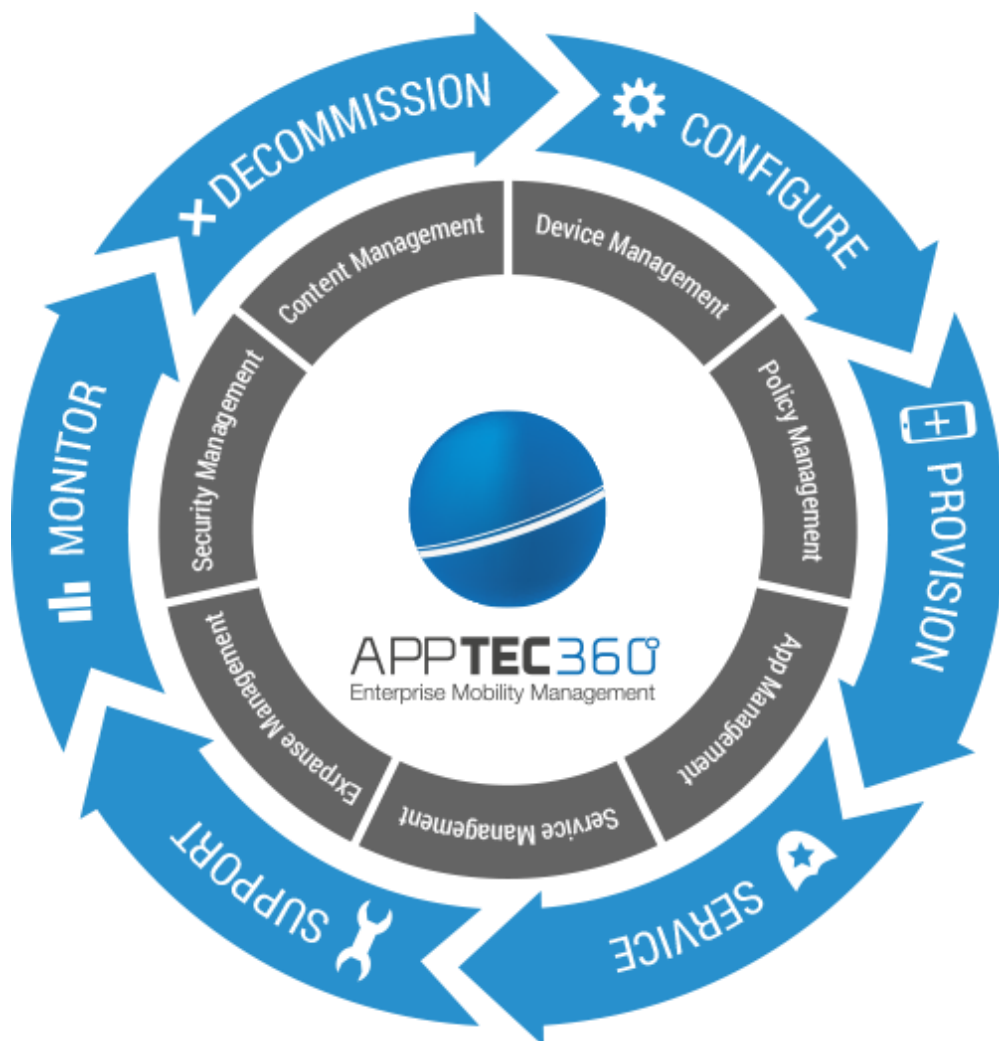




*AppTec360 Enterprise Mobile Manager & ContentBox  
Administration Manual | Version 4.3.1 (181113.0)*





# Table of Contents

<b>Table of Contents</b> .....	2
<b>I. GENERAL OVERVIEW</b> .....	13
Introduction to AppTec360 .....	13
Supported Devices and Platforms.....	14
Explanation of the “Supervised-Mode” on Apple Devices .....	14
Explanation of the „Android for Work Device Owner Mode“ on Android Devices .....	15
Upload your own Apps to the Google Play Store .....	15
Activate the supervised mode.....	18
Adding a device to the DEP .....	19
<b>II. Requirements / Installation</b> .....	20
Requirements .....	20
System requirements .....	20
Firewall regulations.....	20
IP-Address and DNS Resolution .....	22
SSL-Certificate .....	22
License keys.....	22
Installation example with VMware.....	23
Default Passwords of the Virtual Appliance.....	26
Configuration of the Virtual Appliance .....	27
Configure from external host.....	33
Security Recommendations .....	34
<b>III. General Settings</b> .....	35
Account Overview.....	35
Overview .....	35
Bug Report.....	36
Feature Request .....	37
Global Configuration.....	38
eMail Settings.....	38
eMail Templates.....	38
Privacy .....	40
GPS Access.....	40
Role Based Access .....	41
Role Management .....	41



<i>Role Assignments</i> .....	42
<i>Assignment of a role</i> .....	43
<i>Self Service</i> .....	43
<i>API Access</i> .....	44
iOS Configuration .....	49
APNS Certificate .....	49
DEP .....	53
<i>Pool Enrollment URL's</i> .....	62
<i>MDM Profile – Apple Configurator</i> .....	64
Android Configuration .....	68
Android Configuration .....	68
Auto Enrollment.....	69
Android for Work .....	69
First Method: Android for Work Account (Google Account) .....	69
Second Method: G-Suite Account.....	70
AFW Enrollment.....	72
Method 1: QR Code Enrollment .....	72
Method 2: NFC Enrollment.....	73
Method 3: Google Account.....	73
KNOX Enrollment .....	74
Windows Configuration .....	75
Windows Configuration .....	75
Content Box .....	77
Configuration .....	77
LDAP Configuration.....	79
LDAP Overview .....	79
Universal Gateway .....	80
App Management .....	81
In-House App DB.....	81
Android .....	81
<i>Update Target</i> .....	82
iOS .....	82
<i>Update Target</i> .....	83
Windows.....	83
Black-& Whitelisting.....	84
Android .....	84



Apple.....	85
Windows.....	86
Third Party Apps .....	87
Android .....	87
iOS .....	87
VPP / KNOX .....	87
VPP Token.....	88
Knox Key.....	89
VPP Licenses .....	90
App Store .....	90
Region .....	90
App Settings .....	91
iOS App Settings.....	91
Android App Settings .....	91
Remote Control .....	92
<b>IV.    Mobile Management.....</b>	<b>97</b>
Mobile Management Screen .....	97
Device filter .....	97
Search window .....	97
Options gear .....	97
Navigation arrows .....	97
Administration account-settings.....	98
Corporate administration (Root-Node) in Mobile Management.....	99
Create a Subgroup .....	99
Rename Root Node.....	100
Mass Enrollment .....	100
Mass Assignment .....	101
Group Management in Mobile Management.....	102
Create a Subgroup .....	103
Edit selected Group .....	103
Delete selected Group .....	104
Create a User .....	105
Create a new Admin-User .....	106
Add and enroll a Device.....	108
Profile Management in Mobile Management.....	110
Create a profile.....	110



Edit Profile.....	110
Copy Profile .....	111
Delete Profile .....	111
Device Management in Mobile Management.....	113
Android .....	113
Edit Device.....	114
Clear Passcode.....	114
Lock Device .....	114
Delete Device .....	115
Wipe Device.....	115
Enterprise Wipe.....	116
Send Message .....	116
Send Enrollment Request.....	117
iOS .....	118
Edit Device.....	119
Clear Passcode.....	119
Lock Device .....	120
Delete Device .....	120
Enterprise Wipe.....	121
Send Message .....	121
Send Enrollment Request.....	122
Remove MDM .....	122
Windows.....	123
Lock Device .....	124
Delete Device .....	124
Wipe Device.....	124
Enterprise Wipe.....	125
Content Management.....	127
File Explorer.....	130
Trash.....	131
<b>Configuration iOS.....</b>	<b>133</b>
General.....	133
General Information.....	133
Settings.....	134
Config Revision .....	134
Device Log .....	134



Asset Management (only on device level) .....	135
Asset Management (only on device level) .....	135
Security Management .....	136
Anti Theft (only on device level) .....	136
GPS Information (only on device level) .....	136
Wipe & Lock (only on device level) .....	136
Message (only on device level) .....	137
Security Configuration.....	138
Passcode .....	138
Encryption .....	139
End of Life (only on device level) .....	141
Wipe (only on device level) .....	141
Restriction Settings.....	142
Device Functionality .....	142
iCloud.....	144
Security and Privacy.....	144
BYOD.....	144
Built-In iOS Security (Container) .....	144
Activation.....	145
SecurePIM Password.....	145
SecurePIM Security.....	146
SecurePIM Browser .....	146
Exchange .....	147
Connection Management .....	148
Wifi .....	148
APN.....	151
Cellular .....	151
AirPrint.....	151
AirPlay .....	151
PIM Management .....	152
Exchange Active Sync .....	152
eMail .....	152
CalDav.....	153
Subscribed Calendars.....	154
LDAP.....	154
Webclips.....	155



Web Content Filter .....	155
App Management .....	156
Enterprise App Manager.....	156
Installed Apps (only on device level) .....	156
Mandatory Apps .....	157
Web Apps.....	159
Restriction & Settings.....	160
Blacklisted / Whitelisted Apps .....	160
SysApp Restrictions .....	160
App-VPN .....	161
App Settings .....	161
Enterprise App Store.....	163
iTunes Apps.....	163
In-House.....	165
Kiosk Mode .....	168
Content Management.....	170
ContentBox .....	170
<b>Android Configuration .....</b>	<b>170</b>
General.....	170
Device Overview (only on device level) .....	171
Config Revision .....	171
Device Log .....	171
Device Settings .....	172
Client Configuration.....	172
Asset Management (only on device level) .....	173
Asset Management (only on device level) .....	173
Security Management .....	175
Anti Theft (only on device level) .....	175
GPS Information (only on device level) .....	175
Wipe & Lock (only on device level) .....	175
Message (only on device level) .....	176
Security Configuration.....	177
Passcode .....	177
Encryption .....	178
End of Life (only on device level) .....	179
Wipe (only on device level) .....	179



Restriction Settings.....	181
Restrictions .....	181
Allow Screen Capture .....	182
Allow screen capture.....	182
Allow Clipboard .....	182
Allow clipboard .....	182
AFW Device Owner .....	183
BYOD Container .....	187
Android for Work .....	187
Android for Work .....	187
Divide Exchange .....	187
System Apps .....	188
Samsung KNOX.....	188
Activation.....	188
Knox Passcode .....	188
Knox Security .....	189
Knox Exchange .....	189
Knox eMail .....	190
Knox Apps.....	191
Connection Management .....	191
Wifi .....	191
VPN.....	192
Restrictions .....	193
Bluetooth .....	195
PIM Management .....	197
Exchange .....	197
eMail .....	198
AFW Gmail Exchange.....	199
Touchdown Exchange .....	200
App Management .....	201
Enterprise App Manager.....	201
Installed Apps (only on device level) .....	201
System Apps (only on device level) .....	204
Mandatory Apps .....	205
Sys App Restrictions .....	208
Samsung Apps.....	209



Huawei Apps .....	209
Enterprise App Store.....	210
Playstore .....	210
In-House.....	213
AFW Playstore .....	215
Kiosk Mode & Launcher.....	215
Kiosk Mode .....	215
AppTec Launcher .....	217
AppTec Settings.....	217
Wallpaper .....	218
Content Management.....	219
<b>Configuration Windows Phone .....</b>	<b>220</b>
General.....	220
Device Overview (only on device level) .....	220
Config Revision (only on device level) .....	221
Device Log (only on device level) .....	221
Asset Management (only on device level) .....	222
Asset Management (only on device level) .....	222
Security Management .....	224
Security Configuration.....	224
Passcode .....	224
End of Life (only on device level) .....	225
Wipe (only on device level) .....	225
Restriction Settings.....	226
Device Functionality .....	226
Connection Management .....	228
Wifi .....	228
Wifi Restrictions .....	229
VPN.....	229
VPN Restrictions.....	230
Bluetooth .....	231
NFC.....	231
PIM Management .....	232
Exchange Active Sync .....	232
eMail .....	233
App Management .....	234



Enterprise App Manager.....	234
Mandatory Apps.....	234
Whitelisted / Blacklisted Apps.....	234
Enterprise App Store.....	237
Windows store.....	237
In-House.....	239
Kiosk Mode .....	241
Kiosk Mode .....	241
<b>Configuration Windows 10 PC .....</b>	<b>242</b>
General.....	242
Device Overview (only on device level) .....	242
Settings.....	243
Config Revision (only on device level) .....	243
Device Log (only on device level) .....	243
Asset Management (only on device level) .....	244
Security Management .....	245
Anti Theft (only on device level) .....	245
GPS Information (only on device level) .....	245
GPS Settings .....	245
Security Configuration.....	246
Passcode .....	246
Restriction Settings.....	247
Device Functionality .....	247
Connection Management .....	248
Wifi .....	248
Wifi Restrictions .....	249
VPN.....	250
VPN Restrictions.....	250
Bluetooth .....	250
PIM Management .....	251
Exchange Active Sync .....	251
eMail .....	252
<b>Configuration MacOS .....</b>	<b>253</b>
General.....	253
Device Overview (only on device level) .....	253
Config Revision (only on device level) .....	254



Device Log (only on device level) .....	254
Asset Management (only on device level) .....	255
Security Management .....	256
Security Configuration.....	256
Passcode .....	256
Certificate .....	256
Restriction Settings.....	257
Device Functionality .....	257
iCloud.....	257
Media Management.....	258
Connection Management .....	259
Wifi .....	259
AirPrint.....	261
AirPlay .....	261
PIM Management .....	262
Exchange Active Sync .....	262
eMail .....	262
CalDav.....	263
CardDav .....	264
LDAP.....	264
<b>V. Dashboard &amp; Reporting .....</b>	<b>265</b>
Dashboard .....	265
Extended Reporting.....	266
Compliance Reports.....	267
Rooted Devices.....	267
Roaming Devices.....	267
Roaming Enabled Devices .....	268
Supervised Devices.....	268
Device Reports.....	269
Devices by Ownership .....	269
All Devices .....	269
SAFE Devices .....	270
App Reports.....	271
Installed Apps.....	271
Most Installed Apps .....	271
Mandatory Apps.....	273



<b>VI.    <i>Mandate Management</i></b> .....	274
Display .....	274
List all clients .....	274
APNS expiry dates .....	275
Account Information .....	276
Registration of an additional AppTec-License.....	277
CONTACT.....	278
DISCLAIMER.....	278



# **I. *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, IT-administrators 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 Devices and Platforms

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.

Supported software versions minimums:

iOS devices from iOS Version 3.0

Android devices from Version 2.3

Windows devices from Version 8

Up to and including Android Version 4.1.x, the “AppTec MDM Agent for Samsung” must be installed on the Samsung devices, in order to successfully connect the device to the server.

## 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.

<b>Available in the Supervised-Mode</b>
---

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.



## Explanation of the „Android for Work Device Owner Mode“ on Android Devices

The Android for Work Device Owner Mode (in short AfW Device Owner) extends Android Devices by a significant amount of APIs. So you can set Restrictions that normally required Samsung SAFE or never were possible in the first place.

To use the AfW Device Owner Mode some requirements have to be fulfilled. The device has to support Android for Work in the Device Owner Mode (ask your manufacturer to get sure) and you have to link the management console with Google. See [Android for Work](#) for information.

A detailed explanation of how to enroll devices into the AfW Device Owner Mode can be found here: [AFW Enrollment](#)

## 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.

Create application

Default language \*

English (United Kingdom) – en-GB ▼

Title \*

AppTec Demo App

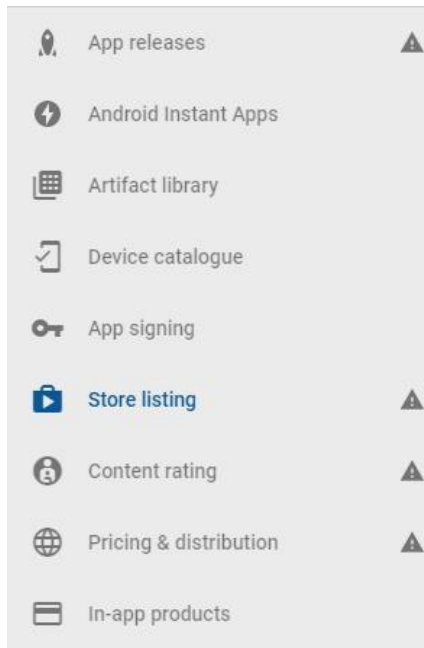
15/50

CANCEL

CREATE



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.

#### Managed Google Play

☒ Turn on advanced managed Google Play features

Organisations and schools use managed Google Play to choose the apps available to their staff and students. Free apps are already available through managed Google Play. To license your paid app for organisations to purchase, or to target your app to specific organisations, turn on advanced managed Google Play features. [Learn more](#)

☒ Privately target this app to a list of organisations.

**CHOOSE ORGANISATIONS**

This app is privately targeted to **1 organisation**.

You can also target alpha or beta releases of your app to organisations. [Manage alpha or beta releases](#) or [Learn more](#)






After 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.

### Review summary

This release is ready to be rolled out.

### APKs in this release

Version code	Uploaded	Installs on active devices
1 APK added		
 1	3 minutes ago	No data  

### What's new in this release?

Default – German – de-DE  
Initial release of the demo app


🌐 1 language translation


PREVIOUS


DISCARD

START ROLL-OUT TO PRODUCTION


It may 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.


**Google Play**





**Apps**

My managed apps  
Shop  
Updates  
Admin Settings  
Help Centre




## AppTec Demo App


Business



**APPROVED**

UNAPPROVE

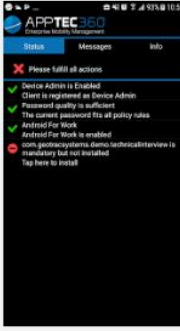
APPROVAL PREFERENCES

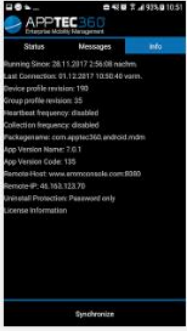
 This app is available in certain countries.


**APPTec360**  
 Enterprise Mobility Management



### Quick Overview







## 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“
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 your 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!



## II. Requirements / Installation

### Requirements

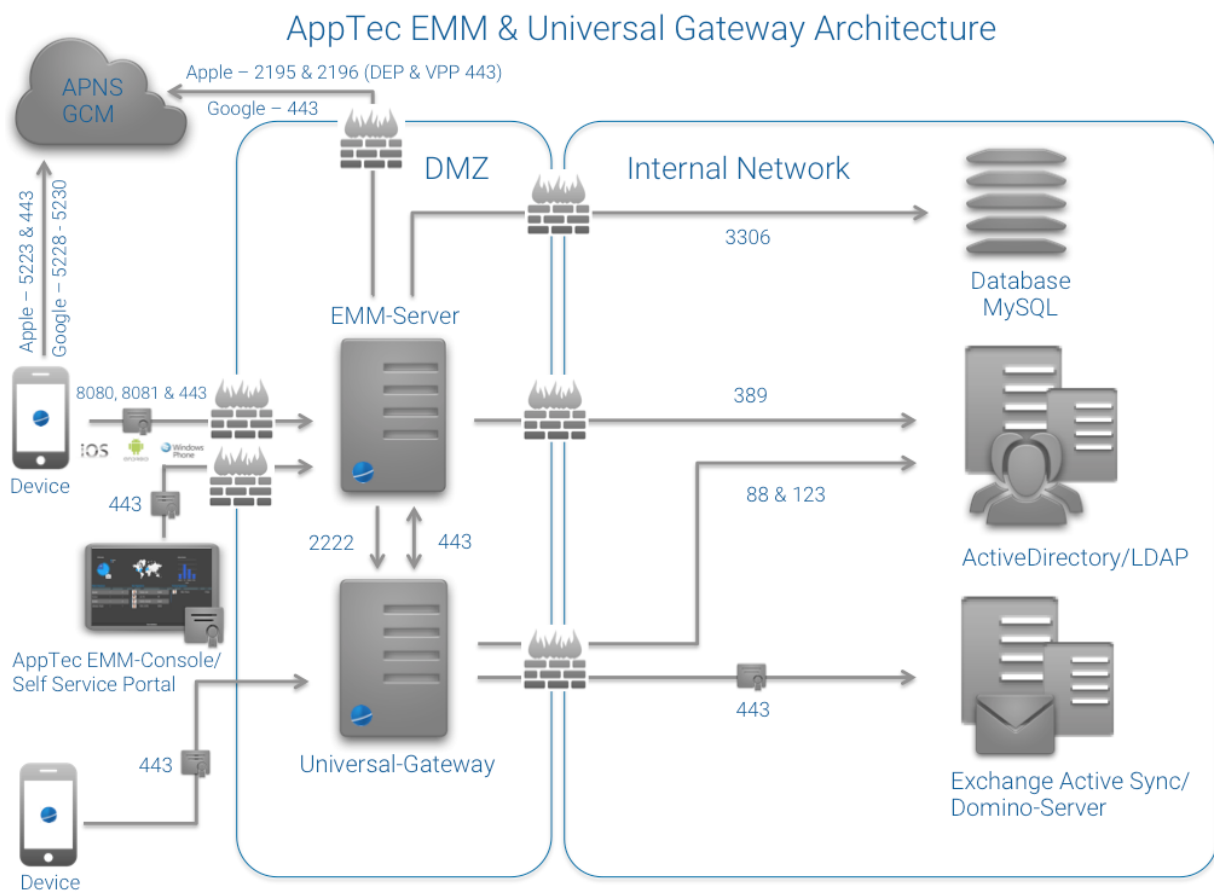
#### System requirements

The virtual appliance will be made available in the Open-Virtual-Format (OVF). This can be imported into the following systems:

- VMWare
- MS Hyper V
- Virtual Box
- Citrix Xen Server

Additionally, 4 GB RAM/working memory and 20 GB of available hard drive space are required. The appliance is based on Ubuntu 64bit.

#### Firewall regulations





Any (external/Devices) → | → AppTec Appliance / emmconsole.com

Ports:

443: Management, Enterprise AppStore & Windows Phone Communication

8080: Android & iOS Communication

8081: Enrollment iOS

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 (GCM), has to be reachable without proxy

Domain Controller → | → AppTec-Server / emmconsole.com

Ports:

389, (LDAPS 636): User synchronization with LDAP

Apptec Appliance → | → Any

Port:

443

Used for the Android Push Service (GCM).

The Port 443 to external is used to search for apps in our console. Sadly we cannot provide a specific IP or range because of the network structure of the provider. Should this feature be wanted, port 443 to any has to be open.

AppTec Appliance → | → emmconsole.com

Ports:

443: AppTec Appliance Updates, APNS certificate generation

AppTec Appliance → | → Apple Network (17.0.0.0/8)

Ports:

2195, 2196: Apple Push Service & Feedback Service

443: DEP & VPP



## IP-Address and DNS Resolution

The AppTec server must be accessible via a public IP-address. Additionally, you will also need the respective enabled hostname and/or DNS registration.

To enroll Windows-Phone Devices you also need to set up a subdomain in the form of “enterpriseenrollment.<Appliance Domain>”, pointing to the appliance.

## SSL-Certificate

You need a SSL Certificate for the hostname issued by a Certificate Authority that is trusted on the (only public trusted certificates are supported). Additionally, an intermediate certificate for CA and Private Key (not password protected) is required. Please note, that the Wildcard-Certificates are not supported.

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

## SMTP-Relay

An e-mail server and/or an email-relay is required, to allow the AppTec360 server to send emails to the respective users.

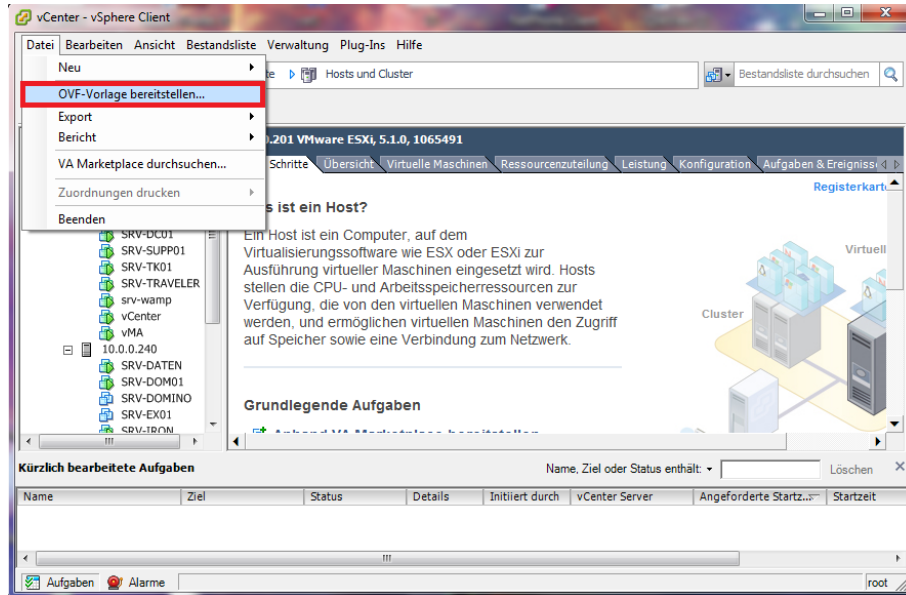
## License keys

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.

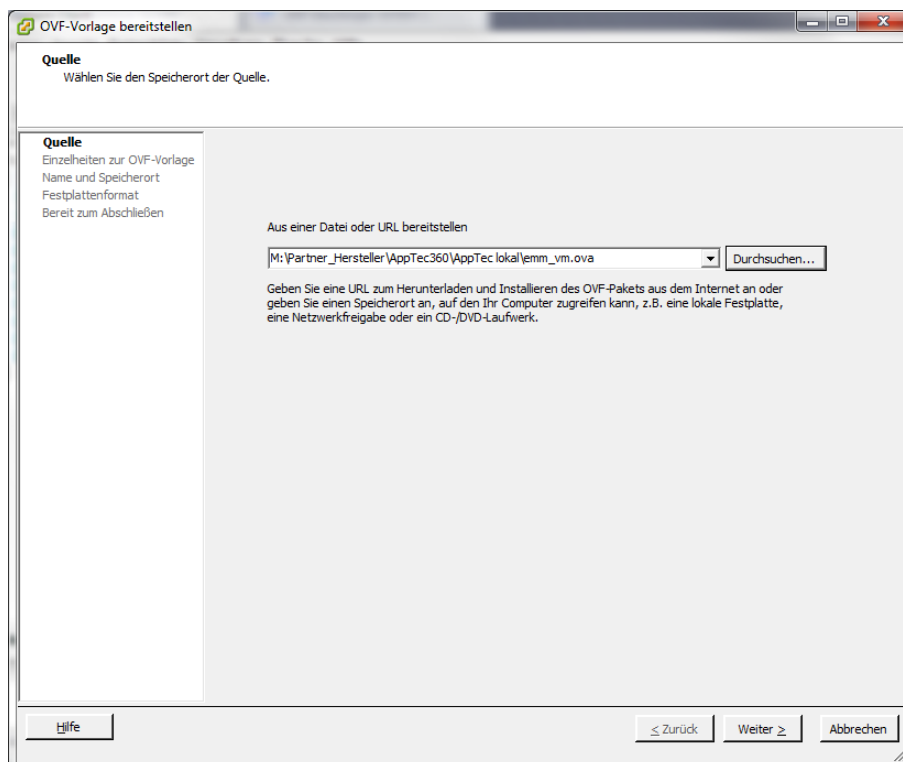


## Installation example with VMware

- Prepare “File” > “OVF-Template...”

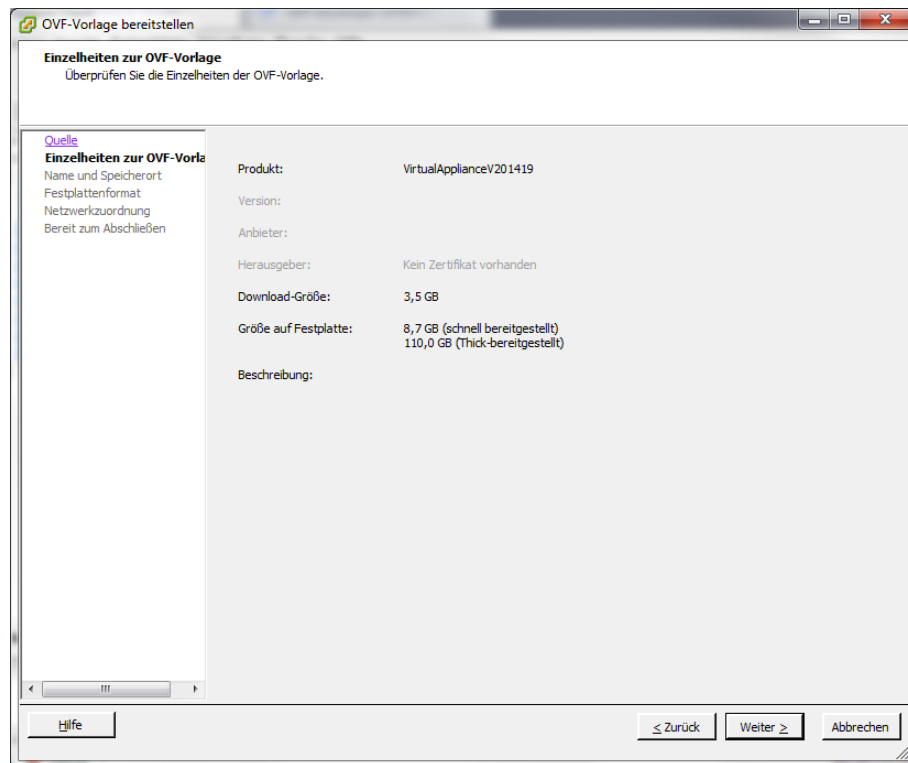


- Afterwards, select the available OVA-Image and confirm with “continue”.

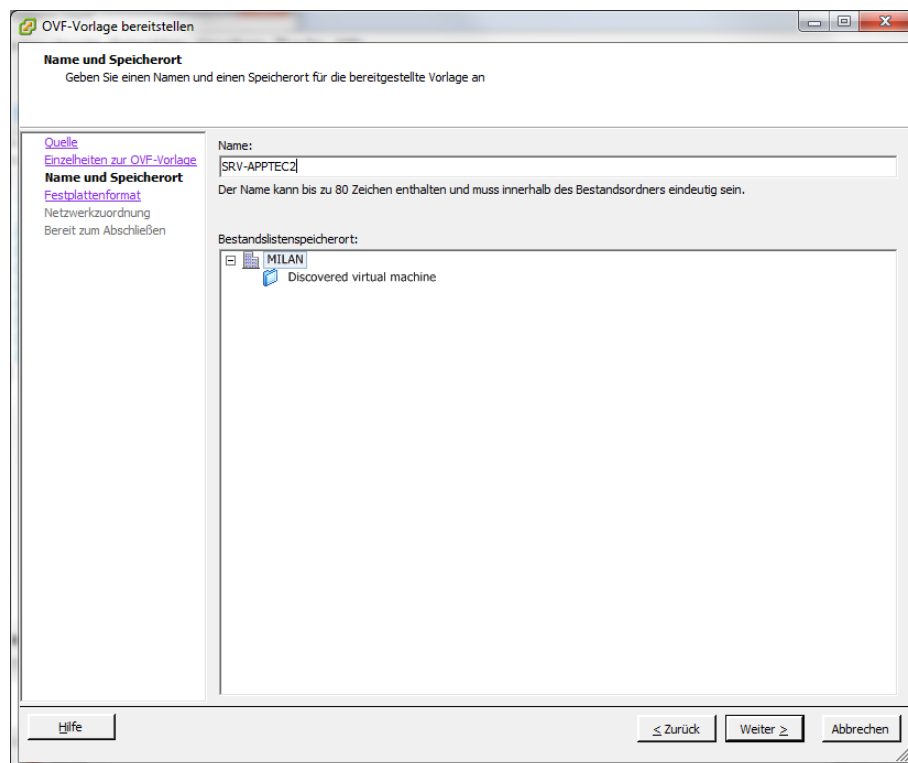




- Confirm details in the OVF-template with “continue”.

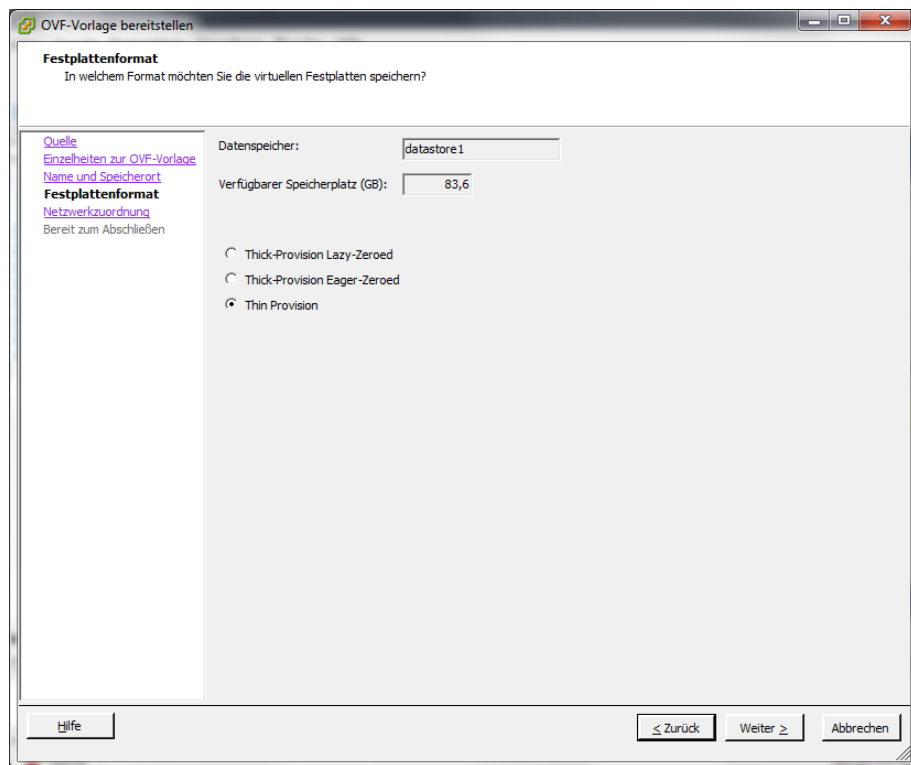


- Here you can name the VM whatever you want.

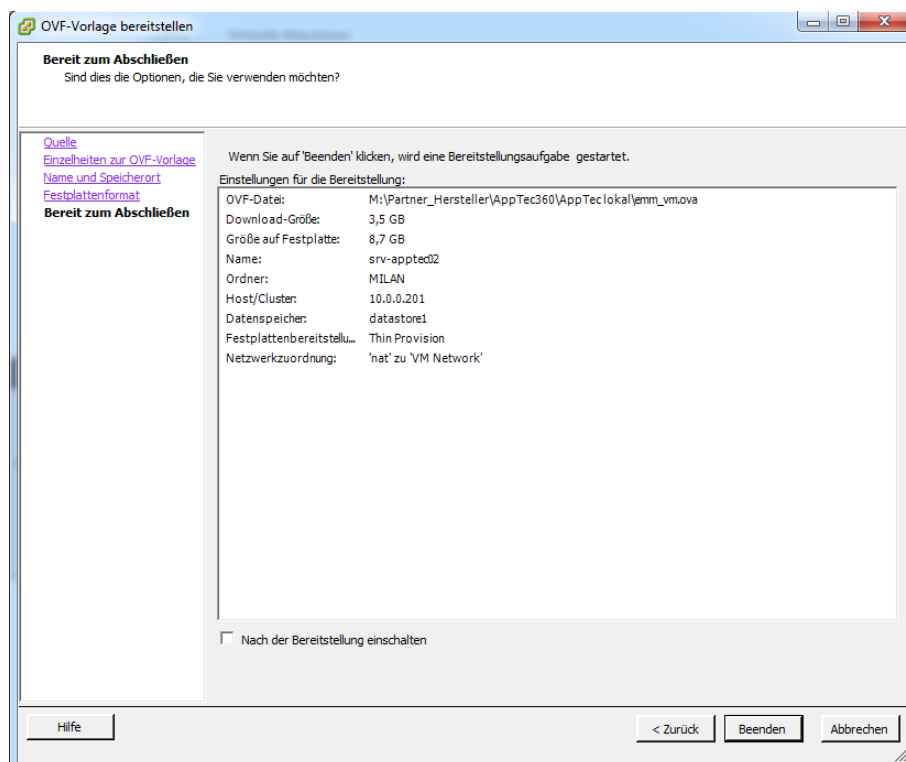




- Confirm hard drive format of the VM with “continue”.

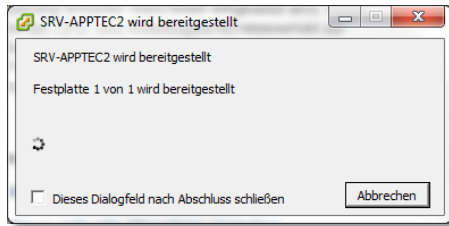


- Conclude the last overview of the configuration by clicking “end”.





- Please wait until the VM has been successfully installed.



Please note that upgrades to the Ubuntu operating system on newer versions can lead to the AppTec server not functioning. We therefore recommend NOT to perform upgrades on a newer operating system versions! The only exception is the upgrade from Ubuntu 12 to 14. For more information about this contact [support@apptec360.com](mailto:support@apptec360.com). The security updates, however, should be applied!

### Default Passwords of the Virtual Appliance

#### Root Password

apptec

#### Default User

apptec

#### Password for User “apptec”

apptec

#### MySQL Root User

root

#### MySQL Root Password

apptec

#### MySQL Default User

AppTec

#### MySQL Default User Password

AppTec



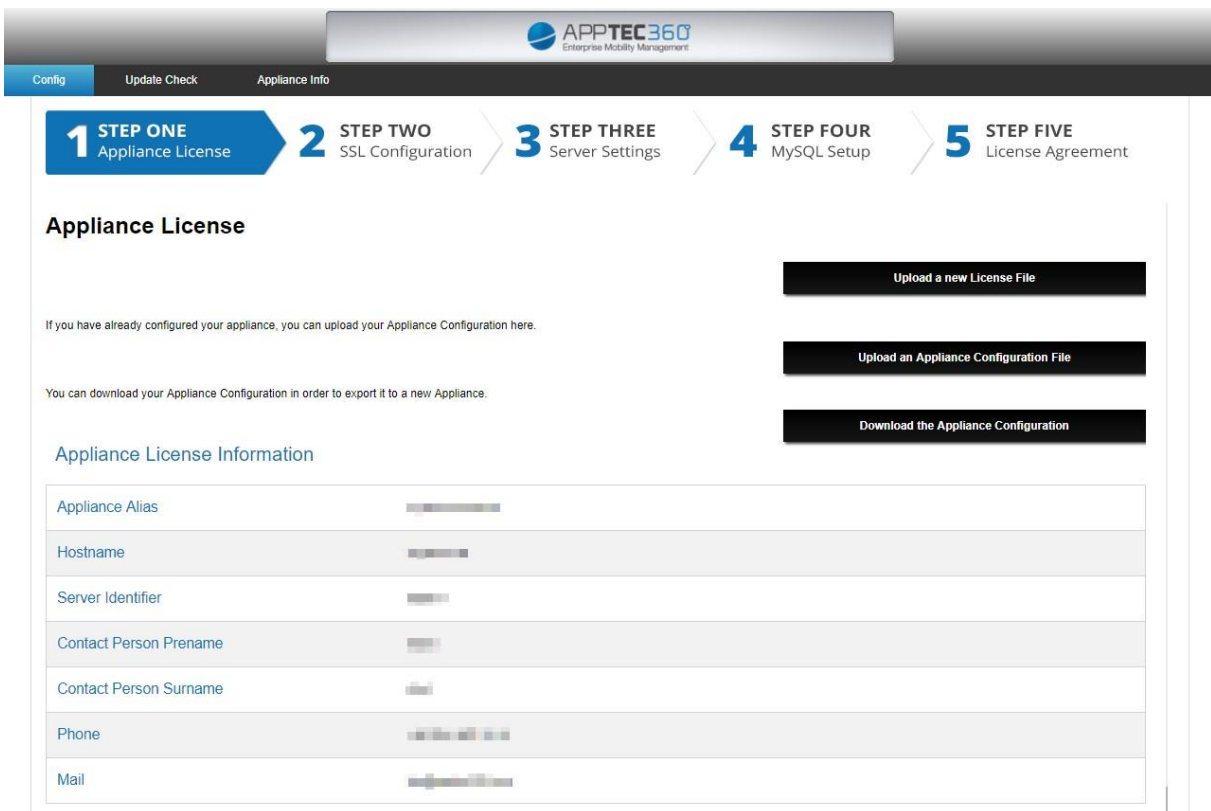
## Configuration of the Virtual Appliance

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

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

### Step 1

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.



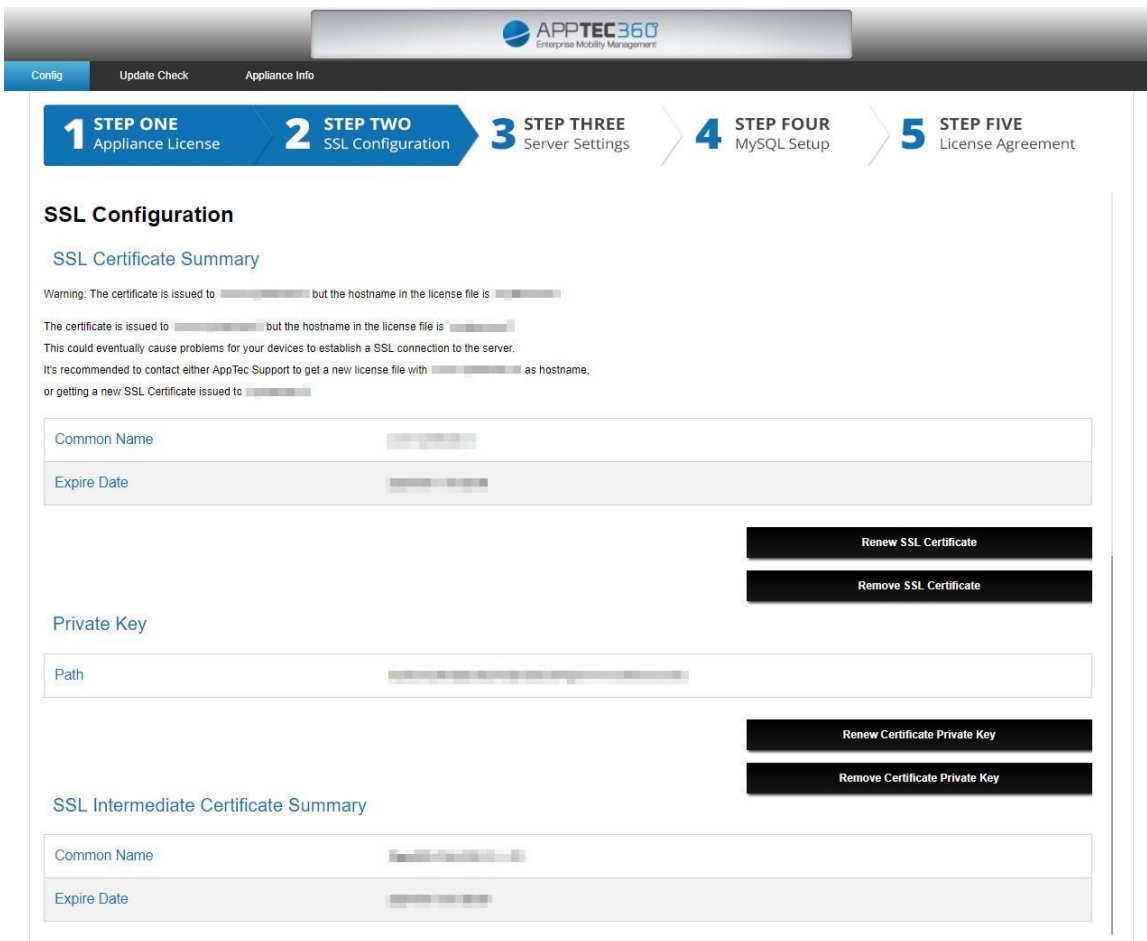
The screenshot displays the AppTec360 configuration interface. At the top, there is a navigation bar with the AppTec360 logo and the text 'Enterprise Mobility Management'. Below this, a progress bar shows five steps: 1. STEP ONE Appliance License (highlighted), 2. STEP TWO SSL Configuration, 3. STEP THREE Server Settings, 4. STEP FOUR MySQL Setup, and 5. STEP FIVE License Agreement. The main content area is titled 'Appliance License'. It contains three buttons: 'Upload a new License File', 'Upload an Appliance Configuration File', and 'Download the Appliance Configuration'. Below these buttons, there is a section titled 'Appliance License Information' which contains a table with the following fields: Appliance Alias, Hostname, Server Identifier, Contact Person Prenom, Contact Person Surname, Phone, and Mail. Each field has a corresponding input area with a small icon indicating the type of data entered.

Appliance License Information	
Appliance Alias	
Hostname	
Server Identifier	
Contact Person Prenom	
Contact Person Surname	
Phone	
Mail	



## Step 2

1. Upload the **“SSL-Certificate”** for the URL the license was issued for.  
You can see the URL in Step 1.
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.



The screenshot shows the AppTec360 Enterprise Mobility Management interface. At the top, there's a navigation bar with 'Config', 'Update Check', and 'Appliance Info'. Below this is a progress bar with five steps: 1. STEP ONE Appliance License, 2. STEP TWO SSL Configuration (active), 3. STEP THREE Server Settings, 4. STEP FOUR MySQL Setup, and 5. STEP FIVE License Agreement.

The main section is titled 'SSL Configuration'. It includes a sub-section 'SSL Certificate Summary' with a warning: 'Warning: The certificate is issued to [redacted] but the hostname in the license file is [redacted]. This could eventually cause problems for your devices to establish a SSL connection to the server. It's recommended to contact either AppTec Support to get a new license file with [redacted] as hostname, or getting a new SSL Certificate issued to [redacted]'. Below this are input fields for 'Common Name' and 'Expire Date'. To the right of these fields are two buttons: 'Renew SSL Certificate' and 'Remove SSL Certificate'.

Below the summary is the 'Private Key' section with a 'Path' input field. To the right of this field are two buttons: 'Renew Certificate Private Key' and 'Remove Certificate Private Key'.

At the bottom is the 'SSL Intermediate Certificate Summary' section with input fields for 'Common Name' and 'Expire Date'.

**Hint:** If you also want to use Windows Phone Devices you have to set up a separate Subdomain called “enterpriseenrollment.<Appliance FQDN>”.

You also have to get a certificate for this domain and upload on the bottom of the page in step 1.

## Step 3


1. Please enter the global support eMail address. This address will be used when you send the enrollment mails to the user.
2. Please change the username and password for the Server-/License manager



**Hint:** This is **not** the login to manage the devices. With this login you can add and remove licenses into the server in a multitenant environment.

The login name to manage the devices is the eMail address shown in “Included Client Licenses”- section in Step 1.

You will receive the password for the login per eMail, after you have finished the configuration in Step 5.



Config
Update Check
Appliance Info

**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

### Server Settings

Settings Summary

Server Domain	[REDACTED]
Console Path	/opt/console/
Apache Config Path	/opt/lampp/etc/httpd.conf
VHOST Path	/opt/lampp/etc/extra/httpd-vhosts.conf
VHOST SSL Path	/opt/lampp/etc/extra/httpd-ssl.conf
PHP Ini	/opt/lampp/etc/php.ini
MySQL Ini	/opt/lampp/etc/my.cnf

### Server Settings

Global Support eMail Address

[REDACTED]

You can use the Server Manager Credentials to login at mydevice.at in order to export your data or delete accounts.  
 Don't use your email address as username, use something like "verySecretUsername" instead.

Username for Server Manager

[REDACTED]

Password for Server Manager

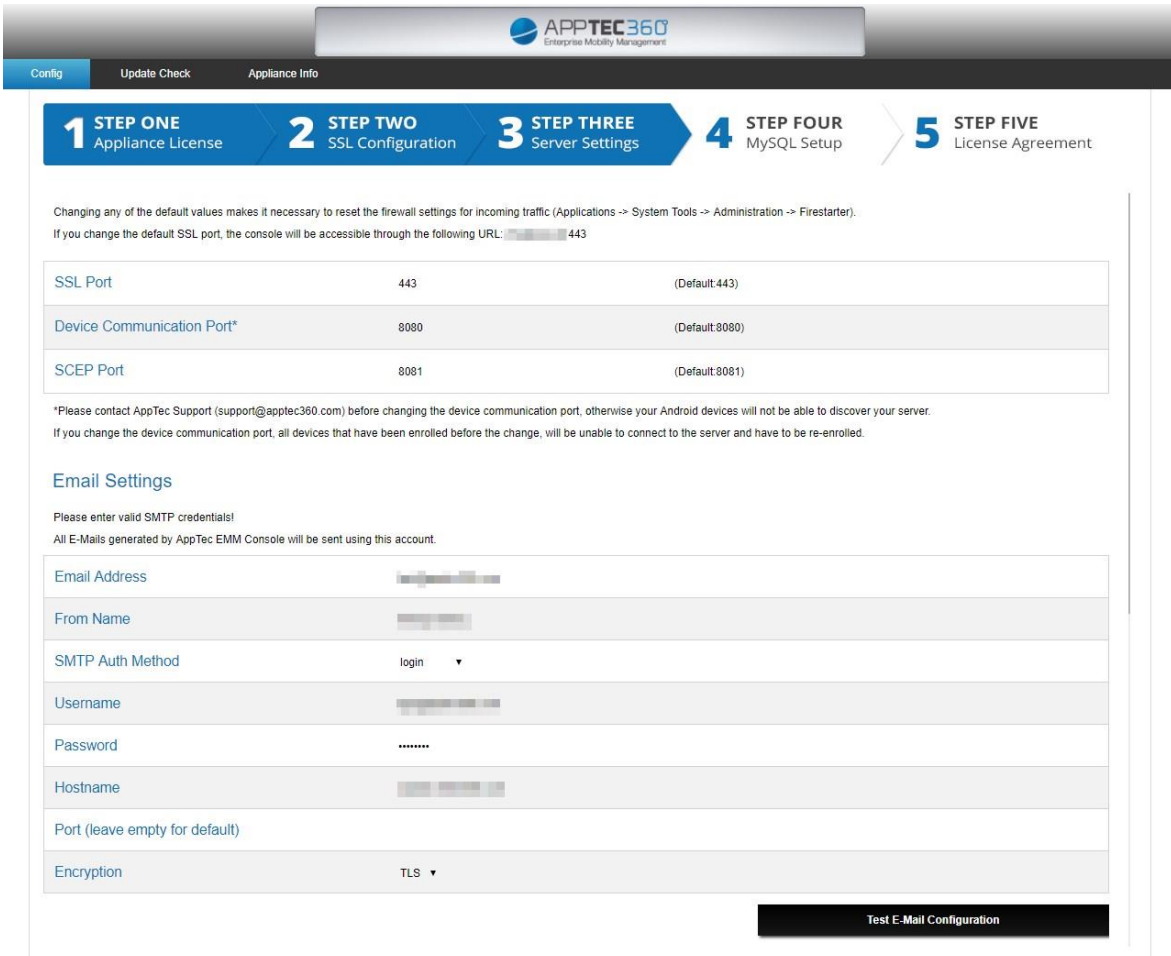
[REDACTED]

All data in the MySQL Database will be encrypted with the following key.

If you loose this key, or change this key after you configured the appliance, all your data will be lost.



- If needed for your environment, you can change the Ports, else the default values will be used.



Config Update Check Appliance Info

**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

Changing any of the default values makes it necessary to reset the firewall settings for incoming traffic (Applications -> System Tools -> Administration -> Firestarter).  
 If you change the default SSL port, the console will be accessible through the following URL:  443

SSL Port	443	(Default:443)
Device Communication Port*	8080	(Default:8080)
SCEP Port	8081	(Default:8081)

\*Please contact AppTec Support (support@apptec360.com) before changing the device communication port, otherwise your Android devices will not be able to discover your server.  
 If you change the device communication port, all devices that have been enrolled before the change, will be unable to connect to the server and have to be re-enrolled.

### Email Settings

Please enter valid SMTP credentials!  
 All E-Mails generated by AppTec EMM Console will be sent using this account.

Email Address	<input type="text"/>
From Name	<input type="text"/>
SMTP Auth Method	login ▼
Username	<input type="text"/>
Password	<input type="password"/>
Hostname	<input type="text"/>
Port (leave empty for default)	<input type="text"/>
Encryption	TLS ▼


**Test E-Mail Configuration**

- In the “Email Settings”, please enter the SMTP-Credentials for the eMail Account.  
 This account will be used to send emails to the user and also to send Bug Reports and Feature Requests to “[support@apptec360.com](mailto:support@apptec360.com)”. After you have entered the eMail settings please press on the right below button on “Save”.  
 Now you can test the eMail configuration.



## **Step 4**

1. If you want to use the internal database you can skip this step or you can enter the information for the external database.

 APPTEC360  
Enterprise Mobility Management

ConfigUpdate CheckAppliance Info

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

### MySQL Setup

The MySQL connection has been successfully tested at 2017-09-27 12:01:59

If you change the settings after the initial configuration, you have to reconfigure your appliance by clicking on "Configure now" in step 5

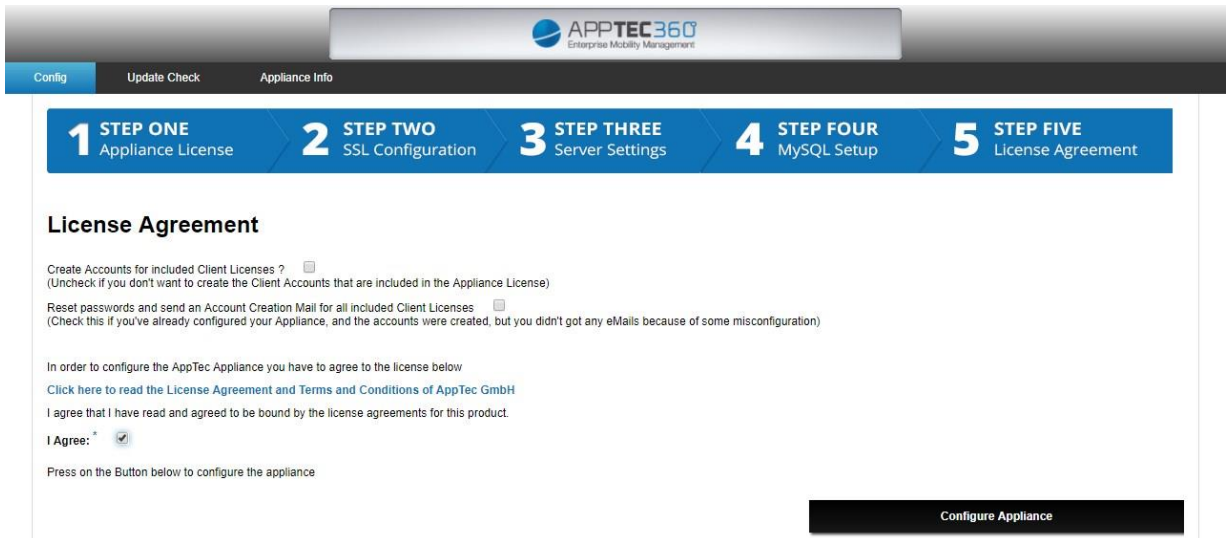
IP Address or Hostname	127.0.0.1	(Default: 127.0.0.1)
Username	AppTec	(Default: AppTec)
Password	AppTec	(Default: AppTec)
Port	3306	(Default: 3306)



## **Step 5**

1. Please make sure “Create Accounts for included Client Licenses” is checked. If not check it, and save the settings.  
Next, 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.



The screenshot shows the AppTec360 configuration interface. At the top, there is a navigation bar with tabs: Config, Update Check, and Appliance Info. Below this is a progress bar with five steps: 1 STEP ONE Appliance License, 2 STEP TWO SSL Configuration, 3 STEP THREE Server Settings, 4 STEP FOUR MySQL Setup, and 5 STEP FIVE License Agreement. The current step, Step 5, is highlighted. The main content area is titled "License Agreement" and contains the following text:

Create Accounts for included Client Licenses ? ☒  
(Uncheck if you don't want to create the Client Accounts that are included in the Appliance License)

Reset passwords and send an Account Creation Mail for all included Client Licenses ☒  
(Check this if you've already configured your Appliance, and the accounts were created, but you didn't got any eMails because of some misconfiguration)

In order to configure the AppTec Appliance you have to agree to the license below  
[Click here to read the License Agreement and Terms and Conditions of AppTec GmbH](#)

I agree that I have read and agreed to be bound by the license agreements for this product.

I Agree: ☒

Press on the Button below to configure the appliance

At the bottom right, there is a black button labeled "Configure Appliance".

## **Congratulations!**

You have finished the configuration of the virtual appliance.

You are now able to login into the console and manage your devices.

The login name to manage the devices is the eMail address shown in “Included Client Licenses”- section in Step 1.

You will receive the password for the login per eMail, after you have finished the configuration in Step 5.

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

You will find the hostname of your appliance in Step 1  
(e.g <https://emm.example.com> ).



## Configure from external host

If you'd like to configure your AppTec appliance from an external host, perform the following steps:

- Create a file named “externalConfigPassword” in /opt/console/application/configs/
- Enter a password in this file, for example “myVerySecretPassword” (an empty password is not allowed).
- Type the following URL in your browser  
http://<myHostname>/public/config/extconfig/pwd/myVerySecretPassword  
(configuration over HTTPS is possible after the appliance has been configured at least once).
- Now you can configure your appliance from an external host. The access is valid for an hour. Retype the URL if the session had expired..
- **Please delete the “externalConfigPassword” file after successful configuration**



## Security Recommendations

It's recommended to perform the following steps to secure your AppTec appliance. This is not a full set of instructions, it's just a recommendation for a basic configuration.

- Change password for user root and apptec
- Disable autologin for user apptec
- Change password for MySQL user "root" and "AppTec"
- Change the default SSH server port
- Block port 80 in your console, don't allow incoming HTTP traffic, only use HTTPS (once configured, an external configuration over HTTPS is possible too)
- Delete the file /opt/console/application/configs/externalConfigPassword
- Configure the firewall

### Quick Steps

#### Three Initial Steps for the Enterprise Mobile Manager

1. To manage iOS devices upload an **Apple Push Certificate** under General Settings > iOS Configuration.
2. **Add a User and a Device.** Using the gear icon whilst a group is selected, click "Add User". To add a device, select the user the device should belong to, select the gear icon and click "Add and Enroll a device".
3. To push Device- or Group Profile configuration changes onto the device, click on "Save" and then on "Assign now" at the bottom right corner of the console.



## III. General Settings

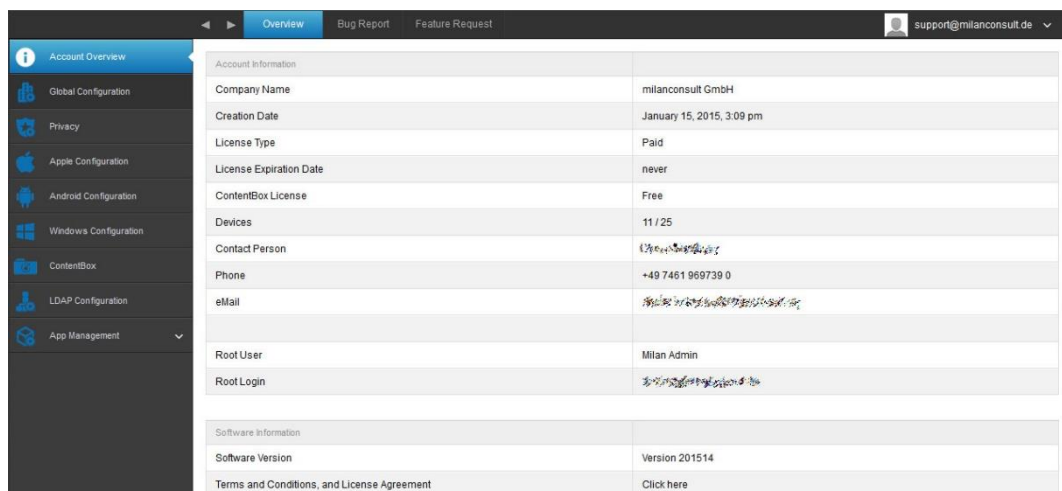
### Account Overview

#### Overview

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

Company Name	Your company name
Creation Date	Creation date of AppTec
License Type	Paid = paid license Free = unpaid license
License Expiration Date	Expiration date of your AppTec license
ContentBox License	Free = free license for 25 devices Paid = paid license for x devices
Devices	How many devices have been registered and how many more can be registered
Contact Person	provided contact person
Phone	provided telephone number
eMail*	provided email address
Root User	user on the EMM console
Root Login	email with which you register on the EMM Console
Software Version	current Software Version
Terms and Conditions, and License Agreement	General conditions (redirect to the AppTec webpage, where you will find varied PDF files on the topic)

**\*Note:** later you will see this account like every other account. If you change this eMail address you have to log in with this new address from now on.



The screenshot shows the 'Account Overview' page in the AppTec360 web interface. The left sidebar contains navigation links: Account Overview (selected), Global Configuration, Privacy, Apple Configuration, Android Configuration, Windows Configuration, ContentBox, LDAP Configuration, and App Management. The main content area is divided into two sections: 'Account Information' and 'Software Information'. The 'Account Information' section displays details for 'milanconsult GmbH', including creation date (January 15, 2015, 3:09 pm), license type (Paid), license expiration date (never), content box license (Free), devices (11 / 25), contact person, phone (+49 7461 969739 0), email, root user (Milan Admin), and root login. The 'Software Information' section shows the software version (Version 201514) and a link to the terms and conditions and license agreement (Click here).

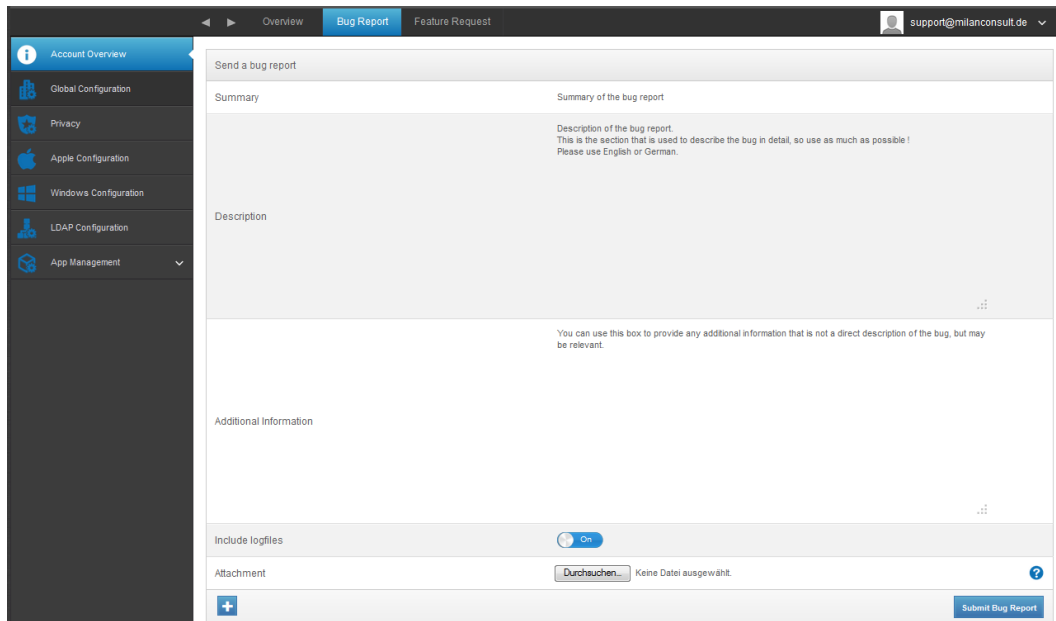
Account Information	
Company Name	milanconsult GmbH
Creation Date	January 15, 2015, 3:09 pm
License Type	Paid
License Expiration Date	never
ContentBox License	Free
Devices	11 / 25
Contact Person	
Phone	+49 7461 969739 0
eMail	
Root User	Milan Admin
Root Login	
Software Information	
Software Version	Version 201514
Terms and Conditions, and License Agreement	<a href="#">Click here</a>



## Bug Report

A bug report can be sent directly to support, via the internet interface.

Summary	A brief synopsis of your problem
Description	A detailed description of your problem, please be as specific as possible
Additional Information	Additional information that do not directly relate to the problem, but could prove useful
Include logfiles	Option to send the log files along
Attachment	Attach to the bug report
Blue Plus Symbol	For additional attachments
Submit Bug Report	Send bug report



The screenshot shows the 'Bug Report' section of the AppTec360 administration interface. The top navigation bar includes 'Overview', 'Bug Report' (selected), and 'Feature Request'. A user profile 'support@milanconsult.de' is visible in the top right. The left sidebar contains a menu with 'Account Overview' (selected), 'Global Configuration', 'Privacy', 'Apple Configuration', 'Windows Configuration', 'LDAP Configuration', and 'App Management'. The main content area is titled 'Send a bug report' and contains the following sections:

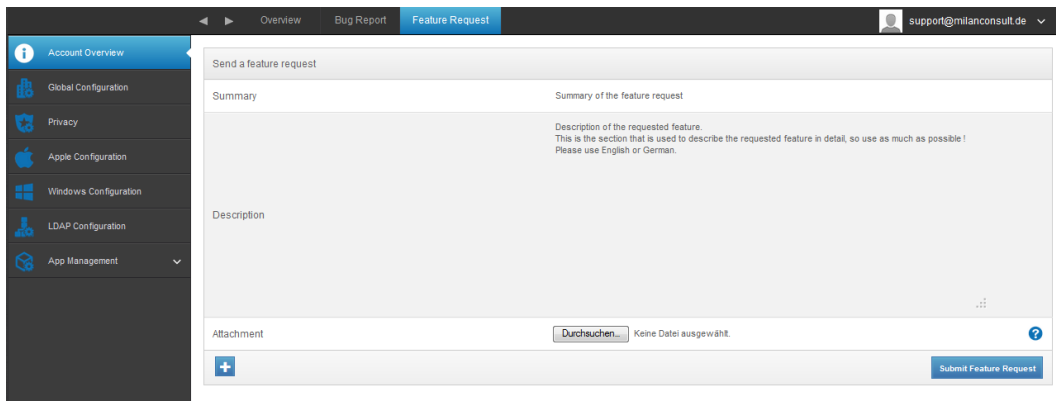
- Summary:** A text area for a brief synopsis of the problem.
- Description:** A large text area for a detailed description of the problem, with instructions: 'Description of the bug report. This is the section that is used to describe the bug in detail, so use as much as possible! Please use English or German.'
- Additional Information:** A text area for additional information that is not a direct description of the bug, with instructions: 'You can use this box to provide any additional information that is not a direct description of the bug, but may be relevant.'
- Include logfiles:** A toggle switch currently set to 'On'.
- Attachment:** A button labeled 'Durchsuchen...' (Browse...) with the text 'Keine Datei ausgewählt.' (No file selected.) and a blue plus icon for additional attachments.
- Submit Bug Report:** A blue button at the bottom right to submit the report.



## Feature Request

A feature request can be sent directly to support via the internet interface.

Summary	A brief synopsis of your problem
Description	A detailed description of your problem, please be as specific as possible
Attachment	Attach to the bug report
Blue Plus Symbol	For additional attachments
Submit Feature Request	Send feature request



Send a feature request

Summary

Summary of the feature request

Description

Description of the requested feature.  
This is the section that is used to describe the requested feature in detail, so use as much as possible!  
Please use English or German.

Attachment

Durchsuchen... Keine Datei ausgewählt.

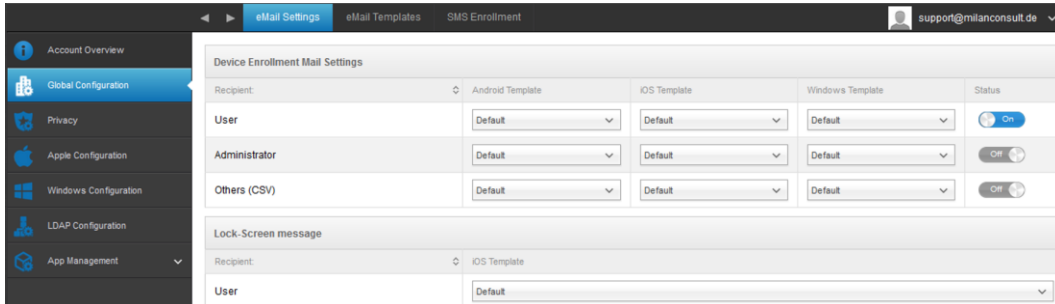
Submit Feature Request



## Global Configuration

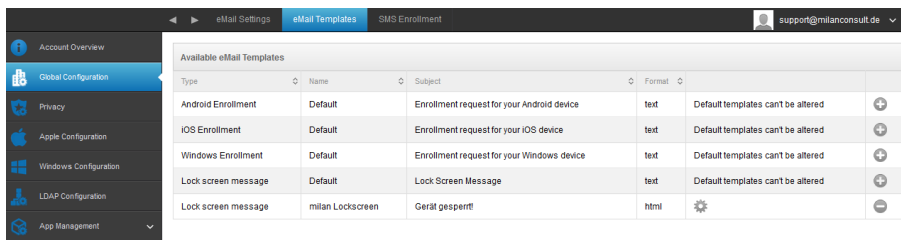
### eMail Settings

This is where the templates can be established for the respective scenarios and operating systems.



### eMail Templates


Here, you have the option to create templates for a variety of scenarios, such as for a Lock Screen or also the general email for the rollout.



Type	Name	Subject	Format	
Android Enrollment	Default	Enrollment request for your Android device	text	Default templates can't be altered
iOS Enrollment	Default	Enrollment request for your iOS device	text	Default templates can't be altered
Windows Enrollment	Default	Enrollment request for your Windows device	text	Default templates can't be altered
Lock screen message	Default	Lock Screen Message	text	Default templates can't be altered
Lock screen message	milan Lockscreen	Gerät gesperrt!	html	⚙️

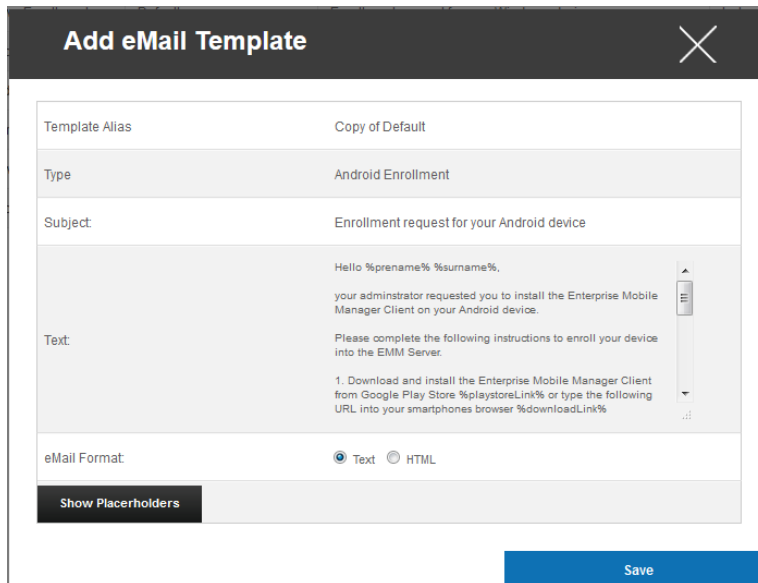
The default templates cannot be edited or erased.

With the “Plus Symbol”, after the respective Standard Templates, additional Templates can be created.

With the  Symbol, you make changes to the Template.



An example could look like the following:



The screenshot shows a modal window titled "Add eMail Template" with a close button (X) in the top right corner. The form contains the following fields:

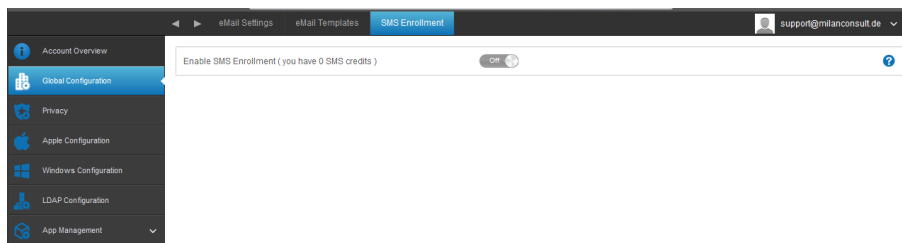
- Template Alias:** Copy of Default
- Type:** Android Enrollment
- Subject:** Enrollment request for your Android device
- Text:** A text area containing the following content:  
Hello %prename% %surname%,  
your administrator requested you to install the Enterprise Mobile Manager Client on your Android device.  
Please complete the following instructions to enroll your device into the EMM Server.  
1. Download and install the Enterprise Mobile Manager Client from Google Play Store %playstoreLink% or type the following URL into your smartphones browser %downloadLink%
- eMail Format:** Radio buttons for ☒ Text and ☐ HTML
- Show Placeholders:** A button located below the email format options.

A blue "Save" button is located at the bottom right of the dialog.

### 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.



The screenshot shows the "SMS Enrollment" settings page. On the left is a navigation menu with the following items: Account Overview, Global Configuration (selected), Privacy, Apple Configuration, Windows Configuration, LDAP Configuration, and App Management. The main content area has a breadcrumb trail: eMail Settings > eMail Templates > SMS Enrollment. At the top right of the main area is a user profile icon and the email address support@milanconsult.de. Below the breadcrumb trail is a toggle switch for "Enable SMS Enrollment ( you have 0 SMS credits )", which is currently turned off. A help icon (?) is located to the right of the toggle.

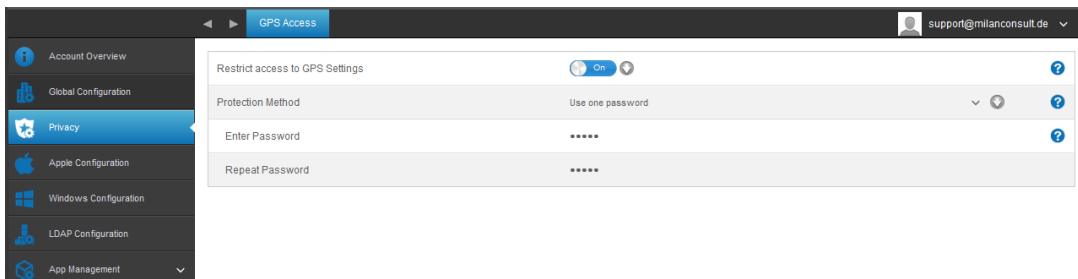


## Privacy

### GPS Access

In “GPS Access” you can set the localizing of a device with one or even two passwords for users, such as the board of directors and the IT department – “four-eyes-principle”.

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 2 <sup>nd</sup> chosen password
optional: Repeat Password 2	Re-enter 2 <sup>nd</sup> chosen password



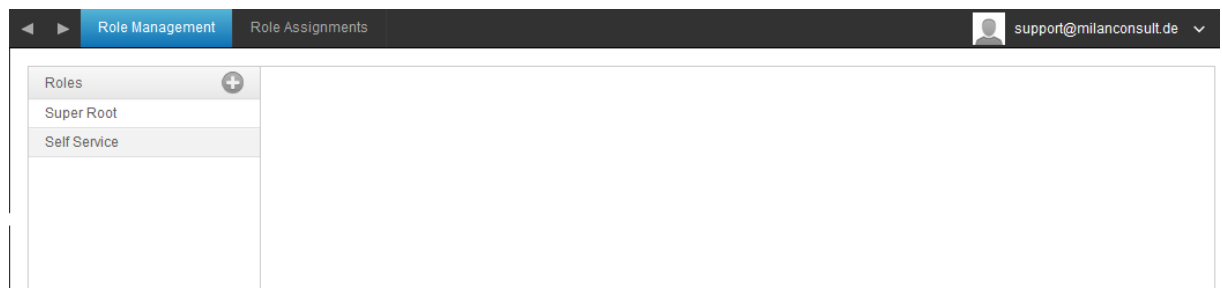


## Role Based Access

### Role Management

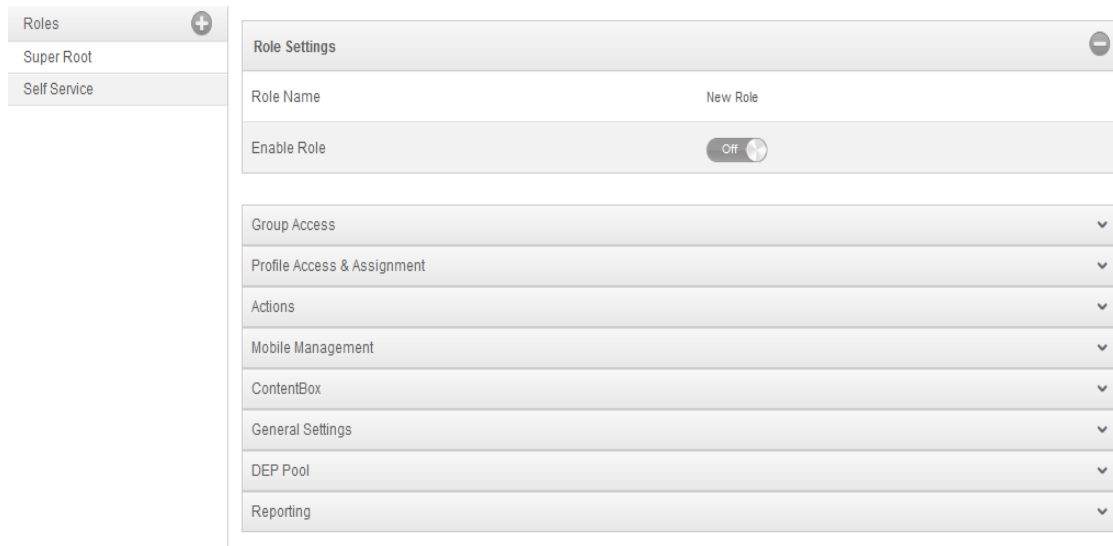
With the Role Management, it is now possible to perform role assignments for both Users and Admins.

This way, certain privileges can be assigned based on roles.



Super Root	“Super Admin” has access to all settings and configurations
Self Service (see below for further details)	Has sole access to “General Information”, “Asset Management” and “Anti Theft” (device localizing)

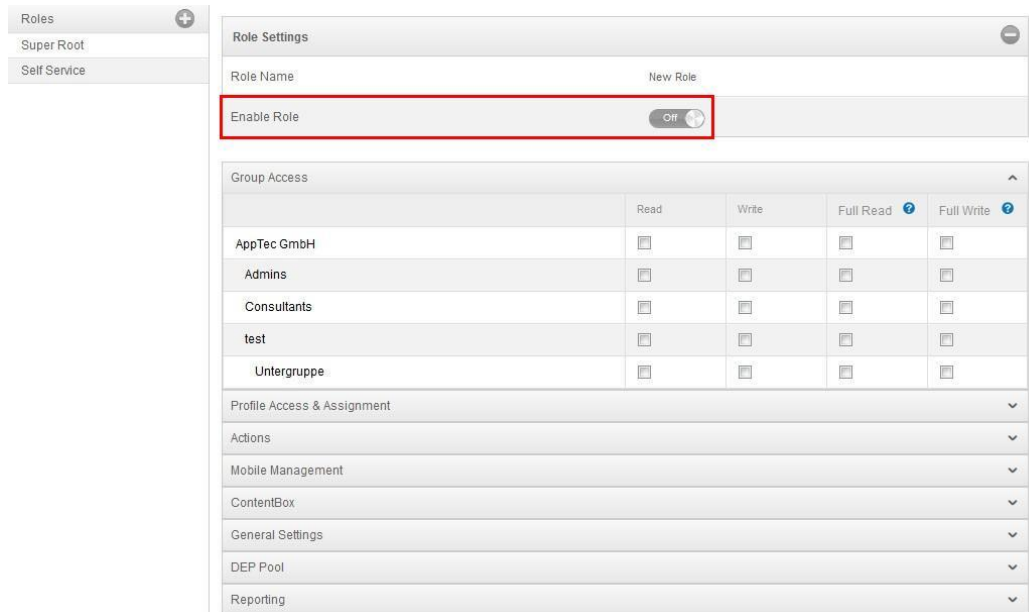
With the Plus Symbol a “new role” can be defined.



Here you can assign the new role a name and configure the permissions, according to your needs.



Please note that the role must be activated with “Enable Role”.



The screenshot shows the 'Role Settings' page for a new role. On the left, a sidebar lists 'Roles', 'Super Root', and 'Self Service'. The main area has a 'Role Name' field and a 'New Role' button. Below this is the 'Enable Role' toggle, which is currently 'Off' and is highlighted with a red box. Underneath is a 'Group Access' table with columns for 'Read', 'Write', 'Full Read', and 'Full Write'. The table lists groups: AppTec GmbH, Admins, Consultants, test, and Untergruppe, each with checkboxes for the four access levels. At the bottom, there are expandable sections for 'Profile Access & Assignment', 'Actions', 'Mobile Management', 'ContentBox', 'General Settings', 'DEP Pool', and 'Reporting'.

Read	Read privileges for the group (read only, no changes allowed)
Write	Write privileges for the selected group (changes can be made)
Full Read	The read privileges also apply to all sub-groups
Full Write	The write privileges also apply to all sub-groups

### Role Assignments

Here you are furnished with a complete overview of which role is assigned to which user. Likewise, you can see in the “Role Status”, if the role is currently activated.



The screenshot shows the 'Role Assignments' page. The top navigation bar includes 'Role Management' and 'Role Assignments'. The user 'support@milanconsult.de' is logged in. Below is a table with columns: Name, eMail, Role, and Role Status.

Name	eMail	Role	Role Status
Philipp [redacted]	[redacted]@apptec360.com	Test	Role enabled
Support [redacted]	support@	Super Root	Role enabled



### Assignment of a role

The assignment is performed in “Mobile Management”, by editing a user.  
 Here then, the “Assigned Roles” can be distributed to one or several roles.

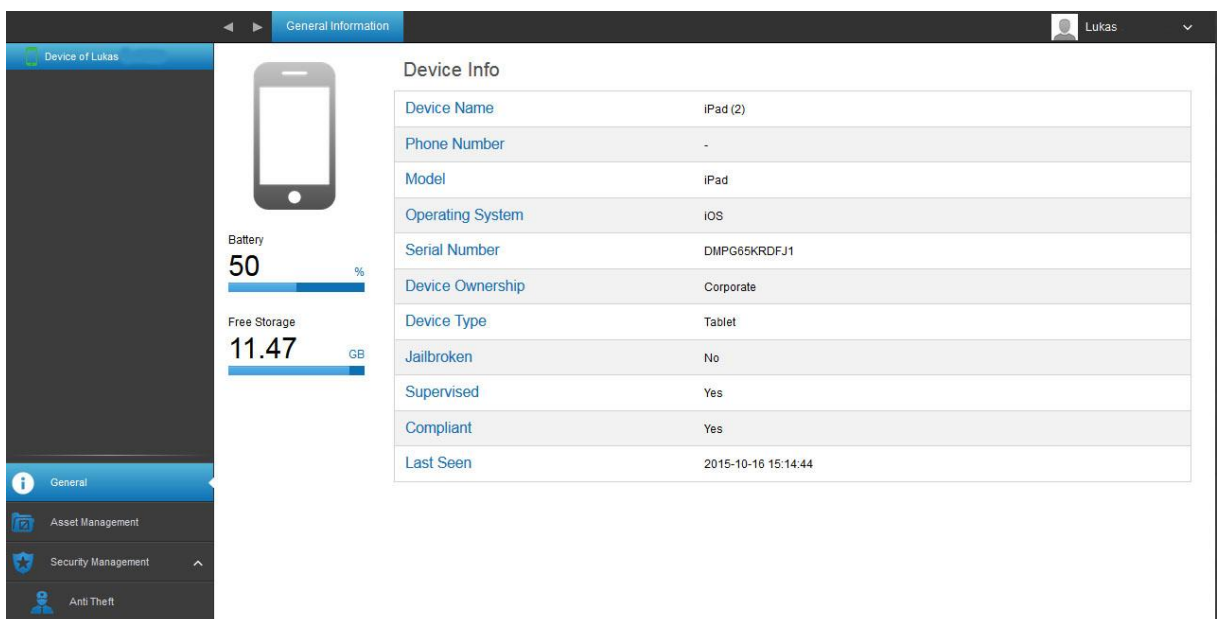
Assigned Roles	Super Root x	Test x	Self Service x
----------------	--------------	--------	----------------

### Self Service

For this, the user must be assigned a password, this is also accomplished under “Edit User” in “Mobile Management”.

Enter new password	?
Repeat new password	?

The user can then register at the already familiar URL  
 (i.e. if the AppTec Cloud is used) with their provided email address and the password that was defined by you.  
 With the Self Service Portal access is only available to “General Information”, “Asset Management” and the “Anti Theft” which provides the device localizing.



The screenshot displays the 'General Information' tab for a device named 'Device of Lukas'. The interface includes a sidebar with navigation options: General, Asset Management, Security Management, and Anti Theft. The main content area shows a device icon, battery status (50%), and free storage (11.47 GB). To the right, a 'Device Info' table lists various attributes.

Device Info	
Device Name	iPad (2)
Phone Number	-
Model	iPad
Operating System	iOS
Serial Number	DMPG65KRDFJ1
Device Ownership	Corporate
Device Type	Tablet
Jailbroken	No
Supervised	Yes
Compliant	Yes
Last Seen	2015-10-16 15:14:44



## API Access

AppTec APIs require an authentication token (api key) and a private key which can be obtained in the "API Access" Tab. Login into to AppTec EMM, go to General Settings → Role Based Access → API

Access to generate your api key and PEM encoded private key. The private key can only be downloaded once. After the download has started the key get's deleted, and the "Download" button disappears. If you lose your private key you have to generate a new one.

### **Access AppTec REST API**

The REST API is available by the following URL. All requests have to be send via HTTPS POST.

<AppTec EMM URL>/public/external/api

**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	signature inbase64	Base64 encoded signature of the payload

The request body must be a json encoded object. The object must contain the following values.

Field	Field Value	Description
api	device/listdevices	name of the api
params	object	additional parameters that may be necessary for the api call
time	1529662725	Unix Timestamp (UTC) of the client machine. Max time difference between client and server is 30 minutes.

Example: {"api":"deviceVlistgpsdata","time":1529664840,"params":{"deviceid":"10"}}

A full HTTP request looks like this

POST /public/external/api HTTP/1.1

Host: myapptecemm.com

Accept: \*/\*

Content-Type: application/json

auth: 1234567890abcdefghijklmnopqrstuvwxyz

signature:

a/bnOV466a0SiyVfsbbspZ+NxiTpmeF18NkfnOlq+OrEZDu9+VW7ESKziPXvwkTM5B9j/t1WGN1mRcl

Ke80m8fDKPj+lr3BqoMJe7wGXift+uy6iS7Chpdz2iZA4KPxkxU9ZGU2cdQ/SQceX57pi+ch7ApxBEVX2

+lJapTwA6CfB0mJFaf4MPcg/7LZWkzKxKF7LN/WzNJHiy/vSpZcqjbXjpC4HWrX6j2uZG5eSP8kYcTR

9VQfGtkX9pcyaNAwguR7zOOwMu/8L0oKq21/19rkabE4ZgUjtKS2++q+rh6mrP1g4BCZ7Xq/wvgZkaP

b0CStBdMRvj46i3enxCXcLQQ==

Content-Length: 74

{"api":"deviceVlistgpsdata","time":1529665112,"params":{"deviceid":"10"}}

On success the API returns a json encoded answer object and HTTP status code 200.



A response object for a successful API call always contains the field success. The field has either the value true, otherwise the response object will contain an array with the key errors, which contains a list of error messages.

If an error occurs, the HTTP status code will be 4xx or 5xx depending on the error.

The API will return

a human readable error message.

Example answer for a successful API call with HTTP 200 Code

```
{"status":true}
```

#### **API: List all devices**

Functionality: Returns a list of all devices containing the AppTec ID, IMEI and Serial

API URI: device/listdevices

Optional Parameters: none

Example Request Data

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

Example Response

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

#### **API: Get (GPS) Position List**

Functionality: Returns a list of all stored position log entries.

API URI: device/listposition

Mandatory Parameters: id: the device id

Optional Parameters: none

Example Request Data

```
{
  "api": "device/ listposition ",
  "params": {
    "id":10
  },
  "time": 1529662725
}
```

Example Response

```
{
  "success": true,
  "errors": [],
  "list":[
    {"time":"1535643051","pos":"47.549581,7.596334"},
    {"time":"1529673051","pos":"47.549581,7.596334"},
    {"time":"1529670029","pos":"48.1224667,7.7359751"},
    {"time":"1529640124","pos":"48.1224667,7.7359751"}
  ]
}
```



```
]
}
```

#### Example Code in PHP

```
$apiUrl = "https://myapptecemm.com/public/external/api";
$privateKeyPath = 'path/to/private.key';
$apptecAPIAuthToken = "1234567890abcdefghijklmnopqrstuvwxyz";
$requestData = array(
    "api" => "user/listusers",
    "time" => time(),
    "params" => array()
);
//sign the request data json with the API private key
$signatureOfRequestData = "";
//encode the request data to json
$jsonEncodedRequestData = json_encode($requestData);
//read private key
$privateKeyData = file_get_contents($privateKeyPath);
if ($privateKeyData === false) {
    die("can't read private key");
}
//convert private key into openssl resource
$privateKeyResource = openssl_pkey_get_private($privateKeyData);
if ($privateKeyData === false) {
    die("can't parse private key");
}
//sign the request data with the private key
$signAlgorithm = OPENSSL_ALGO_SHA512; //constant for sha512 algorithm
$binarySignatureOfRequestData;
if (!openssl_sign($jsonEncodedRequestData, $binarySignatureOfRequestData,
    $privateKeyResource,
    $signAlgorithm)) {
    die("failed to sign data");
}
$signatureOfRequestData = base64_encode($binarySignatureOfRequestData);
if (!function_exists('curl_init')) {
    die('curl not installed');
}
$ch = curl_init();
if ($ch === false) {
    die('failed to init curl');
}
curl_setopt($ch, CURLOPT_URL, $apiUrl);
curl_setopt($ch, CURLOPT_HEADER, 0);
curl_setopt($ch, CURLOPT_RETURNTRANSFER, true);
curl_setopt($ch, CURLOPT_TIMEOUT, 10);
curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, 2);
curl_setopt($ch, CURLOPT_SSL_VERIFYHOST, true);
//setup header fields
$header[] = 'Content-Type:application/json';
$header[] = 'auth:' . $apptecAPIAuthToken;
$header[] = 'signature:' . $signatureOfRequestData;
```



```

curl_setopt($ch, CURLOPT_HTTPHEADER, $header);
//set payload
curl_setopt($ch, CURLOPT_POSTFIELDS, $jsonEncodedRequestData);
$output = curl_exec($ch);
$error = curl_error($ch);
$lastReceivedHttpCode = curl_getinfo($ch, CURLINFO_HTTP_CODE);
curl_close($ch);
if ($output === false) {
    die("invalid answer from server");
}
if ($lastReceivedHttpCode != 200) {
    echo "http error: $lastReceivedHttpCode\n";
    die($output);
}
$outputArray = json_decode($output, true);
if (!is_array($outputArray)) {
    die("failed to parse output");
}
echo "answer:\n" . print_r($output, true) . "\n";

```

Example Code in Java

```

public static void main(String[] args) {
    String apiUrl = " https://myapptecemm.com/public/external/api ";
    String privateKeyPath = "path/to /private.key";
    String apptecAPIAuthToken = "1234567890abcdefghijklmnopqrstuvwxyz";
    try {
        int unixTimestamp = (int) (System.currentTimeMillis() / 1000L);
        //JSON API https://github.com/stleary/JSON-java
        //feel free to use another one
        JSONObject params = new JSONObject();
        //set request data
        JSONObject requestData = new JSONObject();
        requestData.put("api", "user/listusers");
        requestData.put("time", unixTimestamp);
        requestData.put("params", params);
        String signatureOfRequestData = "";
        String jsonEncodedRequestData = requestData.toString();
        //read pem encoded private key from file
        String privateKeyPEM = "";
        BufferedReader bufferedReader = new BufferedReader(new
        FileReader(privateKeyPath));
        String line;
        while ((line = bufferedReader.readLine()) != null) {
            privateKeyPEM += line + "\n";
        }
        bufferedReader.close();
        //convert the data into binary format
        privateKeyPEM = privateKeyPEM.replace("-----BEGIN PRIVATE KEY-----\n", "");
        privateKeyPEM = privateKeyPEM.replace("-----END PRIVATE KEY-----", "");
        byte[] encoded = Base64.getMimeDecoder().decode(privateKeyPEM);
        //create private key object from binary format data
        PKCS8EncodedKeySpec spec = new PKCS8EncodedKeySpec(encoded);
    }
}

```



```

KeyFactory kf = KeyFactory.getInstance("RSA");
PrivateKey privateKey = kf.generatePrivate(spec);
//sign the request data
Signature privateSignature = Signature.getInstance("SHA512withRSA");
privateSignature.initSign(privateKey);
privateSignature.update(jsonEncodedRequestData.getBytes("UTF-8"));
byte[] signature = privateSignature.sign();
//encode the binary signature into base64
signatureOfRequestData = Base64.getEncoder().encodeToString(signature);
//connect to the api
URL myurl = new URL(apiUrl);
HttpsURLConnection con = (HttpsURLConnection) myurl.openConnection();
con.setRequestMethod("POST");
//set headers
con.setRequestProperty("Content-Type", "application/json");
con.setRequestProperty("auth", apptecAPIAuthToken);
con.setRequestProperty("signature", signatureOfRequestData);
con.setDoOutput(true);
con.setDoInput(true);
DataOutputStream output = new DataOutputStream(con.getOutputStream());
output.writeBytes(jsonEncodedRequestData);
output.close();
DataInputStream input = new DataInputStream(con.getInputStream());
//read answer
String answer = input.readLine();
input.close();
int lastReceivedHttpCode = con.getResponseCode();
if (lastReceivedHttpCode != 200) {
    System.out.println("http error: " + lastReceivedHttpCode);
    System.out.println(answer);
    return;
}
System.out.println("answer: " + answer);
} catch (Exception e) {
    System.out.println("error: " + e.getMessage());
    e.printStackTrace();
}
}
}
}

```



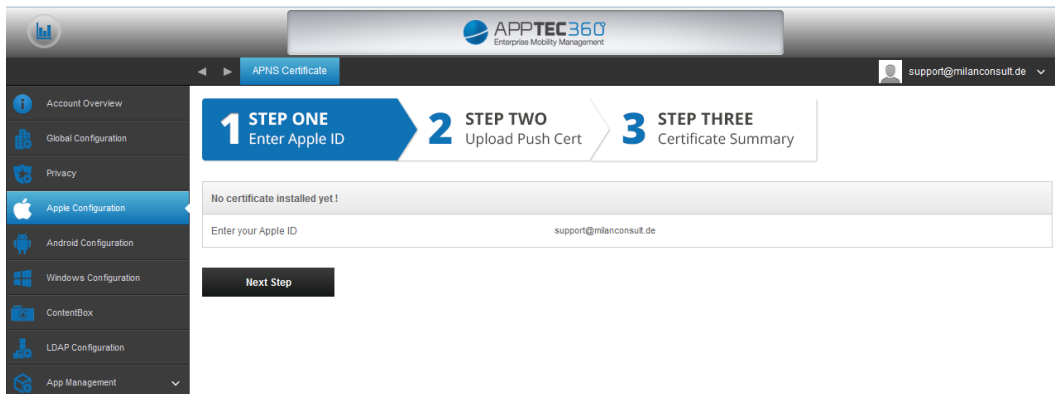
## iOS Configuration

### APNS Certificate

Here you can upload and manage an APNS-certificate – this certificate is necessary, so that AppTec and the iOS end user devices can communicate with each other.

Please note: this procedure must be repeated every year, due to the fact that an APNS certificate is only valid for one year.

In this case, the same Apple ID must be used, otherwise a future management of the iOS devices will not be possible and all devices must enrolled again.



The screenshot shows the AppTec360 web interface for APNS Certificate configuration. The top navigation bar includes the AppTec360 logo and the text "Enterprise Mobility Management". A user profile dropdown shows "support@milanconsult.de". The left sidebar contains a menu with options: Account Overview, Global Configuration, Privacy, Apple Configuration (selected), Android Configuration, Windows Configuration, ContentBox, LDAP Configuration, and App Management. The main content area displays a three-step process: STEP ONE Enter Apple ID (active), STEP TWO Upload Push Cert, and STEP THREE Certificate Summary. Below the steps, a message states "No certificate installed yet!". A form field labeled "Enter your Apple ID" contains the text "support@milanconsult.de". A "Next Step" button is located below the form field.

- First, enter your Apple ID and click on “Next Step” (Recommendation: in this case a generic Apple ID should be used)
- Next, download the “signedPushCertificate.txt” database, by clicking on it.
- Next, click on „Apple Push Certificates Portal“, you should be redirected to the following URL:

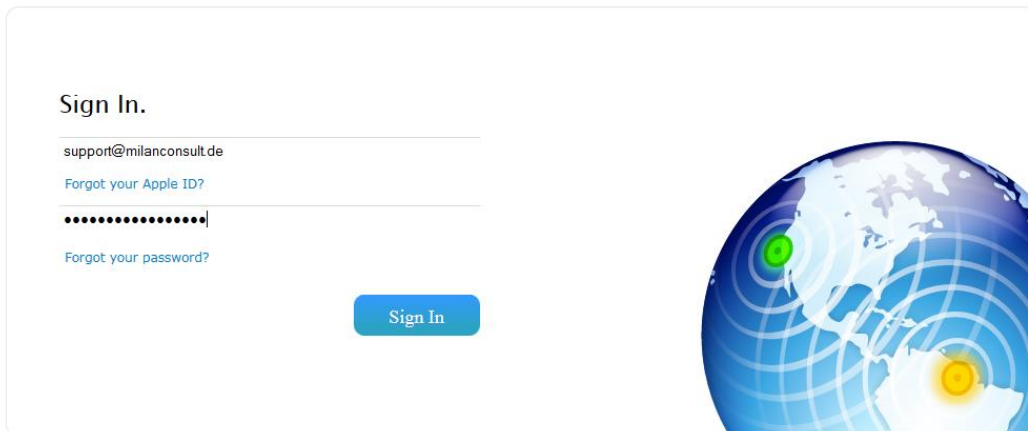


The screenshot shows the AppTec360 web interface for APNS Certificate configuration, Step Two: Upload Push Cert. The top navigation bar and left sidebar are identical to the previous screenshot. The main content area displays the three-step process: STEP ONE Enter Apple ID, STEP TWO Upload Push Cert (active), and STEP THREE Certificate Summary. Below the steps, a message states "Register your signed push certificate." followed by three numbered instructions: 1. Download this signedPushCertificate.txt, 2. Upload the certificate to Apple Push Certificates Portal, and 3. You will get a .pem file. Upload the .pem file. Below the instructions, a section labeled "Choose your .PEM file" contains a file selection button labeled "Durchsuchen" and the text "Keine Datei ausgewählt.". Below this section are "Upload" and "Back" buttons.



- Now, sign in with your Apple Account.

## Apple Push Certificates Portal



Sign In.


support@milanconsult.de

[Forgot your Apple ID?](#)

.....

[Forgot your password?](#)

[Sign In](#)

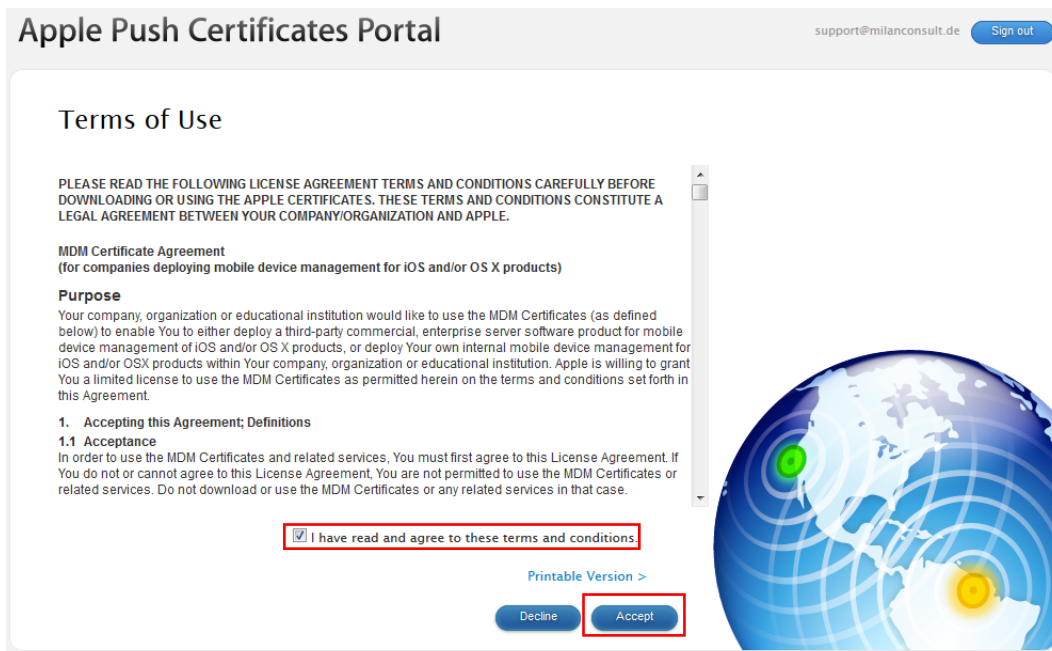


- Once you have successfully signed in, click on “Create a Certificate”.

## Certificates for Third-Party Servers

[Create a Certificate](#)

- Accept the General Terms and Conditions



Apple Push Certificates Portal

support@milanconsult.de [Sign out](#)

### Terms of Use

PLEASE READ THE FOLLOWING LICENSE AGREEMENT TERMS AND CONDITIONS CAREFULLY BEFORE DOWNLOADING OR USING THE APPLE CERTIFICATES. THESE TERMS AND CONDITIONS CONSTITUTE A LEGAL AGREEMENT BETWEEN YOUR COMPANY/ORGANIZATION AND APPLE.

**MDM Certificate Agreement**  
(for companies deploying mobile device management for iOS and/or OS X products)


**Purpose**  
Your company, organization or educational institution would like to use the MDM Certificates (as defined below) to enable You to either deploy a third-party commercial, enterprise server software product for mobile device management of iOS and/or OS X products, or deploy Your own internal mobile device management for iOS and/or OS X products within Your company, organization or educational institution. Apple is willing to grant You a limited license to use the MDM Certificates as permitted herein on the terms and conditions set forth in this Agreement.

**1. Accepting this Agreement; Definitions**  
**1.1 Acceptance**  
In order to use the MDM Certificates and related services, You must first agree to this License Agreement. If You do not or cannot agree to this License Agreement, You are not permitted to use the MDM Certificates or related services. Do not download or use the MDM Certificates or any related services in that case.

☒ I have read and agree to these terms and conditions.

[Printable Version >](#)

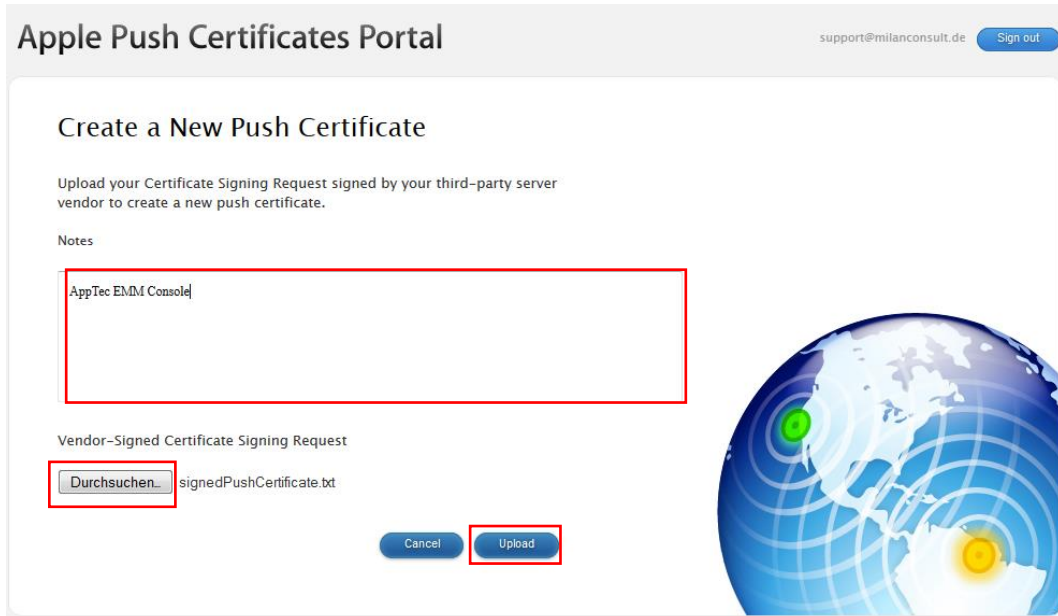
[Decline](#) [Accept](#)





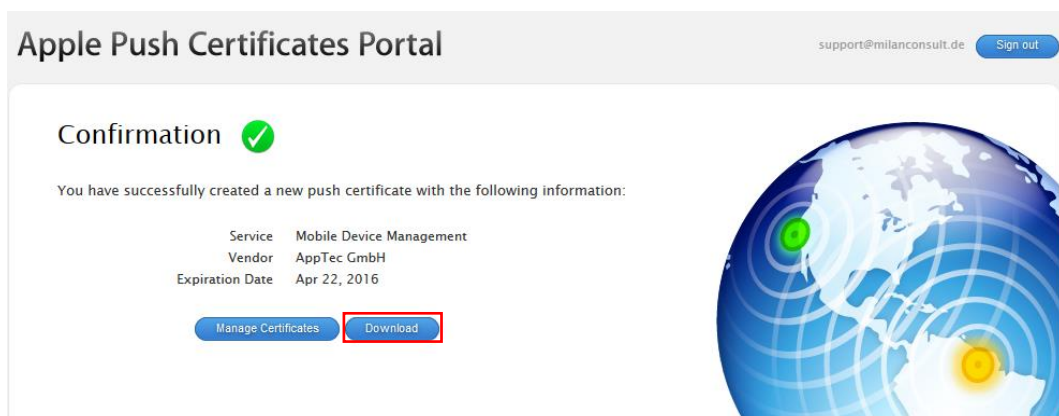
Click on „search...“and select the “signedPushCertificate.txt”, that you created.

- If needed, write an explanation (for a possible future classifying) in “Notes”.
- Then click on “Upload”.



The screenshot shows the 'Apple Push Certificates Portal' interface. At the top, there's a header with the portal name, a support email address, and a 'Sign out' button. The main heading is 'Create a New Push Certificate'. Below it, a text block instructs the user to upload a Certificate Signing Request signed by a third-party server vendor. A 'Notes' section contains a text area with 'AppTec EMM Console' entered. The 'Vendor-Signed Certificate Signing Request' section features a file input field with a 'Durchsuchen...' button, followed by the filename 'signedPushCertificate.txt'. At the bottom right of this section are 'Cancel' and 'Upload' buttons. A globe graphic is visible on the right side of the page.

- As a result you should see the following display



The screenshot shows the 'Confirmation' page of the 'Apple Push Certificates Portal'. It features a green checkmark icon and a message stating: 'You have successfully created a new push certificate with the following information:'. Below this, a table displays the certificate details:

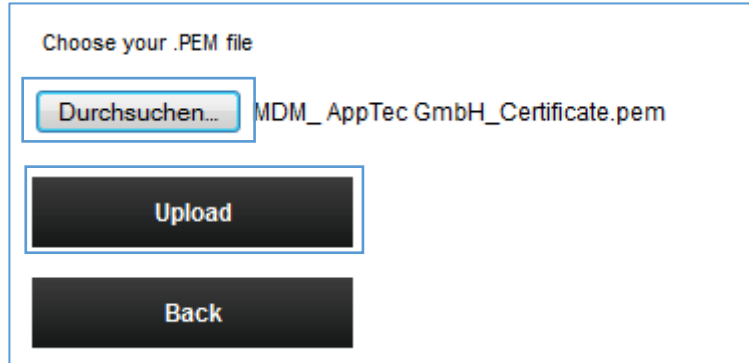
Service	Mobile Device Management
Vendor	AppTec GmbH
Expiration Date	Apr 22, 2016

At the bottom, there are two buttons: 'Manage Certificates' and 'Download', with the latter highlighted by a red box. A globe graphic is visible on the right side of the page.

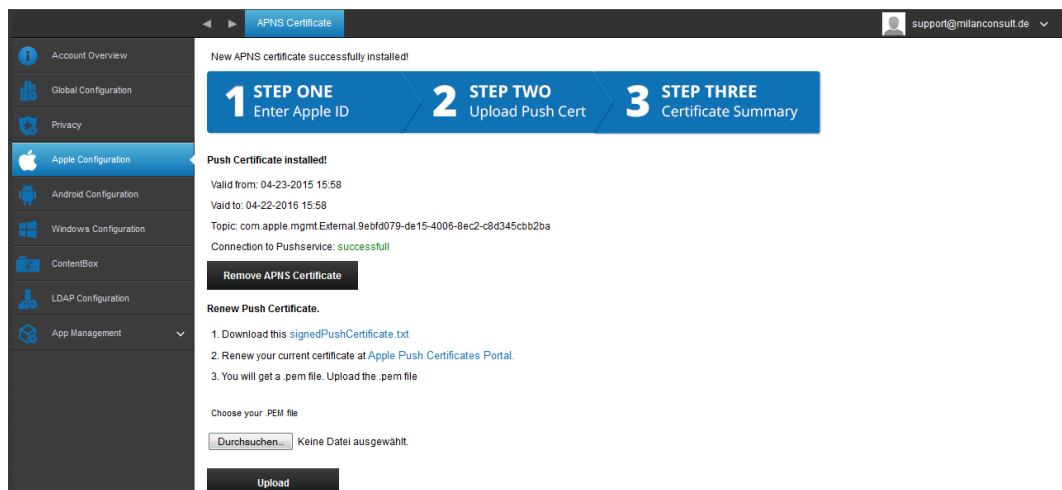
- Click on “Download”



- Now return to the AppTec Console and select “Choose your .PEM file”  
“Search...” underneath.
- Now, select the downloaded database and then click on “Upload”.



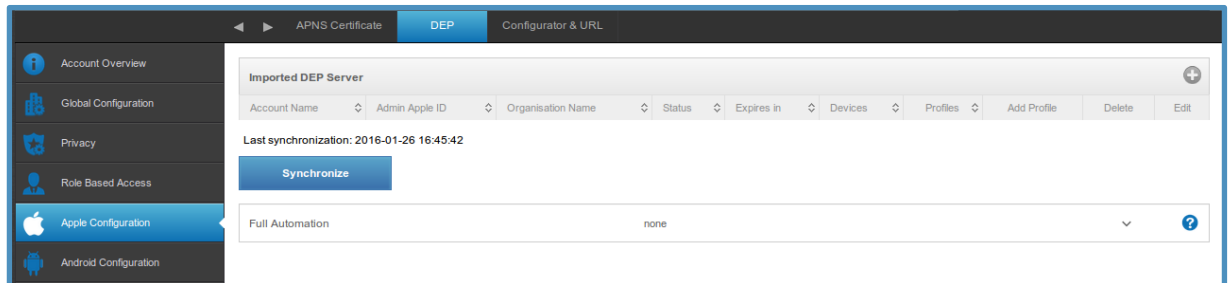
- Should this procedure complete successfully, then you should receive the following display – now you can enroll and manage Apple devices.



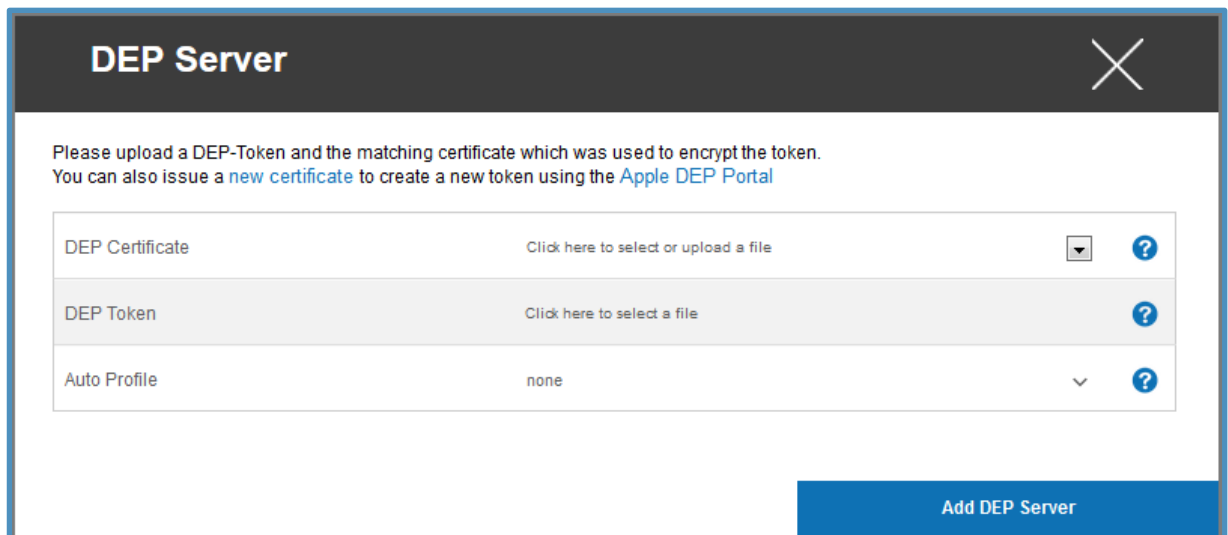


## DEP

Simplify the deployment of personal devices. Register the devices during the activation with App Tec and skip the elemental configuration steps, in order to quickly make the devices more easily available.



With the “Plus Symbol”, you can add the new DEP-Token, after which you will see the following display.

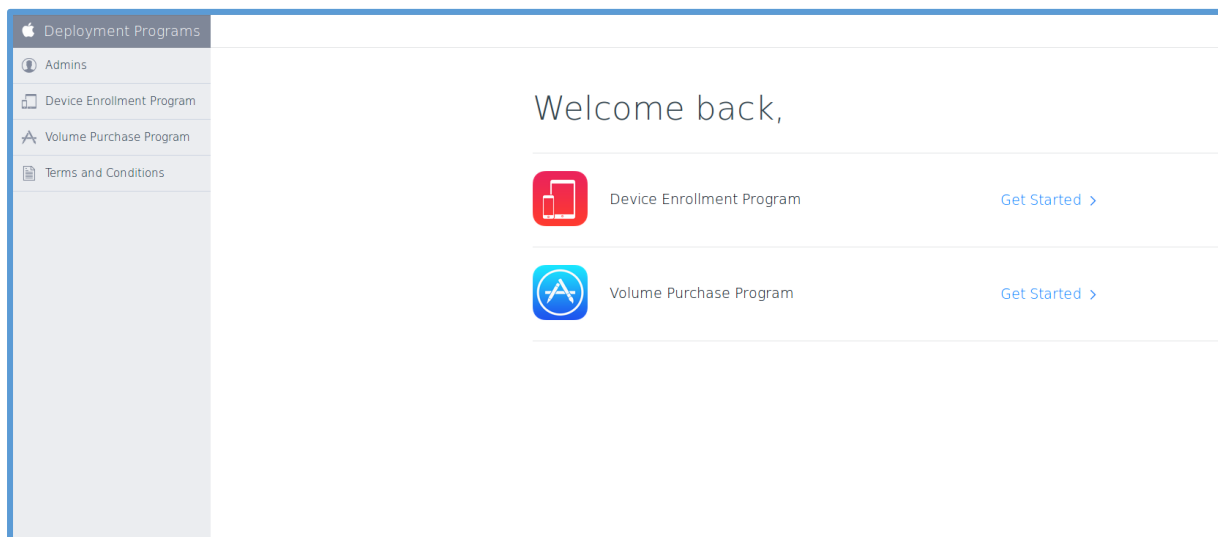


DEP Certificate	Here you have to upload the DEP certificate (PKCS12 file) which you received from Apple. <u>Or:</u> The Console can also generate a certificate, by selecting “new certificate”, which you can then download and later upload to the Apple DEP Portal.
DEP Token	Here you must upload the DEP Token that you received from Apple
Auto Profile	Automatic profile assignment

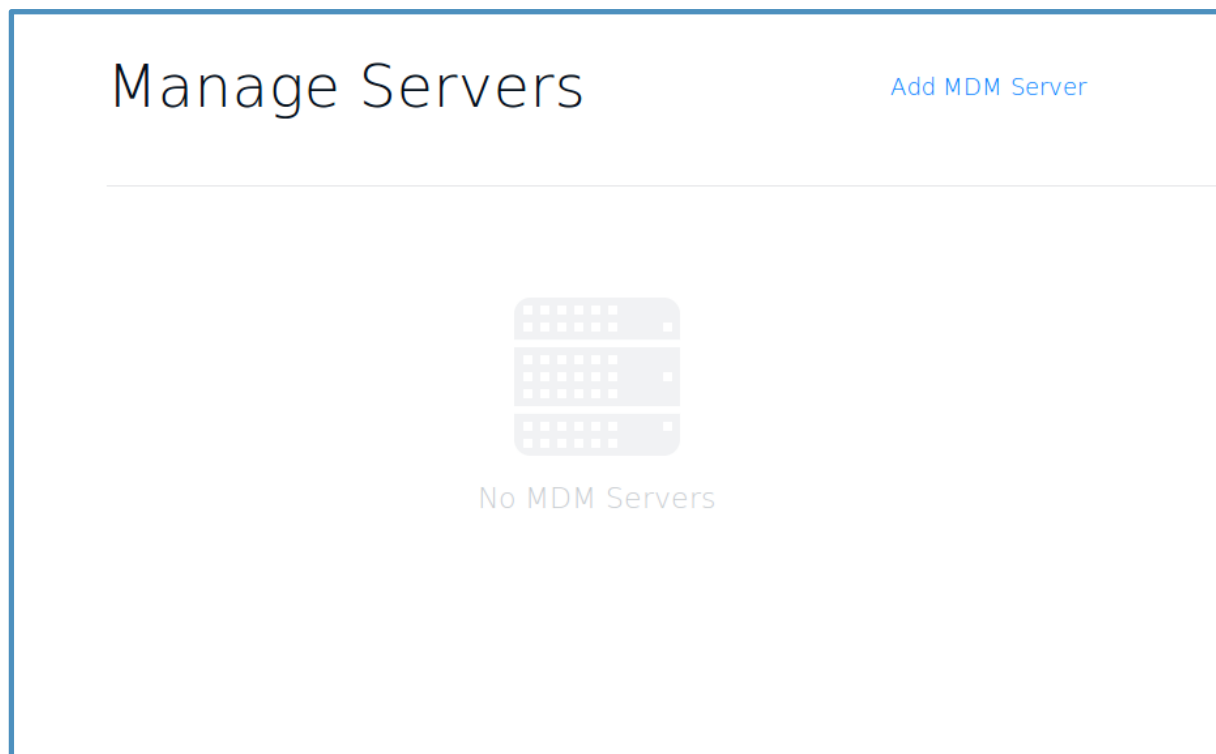


Open the Apple DEP Portal and add a new DEP Server.

Register in the Apple Portal and select “Device Enrollment Program” in the left column.



Click on “Add MDM Server“, in order to generate a new server.





Enter a name of your choice and activate “Automatically Assign New Devices”, so that new additional DEP devices can be automatically synced with the server.

## Add MDM Server

---

1. MDM Server Name.

DEP Server

Enter a name to refer to this server, department or location.

☐ Automatically Assign New Devices [?](#)

---

CancelNext

Now, upload the certificate (public Key), which you have already downloaded in the foreground via the Console – as long as you have selected “new certificate” in the AppTec Console in the foreground – otherwise, upload the same certificate here, that you also used on the AppTec Console.

## Add “DEP Server”

---

2. Upload Your Public Key.

Choose File...DEP\_Credential....

The public key certificate is used to encrypt the Authentication Token file for secure transfer to your MDM Server.

---

PreviousCancelNext




In this area, download the Token. In the next step, this Token must be uploaded to the AppTec Console.

## Add "DEP Server"

---

3. Download and Install your Server Token.

 Your Server Token

Contact your MDM vendor for installation instructions.


---

Previous







Done

Now return to the AppTec Console and upload the Token that you just downloaded, with "DEP Token".

### DEP Server



Please upload a DEP Token and the matching certificate which was used to encrypt the token.  
You can also issue a [new certificate](#) to create a new token using the [Apple DEP Portal](#)

DEP Certificate	DEP_Credential.p12(ID: 158)		
DEP Token	57 [REDACTED].p7m		
Auto Profile	none		

Add DEP Server

**Please note:** afterwards you can return to this point in order to change the "Auto Profile" point. After you have added the Server, you can edit it with the gear icon.

Click on "Add DEP Server", in order to add the server.




The table should now be populated with the information about the server that you just added. As you can see in the table, currently no devices have been added yet.

Imported DEP Server									
Account Name	Admin Apple ID	Organisation Name	Status	Expires in	Devices	Profiles	Add Profile	Delete	Edit
DEP Server		AppTec GmbH	Active	365 days		0	+	-	⚙

Return to the Apple DEP Portal, here the previously added servers should be displayed. Now, click on the name of the server.

# Manage Servers

[Add MDM Server](#)

Server Name	Number of Devices	Last Connected	Last Connected IP
 <a href="#">DEP Server</a>	0	Never	-

Select “Manage Devices” in the left column.

Deployment Programs

Admins

Device Enrollment Program

Manage Servers

**Manage Devices**

View Assignment History

Volume Purchase Program

Terms and Conditions

Search for Serial Number

## Manage Devices

1. Choose Devices By:  
☒ Serial Number ☐ Order Number ☐ Upload CSV File  

ABCD1234567, EFGH1234567

2. Choose Action:  

Assign to Server

OK



Now, add a device to the Apple DEP Server and assign it to the server that you just created.

## Manage Devices

---

1. Choose Devices By:

☒ Serial Number    ☐ Order Number    ☐ Upload CSV File

---

2. Choose Action:


Assign to Server    DEP Server

---

OK

Should the assignment have been performed successfully, then you should receive the following message.

Assignment Complete



Please ensure your MDM server uploads a new profile before these devices are activated.

OK



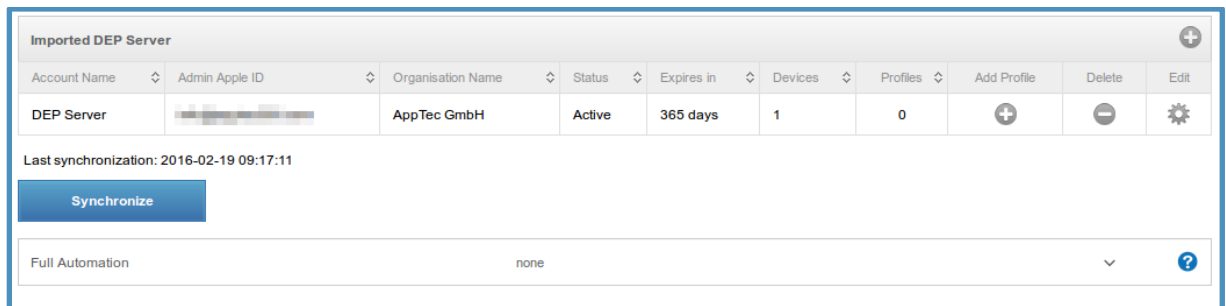
Please note: DEP profiles are independent of a MDM profile. These allow for additional device configurations, which can be applied during the activation of the device.

In order to apply these new changes on the device, the device must be reset (factory settings) and the activation of the device must be performed again.

Return to the AppTec Console and click on “Synchronize”, in order to refresh the server data.

Subsequently, the new device should be displayed.

Click on the Plus-Symbol in the column “Add Profile”, in order to add a DEP Profile.



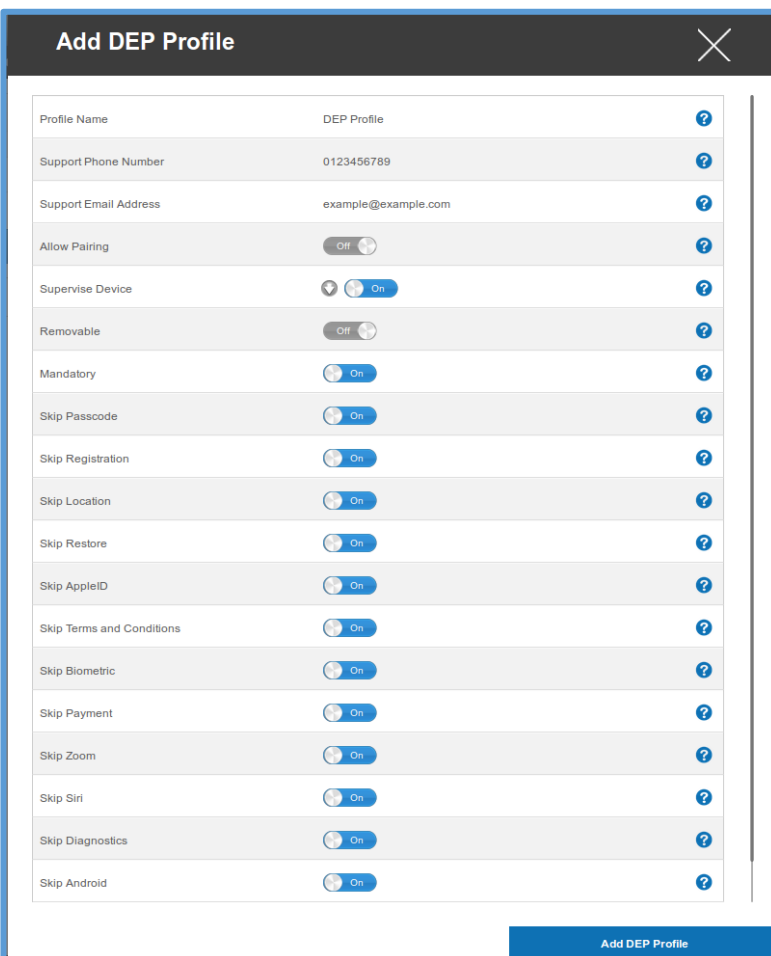
Account Name	Admin Apple ID	Organisation Name	Status	Expires in	Devices	Profiles	Add Profile	Delete	Edit
DEP Server	[REDACTED]	AppTec GmbH	Active	365 days	1	0	+	-	⚙️

Last synchronization: 2016-02-19 09:17:11

**Synchronize**

Full Automation: none

This will open a Popup with various options that you can configure and adapt to your needs.



### Add DEP Profile

Profile Name	DEP Profile	?
Support Phone Number	0123456789	?
Support Email Address	example@example.com	?
Allow Pairing	Off	?
Supervise Device	On	?
Removable	Off	?
Mandatory	On	?
Skip Passcode	On	?
Skip Registration	On	?
Skip Location	On	?
Skip Restore	On	?
Skip AppleID	On	?
Skip Terms and Conditions	On	?
Skip Biometric	On	?
Skip Payment	On	?
Skip Zoom	On	?
Skip Siri	On	?
Skip Diagnostics	On	?
Skip Android	On	?

**Add DEP Profile**

After you have performed the desired configurations, you can add the profile with “Add DEP Profile”.








Profile Name	Name of the profile
Support Phone Number	Phone Number that should be called if the user needs help
Support Email Address	Email Address that should be messaged if the user needs help
Allow Pairing	Allows connection between device and PC
Supervise Device	Sets the device in supervised mode
Removable	Allows user to remove the device profile
Mandatory	Forces supervised mode
Skip Passcode	Skips setup of the passcode
Skip Registration	Skips device-registration
Skip Location	Skips setup of GPS service
Skip Restore	Skips the restore options
Skip AppleID	Skips the setup of an AppleID
Skip Terms and Conditions	Skips the Terms and Conditions
Skip Biometric	Skips setup for TouchID
Skip Payment	Skips setup for payment information
Skip Zoom	Skips zoom setup
Skip Siri	Skips Siri setup
Skip Diagnostics	Skips the option to send diagnostic information
Skip Android	Skips Android import
Skip FileVault	Skips FileVault setup

Now the profile will be displayed in the table "Profiles" and/or a counter will increase by one number. You can click on the number, in order to list all of the profiles.

However, you cannot edit the profiles, they can only be removed.

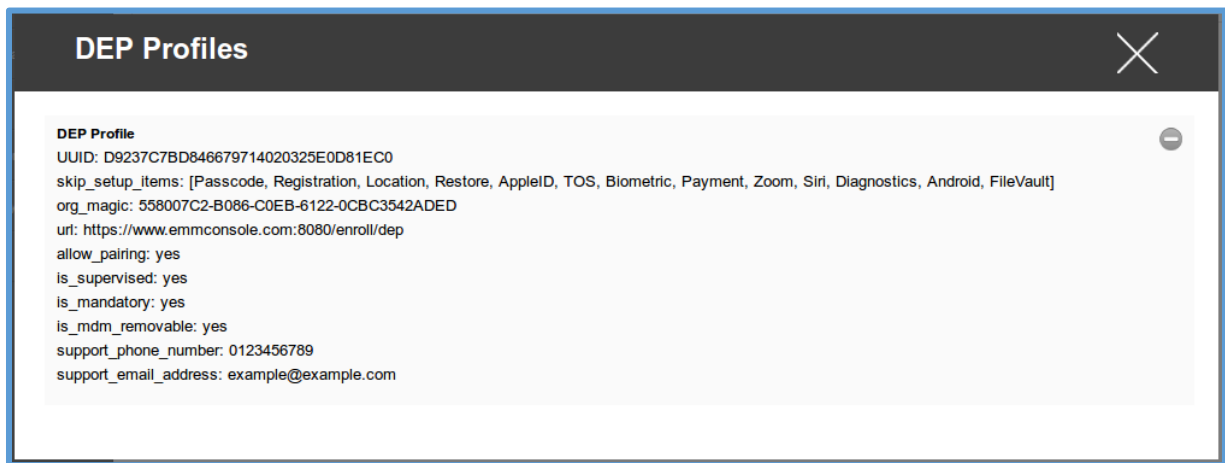
If a profile has been assigned to a device, then the profile cannot be removed.

Imported DEP Server										
Account Name	Admin Apple ID	Organisation Name	Status	Expires in	Devices	Profiles	Add Profile	Delete	Edit	
DEP Server		AppTec GmbH	Active	365 days	1	1				
Last synchronization: 2016-02-19 09:17:11										
<b>Synchronize</b>										
Full Automation none 										



If you want to remove the profile, you can accomplish this with the Minus-Symbol in the upper right hand corner.

You can click on the number to list all profiles



Return to the Mobile Management and refresh the page.

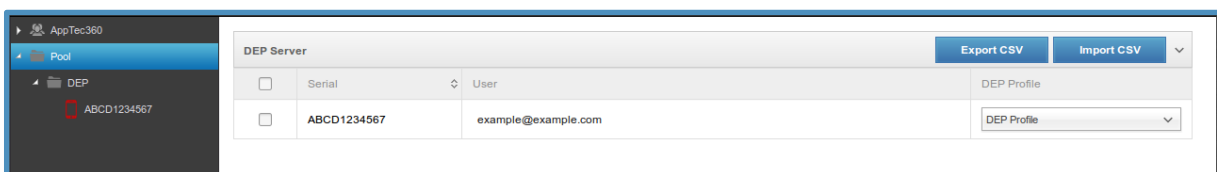
A Pool Category will be listed, where your DEP device can be seen.

Click on "DEP" - here you can see all of the DEP devices, based on their serial number.

In the User-Column, you can add the desired user's email-address that is to receive the device.

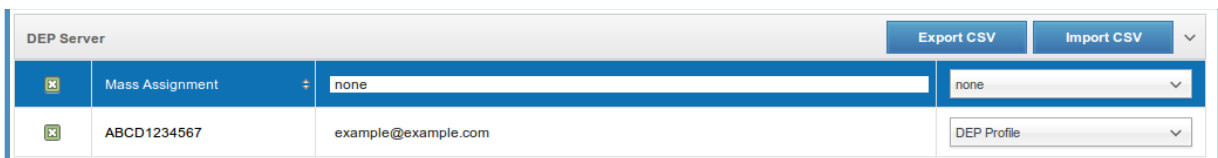
In the DEP Profile-Column, select the previously generated profile.

You can also import a CSV file, in order to perform these configurations. To receive a template, you can click on "Export CSV".



You can also perform changes for multiple DEP devices, by clicking the checkbox next to the device name / serial number.

In order to select all of the devices, you can select the checkbox in the first column, next to "Serial".

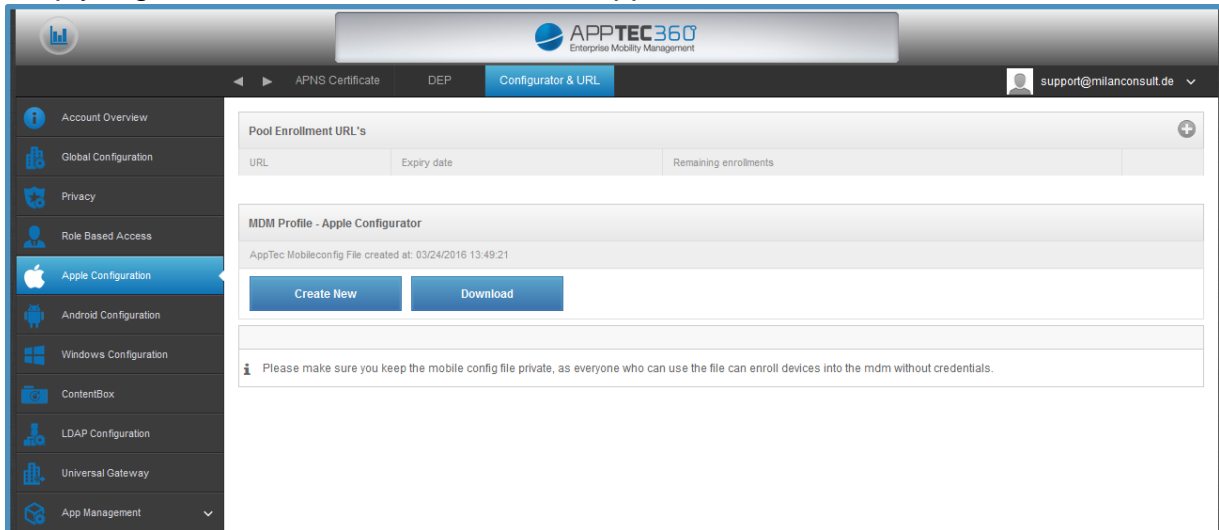


Once you have performed your configurations, click on "Save & Assign", in the bottom right hand corner, in order to save the changes.



## Configurator & URL

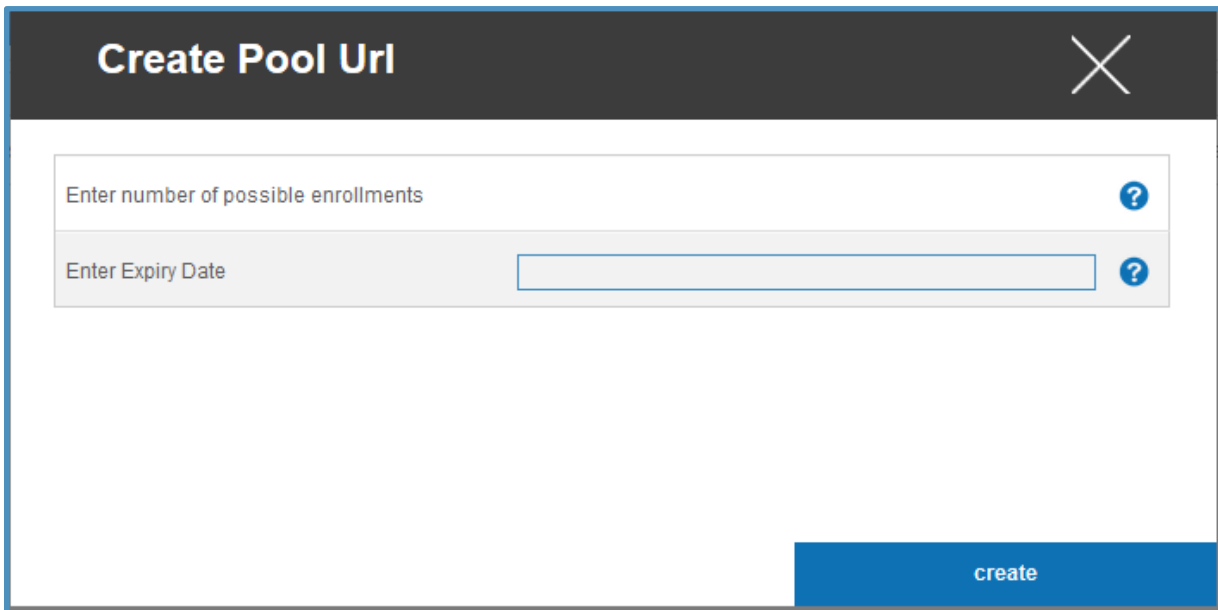
In this area, you can definitely simplify the enrollment of iOS devices. Consequently, the devices do not need to be assigned to the User, but they are simply registered as a Pool Device in the AppTec Console.



### Pool Enrollment URL's

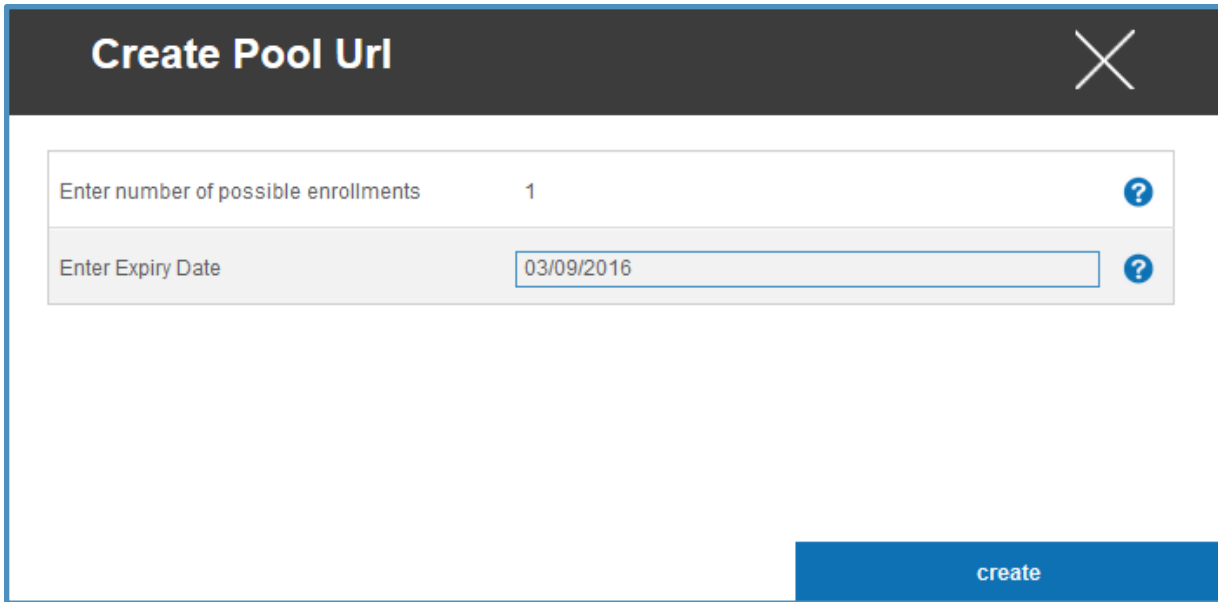
Generate a new URL for yourself, by clicking on the Plus-Symbol, in the upper right hand corner.

This will display the following Popup.



Enter number of possible enrollments	Number of times a device can be enrolled with the URL
Enter Expiry Date	Date when the Enrollment-URL expires





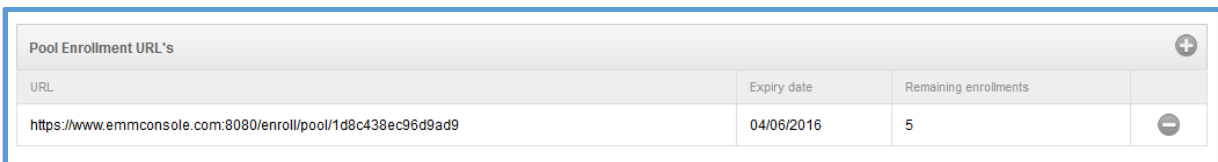
**Create Pool Url** [Close X]

Enter number of possible enrollments: 1 [?]

Enter Expiry Date: 03/09/2016 [?]

**create**

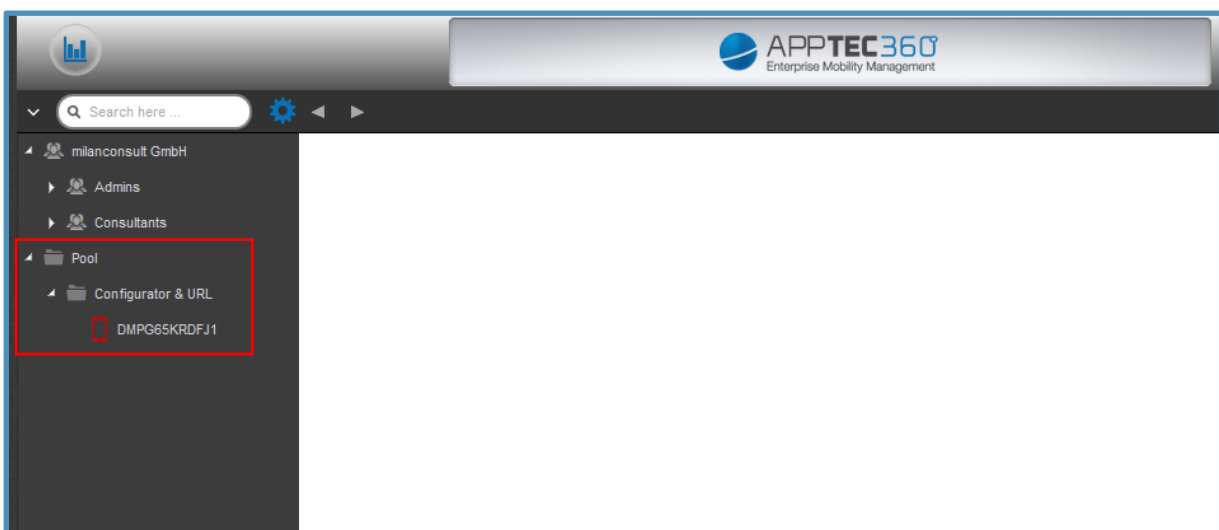
Once you have clicked on “create”, you should receive a similar overview, to the one in the following screenshot.



Pool Enrollment URL's [Add +]			
URL	Expiry date	Remaining enrollments	
https://www.emmconsole.com:8080/enroll/pool/1d8c438ec96d9ad9	04/06/2016	5	[Remove -]

With this, you can access the URL on your iOS device with the Safari Browser and you will be able to directly access the Profile-Installation.

Once you have performed them, you will receive the following overview in Mobile Management of the AppTec Console.

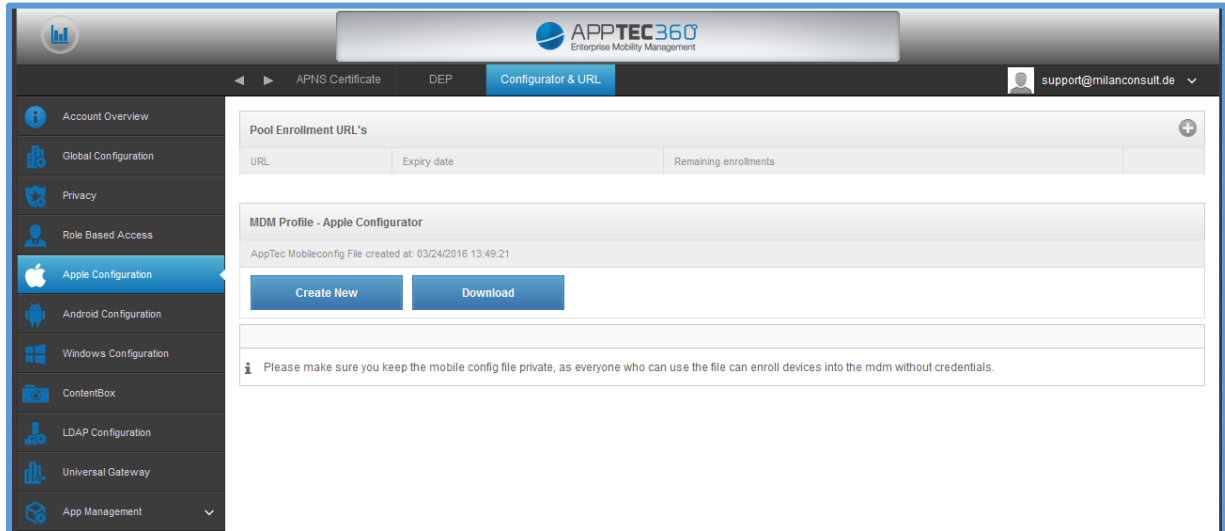


Right away, the device should be displayed in green. Depending on your needs, you can move the device with Drag & Drop.

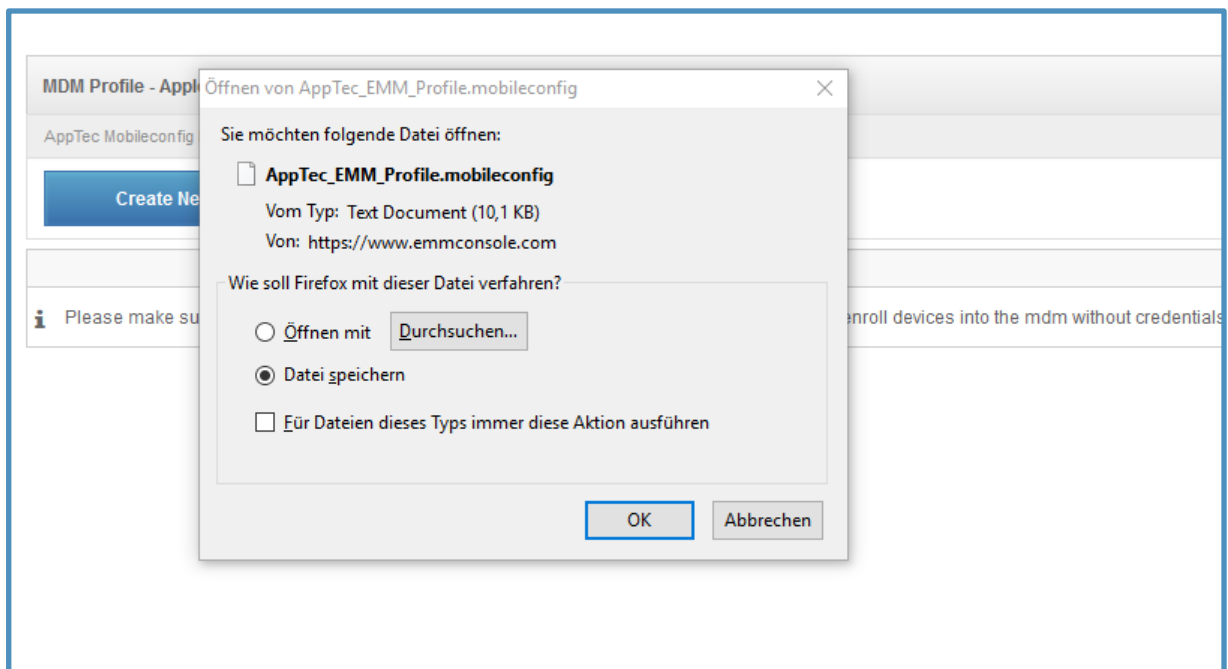


## MDM Profile – Apple Configurator

Click on “Create New“, in order to generate a “.mobileconfig“ file or upload it – as long as you have generated a mobileconfig file with “Download“.

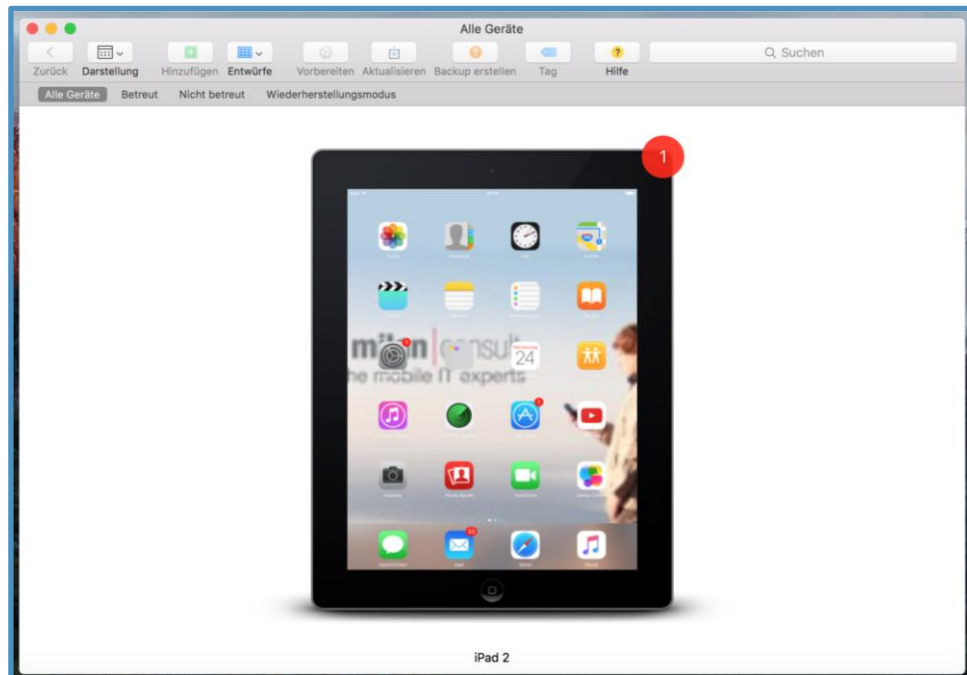


Confirm the following dialogue with “save file“.

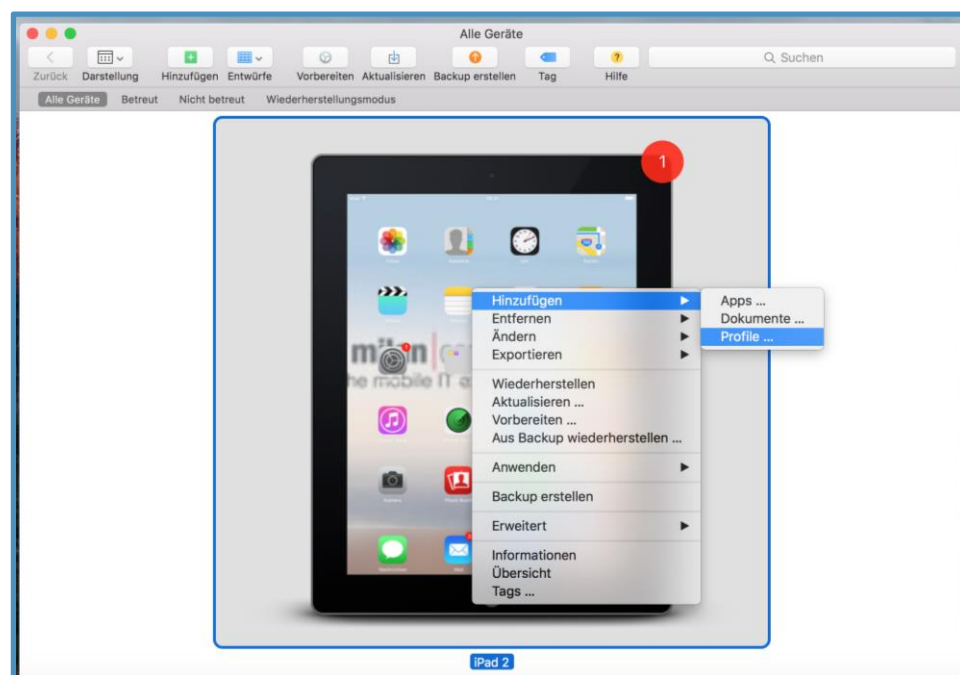




Now, on your Mac open the Apple Configurator and connect your desired iOS device to your Mac via a USB cable– You will receive the following display.

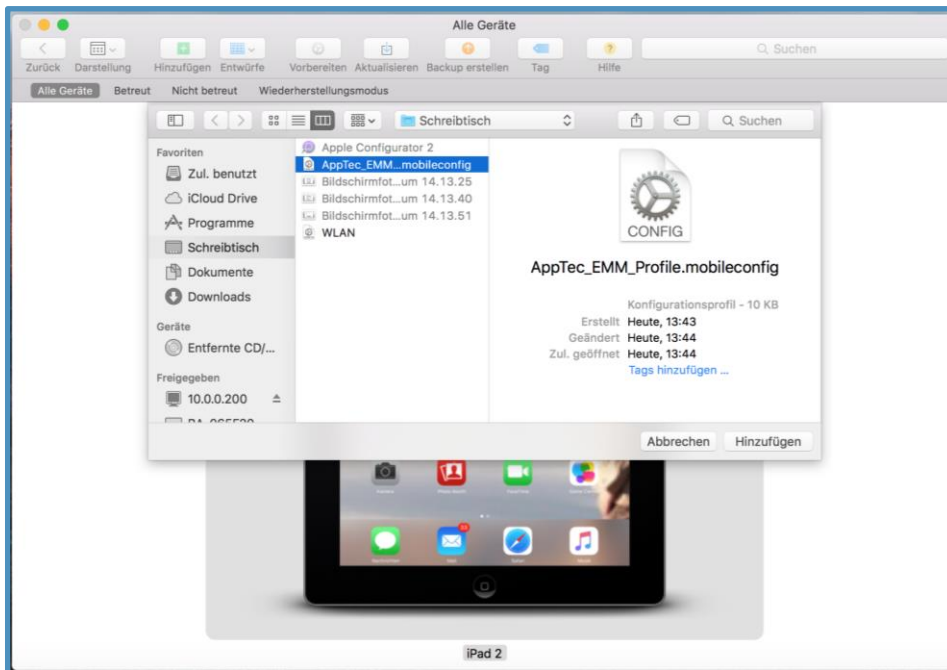


Now, right click the device, select “add” and then “profiles ...”.

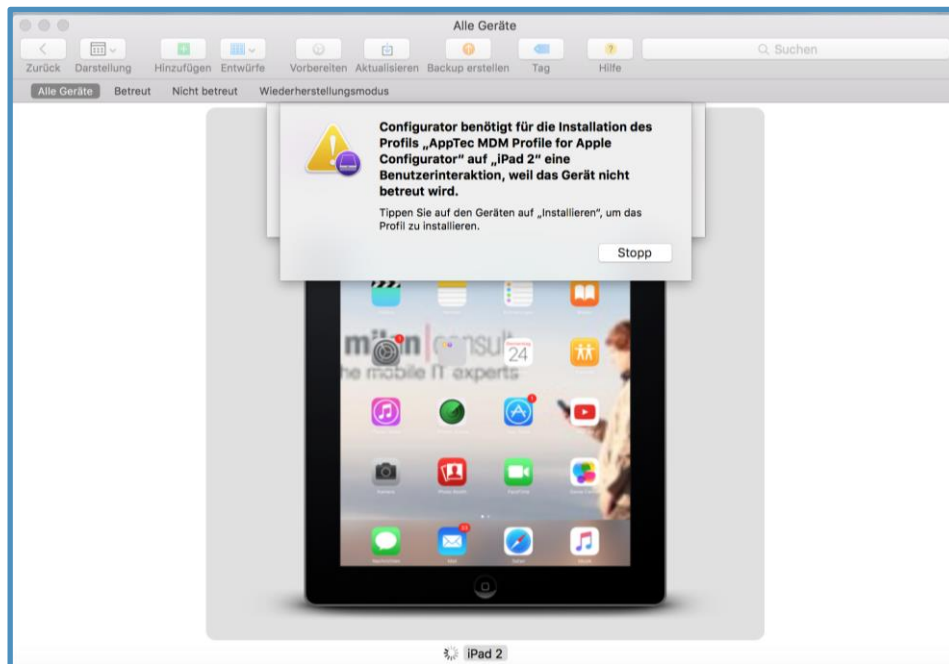




Now, select the previously generated and/or downloaded profile and click on “add”.

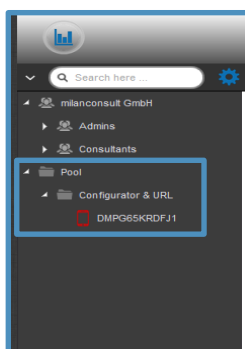
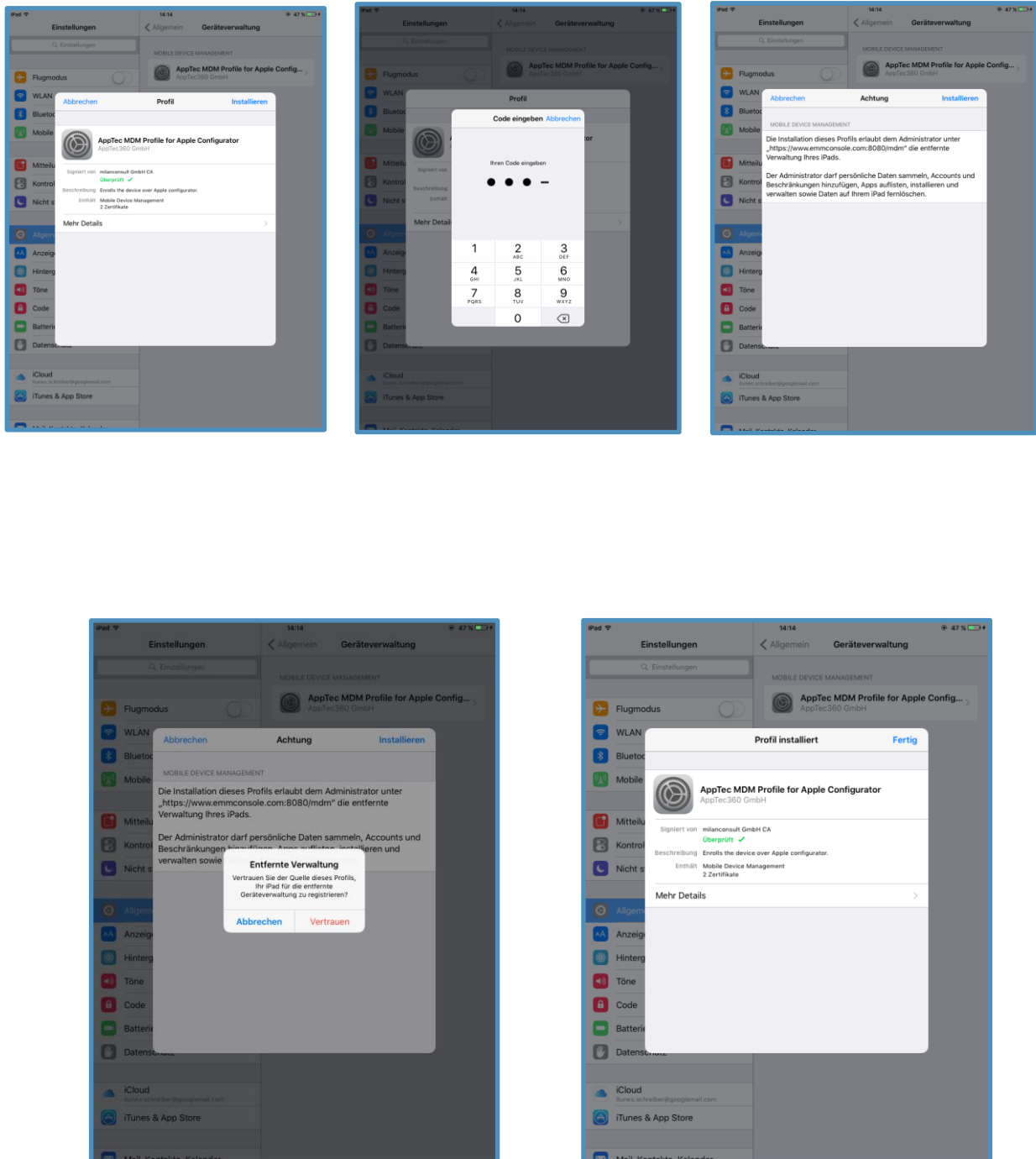


Shortly, you will receive the following overview. Now, you will prompted to perform the profile installation on the end user device.





Just as on the following screenshots, perform the Profile-Installation.



Once you have successfully performed the profile installation, you will be able to see the device in the Mobile Management and then move it with Drag & Drop, according to you needs.



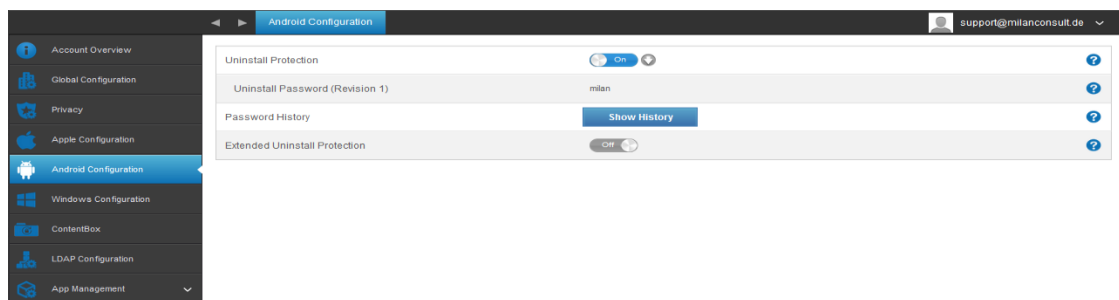
## Android Configuration

### Android Configuration

Uninstall Protection	<p>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.</p> <p>There are two options for removing the device administrators:</p> <ol style="list-style-type: none"> <li>Manually on the device           <ul style="list-style-type: none"> <li>→ open EMM App on the device</li> <li>→ switch to the Status tab</li> <li>→ tap on “Uninstall Protection”</li> <li>→ enter the password</li> <li>You can use the Revision to get the correct password from the “Password History” in the console.</li> <li>→ Scroll down and tap the newly added point, “Tap to uninstall AppTec MDM App” (you have 20 seconds to perform this task)</li> <li>→ Confirm the dialogue “Uninstall AppTec MDM App” with “ok”.</li> <li>This will unenroll the device from the console.</li> <li>→ To remove the App from the device confirm the dialogue “AppTec MDM will be uninstalled” with “UNINSTALL”</li> </ul> </li> <li>the automatic (Console)           <ul style="list-style-type: none"> <li>→ select the Device in the console</li> <li>→ click on the blue gear icon and select “Enterprise Wipe”</li> </ul> </li> </ol> <p>Note: Only available with Android 4.x and lower versions or on devices with the SAFE API</p>
Uninstall Password (Revision x)	<p>The established password, with which the user can remove the device administrator</p> <p>Revision x = counter, how often the password has already been changed</p>



	It is important which password the user needs, because it is possible that the device has not communicated with the AppTec 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



### Auto Enrollment

Here you can enable the Auto Enrollment feature to enroll your devices automatically when the Apptec app is opened on the device

Enable Auto Enrollment	If enabled, an Android device can automatically enroll if you've whitelisted it's serial or IMEI
Whitelisted Serials	Here you can enter multiple Serials for the Auto Enrollment
Serials Editor	Here you can edit the serial itself, the related Action, eMail, Device Type, the Ownership oder delete it. Also you can import or export a CSV file
Whitelisted IMEI	Here you can enter multiple IMEIs for the Auto Enrollment
IMEI Editor	Here you can edit the IMEI itself, the related Action, eMail, Device Type, the Ownership oder delete it. Also you can import or export a CSV file

### Android for Work

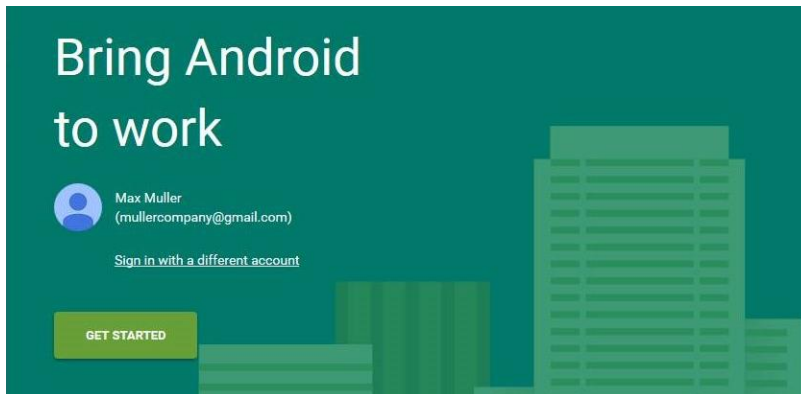
Here you can setup Android for Work. This is necessary to use all Android for Work features.

#### First Method: Android for Work 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 for Work 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”

**Organisation name**

Max Muller Company

**Enterprise mobility management  
(EMM) provider**

AppTec Enterprise Mobile Manager

☒ I have read and agree to the [Android for Work agreement](#).

PREVIOUS

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 for Work 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 for Work 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 for Work 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 for Work Container.



## AFW Enrollment

Here you can activate the Android for Work Enrollment. Using this Method will enroll your Devices into the [Android for Work Device Owner Mode](#). In this mode you will have the full control over the device.

Enable AFW Enrollment	Activates the AFW Enrollment <b>Caution:</b> If you disable AFW Enrollment, existing QR Codes and already configured NFC programmer devices will stop working. If you enable AFW Enrollment again, you'll have to resend NFC push configurations / generate new QR codes.
Enable Auto Discover	When a device enrolls itself via "AFW 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 enroll.

Note on Method 1 & 2: „Welcome Screen“ means 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)

1. Factory reset the device
2. Generate the QR Code for the Enrollment using one of the two following methods:
  - a. Click in „General Settings -> Android Configuration -> AFW Enrollment“ on „Generate QR Code“. Choose if you wish to skip the storage encryption and/or all system apps should be removed.
  - b. (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 for Work Device Mode.
  - a. If you used the QR Code in „General Settings“ you can find your device in „Pool -> AFW 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.
  - b. 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 -> AFW 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 AppTec 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 for Work Enrollment should start
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 for Work 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. <b>Caution:</b> 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 a 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://eu-kme.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 enrolling via KNOX Enrollment can be found in „Pool -> KNOX Enrollment“, or within the user you specified in the Auto Discover.



## Windows Configuration

### Windows Configuration

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

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 AppTec 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



Windows Configuration

support@milanconsult.de

Instant DM Connection	<input checked="" type="checkbox"/> On	?
Initial Retry Time	15 Seconds	▼ ?
Connection Retries	10	▼ ?
Maximum Sleep Time	4 Hours	▼ ?
First Sync Retries	10	▼ ?
First Retry Interval	2 minutes	▼ ?
Second Sync Retries	10	▼ ?
Second Retry Interval	5 minutes	▼ ?
Regular Sync Retries	10	▼ ?
Regular Retry Interval	4 Hours	▼ ?



## Content Box

### Configuration

Here you can configure the ContentBox.

You can think of the ContentBox as an Enterprise Dropbox.

Enable ContentBox	Enable ContentBox
Use external ContentBox installation	The ContentBox can also be operated with your ownCloud 7 server
URL	Complete URL of the OwnCloud entity
Root User	Root User of the OwnCloud Account
Root Password	Root password of the OwnCloud 7 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 read = read write = write delete = delete 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
<b>WebDAV Credentials</b>	
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.

Last synchronization: 2015-06-22 13:49:35

**Synchronize ContentBox**

You don't have a subscription for the AppTec ContentBox. Your ContentBox access is limited to 25 devices.

Contact [sales@apptec360.com](mailto:sales@apptec360.com) to purchase a license for all your devices

Select the 25 devices that can access the ContentBox

#		Device	OS	Type	Owner
1		Device of Fabian	iOS	Tablet	Fabian
2		Device of Matthias	Android	Phone	Matthias
3		Device of Michael	iOS	Phone	Michael
4		Device of Michael	iOS	Tablet	Michael
5		Device of Martina	iOS	Phone	Martina
6		Device of Yasemin	iOS	Phone	Yasemin
7		Device of Michael	iOS	Phone	Michael
8		Device of Tanja	Android	Phone	Tanja I
9		Device of Fabian	iOS	Tablet	Fabian
10		Device of Lukas	iOS	Tablet	Lukas
11		Device of Daniel	Android	Phone	Daniel
12		Device of Fabian .....	iOS	Tablet	Fabian .....

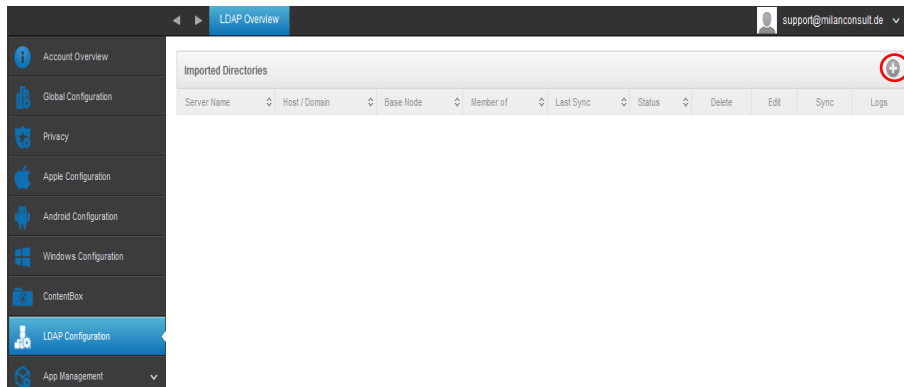


## LDAP Configuration

### LDAP Overview

Should your Active Directory be accessible externally or if you have decided on AppTec's On-Premise option, you can perform a LDAP import.

This is performed via the “Plus Symbol”, as marked on the screenshot.



Enter your Active Directory Data and click on “Add LDAP Server”:

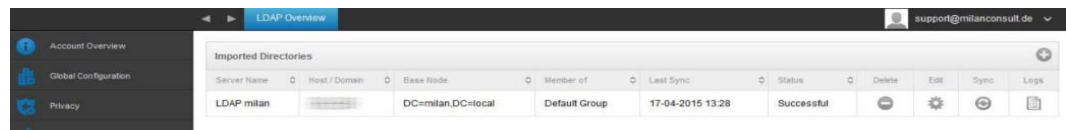
**Add LDAP Server** ✕

Server Name	
Type	<input checked="" type="radio"/> Active Directory
Host Domain	
Host Address	<span>?</span>
Port	<span>?</span>
Username	<span>?</span>
Password	
Repeat password	
Connection Security	<input checked="" type="radio"/> No Encryption <input type="radio"/> Use SSL <input type="radio"/> use TLS
Base DN	<span>?</span>
Member of	milan <span>▼</span> <span>?</span>
Check users for valid eMail ?	<input type="checkbox"/> Off <span>?</span>
Only activated users?	<input type="checkbox"/> Off <span>?</span>
Filter by Attributes ?	<span>?</span>
Test connection ?	<input checked="" type="checkbox"/> On <span>?</span>

Add LDAP Server



Should this process have been successful, then you will see this display:



Delete	Delete LDAP Server
Edit	Edit LDAP Server
Sync	Synchronize the LDAP Server
Logs	Disbursement of LDAP Logs

## Universal Gateway

Imagine, that during the configuration of email on smartphones and tablets, you would never have to enter a password and that you could ensure that only the devices, that are managed by the AppTec Mobile Device Management, could gain access to your email server.

This is precisely what is ensured with AppTec's Universal Gateway.

For your colleagues, this is an extreme improvement in security and a potent simplification of the initial mobile device configuration, all of which is provided by AppTec's Mobile Device Management.

If you are interested contact us at [sales@apptec360.com](mailto:sales@apptec360.com)

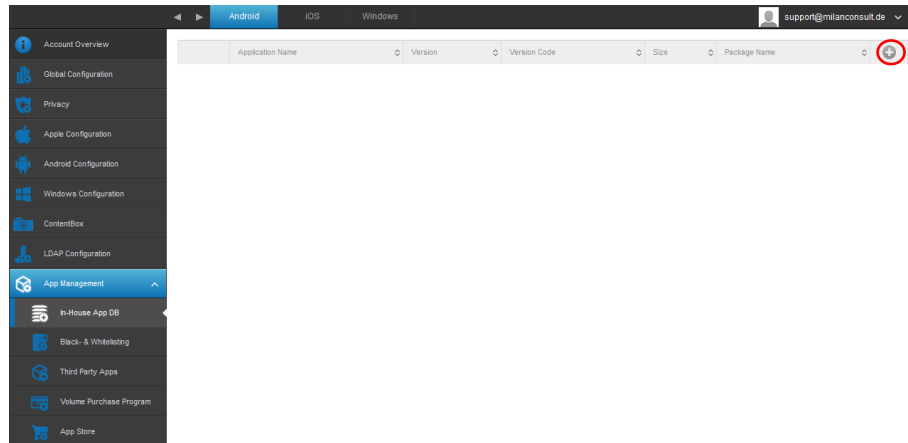


## App Management

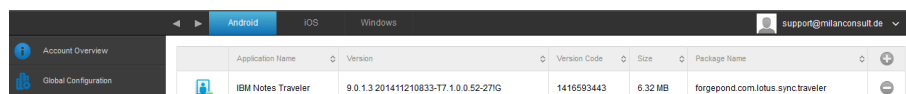
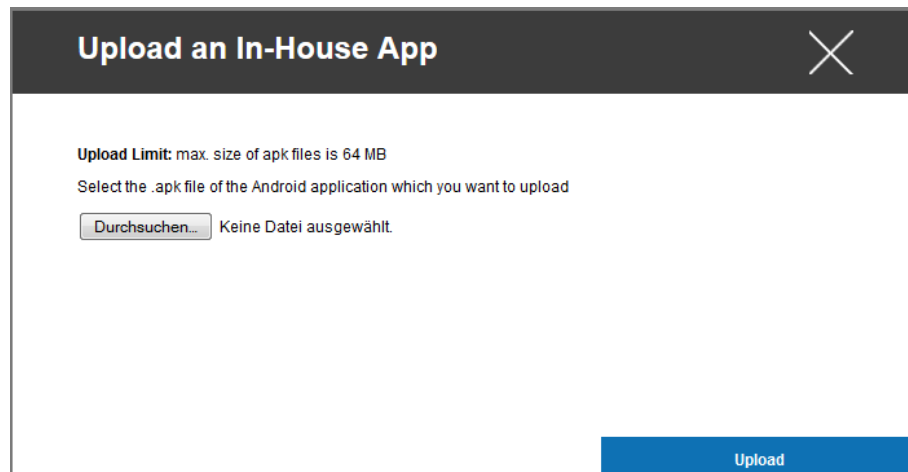
### In-House App DB

#### Android

Here you can upload the Android Apps that you developed with the “Plus Symbol” and distribute them later in Mobile Management.



With “Search...” you can select the .apk file and upload it with “Upload”.





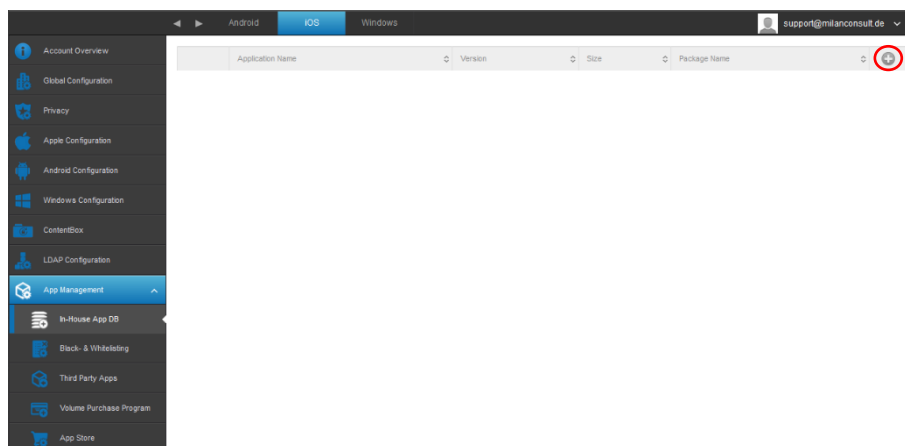
## Update Target

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.

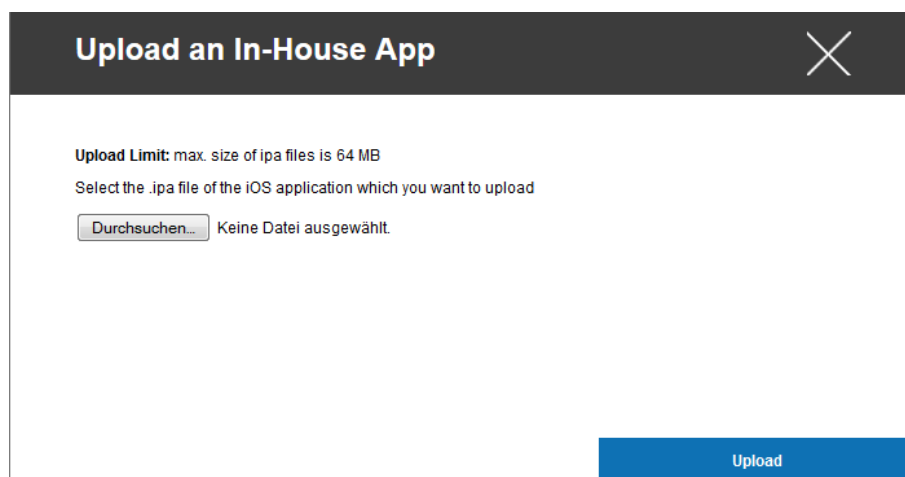
If you have not selected an Update Target, the highest version will be used.

## iOS

Here you can upload the iOS Apps that you developed with the “Plus Symbol” and distribute them later in Mobile Management.



With “Search...” you can select the .ipa file and upload it with “Upload”.





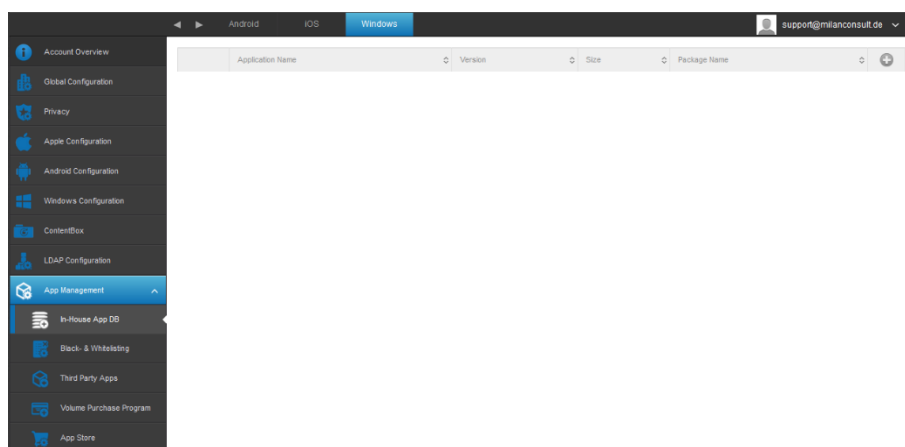
### Update Target

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.

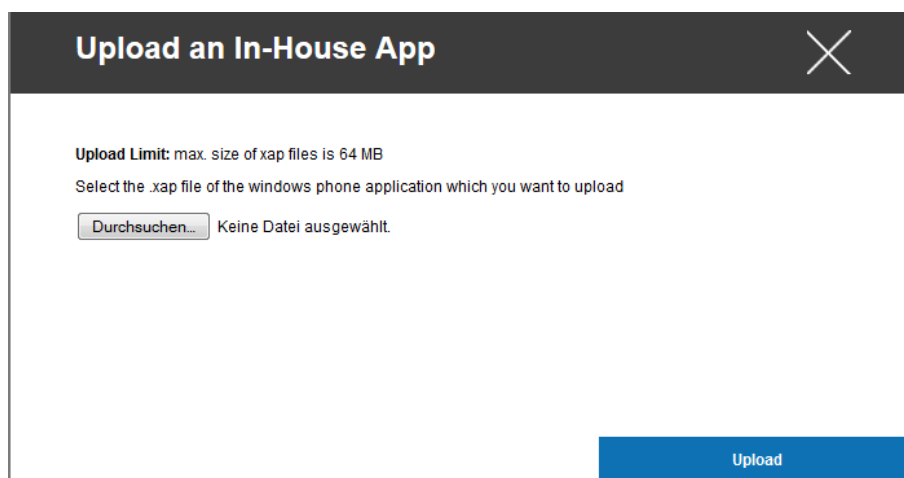
If you have not selected an Update Target, the highest version will be used.

### Windows

Here you can upload the Windows Phone Apps that you developed with the “Plus Symbol” and distribute them later in Mobile Management.



With “Search...” you can select the .xap file and upload it with “Upload”. However, these files must remain unsigned, otherwise an upload is not possible.



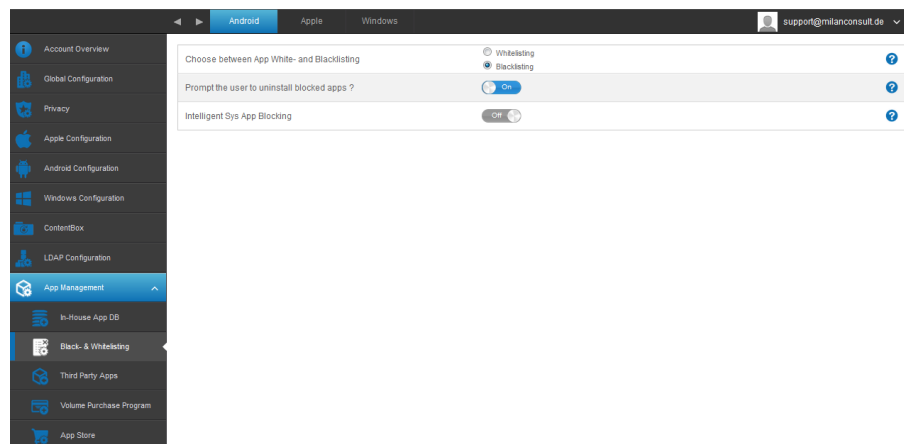


## Black-& Whitelisting

### Android

Here you can establish, if you would like to work with White- or Blacklisting.

Whitelisting	Only certain Apps are allowed, all other Apps cannot be installed/implemented
Blacklisting	Certain Apps are blocked, all others can be installed/implemented
Prompt the user to uninstall blocked apps?	Prompt the user to uninstall blocked Apps. With SAFE this occurs automatically.
Intelligent Sys App Blocking	When “whitelisting” is activated, then all System-Apps are deactivated with this function





Apple

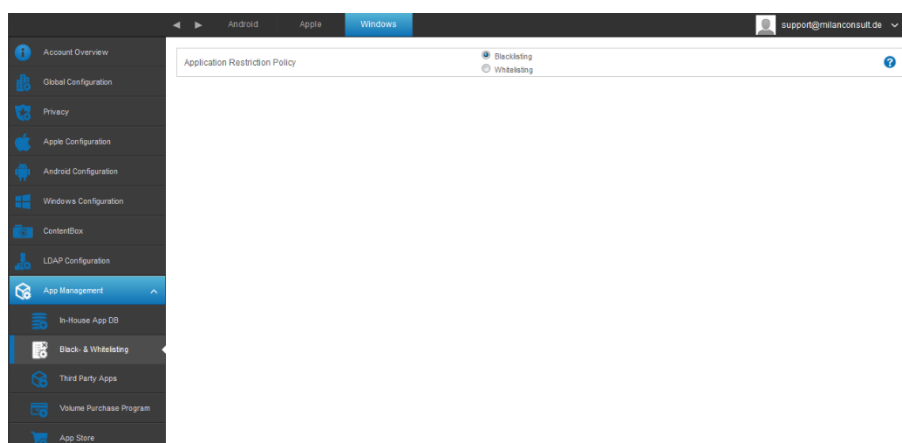
Choose between App Black- and Whitelisting

Whitelisting	Nur vom Admin festgelegte Apps sind verfügbar
Blacklisting	Eine vom Admin festgelegte Liste an Apps wird blockiert



## Windows

Whitelisting	Only certain Apps are permitted, all other Apps cannot be installed / implemented
Blacklisting	Certain Apps are blocked, all others can be installed/ implemented



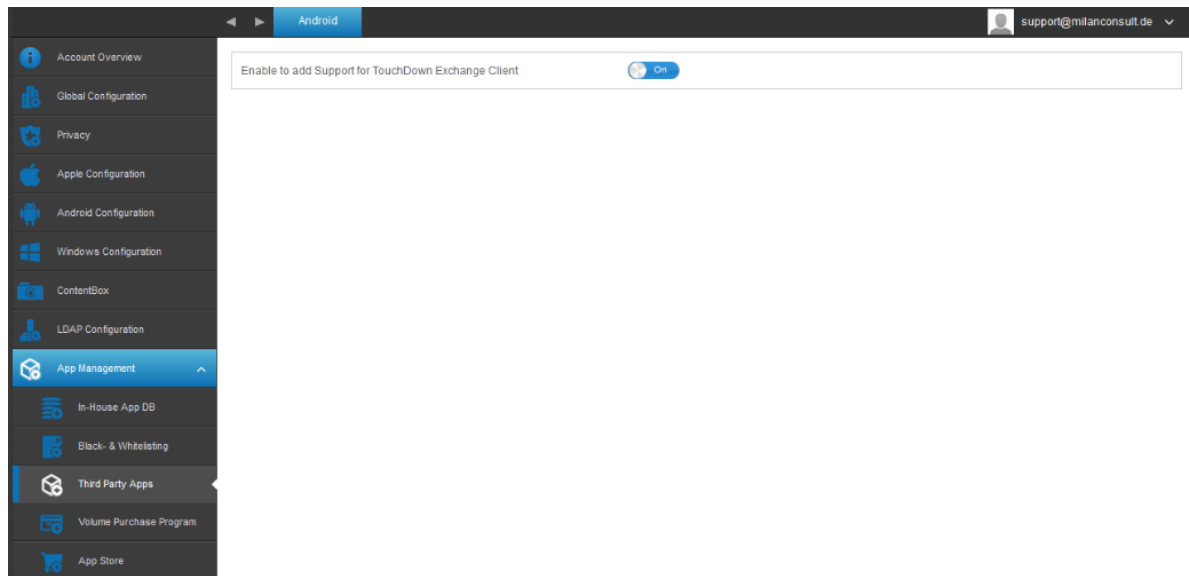


## Third Party Apps

### Android

If the native Mail Client is not supported under Android, you can activate a 3<sup>rd</sup> Party App “TouchDown” here.

Then you can configure it under: “Mobile Management “> „PIM Management“> „Touchdown Exchange“.



### iOS

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

### VPP / KNOX

The Volume Purchase Program (VPP) from Apple allows you to obtain licenses for a paid App.

Once purchased, you have the option to distribute the license to users, who can then install the App on the end user device for free.

Should the app be uninstalled on an end user device, you will be credited back the license and then you can distribute it to other users again.

Samsung devices can use KNOX, as long as the devices support it and as long as you have a valid license key.

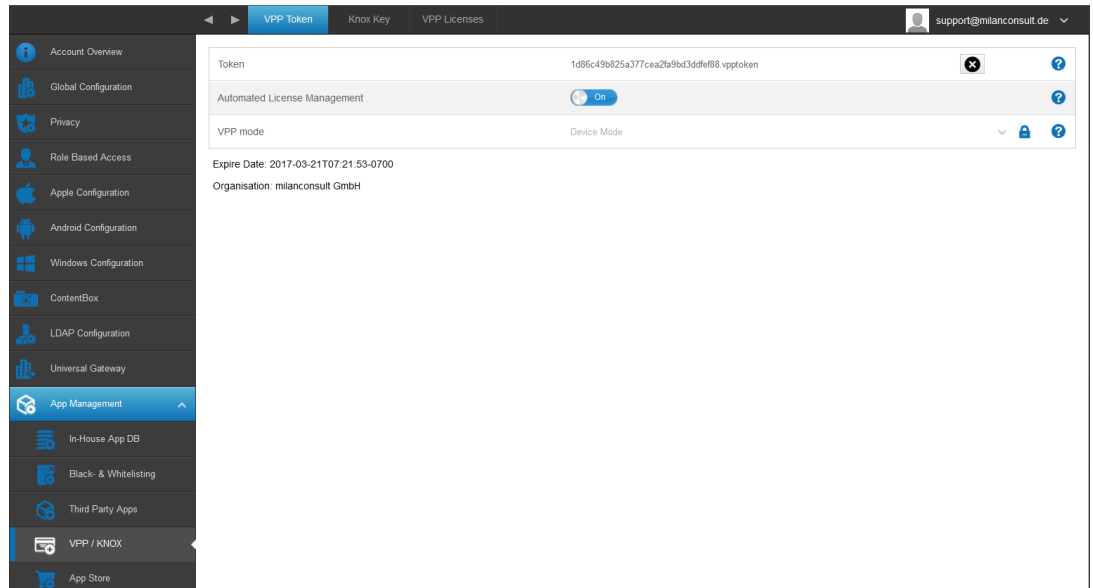
With KNOX, two different profiles can be run on the end user device and thereby separating private and corporate files from each other.



## VPP Token

Here you can upload the purchased VPP Token, by clicking on “Click here to select a file”.

Don't forget to back up this configuration by clicking “Save”.



Token	Your uploaded VPP Token
Automated License Management	<p>With this, the automatic License Management is activated</p> <p>Should this be the case, then the moving of the users/devices to another group, will automatically assign the group's profile VPP License</p> <p>Previously installed Apps/Licenses will not be withdrawn, this must be performed manually afterwards</p>
VPP mode	<p><u>User Mode:</u> VPP Licenses are assigned to an Apple-ID. This way, the License/App can be used on multiple devices with the same Apple ID.</p> <p><u>Device Mode:</u> VPP Licenses are directly assigned to a device (only iOS 9 or higher)</p> <p>Thereby an Apple-ID is not required on the device and it is not necessary to confirm the App Store Installation Dialogue.</p> <p><u>Warning:</u> A change in these settings terminates all previous VPP connections on the end user devices. If this desired, confirm it with a click on the lock.</p>



You can look up the VPP Tokens' expiration via "Expire Date". Before this is performed, the VPP File must be refreshed respectively. The assigned token's company, will be displayed in the "Organization" field.

### Knox Key

Here you can insert your purchased Samsung KNOX-Key.

KNOX License Key	Insert KNOX-Key here.
------------------	-----------------------



## VPP Licenses

If you have defined a VPP-Account, then you will gain an overview of your purchased VPP-Apps.

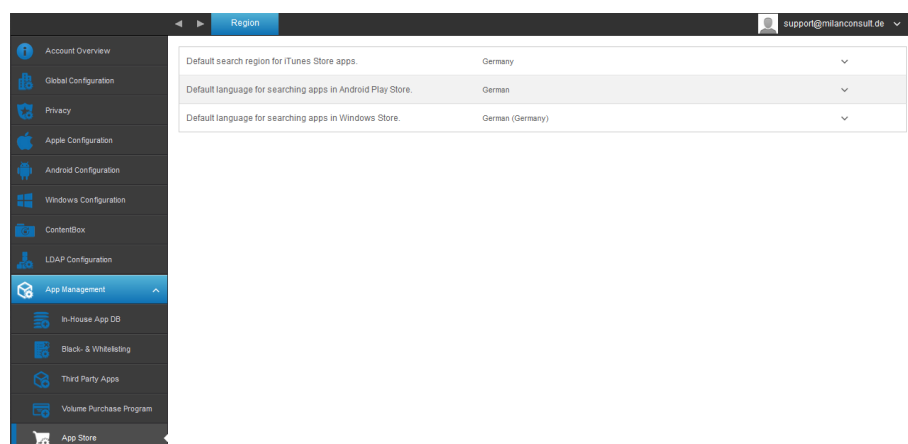
App Name	Version	Price	Assign Status	Total	Free
 Evernote	6.0.15	free	Assigned	100	100
 GoodReader for Good	4.8.0	free	Assigned	1	1

App Name	Name of the app
Version	Current Version of the app
Price	Original price of the app
Assign Status	Assignment status of the app
Total	Total number of apps
Free	Remaining available apps

## App Store

### Region

Default search region for iTunes Store apps.	Region for which iTunes Store (Apple Apps) should be used as a default search.
Default language for searching apps in Android Play Store.	Standard for which Google PlayStore (Android Apps) should be used as a default.
Default language for searching apps in Windows Store.	Standard for which Windows Phone Store (Windows Phone Apps) should be used as a default.





## App Settings

Here you can define the default app settings. These can be changed for every single app installation.

### iOS App Settings

Keep up to date	Keeps the up to date based on the Update Target
Overtake when unmanaged	If this app is already installed as unmanaged (not via MDM), it will become managed
Remove app when MDM profile is removed	The app will get removed if you remove the MDM profile
Prevent backup of the app data	Prevent the backup of the app data

### Android App Settings

Keep up to date	Keeps the up to date based on the Update Target
-----------------	---

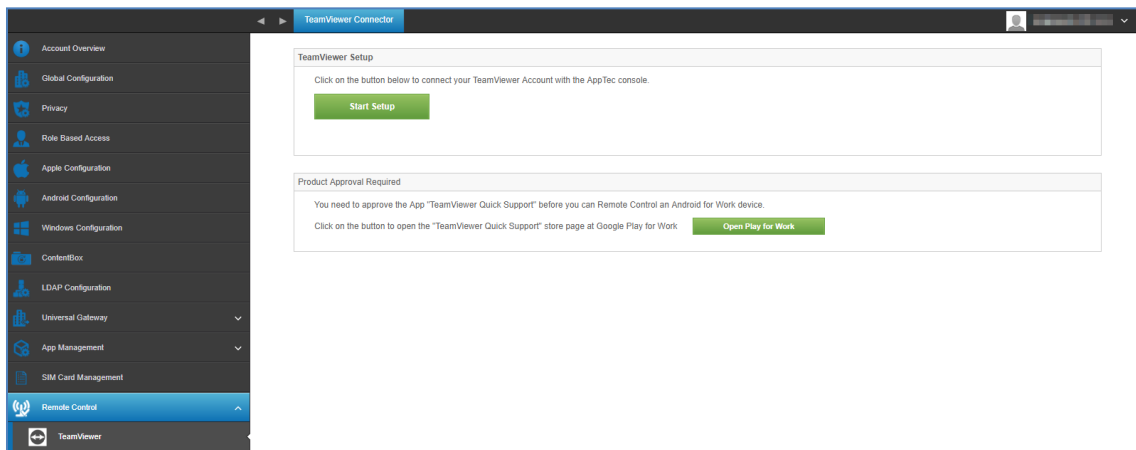


## Remote Control TeamViewer

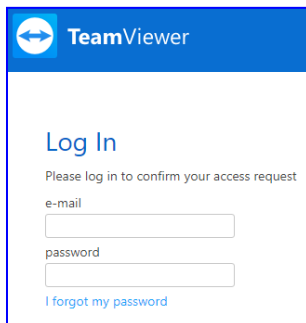
### Connecting the Console to the Teamviewer Account

*Note: In the free trial version you are not able to connect your teamviewer account. You will have a free demo account linked instead.*

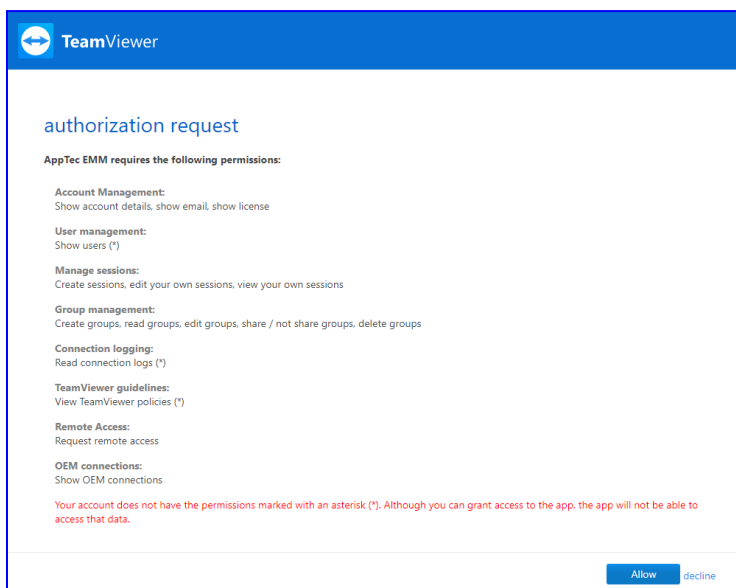
Go to General Settings -> Remote Control -> TeamViewer. Here you can link your teamviewer account with the console or see information about your currently connected account. Also you are able to view all currently active sessions if you go to "Active Sessions".



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.

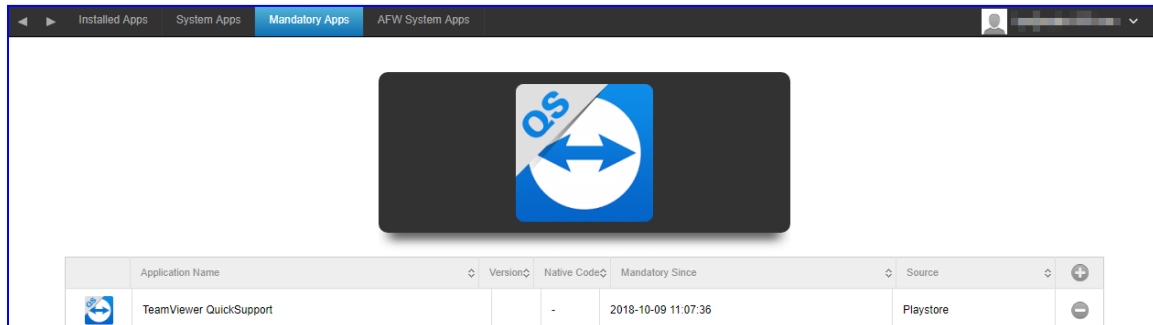


After logging in, you have to authorize the Apptec MDM to use this account. After confirming this, you have to wait a few seconds and the Account is connected.



### **Install TeamViewer QuickSupport**

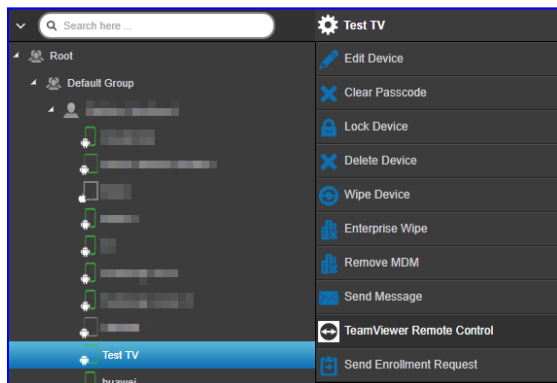
Add the app “TeamViewer QuickSupport” to the mandatory apps of your your device profile or group profile and click on “Assign Now”. Wait until the App is installed on the device.



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**

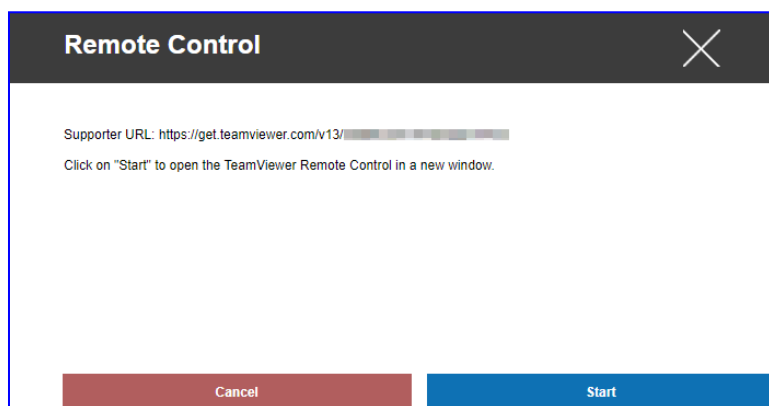
To remote control your device, select the device, click on the wheel and choose “TeamViewer Remote Control”



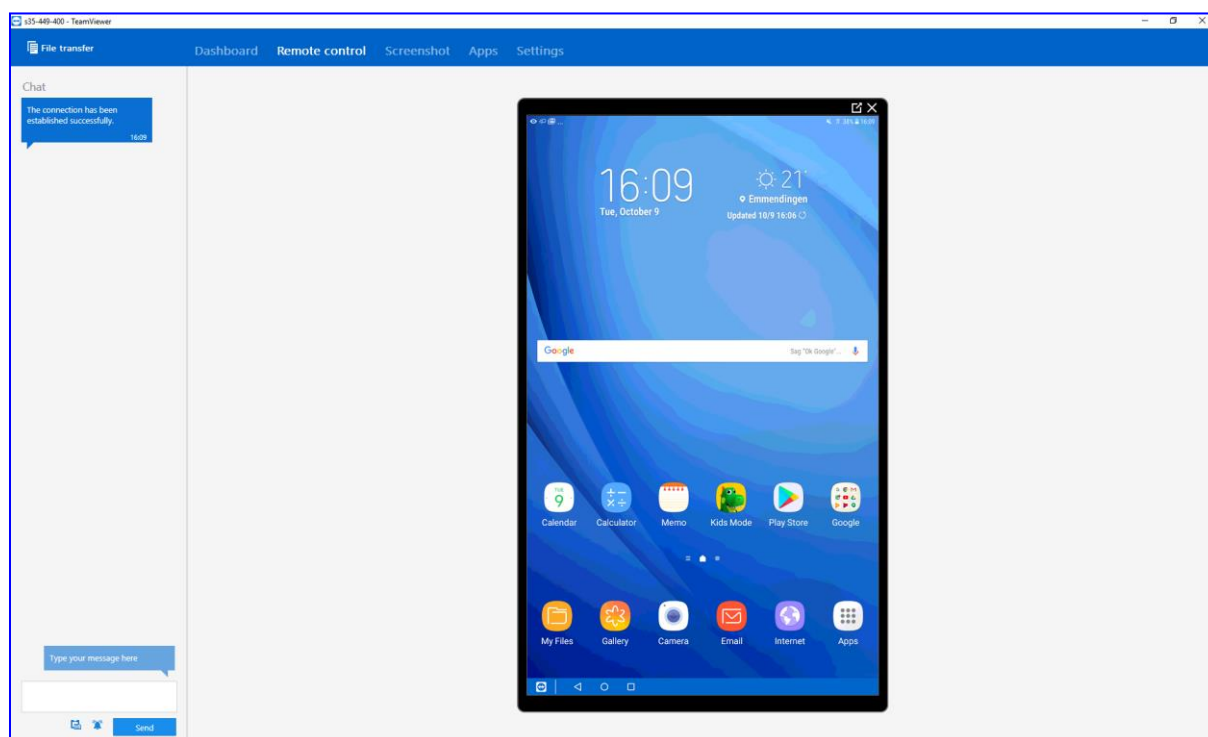
If there is already an active session, you can either use the old session or create a new one.

Confirm that you want to create a new TeamViewer Session.



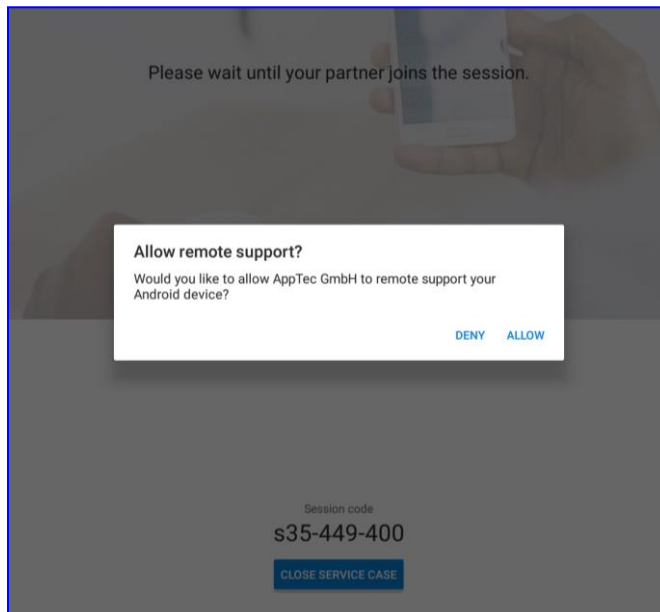


After a few seconds you will get a link for your TeamViewer Session. You can click on "Start" to open this link in a new window.



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 apptec app. 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 apptec app manually.

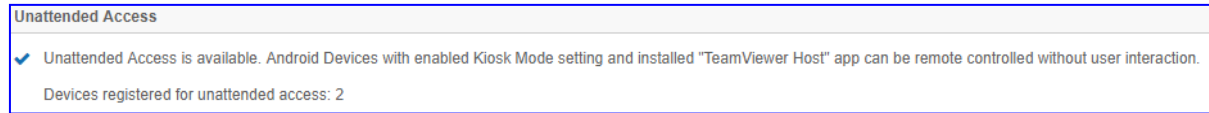
On some Android devices (e.g. Samsung) it is required to install an additional app as addon. The teamviewer app on the device will inform you about that, if this is necessary on your device.



## Unattended Access

*Note: Unattended Access is only possible on Android.*

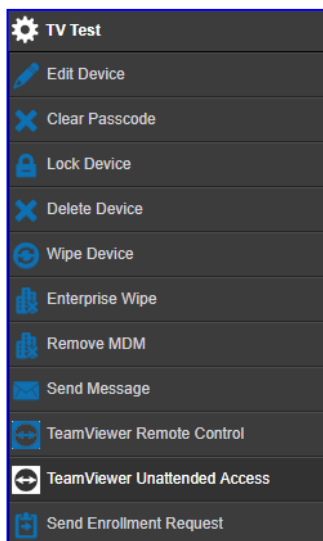
You can connect to your device, without accepting the connection on the device, if your TeamViewer Account is using a „Tensor“ License.



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.



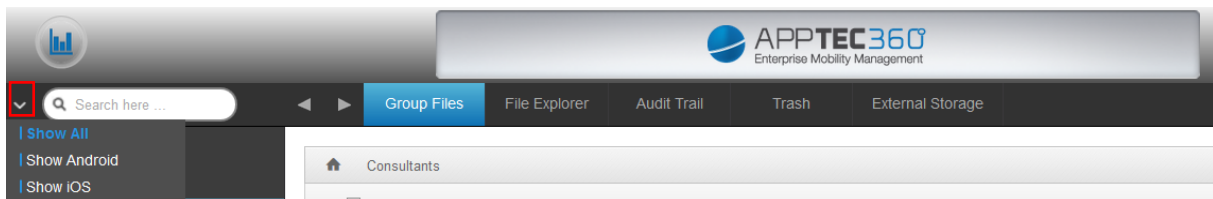
## ***IV. Mobile Management***

---

### 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



My Profile	Edit the Admin's account details
Log Out	Log out of the Appliance

### User Information

Username	User name and/or email address of the account
Name	Administrator's first name
Surname	Administrator's surname
Login Name	Administrator's login name
eMail Address	Administrator's email address
Alternative eMail address	Administrator's alternate email address
Picture	Profile picture
Phone Number	Administrator's phone number
Mobile Number	Administrator's 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!



## Corporate administration (Root-Node) in Mobile Management



When you have reached the Root-Node (first group), you can perform a variety of settings for your 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

### 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)

**Create Group**
✕

Group Name

Parent Group
Root Node
▼

Create group



## Rename Root Node

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

**Default Title**
✕

Root Node Name

Update Name

## Mass Enrollment

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

**Mass Enrollment**
✕

	Name	eMail	Alternative eMail	Phone Number	eMail	alt. eMail	SMS	iOS	Android	Windows	Phone	Tablet	Emp.	Corp.
☰	Consultants				<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Lukas	██████████	██████████		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Matthias	██████████	██████████		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Felix	██████████	██████████		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Fabian Kola	██████████	██████████	██████████	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Max Mustermann	██████████			<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Daniel	██████████	██████████		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
☰	Admins				<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Tanja	██████████			<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Michael	██████████		██████████	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Martina	██████████			<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Milan	██████████		██████████	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Yasemin	██████████			<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Start Mass Enrollment

Export as CSV

Import CSV

On average it takes 10 seconds for creating and enrolling one device  
 You can easily create users by adding them at the end of a exported CSV. Import the CSV afterwards and start the Mass Enrollment.  
 Example: Philipp Reiss; philipp.reis@apptec360.com; pr@apptec360.com; +41 61 511 3210;;;  
 Your account is limited to 25 devices. You can add 10 devices.



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.

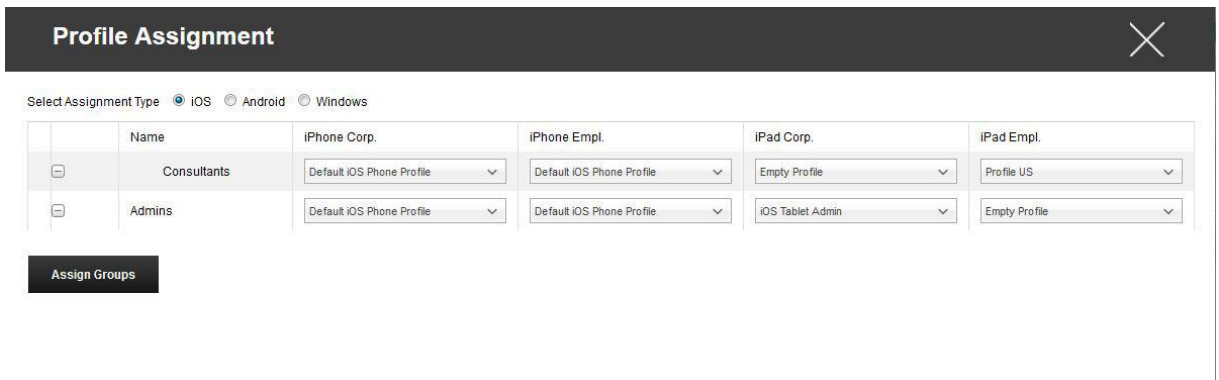
As a final step, you can establish whether the respective device is corporate or private (BYOD).

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



Profile Assignment					
Select Assignment Type <input checked="" type="radio"/> iOS <input type="radio"/> Android <input type="radio"/> Windows					
	Name	iPhone Corp.	iPhone Empl.	iPad Corp.	iPad Empl.
	Consultants	Default iOS Phone Profile	Default iOS Phone Profile	Empty Profile	Profile US
	Admins	Default iOS Phone Profile	Default iOS Phone Profile	iOS Tablet Admin	Empty Profile

**Assign Groups**



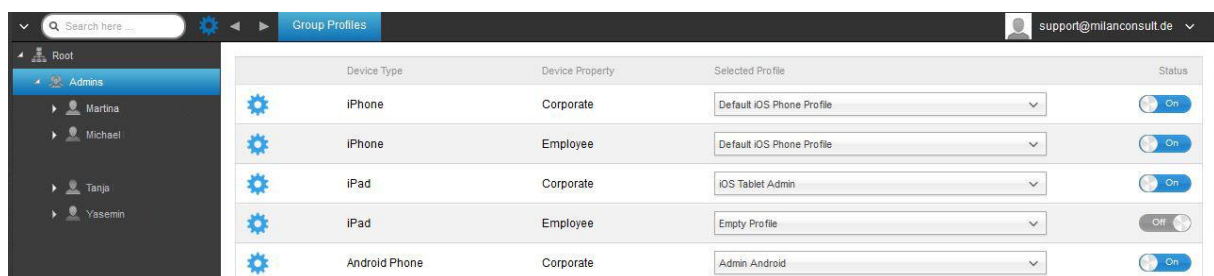
## Group Management in Mobile Management

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 User	Create a user for the respective (sub)group



### Create a Subgroup

## Create Group



Group Name

Parent Group

Admins

▼

Create group


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

## Update Group



Group Name

Admins

Parent Group

Root Node

▼

Update group



### 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 User**
✕

Name	mandatory	Vorname des Users
Surname	mandatory	Nachname des Users
Login Name		Login Name des Users <span style="float: right; color: blue;">?</span>
eMail Address	mandatory	E-Mail Adresse des Users
Alternative eMail Address		Alternative E-Mail Adresse (des Users)
Picture		<div style="display: flex; align-items: center;"> <span>Click here to select a file</span> <div style="border: 1px solid blue; padding: 2px 5px; margin-left: 10px;">profile picture of the user</div> <span style="margin-left: 10px; color: blue;">?</span> </div>
Phone Number		Telefonnummer (wichtig bei SMS Enrollment)
Mobile Number		Telefonnummer
Phone Extension		Durchwahl
Location		Standort
Position		Position
Usergroup		<div style="display: flex; align-items: center;"> <span>Admins</span> <div style="border: 1px solid blue; padding: 2px 10px; margin-left: 5px;">assigned group</div> <span style="margin-left: 5px;">▼</span> </div>
<p>Hier können Sie einen Kommentar hinzufügen!</p> <p>Comment</p>		

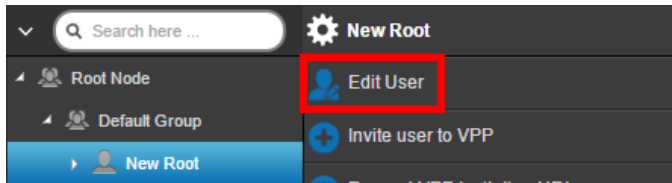
Create User



## 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”



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 Information** ✕

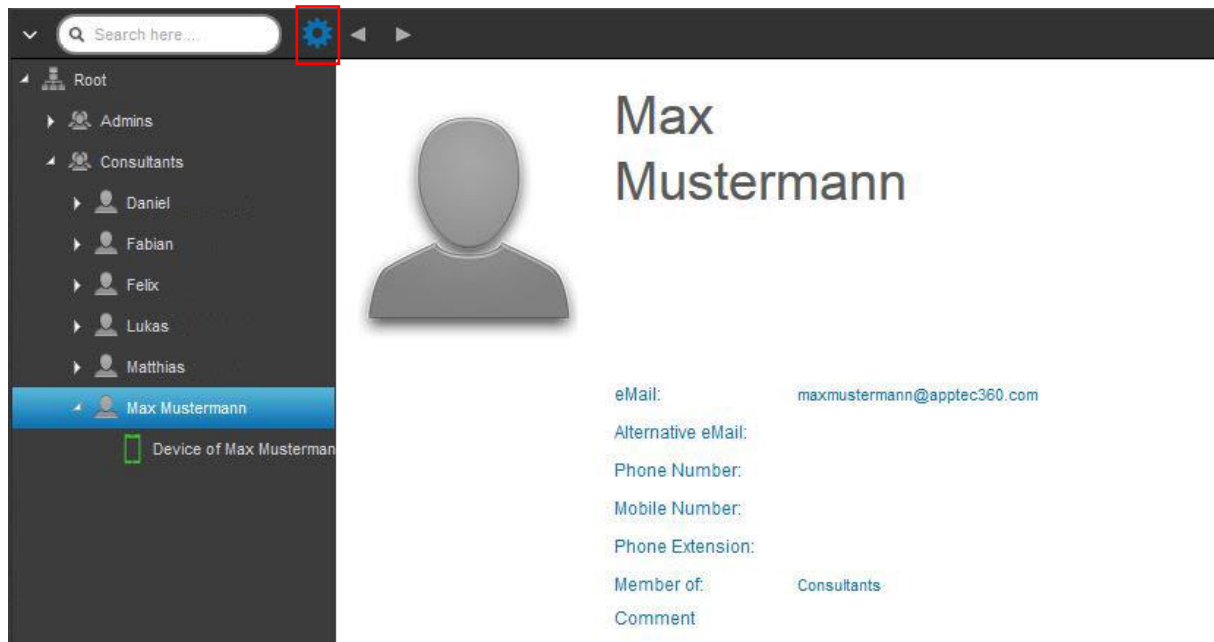
Username	<input type="text"/>
Name	New
Surname	Root
Login Name	<input type="text"/> ?
eMail Address	email@address.com
Alternative eMail Address	<input type="text"/>
Picture	<input type="text"/> Click here to select a file ?
Phone Number	<input type="text"/>
Mobile Number	<input type="text"/>
Phone Extension	<input type="text"/>
Location	<input type="text"/>
Position	<input type="text"/>
Usergroup	Default Group ▾
Assigned Roles	<div><input type="text" value="Super Root"/> ✕   <input type="text"/></div>
Comment	<input type="text"/>
Enter new password	<input type="password"/> ?
Repeat new password	<input type="password"/> ?

Save



## 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:

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:

Add Device
✕

Selected User	Max Mustermann
Device name	Device of Max Mustermann
Phone Number, e.g. +49160123456	
Alternative eMail	
Device Owner	<input checked="" type="radio"/> Corporate Property <input type="radio"/> Employee Property
Choose operating system	<input checked="" type="radio"/> Android <input type="radio"/> iOS <input type="radio"/> Windows
Choose device type	<input checked="" type="radio"/> Phone <input type="radio"/> Tablet
Send enroll request now ?	<input checked="" type="checkbox"/> On <span style="float: right; color: blue;">?</span>
Send request to alternative eMail ?	<input type="checkbox"/> Off <span style="float: right; color: blue;">?</span>
Send enrollment SMS ?	<input type="checkbox"/> Off <span style="float: right; color: blue;">?</span>
You have 10 SMS credits left	

Add Device

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 Android, iOS and Windows Phone devices
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)

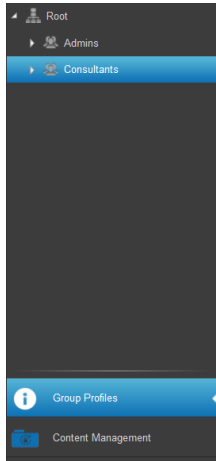
After the Enrollment Request has been sent, the device will be displayed (marked red) right away.





















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.



Device Type	Device Property	Selected Profile	Status
 iPhone	Corporate	Default iOS Phone Profile	
 iPhone	Employee	Default iOS Phone Profile	
 iPad	Corporate	Default iOS Tablet Profile	
 iPad	Employee	Default iOS Tablet Profile	
 Android Phone	Corporate	Default Android Phone Profile	
 Android Phone	Employee	Default Android Phone Profile	
 Android Tablet	Corporate	Default Android Tablet Profile	
 Android Tablet	Employee	Default Android Tablet Profile	
 Windows Phone	Corporate	Default Windows Phone Profile	
 Windows Phone	Employee	Default Windows Phone Profile	

	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.

**Copy Group Profile**
✕

Source Profile Name	Default iOS Phone Profile
New Profile Name	Copy of Default iOS Phone Profile
Profile Type	Phone Profile <span style="float: right;">▼</span>

Copy

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!

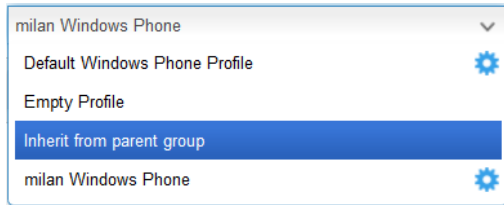
**Delete Group Profile**
✕

Profile to Delete	Default iOS Phone Profile
-------------------	---------------------------



## 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.

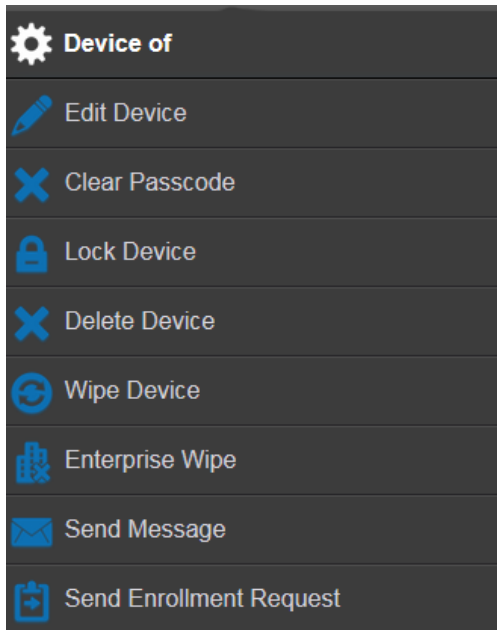


## Device Management in Mobile Management

When you select a device, you can perform a variety of tasks via the “gear”.

These are different, depending on the OS platforms (Android, iOS, Windows Phone)

### Android



Edit Device	Edit device information
Clear Passcode	Delete 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 AppTec are deleted (device will be separated from MDM)
Send Message	Send Push notifications to the device Message will be displayed in the AppTec App (Message Tab)
Send Enrollment Request	Send (repeated) enrollment request



### Edit Device

Here you can update a variety of device information.

**Update Device**
✕

Selected User	Matthias
Device name	Device of Matthias
Phone Number, e.g. +49160123456	
Device Owner	<input checked="" type="radio"/> Corporate Property <input type="radio"/> Employee Property
Choose device type	<input checked="" type="radio"/> Phone <input type="radio"/> Tablet

Save

Selected User	Device user
Device name	Device name
Phone Number	Device telephone number
Device Owner	Corporate = corporate property Employee = employee property
Choose device type	Type of the selected 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.

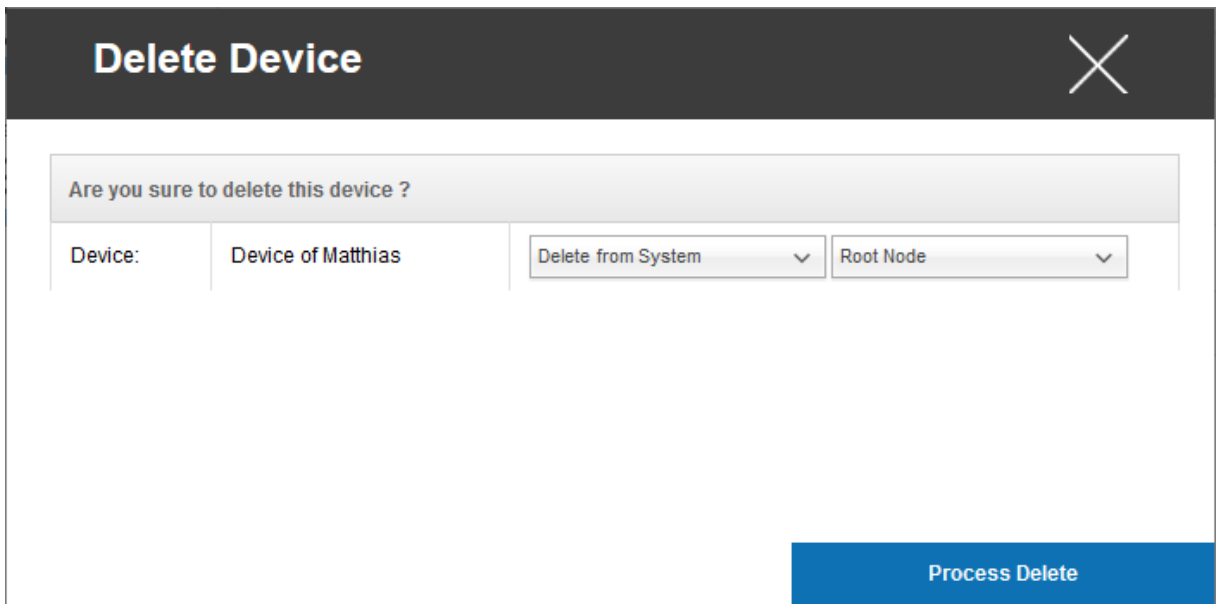
### Lock Device

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 AppTec (“Delete from System”) or if the device should be removed from AppTec and additionally be restored to its factory settings (“Wipe & Delete”).



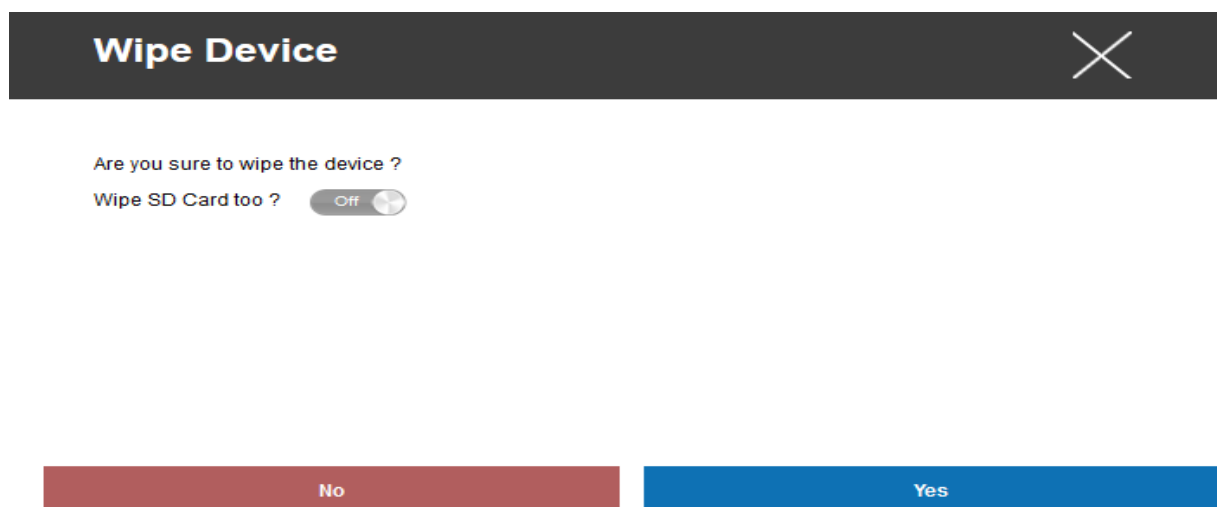
The dialog box has a dark header with the title "Delete Device" and a close button (X). The main content area contains a confirmation message "Are you sure to delete this device ?". Below this, there is a form with two rows. The first row has a label "Device:" followed by the text "Device of Matthias". The second row has two dropdown menus: the first is set to "Delete from System" and the second is set to "Root Node". At the bottom right of the dialog is a blue button labeled "Process Delete".

n

### 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”.



The dialog box has a dark header with the title "Wipe Device" and a close button (X). The main content area contains a confirmation message "Are you sure to wipe the device ?". Below this, there is a label "Wipe SD Card too ?" followed by a toggle switch currently set to "Off". At the bottom of the dialog are two buttons: a red button labeled "No" and a blue button labeled "Yes".



## Enterprise Wipe

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

Only the information, apps and profiles provided by AppTec 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.


**Enterprise Wipe device?** 

Are you sure to Enterprise Wipe the device ?

No

Yes

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

**Send a message** 

Subject	Wichtig! Bitte bei Ihrer IT melden!
Message	<div>Sehr geehrter Herr Mustermann, bitte melden Sie sich umgehend bei Ihrer IT-Abteilung.</div>


Send Message






### 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.

**Send Enrollment Request** 

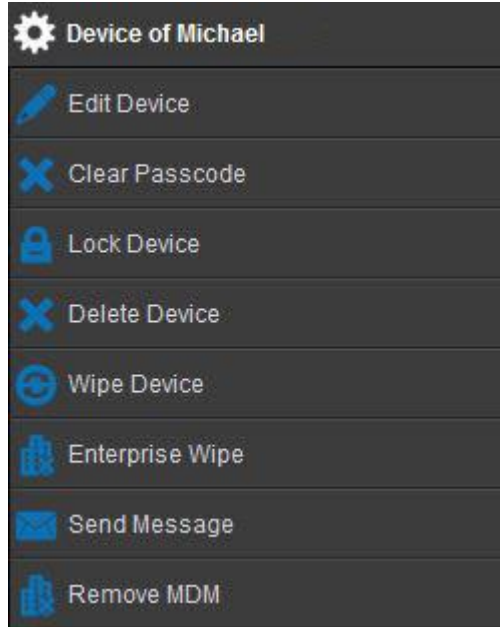
Send enroll request now ?	<input checked="" type="checkbox"/> On	
Alternative eMail address	matthias <input type="text"/> .com	
Send to alt. eMail address ?	<input type="checkbox"/> Off	
Send enroll SMS ?	<input type="checkbox"/> Off	

Enroll now



iOS

When the device is connected (green):



When the device is not connected (red):




Edit Device	Edit device
Clear Passcode	The device passcode is erased
Lock Device	Lock device (lock screen)
Delete Device	Remove device from AppTec
Wipe Device	Restore device to factory settings
Enterprise Wipe	The information, apps and profiles provided by AppTec are deleted (device is separated from MDM)
Send Message	Send Push Notifications to the device Message will be displayed in the AppTec App (Message Tab)
Send Enrollment Request	Send (repeated) Enrollment request
Remove MDM	Remove MDM from the end user device (same effect as "Enterprise Wipe")



### Edit Device

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

## Update Device




Selected User	Matthias
Device name	Device of Matthias
Phone Number, e.g. +49160123456	
Device Owner	<input checked="" type="radio"/> Corporate Property <input type="radio"/> Employee Property
Choose device type	<input checked="" type="radio"/> Phone <input type="radio"/> Tablet

Save

### 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).

## Clear Passcode?



Are you sure to remove the passcode from the device ?

NoYes




### Lock Device

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

### Delete Device

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

## Delete Device



Are you sure to delete this device ?


Device:	Device of Matthias	Delete from System ▼	Root Node ▼
---------	--------------------	----------------------	-------------

Process Delete

### Wipe Device

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

## Wipe Device



Are you sure to wipe the device ?


No

Yes



### Enterprise Wipe

Only the information, apps and profiles provided by AppTec 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.

**Enterprise Wipe device?** 


Are you sure to Enterprise Wipe the device ?

No

Yes

### Send Message

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

**Send a message** 

Subject

Wichtig! Bitte bei Ihrer IT melden!

Message


Sehr geehrter Herr Mustermann,  
bitte melden Sie sich umgehend bei Ihrer IT-Abteilung.




Send Message



### Send Enrollment Request

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


**Send Enrollment Request** 

Send enroll request now ?	<input checked="" type="checkbox"/> On	
Alternative eMail address	matthias <input type="text"/> com	
Send to alt. eMail address ?	<input type="checkbox"/> Off	
Send enroll SMS ?	<input type="checkbox"/> Off	

Enroll now

### Remove MDM

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“.

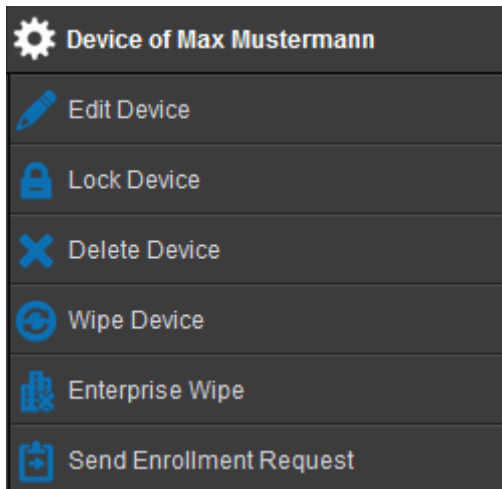
**Remove MDM from device?** 

Are you sure to remove MDM from device ?

NoYes



## Windows



Edit Device	Edit device
Lock Device	Lock device (lock screen)
Delete Device	Remove device from AppTec
Wipe Device	Restore devices to their factory settings
Enterprise Wipe	Information, apps and profile provided by AppTec are deleted
Send Enrollment Request	Send enrollment request (again)

### Edit Device

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

**Update Device**
✕

Selected User	Matthias
Device name	Device of Matthias
Phone Number, e.g. +49160123456	
Device Owner	<input checked="" type="radio"/> Corporate Property <input type="radio"/> Employee Property
Choose device type	<input checked="" type="radio"/> Phone <input type="radio"/> Tablet

Save




### Lock Device

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

### Delete Device

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

## Delete Device



Are you sure to delete this device ?


Device:	Device of Matthias	Delete from System	Root Node
---------	--------------------	--------------------	-----------

Process Delete

### Wipe Device

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

## Wipe Device



Are you sure to wipe the device ?

NoYes



### Enterprise Wipe

Only the information, apps and profiles provided by AppTec 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.

**Enterprise Wipe device?** 


Are you sure to Enterprise Wipe the device ?



No

Yes



### Send Enrollment Request



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

**Send Enrollment Request** 

Send enroll request now ?  

Alternative eMail address  .com

Send to alt. eMail address ?  

Send enroll SMS ?  

Enroll now







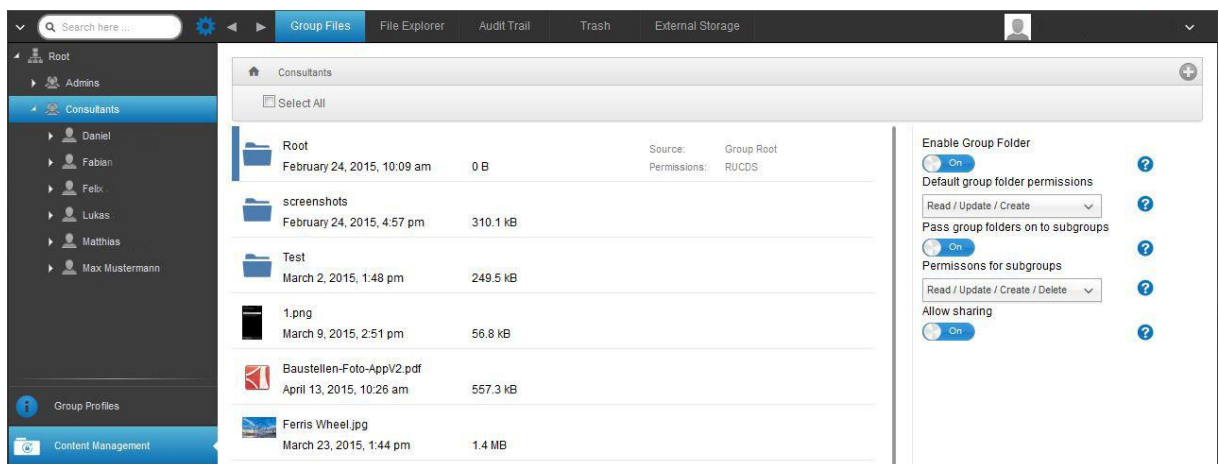
## Content Management


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

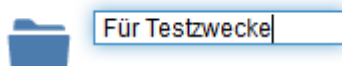
“Group Files” represents a fundamental part ContentBox. Here you establish settings, upload documents, create new folders, etc.




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.

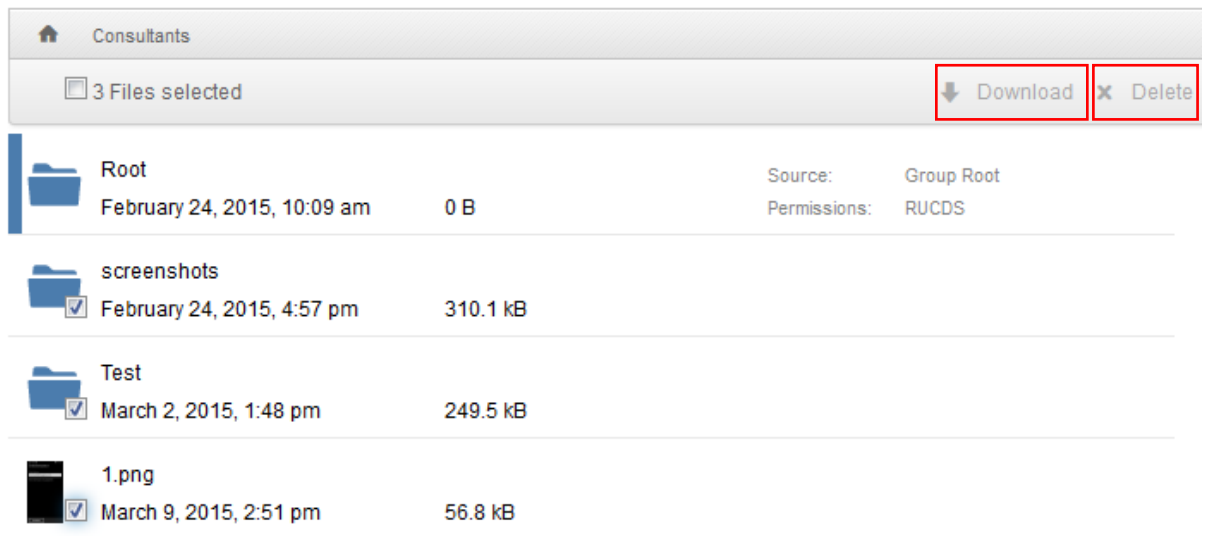


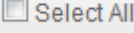
Via “Upload Files”, you can upload data. Here your Standard-Explorer will be opened. You can, of course, perform these two actions in every (sub) folder.

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

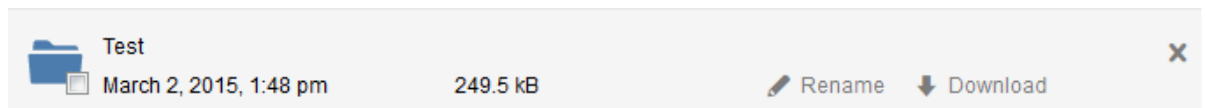


You can select several folders and files and download them with “Download” or you can erase them by clicking “Delete”.



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:

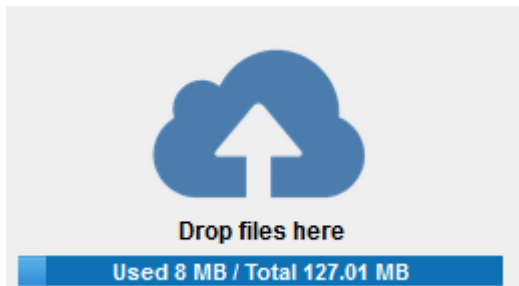


- W
- With “Rename”, you can rename the folder/file
- With “Download”, you can download the folder/file
- With the “X”, you can delete the folder/file



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.

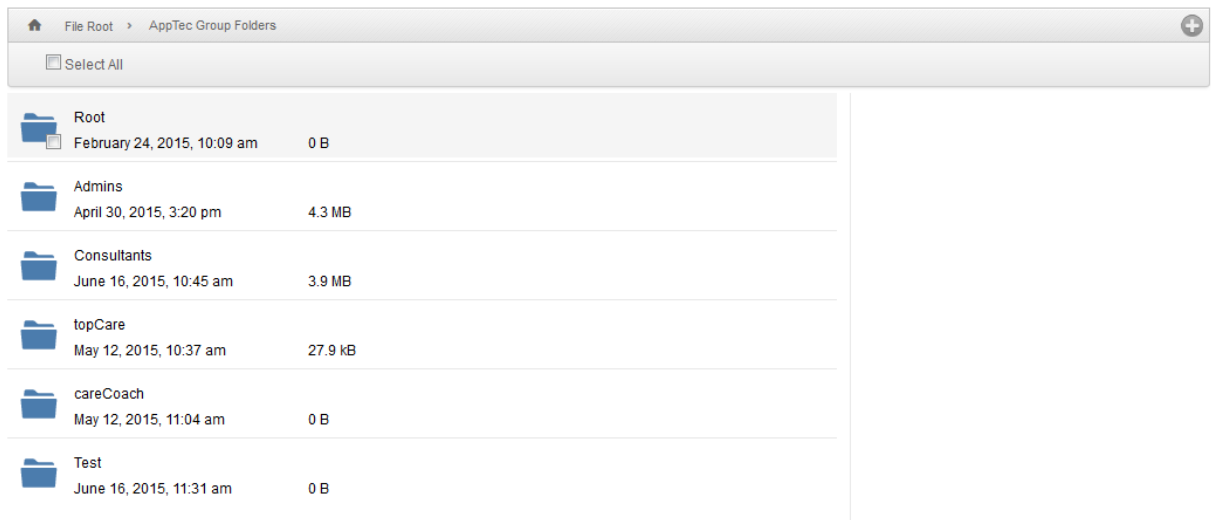




## File Explorer

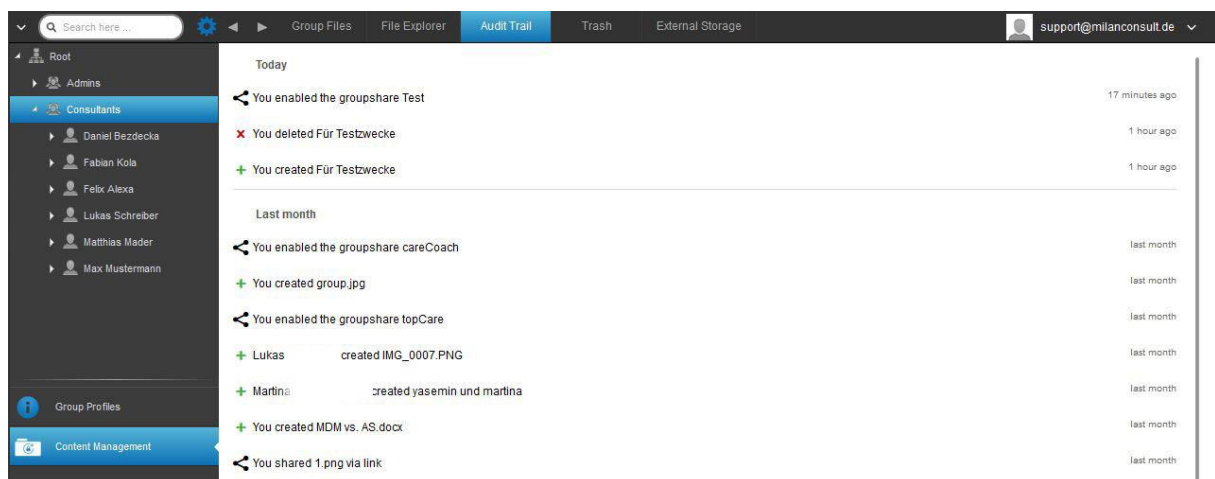
With the “File Explorer“, you can manage all folders and files – regardless of the group where they are filed.

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.



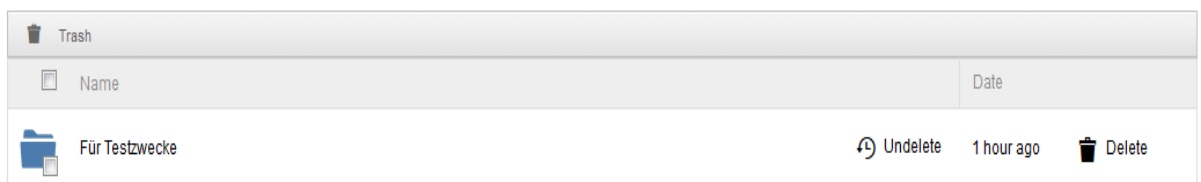


## Trash

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

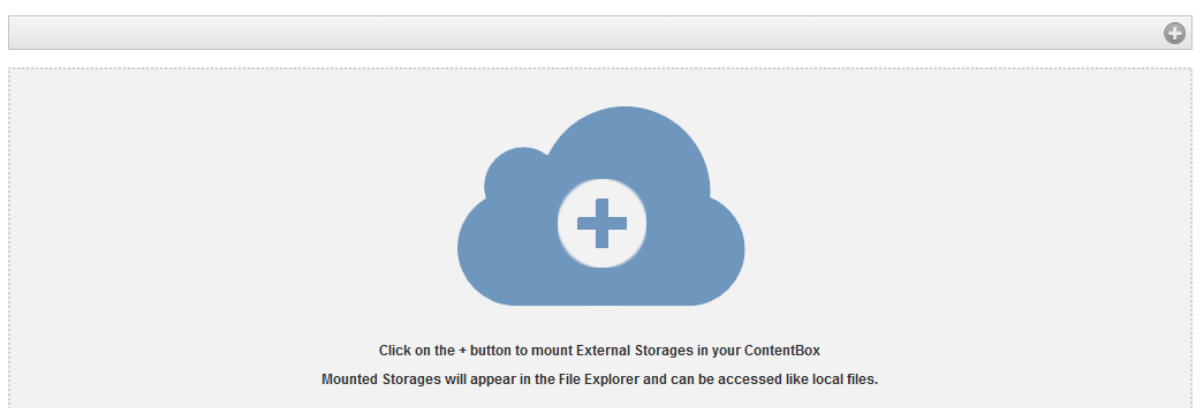
- With “Undelete“, you can recover the data/folder.
- With “Delete“, you can permanently delete the data/folder – you must confirm the dele command once more.

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
<b>Amazon S3</b>	
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
<b>FTP</b>	
Display Name	Display name
Host	Host-Address
Username	Username
Password	Password
Root	Main menu
Secure ftps://	
<b>SFTP</b>	
Display Name	Display name
Host	Host-Address
Username	User name
Password	Password
Root	Main menu
<b>ownCloud</b>	
Display Name	Display name
URL	ownCloud URL
Username	Username
Password	Password
Remote Subfolder	Standard folder
Secure https://	
<b>WebDAV</b>	
Display Name	Display name
URL	WebDAV URL
Username	User name
Password	Password
Root	Main menu
Secure https://	
<b>Windows Share</b>	Support for Windows Share will be available soon
<b>SharePoint</b>	Support for Microsoft SharePoint will be available soon



## Configuration iOS

### 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!

#### Profile Information

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 renamed here
Operating System	Profile's valid OS
Created At	Creation date
Created By	Creator of the profile
Last Change	Date and time the last changes were performed
Changed By	Indicates who created the changes
Profile Revision	Number of times the profile has already been changed

#### 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 AppTec 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 AppTec 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 onto the group profile, you will directly access this profile and you can establish the settings.

With the  symbol, you can revert the designated apps to the settings of the group profile.

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

## Device Log

Under this point you will receive a listing of all actions that have taken place on the end user device, including creating, deleting etc.

Event Log (last 50 events)		
	Event	Date
	User deleted MDM-Profile from device	
	Device enrolled	
	Device enrollment request sent	
	Device assigned to user	
	Device created	



## 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	<p>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)</p> <p>When you go into another cellular network, the "Current MCC/MNC" and "SIM MCC/MNC" are therefore different.</p>

#### Bluetooth

Bluetooth MAC	Bluetooth MAC Address
---------------	-----------------------

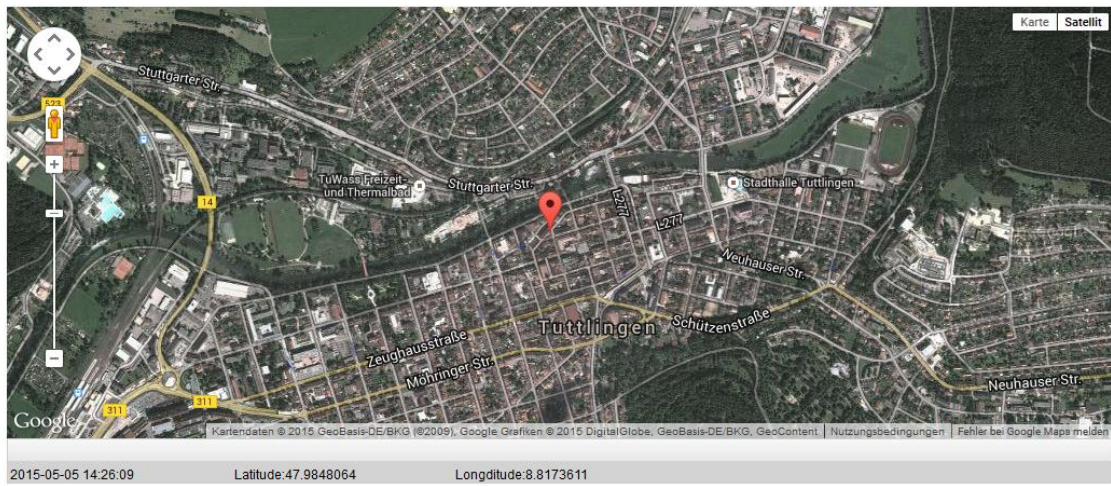


## Security Management

### 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 “Open Message Dialog“, you can send a push-notification.

Open Message Dialog

Subsequently, the following window should open. You can fill in the subject and a message and send it to an end user device.

**Send a message** 

Subject	Test: Bitte bei Ihrer IT melden
Message	<div>Diese Nachricht dient zur Testzwecken! Bitte melden Sie sich bei Ihrer EDV Abteilung. Mit freundlichen Grüßen Ihre IT-Abteilung</div>

Send Message



## 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)

### Installed Certificates

Displays the certificates that are available on the device

Passcode Certificate Encryption Single Sign On			
support@milanconsult.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

**Wipe Device** 

Are you sure to wipe the device ?

No

Yes

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



<b>Available in the Supervised-Mode</b>	
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

<div>  On         </div>	
Whitelisted URLs 	
http://www.apptec360.com/	
Blacklisted URLs 	
www.facebook.com	
Bookmark Title	Bookmark URL 
AppTec English	http://www.apptec360.com/en_home.html 

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

### Wifi

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
<b>None</b>	Establish no Proxy
<b>Manual</b>	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
<b>Automatic</b>	Establish a Proxy automatically
Proxy Server URL	URL for access to the Proxy settings
Security Type	Establish Security Type for the AP
<b>WEP</b>	
Password	Password for the AP
<b>WPA/WPA2</b>	
Password	Password for the AP
<b>WEP Enterprise – WPA / WPA2 Enterprise – Any Enterprise</b>	
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 Control)
Provision PAC	Configuration of Provision PAC
Provision PAC Anonymously	Anonymous Provision of PAC
Inner Authentications	Authentication protocol 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)
<b>None</b>	Establish no security



VPN

Connection Name	Name of the VPN-Profile
VPN Type	
<b>VPN</b>	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
<b>Per-App VPN</b>	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
<b>None</b>	Establish no Proxy
<b>Manual</b>	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
<b>Automatic</b>	Establish a Proxy automatically
Proxy Server URL	URL for access to the Proxy settings
Show Placeholders	Displays all available user-variables , that AppTec 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	
<b>Manual</b>	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
<b>Automatic</b>	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



<b>Incoming Mail</b>	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

<b>Outgoing Mail</b>	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.

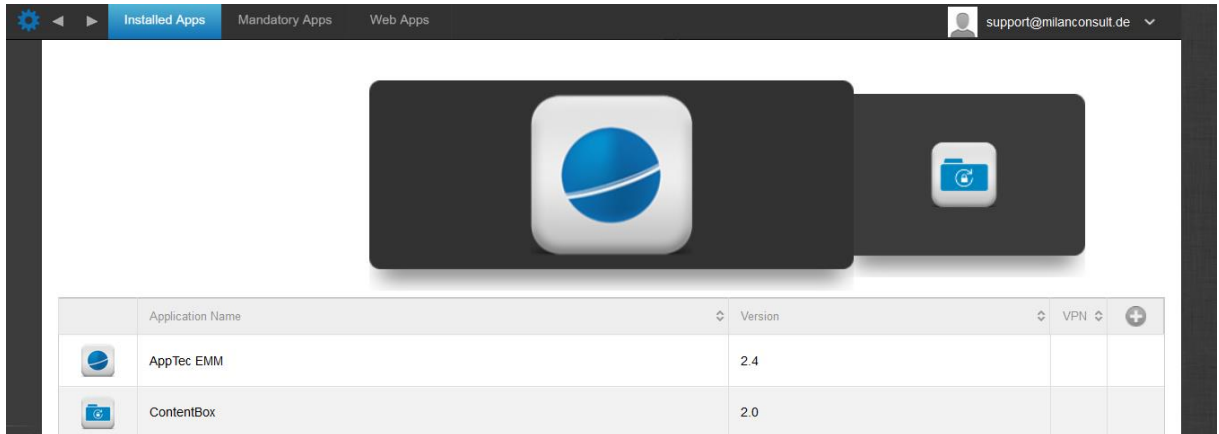
Allowed Websites	
<b>Limit Adult Content</b>	Webfilter is automatically applied for adult content
Permitted URLs	With the + symbol add permitted pages
Blacklisted URLs	With the + symbol add blocked pages
<b>Specific Websites Only</b>	Only specific content can be displayed, which you can add with the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




## App Management

### Enterprise App Manager

#### Installed Apps (only on device level)



Via the  symbol, new Apps can be pushed directly onto the end user device.

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.

Please note that this is a onetime command. Should this App not arrive on the end user device, for any reason, the command will not be repeated!



## 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".


**Upload an In-House App**
✕

**Upload Limit:** max. size of ipa files is 50 MB

Select the .ipa file of the iOS application which you want to upload

Keine Datei ausgewählt.

## 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.




◀

Installed Apps


Mandatory Apps


Web Apps



support@milanconsult.de

▼



	Application Name	Mandatory Since	Source	
	mytaxi - Die Taxi App	March 3, 2015, 1:26 pm	iTunes	

This can be, just as with the “Installed Apps”, an Apple App Store App, but also an In-House App.

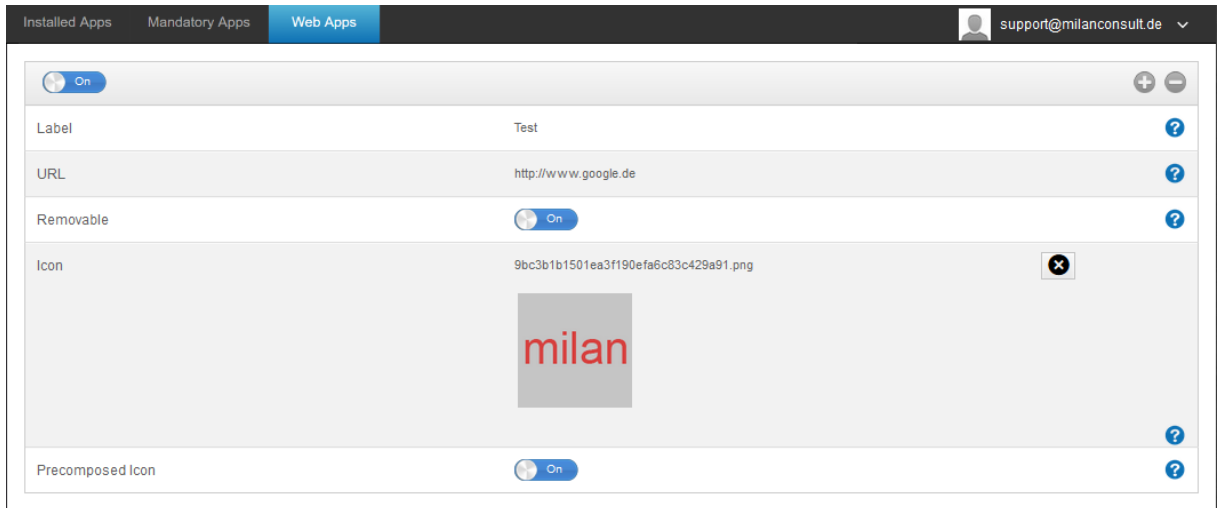
Should this involve a supervised device, then the app will be installed automatically.

The servicing follows just as under the Installed Apps point.



## 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
<u>Removable</u>	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

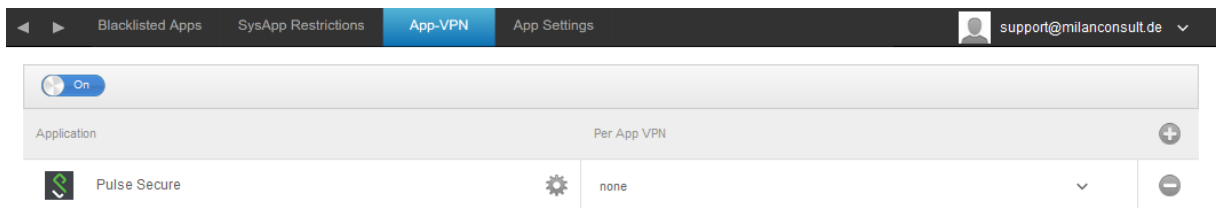
Block specific apps or functions of your device

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 JavaScript	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.



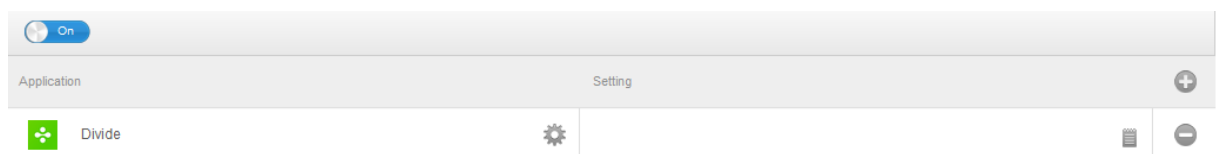
## App Settings

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 AppTec 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:

**App Settings** 

PLIST


Key / Value

Show Placeholders

Save


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.

**App Settings** 


PLIST

Key / Value

Key	Value	Type	
-----	-------	------	---

Show Placeholders

Save

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



**App Settings**
✕

PLIST

Key / Value

Key	Value	Type	+
email_address	%usermail%	String ▼	-


Show Placeholders

Save

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 AppTec 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.

Application Name	↕	Version	↕	+
------------------	---	---------	---	---



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.

**Select an application**
✕

**Apple iTunes**

Tablet ▾

Germany ▾

Search Now

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


**Select an application**
✕

**Apple iTunes**

Tablet ▾

Germany ▾

Search Now




**DB Navigator für iPad**  
Deutsche Bahn  
Reisen

Mit dem DB Navigator erhalten Sie den perfekten Routenplaner für die Navigation im ÖPNV. Egal ob ICE, Regionalverkehr, S-Bahn oder U-Bahn, Sie haben stets Zugriff auf den aktuellen Fahrplan mit übe...

free

---




**Catch The Right Dots Kicktipp**  
ZDFmediathek Das Erste One For Eleven Tipico Sports bwin 7TV Mediathek TorAlarm Brasilien Quizduell DB Navigator Kleiderkreisel Cookie Jam NettoApp Magine SPORTSCHAU Math 42 Marcophono RegenRadar Tayasui  
Hongxiang Jin  
Spiele

Catch the right dots falling from top. The bottom line will change color all the time, make sure only the right dots with the same color touch the bottom. Or game is over. Tap on dots can remove t...

free

---



**Capitaine Train: Bahn-Tickets Kaufen**  
Capitaine Train  
Reisen

Capitaine Train ist die schnellste und günstigste Art Fahrkarten zu kaufen. Seit 2011 vertrauen uns rund eine halbe Millionen User beim Kauf ihrer Fahrkarten für die Deutsche Bahn, SNCF, Thalys, Ly...

free

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



**Install DB Navigator für iPad ?**
✕

Keep up to date
Off

Remove app when MDM profile is removed.
On 
?

Prevent backup of the app data.
Off 
?

App VPN
none

Install

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 AppTec AppStore.

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

### In-House

◀ ▶ iTunes Apps In-house
 support@milanconsult.de ▼

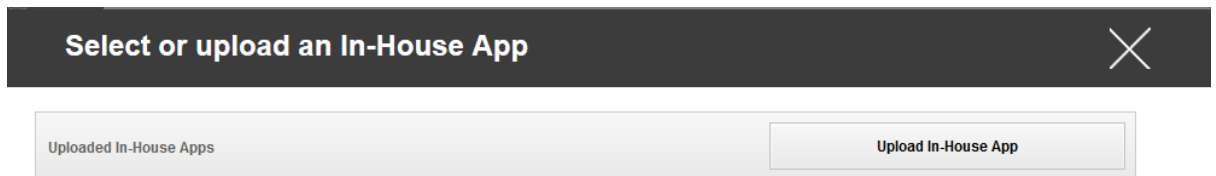
	Application Name	Version	+
	WordPress	4.9	



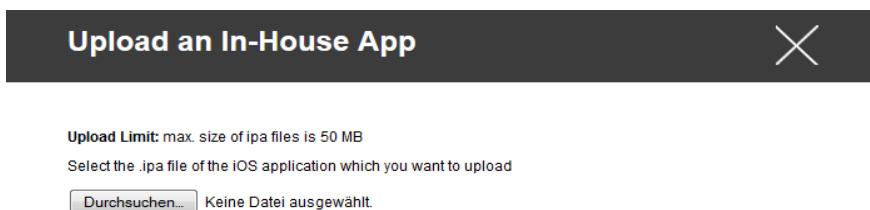
Under the point “In-House“, you can upload internally developed Apps and distribute them.

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

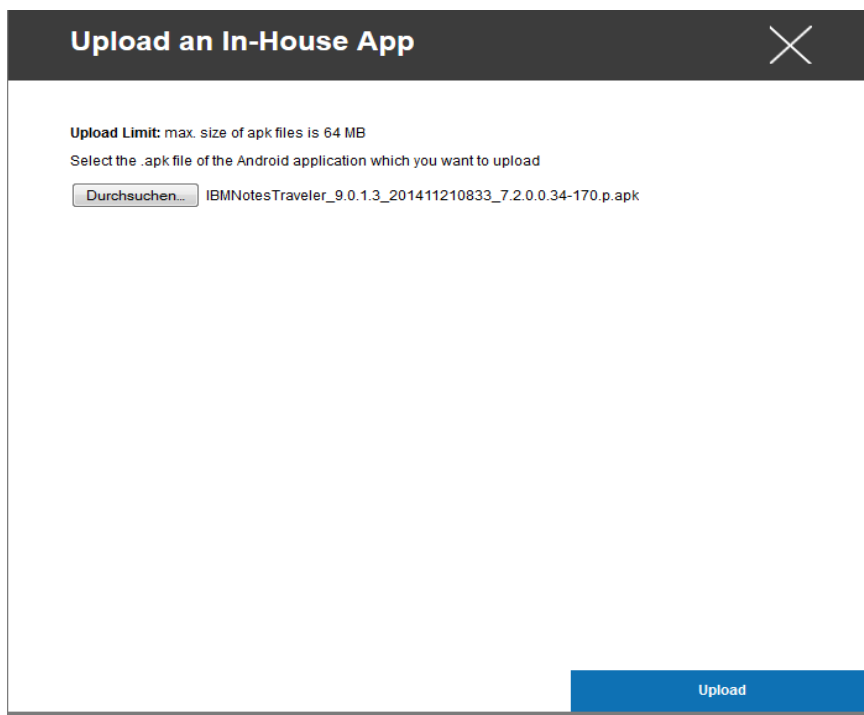
If you have never distributed In-House App, you will then receive the following overview:



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



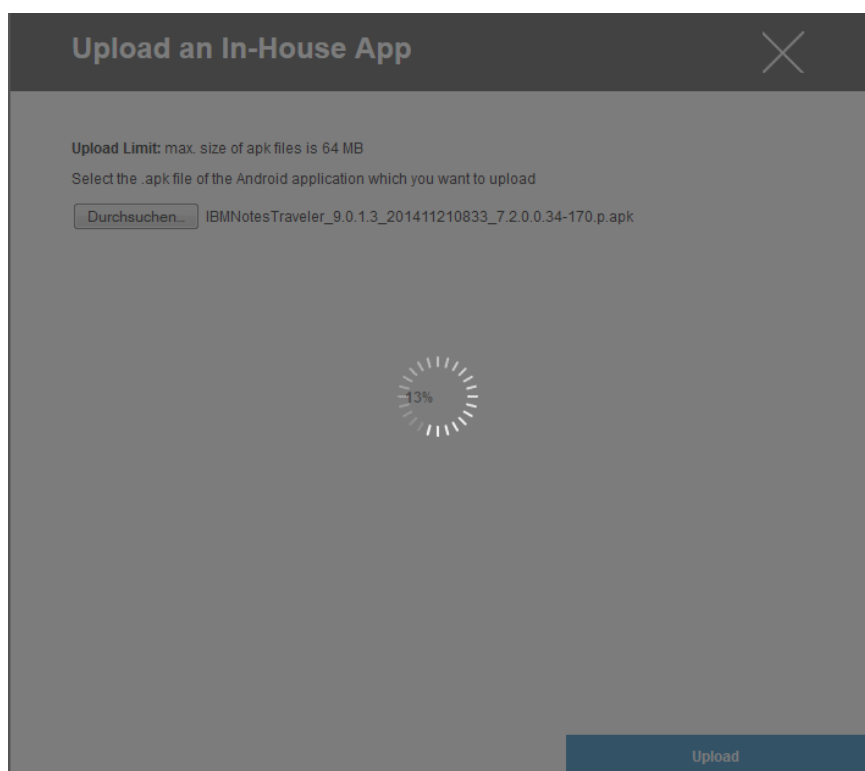
select  
.ipa  
click



Now,  
with  
“Search...” an  
file and then  
on “Upload”.

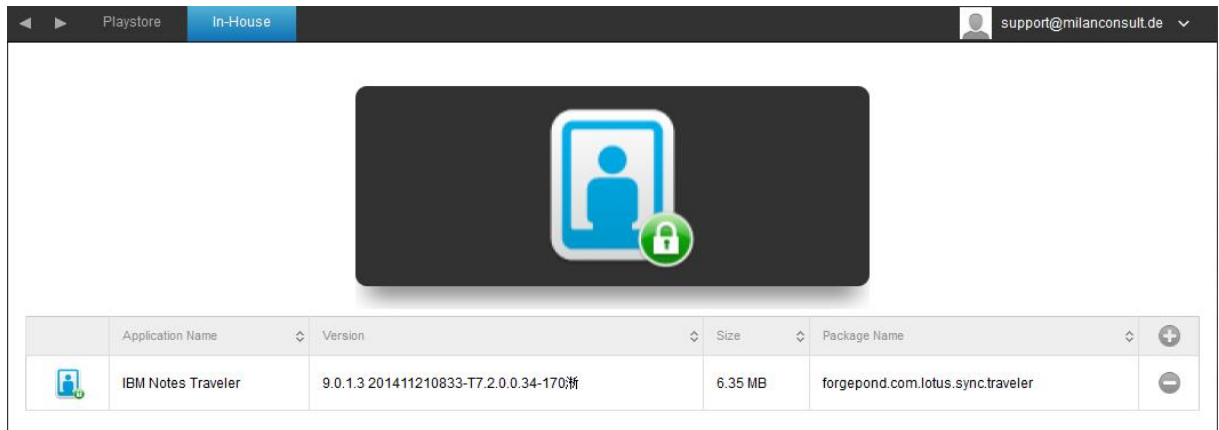


Your App will now be uploaded. In the middle of the circle, you can see the percentage of how much of your App has been already uploaded.



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 AppTec 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

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.

Available in Supervised Mode	
Application Type	Package
	URL
<b>Package</b>	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”
<b>URL</b>	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
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

## Content Management

### ContentBox

Here you can activate/deactivate ContentBox

Enable ContentBox	Enable ContentBox
-------------------	-------------------

## Android Configuration

Depending on if you have currently selected a 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
Profile Revision	Number of times the profile has already been updated




### 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
Phone Number	Phone number
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
Last Seen	Point in time, when the device last connected to AppTec

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

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

### Device Log

Here you will receive various device logs. If needed, you can directly find out the cause of an error here.



## 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
Enforcement action after disabling Device Management	Action that is to be taken, when device management is deactivated: → do nothing = no action → Lock Device = lock device → Wipe Device = device will be restored to factory settings
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 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 Network Location 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



## Asset Management (only on device level)

### 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



	<p>The IMSI is comprised of a maximum of 15 digits and is configured in the following manner:</p> <ul style="list-style-type: none"> <li>• (MCC), 3 digits</li> <li>• (MNC), 2 or 3 digits</li> <li>• Mobile Subscriber Identification Number (MSIN), 1-10 digits</li> </ul>
Current MCC/MNC	See "SIM MCC/MNC"
SIM MCC/MNC	<p>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.</p> <p>Meaning the SIM card's country/Mobile Network Code.</p> <p>If you roam into another mobile network, then logically, the "Current MCC/MNC" and "SIM MCC/MNC", will be different.</p>

### Bluetooth

Bluetooth MAC	Bluetooth MAC address
---------------	-----------------------

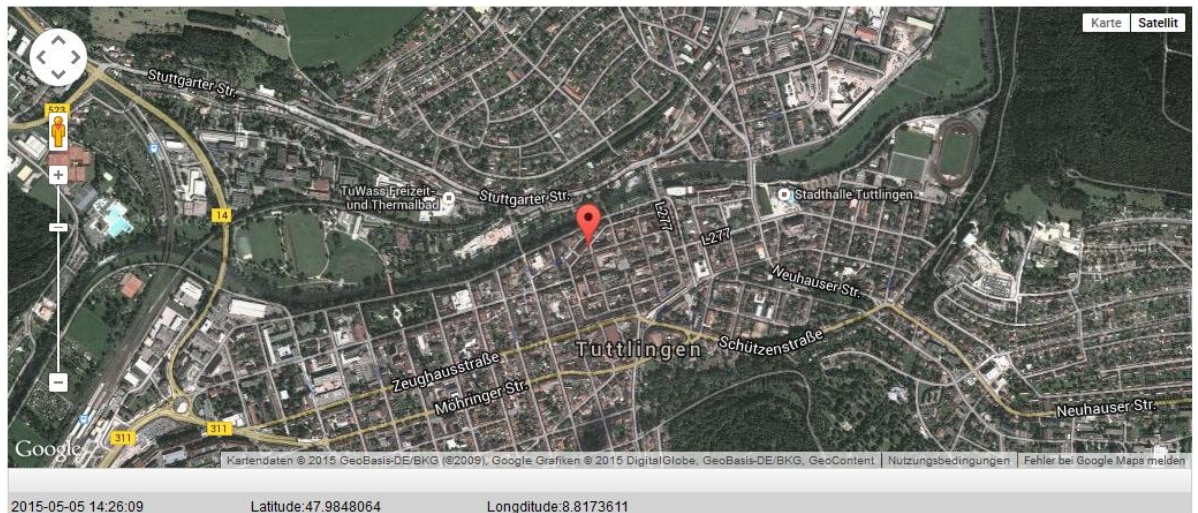


## Security Management

### 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 AppTec )
Lock Screen	Screen lock is activated, it is sufficient to unlock the device with the device-password/PIN




Message (only on device level)

With “Open Message Dialog“, you can send a push-notification.

Open Message Dialog

Subsequently, the following window should open. You can fill in the subject and a message and send it to an end user device.

**Send a message** 

Subject	Test: Bitte bei Ihrer IT melden
Message	<div>Diese Nachricht dient zur Testzwecken! Bitte melden Sie sich bei Ihrer EDV Abteilung. Mit freundlichen Grüßen Ihre IT-Abteilung</div>

Send Message



## 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 user inactivity until time lock
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	<p>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.</p> <p>Likewise, the Password Policy will be automatically switched to 6 alphanumeric symbols</p>
Require SD Card Encryption	<p>This setting only applies to Samsung devices!</p> <p>If this setting is activated, the external SD card can be encrypted and can only be manually un-encrypted on the end user device.</p> <p>Likewise, the Password Policy will be automatically switched to 6 alphanumeric symbols</p>

## AntiVirus

Scan Method	<p>Quick = Only apps will be scanned for damaged code / viruses</p> <p>Full = The entire system will be scanned for damaged code / viruses</p>
Scan Interval	Interval for examination (Quick / Full)
Update Check	How often the app and its database should be updated (viruses / damaged code)
Protection Mode	At the launch and installation of the App, a scan for damaged code is performed
Self-Configuration	If activated, the user will be able to configure/change settings on the end user device
Connect During Roaming	Connect while the end user device is roaming



## 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
-------------------	--

Wipe Device

Are you sure to wipe the device ?

Wipe SD Card too ?
☐

No

Yes

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 Network Location	On = Permanent internet-localizing Off = Permanent deactivation of internet-localizing User choice = selected by the user



For Samsung devices with the SAFE 2.0 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 Sideload)	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.



## AFW Device Owner

(Device has to be in [Android for Work Device Owner Mode](#))

<b>Security</b>	
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
<b>App Management</b>	
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.
<b>Connectivity</b>	
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
<b>Bluetooth</b>	
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.
<b>Account Management</b>	
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 Remove User	Specifies if managed profiles of this user can be removed, other than by its profile owner.
Disallow Account Modification	Specifies if a user is disallowed from adding and removing accounts, unless they are programmatically added by Authenticator.
<b>Telephony</b>	
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.
<b>System</b>	
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.
<b>Storage</b>	
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.



<b>Keyboard</b>	
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.
<b>Sound</b>	
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.



## BYOD Container

### Android for Work


#### Android for Work

Enable Android for Work	Enable Android for Work (Afw). Afw is supported since Android 5.0, but due to Bugs it's recommended only for devices with Android 5.1.1 and above.
Runtime Permission Policy	Prompt user for new permission requests Always grant new new permission requests Always deny new permission requests
Allow Unknown Sources	If enabled, users can sideload Apps by installing an .apk file.
Allow USB Debugging	If enabled, users can enable USB Debugging.
Allow Cross profile Copy & Paste	If enabled, profiles have a common clipboard
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

### Divide Exchange

You need to approve the App "Divide Productivity" before you can configure Exchange Accounts.

Click on the button to open the "Divide Productivity" Store Page at Google Play for Work

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  you can display them for yourself
Use AppTec Gateway	Choose the Gateway Configuration you want to use.
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
Password	The Password for the given User



Signature	Mail Signature. Note: Some devices require HTML
Number of previous days to sync	Number of days, determining when emails are sync'd back
Device Identifier	The value should be a string containing the EAS DeviceID. It is part of EAS protocol, used for device correlation by some environments
Sync while Roaming	If disabled the Sync is disabled while Roaming
Use Secure Sockets Layer (SSL)	Activates SSL
Accept all certificates	All certificates are accepted. Please select this option, if your Exchange Server uses a self-signed certificate
Enable Tasks	If enabled Tasks are also synchronized
Enable Notes	If enabled Notes are also synchronized

### System Apps

Here you can enable System Apps for the Android for Work Container.

### Samsung KNOX

#### Activation

Under this setting, you can make a PIM (Personal Information Manager) Container available.

You can either open the “Google Divide” Container or the “SecurePIM” Container, as well as Samsung KNOX with the On/Off Buttons.

The selected App will then be installed automatically on the end user device.

### 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 alphanumerical 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

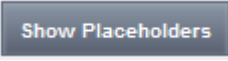
Limit specific device functionalities

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

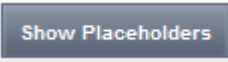
### Knox Exchange



Here you can configure the Exchange-Profile for the KNOX Container.

eMail Address	<p>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</p> <p>With a click  you can display them for yourself</p>
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	<p>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</p> <p>With a click  you can display them for yourself</p>
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
<b>WEP</b>	
Password	Password for the AP



<b>WPA/WPA2</b>	
Password	Password for the AP
<b>802.1x EAP</b>	
EAP-Method	
PWD	Activate/deactivate
PEAP	Activate/deactivate
TTLS	Activate/deactivate
TLS	Activate/deactivate
Authentication	
<b>PWD</b>	
Identity	Identity
Password	Password
<b>PEAP</b>	
Phase 2 Authentication Protocol	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
<b>TTLS</b>	
Phase 2 Authentication Protocol	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
<b>TLS</b>	
CA Certificate	CA certificate
Identity	Identity
Password	Password

### VPN

Connection Type	Establish VPN-connection type



<b>Cisco AnyConnect</b>	
Connection Name	VPN connection name
Server	Server address
Certificate Mode	Disabled = deactivated Automatic = automatic
<b>L2TP (SAFE 2.x)</b>	Only available on SAFE 2.x devices
Connection Name	Connection name
Server	Server address
Enable L2TP Secret	
DNS Search Domains	DNS search domains
<b>PPTP (SAFE 2.0+)</b>	Only available on SAFE 2.x or higher
Connection Name	VPN connection name
Server	Server address
Enable Encryption	Enable encryption
DNS Search Domains	DNS search domains
<b>L2TP / IPSec PSK (SAFE 2.0+)</b>	Only available on SAFE 2.x or higher
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
<b>IPSec XAuth PSK (SAFE 3.0+)</b>	Only available on SAFE 3.0 or higher
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
<b>OpenVPN</b>	
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 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)

### 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 SAFE 2.0 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



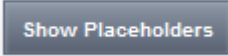
Allow Bluetooth Tethering	Allows using the device as a modem (Bluetooth internet connection)
Allow connection to Computer via Bluetooth	Allow connection to Computer via Bluetooth



## PIM Management

### Exchange

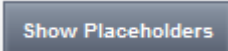
Only available for Samsung SAFE 1.0 or higher!

eMail Address	<p>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</p> <p>With a click  you can display them for yourself</p>
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 ( <i>Hint: Some devices require HTML formatting for the signature</i> )
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 SAFE 2.0 or higher!	
eMail Address	<p>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</p> <p>With a click  you can display them for yourself</p>
Incoming server protocol	Incoming server protocol → IMAP o 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 ( <i>Hint: Some devices require HTML formatting for the signature</i> )
Notify user on receiving new eMail	Notifies user on receiving new email



### AFW Gmail Exchange


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

eMail Address	<p>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</p> <p>With a click  you can display them for yourself</p>
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 ( <i>Hint: Some devices require HTML formatting for the signature</i> )
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



## Touchdown Exchange

If you want to use Touchdown (3rd Party App), you can activate it here and configure it in the foreground.

Hostname of the Exchange Server	Hostname of your Exchange Server (FQDN or IP address)
eMail Address for the Exchange Account	<p>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</p> <p>With a click  you can display them for yourself</p>
Username for the Exchange Account	The username for the respective end user device, please also note the "Placeholders" here
Password for the Exchange Account (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
Allow User to Change Email Signature	Allow user to change email signature
License Key	Touchdown must be licensed separately, your license-code must be entered here
Device Type reported in Exchange Server	Establish the label here, that should be sent from the device to the Exchange Server
Allow Backup of Emails and Settings	Allow backup of emails and settings
Allow Self signed certificates	Allow self-signed certificates
Allow HTML Formatted Email	Allow HTML formatted email
Allow Attachments	Allow attachments
Enable TouchDown Widgets	Should this setting be activated, the user can use TouchDown Widgets on their end user device
Maximum Attachment Size (KB)	Establishes in KB, how big an attachment can be
Maximum Email size (KB)	Establishes in KB, how big an email can be. Should this limit be exceeded, this email will appended to the prescribed size
Signature	Pre-defined signature

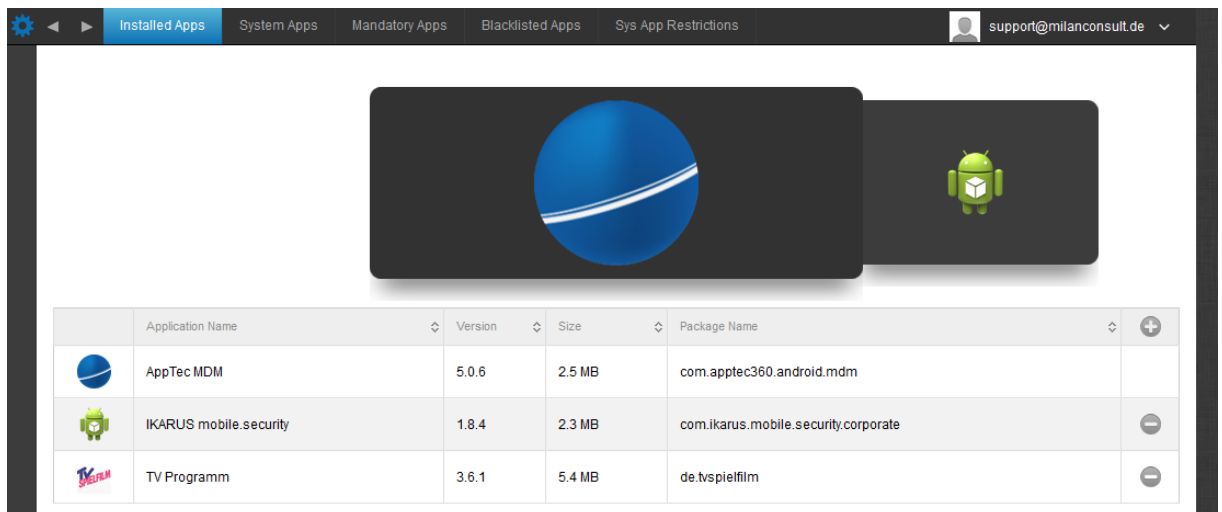





## App Management


### 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.



	Application Name	Version	Size	Package Name	
	AppTec MDM	5.0.6	2.5 MB	com.apptec360.android.mdm	+
	IKARUS mobile.security	1.8.4	2.3 MB	com.ikarus.mobile.security.corporate	-
	TV Programm	3.6.1	5.4 MB	de.tvspielfilm	-

Via the \_symbol, new apps can be pushed to the end user device.

You can push a “Google Play Store“ App from the public AppStore, into the device.








**Select an application**
✕

Google Play Store   Android In-House Apps

German

Free Apps

Search Now


	<b>DB Navigator</b> Deutsche Bahn <small>free</small>	<small>App Berechtigungen - Datenschutz ist uns wichtig. Für Informationen über die Berechtigungen der App DB Navigator besuchen Sie bitte: <a href="http://www.bahn.de/androidrechte">www.bahn.de/androidrechte</a> Egal ob ICE, S-Bahn, Bus oder Straßenbahn, Sie haben stets Zugriff auf den aktuellen Fahrplan in ganz Deutschland und Europa mit über 250.000 Haltestellen. Mit Echtzeit-Informat ...</small>
	<b>DB Zugradar</b> Deutsche Bahn <small>free</small>	<small>Alle Züge auf einen Blick: Mit dem DB Zugradar verfolgen Sie die Züge des DB Nah- und Fernverkehrs live im DB Zugradar und grenzen Sie durch den Filter die Darstellung der Verkehrsmittel (Fernverkehr (ICE und IC/EC), Nahverkehr) und Bahnhöfe ein. Der DB Zugradar stellt auf einer dynamischen Karte das gesamte Streckennetz der Deutschen B ...</small>
	<b>Schallmessung : Sound Meter</b> Smart Tools co. <small>free</small>	<small>Sound Level Meter ist im Paket 4 der Smart Tools Sammlung. (Lautstärke) Achtung! Die meisten Mikrofone sind für die menschliche Stimme (300-3400Hz, 40-60dB) ausgelegt. Also sind die maximalen Werte der Hardware begrenzt. Motorola Milestone(max. 100), Galaxy S(max. 81), Galaxy S2(98dB), Galaxy Tab und HTC Desire HD wurden mit echten Schallpe ...</small>
	<b>München Navigator</b> Deutsche Bahn <small>free</small>	<small>Egal ob Sie die S- oder U-Bahn, die Tram oder den Bus nutzen, mit dem München Navigator (ehemals: Navi S-Bahn München) können Sie ab sofort Ihr passendes Handy-Ticket für den gesamten Münchner Verkehrsverbund (MVG) bis kurz vor Fahrtbeginn kaufen und sich zusätzlich über die Position ihres Zuges oder eventuelle baubedingte Störungen i ...</small>
	<b>Öffi - Fahrplanauskunft</b>	<small>All-in-one App für die Öffentlichen Verkehrsmittel: • Echtzeit-Abfahrtszeiten (inkl. Verspätungen), • nahegelegene Haltestellen (mit Karte), • Verbindungs-Abfragen (von Haustür zu Haustür) und •</small>

Or select an In-House App from the “Android In-House Apps”, which you have uploaded in General Settings.

**Select an application**
✕

Google Play Store   **Android In-House Apps**

Uploaded In-House Apps



**IBM Notes Traveler**  
Version: 9.0.1.3 201411210833-T7.1.0.0.52-271G  
forgepond.com.lotus.sync.traveler

No description available

i

Upload In-House App



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

Upload an In-House App

Upload Limit: max. size of apk files is 64 MB

Select the .apk file of the Android application which you want to upload

Durchsuchen...















Keine Datei ausgewählt

Upload



## System Apps (only on device level)

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

<div> <div>◀ ▶</div> <div>Installed Apps</div> <div><b>System Apps</b></div> <div>Mandatory Apps</div> <div>Blacklisted Apps</div> <div>Sys App Restrictions</div> <div>  support@milanconsult.de ▼         </div> </div>					
					
	Application Name	Version	Size	Package Name	
	Adapt Sound	1.0	2.8 MB	com.sec.hearingadjust	
	AllShare ControlShare Service	1.0.0	355 kB	com.sec.android.allshare.service.cont...	
	AllShare FileShare Service	1.4r476	39 kB	com.sec.android.allshare.service.file...	
	Android-System	4.3-I9300XXUGNG3	35 MB	android	
	Application installer	1.0	39 kB	com.sec.android.preloadinstaller	
	BadgeProvider	1.0	4 kB	com.sec.android.provider.badge	
	BandService	1.42	518 kB	com.sec.android.band	
	Basic Daydreams	4.3-I9300XXUGNG3	32 kB	com.android.dreams.basic	
	Benutzerhandbuch	1.0	23 kB	com.sec.android.widgetapp.webmanual	
	Best Face	20130529.1.0.0.46	199 kB	com.arcssoft.picturesbest.app	
	Bevorzugte Apps	1.0	1.4 MB	com.sec.android.favoriteappwidget	
					



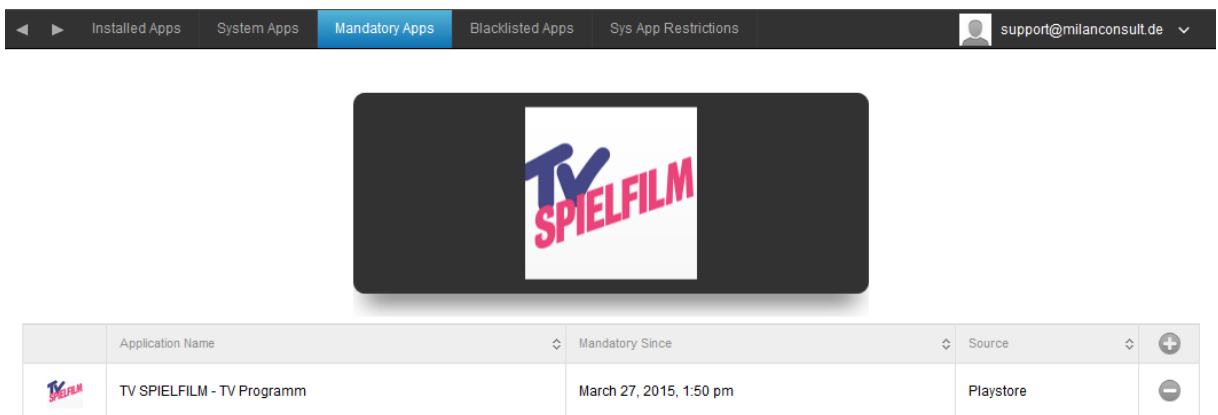
## Mandatory Apps



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.

Just as with “Installed Apps“, it can be a Google Play Store App, but also an 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.



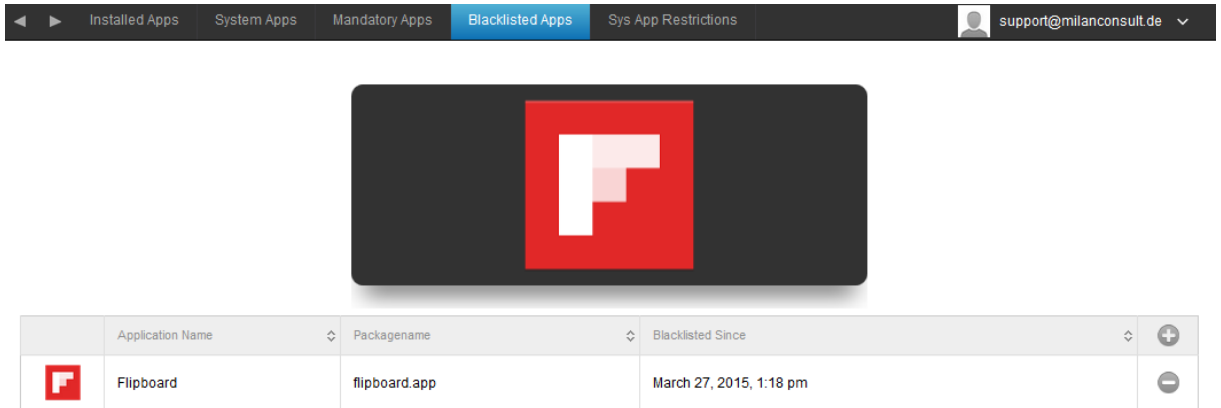
	Application Name	Mandatory Since	Source	
	TV SPIELFILM - TV Programm	March 27, 2015, 1:50 pm	Playstore	



The user interface works exactly the same as with the category “Installed Apps“.




## Blacklisted Apps

Under “Blacklisted Apps“, you can define apps and services, that cannot be installed on the end user device and/or these will be deactivated and set, so that the user cannot run them.



	Application Name	Packagename	Blacklisted Since	
	Flipboard	flipboard.app	March 27, 2015, 1:18 pm	

Via the  , you add additional blacklisted apps or services.

You can either select a Google Play Store App.

**Select an application**
✕

Google Play Store
Packagename

German

▼

Free Apps

▼

Search Now

Or define a “Packagename“.

**Select an application**
✕

Google Play Store
Packagename

Add Package



You will find this Packagename either under the “Installed Apps” / “System Apps” under “Packagename” or you can find it on the left side of the Google Play Store.

Example:

App Name: TV movie – TV show

Google Play Store Link:

<https://play.google.com/store/apps/details?id=de.tvspielfilm&hl=de>

The Packagename is then this one, starting with the “equal sign” and goes up to the “and-symbol”.

Package name: de.movie

This is the same with all Google Play Store Apps.



## 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




## Enterprise App Store

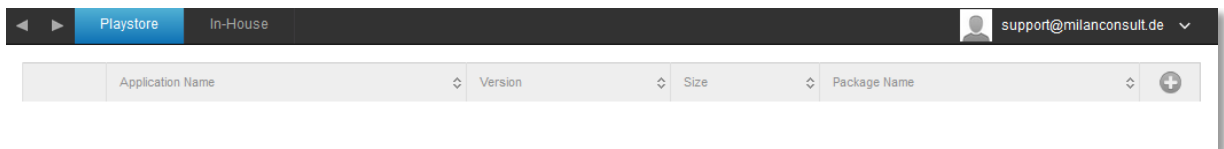
### Playstore

Under this point, you can distribute optional Apps to your users.

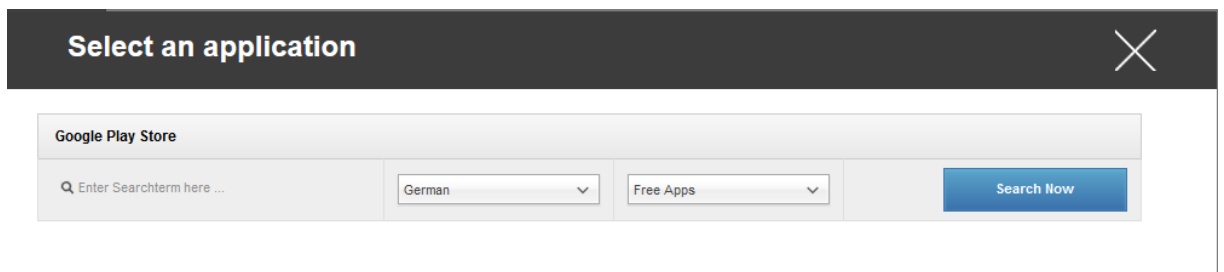
This is simply a linking with the official Google Play Store. It is for this reason, that a Google ID is placed on each device.

Here we recommend, that each user has their own Google Play Store ID.

With the  symbol, you can add additional apps.



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



With “Enter Searchterm here ...”, you can search for an app that is in the Google Play Store.








Select an application
✕

Google Play Store

German ▾

Free Apps ▾

Search Now

	<b>DB Navigator</b> Deutsche Bahn free	App Berechtigungen - Datenschutz ist uns wichtig. Für Informationen über die Berechtigungen der App DB Navigator besuchen Sie bitte: <a href="http://www.bahn.de/androidrechte">www.bahn.de/androidrechte</a> Egal ob ICE, S-Bahn, Bus oder Straßenbahn, Sie haben stets Zugriff auf den aktuellen Fahrplan in ganz Deutschland und Europa mit über 250.000 Haltestellen. Mit Echtzeit-Informat ...
	<b>DB Zugradar</b> Deutsche Bahn free	Alle Züge auf einen Blick: Mit dem DB Zugradar verfolgen Sie die Züge des DB Nah- und Fernverkehrs live im DB Zugradar und grenzen Sie durch den Filter die Darstellung der Verkehrsmittel (Fernverkehr (ICE und IC/EC), Nahverkehr) und Bahnhöfe ein. Der DB Zugradar stellt auf einer dynamischen Karte das gesamte Streckennetz der Deutschen B ...
	<b>Schallmessung : Sound Meter</b> Smart Tools co. free	Sound Level Meter ist im Paket 4 der Smart Tools Sammlung. (Lautstärke) Achtung! Die meisten Mikrofone sind für die menschliche Stimme (300-3400Hz, 40-60dB) ausgelegt. Also sind die maximalen Werte der Hardware begrenzt. Motorola Milestone(max. 100), Galaxy S(max. 81), Galaxy S2(98dB), Galaxy Tab und HTC Desire HD wurden mit echten Schallpe ...
	<b>Meine Bank</b> Deutsche Bank AG free	Vielen Dank für die Rückmeldungen im Play Store und aus der Feedbackfunktion der „Meine Bank“-App. Ihre Anregungen tragen dazu bei, diese App immer weiter zu verbessern. Wofür brauche ich die „Meine Bank“-App? Mit der „Meine Bank“-App erledigen Sie Ihre Bankgeschäfte von überall aus. Prüfen Sie Ihren Konto- oder Depotsta ...
	<b>Ist mein Zug pünktlich?</b>	Fährst Du oft mit der Bahn? Hat Dein Zug oft Verspätung? m.bahn.de bietet die Funktion "Ist mein Zug pünktlich?". Mit dieser App kannst Du oft defahrene Züge speichern und so schnell und einfach auf "Ist

Once you click on the icon or on the name of the app, you will asked once again, if you want to add this app to the App Catalog – confirm this with “yes”.

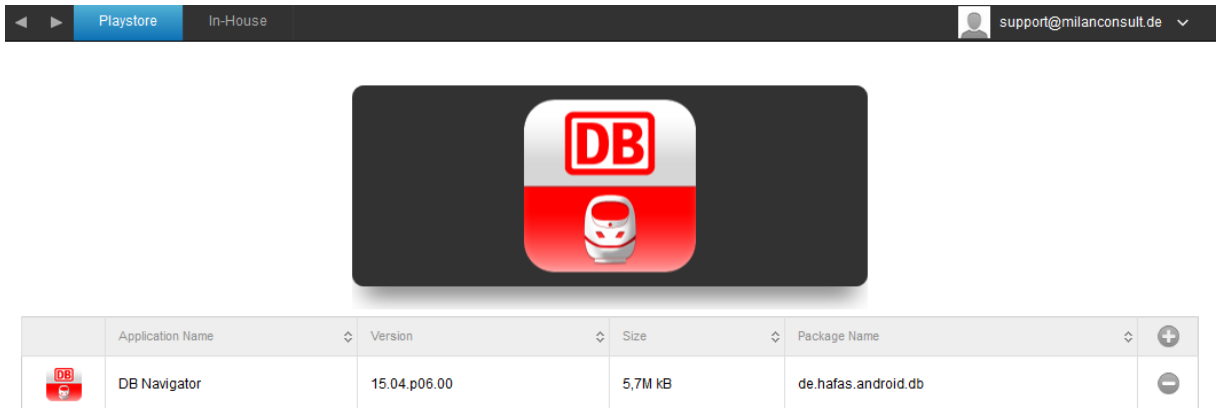
Add app to AppTec App Store ?
✕



Add DB Navigator to the device app catalog.

yes



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



	Application Name	Version	Size	Package Name	
	DB Navigator	15.04.p06.00	5,7M kB	de.hafas.android.db	


Thereby, the App-Store Import is completed and the user can then see AppTec's AppStore.

If the user opens this Store, they can see all of the distributed apps and install them.

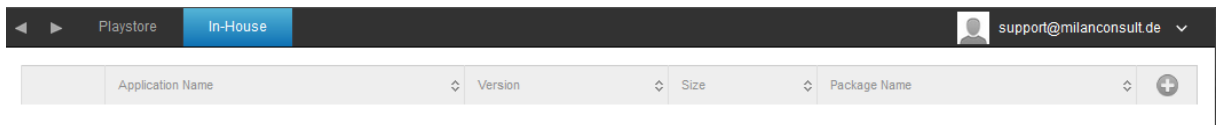


## In-House

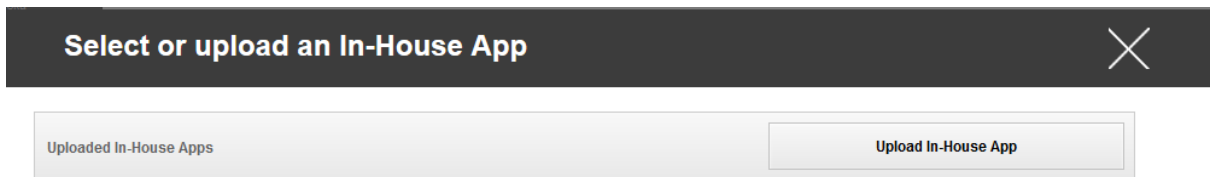
Under the point “In-House“, you can upload and distribute internally developed apps.

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

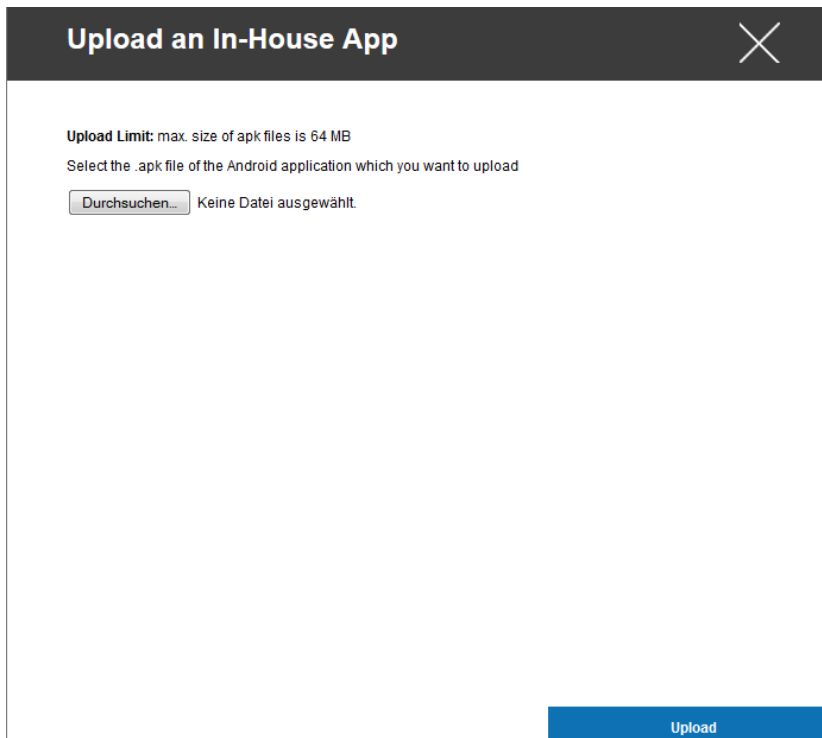
If you are installing an In-House App, you will have the possibility to activate „Keep up to date“. If this is activated and you have defined a newer version in the In-House App DB, the app will be updated on the device.



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”.



**Upload an In-House App** ✕

**Upload Limit:** max. size of apk files is 64 MB

Select the .apk file of the Android application which you want to upload

IBMNotesTraveler\_9.0.1.3\_201411210833\_7.2.0.0.34-170.p.apk

**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.

**Upload an In-House App** ✕

**Upload Limit:** max. size of apk files is 64 MB

Select the .apk file of the Android application which you want to upload

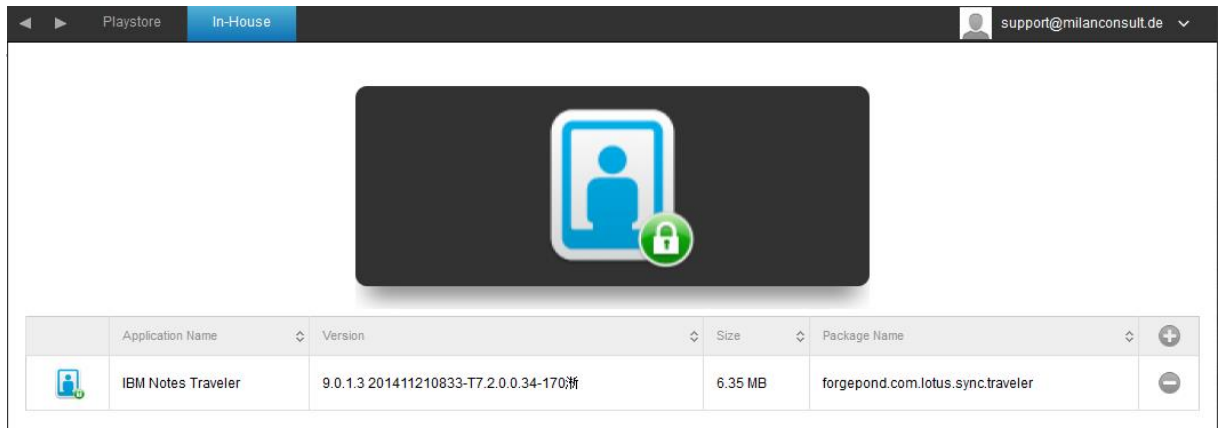
IBMNotesTraveler\_9.0.1.3\_201411210833\_7.2.0.0.34-170.p.apk



**Upload**



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



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.

#### [AFW Playstore](#)

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

## 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
	URL
	Multi App
<b>Single App</b>	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"
<b>URL</b>	If you want to launch a URL in the Kiosk Mode, select "URL" under "Application Type"
URL	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: 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
<b>Multi App</b>	If you select the "Multi App" Kiosk Mode, the use of the AppTec 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 collapsed. 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 AppTec 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 AppTec Console (only available on Samsung devices with SAFE 3.0 or higher)

### AppTec Launcher

Enable AppTec Launcher	On: Enables the Apptec 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 AppTec launcher will be enforced.
Large Icons	On: Shows a larger Version of the App Icons in the Launcher
Hide AppTec App Icon	On: Hides the AppTec App completely
Hide AppTec Store Icon	On: Hides the AppTec Enterprise Store completely

### AppTec Settings

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



Wallpaper

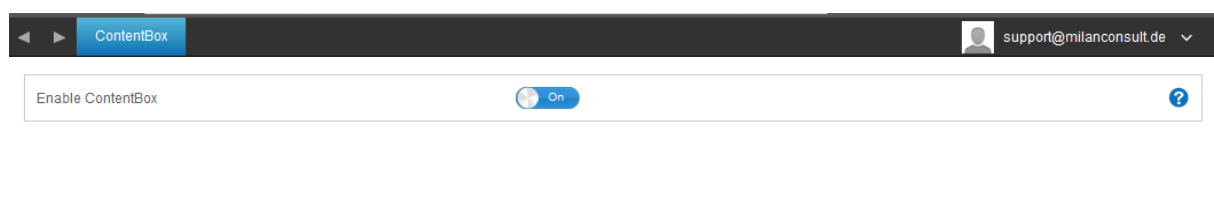
Set custom Wallpaper	Enable/Disable the custom wallpaper
Wallpaper	Set the wallpaper mode to use a color code or an image
Background Color	Specify a background color as hex value, e.g. #000000 for black or #ffffff as white
Wallpaper	Upload the image file you want to use as wallpaper



## Content Management

### Content Management

Under this point, 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.





## Configuration Windows Phone

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

#### Profile Information (only on profile level)

Should you be in a profile, you will receive a quick overview of the profile in relation to Name, OS, Creation Date, Author, etc.

Profile Name	Profile name– can be renamed here directly
Operating System	Profile's Operating System
Created At	Created on
Created By	Profile's creator
Last Change	Date and time, when changes were made on the profile
Changed By	Displays, who made the last changes
Profile Revision	Number of profile revisions

#### Device Overview (only on device level)

The device's summarized overview, which contains the following:


Device Name	Device name
Phone Number	Device phone number
OS Version	Device OS version
Operating System	Operating System (Android / iOS / Windows Phone)
Device Ownership	Corporate or private device
Device Type	Telephone or Tablet
Rooted	Status of whether the device has been rooted
Compliant	Compliant with guidelines
Last Seen	Point in time at which the device last connected to AppTec




### 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 revert the used apps to the group profile's settings.

### Device Log (only on device level)

Here you will receive various device logs.

In the case of an error, you can directly find out about the cause here.



## Asset Management (only on device level)

### Asset Management (only on device level)

#### Device Info

Manufacturer	Device manufacturer
Model	Device model
Operating System	Operating system
OS Version	OS version
Free / Total Memory	Free / Total memory
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)

#### Wi-Fi

WiFi MAC	WiFi MAC address
----------	------------------

#### Cellular

SIM Carrier Network	Carrier network
IMSI	<p>The International Mobile Subscriber Identity (IMSI) serves as a definite network user identification in GSM- und UMTS-mobile networks</p> <p>The IMSI is composed of a maximum of 15 digits and assembled in the following manner: <a href="#">[1]</a></p> <ul style="list-style-type: none"> <li>• (MCC), 3 digits</li> <li>• (MNC), 2 or 3 digits</li> </ul> <p>Mobile Subscriber Identification Number (MSIN), 1-10 digits</p>
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 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

### Security Configuration

#### Passcode

Allow Simple Passwords	Allow simple passwords, such as 1234 or 1111
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	
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.
Allow Password Grace Period Timer	If active, the user can set the time until the password must be reentered. If not, then the password will be requested.




## 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 Device** 

Are you sure to wipe the device ?

No

Yes

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

Allow SD Card	Allow the use of a SD card
Allow Camera	Allow the use of the camera
Enable Storage Encryption	Encrypts the internal data on the end user device, once this function has been activated, it is not possible to reverse this action SD cards will not be encrypted!
Allow USB Connection	Allow USB connection
Allow Voice Recording	Allow voice recording
Allow Location Service	Allow device location service
Allow Screen Capture	Allow screenshots
Allow Developer Unlock	Allows developer mode
Allow AntiTheft Mode	Allows the user to utilize the "Find My Device" service. Should this function have been used prior to deactivation, then it must be manually deactivated on the end user device
Allow Cellular Data Roaming	Allow cellular data roaming
Allow Cortana	Allow voice assistant Cortana
Allow Appstore	Allow the official Appstore
Cellular App Download Limit	Maximum cellular app download limit, via the mobile network
Allow Browser	Allow native browser
Allow Task Switcher	Allow Task-Managers
Allow Search to use Location	Allow search to use location
Allow Moderate Search Filter	Should this function be activated, adult content will not be filtered and blocked
Allow Storing Images From Vision Search	With this setting you can prevent that QR codes are stored as pictures on the end user device. Excluding, the currently scanned code that is on the device.
Allow Save As Office Files	Allows the user to save a file as an Office-File This policy only applies to the Office Hub
Allow Sharing Of Office Files	Allows the user to share Office files This policy only applies to the Office Hub
Allow Action Center Notifications	Allows the display of notifications in the Action Center during device lock
Allow Sync My Settings	Allows the synchronizing of settings across the entire device
Enable Email Data Encryption	Enables email data encryption and their attachments The device password is required to encrypt these files



Allow User Reset	<p>Allows the user to reset the device in settings or with the hardware buttons</p> <p><b>WARNING!</b></p> <p>This setting should only be deactivated, if this involves a corporate device. If for any reason, the device should not be able to establish a connection to the AppTec Server anymore, then the device must be sent to a Nokia Store, in order to restore the device to its factory settings</p> <p>Microsoft can therefore not be held liable for such a problem</p>
Allow User Unenrollment	<p>Allows the user to remove the corporate part from the device and thereby disconnect from the AppTec Servers. Should this happen, it will no longer be possible to manage the device</p> <p><b>WARNING!</b></p> <p>This setting should only be deactivated, if this involves a corporate device. If for any reason, the device should not be able to establish a connection to the AppTec Server anymore, then the device must be sent to a Nokia Store, in order to restore the device to its factory settings</p> <p>Microsoft can therefore not be held liable for such a problem</p>



## 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
<b>WEP Open System</b>	
Password	Password for the AP
<b>WPA PSK</b>	
Password	Password for the AP
<b>WPA EAP</b>	
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
Anonymous User Name	The client only sends its identity, once the RADIUS Server has been authenticated Until then, they will use the identity that is listed here
Logon Domain	Logon Domain
User Name	User name
Password	Password
Server Names	Offers the option to display the name of the RADIUS-Server, that offers the network authentication and authorization
<b>WPA2-PSK</b>	
Password	AP password



<b>WPA2 EAP</b>	
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)
Anonymous User Name	
Logon Domain	
User Name	User name
Password	Password
Server Names	Listing of the servers that should be trusted by the devices
<b>None</b>	No established security
Use Proxy Server	Use of a proxy server
Server Address	Proxy server address
Server Port	Proxy Server's Server Port

### 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 WiFi Hot Spot Reporting	Allow that WiFi Hotspot information can be sent to Microsoft
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
Server	Server address of the VPN Server
VPN Type	Connection type
<b>IKEv2 (native)</b>	A native VPN connection will be used
<b>SSL-VPN (third-party)</b>	A 3 <sup>rd</sup> party app will be used
Third-Party App	
	JunOS Pulse
	SonicWall Mobile Connect
	F5 Big-IP Edge Client
	Checkpoint Mobile VPN
Third-Party Configuration File	Here the content must be entered into the configuration file
Authentication Type	Authentication type
Bypass Local Traffic	When accessing internal resources, traffic will not be routed via the VPN connection
Connection Type	Manual = The user must manually establish/terminate a VPN connection Triggering = The VPN connection will be established automatically, as soon as an app wants to connect to a protected or internal resource. This is AppTec's recommended setting, in order to optimize the best possible performance
Trusted Network Detection	If this function is active, no VPN connection will be established, as long as the user is in a corporate WiFi, due to the fact that the protected resources are directly accessible on the end user device. Should this function be deactivated, a VPN connection will be established via the corporate network A DNS Suffix must be established, in order to define which WIFI is a corporate WiFi
DNS Suffix	Here you can enter the primary DNS Suffix
Use Proxy	Use of a Proxy
Server Address	Server address of the proxy server
Server Port	Server port of the proxy server
Bypass Local Traffic	In the case of internet queries into the local intranet, traffic will not be routed via the Proxy.

### VPN Restrictions

Here you can define various VPN restrictions.



Allow Manual VPN Configuration	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
-----------------	-------------------------------

### NFC

Here you can establish, if NFC should be allowed/forbidden.

Allow NFC	Activate/deactivate NFC
-----------	-------------------------



## 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 (only on device level)

Here all In-House Apps are displayed for you.

Via the  symbol, you can directly assign a new In-House App (.xap file) to the end user device.

#### Mandatory Apps

Here all “Mandatory Apps” are displayed, meaning the mandated required apps on the end user device.


Via the  symbol, you can establish additional In-House App.

#### Whitelisted / Blacklisted Apps

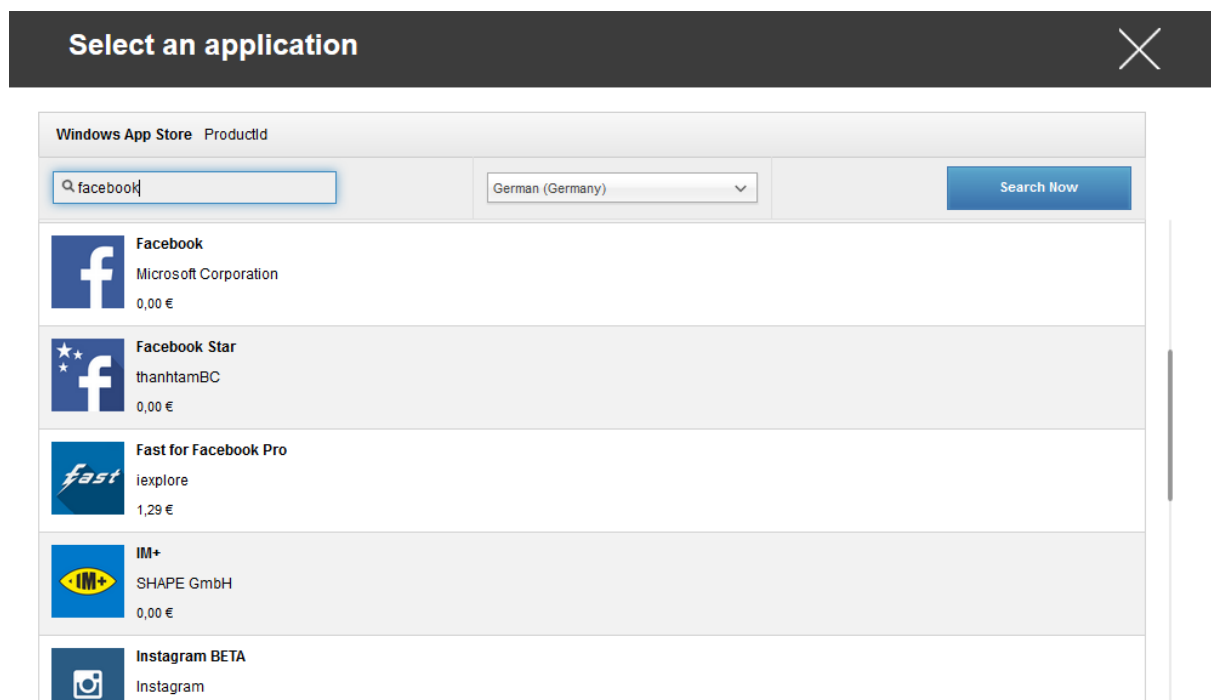
Depending on whether you have selected under “General Settings”> „Black- & Whitelisting“> „Windows“> “Blacklisting” or “Whitelisting”, here you can define blacklisted or whitelisted apps.

Blacklisted apps, means that these apps cannot be installed or run on the end user device. All apps that are not defined here, can be installed and run.

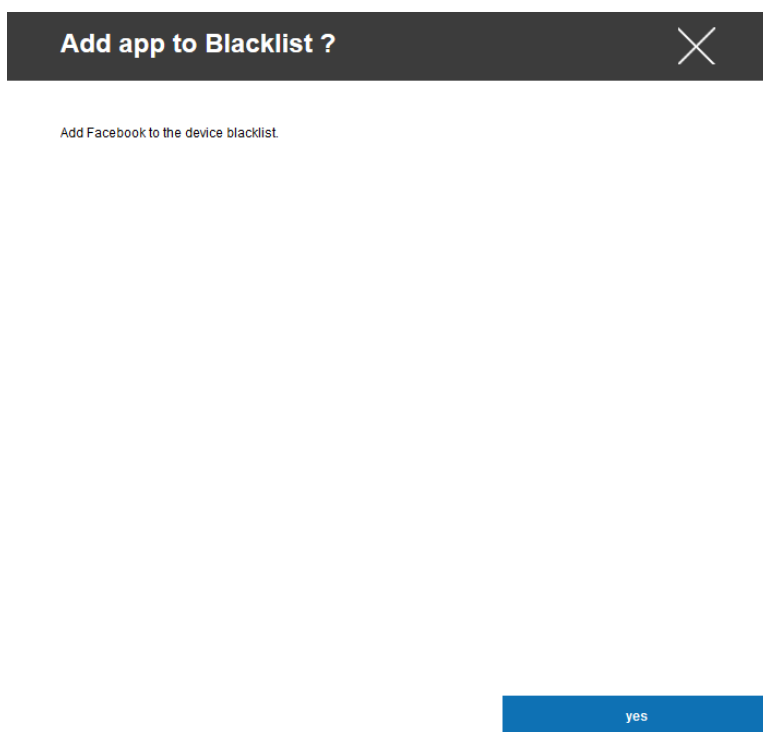
Whitelisted apps, means that only these predefined apps can be installed and/or run.

Likewise, via the  symbol, additional Windows Apps or Product IDs can be established. Simply search for an app. In our example, it would be Facebook. Then click on the App-Icon or on the name of the respective app.



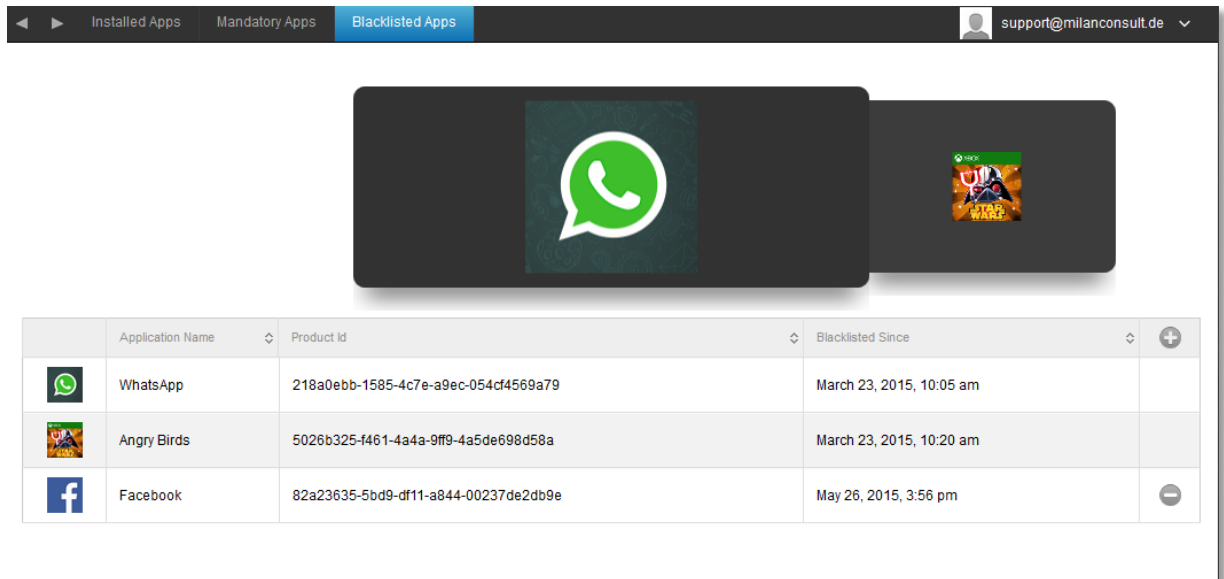






After that, the following window will open, confirm this with “yes”.





Should the App-Import have been successful, you can find the app, that you just defined, in the overview.



	Application Name	Product Id	Blacklisted Since	
	WhatsApp	218a0ebb-1585-4c7e-a9ec-054cf4569a79	March 23, 2015, 10:05 am	
	Angry Birds	5026b325-f461-4a4a-9ff9-4a5de698d58a	March 23, 2015, 10:20 am	
	Facebook	82a23635-5bd9-df11-a844-00237de2db9e	May 26, 2015, 3:56 pm	


In our example, where we are working with “Blacklisted Apps”, it would not be possible to install and/or run “WhatsApp”, “Angry Birds” and “Facebook”, if one these apps had already been installed on the end user device, prior to this regulation.

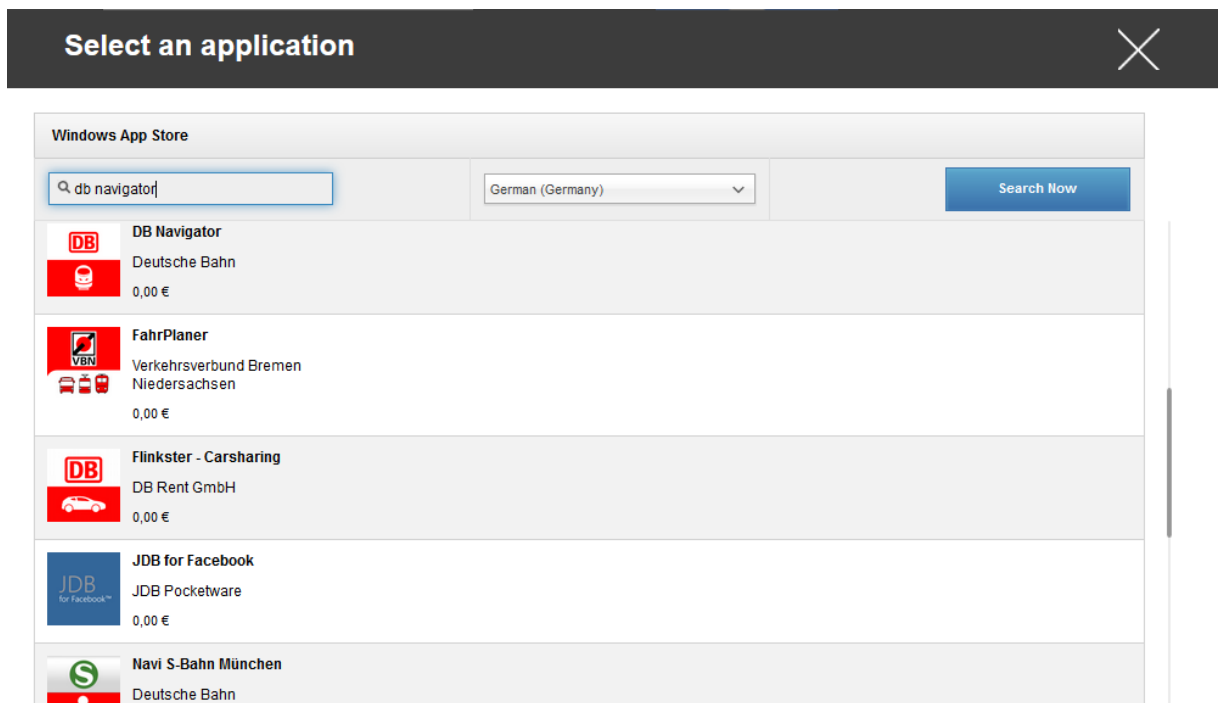


## Enterprise App Store

### Windows store

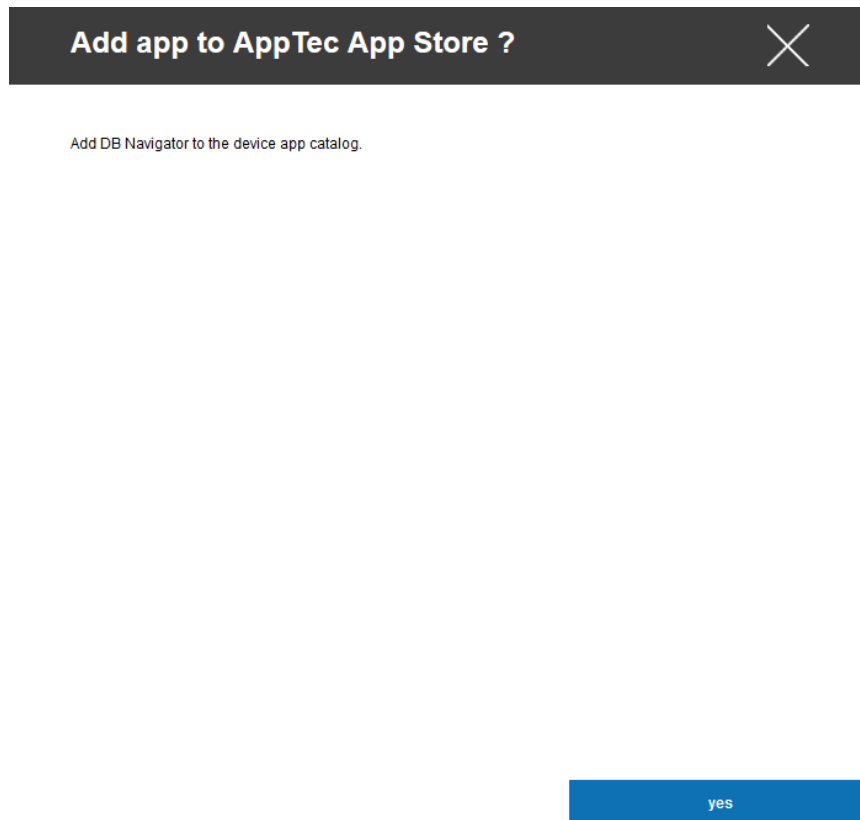
Here you have the option to distribute Windows Apps to the user. This pertains to public Windows Apps and they can optionally be installed by the user via the AppTec Enterprise AppStore.

Via the  symbol, additional Windows Apps can be added.  
With “Enter Search term here ...”, you can search for an app in the Windows Store. Our example shows the “DB Navigator”App.

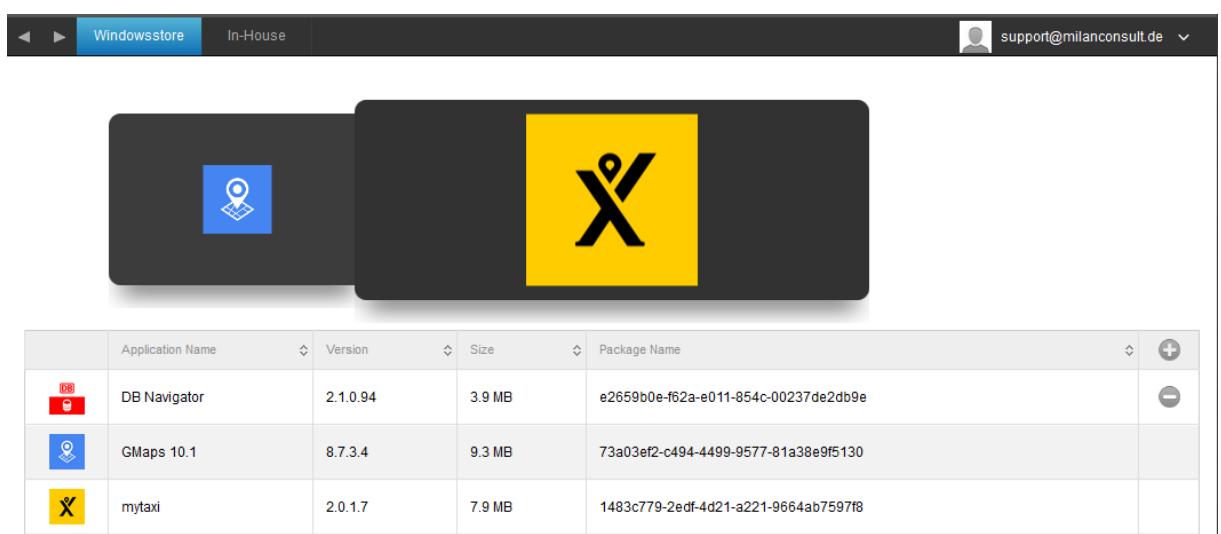




Then the following window will open, confirm this with “yes”.



Should the App-Import have been successful, you can find the previously defined App in the overview.



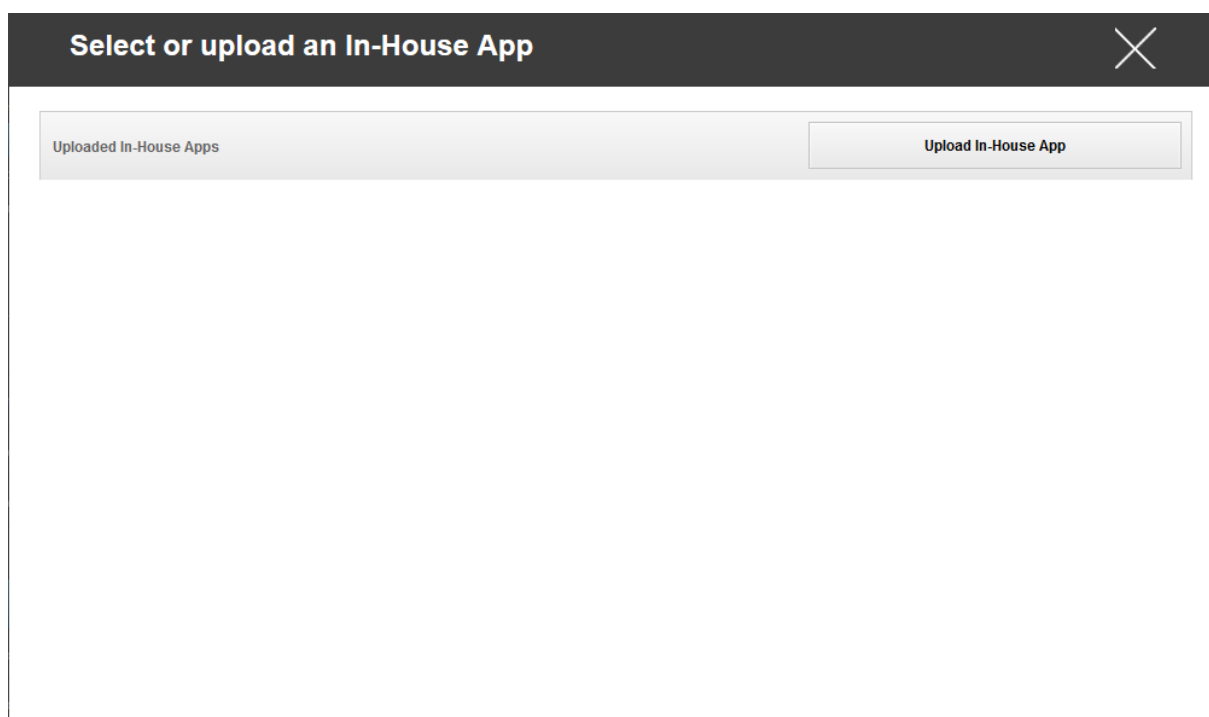


## In-House

Here you have the option to distribute In-House Apps to the users. Here, this involves internally developed Windows Apps and they can be optionally installed by the user via the AppTec Enterprise AppStore.

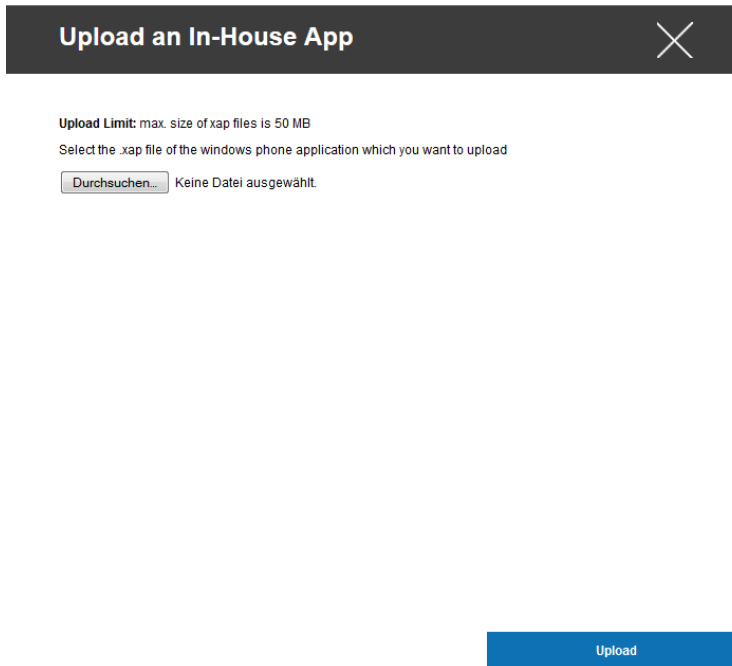
Via the  symbol, additional In-House Windows Apps can be added.

In the window that then opens, click on “Upload In-House App”.





Now, click on “Search...” and select the .xap file.



**Upload an In-House App**

Upload Limit: max. size of .xap files is 50 MB

Select the .xap file of the windows phone application which you want to upload

Keine Datei ausgewählt.

Upload

After you have selected the xap file, you can import the app with “Upload” into your AppTec Enterprise AppStore.

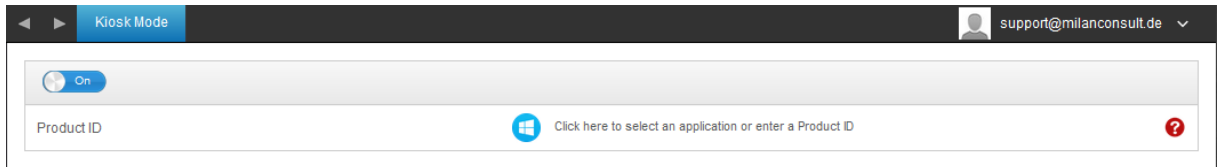
Should the upload have been performed successfully, you can now see the app in the overview.



## Kiosk Mode

### Kiosk Mode

Under the “Kiosk Mode” you can expand the app into full screen mode, after which, it is only possible to use this app.

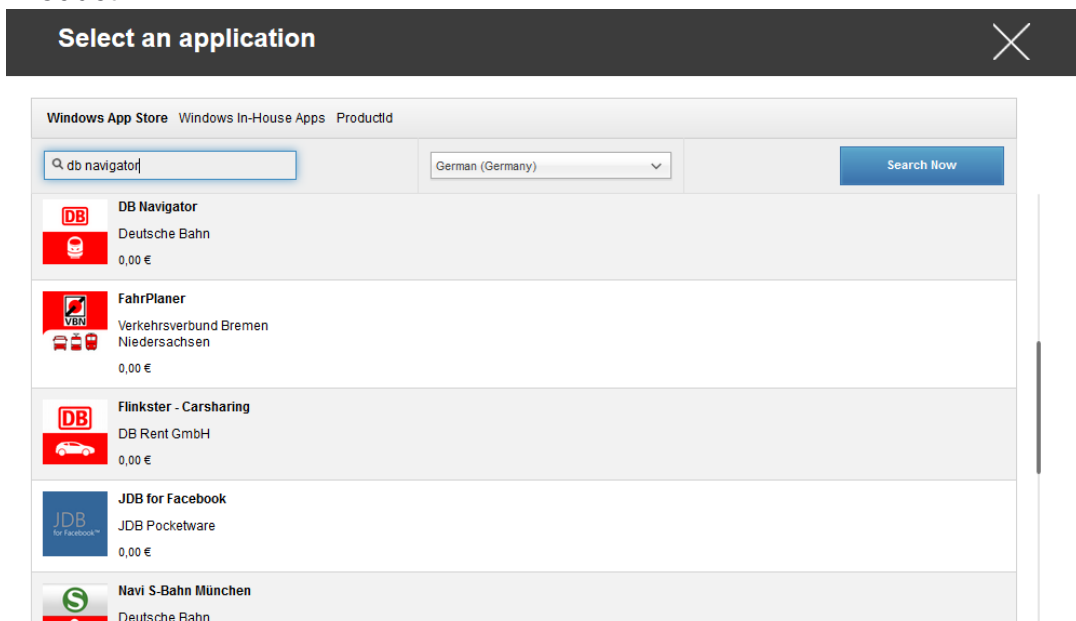


### WARNING!

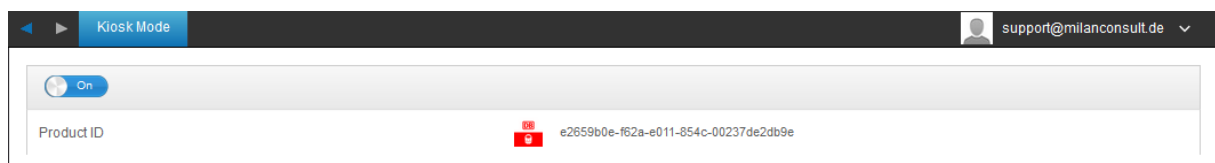
The Kiosk Mode under Windows Phone can only then be deactivated, by restoring the device back to the factory settings.

The App / Product ID that is defined here, will be automatically displayed in full screen mode, after each device restart.

With “Click here to select an application or enter a Product ID”, you can define a public / In-House Windows App or you also have the option to establish a Product ID.



Don't forget to also establish the Kiosk Mode App under “Mandatory App”.





## Configuration Windows 10 PC

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

#### Profile Information (only on profile level)

Should you be in a profile, you will receive a quick overview of the profile in relation to Name, OS, Creation Date, Author, etc.

Profile Name	Profile name– can be renamed here directly
Operating System	Profile's Operating System
Created At	Created on
Created By	Profile's creator
Last Change	Date and time, when changes were made on the profile
Changed By	Displays, who made the last changes
Profile Revision	Number of profile revisions

#### Device Overview (only on device level)

The device's summarized overview, which contains the following:

Device Name	Device name
PC Name	Name of the PC
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




## Settings


Allow Auto Update	Allow or disallow automatic 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 revert the used apps to the group profile's settings.

## Device Log (only on device level)

Here you will receive various device logs.

In the case of an error, you can directly find out about the cause here.



## 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
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 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

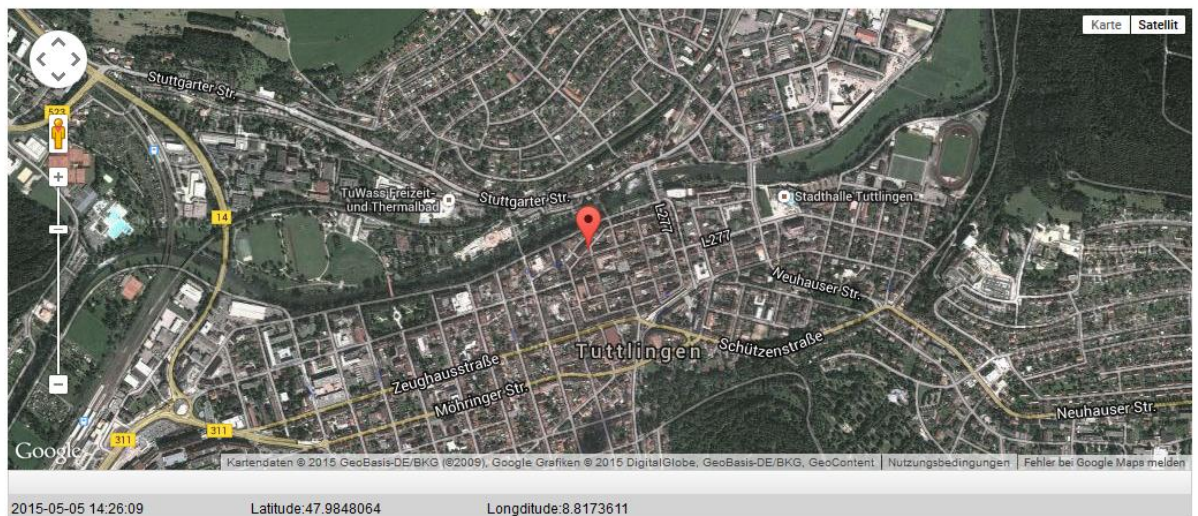


## Security Management

### 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
Allow Password Grace Period Timer	If active, the user can set the time until the password must be reentered. If not, then the password will be requested.



## 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 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 separated by ";".
Allow User Reset	<p>Allows the user to reset the device in settings or with the hardware buttons</p> <p><b>WARNING!</b></p> <p>This setting should only be deactivated, if this involves a corporate device.</p> <p>If for any reason, the device should not be able to establish a connection to the AppTec Server anymore, then the device must be sent to a Nokia Store, in order to restore the device to its factory settings</p> <p>Microsoft can therefore not be held liable for such a problem</p>
Allow User Unenrollment	<p>Allows the user to remove the corporate part from the device and thereby disconnect from the AppTec Servers. Should this happen, it will no longer be possible to manage the device</p> <p><b>WARNING!</b></p> <p>This setting should only be deactivated, if this involves a corporate device.</p> <p>If for any reason, the device should not be able to establish a connection to the AppTec Server anymore, then the device must be sent to a Nokia Store, in order to restore the device to its factory settings</p> <p>Microsoft can therefore not be held liable for such a problem</p>



## 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
<b>WEP Open System</b>	
Password	Password for the AP
<b>WPA PSK</b>	
Password	Password for the AP
<b>WPA EAP</b>	
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
Anonymous User Name	The client only sends its identity, once the RADIUS Server has been authenticated Until then, they will use the identity that is listed here
Logon Domain	Logon Domain
User Name	User name
Password	Password
Server Names	Offers the option to display the name of the RADIUS-Server, that offers the network authentication and authorization
<b>WPA2-PSK</b>	
Password	AP password



<b>WPA2 EAP</b>	
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)
Anonymous User Name	
Logon Domain	
User Name	User name
Password	Password
Server Names	Listing of the servers that should be trusted by the devices
<b>None</b>	No established security
Use Proxy Server	Use of a proxy server
Server Address	Proxy server address
Server Port	Proxy Server's Server Port

### 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
Server	Server address of the VPN Server
VPN Type	Connection type
<b>IKEv2 (native)</b>	A native VPN connection will be used
Authentication Type	Authentication type
Trusted Network Detection	<p>If this function is active, no VPN connection will be established, as long as the user is in a corporate WiFi, due to the fact that the protected resources are directly accessible on the end user device. Should this function be deactivated, a VPN connection will be established via the corporate network</p> <p>A DNS Suffix must be established, in order to define which WIFI is a corporate WiFi</p>
DNS Suffix	Here you can enter the primary DNS Suffix
Use Proxy	Use of a Proxy
Server Address	Server address of the proxy server
Server Port	Server port of the proxy server
URL to automatically retrieve the proxy settings	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



## Configuration MacOS

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

#### Profile Information (only on profile level)

Should you be in a profile, you will receive a quick overview of the profile in relation to Name, OS, Creation Date, Author, etc.

Profile Name	Profile name– can be renamed here directly
Operating System	Profile's Operating System
Created At	Created on
Created By	Profile's creator
Last Change	Date and time, when changes were made on the profile
Changed By	Displays, who made the last changes
Profile Revision	Number of profile revisions

#### Device Overview (only on device level)

The device's summarized overview, which contains the following:


Device Name	Device name
Model	Model
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
Compliant	Shows if device is compliant
Last Seen	Date and time, when changes were made on the profile




### 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 revert the used apps to the group profile's settings.

### Device Log (only on device level)

Here you will receive various device logs.

In the case of an error, you can directly find out about the cause here.



## Asset Management (only on device level)

### Device Info

Model Number	Model Number
Product Name	Product Name
Hostname	Hostname
Local Hostname	Local Hostname
Operating System	Operating system
OS Version	OS version
Serial Number	Serial Number
UDID	UDID
Free / Total Memory	Free / Total Memory

### User Info

UserID	UserID
Username	Username

### 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
---------------	---------------



## Security Management

### Security Configuration

#### Passcode

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 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 Calender	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 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 DVD-RAM	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 DVD	Allow access for DVD disk.
Require Authentication	Require Authentication for the use of this media
Allow CD	Allow access for CD disk.
Require Authentication	Require Authentication for the use of this media



## 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
Proxy Setup	Configuring of a Proxy for every Access Point
<b>None</b>	Establish no Proxy
<b>Manual</b>	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
<b>Automatic</b>	Establish a Proxy automatically
Proxy Server URL	URL for access to the Proxy settings
Security Type	Establish Security Type for the AP
<b>WEP</b>	
Password	Password for the AP
<b>WPA/WPA2</b>	
Password	Password for the AP
<b>WEP Enterprise – WPA / WPA2 Enterprise – Any Enterprise</b>	
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	Anonymous Provision of PAC
Anonymously	
Inner Authentications	Authentication protocol 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	
1	Trusted Certificate	Upload first trusted certificate
2	Trusted Certificate	Upload second trusted certificate
3	Trusted Certificate	Upload third trusted certificate
	Trusted Server Certificate Names	The names of the expected server certificates (in a comma separated list)
	<b>None</b>	Establish no security

### VPN

Connection Name	Name of the VPN-Profile
VPN Type	
<b>VPN</b>	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
Proxy Setup	Configuring of a Proxy for the VPN-connection
<b>None</b>	Establish no Proxy
<b>Manual</b>	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
<b>Automatic</b>	Establish a Proxy automatically
Proxy Server URL	URL for access to the Proxy settings



### HTTP Proxy

Proxy Type	
<b>Manual</b>	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
<b>Automatic</b>	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 AppTec 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



<b>Incoming Mail</b>	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

<b>Outgoing Mail</b>	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

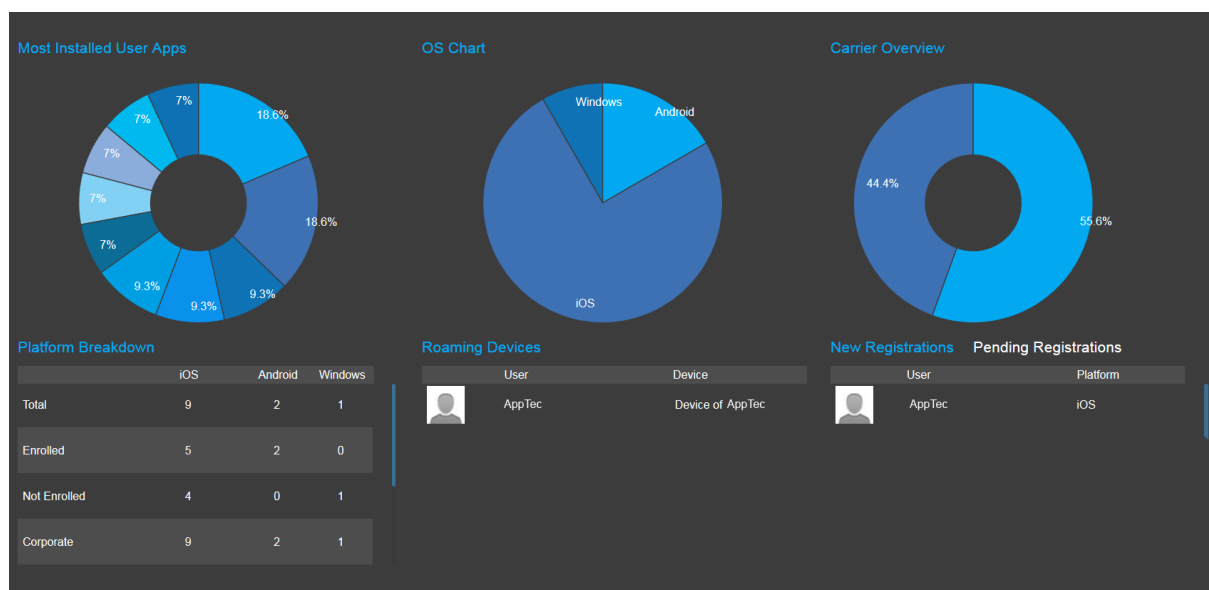


## V. Dashboard & Reporting

### Dashboard

The “Dashboard” displays all of the fundamental information in one glance:

- Most installed apps
- Current end user device status of the end user devices
- Overview of the current platforms
- Devices that have activated roaming
- Utilized network providers
- New registrations / outstanding registrations








## Extended Reporting

The “Extended Reporting” offers detailed views, graphics and overviews that are filled with information.

Usually, you will find the following tabs in the sub-points:

- All (all device)
- iOS (only iOS devices)
- Android (only Android devices)
- if applicable, Windows (only Windows Phone devices)
- In the case of an exception, this will be mentioned explicitly under the sub-point

Under the respective sub-point, you can use  (Export Data) in order to export the current overview as a .csv file.

Should the sub-point contain a graphic, you can hide the graphic with  (Hide Chart) and/or with  (Show Chart) display the graphic (again).

By default, the following points can be found:

Device Alias	Device name
Device Owner	Device owner
eMail	Device eMail
Phone	Telephone number
OS	OS
Last Seen	Last communication with the AppTec Server



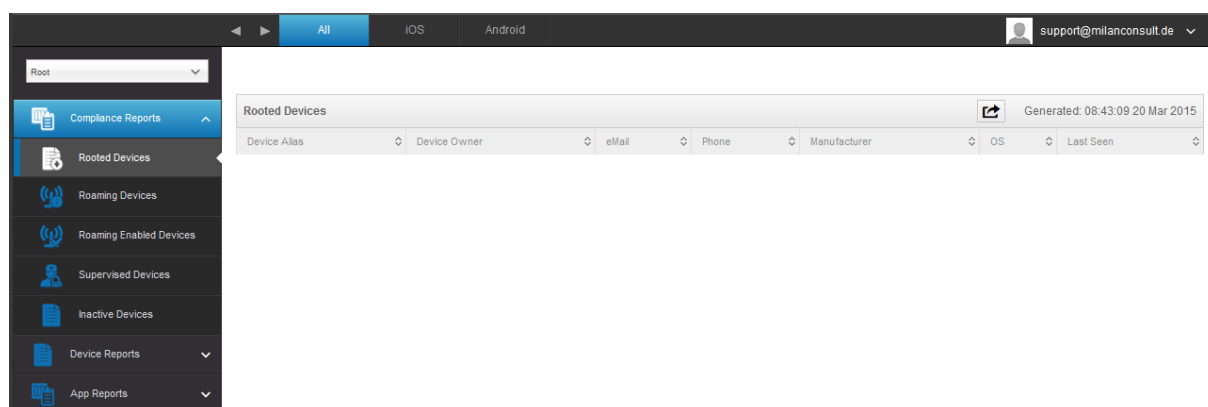
## Compliance Reports

### Rooted Devices

Overview of the devices that have been rooted/ jailbroken.

Additional point in this category:

Manufacturer	Manufacturer
--------------	--------------

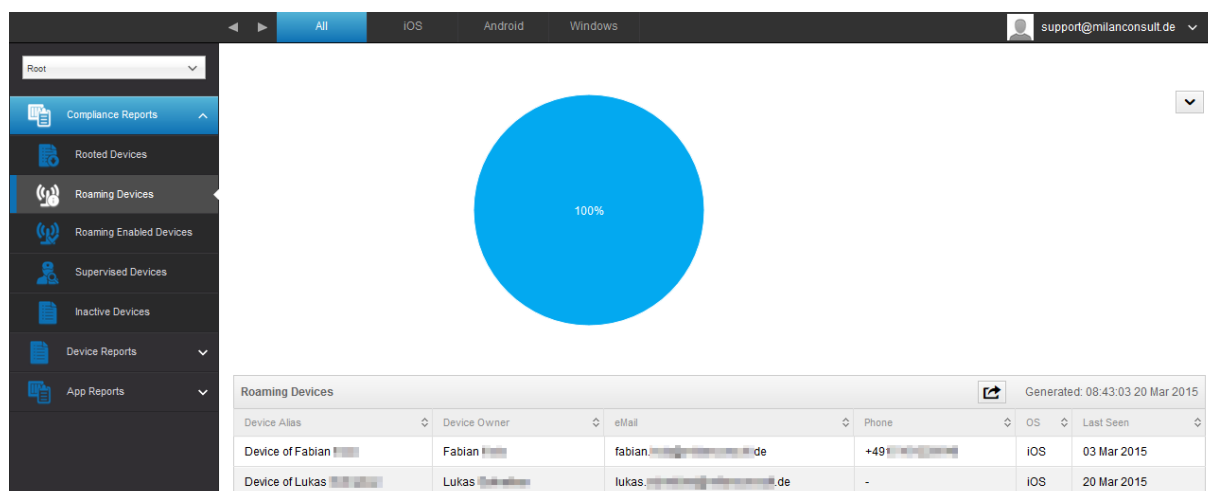


### Roaming Devices

Overview of all of the devices that are roaming.

Additional point in this category:

Phone	Telephone number
-------	------------------



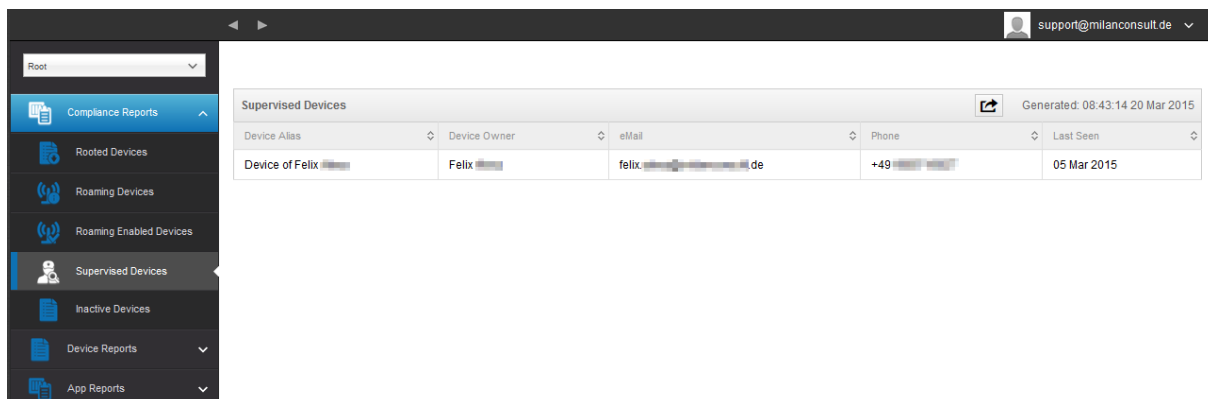


## Roaming Enabled Devices

Overview of all of the devices that have activated roaming.

## Supervised Devices

All the devices that are supervised (excluding iOS devices)



Device Alias	Device Owner	eMail	Phone	Last Seen
Device of Felix	Felix	felix@...de	+49...	05 Mar 2015

## Inactive Devices

List of all inactive Devices.



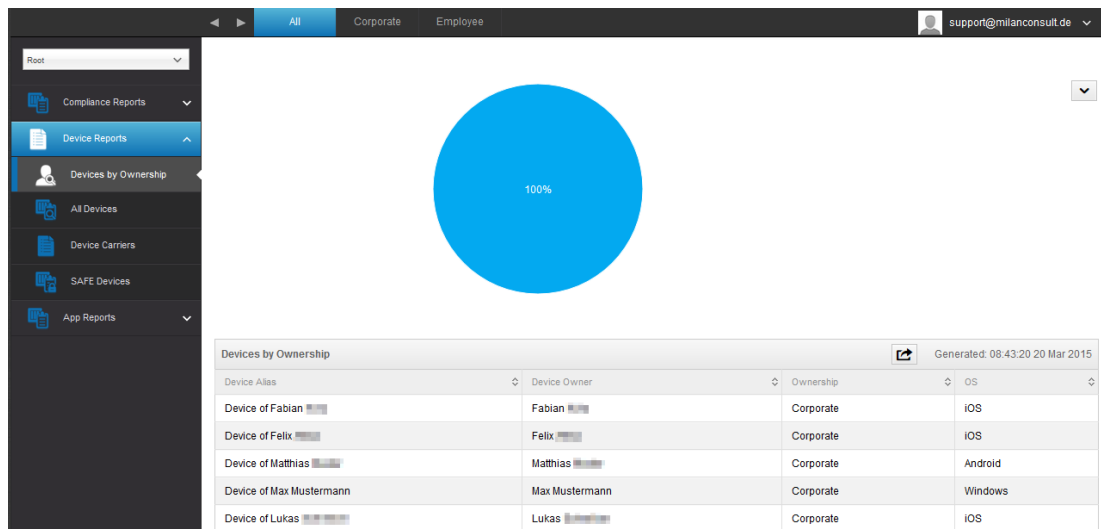
## Device Reports

### Devices by Ownership

Here you can see how many devices have currently been deployed as corporate (corporate devices) and employee (private devices) devices.

Additional point:

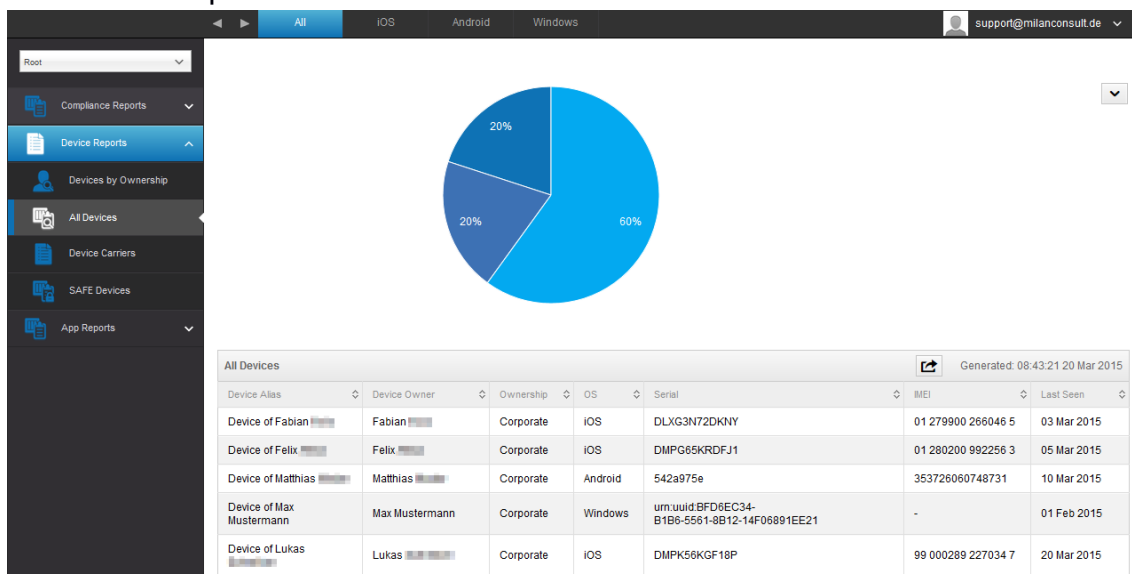
Ownership	Corporate = corporate device Employee = private device
-----------	---



### All Devices

Here you will find an overview of all devices, with the most important information.

Additional points:





Ownership	Corporate = corporate device Employee = private device
Serial	Device serial number
IMEI	Device IMEI number

## D Device Carriers

Carrier	Cellular provider ex. T Mobile, Verizon
---------	--

Here you receive an overview regarding the carrier (cellular provider).

Additional points:

### SAFE Devices

Here you gain 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.

Additional points in this category:

Phone	Telephone number
SAFE Version	SAFE Version



## App Reports

Here you will receive a variety of overviews in regards to apps.

### Installed Apps

Here you will receive an overview of all installed apps.

You can sort them according to the following categories:

- All Apps (all apps will be considered)
- System Apps (only apps from the device manufacturer will be displayed)
- User Apps (only manually installed apps will be displayed, official AppStore and AppTec Enterprise Store)

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

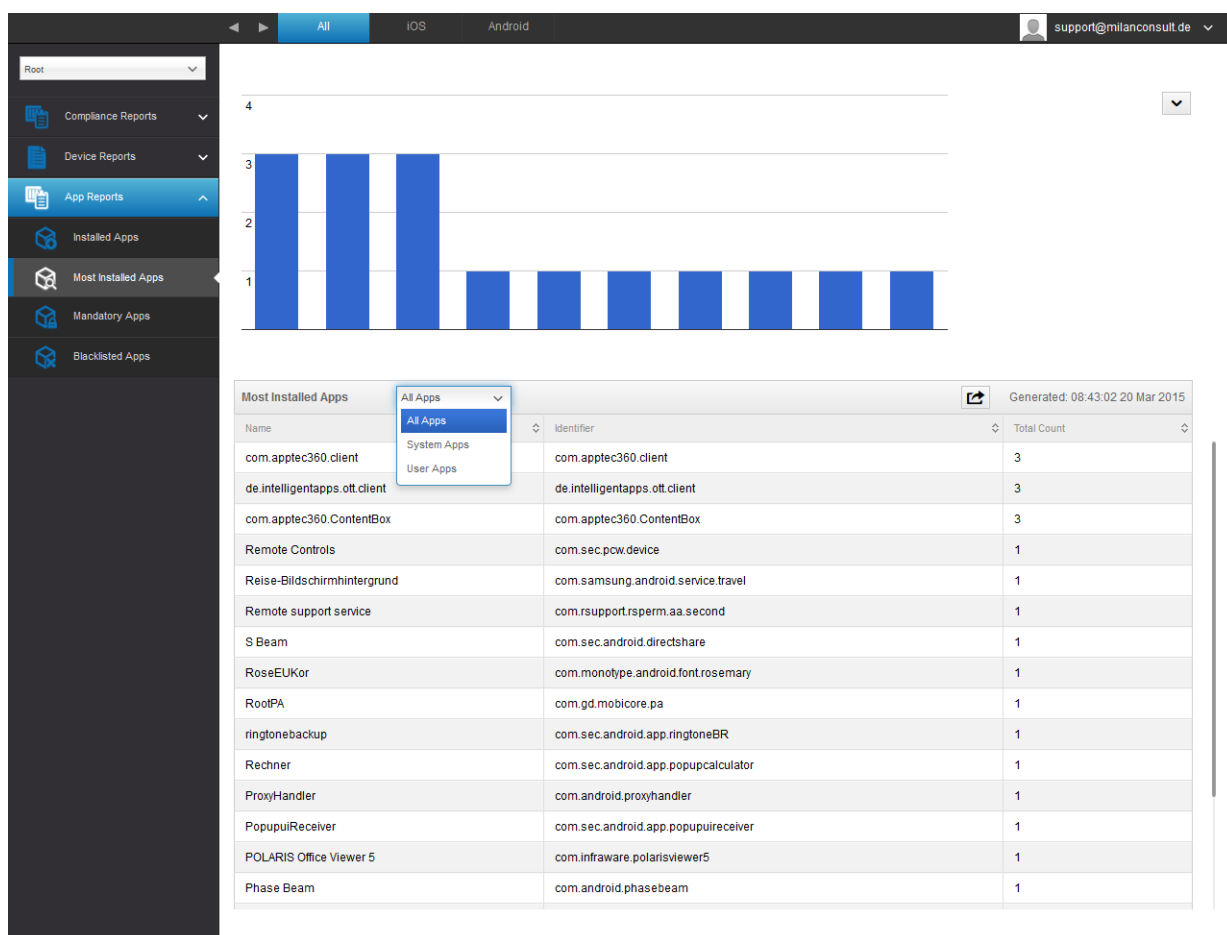
Here you will receive an overview of the apps that have been installed the most.

You can sort them according to the following categories:

- All Apps (all apps will be considered)
- System Apps (only apps from the device manufacturer will be displayed)
- User Apps (only manually installed apps will be displayed, official AppStore and AppTec Enterprise Store)

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 will gain an overview of mandatory (mandated required) apps.

You can sort them according to the following categories:

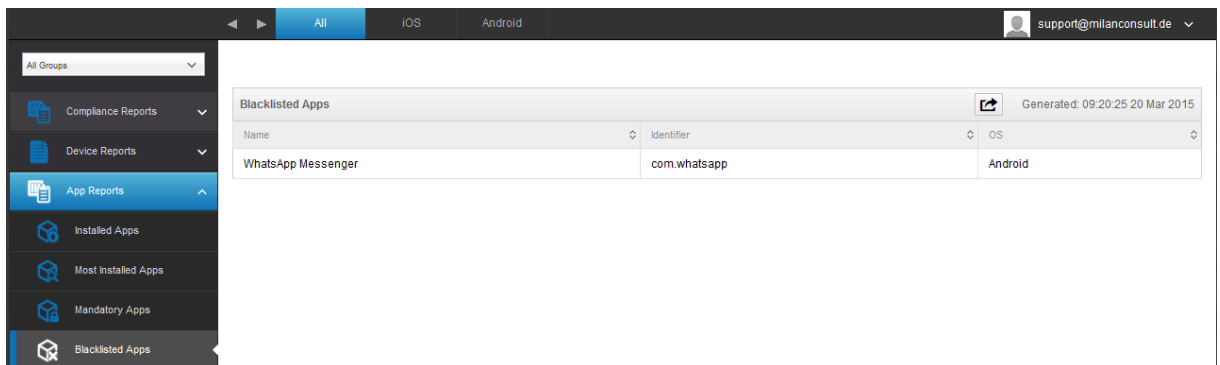
- All Apps (all apps will be considered)
- System Apps (only apps from the device manufacturer will be displayed)
- User Apps (only manually installed apps will be displayed, official AppStore and AppTec Enterprise Store)

Name	Name of the respective app and/or service
Identifier	Definite app/service ID
App Source	Which AppStore is involved: - Google PlayStore - iTunes AppStore (iOS) - Microsoft Store (Windows Phone)
Total Count	How often this app / service has been installed on the end user devices

## Blacklisted Apps

Here you will gain an overview of all defined blacklisted apps.

Name	Name of the respective app and/or service
Identifier	Definite app/service ID
OS	How often this app / service has been installed on the end user devices



The screenshot shows the AppTec360 web interface. On the left is a sidebar menu with options: All Groups, Compliance Reports, Device Reports, App Reports (selected), Installed Apps, Most Installed Apps, Mandatory Apps, and Blacklisted Apps. The main area displays the 'Blacklisted Apps' report. At the top of the report area, there are tabs for 'All', 'iOS', and 'Android', with 'All' currently selected. A user profile icon and email 'support@milanconsult.de' are visible in the top right. The report title 'Blacklisted Apps' is followed by a 'Generated: 09:20:25 20 Mar 2015' timestamp. Below the title is a table with columns: Name, Identifier, and OS. The table contains one entry: 'WhatsApp Messenger' with identifier 'com.whatsapp' and OS 'Android'.

Name	Identifier	OS
WhatsApp Messenger	com.whatsapp	Android



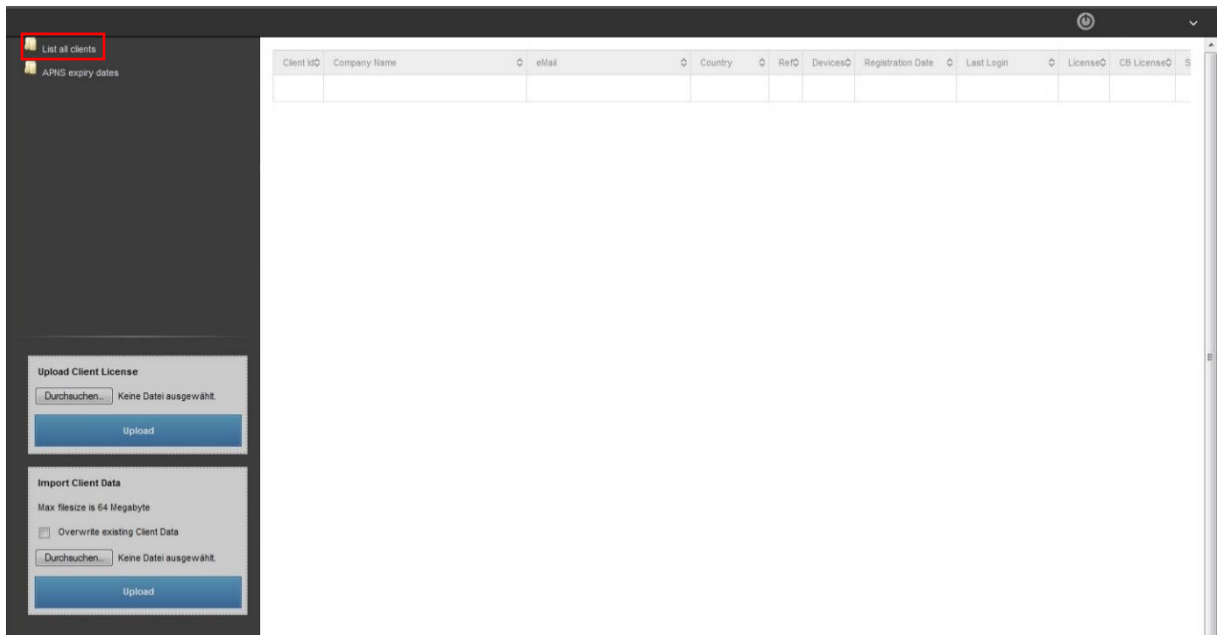
## VI. *Mandate Management*

In the Mandate-Portal, additional AppTec licenses can be uploaded, which will then act as a new AppTec-Instance (called “Client”). This means that multiple clients can be managed and made available, with one installation.

In order to access the respective display, log into the appliance with the “Server Admin Credentials”, which you established during the installation process (“STEP THREE” of the Appliance Config).

### Display

#### List all clients

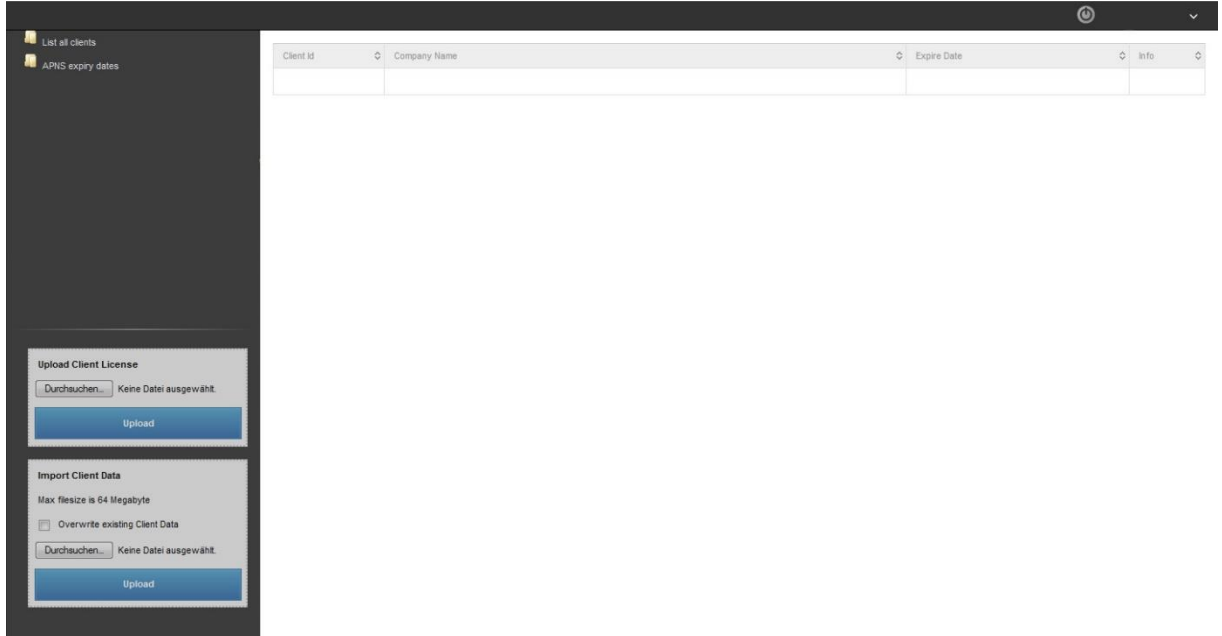


Client ID	Client ID
Company Name	Company name
eMail	Contact person eMail
Country	Country
Ref	Ref
Devices	Number of registered devices
Registration Date	Point in time of the license assignment
Last Login	Last admin account login
License	License type display (Free Paid)
CB License	ContentBox license type (Free Paid)
Status	Current AppTec-Client status
Expired	Displays, if the license has expired



Here you will see an overview of all the assigned AppTec-Clients.

### APNS expiry dates

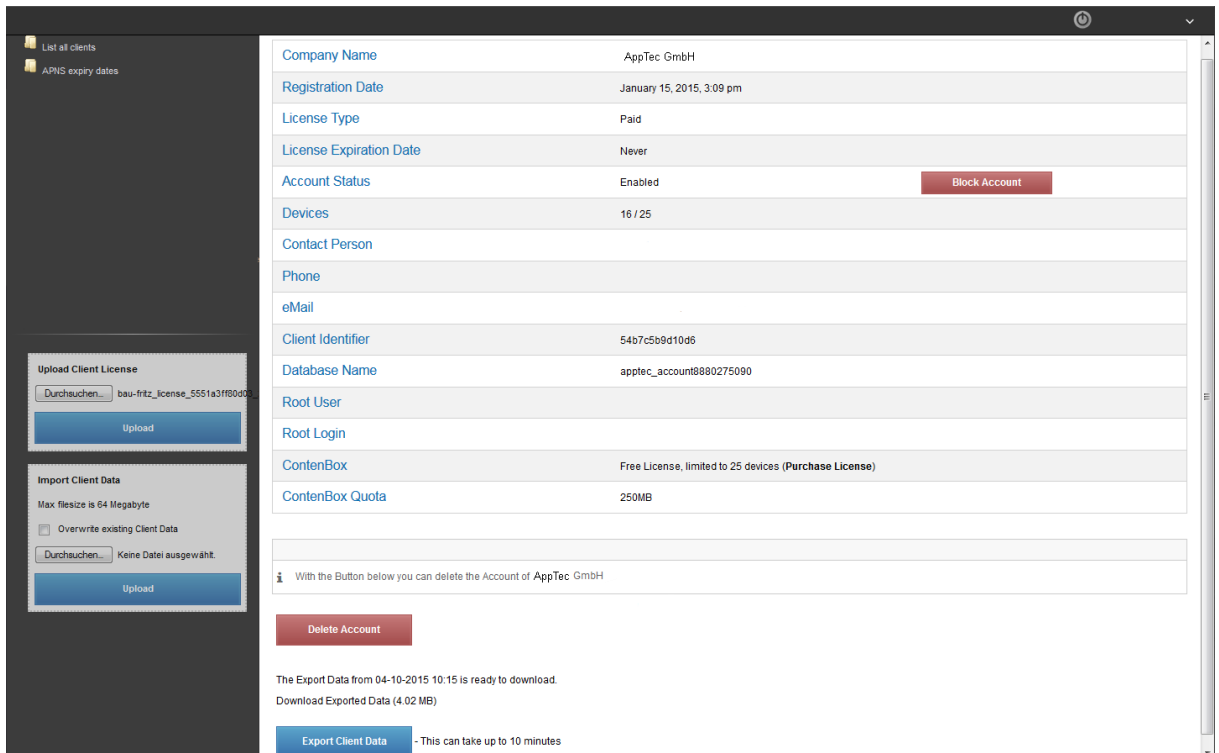


Client ID	Client ID
Company Name	Company Name
Expire Date	Expiration date for the Apple APNS-certificate
Info	Additional information

On this overview page, all of the APNS certificate expiration dates are noted.



## Account Information



Company Name: AppTec GmbH

Registration Date: January 15, 2015, 3:09 pm

License Type: Paid

License Expiration Date: Never

Account Status: Enabled [Block Account](#)

Devices: 16 / 25

Contact Person:

Phone:

eMail:

Client Identifier: 54b7c5b9d10d6

Database Name: apptec\_account8880275090

Root User:

Root Login:

ContentBox: Free License, limited to 25 devices (Purchase License)

ContentBox Quota: 250MB

[Delete Account](#)

The Export Data from 04-10-2015 10:15 is ready to download.  
 Download Exported Data (4.02 MB)

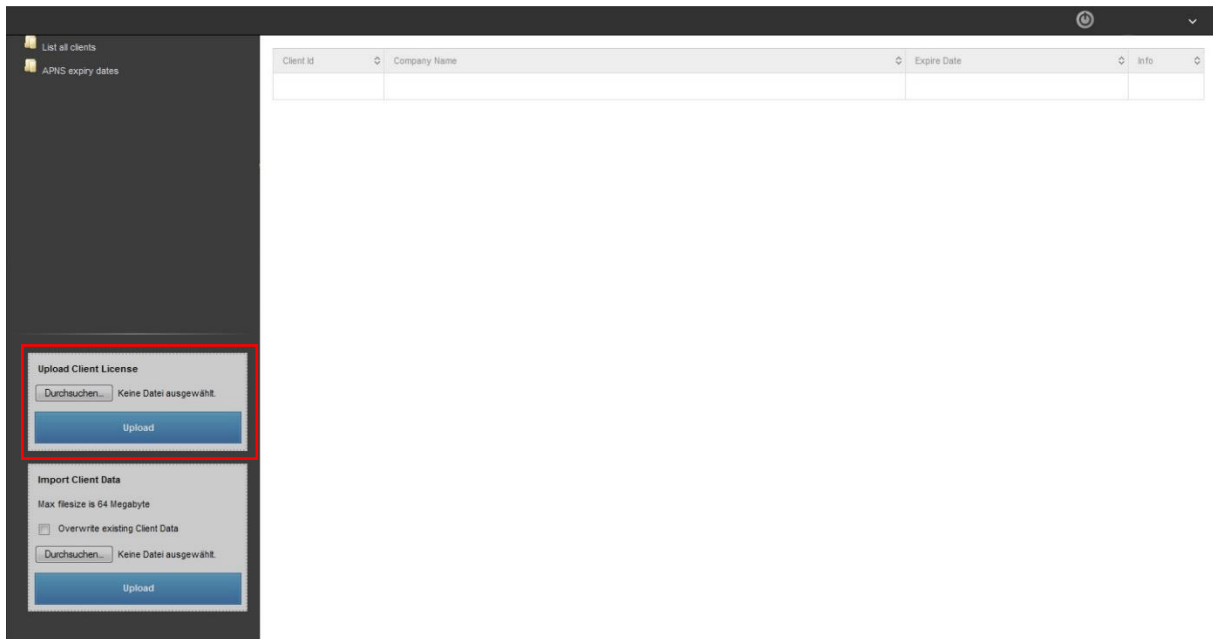
[Export Client Data](#) - This can take up to 10 minutes

Company Name	Company name
Registration Date	License registration date
License Type	License type display (Free Paid)
License Expiration Date	License expiration date
Account Status	Account status (Enabled Disabled)
Devices	Number of registered devices
Contact Person	Contact person
Phone	Contact person telephone number
eMail	Contact person eMail address
Client Identifier	AppTec-Client's client identifier
Database name	AppTec-Client's database name
Root User	Complete Root Users name
Root Login	Root User login name (email)
ContentBox	License information regarding the Content Box
ContentBox Quota	Available ContentBox-Memory

Block Account / Unblock Account	After a click on "Block Account", access to the AppTec-Client is no longer possible
Delete Account	Here you can delete the AppTec-Client



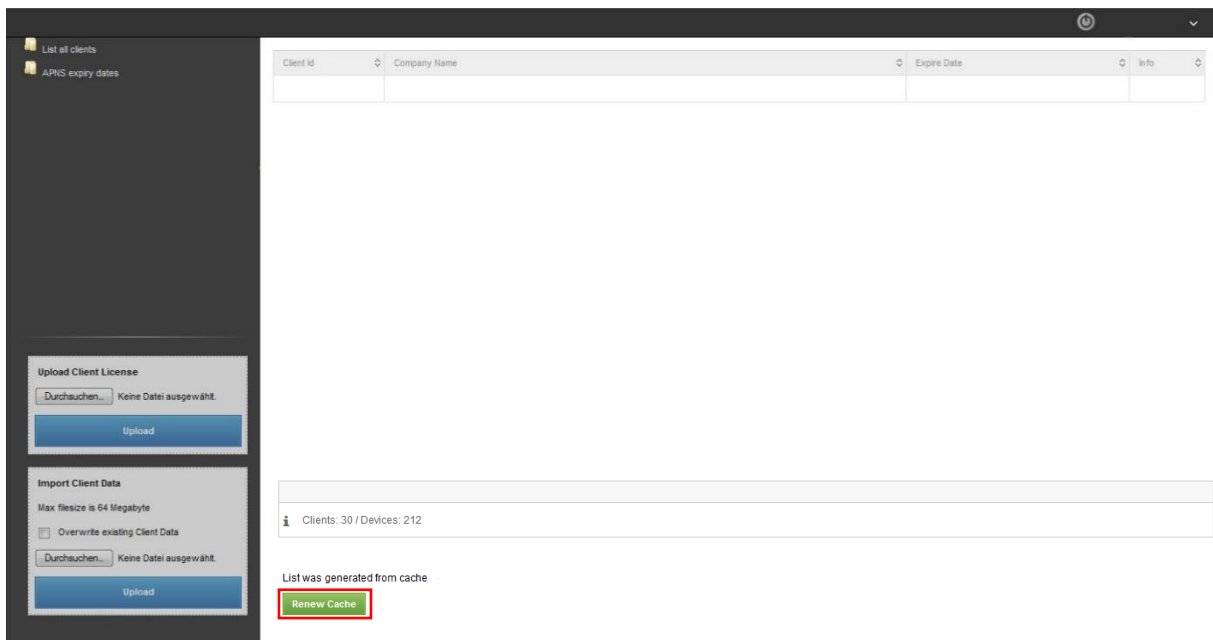
## Registration of an additional AppTec-License



The screenshot shows the AppTec360 interface. On the left sidebar, there are links for 'List all clients' and 'APNS expiry dates'. The main area contains a table with columns: Client id, Company Name, Expire Date, and Info. Below the table, there are two sections: 'Upload Client License' and 'Import Client Data'. The 'Upload Client License' section is highlighted with a red rectangle. It contains a 'Durchsuchen...' button, the text 'Keine Datei ausgewählt.', and an 'Upload' button. The 'Import Client Data' section contains a 'Max filesize is 64 Megabyte' label, a checkbox for 'Overwrite existing Client Data', another 'Durchsuchen...' button, the text 'Keine Datei ausgewählt.', and an 'Upload' button.

After you have received an additional AppTec-License, you can upload this on the Mandate-Portal.

For this, click on “Search“, select the respective license file and then click on “Upload“. The new AppTec-Client is hereby registered successfully.



The screenshot shows the AppTec360 interface after the license upload. The 'Upload Client License' and 'Import Client Data' sections are still visible on the left. In the main area, below the table, there is a summary bar showing 'Clients: 30 / Devices: 212'. Below this, a message states 'List was generated from cache'. At the bottom of this message, a 'Renew Cache' button is highlighted with a red rectangle.

After a click on “Renew Cache“, which actuates an update to the list, the newly registered Client will be displayed.



## CONTACT

Additional questions? Simply contact us under:

For general technical questions

[support@apptec360.com](mailto:support@apptec360.com)

+41 61 511 3210

For questions related to the installation of a virtual appliance

[consulting@apptec360.com](mailto:consulting@apptec360.com)

+41 61 511 3214

## DISCLAIMER

© AppTec GmbH

This documentation is copyright protected. All rights remain with the AppTec GmbH. Any other usage, especially a transfer to a third party, storing within the data system, distribution, editing, performance, display and broadcasting are forbidden. This not only applies to the entire document, but also to parts. Changes may be made at any time.

Other company-, brand name- and product names are trademarks or registered trademarks and that have not been explicitly named at this point, are protected by the trademark laws and belong to the respective owner. <sup>[SEP]</sup>Changes and corrections may be made at any time.