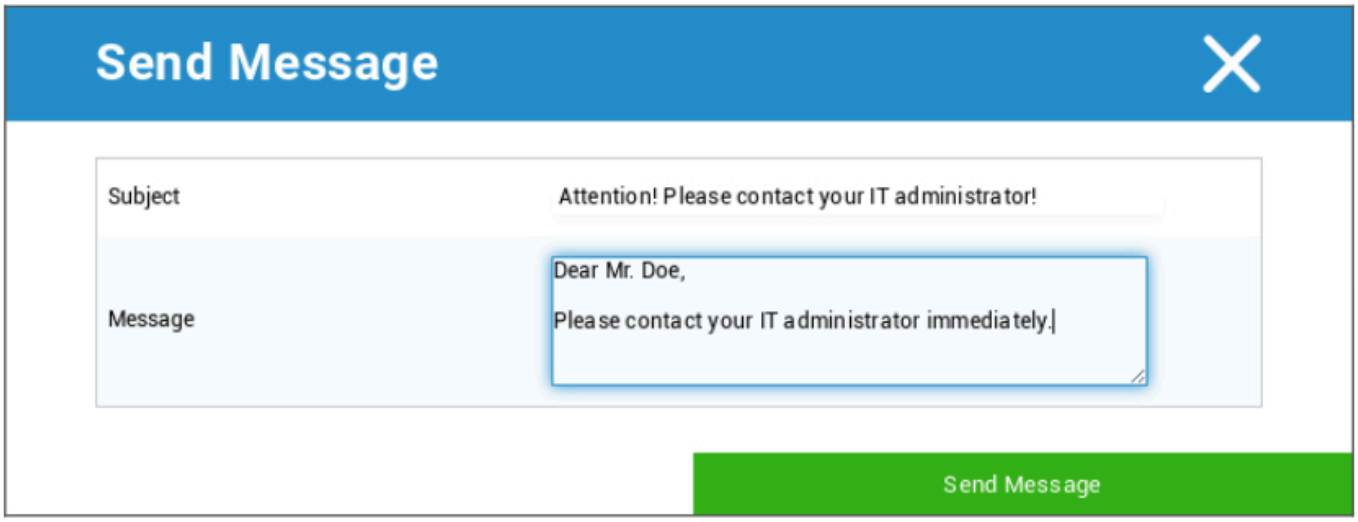
Only the information, apps and profiles provided by AppTec360 are deleted. This way, the corporate data will no longer be available on the end user device. The private area is not affected and continues to remain on the end user device.



With “Remove MDM“ you can remove the MDM profile on the end user device and all other items provided by AppTec.

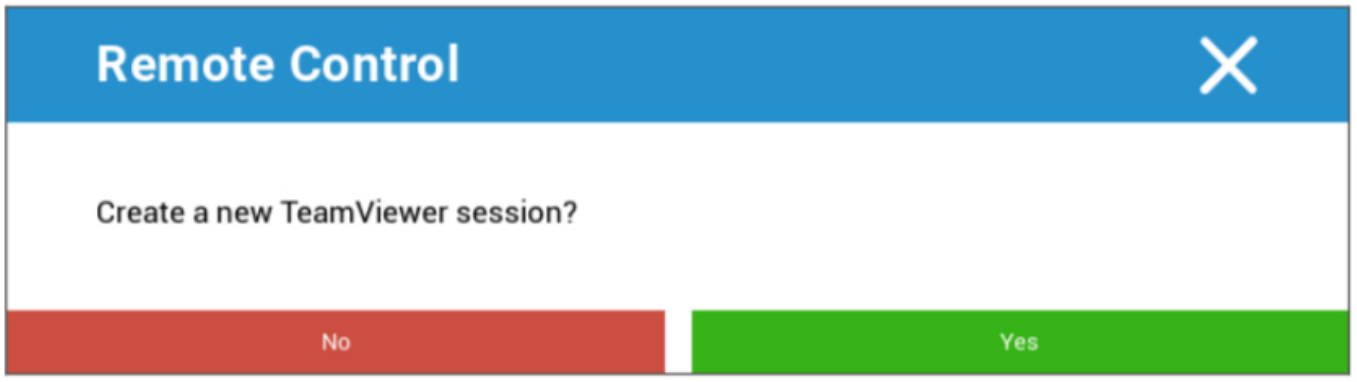
This command performs the same action as “Enterprise Wipe“.

Send Message



Here you can send a Push Notification to the respective device.

TeamViewer Remote Control



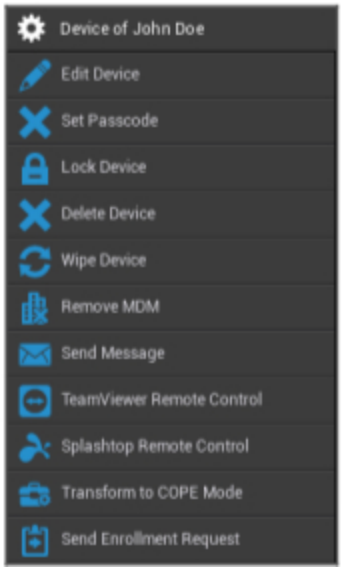
Here a Teamviewer Remote Control session can be started.

Send Enrollment Request

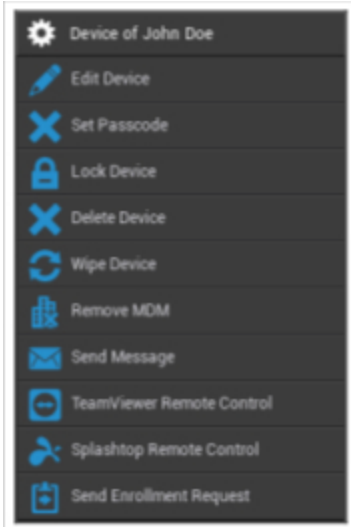
With “Send Enrollment Request“, you can send an Enrollment Request (again), to the respective user.

Android

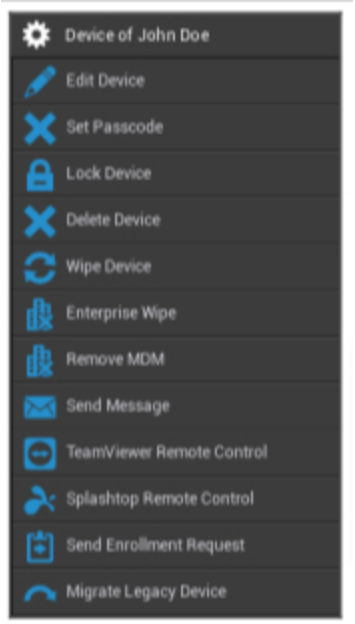
AE Fully Managed Device (Work Managed)



AE Work Profile (Container)



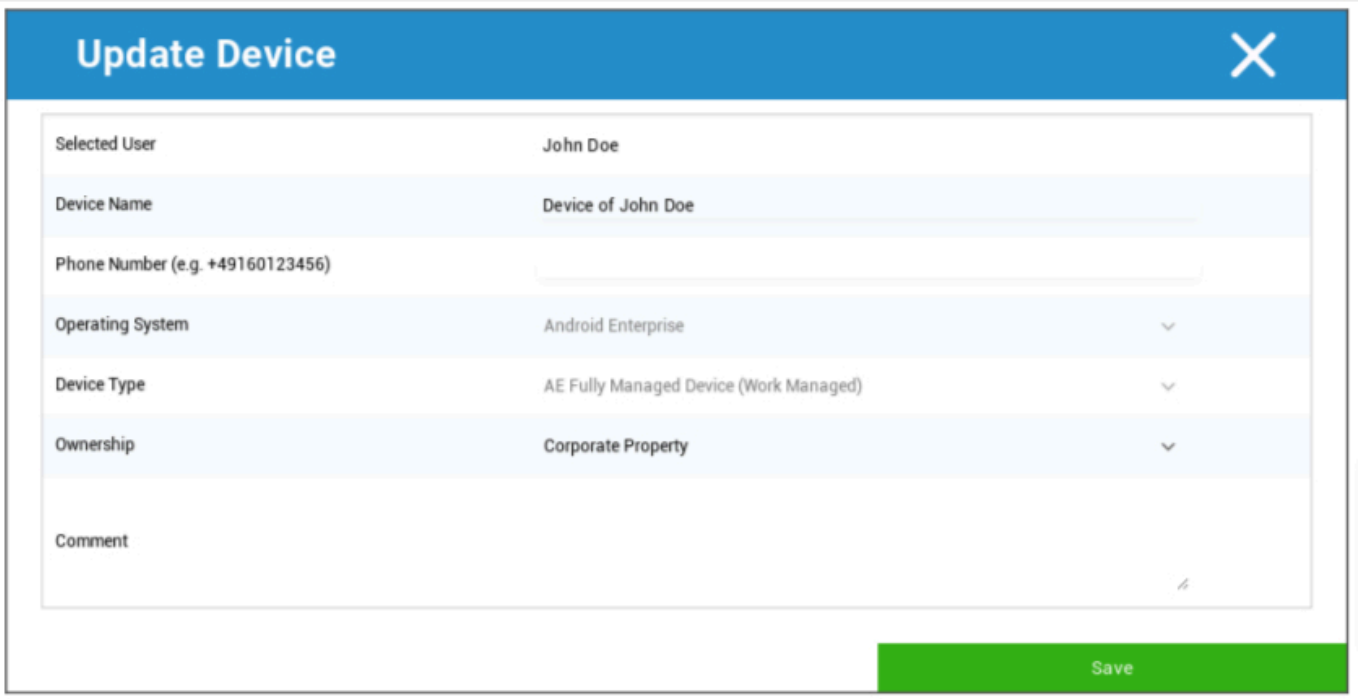
Android Phone | Tablet



Edit Device	Edit device information
Set Passcode	Set device's passcode
Lock Device	Lock device (lock screen)
Delete Device	Delete device from AppTec
Wipe Device	Restore device to factory settings
Enterprise Wipe	Information, Apps, Profiles that are provided by AppTec360 are deleted (device will be separated from MDM)
Remove MDM	
Send Message	Send Push notifications to the device Message will be displayed in the AppTec360 App (Message Tab)
TeamViewer Remote Control	Start a Remote Control session for this device using TeamViewer
Splashtop Remote Control	Start a Remote Control session for this device using Splashtop
Transform to COPE Mode (only on AE Fully Managed Device (Work Managed))	Create a Work Profile on this AE Fully Managed (Work Managed) Device
Send Enrollment Request	Send (repeated) enrollment request
Migrate Legacy Device (only on Android Phone / Tablet when enrolled using Device Owner Mode Provisioning)	Migrate Android Phone / Tablet Profile to AE Fully Managed Device (Work Managed) Profile

Edit Device

Here you can update a variety of device information.



Selected User	Device user
Device Name	Device name
Phone Number	Device telephone number
Operating System	Android Enterprise Android
Device Type	Android Enterprise: • AE Fully Managed Device (Work Managed) • AE Work Profile Mode (Container only) • AE Fully Managed Device with Work Profile (COPE) Android: • Phone • Tablet
Ownership	Corporate = corporate property

	Employee = employee property
Comment	Additional descriptions for the device

Clear Passcode

Here you can remove the device passcode on the selected device. By default on Android, the passcode will be set to “123456“– this can and should be changed by the user afterwards.

Lock Device

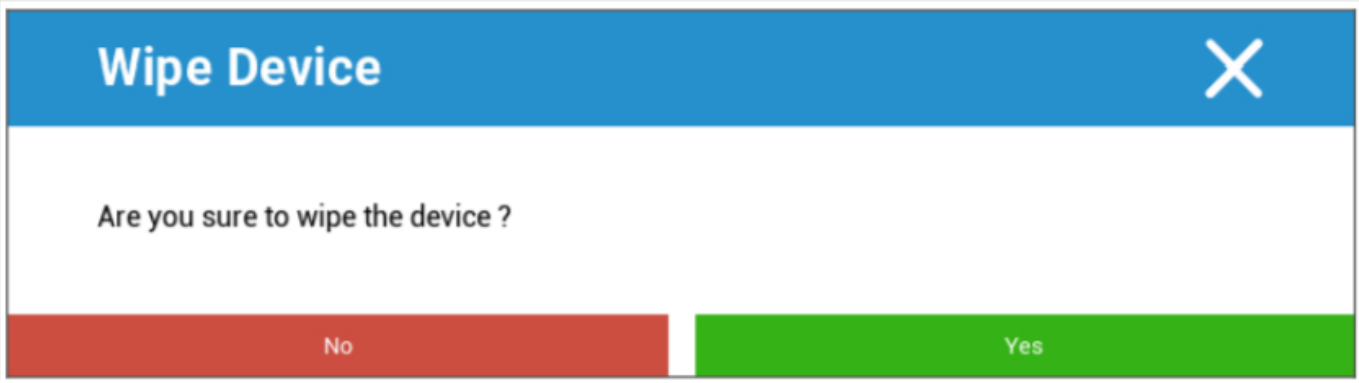
Here a lock device command will be sent to the device (lock screen).

Delete Device

Here a delete command can be performed. You can once again decide, if the device should only be removed from AppTec360 (“Delete from System“) or if the device should be removed from AppTec360 and additionally be restored to its factory settings (“Wipe & Delete).

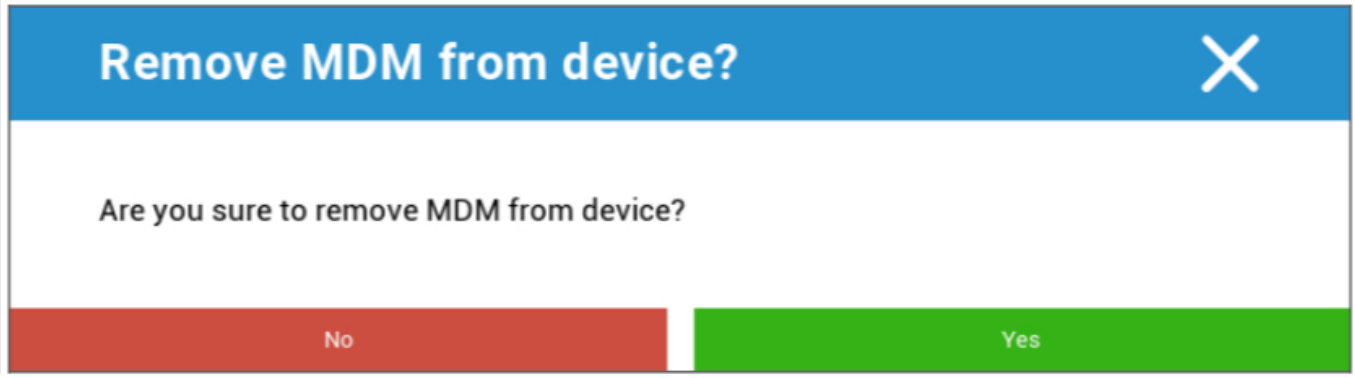
Wipe Device

Under “Wipe Device“ you can perform a complete wipe of the device. The device will then be restored back to its factory settings.



Additionally, if the device contains an SD card, you can erase the SD card. You can accomplish this, by setting „Wipe SD Card too? “ to “On“.

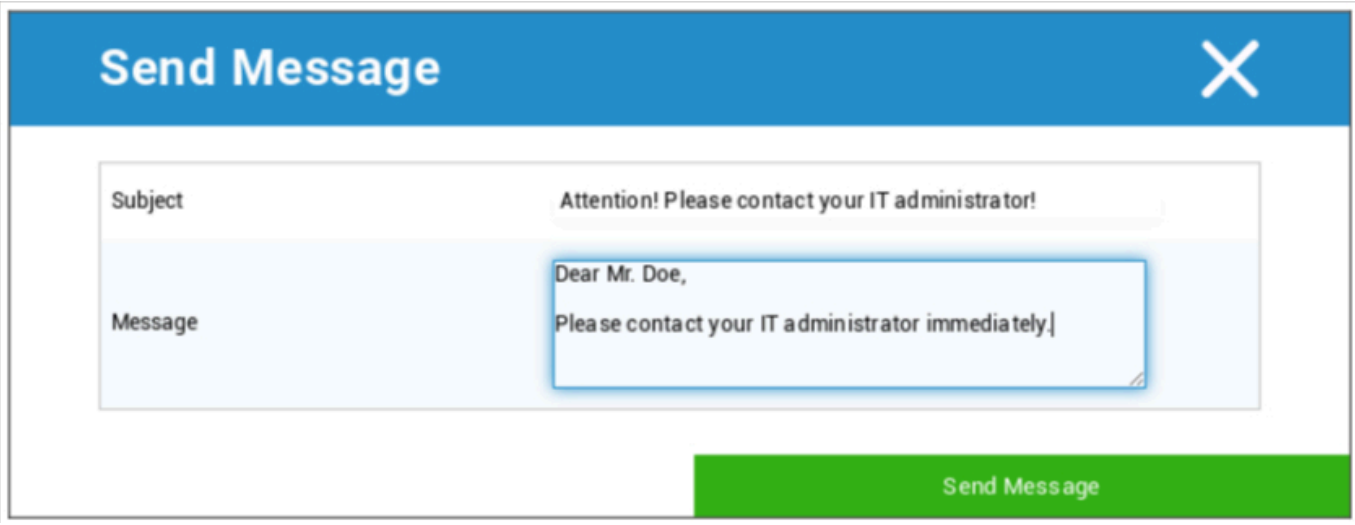
Remove MDM



This is the recommended method, for creating a separation from MDM.

Only the information, apps and profiles provided by AppTec360 are deleted, which means that all corporate data will no longer be available on the end user device. The private sphere, however, is not affected and continues to remain on the end user device.

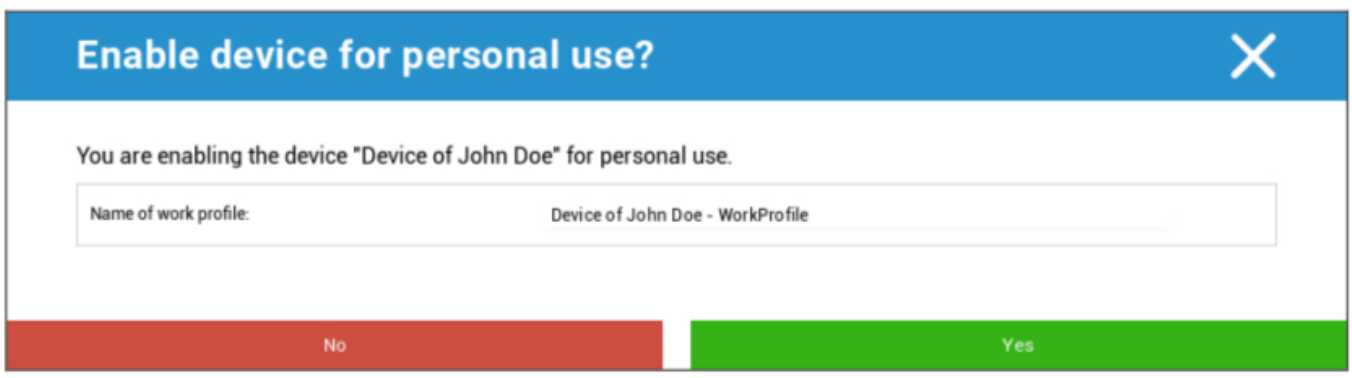
Send Message



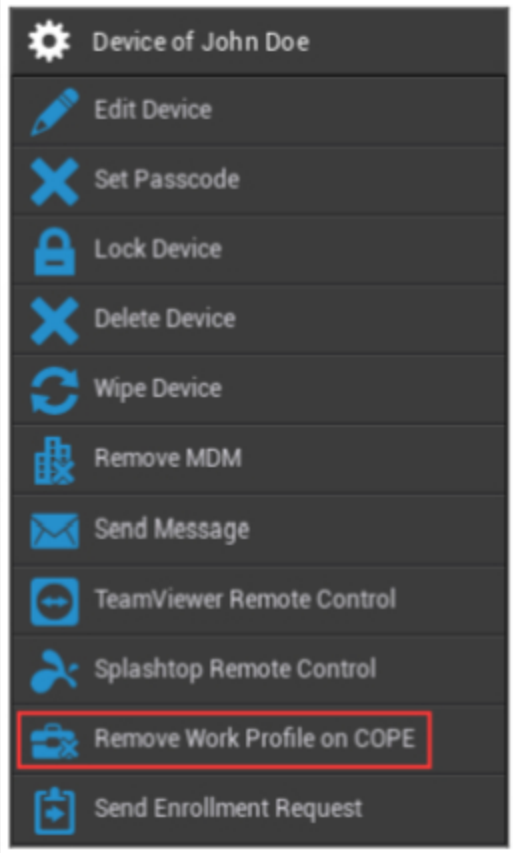
Here you can send a Push Notification to the respective end user device.

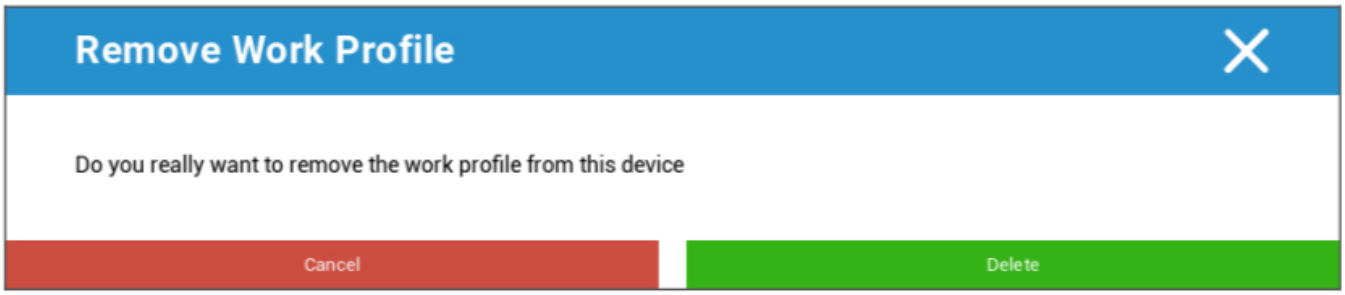
Transform to COPE Mode

Create a Work Profile on this AE Fully Managed (Work Managed) Device



After transforming the device to COPE Mode, you are able to remove the Work Profile by clicking on the gear option **Remove Work Profile on COPE:**




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

Send Enrollment Request

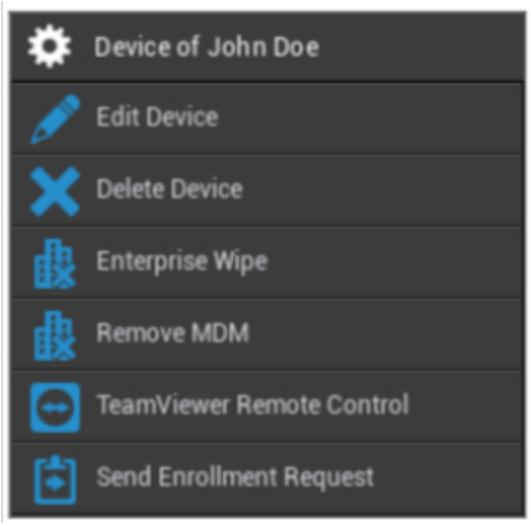
With “Send Enrollment Request“ you can send an Enrollment Request (again), to the respective user.

Please note, that only the newest Enrollment – Request is valid.

Migrate Legacy Device

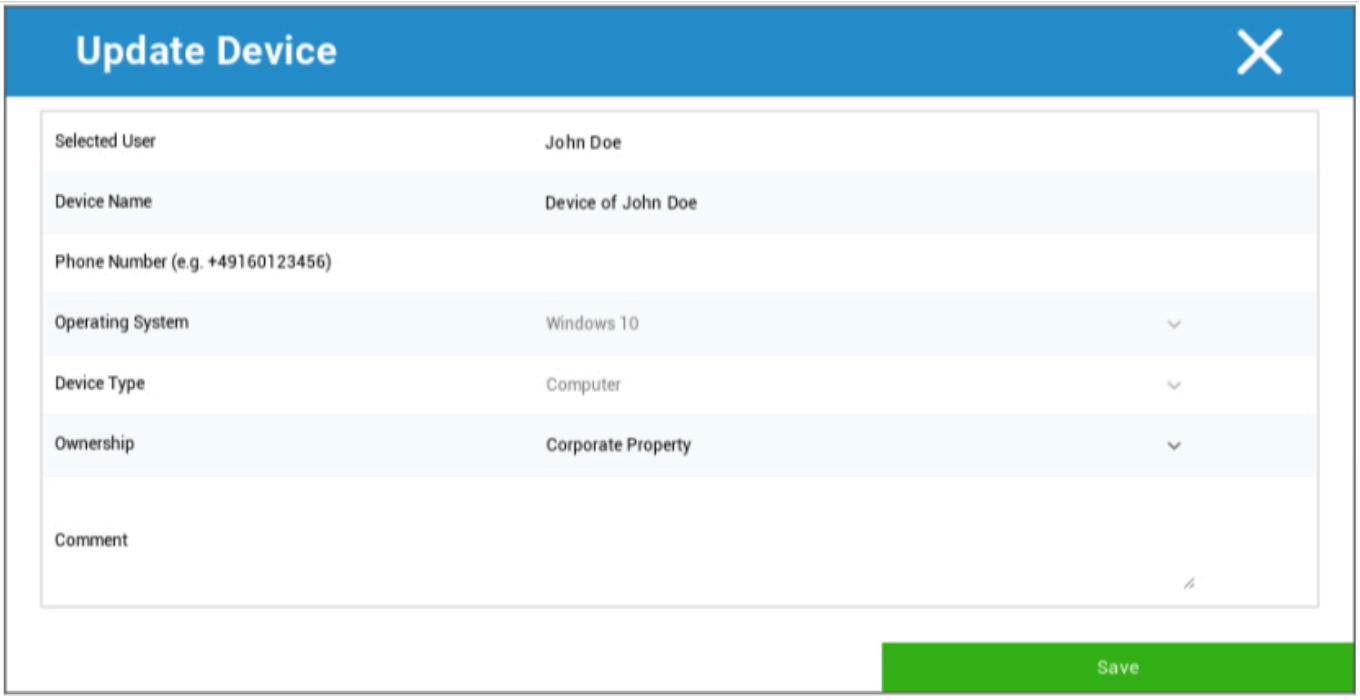
Migrate Android Phone / Tablet Profile to AE Fully Managed Device (Work Managed) Profile

Windows



Device Name	Name of the selected device
Edit Device	Edit device
Delete Device	Remove device from AppTec
Enterprise Wipe	Information, apps and profile provided by AppTec360 are deleted
Remove MDM	
TeamViewer Remote Control	Remote control the device with TeamViewer
Send Enrollment Request	Send enrollment request (again)

Edit Device

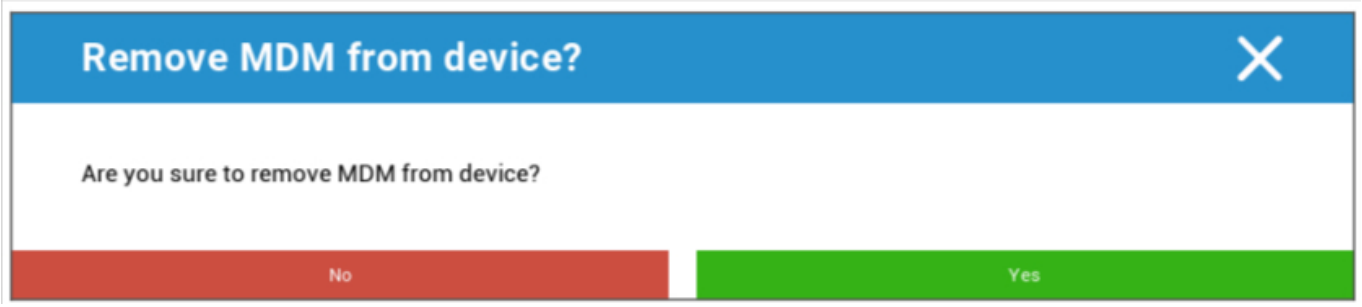


Here you can update a variety of information on the device.

Delete Device

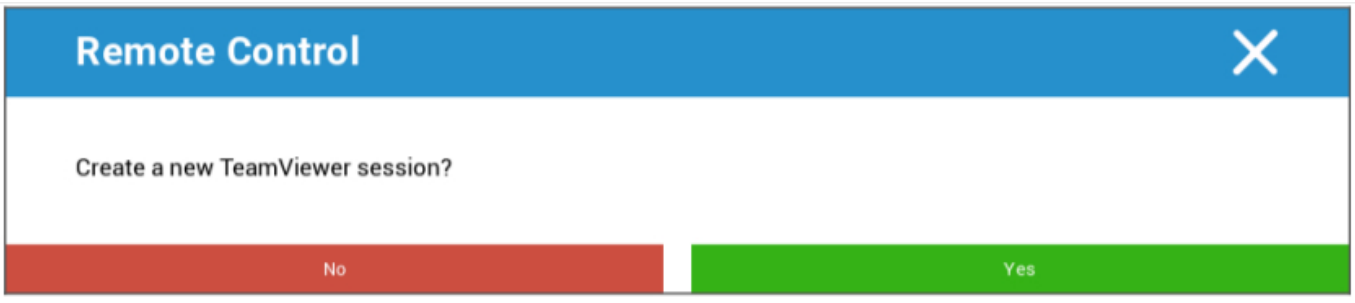
Here the delete command which only removes the device from AppTec360 can be performed.

Enterprise Wipe | Remove MDM



Only the information, apps and profiles provided by AppTec360 are deleted. This way, the corporate data will no longer be available on the end user device. The private area is not affected and continues to remain on the end user device.

TeamViewer Remote Control



Here you can start a TeamViewer Remote Control session for this device.

Send Enrollment Request

With “Send Enrollment Request“, you can send an Enrollment Request (again), to the respective user.

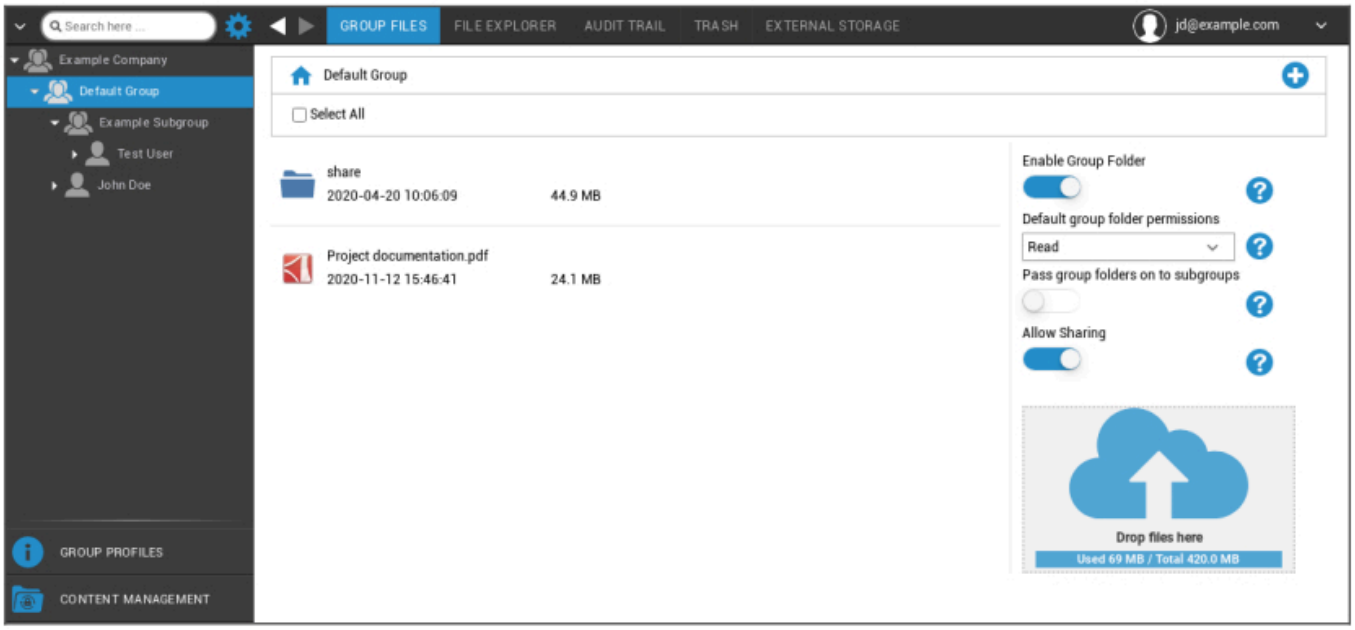
Content Management

When you are in a group, you can manage AppTec's ContentBox with “Content Management“.

With the Content Box you can safely distribute documents and other corporate data to the end user devices.

Group Files

“Group Files“ represents a fundamental part ContentBox. Here you establish settings, upload documents, create new folders, etc.



With the symbol in the upper right hand corner you can create new folders that are designated to the respective group with “Add Folder“.

With the symbol in the upper right hand corner, you can create a new folder via “Add Folder“, that should be assigned to the respective group.

You can name the folder anything you want.

Via “Upload Files“, you can upload data. Here your Standard-Explorer will be opened. You can, of course, perform these two actions in every (sub) folder.

With the symbol in the upper left hand corner, you can return to the main menu.

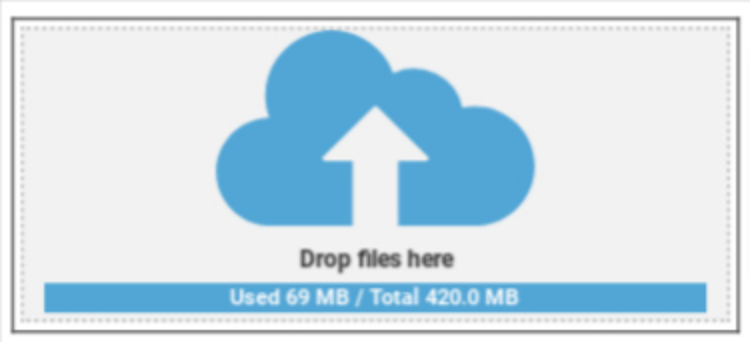
You can select several folders and files and download them with “Download“ or you can erase them by clicking “Delete“.

You can also select all files and folders with and perform the “Download“ and “Delete“ commands.

When you move your mouse over a folder or file, then you will see the following overview:

- With “Rename“, you can rename the folder/file
- With “Download“, you can download the folder/file
- With “Delete“, you can delete the folder/file

Enable Group Folder	If activated, all members of the group have access to the respective folder
Default group folder permissions	Permissions of the users in the selected group: Read = read only permission Update = update permission Create = create permission Delete = delete permission
Pass group folders on to subgroups	If activated, the respective subgroups can have access to the parent data files
Permissions for subgroups	Permissions of the users in the selected subgroup: Read = read only permission Update = update permission Create = create permission Delete = delete permission
Allow Sharing	If activated, the user can share files via a link



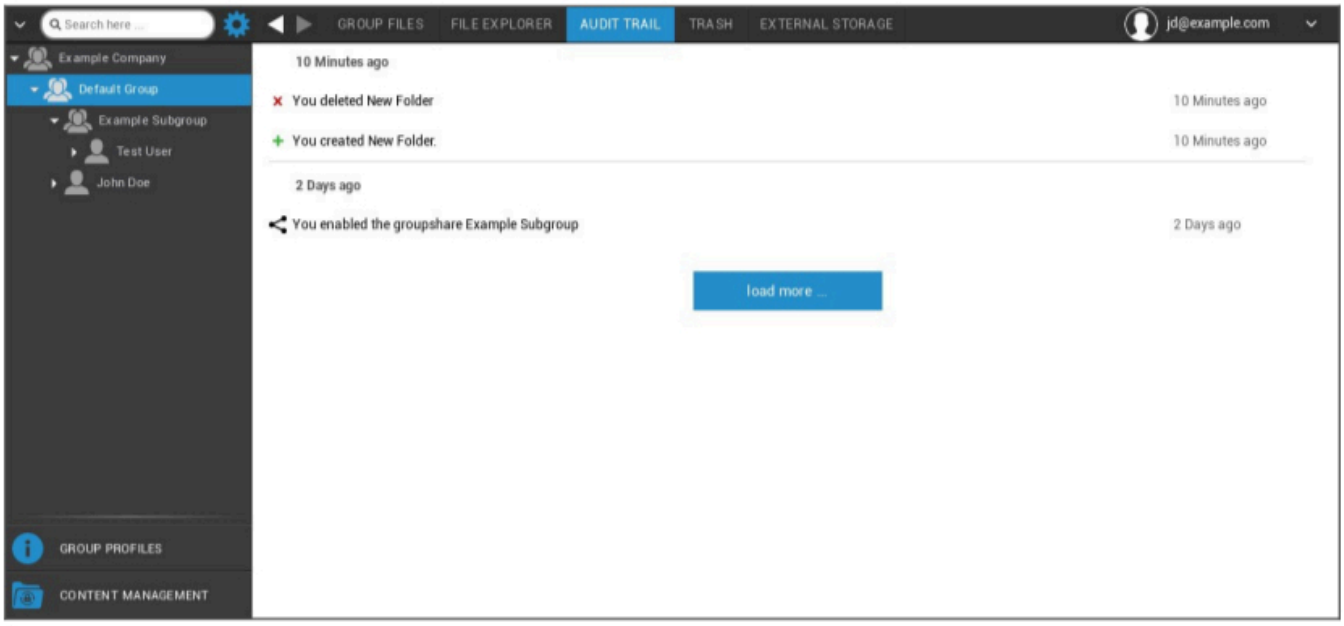
In order to upload files, you can use this field, by pulling a file via Drag & Drop to this window. You can also click on this field, in order to select and upload a file with the help of Internet Explorer.

File Explorer

With the “File Explorer“, you can manage all folders and files – regardless of the group where they are filed.

You will also find the settings and buttons that you learned about in “Group Files“.

Audit Trail



In “Audit Trail“, you can see from the history, which user created, deleted or shared what. This way, you can establish at any time, what was done with the corporate data.

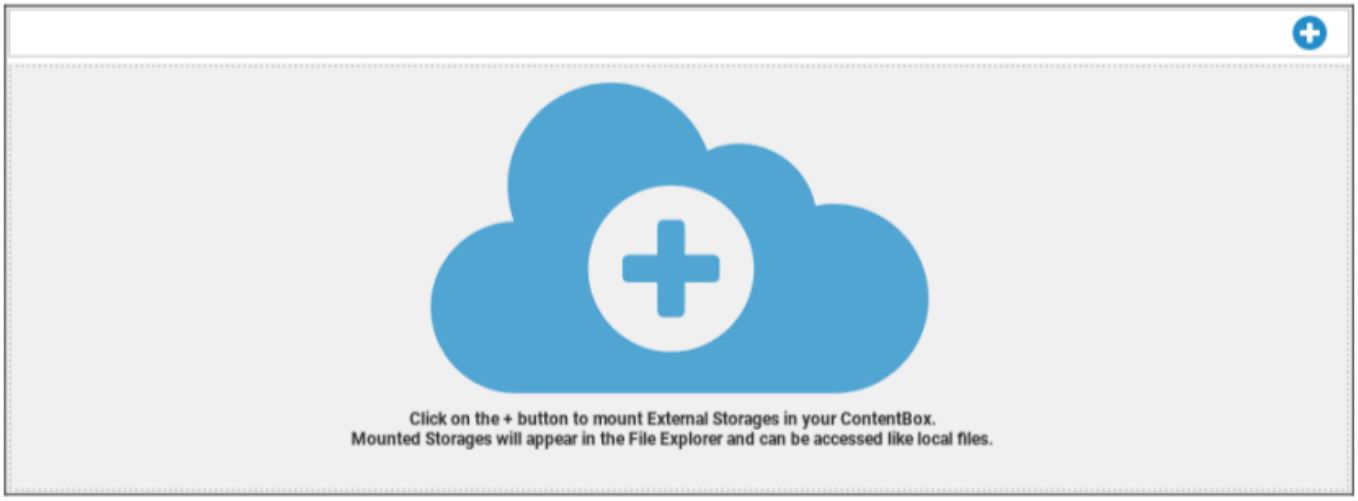
Trash

Should you have deleted something (by accident), you can see the folders and files under “Trash“ and recover them, according to your wishes.

- With “Undelete“, you can recover the data/folder.
- With “Delete“, you can permanently delete the data/folder – you must confirm the dele command once more.

Please note, that the storage capacity that is being utilized in the trash, reduces the “Total Space“ available – this is an ownCloud requirement.

External Storage



Under the heading “External Storage“, you can connect external storage.

With the symbol, (additional) storage can be added.

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

Amazon S3	
Display Name	Display name
Access Key	Access key
Secret Key	Security key
Bucket	Definite identity of the subfolder that has been assigned to you
Hostname (optional)	Hostname (optional)
Port (optional)	Port (optional)
Region	Region (optional)
Enable SSL	Enable SSL
Enable Path Style	Clear Path Address that has been assigned to you

FTP	
Display Name	Display name
Host	Host-Address
Username	Username
Password	Password
Root	Main menu
Secure ftps://	

SFTP	
Display Name	Display name
Host	Host-Address
Username	User name
Password	Password
Root	Main menu

ownCloud	
Display Name	Display name
URL	ownCloud URL
Username	Username
Password	Password
Remote Subfolder	Standard folder
Secure https://	

WebDAV	
Display Name	Display name
URL	WebDAV URL
Username	User name
Password	Password
Root	Main menu
Secure https://	
Windows Share	Support for Windows Share will be available soon
SharePoint	Support for Microsoft SharePoint will be available soon

Audit Log

Here you can find a log that records information about actions that are performed in the MDM console.

With the filter icon you can apply filters to the displayed list.

With the dropdown menu **Items per page**: you can select the amount of items to be displayed in one page of the list.

Action taken / Setting changed	The action that was taken / The setting that was changed
Value	The value of the taken action / changed setting
User	The name of the user that has taken the action / has changed the setting
Date	The timestamp of when this action was taken / this setting was changed
Path / Type	The path to where this action was taken / this setting was changed

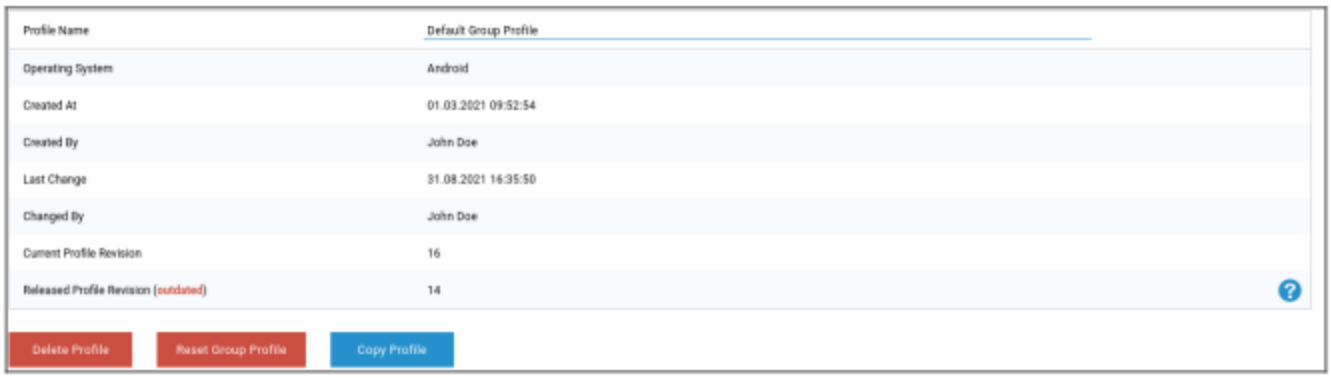
iOS Configuration

General

Depending on whether you have currently selected a group or a device, the display and its sub points are different – please pay careful attention to this!

Group profile overview (only on group level)

When opening a group profile, you will get a quick overview of the profile



Profile Name	Name of the profile (can be changed here)
Operating System	Operating System the profile is for
Created At	Time of creation
Created By	The profile's creator
Last Change	Time of last change to the profile
Changed By	Account that made the last changes
Current Profile Revision	Revision of saved profile state
Released Profile Revision	Assigned profile revision (“Assign now”). If the label shows “(outdated)” behind the text, it means you’ve saved the profile but did not assign it yet, so the devices will still get and older version.

General Information

Should you be directly on the device, you will receive a brief overview of your selected device.

Device Name	Device name
Phone Number	Device telephone number
Model	Model number
Operating System	OS
Serial Number	Device serial number
Device Ownership	Corporate- or private device Corporate = corporate device Employee = private device
Device Type	Device type (Tablet or Phone)
Jailbroken	If there is a Jailbreak on the device
Supervised	Indicates if this is a supervised device
Compliant	If any guidelines were violated
Last Seen	Status of when the device last communicated with the AppTec360 Server

Settings

These settings contain the device name and a predefined background.

Name device to system name	The name that will be issued in the AppTec360 Console (in left hierarchy structure), will be same as on the respective end user device (can be viewed in the device settings)
Use custom wallpaper (supervised devices only)	Here you can pre-define the background, that should be displayed on the end user device (ex. for a type of corporate branding for the device) Is only available in Supervised Mode!
Automatic OS updates	Forces OS updates if available. Only for DEP devices in supervised mode.
Custom Fonts	Here you can add custom fonts.
Name	Optional. The user-visible name for the font. This field is replaced by the actual name of the font after installation.
Font	Upload the font file (.otf or .ttf).

Config Revision

Here you will receive an overview of which group profile is designated to the device.

If you click on the group profile, you will access the profile directly and you can perform settings.

With the symbol, you can revert the assigned apps to the group profile's settings.

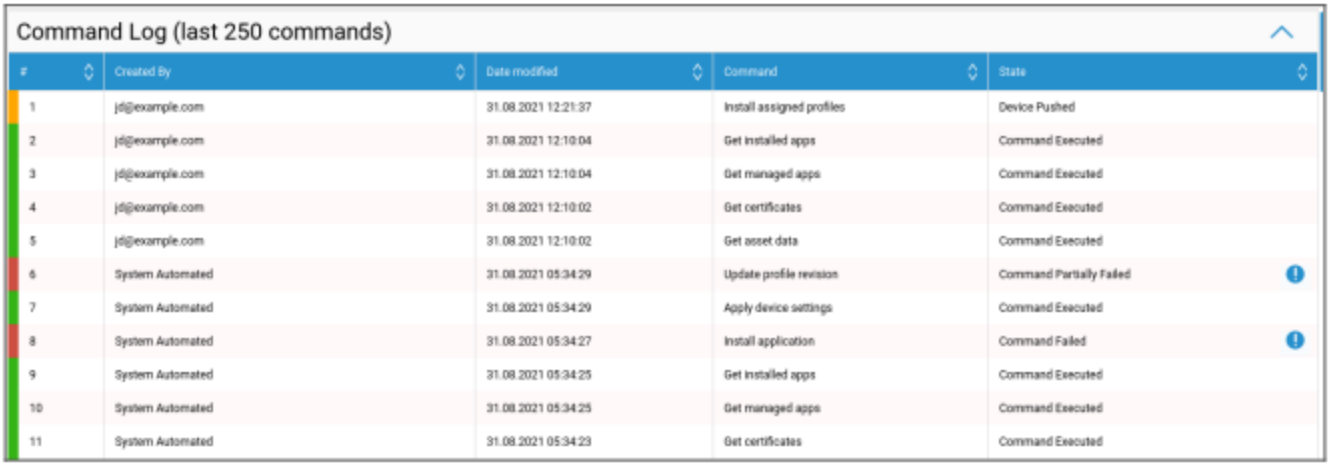
With the symbol, you can reset the device profile to have no settings at all.

“Newer Revision available“ indicates that the group profile has been changed and saved but not assigned. The group profile has to be assigned with “Assign now” on group level to apply the changes to the devices.

Device Log (only on device level)

Command Log

Here you can see which commands where issued for the device and what their status is.



Commands created by “System Automated” are automatically created by the system.

Possible command statuses

Device Pushed	A push request has been sent to the push service (e.g APNS) to tell the device to connect back to the EMM server.
Command Created	The command was created in the system.
Command Sent	The command got sent to the device after it connected to the server.
Command Executed	The command was successfully executed.
Command Failed	The command failed. *
Command Partially Failed	Depending on the device OS some commands may get grouped together. In this some parts of this command group failed. *
Command Executed, eventually Failed	The command was executed but maybe it wasn't.
Command Repushed	The command was repushed by a user.
Discarded	The command was discarded. For example because it was superseded by another command or the device got re-enrolled and old commands got removed

If there is an exclamation mark behind the message, you can get more information by hovering over the icon with your cursor.

Asset Management (only on device level)

Asset Management (only on device level)

Device Info

Model	Model number of the device
Operating System	OS
OS Version	OS version
Serial Number	Serial number
UDID	Device UDID
Device Name	Device name
Supervised	Displays if the device is supervised
Battery Status	Battery status

Wi-Fi

IP Address	Device IP Address
WiFi MAC	WiFi MAC Address

Cellular

Status	Status (SIM card present)
Phone Number	Telephone number
Roaming Status	Current roaming status
Roaming (Voice/Data)	Roaming status for voice/data
IP Address	IP Address
IMEI	IMEI-Number
Operator/Carrier	Cellular service provider
SIM Carrier Network	SIM carrier network
Carrier Version	Carrier version
Modem Firmware	Modem firmware
Current MCC/MNC	See “SIM MCC/MNC“
SIM MCC/MNC	The Mobile Country Code is an established country identification by ITU as per the E.212 Standard, which, in conjunction with the Mobile Network Code (MNC), is used to identify a cellular network (=country code) When you go into another cellular network, the “Current MCC/MNC“ and “SIM MCC/MNC“ are therefore different.

Bluetooth

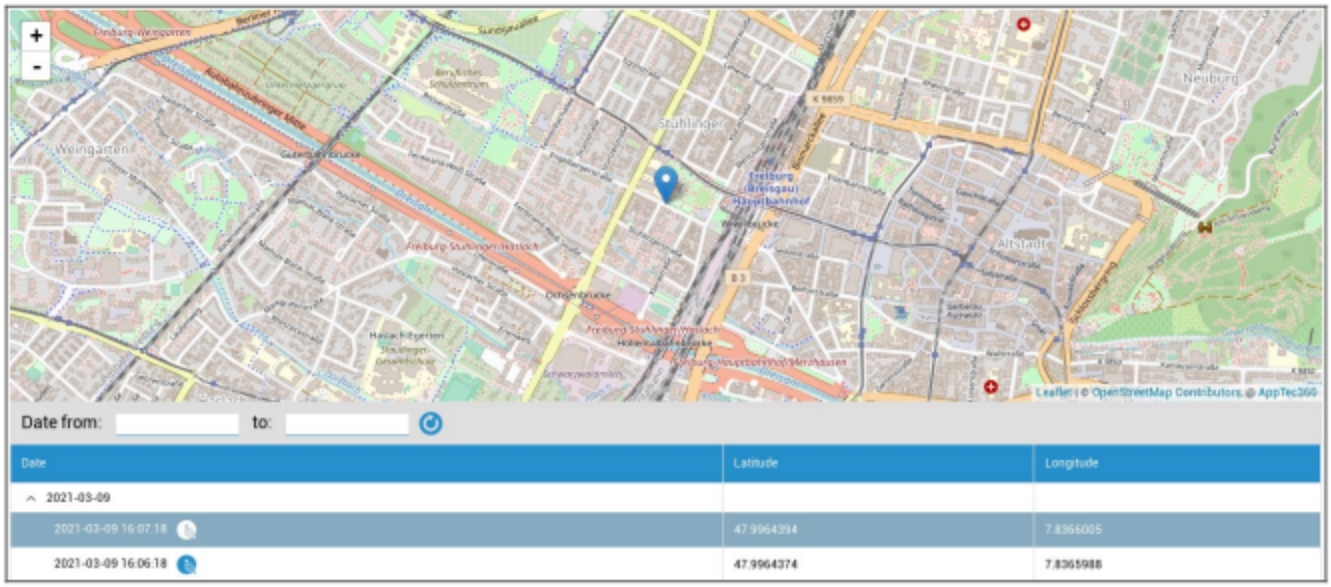
Bluetooth MAC	Bluetooth MAC Address

Security Management

Anti Theft (only on device level)

GPS Information (only on device level)

Here you can assess the current/last location of the device. The localizing can either be protected with one or even two passwords – See: General Settings – Privacy – GPS Access



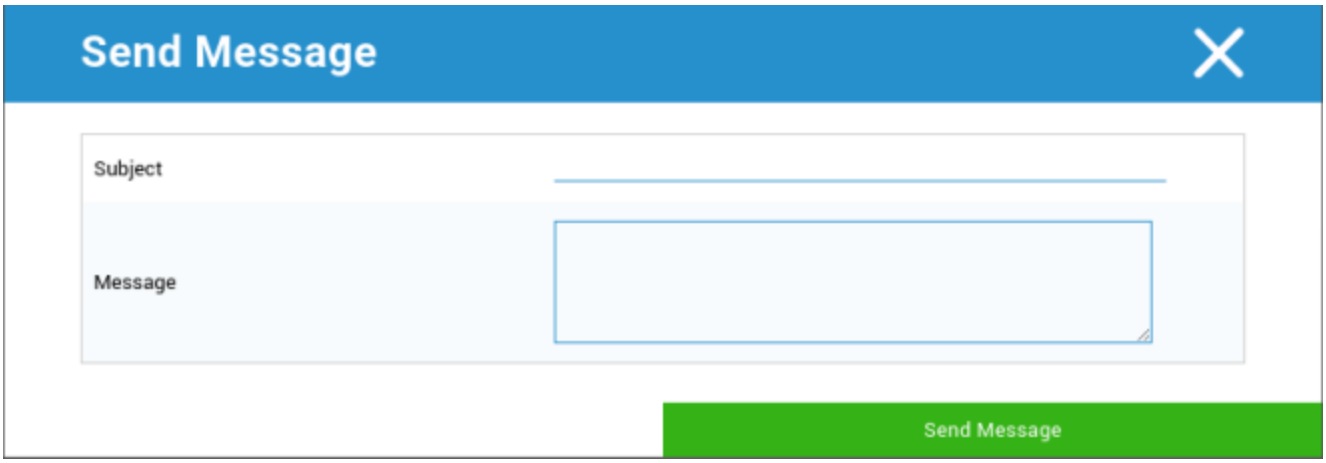
Wipe & Lock (only on device level)

Under “Wipe & Lock“, you can perform the following three actions:

Full Wipe	The device is restored back to its factory settings (corporate, as well as personal data is deleted)
Enterprise Wipe	Only corporate data is removed from the end user device (all apps, data, etc. that were provided by AppTec)
Lock Screen	Screen lock is activated, it is sufficient to unlock the device with the device-password/PIN
Forensic Lockdown (Supervised Devices only)	Should this function be activated with the  symbol, the device will be locked, by displaying a message, which cannot be closed. The employee can also not unlock the device. Only the administrator can unlock the device in the console with the unlock  symbol.
Allow Activationlock (Supervised Devices Only)	Should this function be activated , the device will be locked, as soon as “Find my iPhone“ is activated in the iCloud settings

Message (only on device level)

With the following window, you can fill in the subject and a message and send it to an end user device:



Security Configuration

Passcode

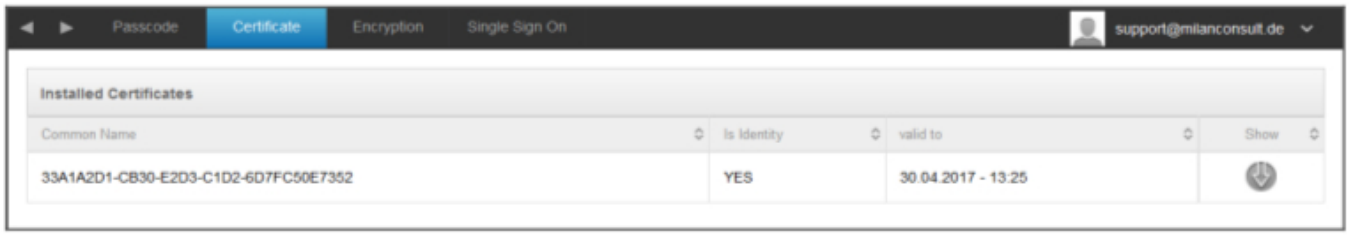
Here you establish the settings for the device password

Code deactivation allowed	When this setting is activated, there is no prompt for entering a password As soon as a password is established, it cannot be deactivated
Allow simple value	Allow the user to use the same, escalating and reducing number strings (ex. 1234, 1111)
Require alphanumeric value	Passwords must contain at least one letter
Minimum passcode length	Minimal password length
Minimum number of complex characters	Minimal number of alphanumeric symbols in the password
Maximum passcode age	Number of days, after which the password must be changed
Maximum Auto-Lock	Maximum time, after which the device is locked
Maximum grace period for device lock	Time, after which the device enters the locked Stand-By
Maximum number of failed attempts	Establishes, how often a password can be entered incorrectly, before a complete device wipe will be performed
Maximum passcode age (1-730 days)	Maximum password age
Passcode history (1-50 passcodes)	The use of an old password is allowed after this number

A click on the trash, opens the Password-Reset Dialog, with which a forgotten device password can be erased.

Certificate (only on device level)

Displays the certificates that are available on the device


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

Encryption

Require storage encryption	Activate the installed device encryption function

Single Sign-On

Under the point “Single Sign-On”, you can configure the Kerberos authentication.

Here, you establish the access credentials and the respective URLs / Apps that are allowed to use the Kerberos Tokens.

Available in Supervised-Mode	
Account Name	Account Name
Principal Name	Unique identity to which Kerberos Tickets can be distributed
Realm	Your Kerberos Realm, that is to be used (ex. your Domain)

With the Symbol, you can establish additional URLs.

URL pattern used to limit this account	To be determined URLs, to which Kerberos Tickets can be distributed

With the Symbol, you can establish additional Apps.

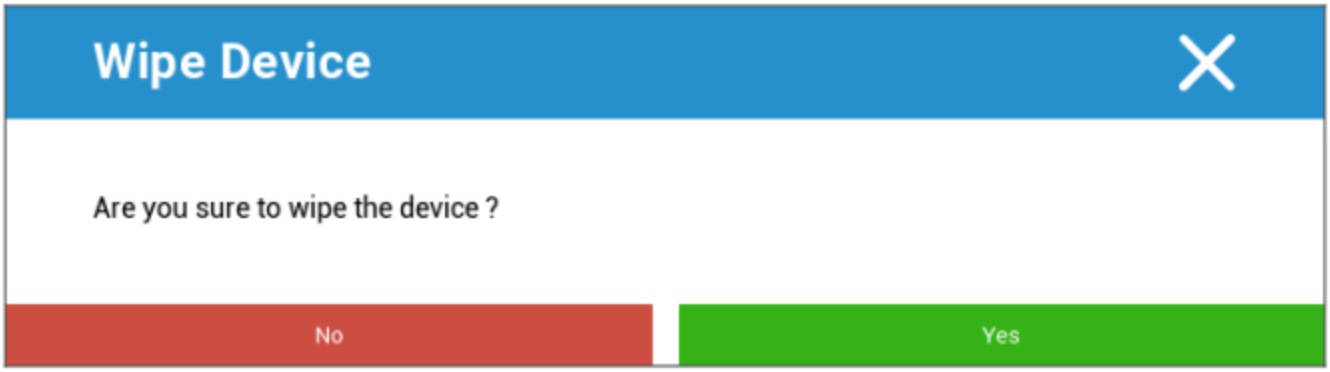
Apps to limit this account	To be determined Apps, to which Kerberos Tickets can be distributed

End of Life (only on device level)

Wipe (only on device level)

Under “Wipe“, you can restore the device to its factory settings. Here the corporate, as well as the private data will be deleted on the end user device.

With a click on the “Minus symbol“ you should receive the following message



With “Yes“ you can perform the wipe.

Under “Wipe Report“ the following items can be displayed

Wiped by	History of who performed the wipe
Date	Date
Status	Status (ex. if the Wipe was performed successfully)

Restriction Settings

Device Functionality

Here you can block individual end user device functionalities

Allow installing apps	Allow installing of apps
Allow camera	Allow the use of the camera
Allow FaceTime	Allow FaceTime
Allow screen capture	Allow screen capture
Allow auto sync while roaming	Allow auto sync while roaming
Allow Siri	Allow Siri
Allow voice dialing	Allow voice dialing
Allow in-app purchase	Allow in-app purchase
Require iTunes Store password for all purchases	Require iTunes Store password for all purchases
Allow multiplayer gaming	Allow multiplayer gaming
Allow adding Game Center friends	Allow adding Game Center friends
Allow open from managed to unmanaged	Allow opening of content in managed apps in unmanaged apps
Allow open from unmanaged to managed	Allow opening of content in unmanaged apps in managed apps
Allow today view in lock screen	When this setting is active, the “Today“ view will be displayed in the Notification Center on the lock screen
Allow control center in lock screen	Allow Control Center on the lock screen
Allow TouchID	Allow TouchID
Allow over-the-air PKI updates	Allow over-the-air PKI updates
Allow passbook while locked	Allow passbook while device is locked
Limit Ad Tracking	These function deactivates Ad Tracking (ex. advertisers cannot use Ad Tracking in order to distribute personalized ads)

Allow Handoff	Allow Handoff
Allow internet results in spotlight	Allow internet results in spotlight (ex. Bing or Wikipedia)
Require passcode on first AirPlay pairing	Require passcode on first AirPlay pairing
Force Watch Wrist Protection	If activated, the Apple Watch is forced to use “Wrist Protection“ (wrist recognition)
Allow iCloud Photo Library	Allows the iCloud Photo Library. If not permitted, then all pictures that were not completely downloaded from iCloud, will be erased on the local storage
Available in the Supervised-Mode	
Allow Account Modification	Allow „mail, contacts, calendar“ modification
Allow AirDrop	Allow AirDrop
Allow App Cellular Modification	This setting blocks the setting for which apps are allowed to use mobile data This setting can, for example, be set manually on the end user device and then this restriction can be activated
Allow Siri querying user-generated content from the web	Web search on certain websites is blocked, ex. Wikipedia, because everyone can make changes as they please
Enable Siri profanity filter	Profanity, that is directed at Siri, is censored
Allow iBook Store	Allow iBook Store
Allow iBook Store Erotica	Allow iBook Store Erotica
Allow modifying Find my Friends settings	Allow modifying Find my Friends settings
Allow Game Center	Allow Game Center
Allow Host Pairing	Control computer pairing
Allow installing configuration profiles	Allow installing of configuration profiles
Allow Remove App	Control apps removal
Allow iMessage	Allow iMessage
Allow erase all contents and settings	Allow erasing of all content and settings

Allow configuring restrictions	Allow configuring restrictions
Allow Podcast	Allow Podcast
Allow Definition Lookup	Allow definition lookup
Allow Predictive Keyboard	Allow predictive keyboard
Allow Auto Correction	Allow auto correction
Allow UI App Installation	If deactivated, no apps can be installed from the public AppStore (the icon will no longer be displayed). However, apps can still be installed via iTunes and the Configurator
Allow Keyboard Shortcuts	Allow keyboard shortcuts, if the device is attached to a physical keyboard
Allow Apple Watch pairing	Forbids a pairing between the device and the Apple Watch, existing connections will be terminated
Allow Passcode modification	If not allowed, no device password can be added, changed or removed
Allow devicename modification	Guideline determining if the device name can be changed
Allow wallpaper modification	Guideline determining if the wallpaper can be changed
Allow automatic app downloads	If deactivated, a purchased app will not be automatically installed on other devices. Does not apply to updates for existing apps
Allow News	Allow News on the iOS device
Allow Enterprise app trust	If set to false, prevents trusting enterprise apps

iCloud

Block certain functionalities during iCloud pairing

Allow backup	Allow backup
Allow document sync	Allow document sync
Allow Photo Stream	Allow Photo Stream
Allow Shared Photo Stream	Allow Shared Photo Stream
Allow Cloud Keychain Sync	Allow Cloud Keychain Sync
Allow managed apps to store data	Allow managed apps to store data
Allow notes and highlights sync for enterprise books	Allow notes & highlights sync for enterprise books
Allow backup of enterprise books	Allow backup of enterprise books

Security and Privacy

Block these functionalities associated with diagnostic data

Allow diagnostic data to be send to Apple	Allow diagnostic data to be sent to Apple
Allow user to accept untrusted TLS certificates	Allow user, to accept untrusted TLS certificates
Force encrypted backups	Force encrypted backups

BYOD

Built-In iOS Security (Container)

iOS always was able to make a difference between managed (business) and unmanaged (private). Everything that comes from the MDM System is treated as managed. For example if you install an App via MDM oder configure an Exchange Account, this will be treated as managed by the iOS.

Everything else that gets configured/installed manually on the device will be treated as unmanaged. For example if the User installs WhatsApp on it's own or if the is adding an Exchange Account. However this separation never affected the contacts. But since iOS 11.3 (and higher) this was also added for the contacts.

Since this is a basic functionality of the operating system you do not need to install something or setup a special container.

Activate the Built-In Function to seperate private and business apps/information/files. This setting will also disable some other functions, that could otherwise turn off parts of this seperation by mistake.

Activation

Activate the Container-Solutions that are supported by AppTec360

Enable Google Divide Container	Enable Google Divide Container
Enable SecurePIM Container	Enable SecurePIM Container

Should you have activated the SecurePIM Container, you will also find the following point under "Activation". Additionally, four more tabs will be opened right away, which are described below.

Support Email Address	Support email address where a user can turn with problems

SecurePIM Password

Under “SecurePIM Password“, you can establish the guidelines for the password security strength.

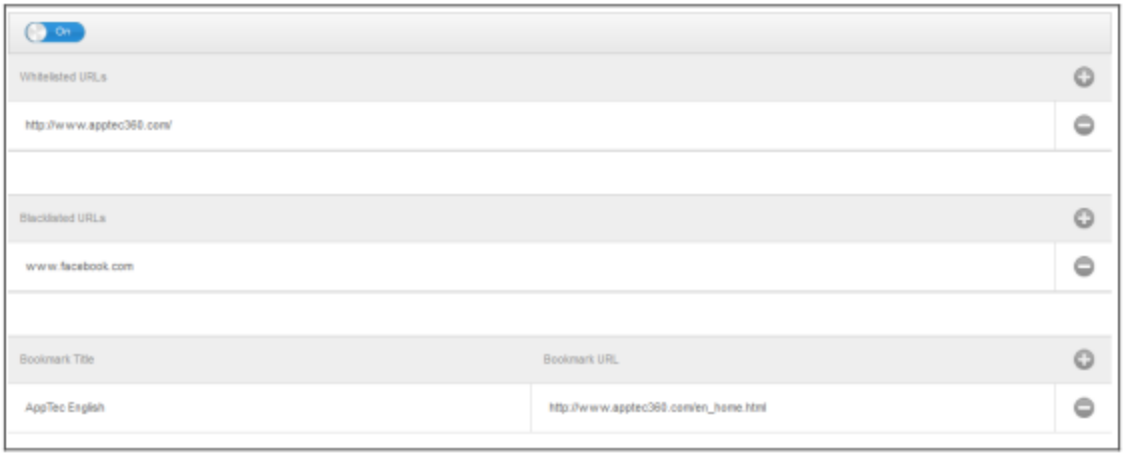
Session Timeout	Here you can establish after how many minutes a new password must be entered again, once SecurePIM runs in the background
Password Length	Password length for access to the SecurePIM Container
Upper Case Characters	Minimum upper case characters
Lower Case Characters	Minimum lower case characters
Special Characters	Minimum special characters
Digits	Minimum digits
Wipe Application	Number of times, a password can be entered incorrectly, before the SecurePIM content is deleted (The App, however, still remains on the end user device)

SecurePIM Security

Under “SecurePIM Security“, you can establish a variety of security settings.

Detect Jailbroken Devices	Should this setting be activated, the access to the SecurePIM Container will be blocked, as soon as the device is detected as jailbroken
Secure Text Fields	The content of the submission fields will be encrypted, no information reaches the OS (iOS) Note: As long as this setting is active, auto-correct is no longer available
Export Contact Data to Device	Should this setting be activated, then the user is allowed to export the Exchange Contacts onto their local device Note: Only the name and telephone number are exported
Show Event Location	Should this setting be activated, the location of the upcoming events will be displayed in the notification bar
Show Event Title	Should this setting be activated, the location of the upcoming event title will be displayed in the notification bar

SecurePIM Browser



Here you can configure the browser of SecurePIM.

With the symbol, you are able to define a new URL.

With the symbol, you are able to remove a defined URL again.

“Whitelisted URLs“ are URLs that can be loaded.

“Blacklisted URLs“ are URLs that cannot be loaded and are thereby blocked.

Please note, that the Whitelist entries carry a higher priority than the Blacklist entries. Under “Bookmark Title“ you can issue a title. With “Bookmark URL“, you can associate URL address with the bookmark title – this way you can distribute individualized bookmarks to the respective users.

Exchange

Under “Exchange“ you can configure an Exchange account.

ActiveSync Email Address	Exchange email address (take note of the “Placeholders“)
ActiveSync Exchange Login	Exchange user names (take note of the “Placeholders“)
ActiveSync Exchange Server	Exchange Server address (FQDN)
ActiveSync Exchange Domain	Exchange Domain address
User Certificate	User certificate
Certificate based authentication	User authenticates themselves with a certificate
Allow S/MIME Encryption	Allows the user to encrypt their mail
Allow S/MIME Signing	Allows the user to sign their mail
CRL Check	If active, the private certificate will be compared to the CRL (Certificate Revocation List)

Connection Management

Wi-Fi

Services Set Identifier (SSID)	SSID of the network that is to be connected
Auto Join	Activate auto join when joining a network
Hidden Network	Activate, in case the AP does not broadcast the SSID

Proxy Setup

Configuring of a Proxy for every Access Point

None		Establish no Proxy
Manual		Establish a manual Proxy
	Proxy Server URL	Address for accessing Proxy Settings
	Port	Establish the port for the Proxy
	Authentication	User name for the authentication on the Proxy
	Password	Password for the authentication on the Proxy
Automatic		Establish a Proxy automatically
Proxy Server URL		URL for access to the Proxy settings

Security Type

Establish Security Type for the AP

WEP	
Password	Password for the AP

WPA/WPA2	
Password	Password for the AP

WEP Enterprise – WPA / WPA2 Enterprise – Any Enterprise			
	Protocols		
	TLS	Activate/Deactivate	
	TTLS	Activate/Deactivate	
	LEAP	Activate/Deactivate	
	PEAP	Activate/Deactivate	
	EAP-FAST	Activate/Deactivate	
	EAP-SIM	Activate/Deactivate	
	Use PAC		Use of PAC (Protected Access Controll)
	Provision PAC	Configuration of Provision PAC	
	Provision PAC Anonymously	Anonymous Provision of PAC	
	Inner Authentications	Authenticationprotocol that should be used: PAP, CHAP, MSCHAP, MSCHAPv2	
	Username	Authentication username	
	Don't use Per-Connection Password	Don't use Per-Connection Password	
	Identity Certificate	Upload/select authentication certificate	
	Outer Identity	Identity that can be seen externally	
	Trust		
	Trusted Certificate 1	Upload first trusted certificate	
	Trusted Certificate 2	Upload second trusted certificate	
	Trusted Certificate 3	Upload third trusted certificate	
	Trusted Server Certificate Names	The names of the expected server certificates (in a comma separated list)	

None	Establish no security

VPN

Connection Name	Name of the VPN-Profile

VPN Type

VPN

All of the device network traffic will be routed via a VPN-connection.

Connection Type	Establish VPN-connection type
IPsec (cisco)	IPsec protocol by cisco
PPTP	PPTP protocol
L2TP	L2TP protocol
Cisco AnyConnect	AnyConnect protocol
Juniper SSL	Juniper SSL protocol
F5 SSL	F5 SSL protocol
SonicWall mConnect	SonicWall mobile Connect
Aruba VIA	Aruba VIA protocol
Custom SSL	Connection via Custom SSL
OpenVPN	OpenVPN protocol

Per-App VPN

When opening a certain app, a VPN-connection will be established

Automatically start Per-App VPN connection		Automatically start Per-App VPN connection
Connection Type		Establish VPN-connection type
	Cisco AnyConnect	AnyConnect protocol
	Juniper SSL	Juniper SSL protocol
	F5 SSL	F5 SSL protocol
	SonicWall mConnect	SonicWall mobile Connect
	Aruba VIA	Aruba VIA protocol
	Custom SSL	Connection via Custom SSL
	OpenVPN	OpenVPN protocol

Proxy Setup

Configuring of a Proxy for the VPN-connection

None	Establish no Proxy
Manual	Manually establish a Proxy
Proxy Server URL	Address for access to Proxy Settings
Port	Establish the port for the Proxy
Authentication	Username for the authentication at the Proxy
Password	Password for the authentication at the Proxy
Automatic	Establish a Proxy automatically
Proxy Server URL	URL for access to the Proxy settings

Show Placeholders	Displays all available user-variables , that AppTec360 can use

APN

Access Point Name	Access Point name
Access Point User Name	Access Point user name
Access Point Password	Access Point password
Proxy Server	Proxy Server address
Port	The respective Proxy port

Cellular

Enable Data Roaming	Enable Data Roaming
Enable Voice Roaming	Enable Voice Roaming
Enable Hotspot	Enable Hotspot

HTTP Proxy

Proxy Type	
Manual	Establish a Proxy manually
Proxy Server URL	Address for access to the Proxy Settings
Port	Establish Proxy port
Authentication	Username for the authentication at the Proxy
Password	Password for the authentication at the Proxy
Automatic	Establish a Proxy automatically
Proxy PAC URL	Proxy PAC URL
Allow direct connection if PAC is unreachable	Allow direct connection (without VPN), if PAC is unreachable
Allow bypassing proxy to access captive networks	Allow bypassing proxy to access captive internal networks

AirPrint

IP Address	Printer IP address
Resource Path	Definite path to the AirPrint device

AirPlay

Device Name	Device name
Password	Pairing password
Whitelist	Define a list of devices, with which the device can pair itself exclusively

PIM Management

Exchange Active Sync

Account Name	Email account name
Exchange ActiveSync Host	Address/FQDN of the server
Allow Move	Allow the moving of emails
Use Only in Mail	Interactions may only occur on the native Mail App
Use SSL	Use SSL encryption
Domain	Server domain
User	Username
eMail Address	email address (only on device level)
Password (only on device level)	User password
Identity Certificate	Select the respective certificate for authentication at the server
Past Days of Mail to Sync	Number of days, up until the emails should be synchronized back. No Limit = unlimited
Enable S/MIME	Enable S/MIME encryption
Signing Certificate	Upload the respective Signing Certificate
Encryption Certificate	Upload the respective Encryption Certificate

eMail

Set up of POP3 / IMAP accounts on the end user device

Account Description	Name des Email Accounts			
Account Type	IMAP	Path Prefix	The Path Prefix for special folders	
	POP			
User Display Name	User display name			
Email Address	User email address			
Allow Move	Allow the moving of emails			
Enable S/MIME	Enable S/MIME encryption			
Signing Certificate	Upload the respective Signing Certificate			
Encryption Certificate	Upload the respective Encryption Certificate			

Incoming Mail

Incoming server settings

Mail Server Address	Mail Server address
Mail Server Port	Mail Server port
User Name	Respective user name
Authentication Type	Authentication Type
None	No Authentication Type
Password (only on device level)	Password prompt
MDM Challenge-Response	
NTLM	NTLM-Authentication
HTTP MD5 Digest	
Use SSL	Use SSL, if needed

Outgoing Mail

Outgoing server settings

Mail Server Address	Mail Server Address
Mail Server Port	Mail Server Port
User Name	Respective User Name
Authentication Type	
None	No authentication method
Password (only on device level)	Password prompt
MDM Challenge-Response	
NTLM	NTLM-Authentication
HTTP MD5 Digest	
Use SSL	Use SSL, if needed
Outgoing password same as incoming	Outgoing password same as incoming
Use only in mail	Activate, if all outgoing emails are to be sent via the Mail-App

CalDav

Configure the set up and distribution of a CalDav Account

Account Description	Display name of the account
Hostname	Hostname and/or IP address
Port	Port of the CalDav Account
Principal URL	Principal URL of the Account
Username	Respective CalDav username
Password (only on device level)	Respective CalDav password
Use SSL	Use SSL, if needed

Subscribed Calendars

Set up and distribution of Subscribed Calendars

Description	Display name of the account
URL	URL of the calendar database
Username	Username of the calendar subscription
Password (only on device level)	Password of the calendar subscription
Use SSL	Use SSL, if needed

LDAP

In this area, set up a LDAP-connection, in order to allow a dynamic certificate exchange, between the end user device and the Active Directory.

Please note that the selected user requires the respective read permission.

Account Description	Account Description
Account Username	User for LDAP-access
Account Password	Password for LDAP-access
Account Hostname	LDAP Server Hostname/IP address
Use SSL	Use SSL, if needed

In the second part, you can define individual filters for searching in the LDAP registry.

Description	Scope	Search Base

Filter description	Search level in the LDAP registry	Define the individual filter

Web Management

Webclips

In this location define bookmarks, with links to webpages, intranet portals etc., which will be visible as an application on the end user device.

Label	Name of the connection on the end user device
URL	Link to the respective website
Removable	If activated, the user can remove the webclip
Icon	Via this dialogue, upload a logo for the connection: Dimensions 180x180, png format
Precomposed Icon	If activated, no additional effects (shadow, reflection) will be displayed on the icon
Full Screen	When opening webclips, the browser opens in full screen mode

Web Content Filter

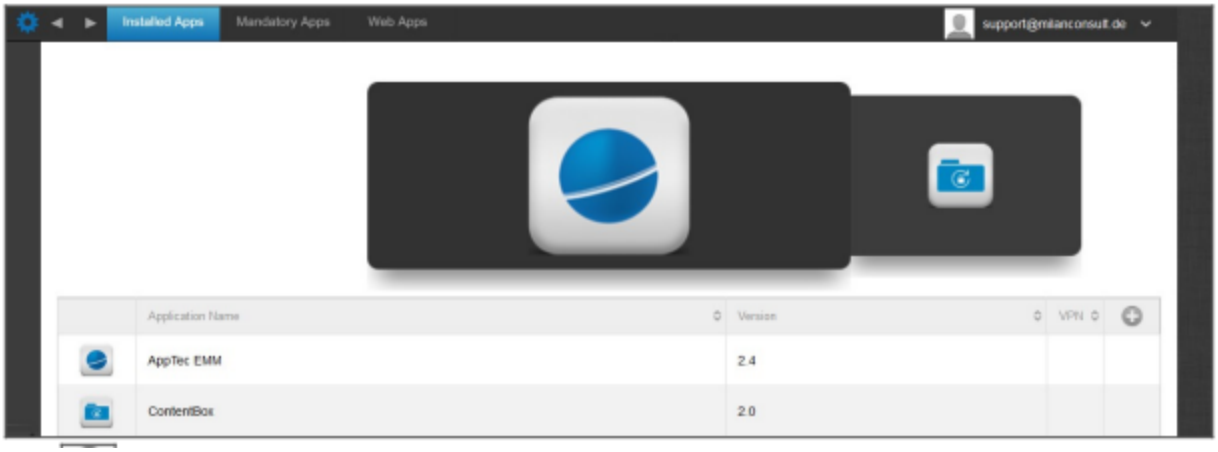
The Web Content Filter makes it possible, to limit access to specific internet pages.

Allowed Websites	
Limit Adult Content	Webfilter is automatically applied for adult content
Permitted URLs	With the + symbol add permitted pages
Blacklisted URLs	With the + symbol add blocked pages
Specific Websites Only	Only specific content can be displayed, which you can add with the + symbol.

App Management

Enterprise App Manager

Installed Apps (only on device level)



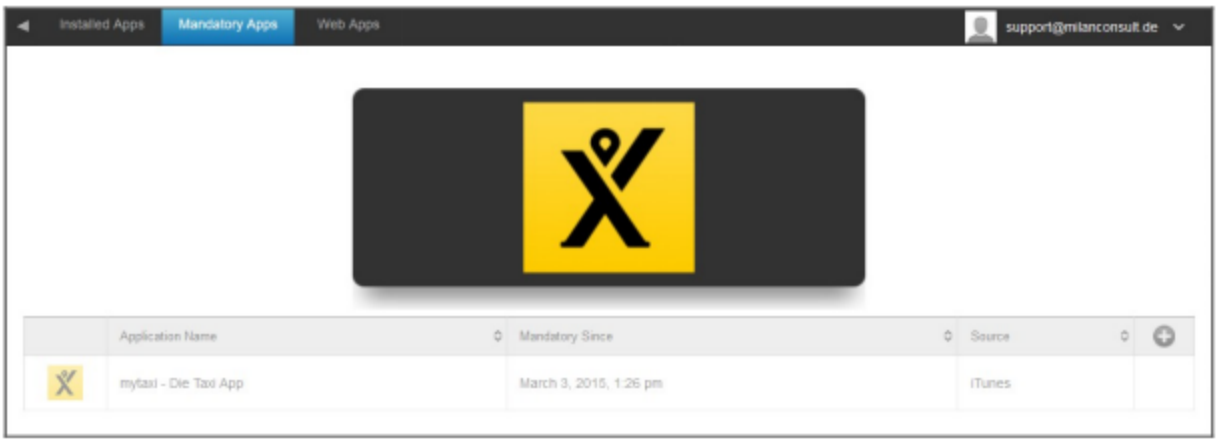
Here you can see the Apps that are currently installed on the device.

Mandatory Apps

Under Mandatory Apps, you can mandate necessary Apps.

The user will continually reminded to install this mentioned App.

Via the , the mandated App can be defined.



This can be an Apple App Store App, but also an In-House App.

Should this involve a supervised device, then the app will be installed automatically.

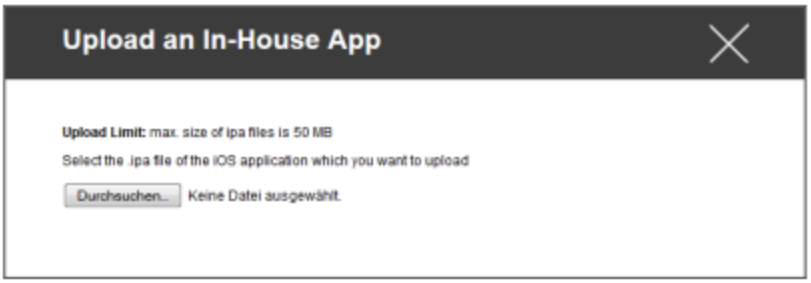
You can push an “Apple AppStore“ App from the public AppStore onto the device, as well as an internally developed In-House App.

Or you can select from “iOS In-House Apps“ category and pick an In-House App, that you uploaded under General Settings.

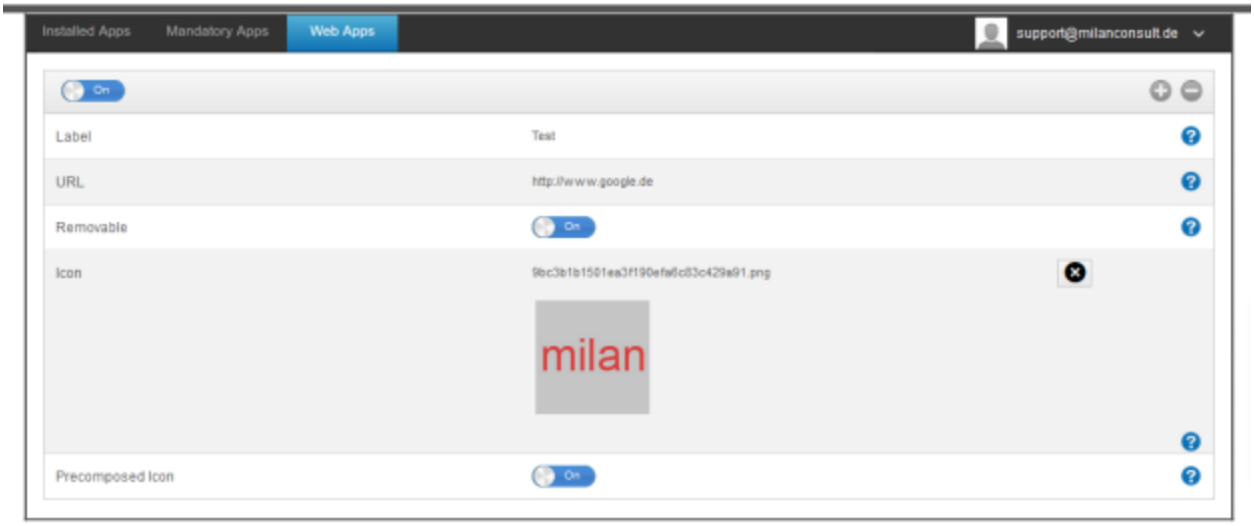
Installation-options

Keep up to date (only supported for VPP per device)	Once a week, it will be determined, if there is an update for the app. If yes, this update will be installed For In-House Apps the Update Target you configured in General Settings will be used for the update process.
Overtake when unmanaged	If the app is already installed, the MDM will take over the app and manage it
Remove app when MDM profile is removed	In the case of a device management removal, the App will be uninstalled
Prevent backup of app data	A backup of app-specific data will not be created
App Setting	Under “App Settings“, you can assign the app certain values into the foreground (as long as the app supports it, if necessary ask the app's developer).

You can also directly select and upload an ipa file, via “Upload In-House App“.



Web Apps



Under the point “Web Apps“, you can, similar as with “Web Clips“, push internet pages or intranet portals as an application onto the end user device, in the area of Web Management. As a default, Web Apps will be displayed in full screen mode, which can be configured under Webclips.

Label	Name of the connection on the end user device
URL	Link to the respective Website
Removable	If activated, the user can remove the Webclip
Icon	Via this dialogue, upload a logo for the connection: Dimensions 180x180, png format
Precomposed Icon	If activated, no additional effects (shadow, reflection) will be displayed on the icon

Restriction & Settings

Blacklisted / Whitelisted Apps

Here you can set the apps that are blocked (or allowed) depending on your settings in “General Settings”. A click on will bring up the known app-search. There you can search for the apps you want to add.

Note that a supervised device is necessary for this function

SysApp Restrictions

Block specific apps or functions of your device

Allow use of YouTube	Allow use of YouTube
Allow use of iTunes Store	Allow use of iTunes Store
Allow use of Safari	Allow use of Safari
Enable autofill	Allows autofill
Force fraud warning	Forces the fraud warning
Enable JavScript	Enables the use of JavaScript
Block pop-ups	Blocks all kind of pup-ups
Allow Cookies	Choose when Safari will accept cookies

App-VPN

Via the symbol, you can define applications that will automatically launch the selected VPN-connection at start-up.

App Settings

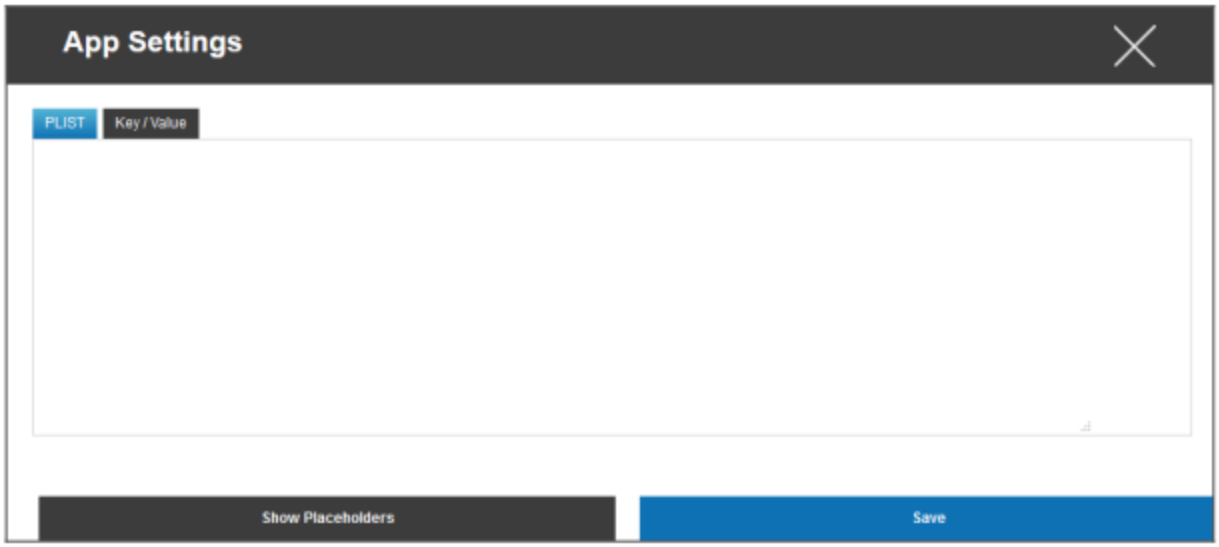
Under “App Settings“, you can assign the app certain values into the foreground (as long as the app supports it, if necessary ask the app's developer).

Via the symbol, you add an (additional) app. You will, once again, find the familiar AppTec360 representation of an App-Import.

Search here for the App that you would like to configure and select it. The settings will only apply to managed apps.

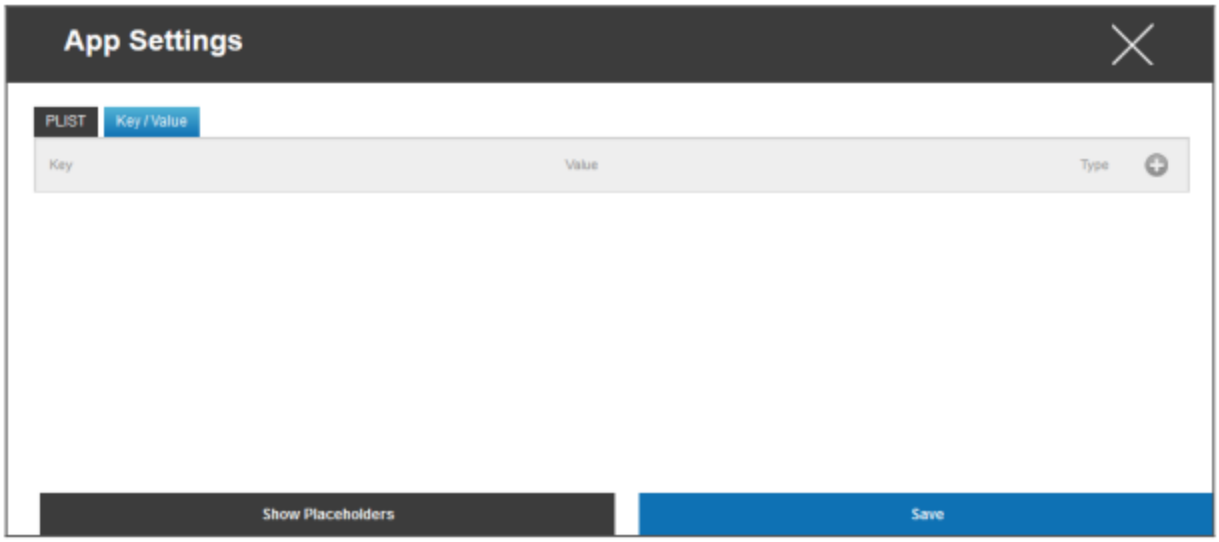
Should the Import should have been successful, you will see the following display:

Now, with a click on , you can perform a variety of configurations. You will then receive the following overview:

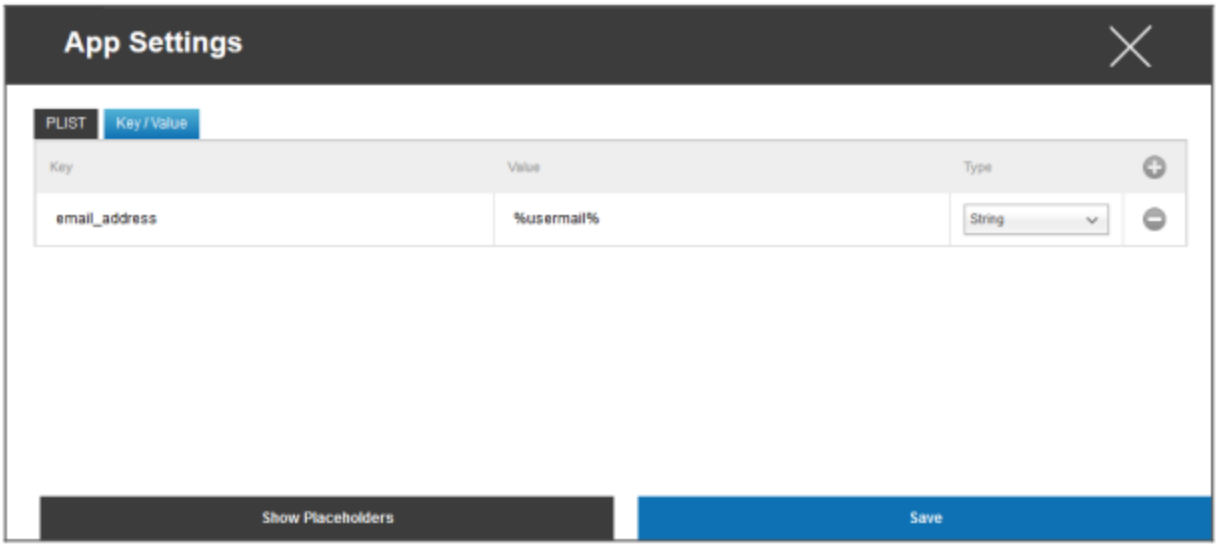


Should you already have a PLIST (source text of configuration), you can add it here and save it all with “Save“.

Under “Key / Value“, you can attach specific configurations to the App



Here, you can establish a new key and its value with the symbol.



Of course, all of AppTec's placeholders are at your disposal

“Type“ explanation:

String	Text
Boolean	True/False
Number	Number

With the symbol, you can remove an app again.

Enterprise App Store

iTunes Apps

Under this point, you can distribute optional Apps for your User.

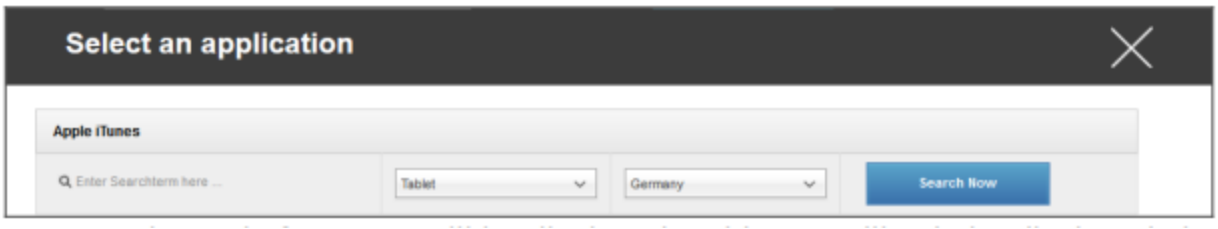
Should there be an App here, it will be installed automatically on the AppTec360 Store's end user device.

These are simply links to the official Apple App Store. For this reason, each end user device must be outfitted with an Apple ID.

At this point, we recommend that each user has their own Apple ID.

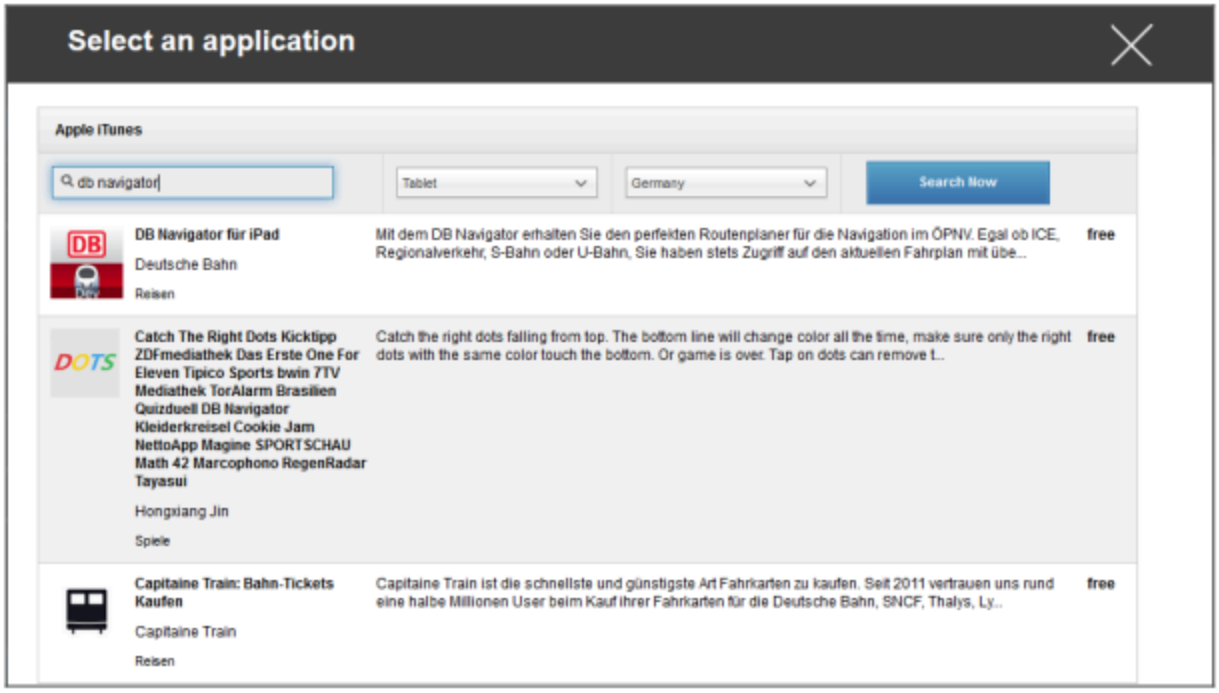
With the symbol, you can add additional Apps.

After that, a window with the following overview should open.



Please note, that only free apps will be displayed, paid apps will only be displayed via VPN.

Under “Enter Search Term here …“, you can search for an app, that is in the Apple App Store.



Once you click on the Icon or on the app's name, you will be asked again to perform additional configurations.

Keep up to date	Once a week, it will be determined, if there is an update for the app. If yes, this update will be installed
Remove app when MDM profile is removed	In the case of a device management removal, the App will be uninstalled
Prevent backup of app data	A backup of app-specific data will not be created
App-VPN	Select a VPN-connection, which will launch on opening the App

After a click on “Install“, the app will be added to the Enterprise App Store and can then be installed on the end user device, via the AppTec360 AppStore.

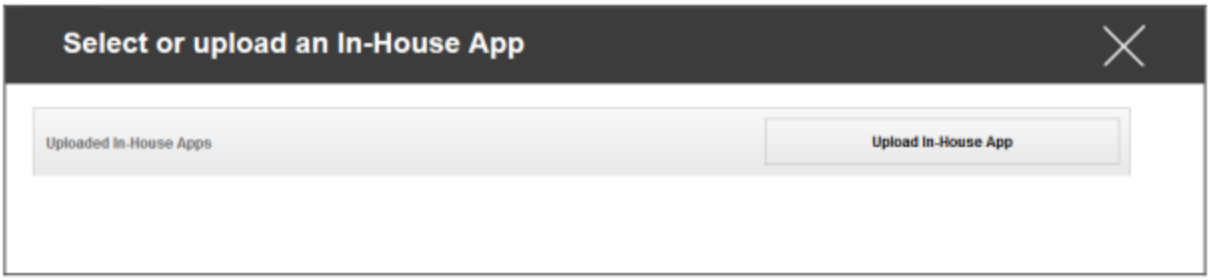
Should the App-Store Import have been successfully, you will receive the following overview:

In-House

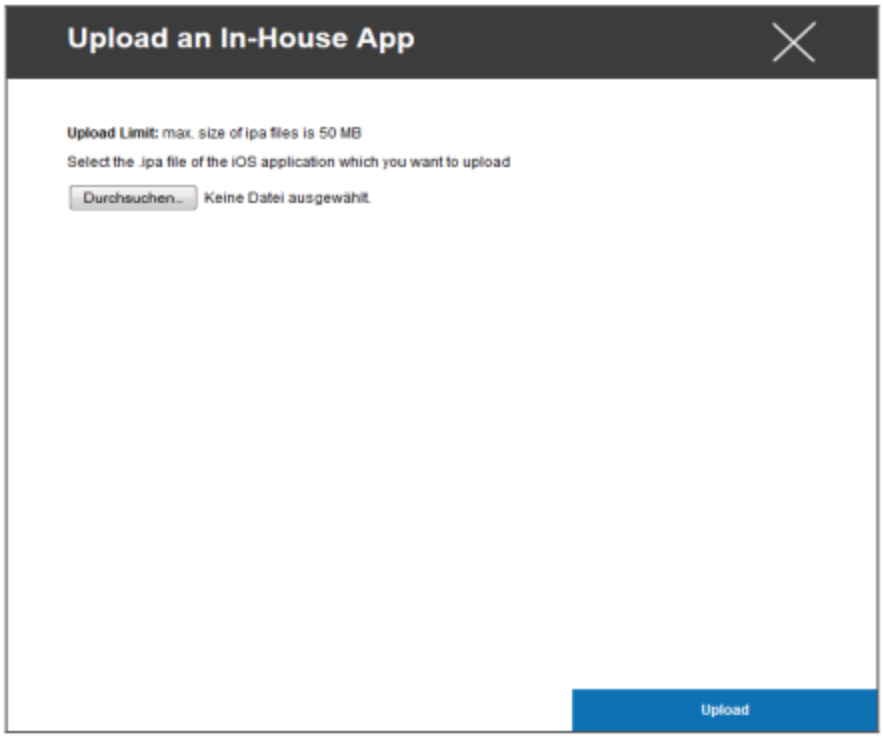
Under the point “In-House“, you can upload internally developed Apps and distribute them.

With the symbol, you can distribute additional In-House Apps.

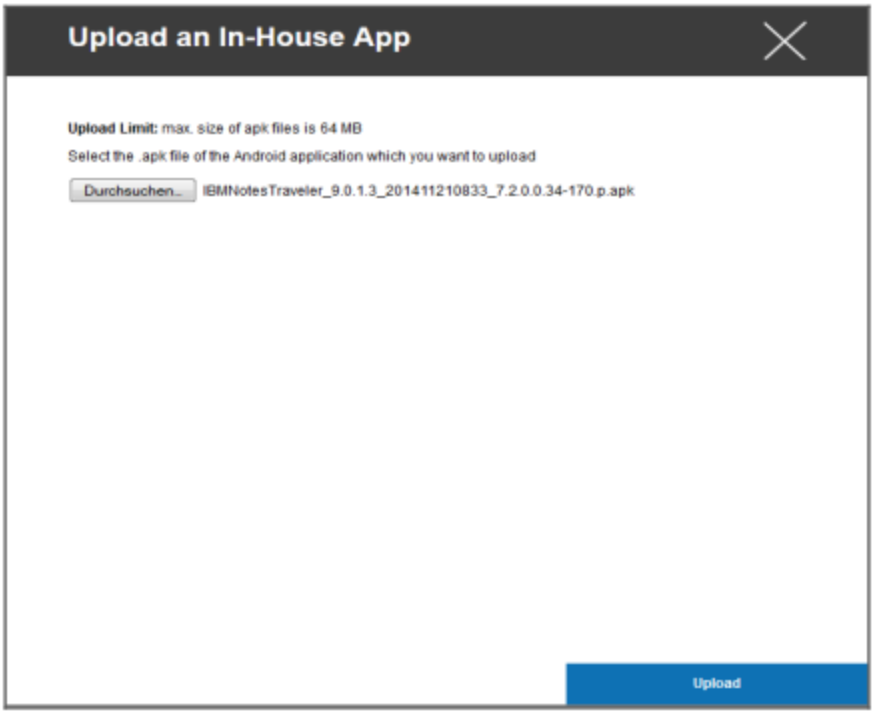
If you have never distributed In-House App, you will then receive the following overview:



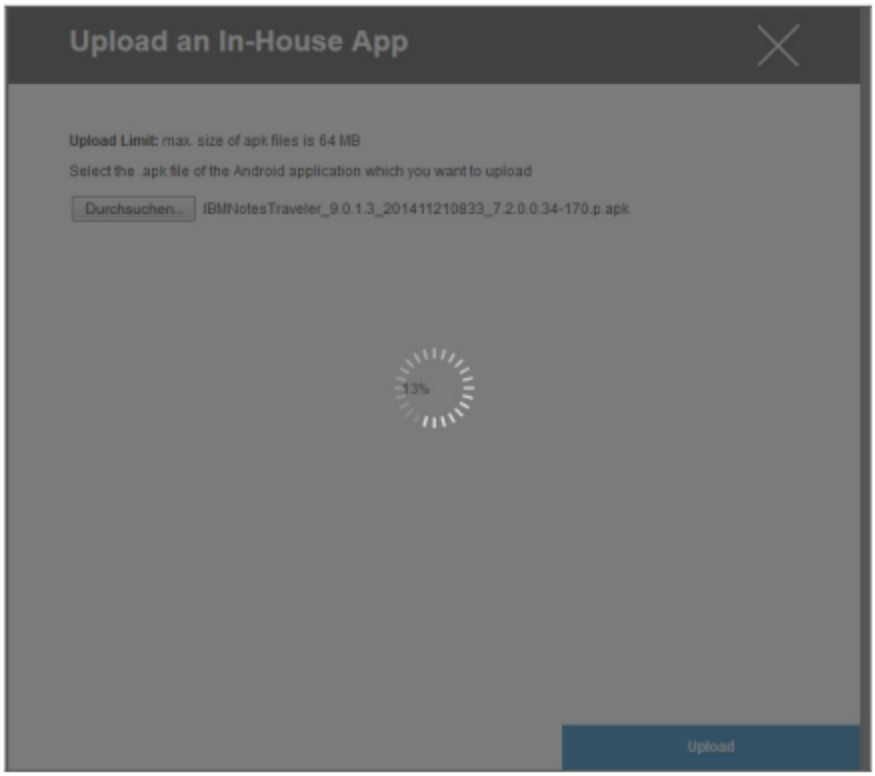
For this, click “Upload In-House App”, you will then receive the following overview:



Now, select with “Search…“an .ipa file and then click on “Upload“



Your App will now be uploaded. In the middle of the circle, you can see the percentage of how much of your App has been already uploaded.



Should the upload of the In-House App have been performed successfully, you will see the newly uploaded app in your App Catalog.

The user now has the option to see and install this app in the AppTec360 Store on the end user device, under the category “In-House“.

Due to the fact that this does not involve a public Apple AppStore App, the user does not need a stored Apple ID on the end user device.

Kiosk Mode

iOS Kiosk Mode is only Available in Supervised Mode

The Kiosk Mode allows you to pre-define an App or URL, so that it will be possible to run/visit this App/URL exclusively.

Additionally, you can deactivate various hardware buttons in the Kiosk Mode.

Application Type

Package

If you want to launch the app in Kiosk Mode, select “Package“ under “Application Type“

Kiosk Application	Click here, in order to select an app, that should launch in Kiosk Mode You will find the current overview of the App Management You can select between “Apple iTunes Apps“ and “iOS In-House Apps“

URL

If you want to launch a URL in the Kiosk Mode, select “URL” under “Application Type“

URL	Now, define the desired URL address
Same Origin Policy	Should this function be active, the user can then only surf the subpages of the predefined URL For example, if you have defined the following URL: www.mypage.com, then the user can surf on www.mypage.com/subpage
Whitelisted URLs	Here you can maintain a Whitelist, all of these URLs are allowed Maximum 1 URL per line A URL must start with http:/ or https://
Blacklisted URLs	Here you can maintain a Blacklist, all of these URLs are disallowed Maximum 1 URL per line A URL must start with http:/ or https://
Clear Browser after inactivity	After inactivity the Browser Cache will be emptied
Exit Password Enabled	If you activate this function, the user has the option, to end the Kiosk Mode with a password, that has been predefined by you
Exit Password	This is the password that has been predefined by you

Kiosk Mode Settings

Scheduled Kiosk Mode	Based on the time of day, you can set the Kiosk Mode, so that then the mode is started and ended automatically at a time, that has been predetermined
Start Time	Start time
Time in minutes	Time in minutes, after which the Kiosk Mode should be ended again
Disable Touch	If activated, touchscreen is deactivated
Disable Device Rotation	If activated, the automatic screen adaptation is deactivated
Disable Ringer Switch	If activated, the ringer switch will then be deactivated. From then on, the behavior is dependent on the previously set function
Disable volume buttons	If activated, the volume buttons will be deactivated
Disable Sleep Wake Button	If activated, the on/off switch will be deactivated
Disable Auto Lock	If activated, the device will not be switched to standby
Enable Voice Over	If activated, the Voice Over Assistant will be activated
Enable Zoom	If activated, the zoom will be activated
Enable Invert Colors	If activated, the inverted display mode will be activated
Enable Assistive Touch	If activated, the AssistiveTouch will be activated
Enable Speak Selection	If activated, the speak selection will be activated
Enable Mono Audio	If activated, the Mono Audio will be activated
VoiceOver	If activated, the user can enable VoiceOver
Zoom	If activated, the user can enable Zoom
Invert Colors	If activated, the user can enable inverted colors
Assistive Touch	If activated, the user can enable assistive touch

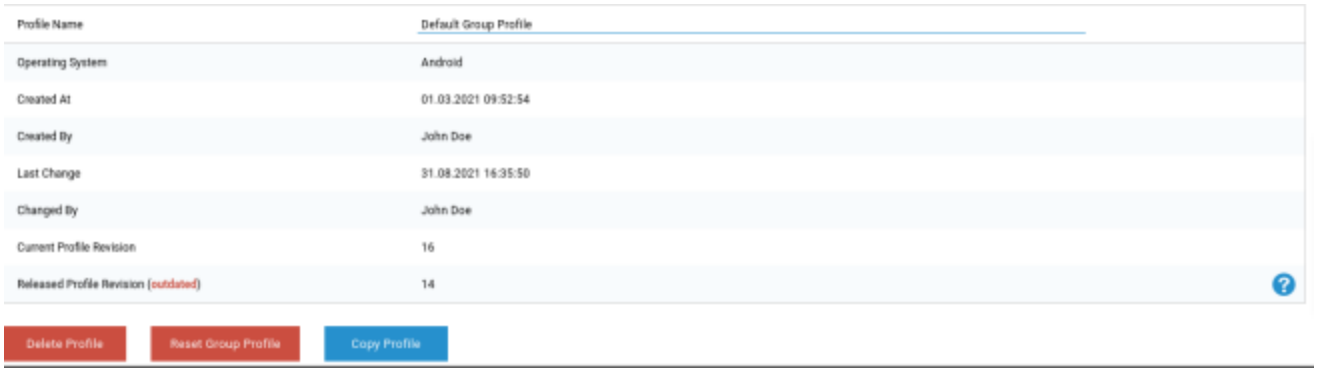
Android Enterprise – Fully Managed Device Configuration

Depending on if you have currently selected a group profile or a device, the overview and its sub points differ – please consider this carefully!

General

Group profile overview (only on group level)

When opening a group profile, you will get a quick overview of the profile.



Profile Name	Name of the profile (can be changed here)
Operating System	Operating System the profile is for
Created At	Time of creation
Created By	The profile's creator
Last Change	Time of last change to the profile
Changed By	Account that made the last changes
Current Profile Revision	Revision of saved profile state
Released Profile Revision	Assigned profile revision ("Assign now"). If the label shows "(outdated)" behind the text, it means you've saved the profile but did not assign it yet, so the devices will still get and older version.

Device Overview (only on device level)

Should you be on a device, you will receive an overview recap of the selected device, the following is contained here:

Device Name	Device name
Location	Location coordinates
Phone Number	Phone number
Assigned Mandatory Apps	Number of assigned Mandatory Apps
OS Version	OS version of the device
Operating System	Operating System (Android Enterprise)
Serial Number	Device serial number
Device Ownership	Corporate or private device
Device Type	AE Work Managed Device
Rooted	Status, indicating if the device has been rooted
Compliant	Guideline compliant
IP Address	IP Address of the device
Last Seen	Point in time, when the device last connected to AppTec
Last Push	Point in time, when the last push was sent to the device
AE Device Owner Mode	Yes
User Assignment	The user or group this device is assigned to

Config Revision (only on device level)

Here you receive an overview of which group profile is assigned to the device.

If you click on the group profile, you will gain direct access to this profile and you can perform settings.

With this symbol, you can revert the distributed apps to the group profile's settings.

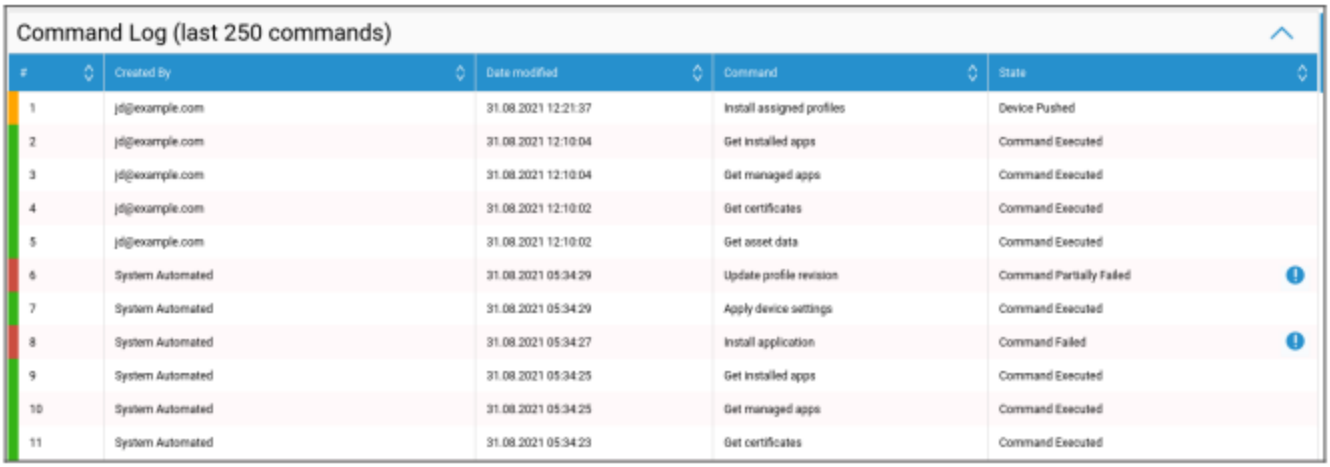
With this symbol, you can revert all of the used apps to the group profile's settings.

“Newer Revision available“ indicates that the group profile has been changed and saved but not assigned. The group profile has to be assigned with “Assign now” on group level to apply the changes to the devices.

Device Log (only on device level)

Command Log

Here you can see which commands where issued for the device and what their status is.



Commands created by “System Automated” are automatically created by the system.

Possible command statuses

Device Pushed	A push request has been sent to the push service (e.g APNS) to tell the device to connect back to the EMM server.
Command Created	The command was created in the system.
Command Sent	The command got sent to the device after it connected to the server.
Command Executed	The command was successfully executed.
Command Failed	The command failed. *
Command Partially Failed	Depending on the device OS some commands may get grouped together. In this some parts of this command group failed. *
Command Executed, eventually Failed	The command was executed but maybe it wasn't.
Command Repushed	The command was repushed by a user.
Discarded	The command was discarded. For example because it was superseded by another command or the device got re-enrolled and old commands got removed

If there is an exclamation mark behind the message, you can get more information by hovering over the icon with your cursor.

Device Settings

Client Configuration

Here you can perform the following configurations on your Android device:

Out of Compliance Time	The user response timeout limit after which the enforcement action is applied.
Enforcement action after compliance timeout	Enforcement action when a user doesn't perfom actions that leads to a compliant device status
Data Collection Frequency	Frequency with which device/GPS-information is to be collected
Device Heartbeat Frequency	Interval in which the device should contact the AppTec360 Server Min. 1 minute Max. 24 hours
Enable Location Updates	If activated, the device sends location updates to the AppTec360 Server
Location Update Time	Determines in what time intervals the device sends location updates to AppTec360
Use Google Location Accuracy for Location Update	If activated, the network location will be used for location updates (if this was deactivated under "Restrictions", then this setting will not affect anything)
Use GPS Location for Location Update	If activated, the GPS will be used for location updates
Allow Mock (Fake) Locations	Allows the forging of location information via third party apps
Lost Connection Action	If enabled, you can specify an action for the case that a device doesn't get a connection to the MDM server in the heartbeat interval. For example, if the device has a heartbeat time of 5 minutes, it connects to the server at 10:35 AM. After that the device leaves the Wi-Fi range. The next heartbeat at 10:40 AM will fail, and the specified action will be executed.
Action	The action that is to be taken, as soon as a device becomes non-compliant. • Lock Device = lock device

		• Wipe Device = device will be restored to factory settings • Wipe Device & SD Card = device will be restored to factory settings and SD Card storage will be deleted
	Threshold	You can specifiy a threshhold of failed Heartbeats which are necessary to trigger the specified action.

Policy Enforcement Mode	Default:	Users will be prompted periodically to execute outstanding actions
	Lazy Policy Enforcement:	Users will never be prompted to execute outstanding actions. All open action will be shown in the AppTec360 Client
	Aggressive Policy Enforcement:	Users will be prompted non stop to execute outstanding actions
AppTec360 Version Lock	If enabled, a version code for the AppTec360 MDM Client can be specified. The AppTec360 client will only update to the specified version. Newer versions will be ignored. A downgrade is NOT possible.	
Version Code	Version code for the AppTec360 MDM Client to be locked on to.	
Disable AppTec360 Notification	If disabled the AppTec360 Client won't show a Notification in the Notification Bar. Thus users can close the AppTec360 client via the task manager. If the AppTec360 client is closed, several features including Kiosk Mode and App Black/Whitelisting will not work properly. Samsung devices offer a protection mechanism for the AppTec360 Client. The notification is disabled by default on Samsung devices that support the KNOX APIs. The notification shouldn't be disabled devices with Android 8.0 or higher.	

Wallpaper

Set custom Wallpaper	Enable/Disable the custom wallpaper
Wallpaper	Set the wallpaper mode to use a color code or an image
Specify a Color	Specify a backgorund color as hex value, e.g. #000000 for black or #ffffff as white
Set Image as Wallpaper	Upload the image file you want to use as wallpaper

Asset Management (only on device level)

Device Info

Model	Device model designation
Operating System	OS
OS Version	OS version
Serial Number	Serial number
Device Name	Device name
Battery Status	Battery status
Free / Total Memory	Free / Total memory
Samsung Safe	Samsung SAFE interface, required for a variety of setting options
SD Card Available	SD Card available
SD Card Emulated	SD Card emulated
SD Card Removable	SD Card removable
SD Free / Total Memory	SD Free / Total SD Card memory

Wi-Fi

IP Address	Device IP address
WiFi MAC	WiFi MAC address

Cellular

Status	Status (SIM card installed)
Phone Number	Phone Number
Roaming (Voice / Data)	Roaming for voice / data
Roaming Status	Current roaming status
IP Address	IP address
Operator/Carrier	Operator/Carrier
Cellular Technology	Cellular Technology
IMEI	IMEI number
ICCID	This is the ID for the SIM card, often times also a Smartcard or Integrated Circuit Card (ICC)
IMSI	The International Mobile Subscriber Identity (IMSI) provides in GSM- and UMTS-mobile networks a definite identification of the network users The IMSI is comprised of a maximum of 15 digits and is configured in the following manner: • Mobile Country Code (MCC), 3 digits • Mobile Network Code (MNC), 2 or 3 digits • Mobile Subscriber Identification Number (MSIN), 1-10 digits
Current MCC/MNC	See "SIM MCC/MNC"
SIM MCC/MNC	The Mobile Country Code is an established country identifier, set by the ITU as per E.212 Standard. This works in conjunction with the Mobile Network Code (MNC) for the identification of the mobile network. Meaning the SIM card's country/Mobile Network Code. If you roam into another mobile network, then logically, the "Current MCC/MNC" and "SIM MCC/MNC", will be different.

Bluetooth

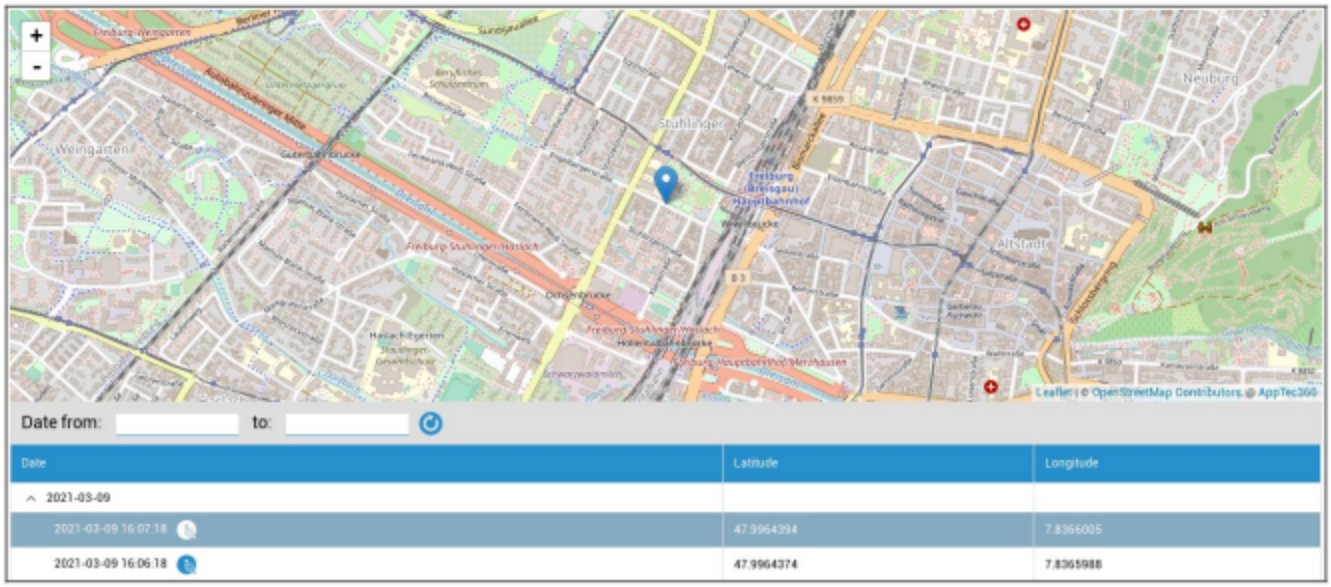
Bluetooth MAC	Bluetooth MAC address

Security Management

Anti Theft (only on device level)

GPS Information (only on device level)

Here you can establish the current/last device location. The localizing can be protected with one or even two passwords – See: General Settings – Privacy – GPS Access



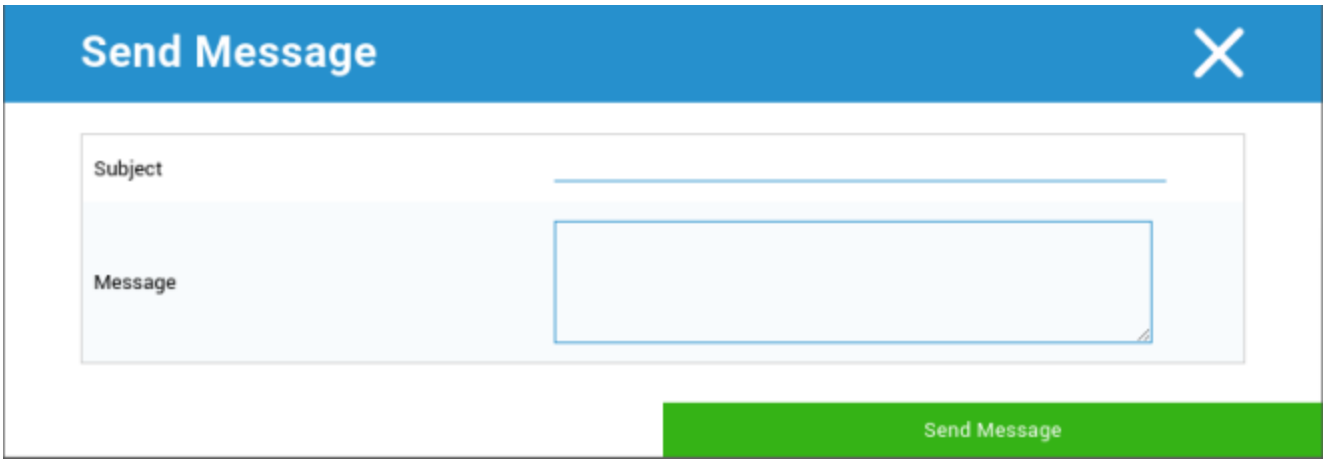
Wipe & Lock (only on device level)

Under „Wipe & Lock“, you can perform the following three actions:

Full Wipe	The device is restored back to its factory settings (corporate, as well as personal data is deleted)
Enterprise Wipe	Only corporate data is removed from the end user device (all apps, data, etc. that were provided by AppTec360)
Lock Screen	Screen lock is activated, it is sufficient to unlock the device with the device-password/PIN

Message (only on device level)

Here you can fill in the subject and a message and send it to an end user device.



Security Configuration

Device Passcode

Under “Passcode“ you can mandate a device password, the following setting options are available to you

Minimum password length	Establishes, the minimum number of symbols a password must have	
Password quality	Unspecified	This policy has no requirements for the password.
	Biometric Weak	This policy allows for low-security biometric recognition technology. This implies technologies that can recognize the identity of an individual to about a 3 digit PIN (false detection is less than 1 in 1,000).
	Something	This policy requires some kind of password or pattern to be set, but doesn't enforce any specific rules.
	Alphabetic	The user must have entered a password containing at least alphabetic (or other symbol) characters.
	Alphanumeric	The user must have entered a password containing at least both, numeric and alphabetic (or other symbol) characters.
	Complex	The user must have entered a password containing at least a letter, a numerical digit and a special symbol, by default. With this password quality, passwords can be restricted to contain various sets of characters, like at least an uppercase letter, etc.
Minimum password length	Set the required number of characters for the password. For example, you can require PIN or passwords to have at least six characters.	
Minimum numerical digits required in password	Minimum numerical digits required in password	
Minimum lowercase letters required in password	Minimum lowercase letters required in password	
Minimum uppercase letters required in password	Minimum uppercase letters required in password	

Minimum non-letter characters required in password	Minimum non-letter characters required in password
Minimum symbols required in password	Minimum symbols required in password

Maximum inactivity time lock	Maximum user inactivity until time lock
Password expiration timeout	Establishes, after which time interval the password expires and a new password must be issued
Password history restriction	Number of previously used password that are not allowed
Maximum failed password attempts	Establishes, how often a password can be entered incorrectly, before a complete device wipe will be performed
Allow Biometric Authentication	Enables authentication via fingerprint or iris scan. Only for Samsung KNOX 2.1 and higher

AntiVirus

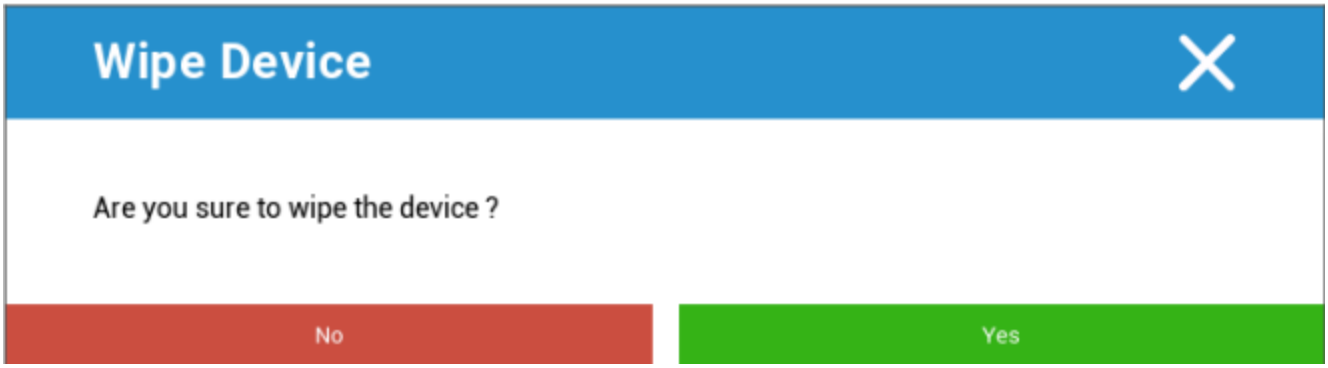
Automatic Scan	Enable periodic automatic scans
Scan Interval	Interval for examination (Quick / Full)
Full Automatic Scan	Enable full automatic scans
Automatic Updates	Enable automatic updates
Update Check Interval	How often the app and its database should be updated (viruses / damaged code)
App Protection	Enable automatic app scan
SD Card Protection	Enable automatic SD Card scan
Wi-Fi Only Update	When enabled, updates will be applied only when the device is successfully connected to a Wi-Fi network

End of Life (only on device level)

Wipe (only on device level)

Under “Wipe“, you can restore the device to its factory settings. Here the corporate, as well as the private data will be deleted on the end user device.

With a click on the “Minus Symbol“ you receive the following message:



With “Yes“ you can perform the wipe.

Under “Wipe Report“ the following items can be displayed

Wiped by	History of who performed the wipe
Date	Date
Status	Status (ex. if the Wipe was performed successfully)

Restriction Settings

Restrictions

Here, a variety of things can be restricted and blocked.

Enable Camera	Allow use of camera	
Force Auto Sync	On	Synchronization is permanently activated
	Off	Synchronization is permanently deactivated
	User choice	Selected by the user
Force Bluetooth	On	Bluetooth is permanently activated
	Off	Bluetooth is permanently deactivated
	User choice	Selected by the user
Force GPS	On	GPS is permanently activated
	Off	GPS is permanently deactivated
	User choice	Selected by the user
Force Network Location	On	Permanent internet-localizing
	Off	Permanent deactivation of internet-localizing
	User choice	Selected by the user

Security		
Disallow Share Location	Specifies if a user is disallowed from turning on location sharing.	
Disallow Safe Boot	Specifies if the user is not allowed to reboot the device into safe boot mode.	
Disallow Network Reset	Specifies if a user is disallowed from resetting network settings from Settings.	
Disallow Factory reset	Specifies if a user is disallowed from resetting the device.	
Enable ADB	Allows the Connection to a PC via ADB	
Disable Keyguard	Disables Keyguard	
Device Owner Lockscreen Info	Sets the device owner information to be shown on the lock screen.	
Compliance Enforcement	Mode Prompt User	User will be prompted to fulfill the necessary actions.
	Mode Lock-Down Container	Hide all apps until all requirements are fulfilled

App Management	
Allow Cross Profile App Linking	Allows apps in the parent profile to handle web links from the managed profile.
Disallow App Control	Specifies if a user is disallowed from modifying applications in Settings or launchers.
Disallow App Installation	Specifies if a user is disallowed from installing applications.
Disallow Uninstall Apps	Specifies if a user is disallowed from uninstalling applications.
Runtime Permission Policy	Specifies how new permission requests from apps will be handled.
Allow Unknown Sources	If enabled, users can sideload Apps by installing an .apk file.

Connectivity	
Disallow Mobile Network Config	Specifies if a user is disallowed from configuring mobile networks.
Disallow Tethering Config	Specifies if a user is disallowed from configuring Tethering & portable hotspots.
Disallow VPN Config	Specifies if a user is disallowed from configuring a VPN.
Disallow Wifi Config	Specifies if a user is disallowed from changing WiFi access points.
Disallow Outgoing NFC Beam	Specifies if the user is not allowed to use NFC to beam out data from apps.
Lock WiFi Configuration	This setting controls whether WiFi configurations created by a Device Owner app should be locked down (that is, be editable or removable only by the Device Owner App, not even by Settings app).
Enable Data Roaming	Activates Data Roaming

Bluetooth	
Disallow Bluetooth	Specifies if bluetooth is disallowed on the device. Requires Android 8.0
Disallow Bluetooth Sharing	Specifies if outgoing bluetooth sharing is disallowed on the device. Requires Android 8.0
Disallow Bluetooth Config	Specifies if a user is disallowed from configuring bluetooth.

Account Management	
Disallow adding managed profile	Specifies if a user is disallowed from adding managed profiles. Requires Android 8.0
Disallow adding Users	Specifies if a user is disallowed from adding new users.
Disallow Remove Managed Profile	Specifies if managed profiles of this user can be removed, other than by its profile owner. Requires Android 8.0
Disallow Account Modification	Specifies if a user is disallowed from adding and removing accounts, unless they are programmatically added by Authenticator.

Telephony	
Disallow Outgoing Calls	Specifies that the user is not allowed to make outgoing phone calls.
Disallow SMS	Specifies that the user is not allowed to send or receive SMS messages.

System	
Disallow Window Creation	Specifies that windows besides app windows should not be created.
Disallow set User Icon	Specifies if a user is not allowed to change their icon.
Disallow Set Wallpaper	User restriction to disallow setting a wallpaper.
Disable Status Bar	Disabling the status bar blocks notifications, quick settings and other screen overlays that allow escaping from a single use device.
Enable Auto Time	Sets the time automatically.
Enable Auto Time Zone	Sets the timezone automatically.
Stay on while plugged in	The device will stay active while connected to a power source.

Storage	
Disallow disable App Verification	Specifies if a user is disallowed from disabling application verification.
Disallow Mount Physical Media	Specifies if a user is disallowed from mounting physical external media.
Enable Backup Service	Backup service manages all backup and restore mechanisms on the device. Setting this to false will prevent data from being backed up or restored. Backup service is off by default. Requires Android 8.0
Enable USB Mass Storage	Enables the usage of USB Mass Storage.

Keyboard	
Disallow Autofill	Specifies if a user is not allowed to use Autofill Services. Requires Android 8.0
Disallow Copy & Paste between Profiles	Specifies if what is copied in the clipboard of this profile can be pasted in related profiles.

Sound	
Disallow Volume Adjustment	Specifies if a user is disallowed from adjusting the master volume.
Disallow Unmute Microphone	Specifies if a user is disallowed from adjusting microphone volume.
Mute Device	Mute device.

Certificate Management

Here you can distribute Trusted Certificates and Identity Certificates to your devices.

Android 8 or higher is required to distribute Trusted Certificates and Android 9 or higher is required to distribute Identity Certificates.

With the “+” you can add multiple certificates.

Trusted Certificates need to be in PEM format.

Identity Certificates need to be in PKCS12 format

Connection Management

Wifi

For this setting, perform the pre-configuration of the end user devices, for access to internal Access Points

Services Set Identifier (SSID)	SSID for the network that is to be connected
Hidden Network	Activate, in case the AP does not broadcast the SSID

Security Type

Establish the AP's security type

WEP

Password	Password for the AP

WPA/WPA2

Password	Password for the AP

802.1x EAP

EAP-Method

PWD	Identity	Identity	
	Password	Password	

PEAP	Phase 2 Authentication Protocol	none	No additional protocol
		MSCHAPV2	MSCHAPV2 protocol
		GTC	GTC protocol
	CA Certificate	CA certificate	
	Identity	Identity	
	Anonymous Identity	Anonymous identity	
	Password	Password	

TTLS	Phase 2 Authentication Protocol	none	No additional protocol
		PAP	PAP protocol
		MSCHAP	MSCHAP protocol
		MSCHAPV2	MSCHAPV2 protocol
		GTC	GTC protocol
	CA Certificate	CA Certificate	
	Identity	Identity	
	Anonymous Identity	Anonymous Identity	
	Password	Password	

TLS	CA Certificate	CA certificate
	Identity	Identity
	Password	Password

VPN

Connection Name	Name of the VPN Connection

VPN Type

VPN

VPN Client

AppTec360 VPN Client	
Gateway Configuration	Select the Gateway VPN Configuration (See **General Settings > Universal Gateway > VPN Settings**)
Always On VPN	Enable Native Lockdown
Enable AppTec360 Lockdown	Enable AppTec360 Lockdown

Built In (Only available on Samsung devices)			
Connection Type	PPTP	Server	Server
		Enable PPTP Encryption	Enable PPTP Encryption
	L2TP / IPSec PSK	Server	Server
		IPSec Pre-Shared Key	IPSec Pre-Shared Key
		Enable L2TP Secret	Enable L2TP Secret
		L2TP Secret	L2TP Secret
	IPSec XAuth PSK	Server	Server
		IPSec Identifier	IPSec Identifier
		IPSec Pre-Shared Key	IPSec Pre-Shared Key
DNS Search Domains	DNS Search Domains		
Expert Settings	DNS Servers	DNS Servers	
	Forwarding Routes	Forwarding Routes	

Open VPN		
Server	Server	
OpenVPN Profile	OpenVPN Profile	
OpenVPN App	OpenVPN for Android (recommended)	
	OpenVPN Connect	
Expert Settings	DNS Servers	DNS Servers
	Forwarding Routes	Forwarding Routes

Samsung / Strong Swan			
Connection Type	PPTP	Server	Server
		Username	Username
		Password	Password
		Enable PPTP Encryption	Enable PPTP Encryption
	L2TP / IPSec PSK	Server	Server
		IPSec Pre-Shared Key	IPSec Pre-Shared Key
		Username	Username
		Password	Password
		Enable L2TP Secret	L2TP Secret
	IPSec XAuth PSK	Server	Server
		IPSec Identifier	IPSec Identifier
		IPSec Pre-Shared Key	IPSec Pre-Shared Key
		Username	Username
		Password	Password
Expert Settings	DNS Servers	DNS Servers	
	Forwarding Routes	Forwarding Routes	

Cisco Any Connect		
Server	Server	
Certificate Mode	Disabled	Disabled
	Automatic	Automatic
Expert Settings	DNS Servers	DNS Servers
	Forwarding Routes	Forwarding Routes

Per-App VPN

VPN Client

AppTec360 VPN Client		
Gateway Configuration	Select the Gateway VPN Configuration (See **General Settings > Universal Gateway > VPN Settings**)	
VPN Apps	VPN Apps	
Always On VPN	Enable Native Lockdown	Always On VPN
Enable AppTec360 Lockdown	Enable AppTec360 Lockdown	

Samsung / Strong Swan			
Connection Type	PPTP	Server	Server
		VPN Apps	VPN Apps
		Username	Username
		Password	Password
		Enable PPTP Encryption	Enable PPTP Encryption
	L2TP / IPSec PSK	Server	Server
		VPN Apps	VPN Apps
		IPSec Pre-Shared Key	IPSec Pre-Shared Key
		Username	Username
		Password	Password
		Enable L2TP Secret	L2TP Secret
	IPSec XAuth PSK	Server	Server
		VPN Apps	VPN Apps
		IPSec Identifier	IPSec Identifier
		IPSec Pre-Shared Key	IPSec Pre-Shared Key
		Username	Username
		Password	Password
Expert Settings	DNS Servers	DNS Servers	
	Forwarding Routes	Forwarding Routes	

Restrictions

Here you can set the restrictions, in relation to the connection management.

Allow Data Roaming	Allow mobile data while roaming
Force Data Roaming	If activated, roaming for mobile data is permanently activated (not recommended!) This setting overwrites the "Allow Data Roaming" setting!
Following settings are only available on SAFE 2.x or higher	
Allow Emergency Calls Only	Allow Emergency Calls Only
Allow WiFi	Allow WiFi
WiFi Network Minimum Security Level	WiFi network minimum security level Open = all types of WiFi are permitted
Forbid user to add WiFi networks	The user may not add a WiFi network themselves This setting is only possible, if a WiFi profile was defined under "Connection Management"
Allow SMS & MMS	All = All SMS & MMS traffic is allowed Incoming SMS Only = Only incoming SMS messages are allowed Outgoing SMS Only = Only outgoing SMS messages are allowed None = No SMS / MMS traffic is allowed
Allow Sync during Roaming	Allow Sync during Roaming On = activated Off = deactivated User choice = user's choice
Allow Voice Roaming	Allow Voice Roaming On = activated Off = deactivated User Choice = user's choice
Use System http Proxy Server	The use of a HTTP proxy server, which is provided by the system's settings in settings, is dependent on the connected network (WiFi or APN)

PIM Management

Gmail Exchange

Info: This Configuration will be applied to the Gmail app. So you have to approve and install Gmail.

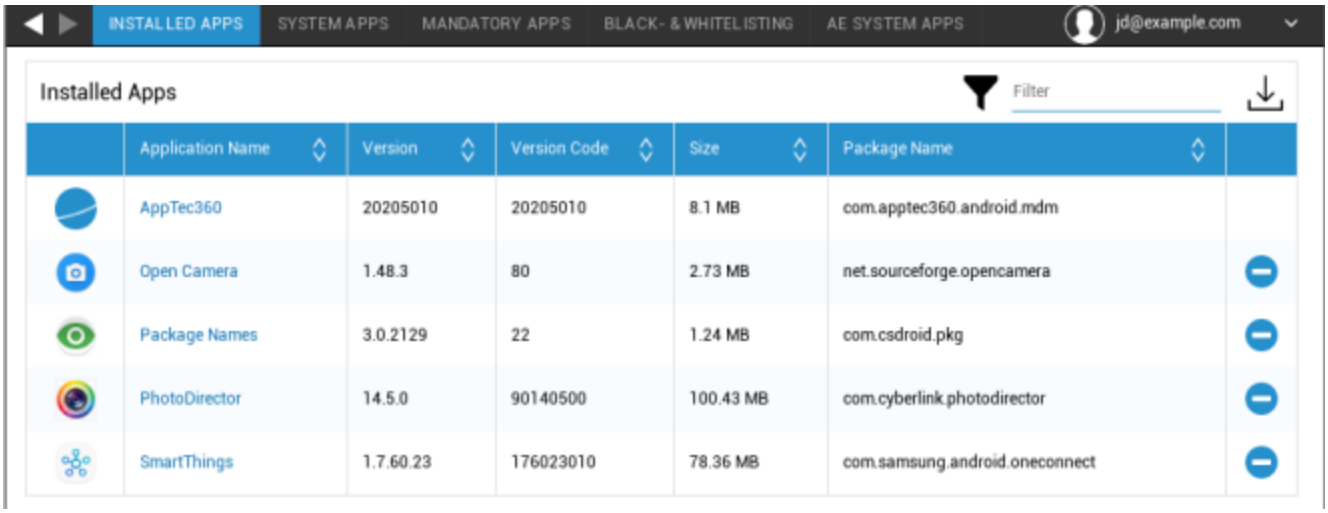
eMail Address	The provided user's email address Please note the "Placeholders", which you can use to work with credentials and you do not perform changes manually on every device With a click on you can display them for yourself
Server Hostname	Server address of your Exchange Servers
Login name	The Login-Name for the respective end user device, please also note the "Placeholders here
Signature	A signature can be attached (Hint: Some devices require HTML formatting for the signature)
Number of previous days to sync	Number of days, determining when emails are sync'd back
Device Identifier	Ein String der die EAS DeviceID enthält. Dies ist Teil des EAS Protokols und wird in einigen Umgebungen benötigt
Use Secure Sockets Layer (SSL)	Use a SSL connection
Accept all certificates	All certificates are accepted. Please select this option, if your Exchange Server uses a self-signed certificate

App Management

Enterprise App Manager

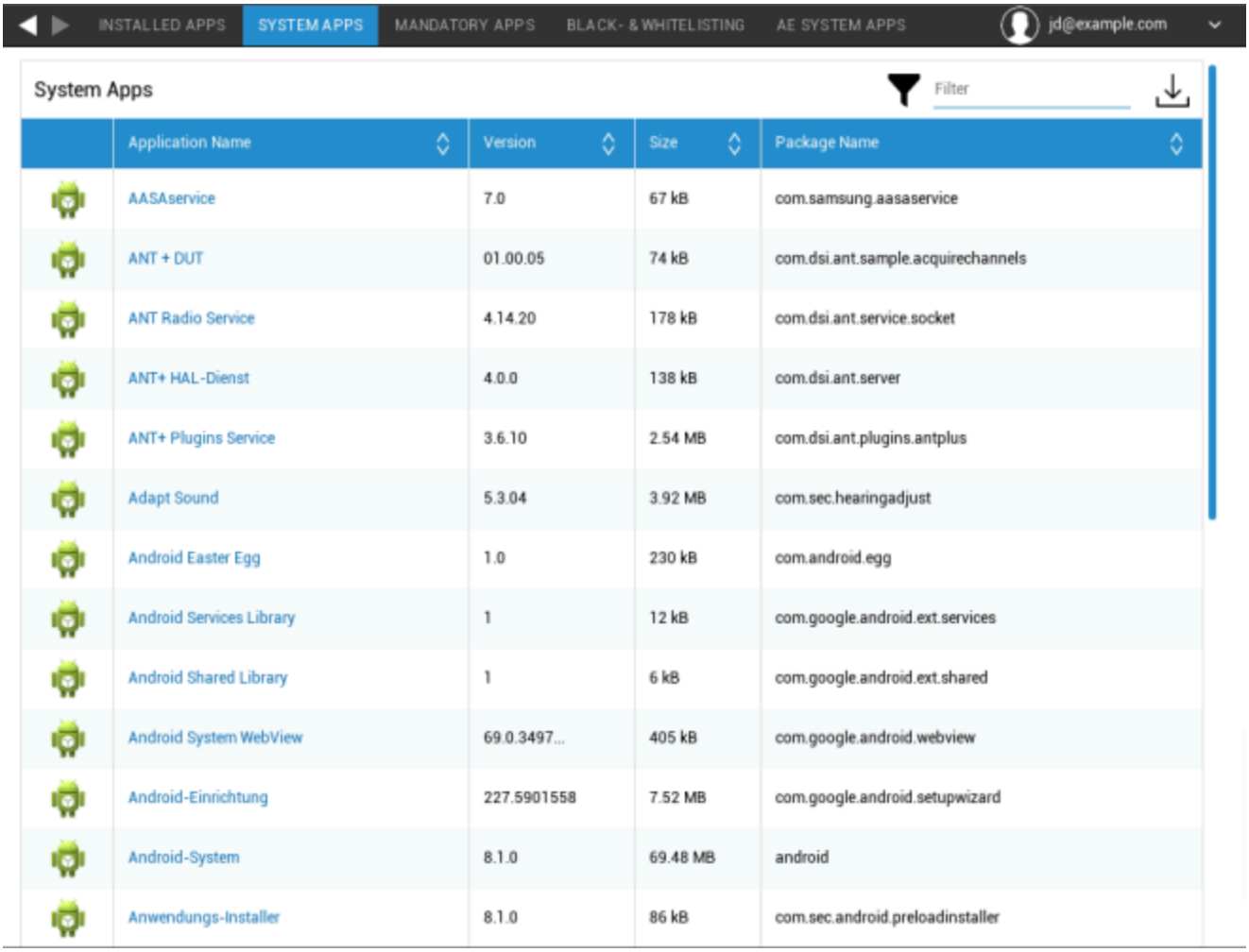
Installed Apps (only on device level)

Here all Apps that are currently installed on the end user device will be displayed for you.



System Apps (only on device level)

Under the “System Apps“, all of the apps and services that have already been installed on the end user device by your device manufacturer will be listed for you.

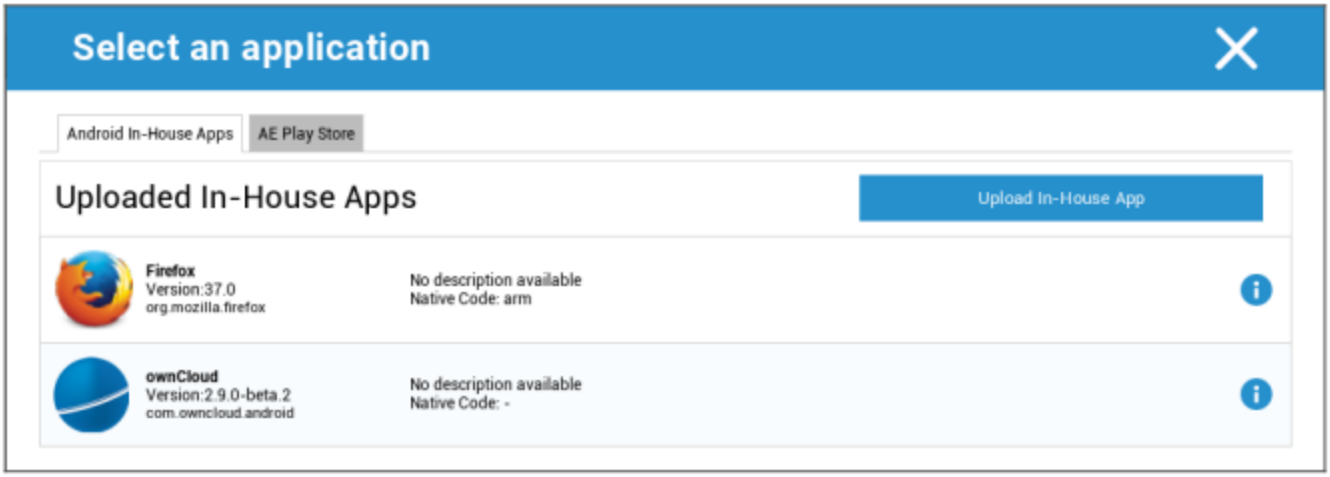


Mandatory Apps

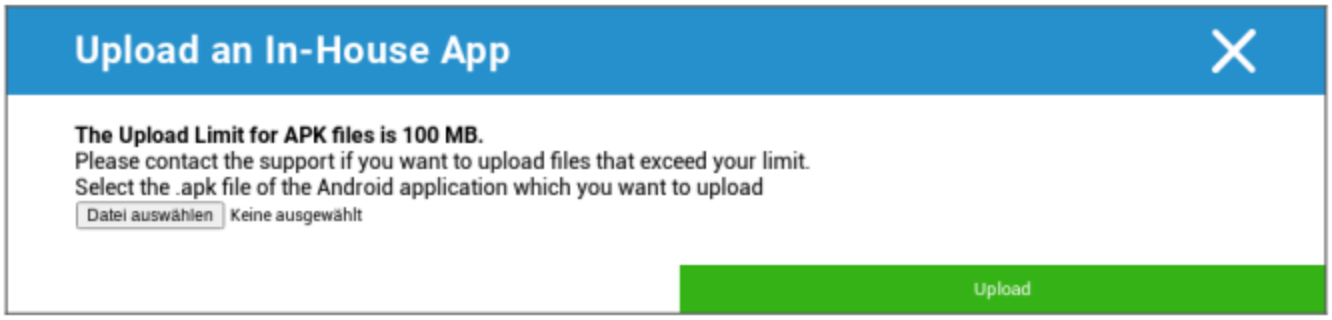
Under the Mandatory Apps, you can establish the mandated required apps. The user will continually prompted to install this designated app.

Via the , the mandated required app can be defined.

This can be an In-House App from the “Android In-House Apps“, which you have uploaded in General Settings.

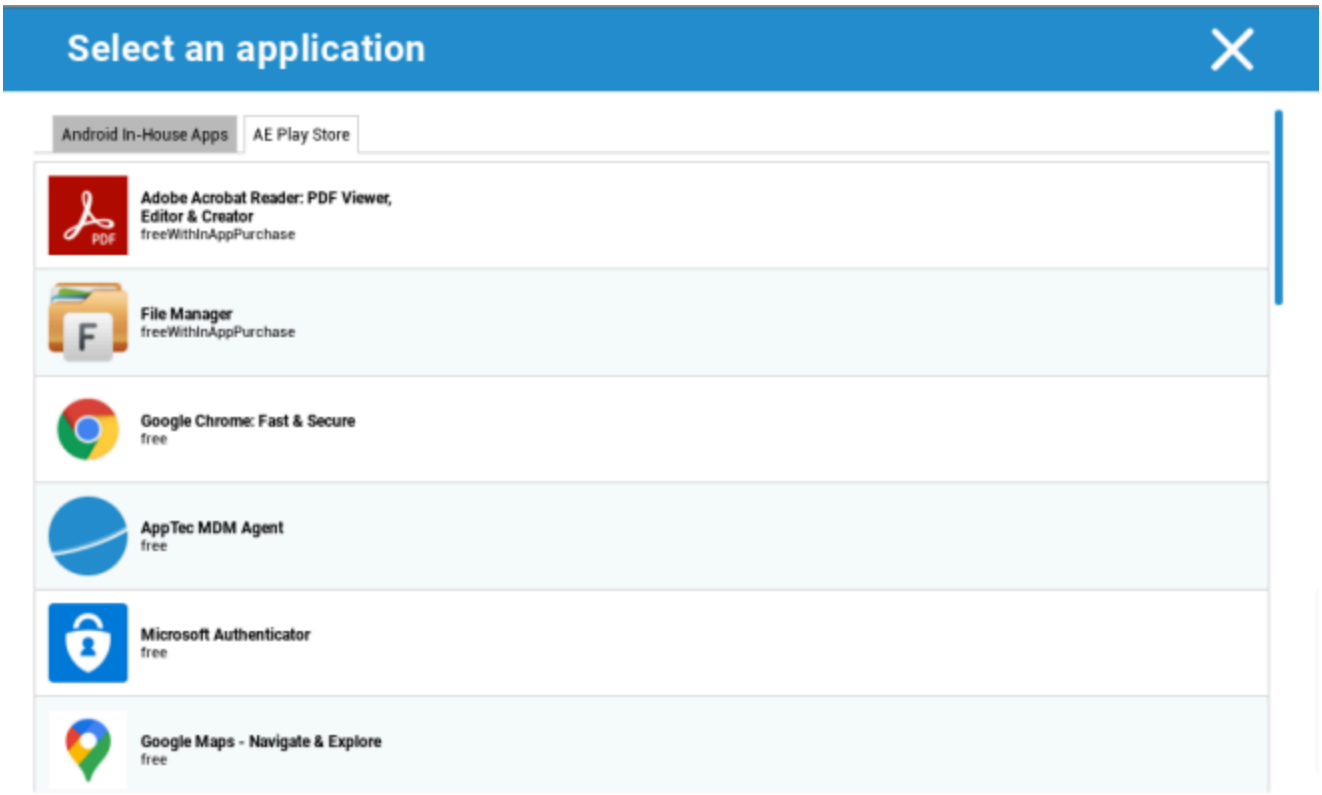


You can also directly select and upload an apk file with “Upload In-House App“.



If you are installing an In-House App, you will have the possibility to activate „Keep up to date“. If this is activated and you have defined a newer version in the In-House App DB, the app will be updated on the device.

Or it can be a “AE Play Store“ App from the Google Work Play Store.



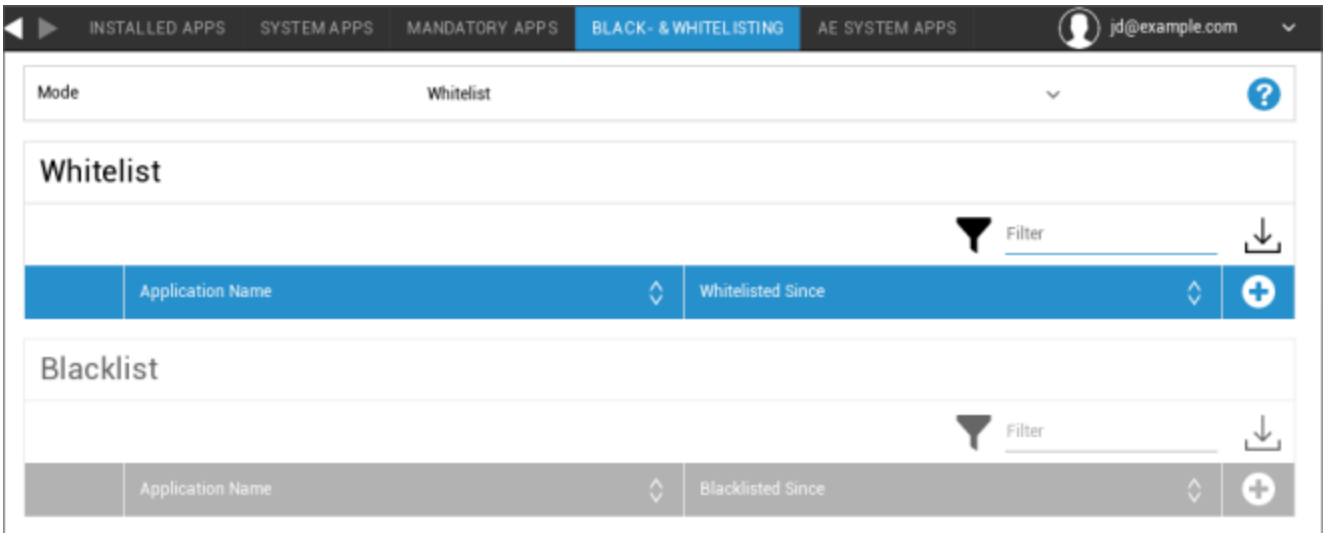
Only approved “AE Play Store Apps” will be shown in this tab.

To approve an “AE Play Store App” please go to “General Settings” > “App Management” > “AE Play Store” and add an app via the button which will redirect you to the “Play Store Apps” tab (or you can directly go to the “Play Store Apps” tab).

In the “Play Store Apps” tab you can search for apps. When you click on an app, the app page opens and here you can approve the app by clicking on "Approve".

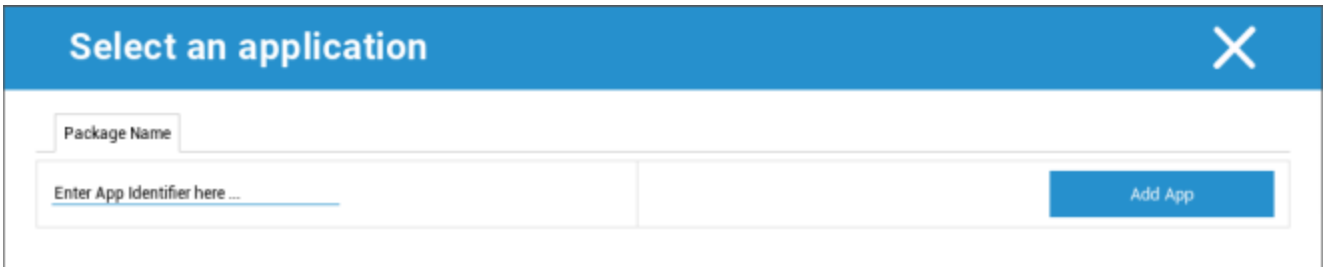
Black- & Whitelisting

Under “Black- & Whitelisting“, you can choose between the Mode “Whitelist“ and the Mode “Blacklist“.



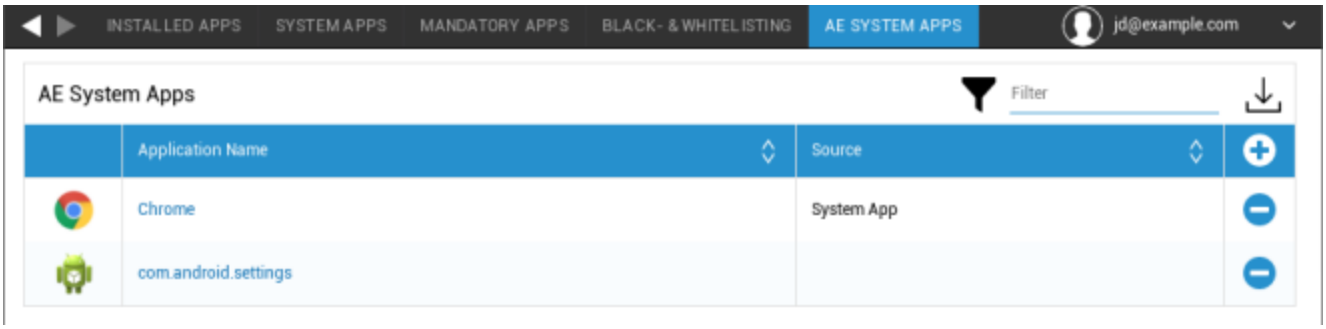
Whitelist	Only apps and services, that are added to the list can be installed on the end user device. If these are already pre-installed on the end user device they will be activated and set, so that the user can run them.
	All other apps that are not added to the list cannot be installed on the end user device. If these are already pre-installed on the end user device they will be deactivated and set, so that the user cannot run them.
Blacklist	Apps and services, that are added to the list cannot be installed on the end user device. If these are already pre-installed on the end user device they will be deactivated and set, so that the user cannot run them.
	All other apps that are not added to the list can be installed on the end user device. If these are already pre-installed on the end user device they will be activated and set, so that the user can run them.

Via the , you add additional apps or services to the currently used list.
Via the , you add additional apps or services to the currently inactive list.
You can define a “Packagename“:

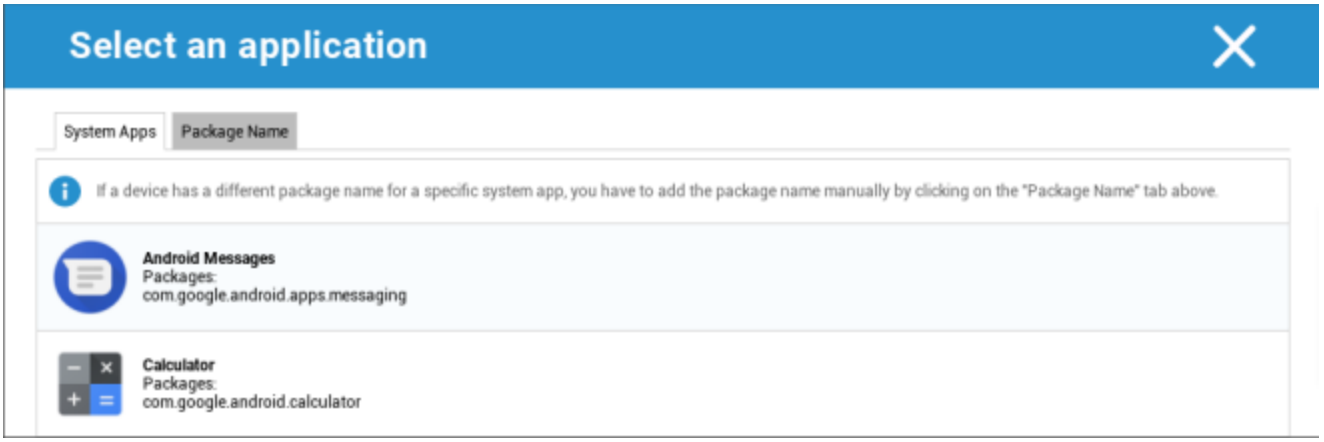

Select an application
Package Name
Enter App Identifier here ...
Add App

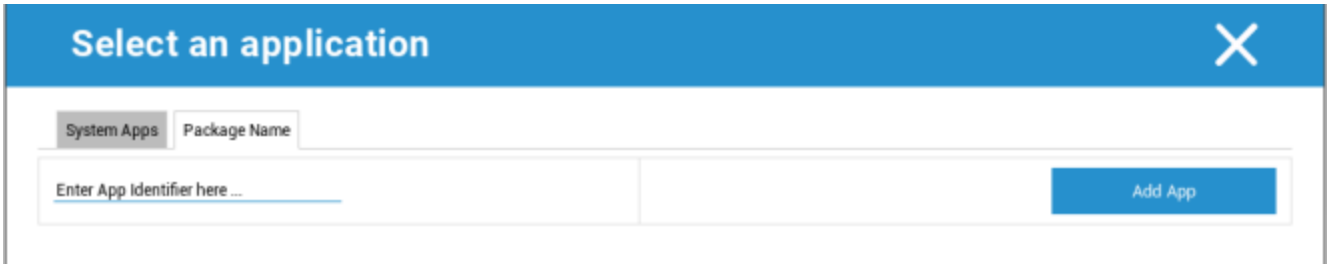
AE System Apps

Here you can define a list that contains specific system apps that should be activated on the devices.



If you click on the button, you can choose from a list of possible system apps provided by Google or directly enter the package name of a system app that should be activated.





Please keep in mind that the system apps in the list provided by Google are only apps that can be system apps, but do not necessarily have to be system apps on your devices.

However, this list only affects apps that are already pre-installed.

Adding apps that are not pre-installed on your devices will not affect your devices, regardless of whether the app is from the list provided by Google or the app's package name is entered directly.

Restrictions & Settings

App Management Settings

Here you can configure the device's behaviour regarding app updates.

Update Check Frequency	Specify in which interval the AppTec360 Client will search for app updates. The default value is 24 hours.
Wi-Fi Threshold	Apps that are bigger than the specified size will be downloaded over Wi-Fi. If "Wi-Fi only" is selected, all apps will be downloaded via Wi-Fi.

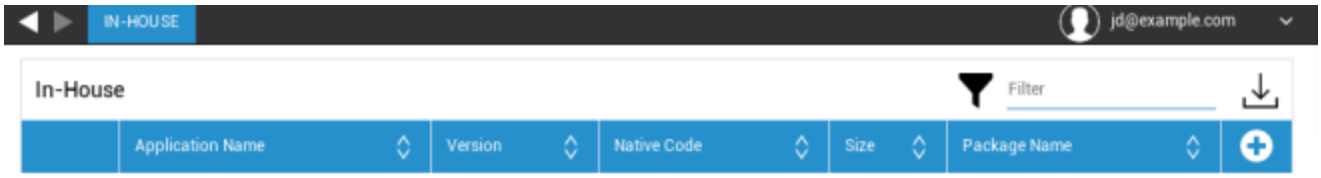
Enterprise App Store

In-House

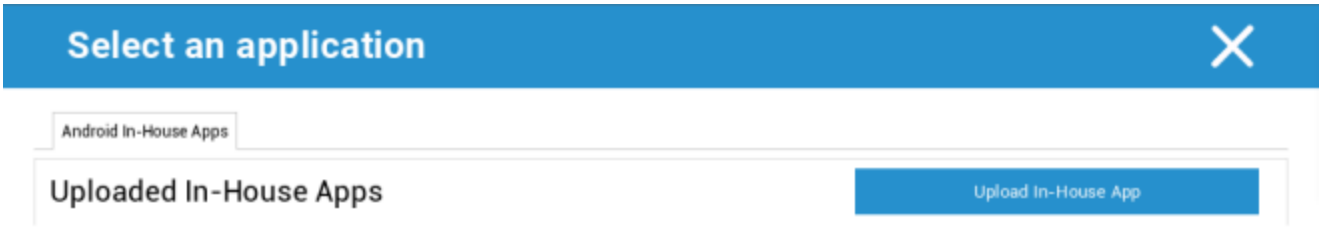
Under the point “In-House“, you can upload and distribute internally developed apps.

With the symbol, you can distribute additional In-House Apps.

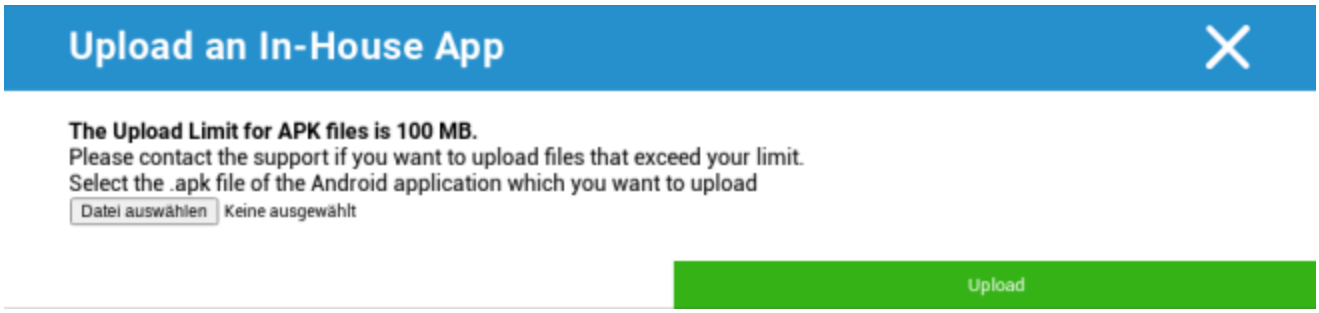
If you are installing an In-House App, you will have the possibility to activate „Keep up to date“. If this is activated and you have defined a newer version in the In-House App DB, the app will be updated on the device.



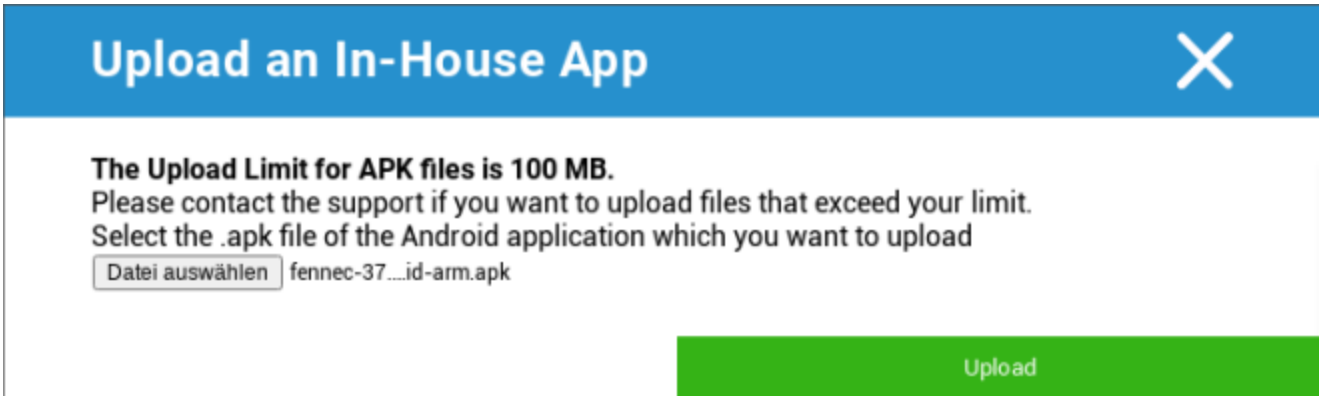
Should you not have distributed In-House Apps, you will then receive the following overview:



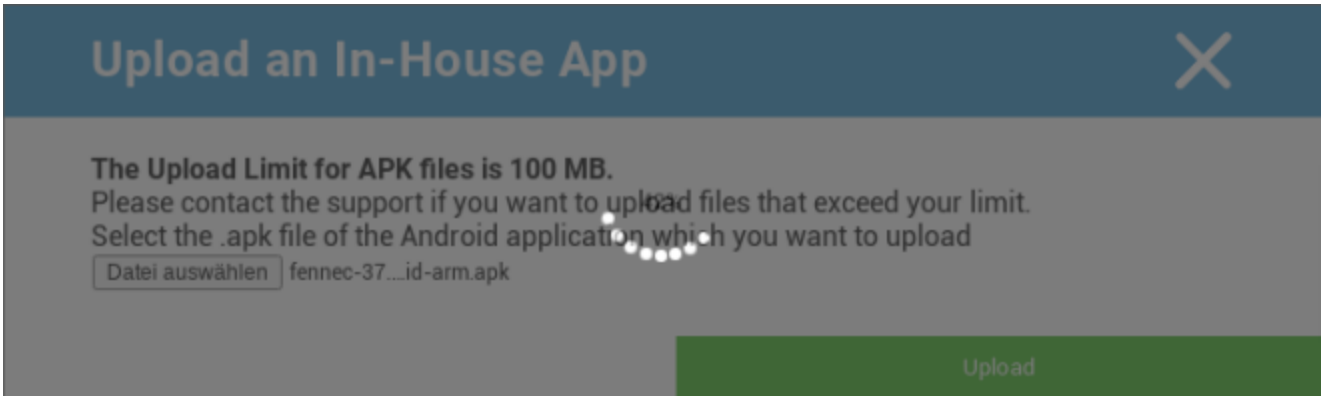
For this, click on “Upload In-House App”, you will then receive the following overview:



Now, choose with “Search…“an .apk file and then click on “Upload“.



Your app will now be uploaded, in the middle of the circle you will see a percentage indicator, showing how much of your app has already been uploaded.



Should the upload of your In-House App have been successful, you can then find the uploaded app in your App Catalog.

The user now has the option to see and install this app in the AppTec360 Store on the end user device, under the category “In-House“.

Due to the fact that this not involve a Google PlayStore App, the user does not need a stored Google ID on their respective end user device.

Enterprise Play Store

AE Play Store

Here you can add Apps to the Android Enterprise Playstore. Please note that you have to approve Apps with your AE Administrator Account before you can add them.

For approving an app please see the instructions in Mandatory Apps.

Kiosk Mode & Launcher

Kiosk Mode

The Kiosk Mode allows you to pre-define an app or an URL. Then it will be exclusively possible to run/visit this app and or URL.

Likewise, various hardware buttons can be deactivated in the Kiosk Mode diverse.

Automatic Start	Automatically starts the Kiosk Mode, as soon as the profile reaches the end user device
Scheduled Kiosk Mode?	You can plan a time for the Kiosk Mode, this will then start and end automatically, at a time set by you
Start Time	Start time
Time in minutes	Time in minutes, after which the Kiosk Mode should end again

Application Type

Single App	If you want to start the App in the Kiosk Mode, select Package" under "Application Type"
Kiosk Application	Click here, in order to select an app that should be started in Kiosk Mode You will find the usual App Management's overview You can select between a "Google Play Store", "Android In-House Apps" and a "Packagename"

Application Type

URL	If you want to launch a URL in the Kiosk Mode, select "URL" under "Application Type" Then define your desired URL address
Clear browser after inactivity	Here you can define a time interval in minutes, after which the Kiosk Mode should be relaunched
Clear Web Cache and Cookies	If you activate this function, then after a restart of the Kiosk Mode, the Web Cache (cookies and cached pictures) will be erased
Same Origin Policy	Should this function be active, then the user can only surf the subpages of a defined URL For example, you defined the following URL:www.mypage.com Then, the user can surf on: www.mypage.com/subpage
Whitelisted URLs	Here you can maintain a Whitelist, all these URLs are allowed Maximum 1 URL per line A URL must start with http:/ or https://
Blacklisted URLs	Here you can maintain a Blacklist, all these URLs are not allowed Maximum 1 URL per line A URL must start with http:/ or https://
Screen Orientation	This setting relates to the screen adjustments Automatic = automatic Portrait = vertical format Landscape = landscape mode

Multi App	If you select the "Multi App" Kiosk Mode, the use of the AppTec360 Launcher will be enforced.
Apps	Application: Select a Playstore or an In-House App as Kiosk Application. It's also possible to enter a packagename. The selected Kiosk Application must be installed on the device. Remember to set the Kiosk Application as mandatory. Shortcut on Homescreen: If set to "On" a shortcut on the homescreen will be created. If set to "Off" the App will still show up in the App List.

Exit Password Enabled	If you activate this function, then it is possible for the user, to end the Kiosk Mode, with a password that has been predefined by you
Exit Password	This is the password, that was predefined by you
Auto Collapse Status Bar	If enabled, the Status Bar will automatically be collpased. With that option users can see the information at the Status Bar, but can't access it's functions
Disable Status Bar	The Status Bar contains Notifications, Shortcuts and Information. Only available for Samsung devices with SAFE 4.0 or greater.
Disable Volume Keys	Disable volume keys (only available on Samsung devices with SAFE 3.0 or higher)
Disable On / Off Switch	Disable On / Off switch (only available on Samsung devices with SAFE 3.0 or higher)
Disable Home Button	Disable Home button. If this function has been activated, then the Kiosk Mode can only be terminated in the AppTec360 Console (only available on Samsung devices with SAFE 3.0 or higher)
Disable Navigation Bar	With this you can disable the Navigation Bar (Back / Menu) If this function has been activated, then the Kiosk Mode can only be terminated in the AppTec360 Console (only available on Samsung devices with SAFE 3.0 or higher)

AppTec360 Launcher

Enable AppTec360 Launcher	On: Enables the AppTec360 Launcher. The User has to set it as default Launcher one time. Note: If the Kiosk Mode is enabled, and the Kiosk Mode is set to "Multi App", the usage of AppTec360 launcher will be enforced.
Large Icons	On: Shows a larger Version of the App Icons in the Launcher
Hide AppTec360 App Icon	On: Hides the AppTec360 App completely
Hide AppTec360 Store Icon	On: Hides the AppTec360 Enterprise AppStore completely

AppTec360 Settings

Enable AppTec360 Settings App	The AppTec360 Settings App provides control over WiFi and Bluetooth connections
Enable Settings in Multi App Kiosk Mode	If enabled, users can access the AppTec360 Settings App while the Multi App Kiosk Mode is active

Remote Control

Splashtop

To start a remote control session for your device, the App "Splashtop Streamer" needs to be installed on the device by adding the App to **App Management → Enterprise App Manager → Mandatory Apps**.

Afterwards, configure the following settings for Splashtop:

Enable Splashtop	If enabled, AppTec360 will configure the Splashtop app to allow remote control
Deploy Code	Go to https://my.splashtop.com and login into your Splashtop account. Click on "Add Computer" and copy the 12 digit deploy code from the resulting page.
Set Custom Deploy Gateway?	Deploy Gateway
Deploy Gateway Domain / Host	Deploy Gateway
Certificate Verfication	Certificate Verfication

Then you can use the option Splashtop Remote Control the context menu (gear next to the search bar, when the device is selected or right click on the device in the tree) to start the remote control session.

TeamViewer

To start a remote control session for your device, the App "TeamViewer QuickSupport" needs to be installed on the device by adding the App to **App Management → Enterprise App Manager → Mandatory Apps**.

Then you can use the option **TeamViewer Remote Control** the context menu (gear next to the search bar, when the device is selected or right click on the device in the tree) to start the remote control session.

Content Management

ContentBox

Here you can activate the ContentBox.

As soon as you switch “Enable ContentBox“ to “On“, a separate ContentBox App will be installed automatically on the end user device.

Secure Browser

Here you can configure settings for the AppTec360 Secure Browser.

As soon as you switch the section in “Secure Browser“ to “On“, a separate Browser App will be installed automatically on the end user device.

Require Password	Require the user to set up and use a password to access the browser.
Minimal required password length	Set the required number of characters for the password
Required Password Quality	Set the required password quality
Restrict Downloads / Open In	
Restrict Uploads	
Upload Whitelist	A list of URLs for which uploading will always be allowed.
Allow Copy	Allow copying, cutting or sharing text inside the web pages.
Allow Screen Capture	Allow capturing screenshots.
Data cleanup frequency	Select with which frequency, ALL the user data (history, cache etc.) should be automatically removed.
Company Bookmarks	The Bookmarks will show up in the "Company bookmarks" folder in the browsers bookmarks. They are not editable by the user.
Hide Address Bar	
In-Browser Whitelisting (without Universal Gateway)	Enables client-side URL whitelisting. • Company Bookmarks are always whitelisted • Supported for 100 URLs only • Please use the Universal Gateway for unlimited Black- and Whitelisting
Whitelisted URLs	A list of allowed URLs.
Gateway based Black- and Whitelisting	Blacklisting has the following requirements: • A working AppTec360 Universal Gateway ("General Settings" → "Universal Gateway")

	• A working VPN configuration with a specified DNS server ("General Settings" → "Universal Gateway" → "VPN Settings") • A Blacklist configuraton ("General Settings" → "Universal Gateway" → "Domain Blacklist") • A valid VPN connection in the profile ("Connection Management" → "VPN")

Additional API

Samsung KNOX

Restrictions

Allow SD Card	
Allow SD Card Write	
Allow Screen Capture	
Allow Clipboard	
Backup settings and app data in Google Cloud	
Restore settings from Google Cloud when reinstalling an app	
Allow USB Debugging	
Allow Google Crash Report	
Allow Factory Reset	
Allow OTA Upgrade	
Allow USB host storage	If enabled, a user can connect any pen drive (portable USB storage), external HD, or Secure Digital (SD) card reader, and it is mounted as a storage drive on the device.
Allow USB Media Player (MTP,PTP)	
Allow Microphone	Disables the microphone for third-party applications
Allow NFC (Near Field Communication)	
Allow Unknown Sources (APK Sideloading)	If enabled the side-loading of Apps (APK files) is allowed. Once this setting is disabled, the user has to enable it manually when you reallow the installation of APKs from unknown sources.
Allow User Creation	If enabled, user are allowed to create multiple accounts on the device, e.g. Guest Accounts

Email

eMail Address	
Incoming server protocol	
Incoming server address	
Incoming server port	
Incoming server login/username	
Incoming server password	
Incoming server uses SSL	
Incoming server uses TLS	
Incoming server accept all certificates	
Outgoing server protocol	
Outgoing server address	
Outgoing server port	
Outgoing Server uses extra credentials	If disabled, the system uses the incoming credentials for the outgoing server too.
Outgoing server login/username	
Outgoing Server Password	
Outgoing server uses SSL	
Outgoing server uses TLS	
Outgoing server accept all certificates	
Set Signature	
Signature	Note: For some devices the signature has to be specified in HTML format.
Notify user on receiving new eMail	

Exchange

eMail Address	
Server Hostname	The hostname of the Exchange Server
Login Name	The username which is used to login to the Exchange Server
Domain	If an ACL Gateway Configuration is enabled and the Domain field is not empty, the AppTec360 Universal Gateway will authenticate the device with the following name "Domain\Login Name
Password	
Number of previous days to sync	
Frequency to sync eMail	
Sync while Roaming	
Set Signature	
Signature	Note: For some devices the signature has to be specified in HTML format.
Default account	
Use Secure Sockets Layer (SSL)	
Use Transport Layer Security (TLS)	
Accept all certificates	

APN

APN Display Name	
Access Point Name	Name of the APN
Outgoing server protocol	
MCC - Mobile Country Code	Leave empty to use mmc of installed SIM
MNC - Mobile Network Code	Leave empty to use mnc of installed SIM
Server Address	
Server port number	
Server proxy address	
MMS server address	Leave empty for default
MMS port number	Leave empty for default
MMS proxy address	Leave empty for default
Username	
Password	
Access Point Type	Accepted types are "default", "mms", "supl".
	If null or empty is passed, by default "default,supl,mms" is used.
	Leave empty for default.
Preferred APN	

Bluetooth

Allow Device discovery via Bluetooth	
Allow Bluetooth Pairing	
Allow Bluetooth Headset devices	
Allow Bluetooth Hands-free devices	
Allow Bluetooth A2DP devices	A2DP, Advanced Audio Distribution Profile allows audio streaming between devices
Allow Outgoing Calls	
Allow Data Transfer via Bluetooth	
Allow Bluetooth Tethering	
Allow connection to Computer via Bluetooth	

Connection

Allow Emergency Calls OnlyAllow Wi-Fi	
Wi-Fi Network Minimum Security Level	
Forbid user to add Wi-Fi networks	This restriction can only be activated if at least one active Wi-Fi Profile is defined under Connection Management
Allow SMS & MMS	
Allow Sync during Roaming	
Allow Voice Roaming	

Android Enterprise – Fully Managed Device with-Work Profile (COPE)

General Explanation of COPE

COPE is an abbreviation for **C**orporate **O**wned **P**ersonally **E**nabled.

The COPE mode allows an Android device to be enrolled as an **Android Enterprise – Fully Managed Device** with integrated **Android Enterprise – Container** profile.

This can either be an Android device that is already enrolled as an **Android Enterprise – Fully Managed Device** and on which the **Android Enterprise – Container** is additionally set up, or a newly enrolled Android device that is directly enrolled as an **Android Enterprise – Fully Managed Device** together with the **Android Enterprise – Container** on top of it.

The COPE mode is available for devices with Android 8, 9 and 10 only

Configuration of Profiles for COPE Devices

Since there is no Configuration profile for COPE mode itself, the configuration of **Android Enterprise - Fully Managed Device** and **Android Enterprise - Container** is separated into two profiles within the COPE profile. It is possible to switch between the two profiles for the configuration of each profile by clicking on the respective button on the left hand side of the console:

Both profiles can be configured as described for each individual profile:

Android Enterprise – Fully Managed Device

Android Enterprise – Container

Reverting to AE Fully Managed Device

The **Android Enterprise – Container** profile can be removed as described in **Mobile Management**.

By removing the Container profile, the COPE profile will be transformed to an **Android Enterprise – Fully Managed Device** profile.

Android Enterprise – Container Configuration

Depending on if you have currently selected a group profile or a device, the overview and its sub points differ – please consider this carefully!

General

Profile Overview (only on profile level)

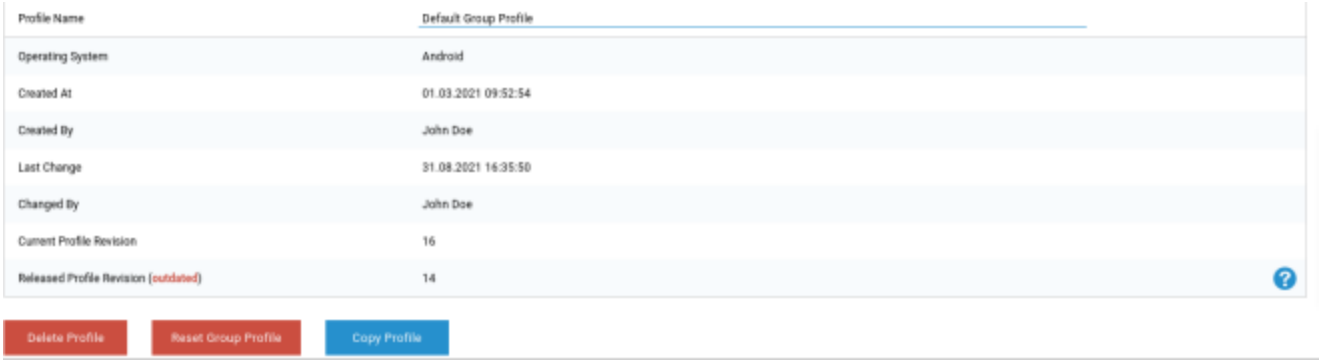
Should you be in a profile, you will receive a brief overview of the profile, in regards to name, OS, creation date, author, etc.

Profile Name	Profile name – can be directly renamed here
Operating System	Valid OS for the profile
Created At	Creation date
Created By	Created by
Last Change	Last change date
Changed By	The User that performed the last changes to this profile
Current Profile Revision	Number of times the profile has already been updated
Released Profile Revision	Number of times the profile has already been updated and has been assigned devices

Delete Profile	Delete Profile
Reset Group Profile	Reset Group Profile
Copy Profile	Copy Profile

Group profile overview (only on group level)

When opening a group profile, you will get a quick overview of the profile.



Profile Name	Name of the profile (can be changed here)
Operating System	Operating System the profile is for
Created At	Time of creation
Created By	The profile's creator
Last Change	Time of last change to the profile
Changed By	Account that made the last changes
Current Profile Revision	Revision of saved profile state
Released Profile Revision	Assigned profile revision ("Assign now"). If the label shows "(outdated)" behind the text, it means you've saved the profile but did not assign it yet, so the devices will still get and older version.

Device Overview (only on device level)

Should you be on a device, you will receive an overview recap of the selected device, the following is contained here:

Device Name	Device name
Location	Location coordinates
Phone Number	Phone number
Assigned Mandatory Apps	Number of assigned Mandatory Apps
OS Version	OS version of the device
Operating System	Operating System (Android Enterprise)
Serial Number	Device serial number
Device Ownership	Corporate or private device
Device Type	AE Work Managed Device
Rooted	Status, indicating if the device has been rooted
Compliant	Guideline compliant
IP Address	IP Address of the device
Last Seen	Point in time, when the device last connected to AppTec
Last Push	Point in time, when the last push was sent to the device
User Assignment	The user or group this device is assigned to

Config Revision

Here you receive an overview of which group profile is assigned to the device.

If you click on the group profile, you will gain direct access to this profile and you can perform settings.

With this symbol, you can revert the distributed apps to the group profile's settings.

With this symbol, you can revert all of the used apps to the group profile's settings.

“Newer Revision available“ indicates that the group profile has been changed and saved but not assigned. The group profile has to be assigned with “Assign now” on group level to apply the changes

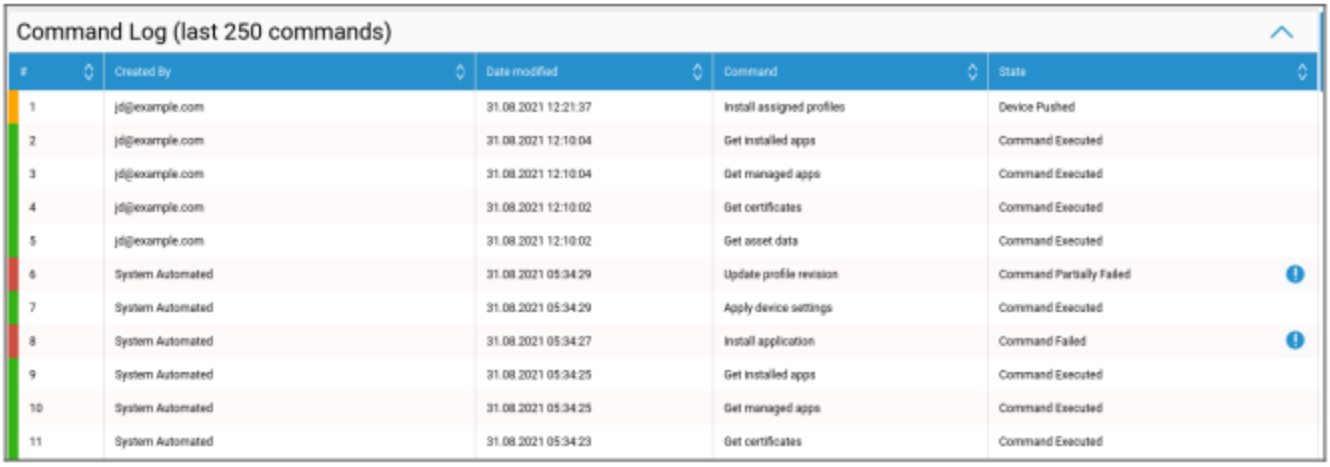
to the devices.

Device Log (only on device level)

Here you will receive various device logs. If needed, you can directly find out the cause of an error here.

Command Log

Here you can see which commands where issued for the device and what their status is.



Possible command statuses

Device Pushed	A push request has been sent to the push service (e.g APNS) to tell the device to connect back to the EMM server.
Command Created	The command was created in the system.
Command Sent	The command got sent to the device after it connected to the server.
Command Executed	The command was successfully executed.
Command Failed	The command failed. *
Command Partially Failed	Depending on the device OS some commands may get grouped together. In this some parts of this command group failed. *
Command Executed, eventually Failed	The command was executed but maybe it wasn't.
Command Repushed	The command was repushed by a user.
Discarded	The command was discarded. For example because it was superseded by another command or the device got re-enrolled and old commands got removed

*If there is an exclamation mark behind the message, you can get more information by hovering over the icon with your cursor.

Device Settings

Client Configuration

Here you can perform the following configurations on your Android device:

Out of Compliance Time	The user response timeout limit after which the enforcement action is applied.
Enforcement action after compliance timeout	Enforcement action when a user doesn't perform actions that leads to a compliant device status
Data Collection Frequency	Frequency with which device/GPS-information is to be collected
Device Heartbeat Frequency	Interval in which the device should contact the AppTec Server Min. 1 minute Max. 24 hours
Enable Location Updates	If activated, the device sends location updates to the AppTec Server
Location Update Time	Determines in what time intervals the device sends location updates to AppTec
Use Google Location Accuracy for Location Update	If activated, the network location will be used for location updates (if this was deactivated under "Restrictions", then this setting will not affect anything)
Use GPS Location for Location Update	If activated, the GPS will be used for location updates
Allow Mock (Fake) Locations	Allows the forging of location information via third party apps
Lost Connection Action	If enabled, you can specify an action for the case that a device doesn't get a connection to the MDM server in the heartbeat interval. For example, if the device has a heartbeat time of 5 minutes, it connects to the server at 10:35 AM. After that the device leaves the Wi-Fi range. The next heartbeat at 10:40 AM will fail, and the specified action will be executed.
Action	The action that is to be taken, as soon as a device becomes non-compliant. • Lock Device = lock device • Wipe Device = device will be restored to factory settings

	• Wipe Device & SD Card = device will be restored to factory settings and SD Card storage will be deleted
Threshold	You can specify a threshold of failed Heartbeats which are necessary to trigger the specified action.

Policy Enforcement Mode	Default:	Users will be prompted periodically to execute outstanding actions
	Lazy Policy Enforcement:	Users will never be prompted to execute outstanding actions. All open action will be shown in the AppTec Client
	Aggressive Policy Enforcement:	Users will be prompted non stop to execute outstanding actions
AppTec Version Lock	If enabled, a version code for the AppTec app can be specified. The AppTec client will only update to the specified version. Newer versions will be ignored. A downgrade is NOT possible.	
Version Code	Version code for the AppTec app to be locked on to.	
Disable AppTec Notification	If disabled the AppTec Client won't show a Notification in the Notification Bar. Thus users can close the AppTec client via the task manager. If the AppTec client is closed, several features including Kiosk Mode and App Black/Whitelisting will not work properly. Samsung devices offer a protection mechanism for the AppTec Client. The notification is disabled by default on Samsung devices that support the KNOX APIs. The notification shouldn't be disabled devices with Android 8.0 or higher.	

Wallpaper

Set custom Wallpaper	Enable/Disable the custom wallpaper
Wallpaper	Set the wallpaper mode to use a color code or an image
Specify a Color	Specify a background color as hex value, e.g. #000000 for black or #ffffff as white
Set Image as Wallpaper	Upload the image file you want to use as wallpaper

Asset Management (only on device level)

Device Info

Model	Device model designation
Operating System	OS
OS Version	OS version
Serial Number	Serial number
Device Name	Device name
Battery Status	Battery status
Free / Total Memory	Free / Total memory
Samsung Safe	Samsung SAFE interface, required for a variety of setting options
SD Card Available	SD Card available
SD Card Emulated	SD Card emulated
SD Card Removable	SD Card removable
SD Free / Total Memory	SD Free / Total SD Card memory

Wi-Fi

IP Address	Device IP address
WiFi MAC	WiFi MAC address

Cellular

Status	Status (SIM card installed)
Phone Number	Phone Number
Roaming (Voice / Data)	Roaming for voice / data
Roaming Status	Current roaming status
IP Address	IP address
Operator/Carrier	Operator/Carrier
Cellular Technology	Cellular Technology
IMEI	IMEI number
ICCID	This is the ID for the SIM card, often times also a Smartcard or Integrated Circuit Card (ICC)
IMSI	The International Mobile Subscriber Identity (IMSI) provides in GSM- and UMTS-mobile networks a definite identification of the network users The IMSI is comprised of a maximum of 15 digits and is configured in the following manner: • Mobile Country Code (MCC), 3 digits • Mobile Network Code (MNC), 2 or 3 digits • Mobile Subscriber Identification Number (MSIN), 1-10 digits
Current MCC/MNC	See "SIM MCC/MNC"
SIM MCC/MNC	The Mobile Country Code is an established country identifier, set by the ITU as per E.212 Standard. This works in conjunction with the Mobile Network Code (MNC) for the identification of the mobile network. Meaning the SIM card's country/Mobile Network Code. If you roam into another mobile network, then logically, the "Current MCC/MNC" and "SIM MCC/MNC", will be different.

Bluetooth

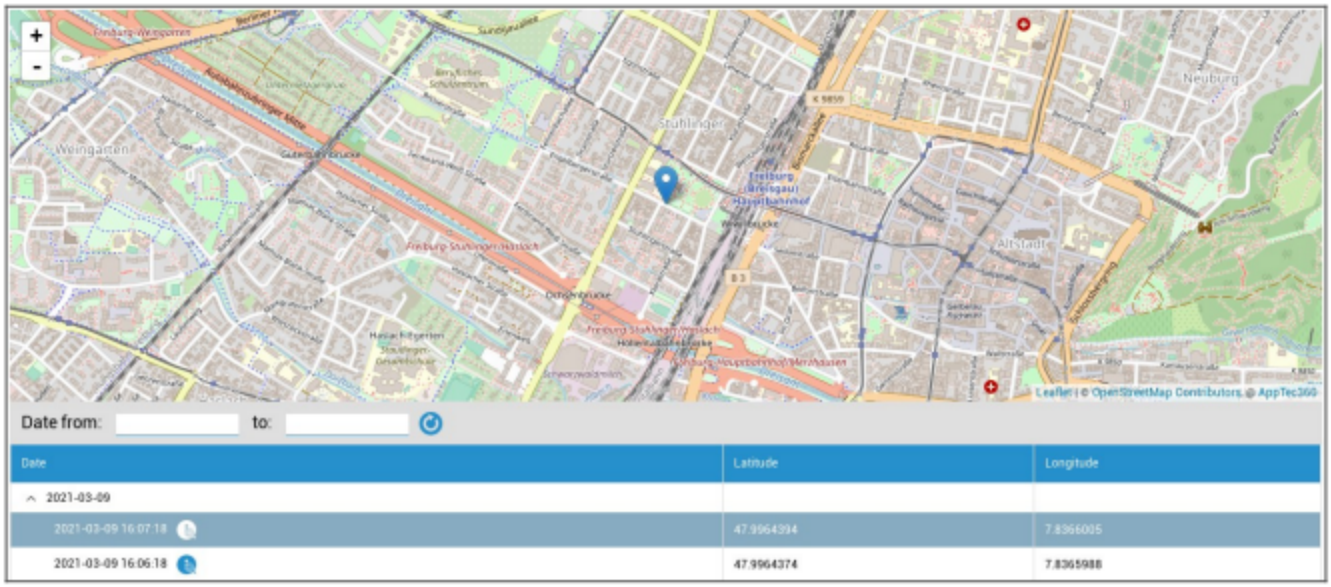
Bluetooth MAC	Bluetooth MAC address

Security Management

Anti Theft (only on device level)

GPS Information (only on device level)

Here you can establish the current/last device location. The localizing can be protected with one or even two passwords – See: General Settings – Privacy – GPS Access



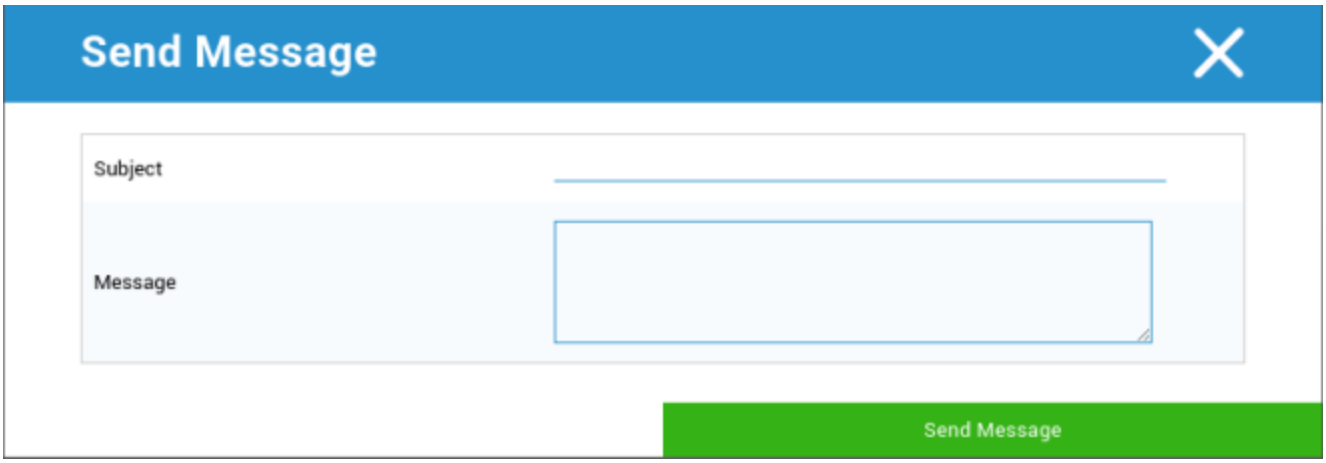
Wipe & Lock (only on device level)

Under „Wipe & Lock“, you can perform the following three actions:

Full Wipe	The device is restored back to its factory settings (corporate, as well as personal data is deleted). Only works for Enhanced Work Profile
Enterprise Wipe	Only corporate data is removed from the end user device (all apps, data, etc. that were provided by AppTec)
Lock Screen	Screen lock is activated, it is sufficient to unlock the device with the device-password/PIN

Message (only on device level)

Here you can fill in the subject and a message and send it to an end user device



Security Configuration

Device Passcode

Under “Passcode“ you can mandate a device password, the following setting options are available to you

Minimum password length	Establishes, the minimum number of symbols a password must have	
Password quality	Unspecified	This policy has no requirements for the password.
	Biometric Weak	This policy allows for low-security biometric recognition technology. This implies technologies that can recognize the identity of an individual to about a 3 digit PIN (false detection is less than 1 in 1,000).
	Something	This policy requires some kind of password or pattern to be set, but doesn't enforce any specific rules.
	Alphabetic	The user must have entered a password containing at least alphabetic (or other symbol) characters.
	Alphanumeric	The user must have entered a password containing at least both, numeric and alphabetic (or other symbol) characters.
	Complex	The user must have entered a password containing at least a letter, a numerical digit and a special symbol, by default. With this password quality, passwords can be restricted to contain various sets of characters, like at least an uppercase letter, etc.
Minimum password length	Set the required number of characters for the password. For example, you can require PIN or passwords to have at least six characters.	
Minimum numerical digits required in password	Minimum numerical digits required in password	
Minimum lowercase letters required in password	Minimum lowercase letters required in password	
Minimum uppercase letters required in password	Minimum uppercase letters required in password	

Minimum non-letter characters required in password	Minimum non-letter characters required in password
Minimum symbols required in password	Minimum symbols required in password

Maximum inactivity time lock	Maximum user inactivity until time lock
Password expiration timeout	Establishes, after which time interval the password expires and a new password must be issued
Password history restriction	Number of previously used password that are not allowed
Maximum failed password attempts	Establishes, how often a password can be entered incorrectly, before a complete device wipe will be performed
Allow Biometric Authentication	Enables authentication via fingerprint or iris scan. Only for Samsung KNOX 2.1 and higher

Container Passcode

Under “Passcode“ you can mandate a container password, the following setting options are available to you

Minimum password length	Establishes, the minimum number of symbols a password must have	
Password quality	Unspecified	This policy has no requirements for the password.
	Biometric Weak	This policy allows for low-security biometric recognition technology. This implies technologies that can recognize the identity of an individual to about a 3 digit PIN (false detection is less than 1 in 1,000).
	Something	This policy requires some kind of password or pattern to be set, but doesn't enforce any specific rules.
	Alphabetic	The user must have entered a password containing at least alphabetic (or other symbol) characters.
	Alphanumeric	The user must have entered a password containing at least both, numeric and alphabetic (or other symbol) characters.
	Complex	The user must have entered a password containing at least a letter, a numerical digit and a special symbol, by default. With this password quality, passwords can be restricted to contain various sets of characters, like at least an uppercase letter, etc.
Minimum password length	Set the required number of characters for the password. For example, you can require PIN or passwords to have at least six characters.	
Minimum numerical digits required in password	Minimum numerical digits required in password	
Minimum lowercase letters required in password	Minimum lowercase letters required in password	
Minimum uppercase letters required in password	Minimum uppercase letters required in password	
Minimum non-letter characters required	Minimum non-letter characters required in password	

in password	
Minimum symbols required in password	Minimum symbols required in password

Maximum inactivity time lock	Maximum user inactivity until time lock
Password expiration timeout	Establishes, after which time interval the password expires and a new password must be issued
Password history restriction	Number of previously used password that are not allowed
Maximum failed password attempts	Establishes, how often a password can be entered incorrectly, before a complete device wipe will be performed

AntiVirus

Automatic Scan	Enable periodic automatic scans
Scan Interval	Interval for examination (Quick / Full)
Full Automatic Scan	Enable full automatic scans
Automatic Updates	Enable automatic updates
Update Check Interval	How often the app and its database should be updated (viruses / damaged code)
App Protection	Enable automatic app scan
SD Card Protection	Enable automatic SD Card scan
Wi-Fi Only Update	When enabled, updates will be applied only when the device is successfully connected to a Wi-Fi network

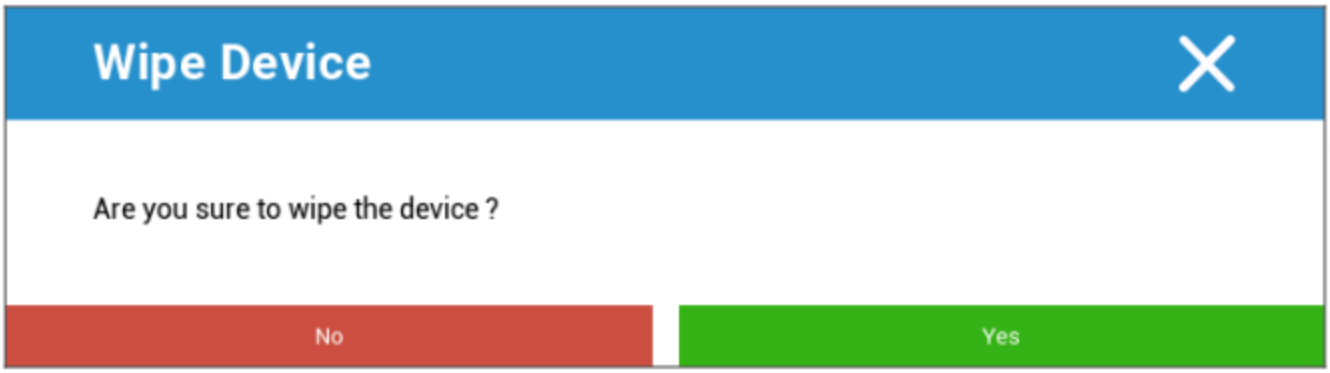
End of Life (only on device level)

Wipe (only on device level)

Under “Wipe“, you can restore the device to its factory settings (Only on Enhanced Work Profile).

Here the corporate, as well as the private data will be deleted on the end user device.

With a click on the “Minus Symbol“ you receive the following message:



With “Yes“ you can perform the wipe.

Under “Wipe Report“ the following items can be displayed

Wiped by	History of who performed the wipe
Date	Date
Status	Status (ex. if the Wipe was performed successfully)

Restriction Settings

Restrictions

Here, a variety of things can be restricted and blocked.

Compliance Enforcement	Mode Prompt User - User will be prompted to fulfill the necessary actions. Mode Lock-Down Container - Hide all apps until all requirements are fulfilled
Runtime Permission Policy	Prompt user for new permission requests Always grant new new permission requests Always deny new permission requests Warning: Some Apps have problems recognizing the permissions if these are set automatically. If you always grant permissions and encounter problems with apps saying that permissions are missing, set this to "prompt user" and re-install the app
Allow outgoing clipboard	Allows copy and pasting from inside the container to the outside
Allow Caller ID Resolution	Shows the name for an incoming call based on contacts in the container
Allow Contact Search Resolution	Allows to search for names in the container contacts when making calls
Allow Bluetooth Contact Sharing	Allows access to container contact in a car
Disallow Outgoing NFC Beam	Disables NFC for the Container
Allow Unknown Sources	If enabled, users can sideload Apps by installing an .apk file.
Allow USB Debugging	If enabled, users can enable USB Debugging.
Disallow Account Modification	Disallows the creation, deletion and modification to Accounts in the container Keep in mind that some apps need to create or modify accounts to work as expected

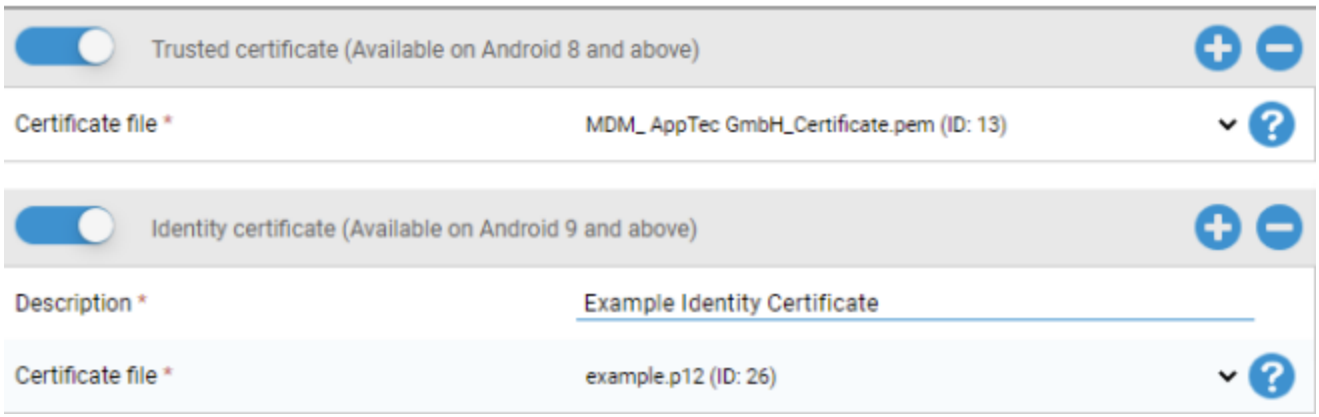
Work Profile Restrictions. Available only on Android 11 devices and higher, with Enhanced Work Profile

Disallow Camera	Specifies if the camera is disallowed in the work profile.
Disallow Bluetooth	Specifies if bluetooth is disallowed in the work profile.
Enable Factory Reset Protection	Activate this to override the Factory Reset Protection of Android to the Google Account you defined in "General Settings" → "Android Configuration" → "Android Enterprise" → "Factory Reset Protection" If this is enabled and you reset the device, you will have to provide the configured Google Account to setup the device again.
Control OS Update	Enable this to set the update behavior to automatic, windowed or postponed.
Update Policy	Automatic: Install automatically as soon as an update is available. Windowed: Install automatically within a daily maintenance window. This also configures Play apps to be updated within the window. This is strongly recommended for kiosk devices because this is the only way apps persistently pinned to the foreground can be updated by Play. Postpone: Postpone automatic install up to a maximum of 30 days.

Personal Profile Restrictions. Available only on Android 11 devices and higher, with Enhanced Work Profile	
Disallow Camera	Specifies if the camera is disallowed in the personal profile.
Disallow Bluetooth	Specifies if bluetooth is disallowed in the personal profile.
Allow Unknown Sources	If enabled, work profile users can sideload Apps by installing an .apk file.

Certificate Management

Here you can distribute Trusted Certificates and Identity Certificates to your devices. Android 8 or higher is required to distribute Trusted Certificates and Android 9 or higher is required to distribute Identity Certificates.



With the “+” you can add multiple certificates.

Trusted Certificates need to be in PEM format.

Identity Certificates need to be in PKCS12 format.

Connection Management

Wifi

For this setting, perform the pre-configuration of the end user devices, for access to internal Access Points

Services Set Identifier (SSID)	SSID for the network that is to be connected
Hidden Network	Activate, in case the AP does not broadcast the SSID

Security Type

Establish the AP's security type

WEP

Password	Password for the AP

WPA/WPA2

Password	Password for the AP

802.1x EAP

EAP-Method

PWD	Identity	Identity
	Password	Password

PEAP	Phase 2 Authentication Protocol	none	No additional protocol
		MSCHAPV2	MSCHAPV2 protocol
		GTC	GTC protocol
	CA Certificate	CA certificate	
	Identity	Identity	
	Anonymous Identity	Anonymous identity	
	Password	Password	

TTLS	Phase 2 Authentication Protocol	none	No additional protocol
		PAP	PAP protocol
		MSCHAP	MSCHAP protocol
		MSCHAPV2	MSCHAPV2 protocol
		GTC	GTC protocol
	CA Certificate	CA Certificate	
	Identity	Identity	
	Anonymous Identity	Anonymous Identity	
	Password	Password	

TLS	CA Certificate	CA certificate
	Identity	Identity
	Password	Password

VPN

Connection Name	Name of the VPN Connection

VPN Type

VPN

VPN Client

AppTec VPN Client	
Gateway Configuration	Select the Gateway VPN Configuration (See **General Settings > Universal Gateway > VPN Settings**)
Always On VPN	Enable Native Lockdown
Enable AppTec Lockdown	Enable AppTec Lockdown

Built In (Only available on Samsung devices)			
Connection Type	PPTP	Server	Server
		Enable PPTP Encryption	Enable PPTP Encryption
	L2TP / IPSec PSK	Server	Server
		IPSec Pre-Shared Key	IPSec Pre-Shared Key
		Enable L2TP Secret	Enable L2TP Secret
		L2TP Secret	L2TP Secret
	IPSec XAuth PSK	Server	Server
		IPSec Identifier	IPSec Identifier
		IPSec Pre-Shared Key	IPSec Pre-Shared Key
DNS Search Domains	DNS Search Domains		
Expert Settings	DNS Servers	DNS Servers	
	Forwarding Routes	Forwarding Routes	

Open VPN		
Server	Server	
OpenVPN Profile	OpenVPN Profile	
OpenVPN App	OpenVPN for Android (recommended)	
	OpenVPN Connect	
Expert Settings	DNS Servers	DNS Servers
	Forwarding Routes	Forwarding Routes

Samsung / Strong Swan			
Connection Type	PPTP	Server	Server
		Username	Username
		Password	Password
		Enable PPTP Encryption	Enable PPTP Encryption
	L2TP / IPSec PSK	Server	Server
		IPSec Pre-Shared Key	IPSec Pre-Shared Key
		Username	Username
		Password	Password
		Enable L2TP Secret	L2TP Secret
	IPSec XAuth PSK	Server	Server
		IPSec Identifier	IPSec Identifier
		IPSec Pre-Shared Key	IPSec Pre-Shared Key
		Username	Username
		Password	Password
Expert Settings	DNS Servers	DNS Servers	
	Forwarding Routes	Forwarding Routes	

Cisco Any Connect		
Server	Server	
Certificate Mode	Disabled	Disabled
	Automatic	Automatic
Expert Settings	DNS Servers	DNS Servers
	Forwarding Routes	Forwarding Routes

Per-App VPN

VPN Client

AppTec VPN Client		
Gateway Configuration	Select the Gateway VPN Configuration (See **General Settings > Universal Gateway > VPN Settings**)	
VPN Apps	VPN Apps	
Always On VPN	Enable Native Lockdown	Always On VPN
Enable AppTec Lockdown	Enable AppTec Lockdown	

Samsung / Strong Swan			
Connection Type	PPTP	Server	Server
		VPN Apps	VPN Apps
		Username	Username
		Password	Password
		Enable PPTP Encryption	Enable PPTP Encryption
	L2TP / IPSec PSK	Server	Server
		VPN Apps	VPN Apps
		IPSec Pre-Shared Key	IPSec Pre-Shared Key
		Username	Username
		Password	Password
		Enable L2TP Secret	L2TP Secret
	IPSec XAuth PSK	Server	Server
		VPN Apps	VPN Apps
		IPSec Identifier	IPSec Identifier
		IPSec Pre-Shared Key	IPSec Pre-Shared Key
		Username	Username
		Password	Password
Expert Settings	DNS Servers	DNS Servers	
	Forwarding Routes	Forwarding Routes	

Restrictions

Here you can set the restrictions, in relation to the connection management

Allow Data Roaming	Allow mobile data while roaming
Force Data Roaming	If activated, roaming for mobile data is permanently activated (not recommended!) This setting overwrites the "Allow Data Roaming" setting!
Use System http Proxy Server	The use of a HTTP proxy server, which is provided by the system's settings in settings, is dependent on the connected network (WiFi or APN)

PIM Management

Gmail Exchange

Info: This Configuration will be applied to the Gmail app. So you have to approve and install Gmail.

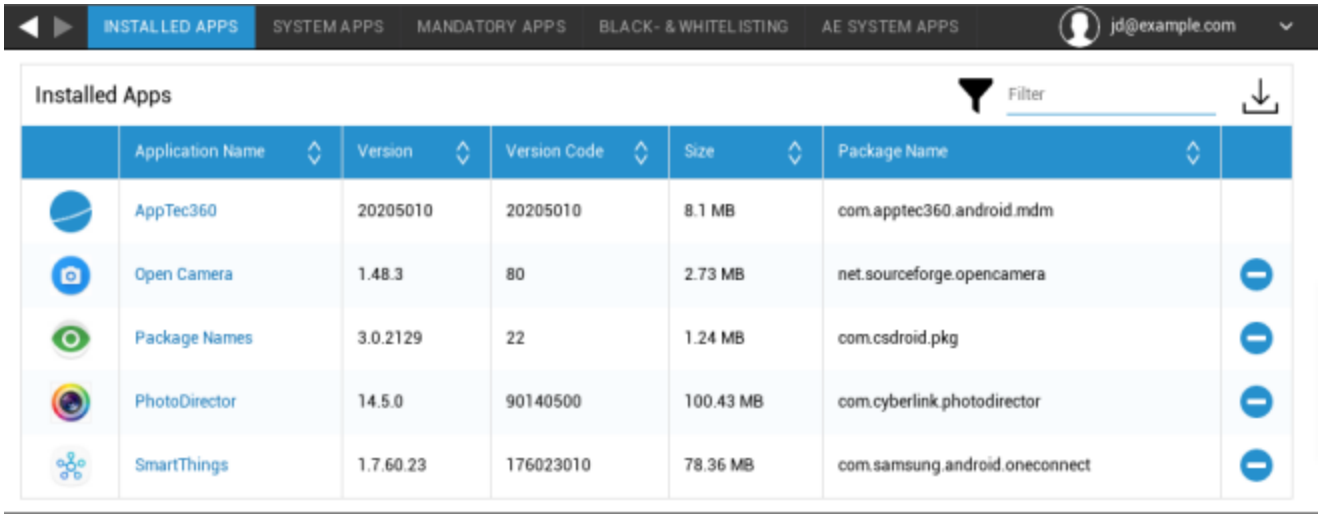
eMail Address	The provided user's email address Please note the "Placeholders", which you can use to work with credentials and you do not perform changes manually on every device With a click on you can display them for yourself
Server Hostname	Server address of your Exchange Servers
Login name	The Login-Name for the respective end user device, please also note the "Placeholders here
Signature	A signature can be attached (Hint: Some devices require HTML formatting for the signature)
Number of previous days to sync	Number of days, determining when emails are sync'd back
Device Identifier	Ein String der die EAS DeviceID enthält. Dies ist Teil des EAS Protokols und wird in einigen Umgebungen benötigt
Use Secure Sockets Layer (SSL)	Use a SSL connection
Accept all certificates	All certificates are accepted. Please select this option, if your Exchange Server uses a self-signed certificate
Allow unmanaged accounts	Allow users to add or remove any Exchange account, other than the account specified in this managed configuration. If this setting is enabled, you can't prevent users from adding other Exchange accounts to Gmail. You also can't control data sharing between other apps and Exchange accounts added by users. This setting should be enabled only if your users need to maintain more than one work Exchange account in Gmail.
Client Certificate	Client Certificate. Only required if your Mail Server expects this to be present.

App Management

Enterprise App Manager

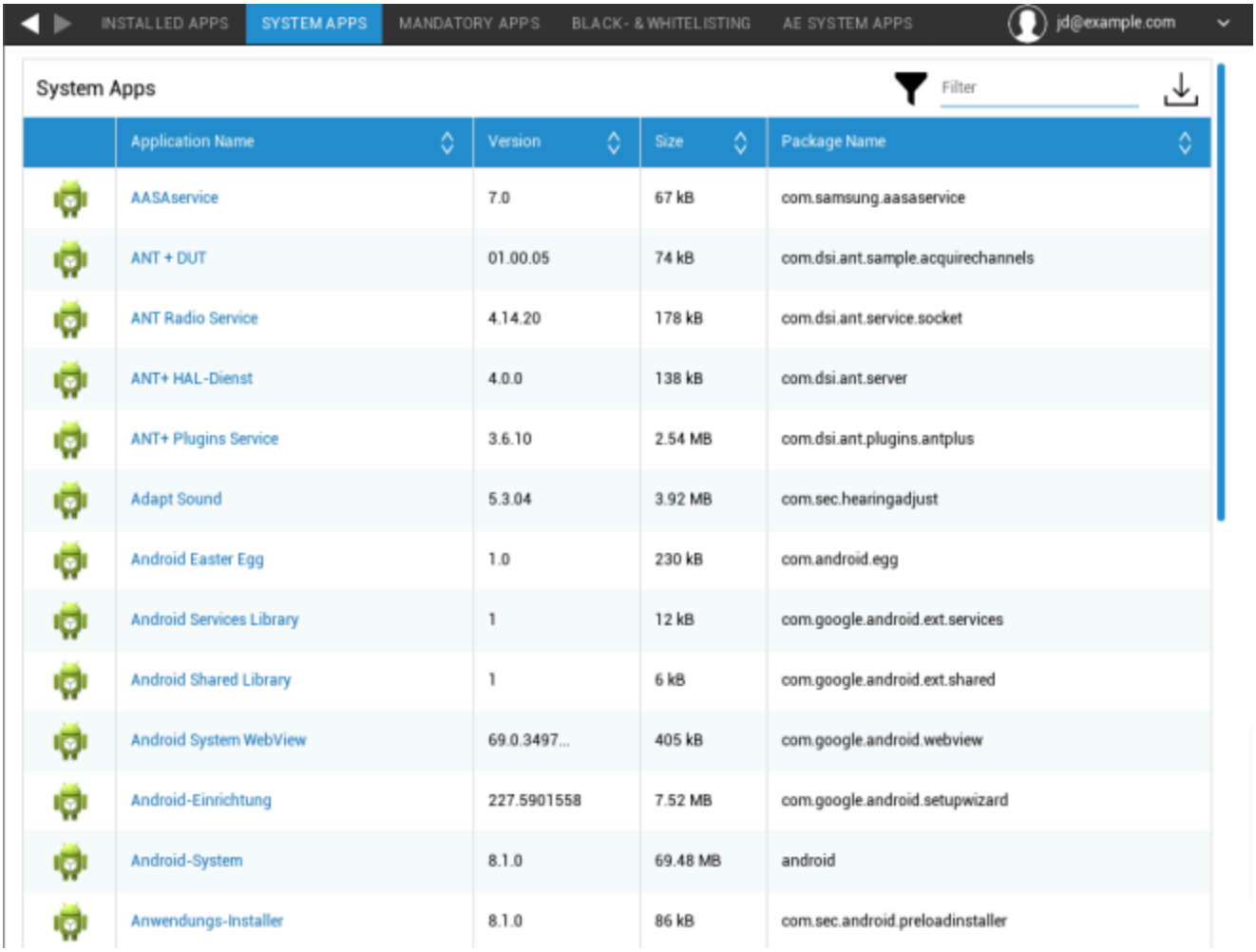
Installed Apps (only on device level)

Here all Apps that are currently installed in the container will be displayed for you.



System Apps (only on device level)

Under the “System Apps“, all of the apps and services that have already been installed on the end user device by your device manufacturer will be listed for you.

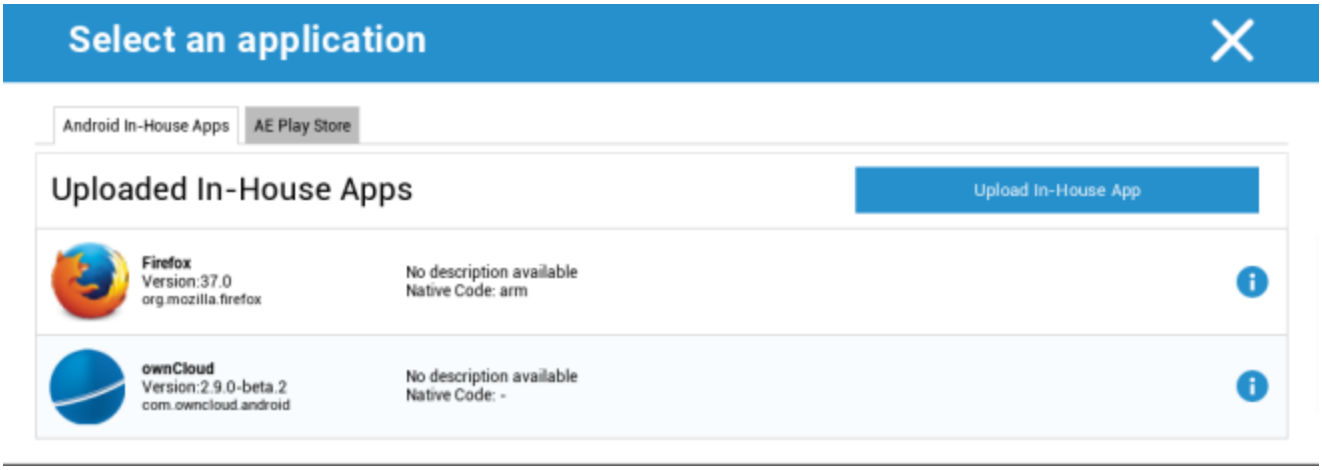


Mandatory Apps

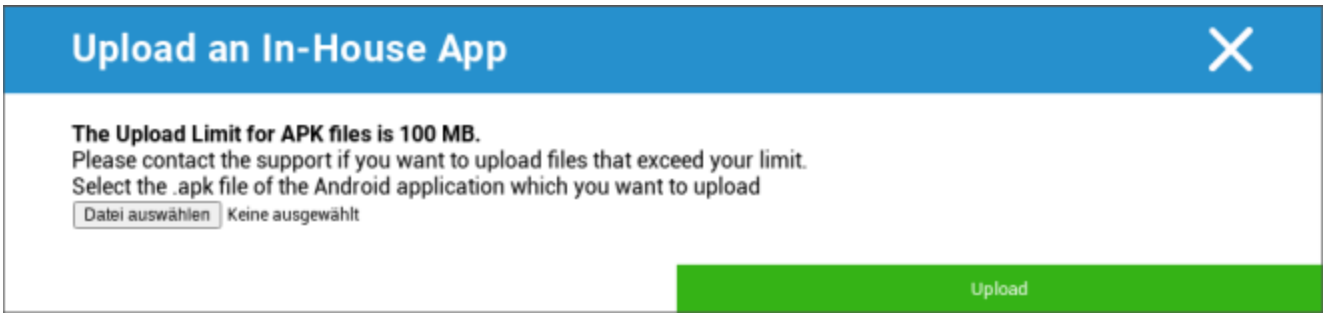
Under the Mandatory Apps, you can establish the mandated required apps. The user will continually prompted to install this designated app, if it is an InHouse App. Play Store apps will be installed automatically.

Via the , the mandated required app can be defined.

This can be an In-House App from the “Android In-House Apps“, which you have uploaded in General Settings.

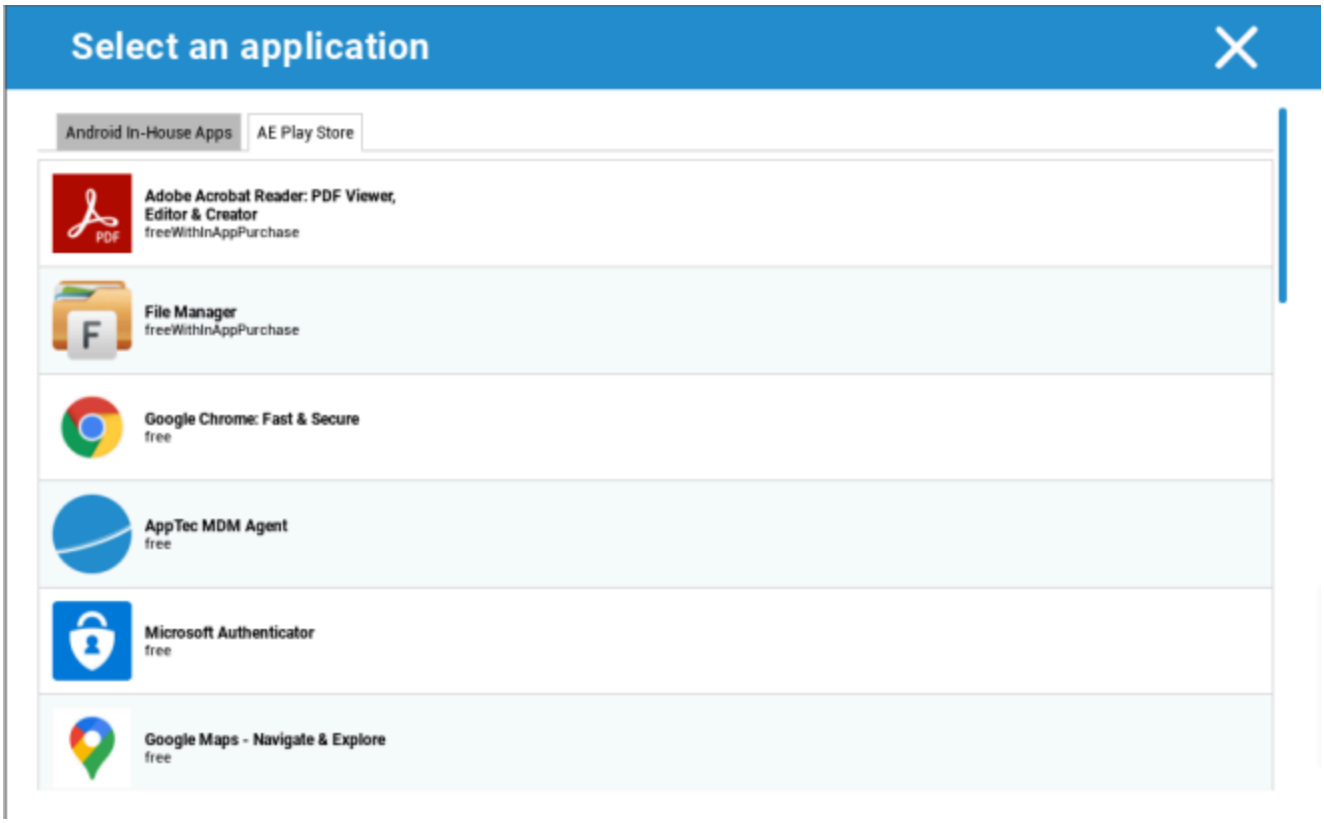


You can also directly select and upload an apk file with “Upload In-House App“.



If you are installing an In-House App, you will have the possibility to activate „Keep up to date“. If this is activated and you have defined a newer version in the In-House App DB, the app will be updated on the device.

Or it can be a “AE Play Store“ App from the Google Work Play Store.



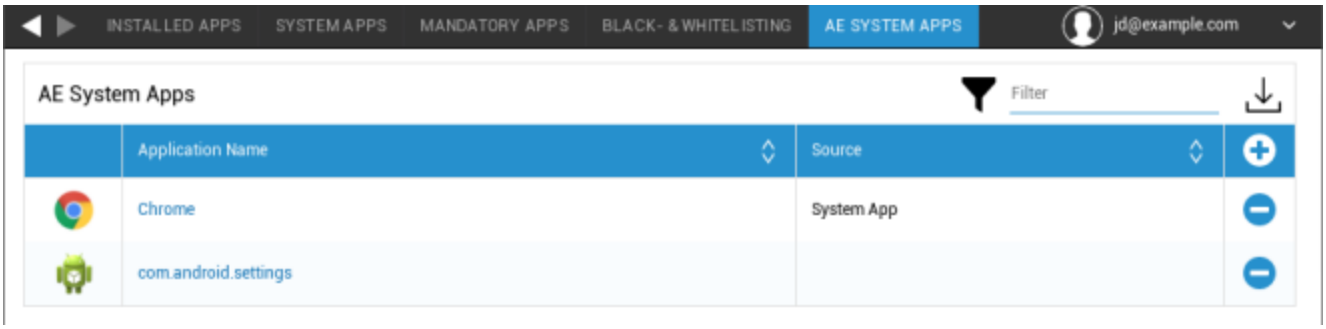
Only approved “AE Play Store Apps” will be shown in this tab.

To approve an “AE Play Store App” please go to “General Settings” > “App Management” > “AE Play Store” and add an app via the button which will redirect you to the “Play Store Apps” tab (or you can directly go to the “Play Store Apps” tab).

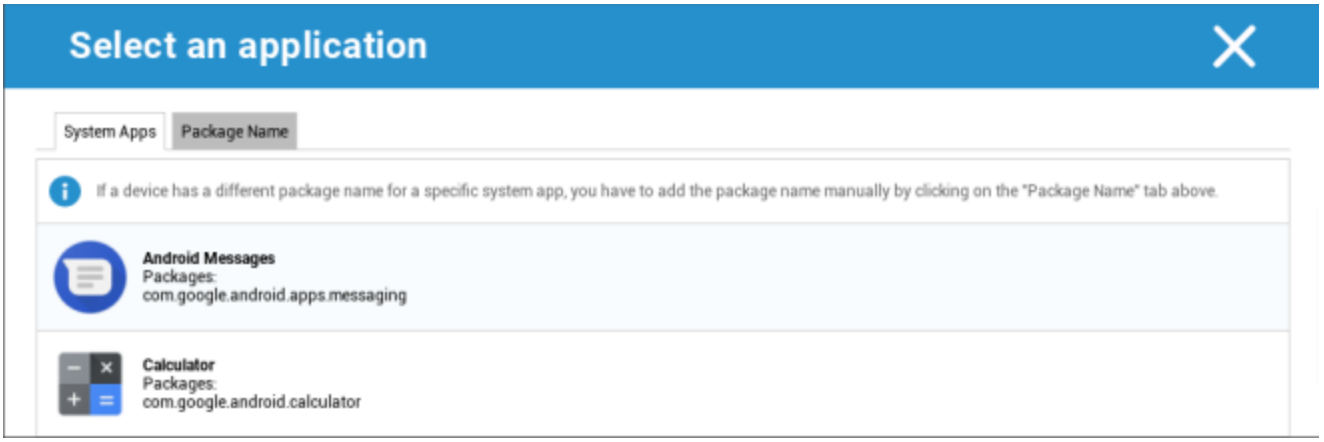
In the “Play Store Apps” tab you can search for apps. When you click on an app, the app page opens and here you can approve the app by clicking on "Approve".

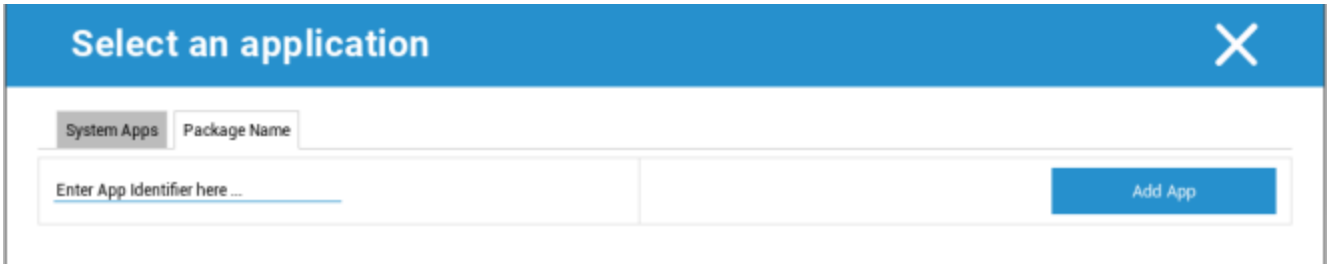
AE System Apps

Here you can define a list that contains specific system apps that should be activated on the devices.



If you click on the button, you can choose from a list of possible system apps provided by Google or directly enter the package name of a system app that should be activated.





Please keep in mind that the system apps in the list provided by Google are only apps that can be system apps, but do not necessarily have to be system apps on your devices.

However, this list only affects apps that are already pre-installed.

Adding apps that are not pre-installed on your devices will not affect your devices, regardless of whether the app is from the list provided by Google or the app's package name is entered directly.

Restrictions & Settings

App Management Settings

Here you can configure the device's behaviour regarding app updates.

Update Check Frequency	Specify in which interval the AppTec Client will search for app updates. The default value is 24 hours.
Wi-Fi Threshold	Apps that are bigger than the specified size will be downloaded over Wi-Fi. If "Wi-Fi only" is selected, all apps will be downloaded via Wi-Fi.

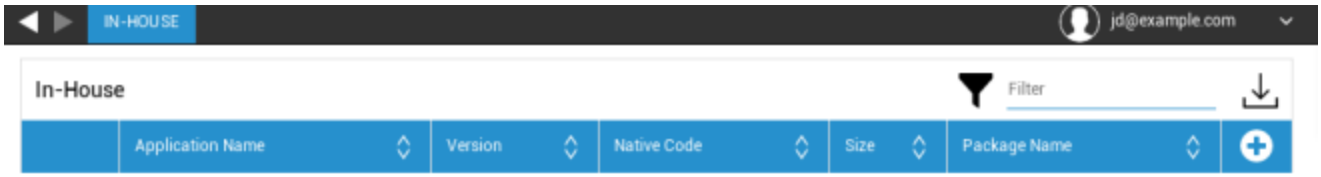
Enterprise App Store

In-House

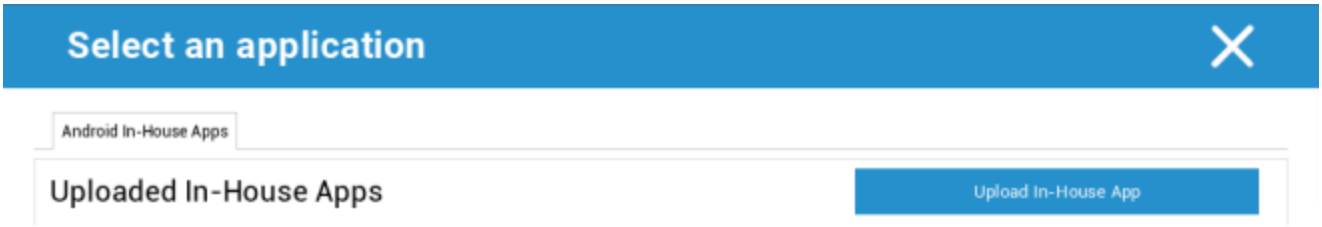
Under the point “In-House“, you can upload and distribute internally developed apps.

With the symbol, you can distribute additional In-House Apps.

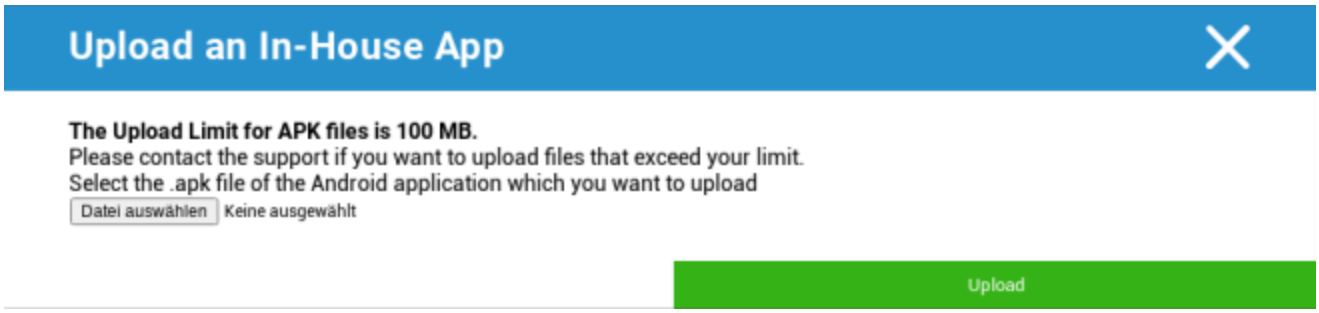
If you are installing an In-House App, you will have the possibility to activate „Keep up to date“. If this is activated and you have defined a newer version in the In-House App DB, the app will be updated on the device.



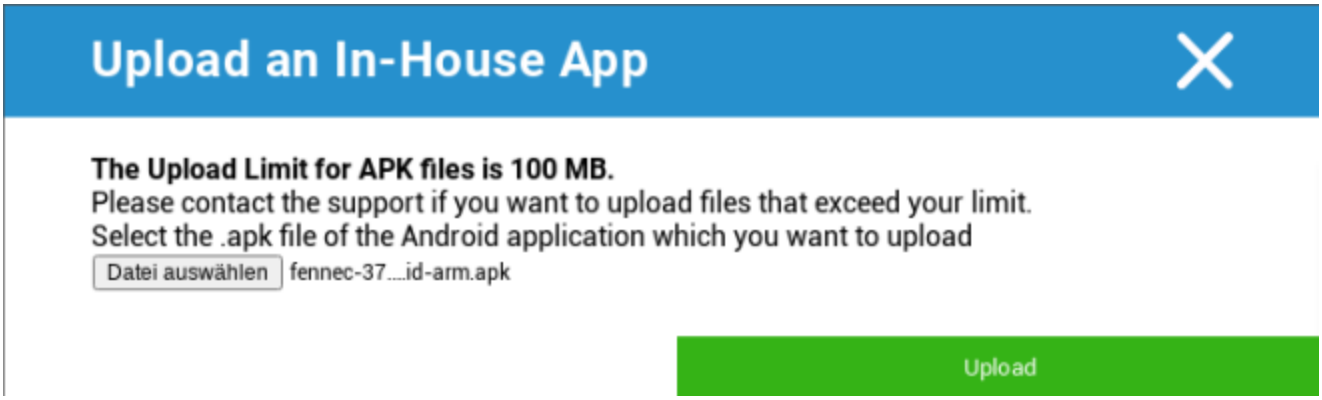
Should you not have distributed In-House Apps, you will then receive the following overview:



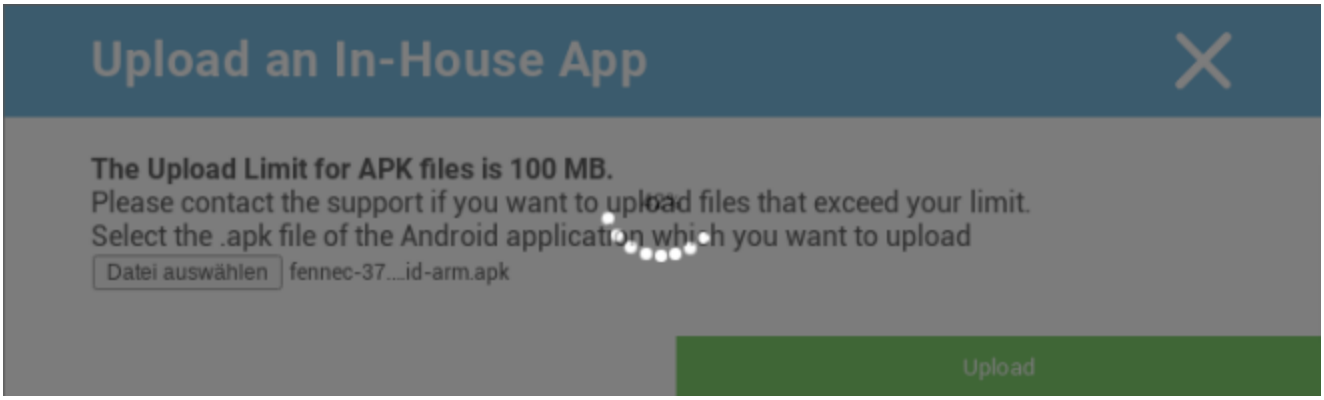
For this, click on “Upload In-House App”, you will then receive the following overview:



Now, choose with “Search…“an .apk file and then click on “Upload“.



Your app will now be uploaded, in the middle of the circle you will see a percentage indicator, showing how much of your app has already been uploaded.



Should the upload of your In-House App have been successful, you can then find the uploaded app in your App Catalog.

The user now has the option to see and install this app in the AppTec Store on the end user device, under the category “In-House“.

Due to the fact that this not involve a Google PlayStore App, the user does not need a stored Google ID on their respective end user device.

Enterprise Play Store

AE Play Store

Here you can add Apps to the Android Enterprise Playstore. Please note that you have to approve Apps with your AE Administrator Account before you can add them.

For approving an app please see the instructions in Mandatory Apps.

Content Management

ContentBox

Here you can activate the ContentBox.

As soon as you switch “Enable ContentBox“ to “On“, a separate ContentBox App will be installed automatically on the end user device.

Secure Browser

Here you can configure settings for the AppTec Secure Browser.

As soon as you switch the section in “Secure Browser“ to “On“, a separate Browser App will be installed automatically on the end user device.

Require Password	Require the user to set up and use a password to access the browser.
Minimal required password length	Set the required number of characters for the password
Required Password Quality	Set the required password quality
Restrict Downloads / Open In	
Restrict Uploads	
Upload Whitelist	A list of URLs for which uploading will always be allowed.
Allow Copy	Allow copying, cutting or sharing text inside the web pages.
Allow Screen Capture	Allow capturing screenshots.
Data cleanup frequency	Select with which frequency, ALL the user data (history, cache etc.) should be automatically removed.
Company Bookmarks	The Bookmarks will show up in the "Company bookmarks" folder in the browsers bookmarks. They are not editable by the user.
Hide Address Bar	
In-Browser Whitelisting (without Universal Gateway)	Enables client-side URL whitelisting. • Company Bookmarks are always whitelisted • Supported for 100 URLs only • Please use the Universal Gateway for unlimited Black- and Whitelisting
Whitelisted URLs	A list of allowed URLs.
Gateway based Black- and Whitelisting	Blacklisting has the following requirements: • A working AppTec Universal Gateway ("General Settings" → "Universal Gateway")

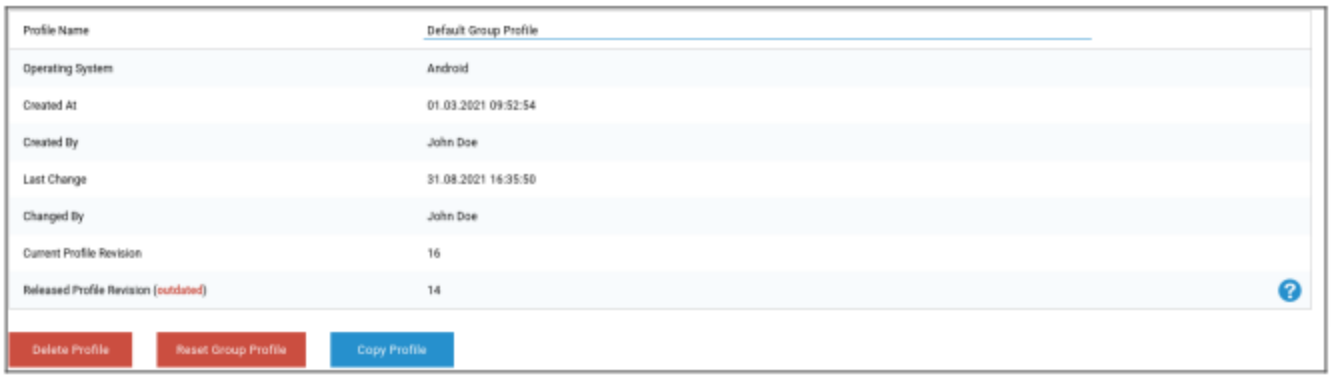
	• A working VPN configuration with a specified DNS server ("General Settings" → "Universal Gateway" → "VPN Settings") • A Blacklist configuraton ("General Settings" → "Universal Gateway" → "Domain Blacklist") • A valid VPN connection in the profile ("Connection Management" → "VPN")

Android Configuration

General

Group profile overview (only on group level)

When opening a group profile, you will get a quick overview of the profile.



Profile Name	Name of the profile (can be changed here)
Operating System	Operating System the profile is for
Created At	Time of creation
Created By	The profile's creator
Last Change	Time of last change to the profile
Changed By	Account that made the last changes
Current Profile Revision	Revision of saved profile state
Released Profile Revision	Assigned profile revision ("Assign now"). If the label shows "(outdated)" behind the text, it means you've saved the profile but did not assign it yet, so the devices will still get and older version.

Device Overview (only on device level)

Should you be on a device, you will receive an overview recap of the selected device, the following is contained here:

Device Name	Device name
Last Known Location	The last known GPS coordinates
Phone Number	Phone number
Assigned Mandatory Apps	The number of assigned mandatory apps
OS Version	OS version of the device
Operating System	Operating System (Android / iOS / Windows Phone)
Serial Number	Device serial number
Device Ownership	Corporate or private device
Device Type	Telephone or Tablet
Rooted	Status, indicating if the device has been rooted
Compliant	Guideline compliant
IP Address	IP Address
Last Seen	Point in time, when the device last connected to AppTec
Last Push	Point in time, when the server sent a push to the device
User Assignment	A dropdown to assign the device to another user

Config Revision (only on device level)

Here you will receive an overview of which group profile is assigned to the device.

If you click on the group profile, you will access the profile directly and you can perform settings.

With the symbol, you can revert the assigned apps to the group profile's settings.

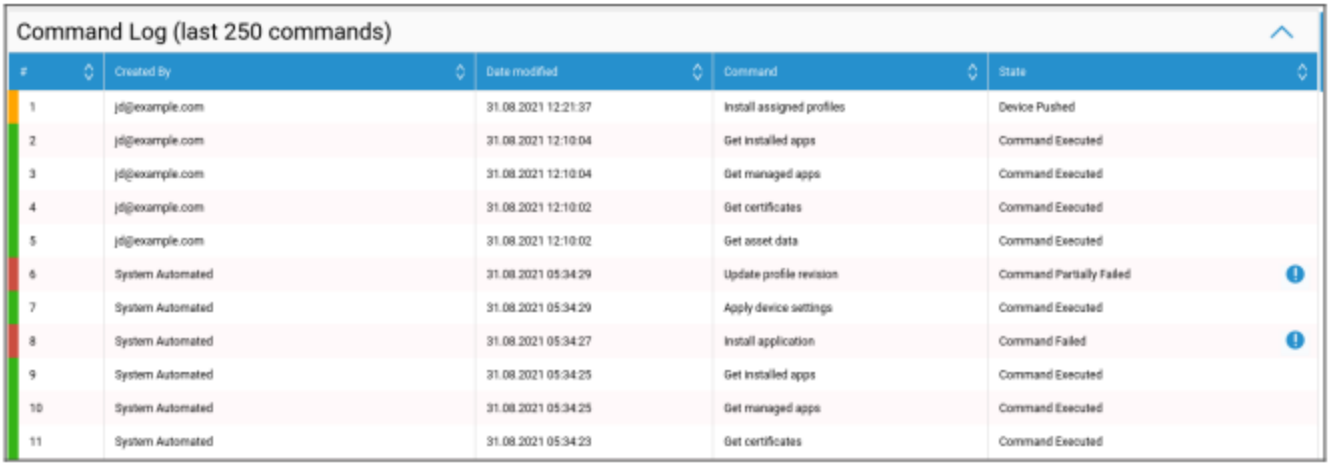
With the symbol, you can reset the device profile to have no settings at all.

“Newer Revision available“ indicates that the group profile has been changed and saved but not assigned. The group profile has to be assigned with “Assign now” on group level to apply the changes to the devices.

Device Log (only on device level)

Command Log

Here you can see which commands where issued for the device and what their status is.



Commands created by “System Automated” are automatically created by the system.

Possible command statuses

Device Pushed	A push request has been sent to the push service (e.g APNS) to tell the device to connect back to the EMM server.
Command Created	The command was created in the system.
Command Sent	The command got sent to the device after it connected to the server.
Command Executed	The command was successfully executed.
Command Failed	The command failed. *
Command Partially Failed	Depending on the device OS some commands may get grouped together. In this some parts of this command group failed. *
Command Executed, eventually Failed	The command was executed but maybe it wasn't.
Command Repushed	The command was repushed by a user.
Discarded	The command was discarded. For example because it was superseded by another command or the device got re-enrolled and old commands got removed

*If there is an exclamation mark behind the message, you can get more information by hovering over the icon with your cursor.

Device Settings

Client Configuration

Here you can perform the following configurations on your Android device:

Warning message after disabling Device Management	Established warning message after disabling Device Management
Out of Compliance Time	Time limit, after which "Enforcement Action after compliance" will be performed, if the device is not compliant. Min. 1 minute Max. 24 hours
Enforcement action after compliance timeout	The action that is to be taken, as soon as a device becomes non-compliant. • do nothing = no action • Lock Device = lock device • Wipe Device = device will be restored to factory settings
Data Collection Frequency	Frequency with which device/GPS-information is to be collected
Device Heartbeat Frequency	Interval in which the device should contact the AppTec360 Server Min. 1 minute Max. 24 hours
Enable Location Updates	If activated, the device sends location updates to the AppTec360 Server
Location Update Time	Determines in what time intervals the device sends location updates to AppTec
Use Google Location Accuracy for Location Update	If activated, the Google Location Accuracy (formerly known as network location) will be used for location updates (if this was deactivated under "Restrictions", then this setting will not affect anything)
Use GPS Location for Location Update	If activated, the GPS will be used for location updates
Allow Mock (Fake) Locations	Allows the forging of location information via third party apps

Lost Connection Action	Enables you to set a certain action which will be performed after a certain amount of heartbeats failed
Policy Enforcement Mode	Defines how aggressive the AppTec360 Client asks the user to perform certain actions which require user input. Interval (Default) = ask in intervals, so the user can put this in the background for a while. No Alert = no popup for any required interaction. You have to open the AppTec360 Client manually to check if there is a required action Constant Alert = The user can only perform the required action. The AppTec360 Client will force itself in the foreground if the user tries to avoid it
AppTec360 Version Lock	Lets you define a version of the AppTec360 Client which is the maximum version the client updates itself to.

Wallpaper

Here you can define a custom wallpaper.

“Specify a Color” lets you define a color in hex format (e.g. #000000). Only hex values are allowed.

“Set Image as Wallpaper” lets you upload an image. Please be aware that different devices with different launchers and OS versions are working differently. There is no general guide line for size and ratio, since this depends on the device.

Use JPG (or JPEG) or PNG for the file format.

Asset Management (only on device level)

Asset Management

Device Info

Model	**Device model designation**
Operating System	OS
OS Version	OS version
AE Support	Support for Android Enterprise (Container and fully managed)
Serial Number	Serial number
Device Name	Device name
Battery Status	Battery status
Free / Total Memory	Free / Total memory
Samsung KNOX	Samsung KNOX API Level
SD Card Available	SD Card available
SD Card Emulated	SD Card emulated
SD Card Removable	SD Card removable
SD Free / Total Memory	SD Free / Total SD Card memory

Wi-Fi

IP Address	Device IP address
WiFi MAC	WiFi MAC address

Cellular

Status	Status (SIM card installed)
Phone Number	Phone Number
Roaming (Voice / Data)	Roaming for voice / data
Roaming Status	Current roaming status
IP Address	IP address
Operator/Carrier	Operator/Carrier
Cellular Technology	Cellular Technology
IMEI	IMEI number
ICCID	This is the ID for the SIM card, often times also a Smartcard or Integrated Circuit Card (ICC)
IMSI	The International Mobile Subscriber Identity (IMSI) provides in GSM- and UMTS-mobile networks a definite identification of the network users The IMSI is comprised of a maximum of 15 digits and is configured in the following manner: • Mobile Country Code (MCC), 3 digits • Mobile Network Code (MNC), 2 or 3 digits • Mobile Subscriber Identification Number (MSIN), 1-10 digits
Current MCC/MNC	See "SIM MCC/MNC"
SIM MCC/MNC	The Mobile Country Code is an established country identifier, set by the ITU as per E.212 Standard. This works in conjunction with the Mobile Network Code (MNC) for the identification of the mobile network. Meaning the SIM card's country/Mobile Network Code. If you roam into another mobile network, then logically, the "Current MCC/MNC" and "SIM MCC/MNC", will be different.

Bluetooth

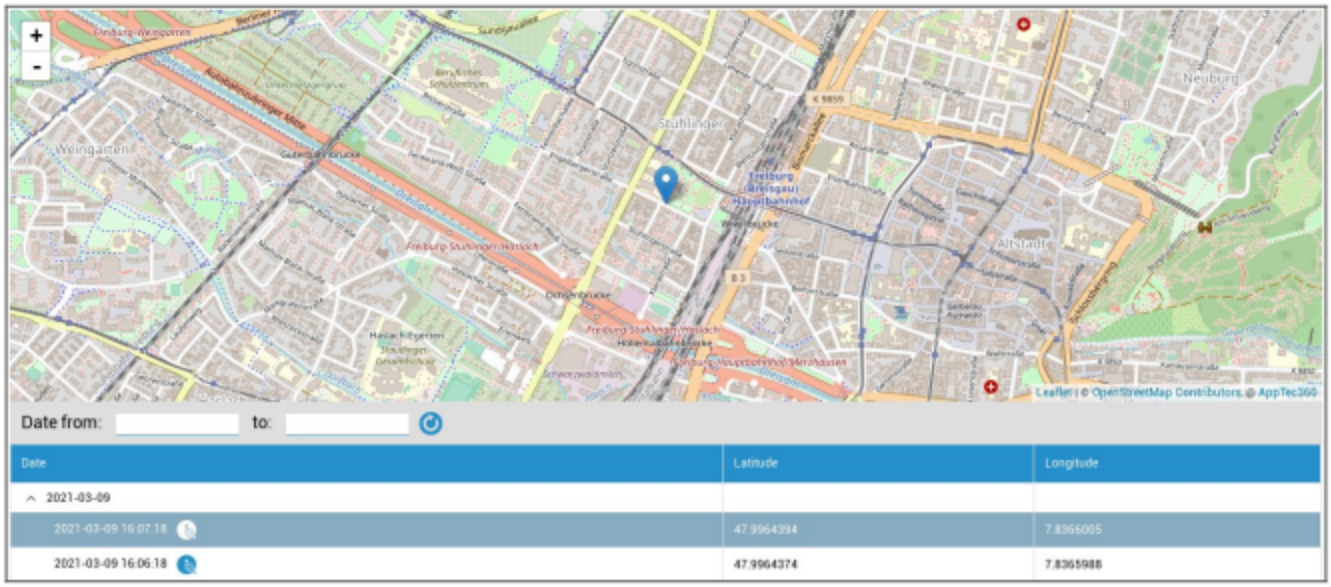
Bluetooth MAC	Bluetooth MAC address

Security Management

Anti Theft (only on device level)

GPS Information (only on device level)

Here you can establish the current/last device location. The localizing can be protected with one or even two passwords – See: General Settings – Privacy – GPS Access



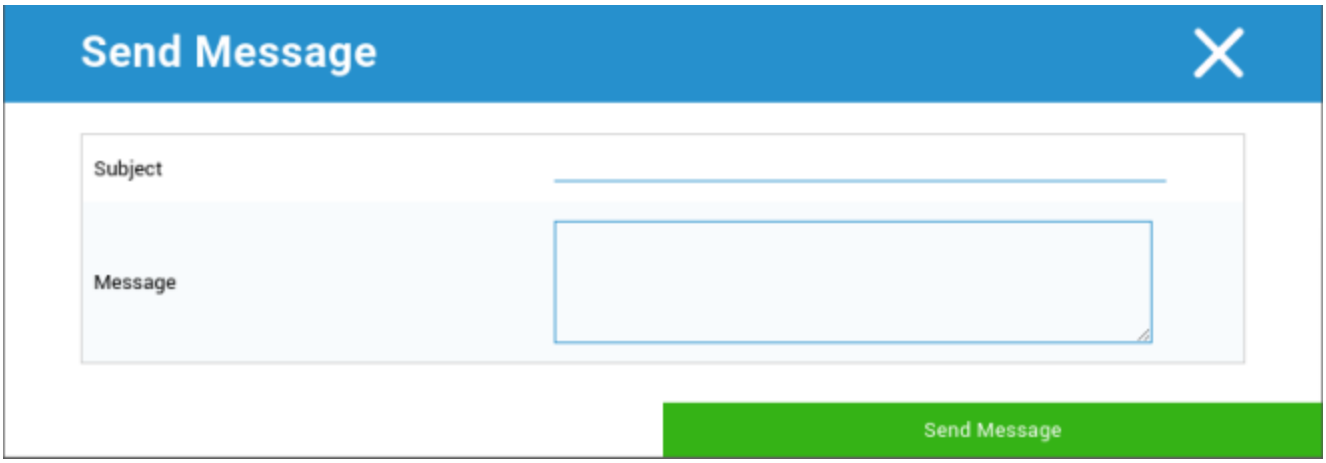
Wipe & Lock (only on device level)

Under „Wipe & Lock“, you can perform the following three actions:

Full Wipe	The device is restored back to its factory settings (corporate, as well as personal data is deleted)
Enterprise Wipe	Only corporate data is removed from the end user device (all apps, data, etc. that were provided by AppTec360)
Lock Screen	Screen lock is activated, it is sufficient to unlock the device with the device-password/PIN

Message (only on device level)

You can fill in the subject and a message and send it to an end user device. This message will be displayed in the AppTec360 Client.



Security Configuration

Passcode

Under “Passcode“ you can mandate a device password, the following setting options are available to you

Minimum password length	Establishes, the minimum number of symbols a password must have
Password quality	Password strength Unspecified = not specified Every password is ok = every password is acceptable at least numeric characters = must contain at least numeric characters at least complex characters = must contain at least special characters at least alphanumerical characters = must contain at least alphanumerical characters at least alphabetic characters = must contain at least alphabetic characters
Maximum inactivity time lock	Maximum screen timeout. This only configures the maximum value which can be selected by the user
Minimum lowercase letters required in password	Minimum lowercase letters required in password
Minimum uppercase letters required in password	Minimum uppercase letters required in password
Minimum non-letter characters required in password	Minimum non-letter characters required in password
Minimum numerical digits required in password	Minimum numerical digits required in password
Minimum symbols required in password	Minimum symbols required in password
Password expiration timeout	Establishes, after which time interval the password expires and a new password must be issued
Password history restriction	Number of previously used password that are not allowed
Maximum failed password attempts	Establishes, how often a password can be entered incorrectly, before a complete device wipe will be performed

Encryption

Under this point, you are able to encrypt the internal device memory, as well as the SD card memory.

Require Storage Encryption	If this setting is activated, the device memory will be encrypted, as long as the device supports this functionality. Once the device memory has been encrypted for the first time, it is no longer possible to un-encrypt it. Likewise, the Password Policy will be automatically switched to 6 alphanumeric symbols
Require SD Card Encryption	This setting only applies to Samsung devices! If this setting is activated, the external SD card can be encrypted and can only be manually un-encrypted on the end user device. Likewise, the Password Policy will be automatically switched to 6 alphanumeric symbols

AntiVirus

Enabling AntiVirus will install Ikarus on the devices. Please be aware that this requires a separate license which can be entered in General Settings → App Management → Third Party Apps.

Automatic Scan	Defines whether or not Ikarus scans automatically and how often it performs this scan Enabling "Full Automatic Scan" will perform a full scan. Otherwise a quick scan will be performed
Automatic Updates	Enables automatic updates of the virus database and sets how often this happens
App Protection	Enables Scan of Apps in addition to the regular Scan which only scans Files
SD Card Protection	Enables SD Card Protection. Without this, the scan is limited to the local storage
Wi-Fi Only Update	Limits Update to Wi-Fi

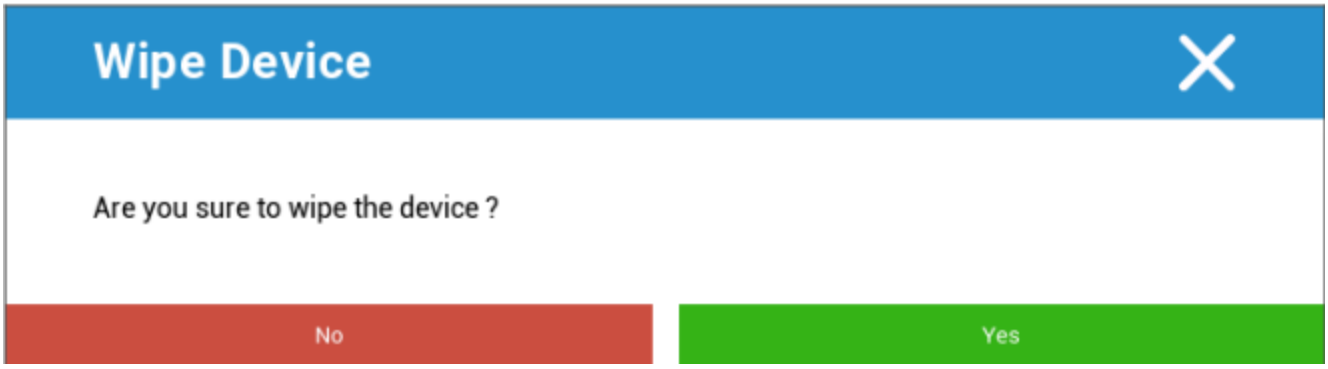
End of Life (only on device level)

Wipe (only on device level)

Under “Wipe“, you can restore the device to its factory settings. Here the corporate, as well as the private data will be deleted on the end user device.

With a click on the “Minus Symbol“ you should receive the following message

Wipe SD Card too?	The SD-card memory will also be erased



With “Yes“ you can perform the wipe.

Under “Wipe Report“ the following items can be displayed

Wiped by	History of who performed the wipe
Date	Date
Status	Status (ex. if the Wipe was performed successfully)

Restriction Settings

Restrictions

Here, a variety of things can be restricted and blocked.

Enable Camera	Allow use of camera
Force Auto Sync	Relates to "Sync" interface On = synchronization is permanently activated Off = synchronization is permanently deactivated User choice = selected by the user
Force Bluetooth	On = Bluetooth is permanently activated Off = Bluetooth is permanently deactivated User choice = selected by the user
Force GPS	On = GPS is permanently activated Off = GPS is permanently deactivated User choice = selected by the user
Force Google Location Accuracy	On = Permanent internet-localizing Off = Permanent deactivation of internet-localizing User choice = selected by the user

For Samsung devices with the KNOX 1.0 or higher interface, the following settings options are available.

Allow SD Card	Allow SD Card
Allow SD Card Write	Allow "write" on the SD Card
Allow Screen Capture	Allow screen capture
Allow Clipboard	Allow clipboard
Backup settings and app data in Google Cloud	Off = deactivate Google Backup On = activate Google Backup User Choice = selected by user
Allow USB Debugging	Allow USB Debugging (is used, for example, for the creation of device-logs (ADB))
Allow Google Crash Report	Allow Google Crash Report to be sent from the apps
Allow Factory Reset	Allows the user to restore the device to its factory settings
Allow OTA Upgrade	Allow "Over-The-Air" Updates
Allow USB host storage	If activated, USB memory, in the form of a HD or a SD card reader, can be connected
Allow USB Media Player (MTP,PTP)	Allow USB Media Player (MTP,PTP)
Allow Microphone	On = allow microphone for 3rd Party Apps Off = block microphone for 3rd Party Apps User Choice = users may select, if the 3rd Party App has access to the microphone
Allow NFC (Near Field Communication)	Allow NFC
Allow Unknown Sources (APK Sideloading)	If enabled the side-loading of Apps (APK files) is allowed. Once this setting is disabled, the user has to enable it manually when you reallow the installation of APKs from unknown sources.
Allow User Creation	Allows the creation of multiple users

AE Device Owner

(Device has to be in Android Enterprise Device Owner Mode) It is recommended to create the devices as “Android Enterprise” device and not as “Android” device.

Security	
Disallow Share Location	Specifies if a user is disallowed from turning on location sharing.
Disallow Safe Boot	Specifies if the user is not allowed to reboot the device into safe boot mode.
Disallow Network Reset	Specifies if a user is disallowed from resetting network settings from Settings.
Disallow Factory reset	Specifies if a user is disallowed from resetting the device.
Enable ADB	Allows the Connection to a PC via ADB
Disable Keyguard	Disables Keyguard
Device Owner Lockscreen Info	Sets the device owner information to be shown on the lock screen.
Compliance Enforcement	Mode Prompt User - User will be prompted to fulfill the necessary actions. Mode Lock-Down Container - Hide all apps until all requirements are fulfilled

App Management	
Allow Cross Profile App Linking	Allows apps in the parent profile to handle web links from the managed profile.
Disallow App Control	Specifies if a user is disallowed from modifying applications in Settings or launchers.
Disallow App Installation	Specifies if a user is disallowed from installing applications.
Disallow Uninstall Apps	Specifies if a user is disallowed from uninstalling applications.
Runtime Permission Policy	Specifies how new permission requests from apps will be handled.
Allow Unknown Sources	If enabled, users can sideload Apps by installing an .apk file.

Connectivity	
Disallow Mobile Network Config	Specifies if a user is disallowed from configuring mobile networks.
Disallow Tethering Config	Specifies if a user is disallowed from configuring Tethering & portable hotspots.
Disallow VPN Config	Specifies if a user is disallowed from configuring a VPN.
Disallow Wifi Config	Specifies if a user is disallowed from changing WiFi access points.
Disallow Outgoing NFC Beam	Specifies if the user is not allowed to use NFC to beam out data from apps.
Lock WiFi Configuration	This setting controls whether WiFi configurations created by a Device Owner app should be locked down (that is, be editable or removable only by the Device Owner App, not even by Settings app).
Enable Data Roaming	Activates Data Roaming

Bluetooth	
Disallow Bluetooth	Specifies if bluetooth is disallowed on the device. Requires Android 8.0
Disallow Bluetooth Sharing	Specifies if outgoing bluetooth sharing is disallowed on the device. Requires Android 8.0
Disallow Bluetooth Config	Specifies if a user is disallowed from configuring bluetooth.

Account Management	
Disallow adding managed profile	Specifies if a user is disallowed from adding managed profiles. Requires Android 8.0
Disallow adding Users	Specifies if a user is disallowed from adding new users.
Disallow Remove Managed Profile	Specifies if managed profiles of this user can be removed, other than by its profile owner. Requires Android 8.0
Disallow Account Modification	Specifies if a user is disallowed from adding and removing accounts, unless they are programmatically added by Authenticator.

Telephony	
Disallow Outgoing Calls	Specifies that the user is not allowed to make outgoing phone calls.
Disallow SMS	Specifies that the user is not allowed to send or receive SMS messages.

System	
Disallow Window Creation	Specifies that windows besides app windows should not be created.
Disallow set User Icon	Specifies if a user is not allowed to change their icon.
Disallow Set Wallpaper	User restriction to disallow setting a wallpaper.
Disable Status Bar	Disabling the status bar blocks notifications, quick settings and other screen overlays that allow escaping from a single use device.
Enable Auto Time	Sets the time automatically.
Enable Auto Time Zone	Sets the timezone automatically.
Stay on while plugged in	The device will stay active while connected to a power source.

Storage	
Disallow disable App Verification	Specifies if a user is disallowed from disabling application verification.
Disallow Mount Physical Media	Specifies if a user is disallowed from mounting physical external media.

Enable Backup Service	Backup service manages all backup and restore mechanisms on the device. Setting this to false will prevent data from being backed up or restored. Backup service is off by default. Requires Android 8.0
Enable USB Mass Storage	Enables the usage of USB Mass Storage.

Keyboard	
Disallow Autofill	Specifies if a user is not allowed to use Autofill Services. Requires Android 8.0
Disallow Copy & Paste between Profiles	Specifies if what is copied in the clipboard of this profile can be pasted in related profiles.

Sound	
Disallow Volume Adjustment	Specifies if a user is disallowed from adjusting the master volume.
Disallow Unmute Microphone	Specifies if a user is disallowed from adjusting microphone volume.
Mute Device	Mute device.

System Update Policy	
Control OS Updates	Enable this to set the update behavior to automatic, windowed or postponed.

BYOD Container

Android Enterprise

Android Enterprise

Enable Android Enterprise	Enable Android Enterprise (AE). AE is supported since Android 5.1 and above.
Compliance Enforcement	Mode Prompt User - User will be prompted to fulfill the necessary actions. Mode Lock-Down Container - Hide all apps until all requirements are fulfilled
Runtime Permission Policy	Prompt user for new permission requests Always grant new new permission requests Always deny new permission requests Warning: Some Apps have problems recognizing the permissions if these are set automatically. If you always grant permissions and encounter problems with apps saying that permissions are missing, set this to "prompt user" and re-install the app
Allow outgoing clipboard	Allows copy and pasting from inside the container to the outside
Allow Caller ID Resolution	Shows the name for an incoming call based on contacts in the container
Allow Contact Search Resolution	Allows to search for names in the container contacts when making calls
Allow Bluetooth Contact Sharing	Allows access to container contact in a car
Disallow Outgoing NFC Beam	Disables NFC for the Container
Allow Unknown Sources	If enabled, users can sideload Apps by installing an .apk file.
Allow USB Debugging	If enabled, users can enable USB Debugging.
Disallow Account Modification	Disallows the creation, deletion and modification to Accounts in the container Keep in mind that some apps need to create or modify accounts to work as expected

Gmail Exchange

Allows you to configure Gmail in the Container. Please be aware that enabling this configuration does not automatically install the app. You still have to add this app as mandatory app.

Email Address	Email Address
Server Hostname	Server Hostname
Login Name	Login Name
Signature	Signature
Number of previous days to sync	Number of previous days to sync.
Device Identifier	EAS Identifier. Keep this empty if your environment does not require this
Use Secure Sockets Layer (SSL)	Enables Usage of SSL. Disabling this may lower security
Accept all certificates	Accepts alls certificates. Enabling this may lower security
Allow unmanaged accounts	Allows the user to add additional accounts
Client Certificate	Upload client certificate if your Exchange server requires this

AE System Apps

Here you can enable System Apps for the Android Enterprise Container. Please keep in mind that the specified app has to be in the storage of the system, otherwise nothing happens.

Container Passcode

Only for Android 7.0 or higher

Allows you to set a specific password requirement for the container.

Minimum password length	Establishes, the minimum number of symbols a password must have
Password quality	Password strength Unspecified = not specified Every password is ok = every password is acceptable at least numeric characters = must contain at least numeric characters at least complex characters = must contain at least special characters at least alphanumerical characters = must contain at least alphanumerical characters at least alphabetic characters = must contain at least alphabetic characters
Maximum inactivity time lock	Maximum Time until the container gets locked. This only configures the maximum value which can be selected by the user
Minimum lowercase letters required in password	Minimum lowercase letters required in password
Minimum uppercase letters required in password	Minimum uppercase letters required in password
Minimum non-letter characters required in password	Minimum non-letter characters required in password
Minimum numerical digits required in password	Minimum numerical digits required in password
Minimum symbols required in password	Minimum symbols required in password
Password expiration timeout	Establishes, after which time interval the password expires and a new password must be issued
Password history restriction	Number of previously used password that are not allowed
Maximum failed password attempts	Establishes, how often a password can be entered incorrectly, before the container gets deleted

Samsung KNOX

Activation

Here you can enable the Samsung KNOX Container. Please be aware that this is no longer supported from Samsung on Android 10 or higher. Use the Android Enterprise Container on Android 10 or higher

Knox Passcode

Establish the guidelines that relate to the settings of the device password

Minimum password length	Establishes, how many symbols the password must have
Password quality	Password strength Every password is ok = Every password is ok At least numeric characters = Minimum numeric characters must be present At least complex characters = Minimum special characters must be present At least alphanumerical characters = Minimum alphanumeric characters must be present At least alphabetic characters = Minimum alphabetic characters must be present
Minimum complex characters required	Minimum complex characters must be present
Maximum Inactivity Timeout	Maximum user inactivity timeout, before keyboard lock
Allow Fingerprint Authentication	Allow fingerprint authentication
Allow Iris Authentication	Allow iris recognition authentication
Max Password Age	Establishes, after what time the password expires and a new password must be issued
Stored Password History	Number of former passwords that are not allowed
Maximum failed password attempts	Establishes, how often the password may be submitted incorrectly, before a complete device wipe will take place

Knox Security

Limit specific device functionalities

Enable Camera	Allow the use of the camera
Allow Samsung KNOX App Store	Allow the use of the Samsung KNOX App Store
Allow Google Play Services	Allow Google Play Services
Allow Browser	Allow the use of the native browser

Allow Screenshots	Allow the creation of Screenshots
Allow Contact Import	If activated, the access of device contacts from the KNOX Container is allowed
Allow Contact Export	If activated, the access to the KNOX contacts from the device is allowed
Allow Calendar Import	If activated, the access of device calendar from the KNOX Container is allowed
Allow Calendar Export	If activated, the access to the KNOX calendar from the device is allowed
Allow Non-Secure Keypad	Allow the use of a Non-Secure Keypad
Enable File Import	Enable File Import into the KNOX Container
Enable File Export	Enable File Export from the KNOX Container

Knox Exchange

Here you can configure the Exchange-Profile for the KNOX Container

eMail Address	The provided user's email address Please note the "Placeholders", which you can use to work with credentials and you do not perform changes manually on every device With a click on **Show Placeholders** you can display them for yourself
Server Hostname	Server address of your Exchange Servers
Login name	The Login-Name for the respective end user device, please also note the "Placeholders" here
Domain	Domain address
Password (only on device level)	Optionally an individual device can be provided a password, should this remain empty, the user will be prompted to enter their Exchange Password
Number of previous days to sync	Number of days, determining when emails are sync'd back
Signature	A signature can be attached
Default Account	Establishes, that this email account is the standard account
Use Secure Sockets Layer (SSL)	Use a SSL connection
Use Transport Layer Security (TLS)	Use a TLS connection
Accept all certificates	All certificates are accepted. Please select this option, if your Exchange Server uses a self-signed certificate

Knox eMail

eMail Address	The provided user's email address Please note the "Placeholders", which you can use to work with credentials and you do not perform changes manually on every device With a click on **Show Placeholders** you can display them for yourself
Incoming server protocol	Incoming server protocol IMAP or POP
Incoming server address	Incoming server address
Incoming server port	Incoming server port
Incoming server login/username	Incoming server login/username
Incoming server password	Incoming server password
Incoming server uses SSL	Incoming server uses SSL
Incoming server uses TLS	Incoming server uses TLS
Incoming server accept all certificates	Incoming server accept all types of certificates
Outgoing server protocol	Outgoing server protocol SMTP
Outgoing server port	Outgoing server port
Outgoing Server uses extra credentials	Additional credentials for the outgoing Server. If this set to "off", then the incoming server settings will be used
Outgoing server login/username	Outgoing server login/username
Outgoing server password	Outgoing server password
Outgoing server uses SSL	Outgoing server uses SSL
Outgoing server uses TLS	Outgoing server uses TLS
Outgoing server accept all certificates	Outgoing server accept all types of certificates
Signature	Here a signature can be attached
Notify user on receiving new eMail	Notify user on receiving new eMail

Knox Apps

Establish apps here that you want to distribute to the end user devices. These will then be available in the KNOX-Container. In order to add an app, please proceed as you would in the menu Mandatory Apps

Application Name	Application Name
Mandatory Since	Point in time, when the app was added
Source	App's source (Play Store | In-House)

By clicking the symbol, the respective app can be removed again

Connection Management

Wifi

For this setting, perform the pre-configuration of the end user devices, for access to internal Access Points

Services Set Identifier (SSID)	SSID for the network that is to be connected
Hidden Network	Activate, in case the AP does not broadcast the SSID
Security Type	Establish the AP's security type

Security Type

WEP

Password	Password for the AP

WPA/WPA2

Password	Password for the AP

802.1x EAP

EAP-Method	

PWD	Identity	Identity
	Password	Password

PEAP	Phase 2 Authentication Protocol	none	No additional protocol
		MSCHAPV2	MSCHAPV2 protocol
		GTC	GTC protocol
	CA Certificate	CA certificate	
	Identity	Identity	
	Anonymous Identity	Anonymous identity	
	Password	Password	

EAP-Method	

TTLS	Phase 2 Authentication Protocol	none	No additional protocol
		PAP	PAP protocol
		MSCHAP	MSCHAP protocol
		MSCHAPV2	MSCHAPV2 protocol
		GTC	GTC protocol
	CA Certificate	CA certificate	
	Identity	Identity	
	Anonymous Identity	Anonymous Identity	
	Password	Password	

TLS	CA Certificate	CA certificate
	Identity	Identity
	Password	Password

VPN

Connection Type	**Establish VPN-connection type**

If you select “Per-App VPN” as VPN Type, the available VPN Clients will change. Per-App VPN limits the VPN to certain apps and starts the VPN connection automatically if a specific app is started.

AppTec360 VPN Client	Uses the AppTec360 VPN Client in combination with the Universal Gateway

Connection Name	VPN connection name
Gateway Configuration	Select the VPN Configuration of the Universal Gateway
Always on VPN	Forces the VPN to be always active, so the whole traffic goes through the VPN.
Enable Native Lockdown	Blocks all networking when the device is not connected to the VPN. Use this carefully since this can cause a complete connection lost if not configured properly. Only for Android Enterprise on Android 7 or higher
Enable AppTec360 Lockdown	Blocks the usage of all Apps until the VPN connection is started

Cisco AnyConnect	
Connection Name	VPN connection name
Server	Server address
Certificate Mode	Disabled = deactivated Automatic = automatic

L2TP (KNOX Only)	Only available on Samsung devices
Connection Name	Connection name
Server	Server address
Enable L2TP Secret	
DNS Search Domains	DNS search domains

Connection Type	**Establish VPN-connection type**

PPTP (KNOX Only)	Only available on Samsung devices
Connection Name	VPN connection name
Server	Server address
Enable Encryption	Enable encryption
DNS Search Domains	DNS search domains

L2TP / IPSec PSK (KNOX Only)	Only available on Samsung devices
Connection Name	VPN connection name
Server	Server address
IPSec Pre-Shared Key	Pre-shared key for authentication
Enable L2TP Secret	
L2TP Secret	
DNS Search Domains	DNS search domains

IPSec XAuth PSK (KNOX Only)	Only available on Samsung devices
Connection Name	VPN connection name
Server	Server address
IPSec Identifier	User name for the connection
IPSec Pre-Shared Key	Password for the connection
DNS Search Domains	DNS search domains

OpenVPN	

Connection Name	Connection name
OpenVPN Profile	Here is where the content of the .ovpn file will be copied
OpenVPN App	There are two different apps for the use of OpenVPN We recommend the "OpenVPN for Android" app. But in the alternative, the "OpenVPN Connect" app can be used

Restrictions

Here you can set the restrictions, in relation to the connection management.

Allow Data Roaming	Allow mobile data while roaming
Force Data Roaming	If activated, roaming for mobile data is permanently activated (not recommended!) This setting overwrites the "Allow Data Roaming" setting!
Following settings are only available on Samsung KNOX 2.0 or higher	
Allow Emergency Calls Only	Allow Emergency Calls Only
Allow WiFi	Allow WiFi
WiFi Network Minimum Security Level	WiFi network minimum security level Open = all types of WiFi are permitted
Forbid user to add WiFi networks	The user may not add a WiFi network themselves This setting is only possible, if a WiFi profile was defined under "Connection Management"
Allow SMS & MMS	All = All SMS & MMS traffic is allowed Incoming SMS Only = Only incoming SMS messages are allowed Outgoing SMS Only = Only outgoing SMS messages are allowed None = No SMS / MMS traffic is allowed
Allow Sync during Roaming	Allow Sync during Roaming On = activated Off = deactivated User choice = user's choice
Allow Voice Roaming	Allow Voice Roaming On = activated Off = deactivated User Choice = user's choice
Use System http Proxy Server	The use of a HTTP proxy server, which is provided by the system's settings in settings, is dependent on the connected network (WiFi or APN)

APN

The following settings are only available on Samsung SAFE 2.0 or higher!

APN Display Name	APN Display Name	
Access Point Name	APN's Name	
Outgoing server protocol	Not set	
	None	
	PAP	PAP protocol
	CHAP	CHAP protocol
	PAP or CHAP	Either the PAP or CHAP protocol
MCC – Mobile Country Code	The MCC is entered here, leave this field blank, if the inserted SIM card's MCC should be used	
MNC – Mobile Network Code	The MNC is entered here, leave this field blank, if the inserted SIM card's MCC should be used	
Server address	Server address	
Server port number	Server port number	
Server proxy address	Server proxy address	
MMS server address	MMS server address, for Standard please leave blank	
MMS port number	MMS port number	
MMS proxy address	MMS proxy address	
User name	User name	
Password	Password	
Access Point Type	Allowed types are: "default", "mms", "supl" If this field is left blank, then "default,supl,mms" will be used	
Preferred APN	APN is preferred	

Bluetooth

Here, a variety of Bluetooth settings can be performed.

The following settings are only available on Samsung KNOX 1.0 or higher!

Allow Device discovery via Bluetooth	Allow device discovery via Bluetooth
Allow Bluetooth Pairing	Allow Bluetooth pairing
Allow Bluetooth Headset devices	Allow Bluetooth Headset devices
Allow Bluetooth Hands-free devices	Allow Bluetooth Hands-free devices
Allow Bluetooth A2DP devices	Allow Bluetooth A2DP audio streaming between devices
Allow Outgoing Calls	Allow outgoing calls viaBT
Allow Data Transfer via Bluetooth	Allow data transfer via Bluetooth
Allow Bluetooth Tethering	Allows using the device as a modem (Bluetooth internet connection)
Allow connection to Computer via Bluetooth	Allow connection to Computer via Bluetooth

PIM Management

Exchange

Only available for Samsung KNOX 1.0 or higher!

eMail Address	The provided user's email address Please note the "Placeholders", which you can use to work with credentials and you do not perform changes manually on every device With a click on **Show Placeholders** you can display them for yourself
Server Hostname	Server address of your Exchange Servers
Login name	The Login-Name for the respective end user device, please also note the "Placeholders here
Domain	Domain address
Password (only on device level)	Optionally, an individual device can be provided a password, should this remain empty, the user will be prompted to enter their Exchange Password
Number of previous days to sync	Number of days, determining when emails are sync'd back
Signature	A signature can be attached (Hint: Some devices require HTML formatting for the signature)
Default Account	Establishes, that this mail account is the standard account
Use Secure Sockets Layer (SSL)	Use a SSL connection
Use Transport Layer Security (TLS)	Use a TLS connection
Accept all certificates	All certificates are accepted. Please select this option, if your Exchange Server uses a self-signed certificate

eMail

Here, you can distribute IMAP and POP accounts to the respective end user devices.

The following settings are only available on Samsung KNOX 1.0 or higher!		
eMail Address	The provided user's email address Please note the "Placeholders", which you can use to work with credentials and you do not perform changes manually on every device With a click on **Show Placeholders** you can display them for yourself	
Incoming server protocol	Incoming server protocol	IMAP oder POP
Incoming server address	Incoming server address	
Incoming server port	Incoming server port	
Incoming server login/username	Incoming server login/username	
Incoming server password (only on device level)	Incoming server password (only on device level)	
Incoming server uses SSL	Incoming server uses SSL	
Incoming server uses TLS	Incoming server uses TLS	
Incoming server accept all certificates	Incoming server accept all types of certificates	
Outgoing server protocol	Outgoing server protocol	SMTP
Outgoing server port	Outgoing server port	
Outgoing Server uses extra credentials	Additional credentials for the outgoing server. If this set to "off", then the incoming server settings will be used	
Outgoing server login/username	Outgoing server login/username	
Outgoing server password (only on device level)	Outgoing server password	
Outgoing server uses SSL	Outgoing server uses SSL	
Outgoing server uses TLS	Outgoing server uses TLS	
Outgoing server accept all certificates	Outgoing server accepts all types of certificates	

Signature	A signature can be attached here (Hint: Some devices require HTML formatting for the signature)
Notify user on receiving new eMail	Notifies user on receiving new email

AE Gmail Exchange

Info: This Configuration will be applied to the Gmail app. So you have to approve and install Gmail.

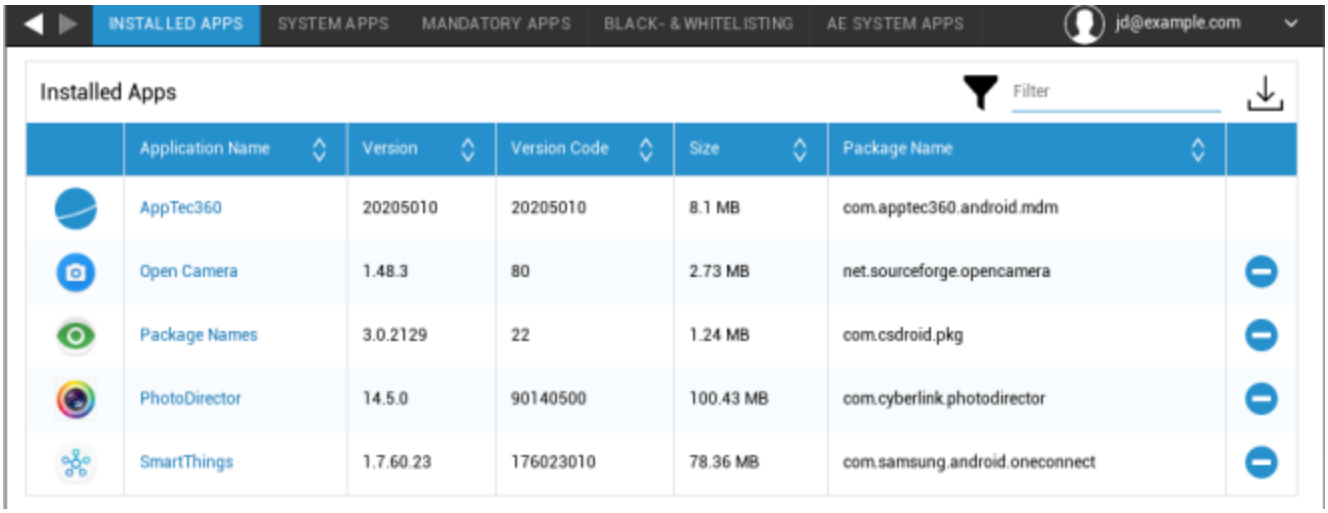
eMail Address	The provided user's email address Please note the "Placeholders", which you can use to work with credentials and you do not perform changes manually on every device With a click on Show Placeholders you can display them for yourself
Server Hostname	Server address of your Exchange Servers
Login name	The Login-Name for the respective end user device, please also note the "Placeholders here
Signature	A signature can be attached (Hint: Some devices require HTML formatting for the signature)
Number of previous days to sync	Number of days, determining when emails are sync'd back
Device Identifier	EAS Identifier. Keep this empty if your environment does not require this
Use Secure Sockets Layer (SSL)	Use a SSL connection
Accept all certificates	All certificates are accepted. Please select this option, if your Exchange Server uses a self-signed certificate
Allow unmanaged accounts	Allows the user to add additional accounts
Client Certificate	Upload client certificate if your Exchange server requires this

App Management

Enterprise App Manager

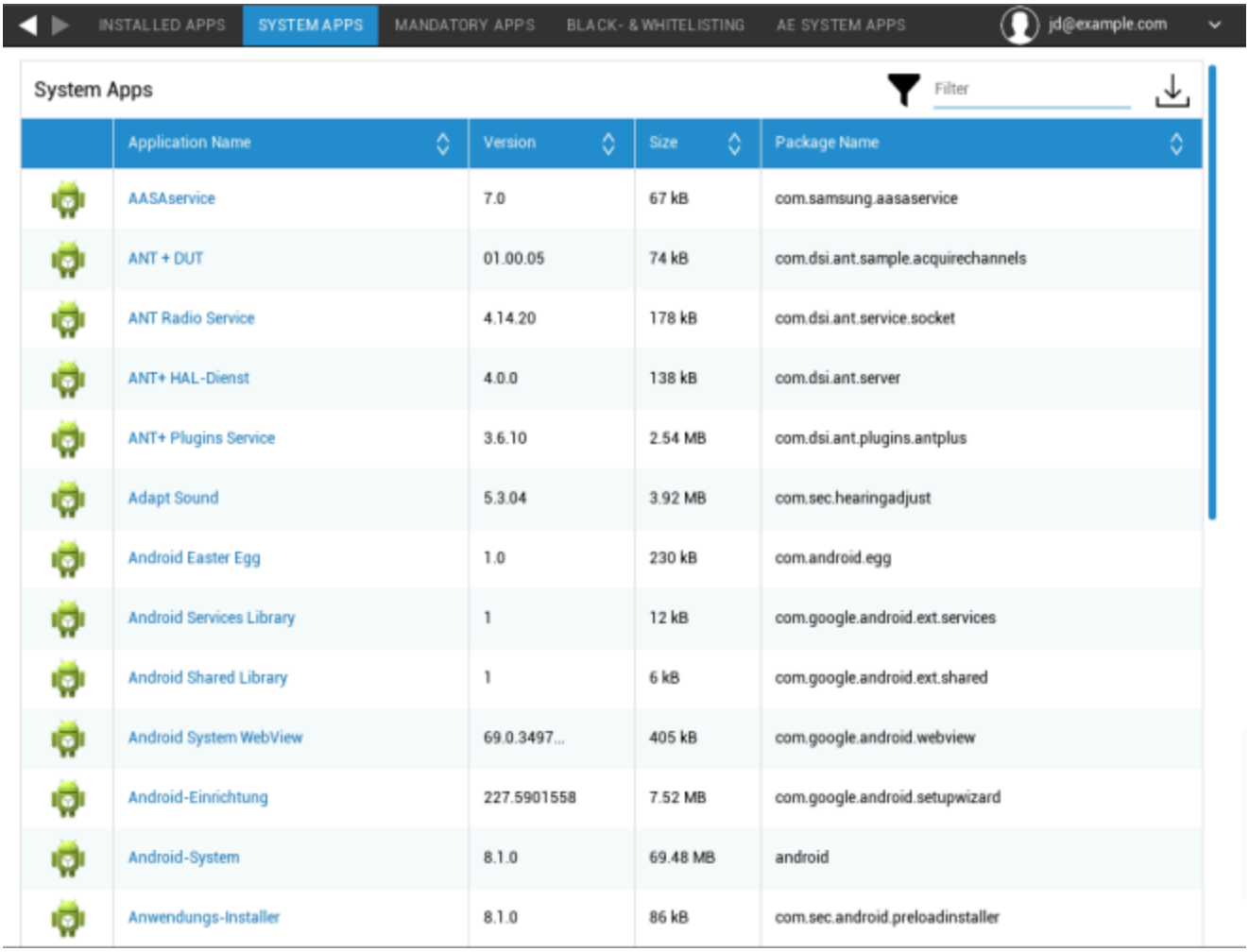
Installed Apps (only on device level)

Here all Apps will be displayed for you that are currently installed on the end user device.


INSTALLED APPS
SYSTEM APPS
MANDATORY APPS
BLACK- & WHITELISTING
AE SYSTEM APPS
jd@example.com
Installed Apps
Filter
Application Name
Version
Version Code
Size
Package Name
AppTec360
20205010
20205010
8.1 MB
com.apptec360.android.mdm
Open Camera
1.48.3
80
2.73 MB
net.sourceforge.opencamera
Package Names
3.0.2129
22
1.24 MB
com.csdroid.pkg
PhotoDirector
14.5.0
90140500
100.43 MB
com.cyberlink.photodirector
SmartThings
1.7.60.23
176023010
78.36 MB
com.samsung.android.oneconnect

System Apps (only on device level)

Under the “System Apps“, all of the pre-installed system will be listed with their package name and version.



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

Mandatory Apps

In Mandatory Apps you can define which apps have to be installed on the device. Depending on your configuration and device the app will be installed automatically or the user will be prompted to install it.

Please be aware that it is recommended to use Android Enterprise for easy app management.

The Scenarios are as listed below:

Normal Play Store Apps

Playstore App Installations always need a user interaction. Additionally a Google Account has to be configured on the device.

InHouse App Installation

On Samsung Devices these apps will be installed silently. Only exception is the container, where the user has to confirm the installation.

In any other scenario, the user has to confirm the app installation.

Android Enterprise Play Store Apps

These Apps will always be installed silently, without user interaction.

To Add a mandatory app, click on the “+” and select the desired app from the list. Please be aware that you cannot install apps from the “Google Play Store” Tab, if the device is configured with Android Enterprise either as fully managed or as container.

If using Android Enterprise, select the apps from the “AE Play Store” section. To make apps available here, confirm them in the Google Enterprise Play store by going to General Settings → AE Play Store → Play Store Apps.

When removing a mandatory app, it will also be uninstalled from the device.

You can click on the name of an app in the mandatory app list and go to the “configuration” tab to configure an app. This requires the usage of Android Enterprise and the app has to support this. Therefore the options available depend on the selected app.

AE System Apps

Here you can enable System Apps for the Android Enterprise devices. Please keep in mind that the specified app has to be in the storage of the system, otherwise nothing happens. 296

Restrictions & Settings

Black- & Whitelisting

Here you can define a black- or a whitelist. All apps on the blacklist will be blocked. All apps which are not in the whitelist, will be blocked. An empty blacklist blocks nothing, while an empty whitelist blocks everything*

**All mandatory apps and apps from the Enterprise App Store will be whitelisted automatically. You don't need to add them manually*

When clicking on the "+" you can either search for an app you want to add to your black- or whitelist or enter a package name manually.

Sys App Restrictions

Under "Sys App Restrictions" you can, amongst other things, block pre-installed apps and services, as you wish.

Disable Browser	Disable standard browser
Disable Calendar	Disable native calendar
Disable Calculator	Disable calculator
Disable Chrome Browser	Disable Chrome browser
Disable Clock	Disable clock
Disable Contacts	Disable Contacts
Disable Dialer	Disable native dialer
Disable eMail	Disable email
Disable Exchange	Disable Exchange accounts
Disable Facebook	Disable Facebook app
Disable Gallery	Disable native gallery app
Disable Gmail	Disable Gmail
Disable Google Books	Disable Google Books
Disable Google Play Kiosk	Disable Google Play Kiosk
Disable Google Maps	Disable Google Maps
Disable Google Music	Disable Google Music
Disable Google Movies	Disable Google Movies
Disable Google Play Store	Disable Google Play Store (public App Store)
Disable Google Plus	Disable Google Plus
Disable Google Search	Disable Google Search
Disable Google Talk / Google Hangouts	Disable Google Talk / Google Hangouts
Disable Music Player	Disable native music player app
Disable Settings	Disable device settings
Disable Sim Toolkit	Disable Sim Toolkit services
Disable SMS / MMS	Disable SMS / MMS
Disable Street View	Disable Street View services
Disable Youtube	Disable Youtube

Samsung Apps

Under “Samsung Apps“, you can define additional settings and/or restrictions for Samsung devices.

Disable AllShare Play / Samsung Link	Disable AllShare Play / Samsung Link
Disable ChatON	Disable ChatON
Disable Game Hub	Disable Game Hub
Disable Group Play	Disable Group Play
Disable Help	Disable Samsung Help
Disable KNOX	Disable Samsung KNOX Container
Disable Memo	Disable Voice Memo
Disable My Files	Disable My Files
Disable Optical Reader	Disable Optical Reader
Disable Polaris Office	Disable Polaris Office
Disable Readers Hub / Samsung Books	Disable Readers Hub / Samsung Books
Disable S Memo	Disable Samsung Memo app
Disable S Translator	Disable Samsung Translator app
Disable S Voice	Disable S Voice assistant
Disable Samsung Apps	Disable Samsung App Store
Disable Samsung Hub	Disable Samsung Entertainment Stores
Disable Video Player	Disable Video Player
Disable Voice Recorder	Disable Voice Recorder
Disable WatchON	Disable WatchON (simulates a remote control)

Huawei Apps

Under “Huawei Apps“, you can define additional settings and/or restrictions on Huawei device.

Disable DLNA	Disable DLNA
Disable App Installer	Disable App Installer
Disable File Manager	Disable File Manager
Disable Backup Manager	Disable Backup Manager
Disable System Updater	Disable System Updater
Disable Tool Box	Disable Tool Box
Disable Weather	Disable Weather
Disable FM Radio	Disable FM Radio

App Management Settings

Here you can define the update behavior of InHouse Apps.

Update Check Frequency defines how often the AppTec360 App looks for updates for InHouse apps. Once a new version has been detected, it will be downloaded and installed.

Wi-Fi Threshold defines if the download should be limited to Wi-Fi connections if the App is bigger than your configured Threshold. If the is smaller or you don’t define a threshold, the app will downloaded in Wi-Fi and in a cellular network.

Enterprise App Store

Please be aware that apps being added here (Enterprise App Store) will NOT make them get installed automatically on the device(s). The user has to open the Enterprise App Store on the device and install the app manually.

If you want to automatically install Apps on the device, please go to "App Management" → "Enterprise App Manager" → "Mandatory Apps" and add the desired apps there.

Under this point, you can distribute optional Apps to your users.

Playstore

Click on the “+” to add a play store app to the store. If using Android Enterprise please, go to “App Management Enterprise Play Store”. Also be aware that a Google Account has to be configured on → the device to install the apps defined here.

In-House

Under the point “In-House“, you can upload and distribute internally developed apps.

Click on the “+” to add an InHouse app to the enterprise app store which can then be installed by the user. In this dialogue you can also upload a new InHouse app.

Enterprise Play Store

Please be aware that apps being added here (Enterprise Play Store) will NOT make them get installed automatically on the device(s). The user has to open the Play Store on the device and install the app manually.

If you want to automatically install Apps on the device, please go to "App Management" → "Enterprise App Manager" → "Mandatory Apps" and add the desired apps there.

Under this point, you can distribute optional Apps to your users.

Here you can add Apps to the Android Enterprise Playstore. Please note that you have to approve Apps in General Settings → AE Play Store → Play Store Apps. These Apps will be added into the normal Google Play Store.

Also be aware that you first have to define a Layout with Apps in General Settings → App Management → AE Play Store → Store Layout.

Apps have to be in a Layout before you can successfully add them to the store.

Kiosk Mode & Launcher

Kiosk Mode

The Kiosk Mode allows you to pre-define an app or an URL. Then it will be exclusively possible to run/visit this app and or URL.

Likewise, various hardware buttons can be deactivated in the Kiosk Mode diverse.

Automatic Start	Automatically starts the Kiosk Mode, as soon as the profile reaches the end user device
Scheduled Kiosk Mode?	You can plan a time for the Kiosk Mode, this will then start and end automatically, at a time set by you
Start Time	Start time
Time in minutes	Time in minutes, after which the Kiosk Mode should end again

Application Type

Single App	If you want to start the App in the Kiosk Mode, select Package" under "Application Type"
Kiosk Application	Click here, in order to select an app that should be started in Kiosk Mode You will find the usual App Management's overview You can select between a "Google Play Store", "Android In-House Apps" and a "Packagename"

Application Type

URL	If you want to launch a URL in the Kiosk Mode, select "URL" under "Application Type" Then define your desired URL address
Clear browser after inactivity	Here you can define a time interval in minutes, after which the Kiosk Mode should be relaunched
Clear Web Cache and Cookies	If you activate this function, then after a restart of the Kiosk Mode, the Web Cache (cookies and cached pictures) will be erased
Same Origin Policy	Should this function be active, then the user can only surf the subpages of a defined URL For example, you defined the following URL:www.mypage.com Then, the user can surf on: www.mypage.com/subpage
Whitelisted URLs	Here you can maintain a Whitelist, all these URLs are allowed Maximum 1 URL per line A URL must start with http:/ or https://
Blacklisted URLs	Here you can maintain a Blacklist, all these URLs are not allowed Maximum 1 URL per line A URL must start with http:/ or https://
Screen Orientation	This setting relates to the screen adjustments Automatic = automatic Portrait = vertical format Landscape = landscape mode

Multi App	If you select the "Multi App" Kiosk Mode, the use of the AppTec360 Launcher will be enforced.
Apps	Application: Select a Playstore or an In-House App as Kiosk Application. It's also possible to enter a packagename. The selected Kiosk Application must be installed on the device. Remember to set the Kiosk Application as mandatory. Shortcut on Homescreen: If set to "On" a shortcut on the homescreen will be created. If set to "Off" the App will still show up in the App List.

Exit Password Enabled	If you activate this function, then it is possible for the user, to end the Kiosk Mode, with a password that has been predefined by you
Exit Password	This is the password, that was predefined by you
Auto Collapse Status Bar	If enabled, the Status Bar will automatically be collpased. With that option users can see the information at the Status Bar, but can't access it's functions
Disable Status Bar	The Status Bar contains Notifications, Shortcuts and Information. Only available for Samsung devices with KNOX 1.0 or greater.
Disable Volume Keys	Disable volume keys (only available on Samsung devices with KNOX 1.0 or higher)
Disable On / Off Switch	Disable On / Off switch (only available on Samsung devices with KNOX 1.0 or higher)
Disable Home Button	Disable Home button. If this function has been activated, then the Kiosk Mode can only be terminated in the AppTec360 Console (only available on Samsung devices with KNOX 1.0 or higher)
Disable Navigation Bar	With this you can disable the Navigation Bar (Back / Menu) If this function has been activated, then the Kiosk Mode can only be terminated in the AppTec360 Console (only available on Samsung devices with KNOX 1.0 or higher)

App Update Settings	
Allow App Updates	Users will be prompted to perform app updates even when Kiosk Mode is active. On devices with Samsung KNOX, apps will be updated silently.
Update Window	Set an interval where users will prompted to install app updates.

TeamViewer	
Enable Unattended Access	If enabled, administrators can remote control the device without user interaction. The app TeamViewer Host needs to be installed on the device.

AppTec360 Launcher

Enable AppTec360 Launcher	On: Enables the AppTec360 Launcher. The User has to set it as default Launcher one time. Note: If the Kiosk Mode is enabled, and the Kiosk Mode is set to "Multi App", the usage of AppTec360 launcher will be enforced.
Large Icons	On: Shows a larger Version of the App Icons in the Launcher
Hide AppTec360 App Icon	On: Hides the AppTec360 App completely
Hide AppTec360 Store Icon	On: Hides the AppTec360 Enterprise AppStore completely

AppTec360 Settings

Enable AppTec360 Settings App	The AppTec360 Settings App provides control over WiFi and Bluetooth connections
Enable Settings in Multi App Kiosk Mode	If enabled, users can access the AppTec360 Settings App while the Multi App Kiosk Mode is active

Remote Control

Splashtop

Shows the current status of the Splashtop Setup. Here you will see the steps you need to perform to remote access the device via Splashtop. Here you also need to enter your deploy code which you can get from the Splashtop website. The deploy code is required to connect to the device.

Teamviewer

Shows the current status of the Teamviewer Setup. Here you will see the steps you need to perform to remote access the device via Teamviewer.

Content Management

Contentbox

Here you can enable the Contentbox for this device. Once activated, the Contentbox App will be installed on the device.

Secure Browser

Here you can enable the Secure Browser for this device. Once activated, the Secure Browser App will be installed on the device. This Browser can be configured to offer a Web Browser on the device which is limited to your needs.

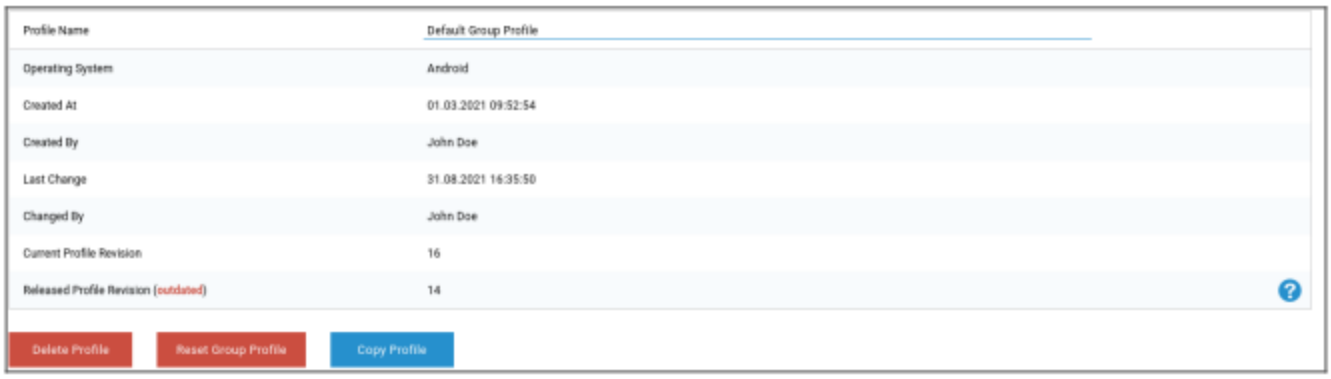
Require Password	Require the user to set up and use a password to access the browser.
Restrict Downloads / Open In	Blocks Downloads from Websites
Restrict Uploads	Restricts Uploads to certain URLs. Provide no URL to block the Upload entirely
Allow Copy	Allow copying, cutting or sharing text inside the web pages.
Allow Screen Capture	Allow capturing screenshots.
Data cleanup frequency	Select with which frequency, ALL the user data (history, cache etc.) should be automatically removed.
Company Bookmarks	The Bookmarks will show up in the "Company bookmarks" folder in the browsers bookmarks. They are not editable by the user.
Hide Address Bar	Hides the Address Bar so the User does not see the URL he is visiting
In-Browser Whitelisting (without Universal Gateway)	Enables client-side URL whitelisting. · Company Bookmarks are always whitelisted · Supported for 100 URLs only · Please use the Universal Gateway for unlimited Black- and Whitelisting
Gateway based Black- and Whitelisting	Blacklisting has the following requirements: · A working AppTec360 Universal Gateway ("General Settings" → "Universal Gateway") · A working VPN configuration with a specified DNS server ("General Settings" → "Universal Gateway" → "VPN Settings") · A Blacklist configuraton ("General Settings" → "Universal Gateway" → "Domain Blacklist") · A valid VPN connection in the profile ("Connection Management" → "VPN")

Configuration Windows 10 PC

General

Group profile overview (only on group level)

When opening a group profile, you will get a quick overview of the profile.



Profile Name	Name of the profile (can be changed here)
Operating System	Operating System the profile is for
Created At	Time of creation
Created By	The profile's creator
Last Change	Time of last change to the profile
Changed By	Account that made the last changes
Current Profile Revision	Revision of saved profile state
Released Profile Revision	Assigned profile revision ("Assign now"). If the label shows "(outdated)" behind the text, it means you've saved the profile but did not assign it yet, so the devices will still get and older version.

Device Overview (only on device level)

The device's summarized overview, which contains the following:

PC Name	Name of the PC
Client	The devices Windows type
Last Known Location	The latitude and longitude of the devices last known location
Assigned Mandatory Apps	Number of Mandatory Apps assigned to the device
PC UID	UID of the PC
OS Edition	Shows your Windows Edition
OS Version	Currently installed Windows Version
OS Build	Current Windows Build
Operating System	Currently installed Operating System
Serial Number	Serial Number of the Device
Device Ownership	The configured Ownership Type
Device Type	The Type of the Device
Rooted	Shows if the Device is rooted
Compliant	Shows if device is compliant
Last Seen	Date and time, when changes were made on the profile
User Assignment	Displays the user or group this device is currently assigned to. You can move the device by selecting a different user or group from the dropdown list.

Settings

Allow Auto Update	Allow or disallow automatical os updates.

Config Revision (only on device level)

Here you will receive an overview of which group profile is assigned to the device.

If you click on the group profile, you will access the profile directly and you can perform settings.

With the symbol, you can revert the assigned apps to the group profile's settings.

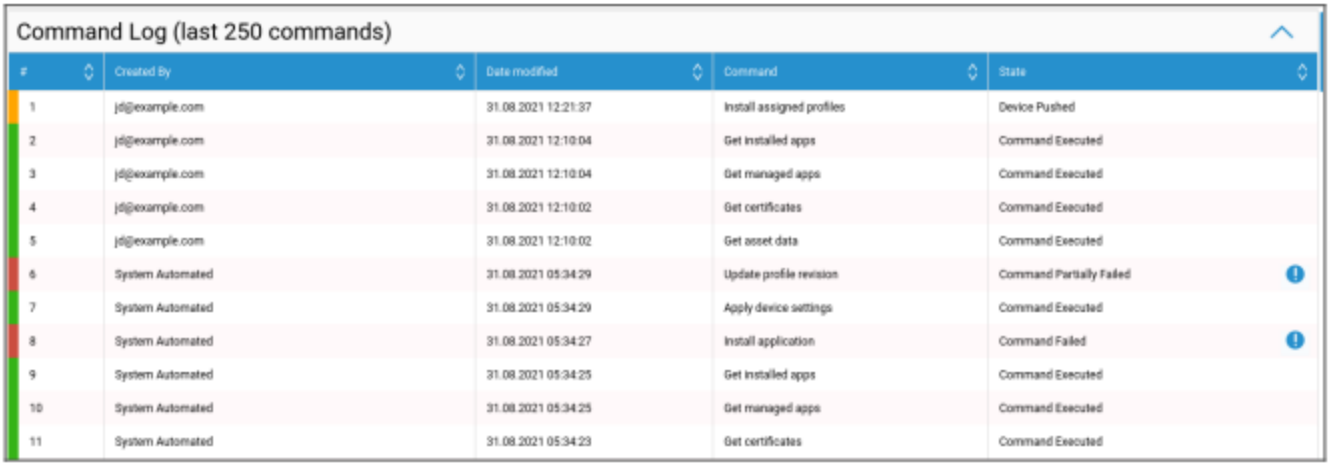
With the symbol, you can reset the device profile to have no settings at all.

“Newer Revision available“ indicates that the group profile has been changed and saved but not assigned. The group profile has to be assigned with “Assign now” on group level to apply the changes to the devices.

Device Log (only on device level)

Command Log

Here you can see which commands where issued for the device and what their status is.



Commands created by “System Automated” are automatically created by the system.

Possible command statuses

Device Pushed	A push request has been sent to the push service (e.g APNS) to tell the device to connect back to the EMM server.
Command Created	The command was created in the system.
Command Sent	The command got sent to the device after it connected to the server.
Command Executed	The command was successfully executed.
Command Failed	The command failed. *
Command Partially Failed	Depending on the device OS some commands may get grouped together. In this some parts of this command group failed. *
Command Executed, eventually Failed	The command was executed but maybe it wasn’t.
Command Repushed	The command was repushed by a user.
Discarded	The command was discarded. For example because it was superseded by another command or the device got re-enrolled and old commands got removed

*If there is an exclamation mark behind the message, you can get more information by hovering over the icon with your cursor.

Asset Management (only on device level)

Device Info

Manufacturer	Device manufacturer
Model	Device model
Model Number	Model Number
Operating System	Operating system
OS Version	OS version
Serial Number	Serial Number
ExchangeID	ExchangeID
Total RAM	Total RAM
Display Resolution	Display resolution
Phone Language	Device language
Firmware Version	Firmware version
DM Client Version	Device Management Client version
Hardware Version	Device hardware version
CPU Architecture	CPU Architecture (processor type)

Cellular

SIM Carrier Network	Carrier network
Phone Number	Phone Number
Roaming Status	Roaming Status
IMEI	IMEI
IMSI	IMSI
Modem Firmware	Modem Firmware

Synchronization Info

Instant DM Connection	The device should immediately create a connection to AppTec
Initial Retry Time	Initial retry time for this first connection
Connection Retries	Number of new connection retries, after a disconnection from the Connection Manager or a WinInet-level error
Maximum Sleep Time	Maximum sleep time after package-sending error
First Sync Retries	Time for the first stage after the enrollment
First Retry Interval	Time for the first stage after the enrollment
Second Sync Retries	Time for the second stage after the enrollment
Second Retry Interval	Time for the second stage after the enrollment
Regular Sync Retries	Time for the additional stages after the enrollment
Regular Retry Interval	Time for the additional stages after the enrollment

Security Management

Anti Theft (only on device level)

GPS Information (only on device level)

Here you can establish the current/last device location. The localizing can be protected with one or even two passwords – See: „General Settings“ > „Privacy“ > „GPS Access“

GPS Settings

Enable GPS Tracking	Enable regular synchronization of GPS information.
Tracking Interval	Set the GPS information synchronization interval.

Security Configuration

Passcode

Minimum Password Length	Minimum password length	
Password Composition	Specifies the number of specific characters the password must contain These are comprised of capital letters, lower case letters, numbers and special symbols	
Password Quality	Here you can set the password quality	
	Alphanumeric	Only numbers and letters
	Numeric	Only numbers
	Numeric or Alphanumeric	Numbers or numbers and letters
Maximum Inactivity Time Lock	Number of minutes of user inactivity on the device, after which the device will be locked. The user must unlock the device after this time, by entering their device password.	
Password Expiration	Set the time till a new password must be set	
Password History Restriction	Number of previously used passwords, that are not allowed	
Maximum Failed Password Attempts	Number of times that the password can be entered incorrectly, before a complete wipe of device is performed	

Antivirus

Antivirus settings - Set scan configuration	
Type of scan	Selects whether to perform a quick scan or full scan
Set scan start	Selects the time of the day that Windows Defender will start the scanning
Scan frequency	Selects the day that Windows Defender scan should run
Signature update frequency	Speciefies the interval in hours that will be used to check for signatures

Config type of files for scanning	
Allow scanning of archive files	Allow or disallow scanning of archives (such as .zip) when being accessed.
Allow scanning of scripts	Allows or disallow Windows Defender Script Scanning functionality.
Allow scanning of emails	Allow or disallow scanning of emails.
Allow scanning of network files	Allow or disallow scanning of network files.
Allow full scanning of mapped network drives	Allow or disallow scanning of mapped network drives (only enabled when full scan is enabled).
Control bidirectional scanning	Controls which sets of files should be monitored.
Allow full scanning of removable drives	Allow or disallow full scanning of removable drives. Only during full scan is initiated.

Type of files to be excluded of scan	
Ignore file types for scanning	Define a set of type of files extensions. Each file extension for each field.
Ignore directory paths	Define a set of directory paths in order to not scan them. One path per field. Examples: "C:\Example", "C:\Windows" or "C:\Users".
Exclude processes from scan	Exclude files that have been opened by specific processes from Microsoft Defender Antivirus scans. . One path per field. Examples: "C:\myFile.exe", "C:\Windows\myProcess.exe", "C:\myScript.bat

Extra Settings	
Allow Realtime monitoring	Allow or disallow Windows Defender Realtime Monitoring functionality
Allow Behavior monitoring	Allow or disallow Windows Behavior Monitoring functionality
Allow Cloud Protection	Allow or disallow Windows Defender send information to Microsoft about any problem it finds. Microsoft will analyze that information, learn more about the problem affecting the device, and offer improved solutions
	Behaviour for sending samples
Allow Windows Defender IOAV protection	Allow or disallow Windows Defender IOAV protection
Allow access to Defenders "On Access protection" UI	
Average CPU load factor	Represents the average CPU load factor for the Windows Defender scan (in percent)

Malware handling	
Low severity	You can define for each severity level how the device handles malware. Available options are: • Clean • Quarantine • Remove • Allow • User defined • Block
Moderate severity	
High severity	
Severe severity	
Days to retain cleaned Malware	Time period in days that quarantine files/items will be stored on the system. The default value is 0, which keeps items in quarantine, and does not automatically remove them. Max value is 90.

Security Center

Windows Security Center - Settings for Windows Security	
Disable Virus & threat protection UI	
Hide Ransomware Data Recovery UI	
Disable Account protection UI	
Disable Firewall and Network protection UI	
Disable App and Browser control UI	
Disallow changes to Exploit protection	Disallow user to make changes to Exploit protection settings
Disable Device security UI	
Hide TPM troubleshooting	Hide TPM troubleshooting settings
Disable Clear TPM button	
Disable device performance and health UI	
Disable family options UI	

Customize Toasts	
Enable customized support info	Enable to display customized support contact info for your company in the bottom right of the security center app.
E-Mail address	Set company's email address
Company name	Set company's name
Company phone	Set company's phone
Help URL	Set company's help URL

Extra Settings	
Disable notifications	Disable the display of Windows Defender Security Center Notifications.
Hide TPM firmware update recommendations	Hide the recommendation to update TPM Firmware when a vulnerable firmware is detected.
Display company name and contact options	Display your company name and contact options in a contact card fly out in Windows Defender Security Center.
Hide Secure Boot	Hide Security Boot area.
Hide Security notification area control	Hide Windows Security notification area control.

Firewall Configuration

Firewall configuration - Global settings	
Ignore authentication set	Ignore the entire authentication set if they do not support all of the authentication suites specified in the set
Type of packet queueing	Specifies how scaling for the software on the receive side is enabled for both the encrypted receive and clear the forward path for the IPsec tunnel gateway scenario.
Disable perform stateful FTP filtering	If it is disabled, it won't performs stateful File Transfer Protocol (FTP) filtering to allow secondary connections
Security association idle time	This field configures the security association idle time, in seconds. Security associations are deleted after network traffic is not seen for this specified period of time.
Preshared key encoding	Set the preshared key encoding
IPSec Exceptions	Configure Internet Protocol exceptions
Certificate revocation list check	

Firewall Profiles (Domain Profile / Private Profile / Public Profile)	
Enable Firewall for this profile	
Disable notifications	Disable displaying notification to the user when an application is blocked from listening on a port.
Block unicast responses to multicast broadcasts	
Enforce authorized application firewall rules	If it is not enforced, authorized application firewall rules in the local store are ignored and not enforced
Enforce global port firewall rules	If it is not enforced, global port firewall rules in the local store are ignored and not enforced. The setting only has meaning if it is set or enumerated in the Group Policy store or if it is enumerated from the GroupPolicyRSoPStore
Enforce firewall rules	If it is not enforced, firewall rules from the local store are ignored and not enforced
Enforce connection security rules	It it is not enforced, connection security rules from the local store are ignored and not enforced
Default outbound action	The action that the firewall does by default on outbound connections
Default inbound action	The action that the firewall does by default on inbound connections
Disable Stealth mode	Stealth mode is a mechanism in Windows Firewall that helps prevent malicious users from discovering information about network computers and the services that they run.
Disable preventing from responding to unsolicited traffic	If disabled, the firewall's stealth mode rules must not prevent the host computer from responding to unsolicited network traffic if that traffic is secured by IPsec

Firewall Rules

Firewall Rules	
Name	Name of the rule
Description	Description of the rule
Action	Specify whether this rule will block the traffic, or allow it. Please consider that the Block option could also block the traffic (depending of the rest of the configuration) between the MDM server and the Device
Direction	
Enable Edge traversal (Only available when **Direction** is set to **inbound traffic**)	Indicates that specific inbound traffic is allowed to tunnel throughout NAT's and other edge devices using the Teredo tunneling technology.

Programs & services	
Define applications, all otherwise	If not enabled, then it will consider all applications
Package Family Name	The Package Family Name that the rule will apply to.
File path of the application	The full application such as C:\Windows\System\Notepad.exe that the rule will apply to
Fully Qualified Binary Name	The Fully Qualified Binary Name that the rule will apply to. A FQBN is a string in the following form: {Publisher\Product\Filename,Version}
Service Name	Enter the name of a Service (e.g "EventLog"). You can get a list of Service Names on Powershell by running the command "Get-Service".

Protocols & ports				
Protocol	The protocol used by the rule.			
	Available values: - Any - Custom - HOPORT - ICMPv4 - IGMP - TCP - UDP - IPv6 - IPv6-Route - IPv6-Frag - GRE - ICMPv6 - IPv6-NoNxt - IPv6-Opts - VRRP - PGM - L2TP	When set to Custom	Insert a protocol number between 0 and 255	The protocol number
		When set to TCP or UDP	Specify local ports, all will be used otherwise	Local ports that the rule will use, range ports are also allowed
			Local Port	Single port or a range of ports. E.g. 100-120,200,300-320.
			Specify remote ports, all will be used otherwise	Remote ports that the rule will use, range ports are also allowed
			Remote Port	Single port or a range of ports. E.g. 100-120,200,300-320.

Scope	
Specify local IPs, any IP otherwise	Set of local IPs, it can be also a range of IPs separated by -
Local IP address	Set of single IPs or a range of IPs separated by -
Specify remote IPs, any remote IP otherwise	Specify a set of remote IPs, it can be also a range of IPs separated by "-".
Remote IP address	Specify single IPs or a range of IPs
Tokens	Tokens that can be set along with Remote Addresses. Tokens Intranet, RmtIntranet and Ply2Renders are supported in Windows 10, version 1809 and later.

Advanced Settings	
Specify profiles, all will be used otherwise	If disabled all profiles will be used

Domain	Domain Profile
Private	Private Profile
Public	Public Profile
Specify interfaces, all will be used otherwise	If disabled all interfaces will be used
Local Area Network	Local Area Network interface
Remote Access	Remote Access interface
Wireless	Wireless interface

Local Principals	
Add authorized local users	Allow to add a list of local users that will use this rule
Authorized users	List of authorized local users for this rule. The user must be in Security Description Definition language (SDDL) format, e.g. PC_NAME\USERNAME. This field must not be filled if a service name is set to use this rule

Restriction Settings

Device Functionality

Allow SD Card	Allow the use of a SD card
Allow Camera	Allow the use of the camera
Allow Location Service	Allow device location service
Allow App Sideloading	Allow installation of Apps from unknown sources
Allow Developer Mode	Allows developer mode
Allow Cellular Data Roaming	Allow cellular data roaming
Allow Cortana	Allow voice assistant Cortana
Allow Search to use Location	Allow search to use location
Allow Adding Non Microsoft Email Account	Specify whether the user is allowed to add non MSA email accounts.
Allow Microsoft Account Connection	Specify whether allow using MSA account for non email related connection authentication and services.
Allow Sync My Settings	Allows the synchronizing of settings across the entire device
Enterprise Protected Domain Names	Specifies the enterprise domain names seperated by ";".
Allow User to disable System Restore	Allows the user to disable System Restore. **WARNING!** This feature should only be used on devices that are owned or provided by the enterprise company or organization or on a user owned device, where the user allows that the device will be fully managed by the enterprise company. If you disable this policy setting, System Restore is turned off, and the System Restore Wizard cannot be accessed. The option to configure System Restore or create a restore point through System Protection is also disabled.

Allow User Unenrollment	Allows the user to remove the corporate part from the device and thereby disconnect from the AppTec360 Servers. Should this happen, it will no longer be possible to manage the device **WARNING!** This feature should only be used on devices that are owned or provided by the enterprise company or organization or on a user owned device, where the user allows that the device will be fully managed by the enterprise company. If you disable this policy setting, users will not be able to remove MDM enrollments. Specify whether the user is allowed to delete the workplace account via workplace control panel. The MDM server always could remotely delete the account.

BitLocker

BitLocker Configuration

General Settings	
Require device encryption	Prompt users to enable device encryption.Depending on the Windows edition and system configuration, users may be asked: - To confirm that encryption from another provider isn't enabled. - To turn off BitLocker Drive Encryption and then turn BitLocker back on.
Encryption methods	
Encryption method for operating system drives	
Encryption method for fixed data-drives	
Encryption method for removable data drives	
Disable warning about third-party disk encryption	Disable the warning prompt about a third-party disk encryption service being used on the device. Starting in Windows 10, version 1803, this setting is only supported for Azure Active Directory joined devices.
Allow running encryption while non-administrator user is logged in	Only supported for Azure Active Directory joined devices

AppTec360 Extensions	
Silent encryption	If selected along with "Require device encryption", the AppTec360 Management Service will run automatic silent encryption of the device drives.
Automatically generate user credentials	The encrypted OS drive will be protected with automatically generated user credentials. Either a TPM PIN, when a TPM is available or a 6 digit textual password. The generated credentials are sent to the email address registered for given device. If this option is turned off, the only possible protection for silent encryption is using TPM. In that case, for devices without a TPM, silent encryption will fail.
Encrypt fixed drives	Any available fixed data drives will be also encrypted and protected with "Automatic Unlock" using a key stored on the OS drive.

OS Drive Settings	
Require additional authentication at startup	This setting allows you to configure whether BitLocker requires an authentication each time the computer starts. This setting is applied during the setup of BitLocker. If you enable this setting, users can configure advanced startup options in the BitLocker setup wizard.
Block BitLocker without a compatible TPM	
TPM only	
TPM and PIN	
TPM and key	
TPM, key and PIN	If you want to require the use of a PIN and a USB flash drive (key), the user must setup BitLocker using the command-line tool "manage-bde" instead of the BitLocker Drive Encryption setup wizard.

Require Minimum PIN length	
Minimum characters	

Configure pre-boot recovery message and	Configure the entire recovery message or replace the existing URL that is displayed on the pre-boot key recovery screen when the OS drive is locked.

URL	Note: Not all characters and languages are supported in pre-boot. It is strongly recommended that you test that the characters you use appear correctly on the pre-boot recovery screen.
	Pre-boot recovery message option
	Custom recovery message
	Custom recovery URL

OS drive recovery options		This setting allows you to control how BitLocker-protected operating system drives are recovered in the absence of the required credentials. This setting is applied during the setup of BitLocker. By default a Certificate-based data recovery agent is allowed, the recovery options can be specified by the user including the recovery password and recovery key and recovery information is not backed up to AD DS.
	Block Certificate-based data recovery agent	Specify whether a data recovery agent can be used with BitLocker-protected operating system drives. Before a data recovery agent can be used it must be added from the Public Key Policies item in either the Group Policy Management Console or the Local Group Policy Editor. Consult the BitLocker Drive Encryption Deployment Guide on Microsoft TechNet for more information about adding data recovery agents.
	BitLocker recovery password settings	
	BitLocker recovery key settings	
	Save BitLocker recovery information to Active Directory Domain Services	
	AD DS BitLocker recovery storage configuration	Storing the key package supports recovering data from a drive that has been physically corrupted.
	Require storage of recovery data to AD DS	Prevent users from enabling BitLocker unless the computer is connected to the domain and

Fixed Drive Settings	
Fixed drives recovery options	This setting allows you to control how BitLocker-protected fixed drives are recovered in the absence of the required credentials. This setting is applied during the setup of BitLocker. By default a Certificate-based data recovery agent is allowed, the recovery options can be specified by the user including the recovery password and recovery key and recovery information is not backed up to AD DS.
Block Certificate-based data recovery agent	
BitLocker recovery password settings	
BitLocker recovery key settings	
Save BitLocker recovery information to Active Directory Domain Services	
AD DS BitLocker recovery storage configuration	Storing the key package supports recovering data from a drive that has been physically corrupted.
Require storage of recovery data to AD DS	Prevent users from enabling BitLocker unless the computer is connected to the domain and the backup of BitLocker recovery information to AD DS succeeds. Note: The recovery password is automatically generated.
Deny write access to unprotected fixed drives	

Removable Drive Settings	
Deny write access to unprotected removable drives	Deny write access to removable data drives which are not protected by Bitlocker. Note: If "Removable Disks: Deny write access" is enabled in the group policy, this policy setting will be ignored.
Deny write access to devices configured in another organisation	Only drives with identification fields matching the computer's identification fields will be given write access. These fields are defined by the "Provide the unique identifiers for your organization" group policy setting.

BitLocker State

Here you can see the current state of BitLocker encrypted drives

C [OS Drive]
Encryption Status
Encrypted (%)
Protection Status
Encryption Method
Key Protectors
Recovery Password

With a click on the button „Rotate recovery password“ you can rotate the BitLocker recovery password.

Certificate Management

Certificate List

Here is a list of certificates that are installed on the device being displayed.

Certificate Configuration

Here you can configure certificates and how they will be installed on the device.

Trusted certificate	
Description	Certificate description
Scope	Certificate deployment scope: Current User vs Device
Certificate store	"Untrusted Certificates" is only available starting Windows 10, version 1803
Certificate file	Upload a PKCS#1 file

Identity certificate			
Description	Certificate description		
Scope	Certificate deployment scope: Current User vs Device		
Key location	The Key Storage Provider to install the private key to.		
		TPM. Fail if no TPM present	
	TPM. If no TPM present, fallback to Software KSP		
	Software Key Storage Provider	Mark private key as exportable	
	Windows Hello for Business	Container name	Specifies the Windows Hello for Business (formerly known as Microsoft Passport for Work) container name.
		PIN prompt text	Specifies the custom text to show on the Windows Hello for Business PIN prompt during certificate enrollment.
Credential	Upload a PKCS#12 File		

SCEP

Description	SCEP Server description		
Deployment Scope	Certificate deployment scope: Current Device vs User		
SCEP Server URLs	One or more servers that issue certificates through SCEP		
Subject	Representation of a X.500 name. E.g. "C=US, O=Microsoft Corporation, CN=foo, 1.2.5.3=bar"		
Subject alternative names	Type	Email address	
		DNS	
		URI	
		User Principal Name (UPN)	
CA Fingerprint	The SHA1 fingerprint of the Certificate Authority certificate. E.g. 31:8F:1E:78:5C:D5:12:9F:7E:3B:AD:F3:1C:C0:19:03:96:43:A9:E5		
Validity period units	Days, Months or Years		
Validity period			
Challenge	Used as the pre-shared secret for automatic enrollment		
Retries	The number of times the device should retry if the server sends a PENDING response. The default value is 5. Maximum value is 30.		
Retry delay	Number of minutes to wait before retry. The default value is 5. The minimum value is 1.		
Key size	Key size in bits		
Hash algorithm	Hash algorithm family		
Key usage	The key usage extension defines the purpose (e.g., encipherment, signature) of the key contained in the certificate. At least one of the "Digital signature" or "Key encipherment" needs to be selected.		
Extended key usage	Specifies extended key usages.Subject to SCEP server configuration. Specify the list of corresponding OIDs, e.g. 1.3.6.1.5.5.7.3.2 (Client Authentication)		
Key location	The Key Storage Provider to install the private key to.		
		TPM. Fail if no TPM present	

	TPM. If no TPM present, fallback to Software KSP			
	Software Key Storage Provider			
	Windows Hello for Business	Container name	Specifies the Windows Hello for Business (formerly known as Microsoft Passport for Work) container name.	
		PIN prompt text	Specifies the custom text to show on the Windows Hello for Business PIN prompt during certificate enrollment.	

Connection Management

Wifi

At this setting, perform the pre-configuration of the end user devices for access to internal Access Points

Service Set Identifier (SSID)	SSID to the network, to which the connection will be established
Auto Join	Activate auto join to the network
Hidden Network	Activate, in case the AP does not broadcast the SSID

Security Type

Establish AP security type

WEP Open System	
Password	Password for the AP

WPA PSK	
Password	Password for the AP

WPA EAP	
Authentication Type	Authentication type, only possible with "PEAP-MSCAHPv2"
Fast Reconnect	Devices can switch between Access Points, without having to authenticate itself again
Guest Access	The user does not have an account and should therefor register as a guest
Quarantine Checks	The client must perform NAP (Network Access Protection) Checks and share the results with the system, that then decides, if the client can connect
Require Crypto Binding	Authentication is only possible via Crypto Binding
Server Validation	The client checks, if the server certificate is valid. If this is the case, a connection will be established
Prompt for Certificates	Allows the user to accept non-trusted certificates
Server Names	Offers the option to display the name of the RADIUS-Server, that offers the network authentication and authorization

WPA2-PSK	
Password	AP password

WPA2 EAP	
Authentication Type	Authentication Type, only possible with "PEAP-MSCAHPv2"
Fast Reconnect	
Guest Access	
Quarantine Checks	Activates the network access protection NAP
Require Crypto Binding	Authentication is only possible via Crypto Binding
Server Validation	
Prompt for Certificates	Prompts for a validated server certificate, name or a Root certificate authentication (CA)
Server Names	Listing of the servers that should be trusted by the devices
None	No established security
Use Proxy Server	Use of a proxy server
Server Address	Proxy server address
Server Port	Proxy Server's Server Port

Use Proxy Server

Enable proxy server usage.

Server Address	Proxy server address used by this network.
Server Port	Proxy server port used by this network.

Wifi Restrictions

Here you can define various Wifi restrictions.

Allow WiFi	Allow/deny WiFi
Allow Internet Sharing	Allow use of a Hotspot
Allow Auto Connect to WiFi Sense Hot Spots	Allow Auto Connect to WiFi Sense Hot Spots
Allow Manual WiFi Configuration	Allow the user to connect to WiFi networks, that have not been defined by AppTec
WLAN Scan Frequency	Establishes the WLAN-Scan interval. Here, a higher value raises the ability to recognize WIFI networks.

VPN

Perform the appropriate settings here, in order to configure VPN connections

Connection Name	Indicated connection name		
VPN type	A Per-App VPN connection is used to secure the traffic of certain Apps.		
	VPN	Always On	This will automatically connect the VPN at sign-in and will stay connected until the user manually disconnects.
	Per-App VPN	VPN Apps	Define Apps that use this VPN Connection
		Per-App Lockdown	Per-App Lockdown makes the selected apps to only have connectivity through this VPN connection. This feature depends on Windows Defender Firewall.
	WIP profile	WIP domain for this connection	Enterprise ID, which is required for connecting this VPN profile with a Windows Information Protection (WIP) policy

Connection type

AppTec360 VPN	
For "AppTec360 VPN" it is required that app sideloading is allowed. Please enable "Allow App Sideloading" in "Security Management" → "Restriction Settings" → "Device Functionality".	
Gateway Configuration	To configure a VPN connection with blacklisting, please select a VPN configuration with a specified DNS server. You can set up a VPN configuration in "General Settings" → "Universal Gateway" → "VPN Settings".

IKEv2		
Servers	List of VPN servers	
Device Tunnel	Enable connection before user logon.	
Authentication method	EAP	EAP XML
	Machine Certificates	
Encryption algorithm		
Integrity check algorithm		
Diffie-Hellman group		
Cipher transform algorithm		
Authentication transform algorithm		
Perfect forward secrecy (PFS) group		

PPTP		
Servers	List of VPN servers	
Authentication method	EAP	EAP XML

L2TP		
Servers	List of VPN servers	
Authentication method	EAP	EAP XML
Encryption algorithm		
Integrity check algorithm		
Diffie-Hellman group		
Cipher transform algorithm		
Authentication transform algorithm		
Perfect forward secrecy (PFS) group		

Automatic		
Servers	List of VPN servers	
Authentication method	EAP	EAP XML

Generic VPN Configurations

Remember credentials at each logon	
Register IP addresses with internal DNS	
Network traffic filtering rules	Limit VPN connection to the defined set of rules.
DNS suffix search list	DNS suffixes to add to the DNS search list for routing short names.
Name Resolution Policy Table (NRPT) rules	Name Resolution Policy table (NRPT) rules define how the DNS resolves names when connected to the VPN.
Trusted network detection	List of DNS suffixes for identifying trusted network.
Split tunneling	Split tunneling means traffic can go over any interface as determined by the networking stack.
Split tunneling routes	List of routes to be added to the routing table for the VPN interface.
Proxy setup	Configures Proxy used with this network
Proxy Address	Proxy server address as a fully qualified hostname or an IP address.
Port	Proxy server port.
Proxy Auto-Config URL	URL to automatically retrieve the proxy settings.

VPN Restrictions

Here you can define various VPN restrictions.

Allow VPN Settings	This guideline allows/forbids the user to deactivate and change the VPN settings
Allow VPN over Cellular	Allows/forbids the device to establish a VPN connection, if the device is using mobile data
Allow VPN Roaming over Cellular	Allows/forbids the device to establish a VPN connection, if the device is roaming

Bluetooth

Here you can establish, if Bluetooth should be allowed/forbidden.

Allow Bluetooth	Activate/deactivate Bluetooth

PIM Management

Exchange Active Sync

Set up of the ActiveSync account on the end user device

Account Name	Email account name
Server Host Name	Server address/FQDN
Domain Name	Server domain
Email Address	Email address
User Name	User name
User Password	Optionally, you can already attach a password to the user here
Use SSL	Use SSL connection
Sync Interval	Here the synchronization interval can be established Manual sync = The user must download their emails and perform a manual synchronization
Mail Age Filter	Amount of time, until the emails should be synchronized No filter = unlimited
Log Level	Establishment of the logging levels for the ActiveSync traffic
Sync Email	Activated = emails are synchronized
Sync Contacts	Activated = contacts are synchronized
Sync Calendar	Activated = calendar is synchronized
Sync Tasks	Activated = tasks are synchronized

eMail

Establishment of POP3/IMAP4 accounts on the end user device.

Account Description	Email account name
Sender Name	Displayed sender name
Domain Name	Domain name for the email account
Email Address	User email address
User Name	User name
User Password	Optionally, you can already attach a password to the user here
Alternative Outgoing Server Credentials	Here it can be defined, if other credentials are required for the outgoing server
Outgoing Domain Name	Outgoing domain name
Outgoing Server User Name	Outgoing server user name
Outgoing Server Password	Outgoing server password
Email Protocol	POP3 or IMAP4, can be used as a protocol
Incoming Mail Server Host Name	Incoming mail server host name
Use SSL for Incoming Mails	Use SSL for incoming emails
Outgoing Mail Server Host Name	Outgoing mail server host name
Use SSL for Outgoing Mails	Use SSL for outgoing emails
Outgoing Server Authentication	An outgoing server authentication is required
Sync Interval	Here the synchronization interval can be established Manual sync = The user must download their emails and perform a manual synchronization
Mail Age Filter	Amount of time, until the emails should be synchronized No filter = unlimited

App Management

Enterprise App Manager

Installed Apps

Here is a list of the apps that are currently installed on the device being displayed.

Mandatory Apps

Here you can configure a list of apps that are mandatory on the device.

This list will be checked every time the device connects to the MDM and install all apps on this list that happen to be not installed on the device, regardless of whether the app was uninstalled or it never was installed before.

You can upload Windows 10 In-House Apps and then add them to this list or you can add Microsoft Office configurations which need to be configured beforehand in „General Settings“ > „App Management“ > „Microsoft Office“.

Sys App Restrictions

Inbox Apps
Allow Alarms and Clock
Allow Calculator
Allow Camera
Allow Contact Support
Allow Cortana
Allow File Explorer
Allow Get Started
Allow Groove Music
Allow Maps
Allow Messaging
Allow Microsoft Edge
Allow Movies And TV
Allow Money
Allow News
Allow OneDrive
Allow OneNote
Allow Outlook Calendar And Mail
Allow People
Allow Phone
Allow Photos
Allow Powerpoint
Allow Settings
Allow Skype
Allow Sports
Allow Store
Allow Voice Recorder
Allow Wallet
Allow Weather

Allow Windows Feedback Hub
Allow Word
Allow Xbox

Setting Pages
Allow Accounts Workplace
Allow Advanced Info
Allow Apps Corner
Allow Block And Filter
Allow Colour Profile
Allow Driving Mode
Allow Email And Accounts
Allow Equalizer
Allow Keyboard
Allow Navigation Bar
Allow Network Airplane Mode
Allow Network Internet Sharing
Allow Network Services
Allow Network Wi-Fi
Allow PC System Bluetooth
Allow Rate Your Device
Allow Restore Update
Allow Sharing
Allow Start
Allow Time Language
Allow Time Region
Allow Windows Default Lock Screen
Allow Work Or School Account

Black- & Whitelisting

Under “Black- & Whitelisting“, you can choose between the Mode “Whitelist“ and the Mode “Blacklist“.

Whitelist	Only apps and services, that are added to the list can be installed on the end user device. If these are already pre-installed on the end user device they will be activated and set, so that the user can run them.
	All other apps that are not added to the list cannot be installed on the end user device. If these are already pre-installed on the end user device they will be deactivated and set, so that the user cannot run them.
Blacklist	Apps and services, that are added to the list cannot be installed on the end user device. If these are already pre-installed on the end user device they will be deactivated and set, so that the user cannot run them.
	All other apps that are not added to the list can be installed on the end user device. If these are already pre-installed on the end user device they will be activated and set, so that the user can run them.

Via the , you add additional apps or services to the currently used list.

Via the , you add additional apps or services to the currently inactive list.

You can either add an app from the „Windows App Store“ or directly enter an „App Identifier“ to add to the black- or whitelist.

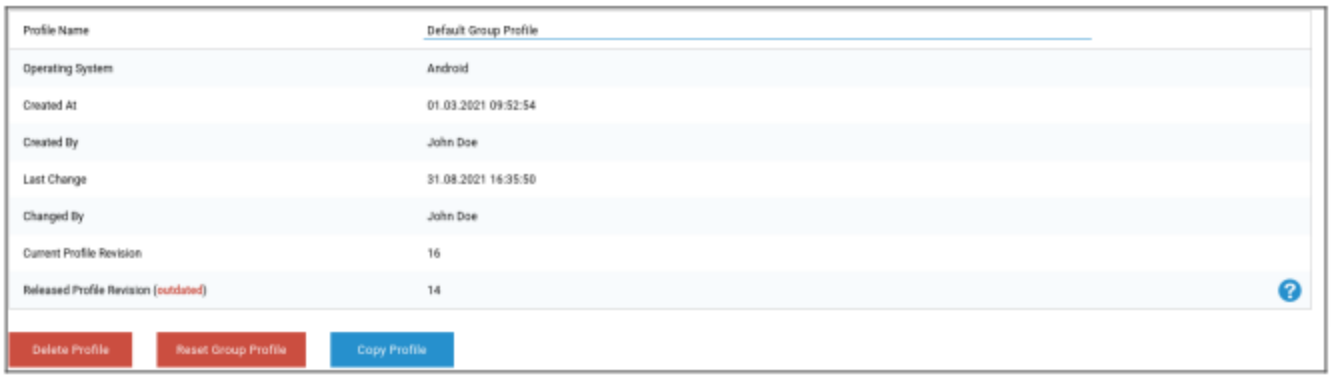
MacOS Configuration

Depending on whether you have selected a profile or a device, the display and its sub-points are different – please pay careful attention to this!

General

Group profile overview (only on group level)

When opening a group profile, you will get a quick overview of the profile.



Profile Name	Name of the profile (can be changed here)
Operating System	Operating System the profile is for
Created At	Time of creation
Created By	The profile's creator
Last Change	Time of last change to the profile
Changed By	Account that made the last changes
Current Profile Revision	Revision of saved profile state
Released Profile Revision	Assigned profile revision ("Assign now"). If the label shows "(outdated)" behind the text, it means you've saved the profile but did not assign it yet, so the devices will still get and older version.

Device Overview (only on device level)

The device's summarized overview.

Device Name	Device name
Model	Model
Operating System	Operating System
Serial Number	Serial number of the device
Device Ownership	The configured Ownership Type
Device Type	The Type of the Device
Compliant	Shows if device is compliant
IP Address	The IP Address the device connected to the server from
Last Seen	Time of the last connection from the device
Last Push	Time of the last push sent to the device
Assignment	Here you can move the device to another user or group

Config Revision (only on device level)

Here you will receive an overview of which group profile is assigned to the device.

If you click on the group profile, you will access the profile directly and you can perform settings.

With the symbol, you can revert the assigned apps to the group profile's settings.

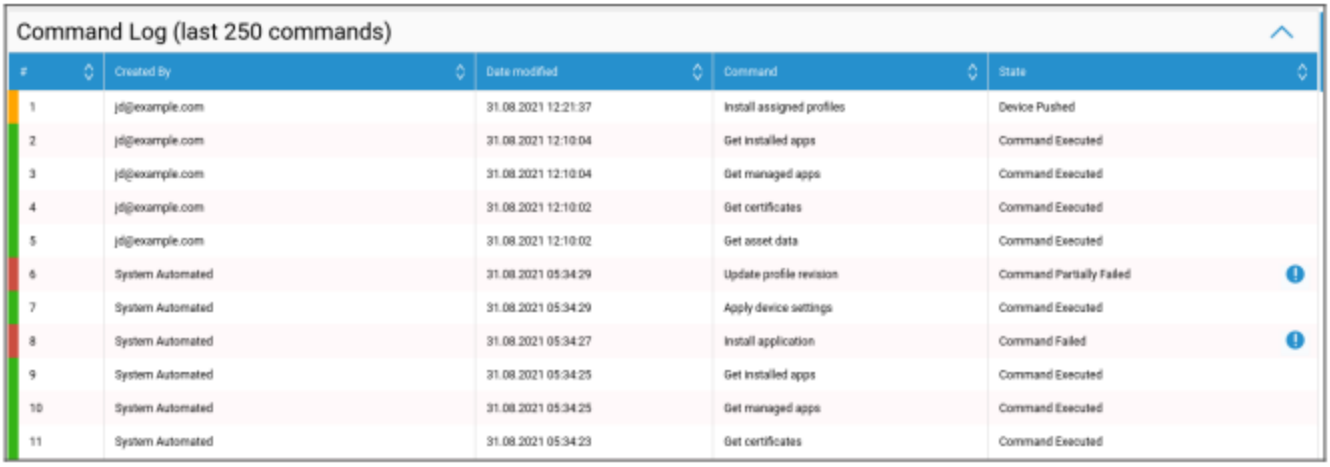
With the symbol, you can reset the device profile to have no settings at all.

“Newer Revision available“ indicates that the group profile has been changed and saved but not assigned. The group profile has to be assigned with “Assign now” on group level to apply the changes to the devices.

Device Log (only on device level)

Command Log

Here you can see which commands where issued for the device and what their status is.



Commands created by “System Automated” are automatically created by the system.

Possible command statuses

Device Pushed	A push request has been sent to the push service (e.g APNS) to tell the device to connect back to the EMM server.
Command Created	The command was created in the system.
Command Sent	The command got sent to the device after it connected to the server.
Command Executed	The command was successfully executed.
Command Failed	The command failed. *
Command Partially Failed	Depending on the device OS some commands may get grouped together. In this some parts of this command group failed. *
Command Executed, eventually Failed	The command was executed but maybe it wasn't.
Command Repushed	The command was repushed by a user.
Discarded	The command was discarded. For example because it was superseded by another command or the device got re-enrolled and old commands got removed

*If there is an exclamation mark behind the message, you can get more information by hovering over the icon with your cursor.

Asset Management (only on device level)

Device Info

Model Number	Model Number
Hostname	Hostname
Local Hostname	Local Hostname
Operating System	Operating system
OS Version	OS version
UDID	UDID
Free / Total Memory	Free / Total Memory

WiFi

IP Address	IP Address
WiFi MAC	WiFi MAC

Cellular

Phone Number	Phone Number
Roaming Status	Roaming Status
Roaming (Voice / Data)	Roaming (Voice / Data)
IP Address	IP Address
Operator/Carrier	Operator/Carrier
SIM Carrier Network	Carrier network
Carrier Version	Carrier Version
ICCID	ICCID
Current MCC/MNC	Current MCC/MNC
SIM MCC/MNC	SIM MCC/MNC

Bluetooth

Bluetooth MAC	Bluetooth MAC

Update Management (only on device level)

Update Info

This tab shows information about the system update settings on the device.

Autocheck enabled	If the system is checking for update automatically.
Automatic App-Update enabled	If the system will install app updates automatically.
Automatic OS-Updates enabled	If the system will install os updates automatically.
Automatic Security-Updates enabled	If the system will install security updates automatically.
App Update Background-Download enabled	If the system will download app updates in the background.
Catalog URL	The URL to the software update catalog the client is using.
Is default catalog	If „yes", Catalog is the default catalog.
Perform periodic check	If "yes", start a new scan.
Previous scan date	The date of the last software update scan.
Previous scan result	The result code of last software update scan.

Security Management

Anti Theft

Wipe & Lock

Full Wipe	Send a command to factory reset the device
Enterprise Wipe	Remove the MDM from the device and remove all MDM Data (e.g. Accounts, Apps)
Lock Screen	Make the device return to the lock screen

Security Configuration

Passcode

Code deactivation allowed	Determines whether the user is forced to set a PIN. Simply setting this value (and not others) forces the user to enter a passcode, without imposing a length or quality.
Allow simple value	Allow the user to use the same, escalating and reducing number strings (ex. 1234, 1111)
Require alphanumeric value	Passwords must contain at least one letter
Minimum passcode length	Minimal password length
Minimum number of complex characters	Minimal number of alphanumeric symbols in the password
Maximum passcode age	Number of days, after which the password must be changed
Maximum Auto-Lock	Maximum time, after which the device is locked
Maximum grace period for device lock	Amount of time the device can be locked without prompting for passcode on unlock
Maximum passcode age (1-730 days, or none)	Days after which passcode must be changed
Passcode history (1-50 passcodes, or none)	Number of unique passcodes before reuse

Certificate

PKCS#1	
Description	Enter a Description for the Certificate
Credential	Upload a pkcs1 File

PKCS#12	
Description	Enter a Description for the Certificate
Credential	Upload a pkcs12 File

Restriction Settings

Device Functionality

Allow Camera	Allow the use of the camera
Allow Game Center	When false, Game Center is disabled and its icon is removed from the Home screen.
Allow multiplayer gaming	When false, prohibits multiplayer gaming.
Allow adding Game Center friends	When false, prohibits adding friends to Game Center.
Allow iCloud Photo Library	If set to false, disables iCloud Photo Library. Any photos not fully downloaded from iCloud Photo Library to the device will be removed from local storage.
Allow Touch ID	If false, prevents Touch ID from unlocking a device.

iCloud

Block certain functionalities during iCloud pairing

Allow document sync	Allow document sync
Allow iCloud Keychain Sync	Allow iCloud Keychain Sync
Allow iCloud Notes	When false, disallows MacOS iCloud Notes services
Allow iCloud BTMM	When false, disallows MacOS Back to My Mac iCloud service.
Allow iCloud FMM	When false, disallows MacOS Find My Mac iCloud service.
Allow iCloud Bookmarks	When false, disallows MacOS iCloud Bookmark sync.
Allow iCloud Mail	When false, disallows MacOS Mail iCloud services.
Allow iCloud Calendar	When false, disallows MacOS Cloud iCloud services.
Allow iCloud Reminders	When false, disallows iCloud Reminder services.
Allow iCloud Addressbook	When false, disallows MacOS iCloud Address Book services.

Media Management

Eject at Logout	Eject all removable media at Logout
Allow Network	Allow access for network media
Allow Internal Disk	Allow access for internal disk.
Require Authentication	Require Authentication for the use of this media
Read Only	The User is only able to read data from the media
Allow External Disk	Allow access for external disk.
Require Authentication	Require Authentication for the use of this media
Read Only	The User is only able to read data from the media
Allow usage of Disk Images	Allow access for Images.
Require Authentication	Require Authentication for the use of this media
Read Only	The User is only able to read data from the media
Allow usage of DVD-RAMs	Allow access for DVD-RAM disk.
Require Authentication	Require Authentication for the use of this media
Read Only	The User is only able to read data from the media
Allow usage of DVDs	Allow access for DVD disk.
Require Authentication	Require Authentication for the use of this media
Allow usage of CDs	Allow access for CD disk.
Require Authentication	Require Authentication for the use of this media

Connection Management

Wi-Fi

Here you can add and configure Wi-Fi connections

Service Set Identifier (SSID)	SSID of the network, to which the connection will be established
Auto Join	Enable auto join for the network
Hidden Network	Enable, in case the AP does not broadcast the SSID
Proxy Setup	Configuring of a Proxy for every Access Point
None	Don’t use a Proxy Server
Manual	Establish a manual Proxy
Proxy Server URL	Address for accessing Proxy Settings
Port	Establish the port for the Proxy
Authentication	User name for the authentication on the Proxy
Password	Password for the authentication on the Proxy
Automatic	Establish a Proxy automatically
Proxy Server URL	URL for the proxy settings file
Security Type	Establish Security Type for the AP
WEP	
Password	Password for the AP
WPA/WPA2	
Password	Password for the AP
WEP Enterprise – WPA / WPA2 Enterprise / Any Enterprise	See Table Error: Reference source not found below
None	Establish no security
Disable MAC address randomization	Disables MAC address randomization for that Wi-Fi network while associated with the network. This also shows a privacy warning in Settings indicating that the network has reduced privacy protections.

Enterprise Wi-Fi Configuration

Note: Only available when “Security Type” is set to an Enterprise Type.

Protocols	Authentication protocol supported on target network
TLS	Enable / Disable Usage
TTLS	Enable / Disable Usage
Inner Authentications	Authentication protocol that should be used: PAP, CHAP, MSCHAP, MSCHAPv2
LEAP	Enable / Disable Usage
PEAP	Enable / Disable Usage
EAP-FAST	Enable / Disable Usage
EAP-SIM	Enable / Disable Usage
Use PAC	Use of PAC (Protected Access Control)
Provision PAC	Configuration of Provision PAC
Provision PAC Anonymously	Anonymous Provision of PAC
Authentication	
Username	Authentication username
Don't use Per-Connection Password	Don't use Per-Connection Password
Password	The password to use
Identity Certificate	Upload/select authentication certificate
Outer Identity	Identity that can be seen externally
Trust	
Trusted Certificate 1	Upload first trusted certificate
Trusted Certificate 2	Upload second trusted certificate
Trusted Certificate 3	Upload third trusted certificate
Trusted Server Certificate Names	The names of the expected server certificates (in a comma separated list)

VPN

Depending on the selected Connection Type, different fields may be visible.

Connection Name	Name of the VPN-Profile
VPN Type	
VPN	All of the device network traffic will be routed via a VPN-connection.
Connection Type	Establish VPN-connection type
IPsec (cisco)	IPsec protocol by cisco
L2TP	L2TP protocol
Custom SSL	Connection via Custom SSL
IKEv2	IKEv2 protocol
Proxy Setup	Configuring of a Proxy for the VPN-connection
None	Establish no Proxy
Manual	Manually establish a Proxy
Proxy Server URL	Address for access to Proxy Settings
Port	Establish the port for the Proxy
Authentication	Username for the authentication at the Proxy
Password	Password for the authentication at the Proxy
Automatic	Establish a Proxy automatically
Proxy Server URL	URL for access to the Proxy settings

HTTP Proxy

Proxy Type	
Manual	Establish a Proxy manually
Proxy Server URL	Address for access to the Proxy Settings
Port	Establish Proxy port
Authentication	Username for the authentication at the Proxy
Password	Password for the authentication at the Proxy
Automatic	Establish a Proxy automatically
Proxy PAC URL	Proxy PAC URL
Allow direct connection if PAC is unreachable	Allow direct connection (without VPN), if PAC is unreachable
Allow bypassing proxy to access captive networks	Allow bypassing proxy to access captive internal networks

AirPrint

IP Address	Printer IP address
Resource Path	Definite path to the AirPrint device

AirPlay

Device Name	Device name
Password	Pairing password
Whitelist	Define a list of devices, with which the device can pair itself exclusively

PIM Management

Exchange Active Sync

Account Name	Name of the account.
eMail Address	The address for the account (e.g. max@company.com)
Server Hostname	Internal Hostname
Login Name	"Domain" and "Login Name" must be blank for device to prompt for user.
Domain	"Domain" and "Login Name" must be blank for device to prompt for user. If an ACL Gateway Configuration is enabled and the Domain field is not empty, the AppTec360 Universal Gateway will authenticate the device with the following name "Domain\Login Name"
Password	The password for the account (e.g. secretUserPassword)
Past Days of Mail to Sync	The number of past days of mail to sync
Use SSL	Use SSL for Internal Exchange Host
Advanced Option	Show Advanced Options
Server Port	Internal Port
Server Path	Internal Path
External Hostname	External Host
External Port	External Port
External Path	External Path
Use SSL for External Exchange Host	Use SSL for External Exchange Host

eMail

Set up of POP3 / IMAP accounts on the end user device

Account Description	Name des Email Accounts
Account Type	
IMAP	
Path Prefix	The Path Prefix for special folders
POP	
User Display Name	User display name
Email Address	User email address

Incoming Mail	Incoming server settings
Mail Server Address	Mail Server address
Mail Server Port	Mail Server port
User Name	Respective user name
Authentication Type	Authentication Type
None	No Authentication Type
Password (only on device level)	Password prompt
MDM Challenge-Response	
NTLM	NTLM-Authentication
HTTP MD5 Digest	
Use SSL	Use SSL, if needed

Outgoing Mail	Outgoing server settings
Mail Server Address	Mail Server Address
Mail Server Port	Mail Server Port
User Name	Respective User Name
Authentication Type	
None	No authentication method
Password (only on device level)	Password prompt
MDM Challenge-Response	
NTLM	NTLM-Authentication
HTTP MD5 Digest	
Use SSL	Use SSL, if needed
Outgoing password same as incoming	Outgoing password same as incoming
Use only in mail	Activate, if all outgoing emails are to be sent via the Mail-App

CalDav

Configure the set up and distribution of a CalDav Account

Account Description	Display name of the account
Hostname	Hostname and/or IP address
Port	Port of the CalDav Account
Principal URL	Principal URL of the Account
Username	Respective CalDav username
Password (only on device level)	Respective CalDav password
Use SSL	Use SSL, if needed

CardDav

Configure the set up and distribution of a CardDav Account

Account Description	Display name of the account
Hostname	Hostname and/or IP address
Port	Port of the CardDav Account
Principal URL	Principal URL of the Account
Username	Respective CardDav username
Password (only on device level)	Respective CardDav password
Use SSL	Use SSL, if needed

LDAP

In this area, set up a LDAP-connection, in order to allow a dynamic certificate exchange, between the end user device and the Active Directory.

Please note that the selected user requires the respective read permission.

Account Description	Account Description
Account Username	User for LDAP-access
Account Password	Password for LDAP-access
Account Hostname	LDAP Server Hostname/IP address
Use SSL	Use SSL, if needed

In the second part, you can define individual filters for searching in the LDAP registry.

Description	Scope	Search Base
Filter description	Search level in the LDAP registry	Define the individual filter

Dashboard & Reporting

Dashboard Settings

Here you can see which dashboards exists, edit them or create new ones. Each Dashboard has their own set of data to show and graph configuration.

Dashboard Settings Control

Public	Sets the Dashboard public, so other users can see the Dashboard. The users of course have to be able to login and view Dashboards. If "Public" is not activated, only the creator can see it.
Default	Sets the Dashboard as default so it automatically opens next time you access the Dashboard View.
	Show the Dashboard and its graphs
	Delete the Dashboard
	Edit the Dashboard Name and Settings
	Make a copy of the Dashboard
	Add a completely new Dashboard

Dashboard View

This shows the Data and Graphs of the selected Dashboard and also lets you change these.

Dashboard Control

	Lets you define which data is shown in the Dashboard, the amount of data to show and in which size to show these data
	Brings you back to the Dashboard Overview
	Resets the currently opened Dashboard to its default
	Saves all the changes you made to the currently opened Dashboard (e.g. which data to show)
	Change chart type to pillar chart
	Change chart type to pie chart
	Change chart type to doughnut chart
	Change chart type to polar area chart
	Change sorting order

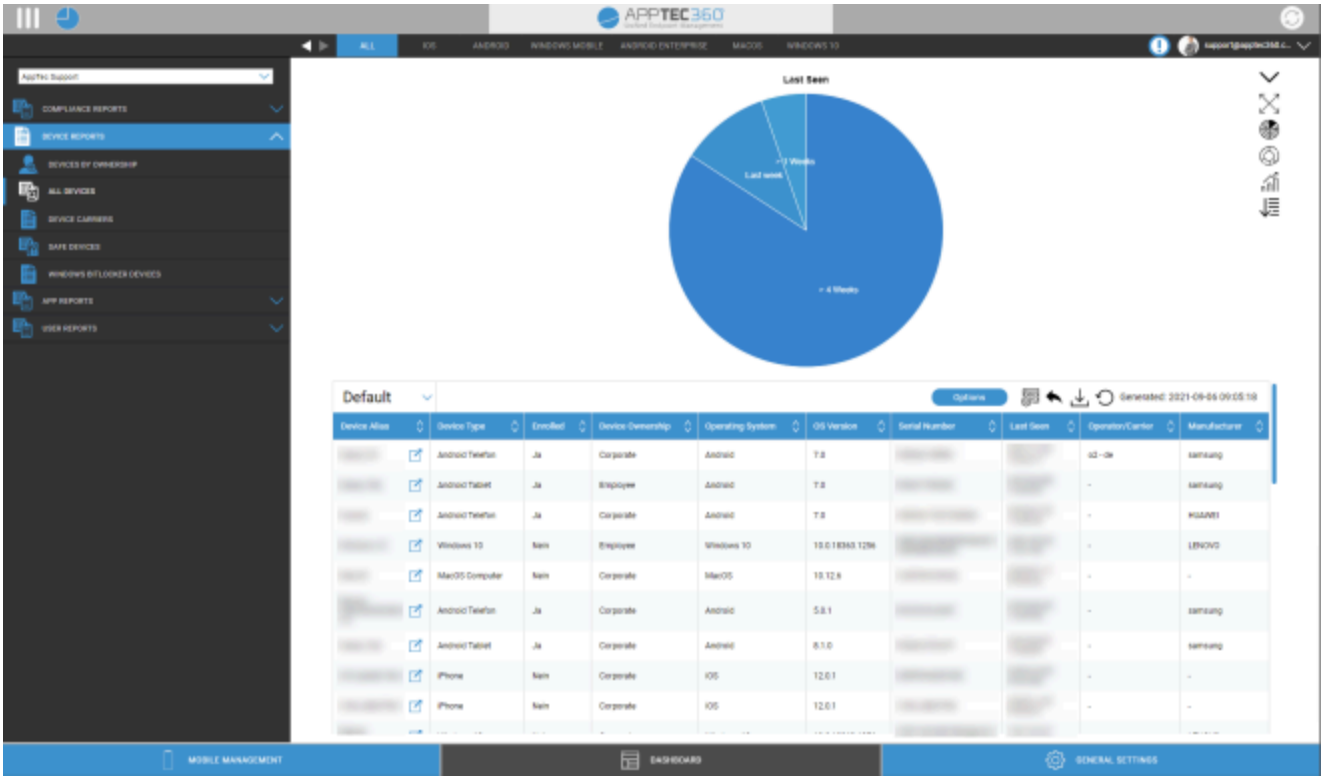
Extended Reporting

The “Extended Reporting“ offers detailed overviews and graphs about device and user information.

There are a few default Reports but all of them can be manually changed to add or remove data to show.

Please note that you can only manually change which data is shown. The selected report category defines the data this is based on. E.g. you will never be able to see Android devices in the iOS report in Device Reports All Devices iOS

On the top left you can limit the data of the reporting to a certain group (and all its sub groups). By default this is set to your root node, so it takes ALL devices and users into account.



Extended Reporting Control

In each overview you can use the following functions to change the report in any way you want:

	Hide chart (If chart is shown)
	Show chart (If chart is hidden)
	Expand chart (If chart is collapsed)
	Collapse chart (If chart is expanded)
	Change chart type to pillar chart
	Change chart type to pie chart
	Change chart type to doughnut chart
	Change chart type to polar area chart
	Change sorting order
	Modify the following parts about the displayed overview: • Add/Remove columns • Specify the order in which the columns are shown • Show/Hide the chart above the table • Select the column that is used for the chart • Filter the data of your table
	Open the setup manager to save and load different reports
	Resets the currently opened Report to default
	Export the current report as a .csv file
	Regenerate data and reload the current report

You can find a list of all default reports on the next pages.

Compliance Reports

Rooted Devices

Overview of the devices that have been rooted/ jailbroken.

Default columns of this report:

Device Alias
Device Owner
E-Mail
Operating System
Phone Number
Last Seen
Manufacturer

Roaming Devices

Overview of all of the devices that are roaming

Default columns of this report:

Device Alias
Device Owner
E-Mail
Device Type
Operating System
Phone Number
Last Seen

Roaming Enabled Devices

Overview of all devices that have activated roaming but don’t necessarily are currently roaming.

Default columns of this report:

Device Alias
Device Owner
E-Mail
Device Type
Operating System
Phone Number
Last Seen

Supervised Devices

Overview of all devices that are supervised in supervised mode (iOS only)

Default columns of this report:

Device Alias
Device Owner
E-Mail
Device Type
Last Seen

Inactive Devices

Overview of all devices which haven’t connected to the server in the last 7 days

Default columns of this report:

Device Alias
Device Owner
E-Mail
Device Type
Operating System
Last Seen

Device Reports

Devices by Ownership

Here you can see how many devices have currently been deployed as corporate (corporate devices) and employee (private devices) devices.

Default columns of this report:

Device Alias
Device Owner
Device Type
Device Ownership
Operating System

All Devices

Here you can see an overview of all devices with the most important information.

Default columns of this report:

Device Alias
Device Type
Enrolled
Device Ownership
Operating System
OS Version
Serial Number
Last Seen
Operator/Carrier
Manufacturer

Device Carriers

Here you can see an overview regarding the carrier (cellular provider).

Default columns of this report:

Device Alias
Device Owner
E-Mail
Operating System
OS Version
Operator/Carrier

SAFE Devices

Here you can see an overview of which devices use SAFE Version.

Because the overview and/or SAFE is only available for Samsung devices, you will not see the usual tabs under this point.

Default columns of this report:

Device Alias
Device Owner
E-Mail
Device Type
Last Seen
SAFE Version

Windows BitLocker Devices

Here you can see an overview of the Windows devices that use BitLocker.

Default columns of this report:

Device Alias
Device Owner
E-Mail

BitLocker State

App Reports

Here you get a variety of overviews in regards to apps. In all of these reports you can click on an entry to further see which versions are installed on the devices and how often. In this view you can click on a specific version again to see which devices have this specific version installed.

Note: It may take some time until the system gets an up to date information from the device. Additionally the reports are not updated every minute. You might need to be patient to see the current status if you just have assigned a new app or version. Manually reloading the report will force the report to show the most up to date data available

Installed Apps

Here you get an overview of all installed apps.

Default columns of this report:

Name	Name of the respective app and/or service
Identifier	Definite app/service ID
Total Count	How often this app / service has been installed on the end user devices

Most Installed Apps

Here you get an overview of the apps that have been installed the most.

Default columns of this report:

Name	Name of the respective app and/or service
Identifier	Definite app/service ID
Total Count	How often this app / service has been installed on the end user devices

Mandatory Apps

Here you get an overview of mandatory (mandated required) apps.

Default columns of this report:

Name	Name of the respective app and/or service
Identifier	Definite app/service ID
App Source	Which AppStore is involved: • Google PlayStore (Android) • iTunes AppStore (iOS)
OS	Operating System

Blacklisted Apps

Here you get an overview of all defined blacklisted apps.

Default columns of this report:

Name	Name of the respective app and/or service
Identifier	Definite app/service ID
App Source	Which AppStore is involved: • Google PlayStore (Android) • iTunes AppStore (iOS)
OS	Operating System

User Reports

Tariff

Here you get an overview of your users phone tariffs and SIM cards.

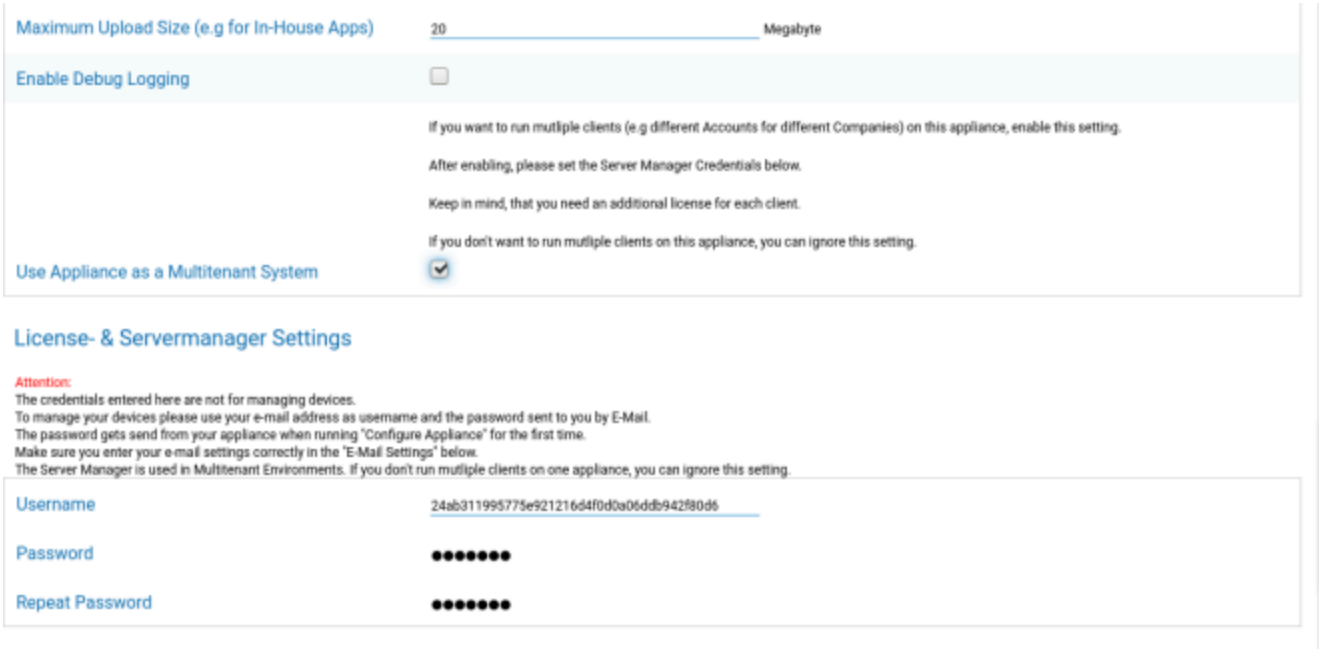
Default columns of this report:

E-Mail
Name
phoneNumber
carrier
tariff
option
price
contractCancelled
contractStart
duringTime
mobileAndData
dataVolume
multiSIM
type
simCardSerial1
simCardSerial2
simCardSerial3
pin1
pin2
puk1
puk2
note

Multitenant Management

The AppTec360 EMM is capable of hosting multiple separate tenants, each with their own users and groups, permissions and global settings.

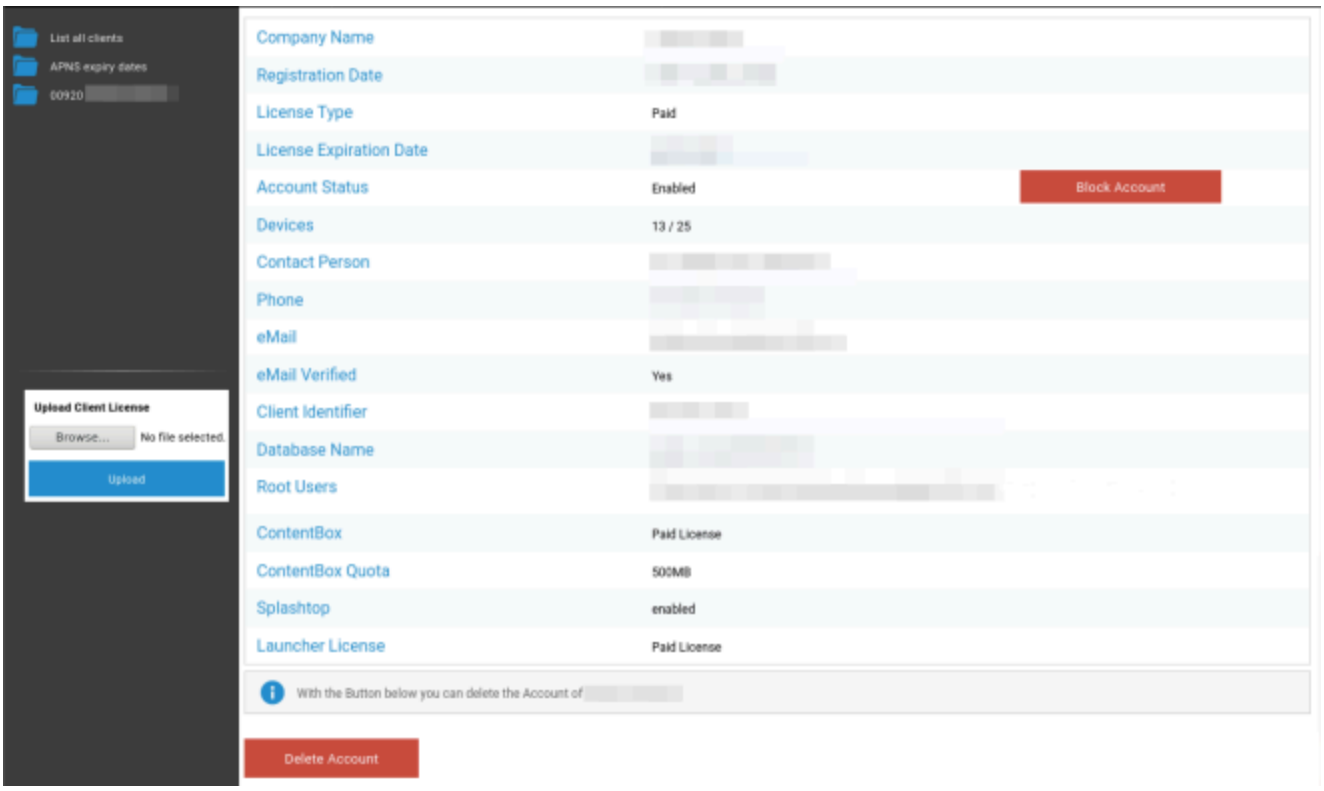
To enable Multitenant capabilities, you have to enable it in the configuration interface of the Appliance in “Step Three – Server Settings”.



In the new menu set a username and a password for the Servermanager. Save the settings and run “Configure Appliance” in “Step Five – License Agreement” to apply the setting.

When the configuration is finished, you can now login with the set credentials through the normal Mobile Management interface.

After login you can see the following view.



On the left you can see all tenants (in this case only one with id 920) and on the right the information about this client. You also have the option to block access to the account as well as to delete the client (CAUTION: This will remove all data related to that client).

On the left you can upload a new client license, which can be either a license update for an existing client or a new license which automatically creates a new client. When a new client is created an email containing the login password is automatically sent to the e-mail address that the license was issued for.

To obtain a new or an updated client license (e.g. when in need for more device licenses) contact your sales representative.

Additional views

List all clients

Shows an overview about all clients in the system.

Client ID	Client ID
Identifier	Client Identifier
Database	Database
Company Name	Company name
eMail	Contact person eMail
Verified	Whether the contact persons eMail is verified or not
Country	Country
Devices	Number of registered devices
Registration Date	Point in time of the license assignment
Last Login	Last admin account login
License	License type display (Free|Paid)
CB License	ContentBox license type (Free|Paid)
Status	Current AppTec-Client status
Expired	Displays, if the license has expired
iOS	Number of iOS Devices
Android	Number of Android Devices
Windows Mobile	Number of Windows Mobile Devices
MacOS	Number of MacOS Devices
Windows 10	Number of Windows 10 Devices
Android Enterprise	Number of Android Enterprise Devices
IOS BYOD (User Enrollment)	Number of IOS BYOD (User Enrollment) Devices
IoT	Number of IoT Devices

APNS expiry dates

Shows an overview of all APNS certificate expiration dates of all clients.

Client ID	Client ID
Company Name	Company Name
Expire Date	Expiration date for the Apple APNS-certificate
Info	Information about the expiration

Contact

Additional questions? Simply contact us under:

For general technical questions

support@apptec360.com

+41 61 511 3210

For questions related to the installation of a virtual appliance

consulting@apptec360.com

+41 61 511 3214

Disclaimer