

AppTec360 Enterprise Mobile Manager & ContentBox Administrationshandbuch | Version 4.3.6 (220609.0)





Inhaltsverzeichnis

INF	HALTSVERZEICHNIS	2
I.	ALLGEMEINES	10
Ein	leitende Worte zu AppTec360	10
Unt	terstützte Geräte und Plattformen	12
Erlä	äuterung des "Supervised-Modus" von Apple Geräten	12
Erlä	äuterung des "Android Enterprise Device Owner Mode" von Android Geräten	13
Eig	ene Apps in den Google Play Store hochladen	13
Ein	Gerät in den supervised Modus versetzen	16
Ein	e Gerät in das DEP aufnehmen	17
II.	VORAUSSETZUNGEN / INSTALLATION	18
Vor	raussetzungen	18
S	Systemvoraussetzungen	18
F	Firewallregelungen	18
IF	P-Adresse und DNS Auflösung	20
S	SSL-Zertifikat	20
L	izenzschlüssel	20
Inst	tallation am Beispiel VMware	21
S	Standard Passwörter für die Appliance	24
K	Konfiguration der virtuellen Appliance	25
V	/on externem Host konfigurieren	31
E	Empfehlung zur Sicherheit	32
<i>III.</i>	GENERAL SETTINGS	33
Acc	count Overview	33
С	Dverview	33
В	Bug Report	34
F	Feature Request	35
Glo	abal Configuration	26
010	sMail Settings	26
с Ф	Mail Centilige	26
9	SMS Enrollment	50
0		
Priv	vacy	38
Ģ	GPS Access	38
Rol	le Based Access	39



Role Management	
Role Assignments	40
Zuweisung der Rolle	40
Self Service	41
iOS Configuration	
APNS Certificate	
DEP	46
Configurator & URL	55
Pool Enrollment URL's	55
MDM Profile – Apple Configurator	57
Android Configuration	61
Android Configuration	
Auto Enrollment	62
Android Enterprise	
Methode 1: Android Enterprise Account (Google Account)	63
Methode 2: G Suite Account	
AE EIIIOIIIIIEII	
Methode 1. QR Code Enforment	
Methode 2: NFC Enrollment	
KNOX Enrollment	
Windows Configuration	
Windows Configuration	
0	
Content Box	
Configuration	70
LDAP Configuration	72
Universal Gateway	
	-
App Management	
In-House App DB	74
Android	74
Update Target	75
iOS	75
Update Target	76
Windows	76
Black-& Whitelisting	
Android	
Apple	79
Windows	
Third Party Apps	
Android	
iOS	81
	Q1
VPP Token	۵۱ دە
V/DD Liconses	۵۵
VII LIGENSES	
λήμοιοι θ	



Region	
App Settings	85
iOS App Settings	85
Android App Settings	
Fernwartung	
TeamViewer	
IV. MOBILE MANAGEMENT	
Oberfläche im Mobile Management	
Gerätefilter	
Suchfenster	91
Optionszahnrad	91
Navigationspfeile	
Administrationskonto-Einstellungen	
Firmenverwaltung (Root-Verzeichnis) ir	n Mobile Management93
Create a Subgroup	
Rename Root Node	94
Mass Enrollment	94
Mass Assignment	
Gruppenverwaltung im Mobile Manager	nent96
Create a Subgroup	97
Edit selected Group	97
Delete selected Group	98
Create a User	
Einen neuen Admin-User erstellen	
Benutzerverwaltung im Mobile Manage	nent101
Add and enroll a Device	
Profilverwaltung im Mobile Managemen	t104
Create a profile	
Edit Profile	
Copy Profile	
Delete Profile	
Vererbung von Profilen	
Geräteverwaltung im Mobile Manageme	nt107
Android	
Edit Device	
Clear Passcode	
Lock Device	
Delete Device	
Wipe Device	
Enterprise Wipe	
Send Message	
Send Enrollment Request	
iOS	
Edit Device	
Clear Passcode	
Lock Device	



Delete Device	
Enterprise Wipe	
Send Message	
Send Enrollment Request	
Remove MDM	
Windows	
Edit Device	
Delete Device	118
Wine Device	118
Enternrise Wine	119
Send Enrollment Request	110
Content Management	
File Explorer	123
Audit Trail	123
Trash	124
Fyternal Storage	
	124
Konfiguration iOS	126
General	126
General Information	
Settings	
Config Revision	
	127
Device Log	
Asset Management (nur auf Device Ebene).	
Asset Management (nur auf Device Ebene)	
Security Management.	
GPS Information (nur auf Device Ebene)	
Message (nur auf Device Ebene)	
Security Configuration	
Passcode	
Certificate (nur auf Device Ebene) Installed Certificates	
Encryption	
Single Sign-On	
End of Life (nur auf Device Ebene)	135
Wipe (nur auf Device Ebene)	
Restriction Settings	136
Device Functionality	
Security and Privacy	
BYOD Container	
Built-In iOS Security (Container)	
Activation	
SecurePIM Password	
SecurePIM Security	
SecurePIM Browser	
Exchange	142
Connection Management	
Wifi	
VPN	
APN	
Cellular	



HTTP Proxy	
AirPrint	
AirPlay	
PIM Management	
Exchange Active Sync	
eMail	
CalDav	
Subscribed Calendars	
LDAP	
Web Management	
Webclips	
Web Content Filter	
App Management	151
Enterprise App Manager	151
Installed Apps (nur auf Device Ebene)	
Mandatory Apps	152
Restriction & Settings	155
Blacklisted / Whitelisted Apps	
SysApp Restrictions	
App-VPN	157
App Settings	
Enterprise App Store	159
iTunes Apps	
In-House	
Kiosk Mode	
Content Management	
ContentBox	166
onfiguration Android	
General	
Device Overview (nur auf Device Ebene)	
Oligant Configuration	
Client Configuration	
Asset Management (nur auf Device Ebene)	
Asset Management (nur auf Device Ebene)	
Arti Theft (nur suf Device Chang)	
Anti Theit (nur auf Device Ebene)	
GPS Information (nur auf Device Ebene)	
Wipe & Lock (nur auf Device Ebene)	
Message (nur auf Device Ebene)	177
Security Configuration	± / 2
Desserts	
Passcode	
Passcode Encryption	
Passcode Encryption AntiVirus	
Passcode Encryption AntiVirus End of Life (nur auf Device Ebene)	
Passcode Encryption AntiVirus End of Life (nur auf Device Ebene) Wipe (nur auf Device Ebene)	
Passcode Encryption AntiVirus End of Life (nur auf Device Ebene) Wipe (nur auf Device Ebene) Restriction Settings	172 173 173 174 174 175 175 175
Passcode Encryption AntiVirus End of Life (nur auf Device Ebene) Wipe (nur auf Device Ebene) Restriction Settings Restrictions	172 173 173 174 174 174 175 175 176 176
Passcode	172 173 173 174 174 174 175 175 175 176 176 176
Passcode Encryption AntiVirus End of Life (nur auf Device Ebene) Wipe (nur auf Device Ebene) Restriction Settings Restrictions Allow Screen Capture Erlauben von Screenshots	172 173 173 174 174 175 175 175 176 176 176 176
Passcode Encryption AntiVirus End of Life (nur auf Device Ebene) Wipe (nur auf Device Ebene) Restriction Settings Restrictions Allow Screen Capture Erlauben von Screenshots Allow Clipboard	172 173 173 174 174 174 175 175 175 176 176 176 176 176
Passcode Encryption AntiVirus End of Life (nur auf Device Ebene) Wipe (nur auf Device Ebene) Restriction Settings Restrictions Allow Screen Capture Erlauben von Screenshots Allow Clipboard Erlauben der Zwischenablage	172 173 173 174 174 174 175 175 175 176 176 176 176 176 176 176 176



BYOD Container	
Android Enterprise	
Android Enterprise	
Divide Exchange	
System Apps	
Samsung Knox	
Activation	
Knox Passcode	
Knox Security	
Knox eMail	
Knox Apps	
Connection Management	
Wifi	
VPN	
Restrictions	
APN	
Bluetooth	
PIM Management	
Exchange	
eMail	
AE Gmail Exchange	
Touchdown Exchange	
App Management	
Enterprise App Manager	
Installed Apps (nur auf Device Ebene)	
System Apps (nur auf Device Ebene)	
Mandatory Apps	
Blacklisted Apps	
Sys App Restrictions	
Enterprise App Store	
Playstore	
In-House	
AE Playstore	
Kiosk Mode & Launcher	210
Kiosk Mode	210
AppTec Launcher	212
AppTec Settings	212
Wallpaper	213
Content Management	
ContentBox	214
Konfiguration Windows Phone	
General	
Device Overview (nur auf Device Ebene)	
Config Revision (nur auf Device Ebene)	
Asset Management (nur auf Gerate Ebene)	
Asset Management (nur auf Gerate Ebene)	
Security Management	
vvipe (flur auf Gerale Eperie)	
Resulction Settings	



Device Functionality	
Connection Management	
Wifi	
Wifi Restrictions	
VPN	
VPN Restrictions	
Bluetooth	
NFC	
PIM Management	
Exchange Active Sync	
eMail	
App Management	
Enterprise App Manager	
Mandatory Apps	
Whitelisted / Blacklisted Apps	
Enterprise App Store	
Windowsstore	
In-House	
Kiosk Mode	
Kiosk Mode	
Konfiguration Windows 10 PC	
General	
Device Overview (nur auf Device Ebene)	
Settings	
Config Revision (nur auf Device Ebene)	
Device Log (nur auf Device Ebene)	
Asset Management (only on device level)	
Security Management	
Anti Theft (nur auf Device Ebene)	
GPS Information (nur auf Device Ebene)	
GPS Settings	
Security Configuration	
Passcode	
Restriction Settings	
Device Functionality	
Connection Management	
Wifi	
Wifi Restrictions	
VPN	
VPN Restrictions	
Bluetooth	
PIM Management	
Exchange Active Sync	
eMail	
Konfiguration MacOS	249
General	249
Device Overview (nur auf Profil Ebene)	
Config Revision (nur auf Device Ebene)	
Device Log (nur auf Device Ebene)	
Asset Management (only on device level)	251



Passcode	
Certificate	
Restriction Settings	
Device Functionality	
iCloud	
Media Management	
Connection Management	
Wifi	
AirPrint	
AirPlay	
PIM Management	
Exchange Active Svnc	
eMail	
CalDay	
CardDay	
LDAP	
	261
Dashboard	
Extended Reporting	
Compliance Reports	
Rooted Devices	
Roaming Devices	
Roaming Enabled Devices	
Supervised Devices	
Device Reports	
Devices by Ownership	
All Devices	
Device Carriers	
SAFE Devices	
App Reports	
Installed Apps	
Most Installed Apps	
Mandatory Apps	
VI. MANDANTEN MANAGEMENT	
Oberfläche	
List all clients	
APNS expiry dates	
Account Information	
Einspielen einer weiteren AppTec-Lizenz	
KONTAKT	
DISCLAIMER	



I. Allgemeines

Einleitende Worte zu AppTec360

Die Enterprise-Mobile-Management-Lösung von AppTec bietet mit ihrer sehr intuitiv bedienbaren Managementkonsole die Möglichkeit, sämtliche mobilen Devices zentral zu verwalten und zu konfigurieren. Der EMM-Server kann hierbei entweder bei Ihnen in Ihrer eigenen Umgebung laufen oder Sie nutzen unsere cloudbasierte Lösung.

Auch wenn es um das Thema der zentralen Installation von unternehmenseigenen Applikationen auf Smartphones geht, sind Sie bei uns genau richtig. Mit dem Enterprise Mobile Manager können Sie innerhalb von wenigen Sekunden, Unternehmensapplikationen und Dokumente auf die Geräte verteilen oder unerwünschte Applikationen durch White- oder Blacklisting blockieren.

Die Nutzung privater Geräte im Unternehmen stellt neue Herausforderungen an die Absicherung von Smartphones und Tablets dar. IT-Administratoren müssen eine Vielzahl unterschiedlicher Geräte schützen, da Mitarbeiter verstärkt ihre Smartphones im Unternehmen nutzen wollen. Wir helfen Ihnen dabei, alle Geräte und die darauf gespeicherten sensiblen Daten ganz einfach gegen unbefugten Zugriff zu schützen und aus einer intuitiven Konsole zu verwalten.



Unterstützte Geräte und Plattformen

AppTec360 bietet Unterstützung für iOS, Android und Windows Phone Geräte. Beachten Sie dabei, dass der Funktionsumfang der genannten Plattformen voneinander differenzieren kann

Minimale unterstützte Softwareversionen:

iOS Geräte ab iOS Version 3.0 Android Geräte ab Version 2.3 Windows Phones ab Version 8

Bis einschließlich Android Version 4.1.x muss auf den Samsung Geräten der "AppTec MDM Agent for Samsung" installiert werden, um das Gerät erfolgreich am Server einbinden zu können.

Erläuterung des "Supervised-Modus" von Apple Geräten

Der Supervised Modus stell eine erweiterte Schnittstelle für iOS Geräte von Apple dar.

Für ein entsprechend konfiguriertes Gerät können zusätzliche Einschränkungen im Bezug auf die Funktionalität des Endgerätes angewendet werden. Diese sind ebenfalls in diesem Administrationshandbuch enthalten und werden diesbezüglich mit einem Banner gekennzeichnet.

Verfügbar im Supervised-Modus

Der "Supervised-Modus" kann über das Programm "Apple Configurator" aktiviert werden. Der Apple Configurator kann als Konfigurations-Tool die Grundeinstellung neuer iOS Geräte setzen (über die USB Schnittstelle)

Das Tool kann sowohl Konfigurationsprofile als auch Apps installieren. Es ist kostenlos, setzt aber einen Mac-Rechner voraus.



Erläuterung des "Android Enterprise Device Owner Mode" von Android Geräten

Der Android Enterprise Device Owner Mode (oder kurz AE Device Owner) erweitert Android Geräte um eine Vielzahl an Schnittstellen. So ist es auf AE Device Owner Geräten möglich Konfigurationen vorzunehmen die vorher entweder gar nicht oder nur auf Samsung Geräten möglich waren.

Um Geräte in den AE Device Owner Mode zu versetzen, müssen einige Bedingungen erfüllt sein. Das Gerät muss Android Enterprise im Device Owner Mode unterstützen (wenden Sie sich bitte hierzu an den Hersteller) und Sie müssen die Management Konsole mit Google verknüpfen, mehr dazu finden sie hier: <u>Android</u> <u>Enterprise</u>

Eine Erklärung, wie Sie die Geräte in den Android Enterprise Device Owner Mode einrollen, finden Sie hier: <u>AE Enrollment</u>

Eigene Apps in den Google Play Store hochladen

Sie haben die Möglichkeit mit Ihrer Inhouse App einen eigenen Eintrag im Playstore einzurichten. Hier können Sie dann Ihre App hosten und beispielsweise die Vorteile der automatischen Updates des Playstores nutzen.

Um dies zu realisieren, benötigen Sie einen Google Developer Account. Loggen Sie sich mit diesem in der Google Play Console (<u>https://play.google.com/apps/publish</u>) ein.

Klicken Sie dann auf "Create Application". Wählen Sie die Standard Sprache und den Titel der App.

Create application

Default language *

English (United Kingdom) – en-GB 🔻

Title *

AppTec Demo App

15/50

CANCEL	CREATE
OANOLL	ORLATE



Auf der nachfolgenden Seite müssen Sie verschiedene Informationen zu Ihrer App eintragen.



<u>Hinweis</u>: Achten Sie darauf, dass Sie bei "Pricing & Distribution" verfügbare Länder angeben und bei "Managed Google Play" beide Optionen auswählen, damit Ihre App nur für Ihre Organisation sichtbar ist.

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



Wenn Sie mit allen Schritten fertig sind, können Sie unter "App releases" rechts unten auf "Review" klicken und abschließend den die App mit "Start Roll-Out to Production" im Playstore veröffentlichen.

This release is ready to be rolled out.						
APKs in this release						
Version code	Uploaded	Installs on active devices				
1 APK added						
	3 minutes ago	No data 🚯				
Vhat's new in this release? Vefault – German – de-DE nitial release of the demo app Xa 1 language translation						
PREVIOUS DISCARD		START ROLL-OUT TO PRODUCT				

Danach kann es einige Zeit dauern bis die App im Store erscheint. Wenn der Vorgang abgeschlossen ist, können Sie Ihre App im Play for Work suchen und freigeben, um diese dann via AppTec zu verteilen.





Ein Gerät in den supervised Modus versetzen

- 1. Öffnen Sie den Apple Configurator
- 2. Klicken Sie das Gerät an und wählen Sie "Vorbereiten"

		14	× .	Q		0		?
Back	View	Add	Blueprints	Preinre	Update Bac	ck Up Tag	1	Help
				Prepare Devices				
				Preparing devices devices before yo	s is the first s ou distribute	step in any deployr them to users.	nent. You need to prep	are
				Prepare with:	Manual Co	onfiguration		\$
					Add to D	evice Enrollment P	rogram	
					Activa	ate and complete e	enrollment	
			· ·		Supervise	e devices devices to pair wit	th other computers	
					Enable SI	hared iPad		
				11				
				Cancel			Previous	Vext

- 3. Wählen Sie "Manuelle Konfiguration" und "Betreuen von Geräten"
- 4. Klicken Sie auf "Weiter"
- 5. (Optional) Nun können Sie einen MDM Server hinterlegen, bei dem das Gerät direkt eingerollt wird. Den hierfür benötigten Link finden Sie unter "General Settings – iOS Configuration – Configurator & URL"
- 6. Wählen Sie Ihre Organisation oder legen Sie eine neue an
- 7. Wählen Sie welche Schritte bei der Ersteinrichtung angezeigt werden sollen und klicken auf "Vorbereiten" (VORSICHT: Hierbei wird das gesamte Gerät gelöscht und zurückgesetzt!)

Nun wird Ihr Gerät in den supervised Modus versetzt. Dieser Vorgang kann einige Minuten dauern. Danach startet das Gerät neu und beginnt die Ersteinrichtung.

Ihr Gerät ist nun im supervised Modus!



Ein Gerät in das DEP aufnehmen

Sie können mithilfe des Apple Configurators auch Geräte zum DEP (Device Enrollment Program) aufnehmen, sofern die Geräte mit iOS 11 oder höher betrieben werden.

Mehr Infos zum DEP finden Sie hier: https://www.apple.com/business/dep/

Folgen Sie den selben Schritten wie bei "Ein Gerät in den supervised Modus versetzen" und haken Sie zusätzlich im ersten Schritt "Zum Geräteregistrierungsprogramm hinzufügen" an. Im Laufe der Vorbereitung, werden Sie nach den Logindaten für Ihren DEP Account gefragt, sofern Sie sich nicht zuvor bereits damit im Apple Configurator eingeloggt haben.

Sobald der Vorgang abgeschlossen ist, ist das Gerät im DEP Portal dem Server "Devices Added by Apple Configurator 2" hinterlegt. Sie können danach die Geräte von diesem auf einen anderen verschieben oder diesen Server verwenden.

Damit haben Sie erfolgreich ein Gerät zum DEP hinzugefügt.



II. Voraussetzungen / Installation

Voraussetzungen

Systemvoraussetzungen

Die virtuelle Appliance wird im Open-Virtual-Format (OVF) bereitgestellt. Diese kann in folgende Systeme importiert werden:

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

Zudem werden 4GB RAM/Arbeitsspeicher und 20GB freier Festplattenspeicher benötigt. Die Appliance basiert auf Ubuntu 64bit

Firewallregelungen





Any (extern/Devices) \rightarrow | \rightarrow AppTec Appliance / emmconsole.com

Ports:

80: Let's Encrypt – nur bei der erstmaligen Einrichtung nötig. Danach via 443
443: Management, Enterprise AppStore & Windows Phone Kommunikation
8080: Android & iOS Kommunkiation

```
Any (Devices) \rightarrow | \rightarrow Any (extern)
```

Ports:

5223, 443: Apple Push Dienst, muss ohne Proxy erreichbar sein,
443 als Fallback, siehe <u>https://support.apple.com/de-de/HT203609</u>
5228-5230: Android Push Dienst (GCM), muss ohne Proxy erreichbar sein

Domain Controller \rightarrow | \rightarrow AppTec-Server / emmconsole.com

Ports:

389, (LDAPS 636): Benutzersynchronisation mit LDAP

Apptec Appliance $\rightarrow | \rightarrow$ Any

Port:

443

Benötigt für den Android Push Dienst (GCM)

Der Port 443 nach außen wird benötigt um in unserer Software nach Apps zu suchen. Leider können wir hier aufgrund der Netzstruktur der Anbieter keine genaue IP oder ein IP Netz angeben. Sollte dieses Feature also gewünscht sein, müsste Port 443 zu Any offen sein.

AppTec Appliance \rightarrow | \rightarrow emmconsole.com

Ports:

443: AppTec Appliance Updates, APNS Zertifikatsgenerierung

AppTec Appliance \rightarrow | \rightarrow Apple Netz (17.0.0.0/8)

Ports:

2195, 2196: Apple Push Dienst & Feedback Dienst 443: DEP & VPP



IP-Adresse und DNS Auflösung

Der AppTec Server muss unter einer öffentlichen IP-Adresse erreichbar sein, zudem benötigen Sie einen entsprechend aufgeschalteten Hostnamen bzw. DNS-Eintrag. Zum Einrollen eines Windows-Phones wird zusätzlich eine Subdomain nach dem Schema "**enterpriseenrollment.<Appliance Domain>**" benötigt. Dieser Eintrag muss auch auf die Appliance zeigen.

SSL-Zertifikat

Sie müssen ein SSL-Zertifikat, passend zum lizenzierten FQDN, während der Einrichtung hochladen. Es wird zudem das Intermediate-Zertifikat der CA und der Private Key (nicht passwortgeschützt) benötigt.

Bitte beachten Sie, dass wir kein Zertifikatsaussteller sind und keine Zertifikate ausstellen oder erneuern. Das SSL Zertifikat erhalten Sie von einem Aussteller Ihrer Wahl.

Für Windows Phone 10 wird zusätzlich ein Zertifikat für die enterpriseenrollment subdomain benötigt.

SMTP-Relay

Ein Emailserver bzw. ein Email-Relay wird benötigt, damit der AppTec360 Server Emails an die entsprechenden Benutzer senden kann.

Lizenzschlüssel

Um den Server erfolgreich aktivieren und installieren zu können benötigen Sie eine gültige Lizenzdatei. Diese können Sie von AppTec360 selbst bzw. von Ihrem entsprechendem Reseller erhalten.



Installation am Beispiel VMware

"Datei" > "OVF-Vorlage bereitstellen…"



Im Nachhinein die bereitgestellte OVA-Image auswählen und mit "weiter" bestätigten.

OVF-Vorlage bereitstellen	
Quelle Wählen Sie den Speicherort der	Quelle.
Quelle Einzelheiten zur OVF-Vorlage Name und Speicherort Festplattenformat Bereit zum Abschließen	Aus einer Datei oder URL bereitstellen M: 'Partner_Hersteller \AppTec360\AppTec lokal\emm_vm.ova Curchsuchen Geben Sie eine URL zum Herunterladen und Installieren des OVF-Pakets aus dem Internet an oder geben Sie einen Speicherort an, auf den Ihr Computer zugreifen kann, z.B. eine lokale Festplatte, eine Netzwerkfreigabe oder ein CD-/DVD-Laufwerk.
Hilfe	∠Zurück Weiter ≥ Abbrechen



> Einzelheiten zu OVF-Vorlage mit "Weiter" bestätigen.

Einzelheiten zur OVF-Vorlage Überprüfen Sie die Einzelheite	en der OVF-Vorlage.			
Quelle Einzelheiten zur OVF-Vorla Name und Speicherort Festplattenformat Netzwerkzuordnung Beszik zw. Abschließen	Produkt: Version:	VirtualApplianceV201419		
	Anbieter: Herausgeber:	Kein Zertifikat vorhanden		
	Größe auf Festplatte:	8,7 GB (schnell bereitgestellt) 110,0 GB (Thick-bereitgestellt)		
	Beschreibung:			
Hilfe			≤ Zurück Weiter ≥	Abbrechen

> Hier können Sie die VM nach Ihren Wünschen benennen.

Name und Speicherort Geben Sie einen Namen u	nd einen Speicherort für die bereitgestellte Vorlage an		
<u>Quelle</u> Einzelheiten zur OVF-Vorlage	Name:		
Name und Speicherort Festplattenformat Netzwerkzuordnung	Der Name kann bis zu 80 Zeichen enthalten und muss innerhalb des Bestandsordners einde	utig sein.	
Bereit zum Abschließen	Bestandslistenspeicherort: Image: MiLAN Image: Discovered virtual machine	_	
Hilfe	<u>≤</u> Zurüd	Weiter ≥	Abbrechen



> Festplattenformat der VM mit "weiter" bestätigen.

Festplattenformat In welchem Format möchte	en Sie die virtuellen Festplatten speid	thern?			
Quelle Einzelheiten zur OVF-Vorlage Name und Speicherort Festplattenformat Netzwerkzurchung Bereit zum Abschließen	Datenspeicher: Verfügbarer Speicherplatz (GB): C Thick-Provision Lazy-Zeroed C Thick-Provision Eager-Zeroe C Thin Provision	datastore 1 83,6 d			
Hilfe			<u>≤</u> Zun	ück Weiter ≥	Abbrechen

> Letzte Ansicht der Konfiguration mithilfe von "Beenden" abschließen.

🕗 OVF-Vorlage bereitstellen			
Bereit zum Abschließen	orwondon mächton?		
Sind dies die Opdonen, die sie w	erwenden nochten?		
Einzelheiten zur OVF-Vorlage	Venn Sie auf 'Beenden' kl	icken, wird eine Bereitstellungsaufgabe gestartet.	
Name und Speicherort Ein	stellungen für die Bereits	stellung:	
Festplattenformat 0	IVF-Datei:	M:\Partner_Hersteller\AppTec360\AppTeclokal\emm_vm.ova	
Bereit zum Abschließen D	ownload-Größe:	3,5 GB	
G	röße auf Festplatte:	8,7 GB	
N	lame:	srv-apptec02	
0	Irdner:	MILAN	
н	lost/Cluster:	10.0.201	
D	atenspeicher:	datastore1	
Fe	estplattenbereitstellu	Thin Provision	
N	letzwerkzuordnung:	'nat' zu 'VM Network'	
	Nach der Bereitstellung	einschalten	
1		1	7 1
Hilfe		< Zurück Beenden	Abbrechen
			li li



> Bitte warten Sie bis die VM erfolgreich installiert wurde.



Bitte beachten Sie, dass Upgrades des Ubuntu-Betriebssystems auf eine höhere Version einen nicht mehr funktionierenden AppTec-Server zur Folge haben kann. Wir empfehlen an dieser Stelle, KEINE Upgrades auf eine neuere Betriebssystemversion durchzuführen! Die einzige Ausnahme bildet das Upgrade von Ubuntu 12 zu 14. Kontaktieren Sie für mehr Infos hierzu support@apptec360.com Jedoch sollten Sicherheitsupdates eingespielt werden!

Standard Passwörter für die Appliance

Root PasswortapptecStandard NutzerapptecPasswort für den Nutzer "apptec"apptecMySQL Root NutzerrootMySQL Root PasswortapptecMySQL Standard NutzerAppTecMySQL Standard Nutzer PasswortAppTecAppTecAppTecAppTecAppTecAppTecAppTec



Konfiguration der virtuellen Appliance

Wichtig: Bevor Sie mit der Konfiguration beginnen, setzen Sie die Auflösung der Anzeige auf mindestens 1280x800 Pixel.

Um den Prozess zu vereinfachen, können Sie Konfigurationsseite extern erreichbar machen. Folgen Sie dafür den Schritten in "Von externem Host konfigurieren"

<u>Schritt 1</u>

- 1. Laden Sie die Lizenzdatei hoch.
- 2. Wenn die Lizenz erfolgreich hochgeladen wurde, sehen Sie, wie unten im Screenshot, die Lizenzinofmrationen

	APPTEC 360' Enterprise Mobility Management
nfig Update Check Appliance I	nfo
1 STEP ONE Appliance License	STEP TWO 3 STEP THREE 4 STEP FOUR 5 STEP FIVE SSL Configuration 3 Server Settings 4 MySQL Setup 5 License Agreement
Appliance License	
	Upload a new License File
f you have already configured your appliance, you ca	an upload your Appliance Configuration here.
	Upload an Appliance Configuration File
/ou can download your Appliance Configuration in or	der to export it to a new Appliance. Download the Appliance Continuention
Appliance License Information	Download the Applicative Configuration
Appliance Alias	
Appliance Alias Hostname	NUMBER OF TAXABLE PARTY
Appliance Alias Hostname Server Identifier	NUMBER OF THE OWNER
Appliance Alias Hostname Server Identifier Contact Person Prename	A parameter A para
Appliance Alias Hostname Server Identifier Contact Person Prename Contact Person Surname	
Appliance Alias Hostname Server Identifier Contact Person Prename Contact Person Surname Phone	i personali Report de la companya de Report de la companya de la compa esta de la companya de



<u>Schritt 2</u>

- 1. Laden Sie das <u>SSL Zertifikat</u> hoch. Diese sehen Sie in Schritt 1.
- 2. Laden Sie den Private Key für das Zertifikat hoch. Wichtig: Der Key darf nicht passwortgeschützt sein.
- 3. Laden Sie das dazugehörigen Intermediate Zertifikat hoch.

CTED ONE	
Appliance License	2 SSL Configuration 3 Step Filter 4 Step Floor 5 Step Floor License Agreemen
SL Configuration	
SSL Certificate Summary	
arning: The certificate is issued to	but the hostname in the license file is
e certificate is issued to b is could eventually cause problems for your c	but the hostname in the license file is developed to the server.
recommended to contact either AppTec Sup	pport to get a new license file with as hostname,
getting a new SSL Certificate issued to	
Common Name	
Expire Date	
Expire Date	
Expire Date	Renew SSL Certificate
Expire Date	Renew SSL Certificate Remove SSL Certificate
Expire Date Private Key	Renew SSL Certificate Remove SSL Certificate
Expire Date	Renew SSL Certificate Remove SSL Certificate
Expire Date Private Key Path	Renew SSL Certificate Remove SSL Certificate
Expire Date Private Key Path	Renew SSL Certificate Remove SSL Certificate Remove SSL Certificate Remove SSL Certificate Key
Expire Date Private Key Path	Renew SSL Certificate Remove SSL Certificate Remove SSL Certificate Renew Certificate Private Key Remove Certificate Private Key
Expire Date Private Key Path SSL Intermediate Certificat	Renew SSL Certificate Remove Certificate Private Key

Hinweis: Wenn Sie auch Windows Geräte verwalten möchten, brauchen sie eine seperate Subdomain: "enterpriseenrollment.[IHR-APPLIANCE-FQDN]".

In diesem Fall müssen Sie dann auch hierfür das Zertifikat in Schritt 2 hochladen.



Schritt 3

- 1. Geben Sie hier die globale Support Mail Adresse ein. Diese wird verwendet um die Enrollment Mails zu versenden.
- 2. Bitte ändern Sie den Nutzernamen und Passwort für den Servermanager.

Hinweis: Dies ist **nicht** der Login um Geräte zu verwalten. Dieser Login wird verwendet um Lizenzen in einer Multi-Mandanten Umgebung zu verwalten.

Der Login Name für die Geräteverwaltung wird in Schritt 1 unter "Mail" angezeigt.

Sie erhalten das Passwort für den Login nachdem Sie die Konfiguration in Schritt 5 abgeschlossen haben.

	Chepres Mcbilly Management	
g Update Check Appliance Info		
1 STEP ONE Appliance License	STEP TWO SSL Configuration 3 STEP THREE Server Settings 4 STEP FOUR MySQL Setup 5 STEP FIVE License Agreement	nt
erver Settings		
Settings Summary		
Server Domain		
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	and the second	
You can use the Server Manager Credentials to login a Don't use your email address as username, use somet	t mydevice.at in order to export your data or delete accounts. hing like "verySecretUsername" instead.	
Username for Server Manager		
Password for Server Manager		
	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.	



4. Falls dies in Ihrer Umgebung benötigt wird, können Sie hier die Ports ändern.

1 Appliance License	SSL Configuration 3 ST	EP THREE over Settings 4 STEP FOUR MySQL Setup 5 STEP FIVE License Agreement
hanging any of the default values makes it necessa you change the default SSL port, the console will t	ary to reset the firewall settings for incoming traffic be accessible through the following URL:	(Applications -> System Tools -> Administration -> Firestarter). 443
SL Port	443	(Default:443)
evice Communication Port*	8080	(Default8090)
CEP Port	8081	(Default:8081)
lease contact AppTec Support (support@apptec3 you change the device communication port, all dev mail Settings ease enter valid SMTP credentials! IE-Mails generated by AppTec EMM Console will I	50.com) before changing the device communication rices that have been enrolled before the change, v be sent using this account.	n port, otherwise your Android devices will not be able to discover your server. Ill be unable to connect to the server and have to be re-enrolled.
Please contact AppTec Support (support@appteC3 you change the device communication port, all dev Email Settings lease enter valid SMTP credentials! II E-Mails generated by AppTec EMM Console will I Email Address	50 com) before changing the device communicatio rices that have been enrolled before the change, v be sent using this account.	n port, otherwise your Android devices will not be able to discover your server. III be unable to connect to the server and have to be re-enrolled.
Please contact AppTec Support (support@appteC3 you change the device communication port, all dev Email Settings lease enter valid SMTP credentials! all E-Mails generated by AppTec EMM Console will I Email Address From Name	30.com) before changing the device communication rices that have been enrolled before the change, w be sent using this account.	n port, otherwise your Android devices will not be able to discover your server. ill be unable to connect to the server and have to be re-enrolled.
Please contact AppTec Support (support@appteC38 ryou change the device communication port, all dev Email Settings Please enter valid SMTP credentials! III E-Mails generated by AppTec EMM Console will I Email Address From Name SMTP Auth Method	50.com) before changing the device communication vices that have been enrolled before the change, we be sent using this account.	n port, otherwise your Android devices will not be able to discover your server.
Please contact AppTec Support (support)@appteC33 ryou change the device communication port, all dev Email Settings Please enter valid SMTP credentials VI E-Mails generated by AppTec EMM Console will I Email Address From Name SMTP Auth Method Username	50 com) before changing the device communication rices that have been enrolled before the change, w be sent using this account.	n port, otherwise your Android devices will not be able to discover your server.
Please contact AppTec Support (support@appteC30 you change the device communication port, all dev Email Settings lease enter valid SMTP credentials all E-Mails generated by AppTec EMM Console will I Email Address From Name SMTP Auth Method Jsername Password	50.com) before changing the device communication vices that have been enrolled before the change, vices be sent using this account.	n port, otherwise your Android devices will not be able to discover your server.
Please contact AppTec Support (support@appteC33 you change the device communication port, all dev Email Settings lease enter valid SMTP credentials! II E-Mails generated by AppTec EMM Console will I Email Address From Name SMTP Auth Method Jsername Password Hostname	50 com) before changing the device communication rices that have been enrolled before the change, v be sent using this account. login • 	n port, otherwise your Android devices will not be able to discover your server.
Please contact AppTec Support (support)@appteC30 tryou change the device communication port, all device Email Settings Please enter valid SMTP credentials! UI E-Mails generated by AppTec EMM Console will is Email Address From Name SMTP Auth Method Jsername Password Hostname Port (leave empty for default)	50.com) before changing the device communication rices that have been enrolled before the change, we be sent using this account. I ogin • I ogin •	n port, otherwise your Android devices will not be able to discover your server. Ill be unable to connect to the server and have to be re-enrolled.

 Geben Sie die SMTP Daten Ihres E-Mail Accounts in den "Email Settings" ein. Dieser Account wird verwendet um Enrollment Mails, Bugreports und Feature Requests an <u>support@apptec360.com</u> zu senden. Wenn Sie die Daten eingetragen haben, speichern Sie diese mit "Save". Danach können Sie diese testen.



<u>Schritt 4</u>

1. Wenn Sie dir interne Datenbank der Maschine nutzen möchten, können Sie diesen Schritt überspringen. Andernfalls können Sie hier die Daten Ihrer Datenbank hinterlegen.

		APPTEL360 Enterprise Mobility Management	
g 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
lySQL Setup			
e MySQL connection has been successfully tested	at at a second		
ou change the settings after the initial configuration, y	ou have to recontigure your appliance by cliv	cking on "Configure now" in step 5	
P Address or Hostname	127.0.0.1	(Default: 127.0.0.1)	
Username	AppTec	(Default: AppTec)	
Password	АррТес	(Default: AppTec)	
Port	3306	(Default: 3306)	



<u>Schritt 5</u>

- 1. Bitte stellen Sie sicher, dass "Create Accounts for included Client Licneses" angehakt ist.
- 2. Setzen Sie den Haken bei "I Agree" und klicken auf "Configure Appliance" um die Konfiguration zu speichern.

Hinweis: Sie müssen jedes mal nach jeder Änderung der Konfiguration auf "Configure Appliance" klicken.

nfig Update Check Ap	ppliance Info			
Appliance License	2 STEP TWO SSL Configuration	3 STEP THREE Server Settings	A STEP FOUR MySQL Setup	5 STEP FIVE License Agreement
License Agreement				
Create Accounts for included Client Licenses	s?	e License)		
Reset passwords and send an Account Crea Check this if you've already configured your	ation Mail for all included Client Licenses [Appliance, and the accounts were created,	but you didn't got any eMails because of	some misconfiguration)	
n order to configure the AppTec Appliance y	you have to agree to the license below			
Click here to read the License Agreement	t and Terms and Conditions of AppTec Gn	ıbH		
I agree that I have read and agreed to be bo	ound by the license agreements for this produ	ct.		
Agree: *				
Press on the Button below to configure the a	appliance			
				Configure Appliance

Glückwunsch!

Sie haben die Konfiguration der Appliance abgeschlossen.

Sie können Sich nun in die Management Konsole einloggen und Geräte verwalten.

Der Login Name für die Geräteverwaltung wird in Schritt 1 unter "Mail" angezeigt.

Sie erhalten das Passwort für den Login nachdem Sie die Konfiguration in Schritt 5 abgeschlossen haben.

Um sich in die Konsole einzuloggen, geben Sie den FQDN in Ihren Browser ein.

Diesen finden Sie in Schritt 1 der Appliance Konfiguration. (Beispiel: <u>https://emm.beispiel.de</u>).



Von externem Host konfigurieren

Wenn Sie die Appliance über einen externen Host konfigurieren möchten, folgen Sie den folgenden Schritten.:

- Erstellen Sie eine Datei namens "externalConfigPassword" in /opt/console/application/configs/
- Geben Sie ein Passwort in dieser Datei an, beispielsweise "myVerySecretPassword" (Ein leeres Passwort ist nicht möglich).
- Geben Sie die folgende URL in Ihren Browser ein: http://<myHostname>/public/config/extconfig/pwd/myVerySecretPassword (Die Konfiguration via HTTPS ist nach der ersten erfolgreichen Konfiguration möglich).
- Nun können Sie die Appliance über einen externen Host konfigurieren. Der Zugriff ist für eine Stunde gültig. Geben Sie die URL erneut ein um eine neue Sitzung zu starten.
- Löschen Sie die Datei "externalConfigPassword" nach der erfolgreichen Konfiguration.



Empfehlung zur Sicherheit

Es wird empfohlen die folgenden Schritte zu befolgen um die Sicherheit der Appliance zu gewährleisten.

Dies ist keine Liste von allen Möglichkeiten, sondern eine kurze Empfehlung für die Basissicherheit.

- Ändern Sie für den root und apptec Nutzer das Passwort
- Deaktivieren Sie den Autologin für den apptec Nutzer
- Ändern Sie das Passwort für die MySQL Nutzer root und AppTec
- Ändern Sie den Standard SSH Port
- Sperren Sie Port 80, blockieren Sie eingehenden HTTP Verkehr und nutzen ausschließlich HTTPS
- Löschen Sie die Datei
 /opt/console/application/configs/externalConfigPassword
- Konfigurieren Sie die Firewall

Erste Schritte

Die 3 ersten Schritte in Ihrer Appliance:

- 1. Um iOS Geräte zu verwalten richtien Sie ein APNS Zertifikat unter "General Settings -> iOS Configuration" ein.
- 2. **Fügen Sie einen Nutzer und ein Gerät hinzu.** Klicken Sie auf das Zahnrad während Sie eine Gruppe angewählt haben und klicken auf "Add User" um einen Nutzer anzulegen. Wählen Sie den Nutzer an, klicken Sie auf das Zahnrad und wählen "Add and Enroll a device" um ein Gerät hinzuzufügen.
- 3. Um Einstellungen an ein Geräte- oder Gruppenrpofil zu senden, klicken Sie auf "Save" und anschließend auf "Assign Now".



III. General Settings

Account Overview

<u>Overview</u>

Hier erhalten Sie einen Überblick über Ihren AppTec Account.

Company Name	Ihr Firmenname
Creation Date	Erstelldatum von AppTec
License Type	Paid = bezahlt
	Free = kostenlose Lizenz
License Expiration Date	Ablaufdatum Ihrer AppTec Lizenz
	Free = Kostenlose Lizenz für 25
ContentBox License	Geräte
	Paid = Gekaufte Lizenz für x Geräte
Devices	Wie viel Geräte registriert und noch
	registriert werden können
Contact Person	angegebene Kontaktperson
Phone	angegebene Telefonnummer
eMail*	angegebene Email Adresse
Root User	User auf der EMM Console
Root Login	E-Mail mit der Sie sich auf der EMM
	Console anmelden
Software Version	aktuelle Software Version
	Allgemeine Geschäftsbedingungen
Terms and Conditions, and	(Weiterleitung auf die AppTec
License Agreement	Webseite, dort finden Sie diverse
-	PDF Dateien hierzu)

*<u>Hinweis:</u> Später wird der Admin-User wie jeder andere angezeigt. Ändern Sie dort die Mail-Adresse, müssen Sie sich folglich auch mit der neuen Mail-Adresse einloggen.

		-	Cveniew Bug Report Feature Request	👤 support@milanconsult.de 🗸
i			Account Information	
	Global Configuration		Company Name	milanconsult GmbH
	Privacy		Creation Date	January 15, 2015, 3:09 pm
			License Type	Paid
	Apple Configuration		License Expiration Date	never
	Android Configuration		ContentBox License	Free
	Windows Configuration		Devices	11/25
			Contact Person	12 per estate and the set
	ContentBox		Phone	+49 7461 969739 0
	LDAP Configuration		eMail	Autor brandstrader and an
	App Management	,		
			RootUser	Milan Admin
			Root Login	To the second second the
			Software Information	
			Software Version	Version 201514
			Terms and Conditions, and License Agreement	Click here



Bug Report

Über die Weboberfläche kann direkt ein Bug Report an den Support geschickt werden.

Summary	Eine kurze Zusammenfassung Ihres Problems
Description	Eine ausführliche Beschreibung Ihres Problems, bitte so detailliert wie möglich
Additional Information	Zusätzliche Informationen die nicht direkt das Problem beschreiben, ggf. jedoch nützliche sein könnten
Include logfiles	Möglichkeit die Logdateien direkt mitzusenden
Attachment	Dem Bugreport einen Anhang mitgeben
,blaues Plussymbol'	Für zusätzliche Anhänge
Submit Bug Report	Bug Report abschicken

		4	I► Overview	Bug Report	Feature Request	supporté	@milanconsult.de	• •
i	Account Overview		Send a bug report					
	Global Configuration		Summary			Summary of the bug report		
						Description of the bug report. This is the section that is used to describe the bug in detail so use as much as possible !		
	Apple Configuration					Please use English or German.		
	Windows Configuration							
	LDAP Configuration		Description					
	App Management 🗸 🗸							
			Additional Information			You can use this box to provide any additional information that is not a direct description of the bug be relevant.	, but may	
			Include logfiles			On Da		
			Attachment			Durchsuchen		0
			+				Submit Bug Rep	ort



Feature Request

Über die Weboberfläche kann auch direkt ein Feature Request an den Support geschickt werden.

Summary	Eine kurze Zusammenfassung Ihres Problems
Description	Eine ausführliche Beschreibung Ihres Problems, bitte so detailliert wie möglich
Attachment	Dem Bugreport einen Anhang mitgeben
,blaues Plussymbol'	Für zusätzliche Anhänge
Submit Feature Request	Feature Request abschicken

		•		Overview	Bug Report	Feature Request	<u>.</u>	support@milanconsult.d	le 🗸
i			Send a fe	ature request					
	Global Configuration		Summan	y			Summary of the feature request		
							Description of the requested feature.	h an nanažila i	
	Apple Configuration						This is the section that is used to describe the requested realitie in detail, so use as indi- Please use English or German.	n as possible :	
	Windows Configuration								
	LDAP Configuration		Descripti	on					
	App Management	~							
			Attachme	nt			Durchsuchen Keine Datei ausgewählt.		0
			+					Submit Feature Requ	uest



Global Configuration

eMail Settings

Hier können die Templates für die jeweiligen Szenarien und Betriebssysteme festgelegt werden.

		🔺 🕨 eMail Settings eMail Templa	ates SMS	3 Enrollment		🧕 support@	milanconsult.de 🗸
0	Account Overview	Device Enrollment Mail Settings					
dð		Recipient:	\$	Android Template	iOS Template	Windows Template	Status
1		User		Default ~	Default ~	Default ~	On On
é	Apple Configuration	Administrator (daniel.bezdecka@milancon	nsult.de)	Default ~	De fault ~	Default ~	011
	Windows Configuration	Others (CSV)		Default 🗸	Default ~	Default ~	Off 🕥
2	LDAP Configuration	Lock-Screen message					
	App Management 🗸 🗸	Recipient:	\$	iOS Template			
		User		Default			~

eMail Templates

Hier sind Sie in der Lage verschiedene Templates für unterschiedliche Szenarien anzulegen, wie z.B. für den Lock Screen (Sperrbildschirm) oder auch die allgemeine E-Mail für das Rollout.

		4	I 🕨 eMail Settings	eħ	lail Templates SMS El	nrollment			support@milanconsi	ult.de 🗸
0	Account Overview	1	Available eMail Templates							
₿			Туре	¢	Name O	Subject	0	Format 0		
			Android Enrollment		Default	Enrollment request for your Android device		text	Default templates can't be altered	O
	Apple Configuration		iOS Enrollment		Default	Enrollment request for your iOS device		text	Default templates can't be altered	0
	Windows Configuration		Windows Enrollment		Default	Enrollment request for your Windows device		text	Default templates can't be altered	0
			Lock screen message		Default	Lock Screen Message		text	Default templates can't be altered	0
	LDAP Configuration		Lock screen message		milan Lockscreen	Geräl gespernt!		html	‡	٠

Die Default Templates können nicht bearbeitet oder gelöscht werden.

Über das "Plus Symbol" hinter des jeweiligen Standard Templates können zusätzliche Templates angelegt werden.

Mit dem 鄰 Symbol können Sie eine Änderung am Template vornehmen.



Ein Beispiel könnte wie folgt aussehen:

Add eMail Template		\times
Template Alias	Copy of Default	
Туре	Android Enrollment	
Subject	Enrollment request for your Android device	
Text:	Hello %prename% %sumame%, 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 %playstoreLint% or type the following URL into your smatphones browser %downloadLink%	A III P H
eMail Format.	● Text ◎ HTML	
Show Placerholders		
	Save	

SMS Enrollment

Hier können Sie das SMS Enrollment Verfahren de- bzw. aktivieren. (Standard: deaktiviert)

Ebenfalls wird Ihnen hier angezeigt, wie viel SMS Credits noch verfügbar sind.




Privacy

GPS Access

Unter "GPS Access" können Sie die Lokalisierung eines Gerätes mit ein oder sogar zwei Passwörtern versehen z.B. für Betriebsrat und IT Abteilung – "vier-Augen-Prinzip".

Postrict access to CDS Sottings	Off = Funktion ist ausgeschaltet
Resinct access to GPS Settings	und es wird kein Passwort zur
	Lokalisierung benötigt
	On = Funktion ist angeschaltet und
	es wir ein Passwort zur
	Lokalisierung benötigt
Protection Method	Use one password = Ein Passwort
	zur Lokalisierung benötigt
	Use two passwords = Zwei
	Passwörter zur Lokalisierung
	werden benötigt
Enter Password (1)	Gewähltes Passwort eintragen
Repeat Password (1)	Gewähltes Passwort nochmals
	eintragen
optional: Enter Password 2	2. gewähltes Passwort eintragen
optional: Repeat Password 2	2. gewähltes Passwort nochmals
	eintragen

			GPS Access		support@milanconsult	.de 🗸
			Restrict access to GPS Settings	⊙ ∩) ⊙		0
	Global Configuration		Protection Method	Use one password	~ ©	0
53			Enter Password	•••••		0
	Apple Configuration		Repeat Password			
	Windows Configuration					
	LDAP Configuration					
	App Management	~				



Role Based Access

Role Management

Mit dem Role Management ist es nun möglich eine Rollenverteilung für User und Admins zu betreiben.

Somit kann individuell anhand von Rollen gewisse Berechtigungen verteilt werden.

•	►	Role Management	Role Assignments	📃 support@milanconsult.de 🗸
	Roles	(0	
	Super	Root		
	Self S	ervice		
i I				

Super Root	"Super Admin" hat Zugriff auf alle
	Einstellungen und Konfigurationen
	Hat lediglich Zugriff auf "General
Self Service (siehe unten für weitere	Information", "Asset Management" und
Details)	das "Anti Theft" (Gerätelokalisierung)

Mit dem Plus Symbol kann eine "neue Rolle" definiert werden.

Roles	0			
Super Root		Role Settings		•
Self Service		Role Name	New Role	
		Enable Role	Off	
		Group Access		~
		Profile Access & Assignment		~
		Actions		~
		Mobile Management		~
		ContentBox		~
		General Settings		~
		DEP Pool		~
		Reporting		~

Hier können Sie der neuen Rolle einen Namen und geben und die Berechtigungen wie gewünscht einstellen.



Beachten Sie hierbei dass die Rolle mit "Enable Role" aktiviert werden muss.

Roles	Role Settings				C			
Super Root Self Service	Role Name	New Role			-			
	Enable Role	Он						
	Group Access				^			
		Read	Write	Full Read 🔞	Full Write 🕝			
	AppTec GmbH	E		<u> </u>				
	Admins							
	Consultants	Ē						
	test							
	Untergruppe	E						
	Profile Access & Assignment	i.			~			
	Actions				~			
	Mobile Management	Mobile Management						
	ContentBox	ContentBox General Settings						
	General Settings							
	DEP Pool				~			
	Reporting							

Read	Leseberechtigung für die Gruppe (Es kann nur eingesehen werden, aber nicht geändert werden)
Write	Schreibberechtigung für die ausgewählte Gruppe (Änderungen können vorgenommen werden)
Full Read	Die Leseberechtigung gilt auch für alle Untergruppen
Full Write	Die Schreibberechtigung gilt auch für alle Untergruppen

Role Assignments

Hier erhalten Sie eine komplette Übersicht welche Rolle welchem User zugewiesen ist, ebenfalls sehen Sie im "Role Status" ob die Rolle aktuell

aktiviert ist.

-	I 🕨 Rol	le Management	Role Assignments		support@milanconsult.de	~
	Name	4	e Mail	\$ Role	\$ Role Status	\$
	Philipp Reis	S	Reiss @apptec360.com	Test	Role enabled	
	Support		support@	Super Root	Role enabled	

Zuweisung der Rolle



Die Zuweisung erfolgt nun im "Mobile Management", indem ein User editiert wird. Hier kann dann unter "Assigned Roles" eine oder mehrere Rollen verteilt werden.

Assigned Roles	Super Root × Test × Self Service ×

Self Service

Hierfür muss dem User ein Passwort zugewiesen werden, dies erfolgt ebenfalls über "Edit User" im "Mobile Management".

Enter new password	0
Repeat new password	8

Der User kann sich dann unter der Ihnen bereits bekannten URL (z.B. <u>www.emmconsole.com</u> sofern die AppTec Cloud genutzt wird) mit seiner hinterlegten E-Mail Adresse und das von Ihnen definierte Passwort anmelden. Beim Self Service Portal hat man lediglich Zugriff auf "General Information", "Asset Management" und dem "Anti Theft", welches zur Gerätelokalisierung dient.

▲ ► Ge	eneral Information			Lukas .	~
Device of Lukas		Device Info			
		Device Name	iPad (2)		
		Phone Number	-		
		Model	IPad		
		Operating System	ios		
Battery 50		Serial Number	DMPG65KRDFJ1		
30	%	Device Ownership	Corporate		
Free Storage		Device Type	Tablet		
11.47	GB	Jailbroken	No		
		Supervised	Yes		
		Compliant	Yes		
General		Last Seen	2015-10-16 15:14:44		
Asset Mananement					
Security Management					
Anti Theft					



iOS Configuration

APNS Certificate

Hier können Sie ein APNS Zertifikat hochladen und verwalten – dieses Zertifikat ist notwendig, damit eine Kommunikation zwischen AppTec und der iOS Endgeräte stattfinden kann.

Hinweis: Diese Prozedur muss jedes Jahr erneut getätigt werden, da das APNS Zertifikat nur ein Jahr gültig ist.

Es muss dann dieselbe Apple ID verwendet werden, ansonsten ist ein zukünftiges Verwalten der iOS Geräte nicht mehr möglich und alle Geräte müssen neu eingerollt werden.

Geben Sie zuerst Ihre Apple ID ein und klicken Sie auf "Next Step"
 (Empfehlung: Es sollte sich hierbei um eine generische Apple ID handeln)

		APNS Certificate	
	Global Configuration	1 Enter Apple ID 2 Ster Two Upload Push Cert 3 Ster Tikke	
Ś	Apple Configuration	No certificate installed yet !	
	Android Configuration	Enter your Apple ID support@mianconsut.de	
	Windows Configuration	Next Step	
	ContentBox		
	LDAP Configuration		
	App Management		

- Laden Sie sich anschließend die "signedPushCertificate.txt" Datei herunter indem Sie darauf klicken.
- Klicken Sie anschließend auf "Apple Push Certificates Portal", Sie sollten nun an folgende URL weitergeleitet werden: <u>https://identity.apple.com/pushcert/</u>

		🔺 🕨 APNS Cettificate	
0			
灥	Global Configuration	Enter Apple ID 2 Upload Push Cert 3 Certificate Summary	
6	Privacy	Register your signed push certificate.	
Ś		1. Download this signedPushCertificate.bd	
÷	Android Configuration	2. Upload the certificate to Apple Push Certificates Portal 3. You will get a pern file. Upload the pern file	
	Windows Configuration	Choose your /PEM file	
6	ContentBox	Durchsuchen	
1	LDAP Configuration	- Unload	
8	App Management 🗸	Purch -	
		bath	



• Melden Sie sich nun bitte mit Ihrem Apple Account an.

Apple Push Certificates Portal

Sign In.		
support@milanconsult.de		
Forgot your Apple ID?		
•••••		
Forgot your password?		
	Sign In	

 Klicken Sie, sobald Sie sich erfolgreich anmelden konnten, auf "Create a Certificate".





Klicken Sie auf "Durchsuchen…" und wählen Sie das von Ihnen vorher erstellte "signedPushCertificate.txt" aus.

- Schreiben Sie sofern erwünscht (für eine evtl. spätere Zuordnung) etwas Aussagekräftiges in die "Notes".
- Klicken Sie anschließend auf "Upload".



o Im Nachgang sollten Sie folgende Ansicht erhalten





• Klicken Sie auf "Download"



- Gehen Sie nun wieder zurück auf die AppTec Console und wählen nun unterhalb von "Choose your .PEM file" "Durchsuchen…" aus.
- Wählen Sie nun die eben heruntergeladene Datei aus und klicken Sie anschließend auf "Upload".

Choose your .PEM file
Durchsuchen MDM_ AppTec GmbH_Certificate.pem
Upload
Back

• Sollte diese Prozedur erfolgreich gewesen sein, erhalten Sie nun folgende Ansicht – nun können Sie Apple Geräte einrollen und verwalten.

		APNS Certificale
		New APNS certificate successfully installed
	Global Configuration	1 STEP ONE 2 STEP TWO 2 STEP THREE
		Enter Apple ID Certificate Summary
Ś		Push Certificate installed!
	Android Configuration	Valid from: 04-23-2015 15:58 Valid to: 04-22-2016 15:58
	Windows Configuration	Topic: com apple mgmt.External.9ebfd079-de15-4006-8ec2-c8d345cbb2ba
	ContentBox	Connection to Pushservice: successfull Remove API/S Certificate
	LDAP Configuration	Renew Push Certificate.
	App Management	1. Download this signedPushCertificate.txt
		2. Renew your current certificate at Apple Push Certificates Portal.
		3. You will get a .pem file. Upload the .pem file
		Choose your. PEM file
		Durchsuchen Keine Datei ausgewählt.
		Upload



<u>DEP</u>

Erleichtern Sie die Einführung eigener Geräte. Melden Sie Geräte während der Aktivierung bei AppTec an und überspringen Sie grundlegende Konfigurationsschritte, um den Benutzern die Geräte schneller und einfacher zur Verfügung zu stellen.

		< ►	APNS Certi	ficate	DEP	Configurator & URL					183. 1931 - 1932 - 1933 - 1933 - 1933 - 1933 - 1933 - 1933 - 1933 - 1933 - 1933 - 1933 - 1933 - 1933 - 1933 - 1933			
0		Imported	DEP Serve	er										0
曲	Global Configuration	Account N	ame	≎ Adr	nin Apple ID	\$ Organisation Name	\$	Status	\$ Expires in	\$ Devices	\$ Profiles	\$ Add Profile	Delete	Edit
13		Last synch	ronization:	2016-01	1-26 16:45:42									
2	Role Based Access	Sy	nchronize											
É	Apple Configuration	Full Auto	mation				n	one					~	0
	Android Configuration													

Mit dem "Plus Symbol" können Sie einen neuen DEP-Token hinzufügen, im Anschluss sehen Sie folgendes Fenster.

DEP Server			\times
Please upload a DEP-Token and the mai You can also issue a new certificate to c	tching certificate which was used to encrypt the token. create a new token using the Apple DEP Portal		
DEP Certificate	Click here to select or upload a file		0
DEP Token	Click here to select a file		0
Auto Profile	none	~	0
		Add DEP Server	

DEP Certificate	Hier müssen Sie Ihr DEP Zertifkat (PKCS12 Datei) welches Sie von Apple erhalten haben hochladen <u>Oder:</u> Die Console kann ebenfalls ein Zertifikat für Sie erstellen, indem Sie "new certificate" auswählen, dieses können Sie anschließend herunterladen und später im Apple DEP Portal hochladen.
	Hier müssen Sie Ihren DEP Token den
DEP Token	Sie von Apple erhalten hochladen
Auto Profile	Automatische Profilzuweisung



Rufen Sie nun das Apple DEP Portal auf und fügen einen neuen DEP Server hinzu.

Melden Sie sich im Apple Portal an und wählen "Device Enrollment Program" in der linken Spalte aus.

Deployment Programs Admins Device Enrollment Program Avolume Purchase Program	Welcome back,	
Ma	nage Servers	Add MDM Server
	No MDM Servers	



Tragen Sie nun einen beliebigen Namen ein und aktivieren Sie "Automatically Assign New Devices", damit neue, hinzukommende DEP Geräte automatisch mit dem Server synchronisiert werden.

Add M	DM Servei	r		
1. MDM S	erver Name.			
DEP Ser	ver			
Enter a na	ime to refer to t	his server, dep	artment or loc	ation.
Auto	matically Assigr	n New Devices	0	
		Cancel	N	lext

Laden Sie nun das Zertifikat (public Key), welches Sie im Vorfeld bereits über die Console heruntergeladen haben – sofern Sie auf der AppTec Console im Vorfeld "new certificate" gewählt haben – andernfalls laden Sie das gleiche Zertifikat hier hoch, welches Sie auch auf der AppTec Console verwendet haben.

Add "DEP Server"	
2. Upload Your Public Key.	
Choose File DEP_Credent	al
The public key certificate is used to Token file for secure transfer to you	encrypt the Authentication r MDM Server.
Previous Can	cel Next



Laden Sie an dieser Stelle das Token herunter. Im nächsten Schritt muss dieser Token in der AppTec Console hochgeladen werden.

Add "DEP Serv	ver"
3. Download and Inst	tall your Server Token.
P Your Server Toke	n
Contact your MDM ve	ndor for installation instructions.
Previous	Done

Gehen Sie nun zurück in die AppTec Console und laden Sie den eben heruntergeladenen Token bei "DEP Token" hoch.

DEP Server				>	<	
Please upload a DEP Token and the matc You can also issue a new certificate to cr	hing certificate which was used to encrypt the token eate a new token using the Apple DEP Portal					
DEP Certificate	DEP_Credential.p12(ID: 158)			•	0	
DEP Token	57	9.p7m	8		0	
Auto Profile	none			~	8	
			Add DEP Ser	ver		

Anmerkung: Sie können im Nachhinein zu diesem Punkt zurückkehren um den Punkt "Auto Profile" abzuändern. Nachdem Sie den Server hinzugefügt haben, können Sie diesen mit dem Zahnrad editieren.

Klicken Sie auf "Add DEP Server", um den Server hinzuzufügen.



In der Tabelle sollten nun Informationen über den eben hinzugefügten Server auftauchen. Wie in der Tabelle zu sehen, sind hier aktuell noch keine Geräte hinzugefügt.

Imported DEP Server												
Account Name 🗘	Admin Apple ID	Organisation Name	Status	¢	Expires in 🗘	D	Devices 🗘	P	Profiles 🗘	Add Profile	Delete	Edit
DEP Server	info@apptec360.com	AppTec GmbH	Active		365 days				0	0	•	*

Gehen Sie zurück in das Apple DEP Portal, hier sollte der vorhin hinzugefügte Server angezeigt werden.

Manage	e Servers		Add MDM Server
Server Name	Number of Devices	Last Connected 👻	Last Connected IP
DEP Server	0	Never	-

Wählen Sie "Manage Devices" in der linken Spalte aus.

C Deployment Programs	
Admins	
Device Enrollment Program	Manage Devices
Manage Servers	
[IIII], Manage Devices	1 Change Devices Dr.
View Assignment History	1. Choose Devices By:
A Volume Purchase Program	Serial Number Order Number Upload CSV File
Terms and Conditions	ABCD1234567, EFGHL0901234
	2 Choose Action
	Assign to Server



Fügen Sie nun ein Gerät dem Apple DEP Server hinzu und weisen Sie dieses dem eben erstellten Server zu.

1. Choose Devices	By:	
Serial Number	Order Number	Upload CSV File
2. Choose Action:		
Assign to Server	→ DEP Server	~

Sollte die Zuweisung erfolgreich gewesen sein, sollten Sie folgende Meldung im Nachhinein erhalten.

Assignment Complete
\checkmark
Please ensure your MDM server uploads a new profile before these devices are activated.
ОК



Anmerkung: DEP Profile sind unabhängig von einem MDM Profil. Diese ermöglichen zusätzliche Geräteeinstellungen, welche während der Aktivierung des Gerätes angewandt werden.

Um diese neuen Änderung auf das Gerät zu bringen, muss das Gerät zurückgesetzt (Werkseinstellungen) werden und die Aktivierung des Geräts muss erneut durchgeführt werden.

Gehen Sie zurück in die AppTec Console und klicken Sie auf "Synchronize", um die Daten des Servers zu erneuern.

Das neue Gerät sollte somit angezeigt werden.

Klicken Sie auf das Plus-Symbol in der "Add Profile" Spalte um ein DEP Profile hinzuzufügen.

Imported DEP Server										O					
Account Name \$	Admin Apple ID	¢	Organisation Name	¢	Status	¢	Expires in	¢	Devices	¢	Profiles 🗘	Add Profil	e	Delete	Edit
DEP Server	here the second second		AppTec GmbH		Active		365 days		1		0	Ο		•	*
Last synchronization: 2016-02-19 09:17:11 Synchronize															
Full Automation none ~										~	0				

Add DEP Profile		X
Profile Name	DEP Profile	0
Support Phone Number	0123456789	0
Support Email Address	example@example.com	0
Allow Pairing	он 🕥	0
Supervise Device	🕥 💮 On	0
Removable	Он	0
Mandatory	On On	0
Skip Passcode	On	0
Skip Registration	On	0
Skip Location	On	0
Skip Restore	On	0
Skip AppleID	On	0
Skip Terms and Conditions	On	0
Skip Biometric	On	0
Skip Payment	On	0
Skip Zoom	On	0
Skip Siri	On	0
Skip Diagnostics	On	0
Skip Android	On On	0
		Add DEP Profile

Nun erhalten Sie einen Popup mit diversen Optionen die Sie nach Bedarf einstellen und anpassen können.

Nachdem Sie die gewünschten Einstellungen vorgenommen haben, können Sie das Profil mit "Add DEP Profile" hinzufügen.



Profile Name	Name des Profils
Support Phone Number	Telefon-Nummer an die sich User bei
	Problemen wenden können
Support Email Address	Email-Adresse an die sich User bei
	Problemen wenden können
Allow Pairing	Erlaubt die Verbindung mit einem
	Computer
Supervise Device	Setzt das Gerät in den Supervised
	Mode
Removable	Erlaubt das Entfernen des Geräteprofils
Mandatory	Erzwingt das Enrollment des Geräts
Skip Passcode	Überspringt die Einrichtung des
	Passworts
Skip Registration	Überspringt die Geräte-Registrierung
Skip Location	Überspringt die Einrichtung des GPS
	Dienstes
Skip Restore	Überspringt die Wiederherstellung
Skip AppleID	Überspringt die Einrichtung der Apple ID
Skip Terms and Conditions	Überspringt die AGB
Skip Biometric	Überspringt die Einrichtung von Touch
	ID
Skip Payment	Überspringt die Einrichtung von
	Zahlungsmöglichkeiten
Skip Zoom	Überspringt die Einrichtung von Zoom
Skip Siri	Überspringt die Einrichtung von Siri
Skip Diagnostics	Überspringt die Einrichtung zum Senden
	von Diagnose-Informationen
Skip Android	Überspringt den Import von Android
Skip FileVault	Überspringt die Einrichtung von
	FileVault

Das Profil wird nun in der Tabelle "Profiles" angezeigt bzw. wird Zähler um eins erhöht. Sie können Sie jedoch nicht bearbeiten, ausschließlich entfernen. Sofern ein Profil einem Gerät zugewiesen ist, kann das Profil nicht entfernt werden.

Imported DEP Server										0		
Account Name \$	Admin Apple ID	Organisation Name	Status	Ŷ	Expires in		Devices	\Diamond	Profiles 🗘	Add Profile	Delete	Edit
DEP Server	100 B (0.00	AppTec GmbH	Active		365 days	1	1		1	0	•	*
Last synchronization: 2016-02-19 09:17:11 Synchronize												
Full Automation none ~										\sim	0	



Möchten Sie das Profil entfernen, können Sie dies mit dem Minus-Symbol oben rechts tun.

Sie können die Zahl anklicken, um alle Profile aufgelistet zu bekommen.

DEP Profiles	\times
DEP Profile UUID: D9237C7BD846679714020325E0D81EC0 skip_setup_items: [Passcode, Registration, Location, Restore, AppleID, TOS, Biometric, Payment, Zoom, Siri, Diagnostics, Android, FileVault] org_magic: 558007C2-B086-C0EB-6122-0CBC3542ADED url: https://www.emmconsole.com:8080/enroll/dep allow_pairing: yes is_supervised: yes is_mandatory: yes is_mandatory: yes is_mdm_removable: yes support_phone_number: 0123456789 support_email_address: example@example.com	0

Kehren Sie zurück zum Mobile Management und laden Sie die Seite neu. Eine Kategorie "Pool" wird aufgelistet, in dieser befindet sich Ihr DEP Gerät. Klicken Sie auf "DEP" – hier können Sie nun alle DEP Geräte anhand der Seriennummer sehen.

In der User-Spalte können Sie nun die gewünschte E-Mail-Adresse des Users, welches das Gerät erhalten soll, hinterlegen.

In der DEP Profile-Spalte wählen Sie das vorhin erstelle Profil aus.

Sie können ebenfalls eine CSV Datei importieren, um diese Einstellungen vorzunehmen. Um eine Vorlage zu erhalten, können Sie auf "Export CSV" anklicken.

▶					
🔺 🚞 Pool	DEP Serv	er	Export CSV	Import CSV 🗸 🗸	
🔺 🚞 DEP		Serial \$	User	DEP Profile	•
ABCD1234567		ABCD1234567	example@example.com	DEP Profile	~

Sie können die Änderungen ebenfalls für mehrere DEP Geräte vornehmen, indem Sie die Checkbox neben dem Gerätename / Seriennummer anklicken.

Um alle Geräte auszuwählen, können Sie die Checkbox in der ersten Spalte neben "Serial" auswählen.

DEP Serv	ver	Export CSV	Import CSV 🗸 🗸	
×	Mass Assignment +	none	none	~
×	ABCD1234567	example@example.com	DEP Profile	~

Nachdem Sie Ihre Anpassungen erledigt haben, klicken Sie auf "Save & Assign" unten rechts, um die Änderungen zu speichern.



Configurator & URL

An dieser Stelle können Sie das Enrollment für iOS Geräte deutlich vereinfachen. Die Geräte müssen somit nicht direkt einem User zugewiesen werden, sondern werden lediglich als Pool Gerät in der AppTec Console erfasst.

		_			Debity Management		_
		APNS Certificat	e DEP	Configurator & URL			👤 support@milanconsult.de 🗸
0	Account Overview	Pool Enrollment URL's					G
虚	Global Configuration	URL	Expiry date		Remaining enrollments		
8	Privacy						
2	Role Based Access	MDM Profile - Apple Con	figurator	40-24			
ú	Apple Configuration	Create New	Dow	mload			
	Android Configuration						
-	Windows Configuration	i Please make sure yo	I keep the mobile cor	nfig file private, as everyone	who can use the file can enroll devic	es into the mdm without credentials.	
6	ContentBox						
do.	LDAP Configuration						
止.	Universal Gateway						
8	App Management 🗸						

Pool Enrollment URL's

Generieren Sie sich eine neue URL indem Sie auf das Plus-Symbol oben rechts klicken.

Somit erhalten Sie folgenden Popup.

Create Pool Url	X
Enter number of possible enrollments	0
Enter Expiry Date	0
	create

Enter number of possible enrollments	Anzahl wie oft mit dieser URL eine
	Gerät enrolled werden kann
Enter Expiry Date	Datum wann die Enrollment-URL
	ungültig ist



Create Pool Url		X
Enter number of possible enrollments	1	0
Enter Expiry Date	03/09/2016	
		create

Nachdem Sie auf "create" geklickt haben, sollten Sie eine ähnliche Ansicht wie im folgenden Screenshot zu sehen erhalten.

Pool Enrollment URL's			0
URL	Expiry date	Remaining enrollments	
https://www.emmconsole.com:8080/enroll/pool/1d8c438ec96d9ad9	04/06/2016	5	•

Somit können Sie diese URL an Ihrem iOS Gerät im Safari Browser aufrufen und gelangen direkt zur Profil-Installation.

Nachdem Sie diese abgeschlossen haben, werden Sie im Mobile Management auf der AppTec Console folgende Übersicht erhalten.



Das Gerät sollte in Kürze grün markiert werden. Nun können Sie nach Belieben das Gerät per Drag & Drop verschieben.



MDM Profile – Apple Configurator

Klicken Sie auf "Create New" um sich eine neue ".mobileconfig" Datei zu erstellen oder laden Sie sie – sofern Sie bereits eine mobileconfig Datei erstellt haben mit "Download" runter.

					360 Inagement	
		APNS Certificate	DEP	Configurator & URL		support@milanconsult.de 🗸
0	Account Overview	Pool Enrollment URL's				θ
曲	Global Configuration	URL	Expiry date		Remaining enrollments	
13	Privacy					
2	Role Based Access	MDM Profile - Apple Confi	gurator			
É	Apple Configuration	AppTec Mobileconfig File crea	ted at: 03/24/2016 13:49:	21		
.	Android Configuration					
-	Windows Configuration	1 Please make sure you	keep the mobile config	file private, as everyone who c	an use the file can enroll devices into the mdm	without credentials.
6	ContentBox	-				
20	LDAP Configuration					
止.	Universal Gateway					
8	App Management 🗸 🗸					

Bestätigen Sie folgenden Dialog mit "Datei speichern".

	Standard Charles Contention Contention Contention (Contention)	`
Create Ne Create Ne Please make su	Sie mochten folgende Datei offnen: [^] AppTec_EMM_Profile.mobileconfig Vom Typ: Text Document (10,1 KB) Von: https://www.emmconsole.com Wie soll Firefox mit dieser Datei verfahren? <u>Ö</u> ffnen mit <u>Durchsuchen</u> <u>Ö</u> dffnen mit <u>Durchsuchen</u> <u>Ö</u> Datei <u>sp</u> eichern <u>F</u> ür Dateien dieses Typs immer diese Aktion ausführen	enroll devices into the mdm without credenti
	OK Abbrechen	



Rufen Sie nun an Ihrem Mac den Apple Configurator auf und schließen Ihr gewünschts iOS Gerät per USB Kabel an Ihren Mac an – Sie werden folgendes Schaubild erhalten.



Tätigen Sie nun einen Rechtsklick auf das Gerät, wählen Sie "Hinzufügen" und anschließend "Profile …" aus.





Wählen Sie nun das vorher erstellte bzw. heruntergeladene Profil aus und klicken Sie auf "hinzufügen".



Sie werden nach kurzer Zeit folgende Übersicht erhalten. Sie werden nun am Endgerät aufgefordert die Profilinstallation durchzuführen.





Gehen Sie wie in folgenden Screenshots die Profil-Installation durch.





Nachdem Sie die Profilinstallation erfolgreich abgeschlossen haben, können Sie das Gerät im Mobile Management sehen und nun per Drag & Drop nach Belieben verschieben.



Android Configuration

Android Configuration

	Wenn diese Funktion aktiviert ist, kann der User den Geräteadministrator nicht ohne das vom Admin festgelegte Passwort deaktivieren und damit die Apptec App nicht entfernen. Das Passwort wird beim Einrollen festgelegt und kann nur durch erneutes einrollen aktualisiert werden.
	Für das Entfernen des Geräteadministrators gibt es zwei verschiedene Optionen:
	a. Manuell an Endgerät öffnen \rightarrow FMM Ann auf dem Endgerät öffnen
	→ Status
	\rightarrow Uninstall Protection anklicken
	→ Passwort eingeben
Uninstall Protection	Mit Hilfe der angezeigten Revision finden Sie in der Konsole bei "Password History" das richtige Passwort.
	→ Nun auf den neu hinzugekommenen Punkt "Tap to uninstall AppTec MDM App" anklicken (hierfür haben Sie 20 Sekunden Zeit)
	→ Den Dialog "Uninstall AppTec MDM App" mit "ok" bestätigen.
	Das Gerät wird nun ausgerollt.
	→ Anschließend können Sie die App über den Dialog "AppTec MDM wird deinstalliert" entfernen
	b. Automatisch über die Console
	 → Führen Sie über das Zahnradmenü den "Enterprise Wipe" durch
	Hinweis: Nur bei Android 4.x und niedriger oder mit Geräten mit der SAFE API verfügbar



Uninstall Password (Revision x)	Das festgelegte Passwort, womit der User den Geräteadministrator entfernen kann Revision x = Zähler, wie oft das Passwort bereits verändert wurde Wichtig welches Passwort der User benötigt, da evtl. das Gerät sich seit einer gewissen Zeit nicht mehr beim AppTec Server gemeldet hat und somit das aktuellste Passwort noch nicht übertragen wurde
Password History	Wenn Sie auf den blauen Button klicken ("Show History"), sind Sie in der Lage alle bereits definierten Passwörter einzusehen
Extended Uninstall Protection	Diese Option bietet einen Schutz für nicht-SAFE Geräte Sofern diese Einstellung aktiviert ist, ist es nicht möglich den Geräte Administrator ohne weiteres zu deaktivieren

	Android Configuration		🧕 support@milanconsult.de 🗸
Account Overview	Uninstall Protection		0
Global Configuration	Uninstall Password (Revision 1)	mian	0
🧱 Privacy	Password History	Show History	0
Apple Configuration	Extended Uninstall Protection	Сон 🌑	0
Android Configuration	-		
Windows Configuration			
ContentBox			
LDAP Configuration			
App Management			

Auto Enrollment

Hier können Sie das Auto Enrollment aktivieren, womit sich ihr Gerät automatisch einrollt wenn Sie die Apptec App öffnen

Enable Auto Enrollment	Wenn aktiviert, rollt sich ihr Gerät automatisch ein, wenn dessen Seriennummer oder IMEI auf der Whitelist steht.
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 Enterprise

Hier können Sie Android Enterprise einrichten. Dies ist notwendig um die Funktionen von Android Enterprise zu verwenden.

Methode 1: Android Enterprise Account (Google Account)

Klicken Sie auf "Prepare Setup", nach einem kurzen Moment sollte dort stattdessen der Button "Start Setup" sein. Dieser bringt Sie auf Googles Setup-Seite für Android Enterprise.

Loggen Sie sich mit dem Google Account ein den Sie nutzen wollen, sofern Sie nicht bereits eingeloggt sind und drücken Sie "Get started".



Geben Sie nun ihren Firmennamen ein. Bestätigen Sie danach die Android Enterprise Agreement und klicken auf "Confirm"

Organisation name

Max Muller Company

Enterprise mobility management (EMM) provider

AppTec Enterprise Mobile Manager

☑ I have read and agree to the <u>Android for</u> <u>Work agreement</u>.

PREVIOUS





Im letzten Schritt beenden Sie die Registrierung und kehren automatisch zur Konsole zurück. Sollte alles geklappt haben, sieht es ungefähr so aus auf der Konsole:

Android for Work Status AppTec MDM is now ready to use Android for Work

Jetzt können Sie damit beginnen den Android Enterprise Container für Ihre Geräte einzurichten.

Methode 2: G-Suite Account

Klicken Sie auf "Use G-Suite" und loggen Sie sich in Ihren Google Admin Account ein. Gehen Sie hier zu "Sicherheit -> "Mehr anzeigen" -> " EMM-Anbieter für Android verwalten" und generieren Sie ein Token. Hinweis: Wenn Sie Android Enterprise Einstellungen in Ihrem G-Suite Account nicht sehen, müssen Sie unter "Weitere Apps und Dienste" Android Geräteverwaltung aktivieren. Nun geben Sie den Token und ihre primäre Domain in der Konsole ein und klicken auf "Save Changes". Wenn Sie fertig sind, klicken Sie auf "Use Android Enterprise Account".

Jetzt sehen Sie den "Create Service Account" Button. Klicken sie auf diesen Button. Dieser Vorgang kann einige Zeit beanspruchen.

Sollte alles geklappt haben, sieht es ungefähr so aus auf der Konsole:

```
Android for Work Status
AppTec MDM is now ready to use Android for Work
```

Jetzt können Sie damit beginnen den Android Enterprise Container für Ihre Geräte einzurichten.



AE Enrollment

Hier können Sie das Android Enterprise Enrollment aktivieren. Hiermit rollen Sie Ihre Geräte in den <u>Android Enterprise Device Owner Mode</u> ein. Anders als beim Android Enterprise Container haben Sie hier die volle Kontrolle über das Gerät.

Enable AE Enrollment	Aktiviert das AE Enrollment. Vorsicht: Wenn den Schalter einmal auf "Off" stellen, werden alle generierten QR Codes und NFC Geräte unbenutzbar. Danach müssen sämtliche QR Codes und NFC Geräte neu generiert werden!
Enable Auto Discover	Verwendet beim AE Enrollment die Auto Discover Zuweisung des Auto Enrollments
Block Unknown Devices	lst diese Option aktiv, werden nur Geräte, welche in der Auto Enrollment Liste eingetragen sind, akzeptiert.

<u>Hinweis zu Methode 1 & 2</u>: Mit "Willkommen" Bildschirm ist grundsätzlich die erste Ansicht nach dem Zurücksetzen gemeint. Diese Ansicht kann sich je nach Android Version und Gerätemodell sehr unterscheiden.

Methode 1: QR Code Enrollment

(benötigt Android 7.0 oder höher)

- 1. Setzen Sie das Gerät auf Werkseinstellungen zurück.
- 2. Generieren Sie den QR Code für das Enrollment auf eine der folgenden Arten:
 - a. Klicken Sie in "General Settings -> Android Configuration -> AE Enrollment" auf "Generate QR Code". Wählen Sie hier aus, ob eine Verschlüsselung des Gerätespeicher durchgeführt werden soll und ob Sie die System Apps behalten wollen.
 - b. (Alternativ) Wählen Sie ein existierendes Gerät. Klicken Sie dort in der "Device Overview" auf den QR Code. Wählen Sie hier aus, ob eine Verschlüsselung des Gerätespeicher durchgeführt werden soll und ob Sie die System Apps behalten wollen.
- 3. Tippen Sie nun 6 mal auf den "Willkommen" Bildschirm des Gerätes um es in den QR Code Enrollment Modus zu bringen.
- 4. Verbinden Sie sich jetzt mit einem WLAN und warten einige Momente
- 5. Scannen Sie nun den QR Code
- 6. Fertig. Ihr Gerät ist nun im Android Enterprise Device Mode eingerollt
 - a. Wenn Sie den QR Code in den General Settings benutzt haben, finden Sie Ihr Gerät nun unter "Pool -> AE Device Owner Devices" (Info: Es ist möglich, dass Sie die Seite neu laden müssen, damit Sie das Gerät sehen). Wenn Sie "Enable Auto Discover" aktiv haben, finden Sie Ihr Gerät bei dem hierbei konfigurierten Nutzer.



b. Wenn Sie den QR Code direkt in einem Geräteprofil verwendet haben, wird das Gerät direkt auf dieses Profil eingerollt.

Methode 2: NFC Enrollment

(Benötigt NFC und Android 6.0 oder höher)

Vorbereitung: Hinterlegen Sie Ihre WLAN Daten unter "General Settings -> Android Configuration -> AE Enrollment -> Data for NFC provisioning". Suchen Sie dann unter "NFC Device" Ihr gewünschtes Admin Gerät. Dieses Gerät wird dann per NFC die Informationen an die weiteren Geräte weitergeben.

- 1. Setzen Sie Ihr Gerät auf Werkseinstellungen zurück
- 2. Bleiben Sie auf dem zurückgesetzten Gerät auf dem "Willkommen" Bildschirm
- 3. Öffnen Sie auf Ihrem Admin Gerät die NFC Pairing App von AppTec
- 4. Wählen Sie hier aus, ob eine Verschlüsselung des Gerätespeicher durchgeführt werden soll und ob Sie die System Apps behalten wollen.
- 5. Halten Sie dann die beiden Geräte Rücken an Rücken
- 6. Nun sollte der Android Enterprise Enrollment Prozess auf dem Gerät starten
- 7. Sie finden Ihr Gerät dann
 - a. Im Pool, sofern Sie kein Auto Discover nutzen
 - b. Bei dem User, den Sie via Auto Discover hinterlegt haben
 - c. Hinweis: Es ist möglich, dass Sie die Seite neu laden müssen, damit Sie das Gerät sehen

Methode 3: Google Account

Wichtig: nutzen Sie diese Methode NUR auf Geräten mit Android 5. Nutzen Sie sonst IMMER die andere Methoden!

(Benötigt Android 5.1 oder höher)

(Hinweis: Bei der Verwendung dieser Methode wird, anders als bei Methode 1 & 2, das Gerät nicht automatisch eingerollt. Sie müssen nach dem initialen Setup das Gerät händisch einrollen oder diesen Vorgang via Auto Enrollment automatisieren)

- 1. Setzen Sie Ihr Gerät auf Werkseinstellungen zurück
- 2. Richten Sie Ihr Gerät soweit ein, bis Sie einen Google Account hinterlegen können
- 3. Geben Sie hier beim Nutzernamen/E-Mail "AE#apptec" ein
- 4. Tippen Sie auf "Weiter"
- 5. Ihr Gerät befindet sich nun im Android Enterprise Device Owner Mode



KNOX Enrollment

Hier können Sie das KNOX Enrollment aktivieren und die Informationen einsehen, die Sie benötigen um im KNOX Deployment Portal ein Enrollment Profil anzulegen. Hinweis: Sie benötigen einen Account beim Samsung KNOX Enrollment Programm (https://www.samsungknox.com/en/knox-deployment-program)

Enable KNOX Enrollment	Aktiviert das KNOX Enrollment. Vorsicht: Wenn den Schalter einmal auf "Off" stellen, wird das Enrollment Profil unbrauchbar. Sie müssen es danach mit dem neuen Eintrag aus "Custom JSON Data" aktualisieren oder ein neues anlegen.	
Enable Auto	Verwendet beim KNOX Enrollment die Auto Discover Zuweisung	
Discover	des Auto Enrollments	

- 1. Loggen Sie sich im Samsung KNOX Mobile Enrollment ein <u>https://eu-kme.samsungknox.com/itadmin</u>
- 2. Gehen Sie zu "MDM Profiles"
- 3. Klicken Sie auf "Add"
- 4. Wählen Sie "Server URI not required for my MDM" und klicken auf "Next"
- 5. Erstellen Sie nun ein Profil mit den Informationen, welche in der Konsole angezeigt werden.

Nun können Sie dieses KNOX Enrollment Profil direkt auf die Geräte aufspielen lassen, wenn Sie die Geräte bei Samsung erwerben.

Alternativ können Sie die KNOX Deployment App herunterladen, mit Ihrem KNOX Deployment Account einloggen und per NFC das Profil an ein anderes Gerät senden.

Wenn das Gerät ein KNOX Enrollment Profil erhalten hat, wird es bei einer bestehenden Internetverbindung automatisch unsere App herunterladen und sich einrollen.

Geräte die per KNOX Enrollment eingerollt werden, finden Sie unter "Pool -> KNOX Enrollment", sofern Sie für das Gerät kein Auto Discover nutzen.

1.



Windows Configuration

Windows Configuration

Hier sind Sie in der Lage folgende Konfigurationen für Ihr Windows Phone zu tätigen:

Instant DM Connection	
Initial Retry Time	Legt den Intervall für den ersten Verbindungsversuch zum Gerät fest, dieser Wert steigt exponentiell
Connection Retries	Gibt an, wie viel Verbindungsversuche der DM- Client unternehmen soll bei einem Verbindungsfehler
Maximum Sleep Time	Gibt die maximale Ruhezeit nach einem Verbindungsfehler an
First Sync Retries	Häufigkeit, wie oft sich das Gerät nach dem ersten einbinden beim Server melden soll
First Retry Interval	Bezieht sich auf "First Sync Retries", hier wird die Zeit in Minuten angegeben z.B. wird unter "First Sync Retries" der Wert "2" eingetragen und bei "First Retry Interval" der Wert "4 Minuten", somit meldet sich das Gerät nach dem ersten Einbinden 2 Mal alle 4 Minuten
Second Sync Retries	Häufigkeit, wie oft sich das Gerät nach Abwicklung des "First Sync Retries" beim Server melden soll
Second Retry Interval	Selbes Prinzip wie für "First Retry Interval" – nur dass es hier selbstverständlich für "Second Sync Retries" gilt
Regular Sync Retries	Häufigkeit, wie oft sich das Gerät für die Zukunft am Server melden soll Standard: "Infinite" Wir empfehlen diesen Wert nicht zu ändern, falls Sie hier nämlich z.B. "10" eintragen, wird sich das Gerät 10x am Server melden und anschließend nicht mehr Somit bricht eine Verbindung zum AppTec Server ab!
Regular Retry Interval	Selbes Prinzip wie für "First/Second Retry Interval" – nur dass es sich hierbei um die Einstellung für die Zukunft handelt

		•	Windows Configuration		support@milanconsult	de 🗸
			Instant DM Connection	(on		0
	Global Configuration		Initial Retry Time	15 Seconds	~	0
			Connection Retries	10	~	0
	Apple Configuration		Maximum Sleep Time	4 Hours	~	0
	Android Configuration		First Sync Retries	10	~	0
-	Windows Configuration	2	First Retry Interval	2 minutes	~	0
	ContentBox		Second Sync Retries	10	~	0
	LDAP Configuration		Second Retry Interval	5 minutes	~	0
	App Management 🗸 🗸		Regular Sync Retries	10	~	0
			Regular Retry Interval	4 Hours	~	0





Content Box

Configuration

Unter diesem Punkt können Sie die ContentBox konfigurieren.

Die ContentBox können Sie sich wie eine Enterprise Dropbox vorstellen.

Enable ContentBox	ContentBox aktivieren		
	Die ContentBox kann ebenfalls mit		
Use external ContentBox	ihrem eigenen ownCloud 7 Server		
installation	betrieben werden		
URL	Vollständige URL der OwnCloud		
	Instanz		
Root User	Root User des owncloud Accounts		
Root Password	Root Passwort des ownCloud 7		
	Accounts		
	Standardberechtigung für eine		
Default group folder permissions	Gruppe, kann individuell je Gruppe		
	geändert werden (im Mobile		
	Management)		
	Wenn aktiv, kann jede Untergruppe		
Share group folder with	alle Ordner der Hauptgruppe lesen,		
subgroups	kann ebenfalls individuell für jede		
	Gruppe angepasst werden (Mobile		
	Management)		
	Berechtigung für die Untergruppe		
	read = lesen		
	write = schreiben		
Permissions for subgroups	delete = löschen		
	Kann je Gruppe individuell		
	eingestellt werden (Mobile		
	Management)		
Allow sharing	Erlaubt es dem User den Inhalt via		
	Links zu teilen, kann individuell für		
	jede Gruppe eingestellt werden		
	Maximale Größe einer Datei		
Maximum File Upload Size in MB	Standard: 512 MB		
	Maximal einstellbar: 2048		
WebDAV Credentials			
	Sie können Ihre ContentBox auch		
	mit WebDav aufrufen.		
	Löschen Sie bitte auf keinen Fall		
WebDAV URL	folgende Ordner:		
	/apptecgroups		
	/apptecgroups/AppTecGroup-X		
Root User	Name des Root Users		



Password	Passwort des Root Users
----------	-------------------------

Die Synchronisation mit der ContentBox erfolgt automatisch, Sie können hier aber zusätzlich mit "Synchronize ContentBox" eine manuelle Synchronisation der ContentBox durchführen.

Ebenfalls können Sie für jedes einzelne Gerät die ContentBox hier deaktivieren bzw. aktivieren.

Dies ist nur dann relevant, wenn Sie die ContentBox nicht zusätzlich lizenziert haben, Ihnen stehen dann dennoch 25 Geräte zur Verfügung um die ContentBox teste zu können – hier können Sie dies für die jeweiligen Geräte aktivieren.

Last sy	nchronization: 2015-06-2	2 13:49:35			
Syn	chronize ContentBox				
You dor	n't have a subscription for	the AppTec ContentBox. Your ContentBox access	is limited to 25 devices.		
Contac Select t	t sales@apptec360.com the 25 devices that can ad	to purchase a license for all your devices ccess the ContentBox			
#	\$	Device	≎ os ≎	Type 🗘	Owner 🗘
1	On On	Device of Fabian	iOS	Tablet	Fabian Kola
2	On On	Device of Matthias	Android	Phone	Matthias
3	On	Device of Michael	iOS	Phone	Michael
4	On	Device of Michael	iOS	Tablet	Michael
5	Оп	Device of Martina	iOS	Phone	Martina
6	On On	Device of Yasemin	ios	Phone	Yasemin
7	On On	Device of Michael	iOS	Phone	Michael
8	On On	Device of Tanja	Android	Phone	Tanja l
9	On 🕙	Device of Fabian	iOS	Tablet	Fabian
10	On On	Device of Lukas	iOS	Tablet	Lukas
11	On	Device of Daniel	Android	Phone	Daniel
12	On	Device of Fabian	iOS	Tablet	Fabian



LDAP Configuration

LDAP Overview

Sollte Ihr Active Directory extern erreichbar sein oder Sie sich für die On-Premise Variante von AppTec entschieden haben, können Sie hier einen LDAP Import vornehmen.

Dies erfolgt über das im Screenshot markierte "Plus Symbol".



Geben Sie Ihre Active Directory Daten an und klicken Sie auf "Add LDAP Server":

Add LDAP Server		\times
Server Name		
Туре	Active Directory	
Host Domain		
Host Address		0
Port		0
Username		0
Password		
Repeat password		
Connection Security	● No Encryption	
Base DN		0
Member of	milan	~ @
Check users for valid eMail ?	Off	0
Only activated users?	Off	0
Filter by Attributes ?		0
Test connection ?	On On	0
	Add LDAP	Server


Sollte dies erfolgreich gewesen sein, erhalten Sie folgende Ansicht:

		P Ove	erview									2	support@	milancons	ult.de 🗸
0	Imported Dire	ctor	ies												0
畿	Server Name	0	Host / Domain	0	Base Node	¢	Member of	¢	Last Sync	0	Status	\$ Delete	Edit	Sync	Logs
1	LDAP milan		101000		DC=milan,DC=local		Default Group		17-04-2015 13:28		Successful	0	\$	•	

Delete	LDAP Server entfernen
Edit	LDAP Server bearbeiten
Sync	Synchronisation des LDAP Servers
Logs	Ausgabe von LDAP Logs

Universal Gateway

Stellen Sie sich vor, dass Sie beim Einrichten von E-Mail bei Smartphones und Tablets nie wieder ein Passwort eingeben müssen und Sie sicherstellen können, dass nur Geräte, welche mit AppTecs Mobile Device Management gemanaged werden, Zugang zu Ihrem E-Mail Server erhalten.

Genau das wird mit AppTecs Universal Gateway sichergestellt.

Das ist eine enorme Steigerung der Sicherheit und eine starke Vereinfachung für die Mitarbeiter bei der Ersteinrichtung der mobilen Geräte durch das Mobile Device Management von AppTec.

Bei Interesse kontaktieren Sie uns via sales@apptec360.com



App Management

In-House App DB

<u>Android</u>

Hier können Sie Ihre eigenentwickelten Android Apps über das "Plus Symbol" hochladen und später im Mobile Management verteilen.



Mit "Durchsuchen..." können Sie die .apk Datei auswählen und mit "Upload" hochladen.



Upload an In-House App	\times
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

		< ►	Android	iOS	Windows			👤 support@milanconsu	ult.de 🕤	Ļ
0	Account Overview		Application N	Name O	Version O	Version Code 🗘	Size 0	Package Name	0	
此	Global Configuration	.	IBM Notes	Traveler	9.0.1.3 201411210833-T7.1.0.0.52-27!G	1416593443	6.32 MB	forgepond.com.lotus.sync.traveler	٥	



<u>Update Target</u>

Mit der Funktion "Update Target" wählen Sie, welche Version der App installiert wird bzw. auf welche Version aktualisiert wird, sofern die Funktion "Keep up to date" für eine App aktiv ist.

Sollte "Keep up to date" für eine App aktiv sein, aber kein Update Target gesetzt sein, wird automatisch die neuste Version als Update Target verwendet.

<u>i0S</u>

Hier können Sie Ihre eigenentwickelten iOS Apps über das "Plus Symbol" hochladen und später im Mobile Management verteilen.



Mit "Durchsuchen..." können Sie die .ipa Datei auswählen und mit "Upload" hochladen.

Upload an In-House App	\times
Upload Limit: max. size of ipa files is 64 MB	
Select the .ipa file of the iOS application which you want to upload	
Durchsuchen Keine Datei ausgewählt.	
	Upload





<u>Update Target</u>

Mit der Funktion "Update Target" wählen Sie, welche Version der App installiert wird bzw. auf welche Version aktualisiert wird, sofern die Funktion "Keep up to date" für eine App aktiv ist. Sollte "Keep up to date" für eine App aktiv sein, aber kein Update Target gesetzt sein, wird automatisch die neuste Version als Update Target verwendet.

<u>Windows</u>

Hier können Sie Ihre eigenentwickelten Windows Phone Apps über das "Plus Symbol" hochladen und später im Mobile Management verteilen.

			ios	Windows						support@milanco	nsulto	de 🗸
0		Application Name			¢	Version	0	Size	\$ Package Name		\$	0
ß												
6												
Ś												
٠												
-												
Ĩ.												
品												
6												
	in-House App DB											
	Black- & Whitelisting											
1.78												

Mit "Durchsuchen..." können Sie die .xap Datei auswählen und mit "Upload" hochladen. Diese Dateien müssen jedoch unsigniert,



ansonsten ist ein Upload nicht möglich.

Upload an In-House App	X
Upload Limit: max. size of xap files is 64 MB Select the .xap file of the windows phone application which you want to uplo Durchsuchen Keine Datei ausgewählt.	bad
	Upload



Black-& Whitelisting

<u>Android</u>

Hier können Sie festlegen, ob Sie mit einem White- oder Blacklisting arbeiten möchten.

Whitelisting	Nur bestimmte Apps sind erlaubt, alle anderen Apps sind nicht installierbar / ausführbar
Blacklisting	Bestimmte Apps sind verboten, alle anderen sind installierbar / ausführbar
Prompt the user to uninstall blocked apps?	Den User dazu auffordern, verbotene Apps zu deinstallieren. Bei SAFE findet dies automatisch statt.
Intelligent Sys App Blocking	Wenn "whitelisting" aktiviert ist, werden mit dieser Funktion alle System-Apps deaktiviert





<u>Apple</u> Choose between App Black- and Whitelisting

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



<u>Windows</u>

Whitelisting	Nur bestimmte Apps sind erlaubt, alle anderen Apps sind nicht installierbar / ausführbar
Blacklisting	Bestimmte Apps sind verboten, alle anderen sind installierbar / ausführbar

		• •	Android	Apple	Windows		🧕 support@milanconsult.de 🗸
		Applicat	on Restriction Pol	icy		Blackisting	0
						 Writelisting 	
J.	LDAP Configuration						
8							
	Black- & Whitelisting						
1	App Store						



Third Party Apps

<u>Android</u>

Falls der native Mail Client unter Android nicht unterstützt wird, können Sie hier die 3rd Party App "TouchDown" aktivieren.

Diese können Sie anschließend unter "Mobile Management" > "PIM Management" > "Touchdown Exchange" konfigurieren.



können Sie Ihre SecurePIM Lizenz eintragen. Nach dem Eintragen können sie via "Save Changes" speichern und die SecurePIM Optionen nutzen.

VPP / KNOX

Das Volume Purchase Program (VPP) von Apple erlaubt es Ihnen Unternehmenslizenzen für Apps zu erwerben.

Nach dem Erwerb sind Sie in der Lage die Lizenz für bestimmte User zu verteilen, diese können die App dann kostenlos auf dem Endgerät installieren.

Sollte die App auf einem Endgerät deinstalliert werden, bekommen Sie diese Lizenz wieder gut geschrieben und können diese erneut an einen anderen User verteilen.

Samsung Geräte können KNOX nutzen, sofern die Geräte es unterstützen und Sie einen gültigen Lizenzschlüssel besitzen.

Mit KNOX können zwei unterschiedliche Profile auf dem Endgerät betrieben werden und somit private und geschäftliche Dateien voneinander abzugrenzen.

<u>VPP Token</u>



Hier können Sie Ihren erworbenen VPP Token hochladen, indem Sie auf "Click here to select a file" klicken.

Vergessen Sie anschließend nicht mit "Save" das Ganze abzuspeichern.

	Ken Knox Key VPP Licenses		support@milancon	sult.de	~
Account Overview Token		1d86c49b825a377cea2fa9bd3ddfef88.vpptoken	8	6	3
Global Configuration Automated Licens	e Management	On)		G	3
VPP mode		Device Mode	~	A 6	3
Role Based Access Expire Date: 2017-	03-21T07:21:53-0700				
Apple Configuration Organisation: milar	consult GmbH				
Android Configuration					
Windows Configuration					
ContentBox					
LDAP Configuration					
Universal Gateway					
App Management					
n-House App DB					
Black- & Whitelisting					
Third Party Apps					
VPP / KNOX					
App Store					
T _l					
Token	Inr nochgeladene				
Automated	Damit wird die au	itomatische Lizenzverwal	tung akti	vie	rt
License	lst dies der ⊢all,	so werden bei Bewegen e	es		
Management	Benutzers/Geräte	es in eine andere Gruppe			
	entsprechende V	PP Lizenzen des Gruppe	nprofils		
	automatisch zuge	ewiesen			
	Bereits vorher ins	stallierte Apps/Lizenzen w	verden ni	cht	[
	zurückgezogen,	dies muss manuell im Na	chhinein		
	geschehen				
VPP mode	User Mode: VPP	Lizenzen werden einer A	vple-ID		
	zugewiesen. Auf	diese Weise kann die Liz	enz/App	au	f
	mehreren Geräte	en mit der gleichen Apple	ID		
	verwendet werde	en.			
	Device Mode: VF	PP Lizenzen werden direk	t einem		
	Gerät zugewiese	n			
	Dadurch wird auf	 diesem keine Annle-ID h	enötiat u	Ind	
	es ist nicht notwe	andia den Ann Store	Shouge u	u	
		a zu heetätigen (nur iOS	Q und bö	she	r)
				2110	')
	Achtung: Ein Äng	lorn diocor Einstellung ha	bt allo		
	historiase VDD	lerin uleset Ettistetturiy He			
			Hate aut.		
	Sotern Sie dies v	vunschen, bestatigen Sie	ales ube	er	
	einen Klick auf d	as Schloss.			

Das Ablaufdatum des VPP Tokens können Sie über "Expire Date" einsehen. Vor Ablauf muss das VPP File entsprechend erneuert werden. Die Firma, auf welche das Token ausgestellt ist, wird in dem Feld "Organisation" angezeigt.



<u>Knox Key</u>

Hier können Sie Ihren erhaltenen Samsung KNOX-Key einspielen.

KNOX License Key	Hier den KNOX-Key eingeben.



VPP Licenses

Sofern Sie einen VPP-Account definiert haben, erhalten Sie auf dieser Seite einen Überblick über Ihre erworbenen VPP-Apps.

\$	App Name 🔷	Version 🗘	Price 🗘	Assign Status	Total 🗘	Free 🗘 🗘
4	Evernote	6.0.15	free	Assigned	100	100
<u></u>	GoodReader for Good	4.8.0	free	Assigned	1	1

App Name	Name der App
Version	Aktuelle Version der App
Price	Ursprünglicher Preis der App
Assign Status	Zuweisungsstatus der App
Total	Gesamtanzahl an Apps
Free	Noch frei verfügbare Apps

App Store

<u>Region</u>

Default search region for iTunes Store apps.	Festlegung darüber, welcher iTunes Store (Apple Apps) als Standard bei der Suche benutzt werden soll.
Default language for searching apps in Android Play Store.	Festlegung darüber, welcher Google PlayStore (Android Apps) als Standard benutzt werden soll.
Default language for searching apps in Windows Store.	Festlegung darüber, welcher Windows Phone Store (Windows Phone Apps) als Standard benutzt werden soll.

		Region		📃 support@milanconsult.de 🗸
0		Default search region for iTunes Store apps.	Germany	~
戯	Global Configuration	Default language for searching apps in Android Play Store.	German	~
13		Default language for searching apps in Windows Store.	German (Germany)	~
ć	Apple Configuration			
٠	Android Configuration			
-	Windows Configuration			
6	ContentBox			
J.	LDAP Configuration			
8	App Management			
	Black- & Whitelisting			
(Third Party Apps			
E				
1	App Store			



App Settings

Hier können Sie die App Einstellungen, welche als Standard verwendet werden, festlegen. Diese können bei jeder App Installation einzeln angepasst werden.

iOS App Settings

	•
Keep up to date	Hält die App aktuell, basierend auf dem
	gewählten Update Target
Overtake when unmanaged	Wenn die App bereits als nicht verwaltet
	(nicht via MDM) installiert ist, wird diese
	verwaltet
Remove app when MDM profile is	Die App wird entfernt, wenn das MDM
removed	Profil entfernt wird
Prevent backup of the app data	Verhindert das Backup der App Daten

Android App Settings

Keep up to date	Hält die App aktuell, basierend auf dem
	gewählten Update Target



Fernwartung TeamViewer

Den TeamViewer Account mit der Konsole verbinden

Hinweis: Sie können in der kostenlosen Testversion in der Cloud keinen eigenen Account verknüpfen. Hier wird Ihnen ein Demo Account bereits automatisch hinterlegt.

Gehen Sie zu Allgemeine Einstellungen -> Fernwartung -> TeamViewer. Hier können Sie Ihren TeamViewer Account mit der Konsole verbinden oder Informationen zu Ihrem verknüpften Account sehen. Unter "Aktive Sitzungen" sehen Sie die aktiven Sitzungen.

•	TeamViewer Connector
Account Overview	TaxmViowar Katun
Global Configuration	Click on the button below to connect your Team/Vewer Account with the AppTec console.
Privacy	Start Setup
Role Based Access	
Apple Configuration	Broduct Instituted
Android Configuration	You need to approve the App "TeamViewer Quick Support" before you can Remote Control an Android for Work device.
Windows Configuration	Click on the button to open the "Team/Vewer Quick Support" store page at Google Play for Work Open Play for Work
ContentBox	
LDAP Configuration	
Universal Gateway 🗸 🗸	
App Management 🗸	
SIM Card Management	
(Remote Control	
TeamViewer	

Klicken Sie auf "Setup starten" um den Account zu verknüpfen.

l er la
LOG III Please log in to confirm your access request
e-mail
password
l forgot my password

Dies führt Sie auf eine neue Seite, wo Sie sich mit Ihrem TeamViewer Account einloggen können.

aı	uthorization request
۱p	pTec EMM requires the following permissions:
	Account Management Show account details, show email, show license
5	User management: Show users (*)
1	Manage sessions: Create sessions, edit your own sessions, view your own sessions
0	Group management: Create groups, read groups, edit groups, share / not share groups, delete groups
8	Connection logging: Read connection logs (*)
1	TeamViewer guidelines: View TeamViewer policies (*)
1	Remote Access: Request remote access
0	DEM connections:
1	Your account does not have the permissions marked with an asterisk (*). Although you can grant access to the app, the app will not be able to

Nach dem Login, müssen Sie Apptec für die Nutzung des Accounts authorisieren.



Nachdem Sie dies bestätigt haben, warten Sie einige Sekunden und der Account ist verknüpft.

TeamViewer QuickSupport installieren.

Fügen Sie die App "TeamViewer QuickSupport" zu den Pflichtapps Ihres Gruppen- oder Geräteprofils hinzu und klicken Sie auf "Jetzt anwenden". Warten Sie bis die App installiert ist.



Wenn Sie versuchen ein Gerät zu erreichen auf dem TeamViewer nicht installiert ist, wird die App auf dem Gerät installiert bzw der Benutzer wird aufgefordert die App zu installieren, je nach Konfiguration des Gerätes.

Starten der Fernwartung

Um die Fernwartung zu starten, wählen Sie das Gerät, klicken auf das Zahnrad und wählen "TeamViewer Fernwartung".





Wenn bereits eine aktive Sitzung existiert, können Sie diese entweder wieder aufnehmen oder verwerfen und eine neue erstellen.

Bestätigen Sie, dass Sie eine neue Sitzung erstellen wollen.

Remote Control		\times
Supporter URL: https://get.teamviewer.com/v13/	new window.	
Cancel	Start	

Nach einigen Sekunden erhalten Sie einen Link für die TeamViewer Sitzung. Klicken Sie auf "Starten" um den Link in einem neuen Fenster zu öffnen.



Dieser Link öffnet TeamViewer und verbindet sich mit dem Gerät.





Nun müssen Sie nur noch den Zugriff auf dem Endgerät bestätigen um das Gerät von der Ferne zu steuern.

Im Falle von iOS bekommen Sie eine Nachricht mit in die Apptec App mit einem Link um die Verbindung aufzunehmen. Abhängig von den Benachrichtigungseinstellungen des Gerätes, kann es sein, dass Sie keine Notification erhalten und manuell die Apptec App öffnen müssen.

Auf einigen Android Geräten (idR Samsung) ist es möglich, dass Teamviewer die Installation einer weiteren App als Addon erfordert. Die Teamviewer App wird Sie darauf hinweisen, falls dies nötig ist.



Unbeaufsichtigter Zugriff

Hinweis: Der unbeaufsichtigte Zugriff ist nur auf Android möglich.

Sie können sich mit dem Gerät, ohne den Zugriff auf dem Gerät zu bestätigen, verbinden, wenn Ihr TeamViewer Account eine "Tensor" Lizenz besitzt.

Uı	nattended Access
~	Unattended Access is available. Android Devices with enabled Kiosk Mode setting and installed "TeamViewer Host" app can be remote controlled without user interaction.
	Devices registered for unattended access: 2

Ob Ihr Account dies unterstützt, können Sie nach dem Verknüpfen in den Allgemeinen Einstellungen prüfen.

TeamViewer	
Enable Unattended Access	On On

Um den unbeaufsichtigten Zugriff zu nutzen, müssen Sie die "TeamViewer Host" App auf dem Gerät installieren und im Profil unter "Kiosk Modus & Launcher" die Funktion "Erlaube unerlaubten Zugriff" aktivieren. Bitte beachten Sie, dass die Funktion nur unter Verwendung des Kiosk Modus zur Verfügung steht.



Nun haben Sie die Möglichkeit über das Zahnradmenü den unerlaubten Zugriff auszuwählen und sich direkt mit dem Gerät zu verbinden. Bitte beachten Sie, dass es einige Momente dauern kann bis Sie den Link für den Verbindungsaufbau erhalten.



IV. Mobile Management

Oberfläche im Mobile Management

Gerätefilter

Über einen Klick auf den Pfeil links oben auf der Oberfläche können Sie diverse Filter für die Anzeige der Geräte auffinden.



Suchfenster

Das Suchfenster erlaubt es Ihnen, alle Geräte beziehungsweise Benutzer nach einem spezifischen Begriff zu durchsuchen.

Optionszahnrad

Nach einem Klick auf das entsprechende Symbol wird Ihnen eine Auflistung der zu Verfügung stehenden Optionen angezeigt. Diese ändern sich je nach aktuellem Fenster und werden in den entsprechenden Kapiteln näher erläutert.

Navigationspfeile

Mit einem Klick auf den linken Pfeil gelangen Sie auf die vorangegangene Seite, danach gelangen Sie mit einem Klick auf den rechten Pfeil auf die geradeeben verlassene Seite.



Administrationskonto-Einstellungen

support@apptec360.com ∽

My Profile	Bearbeiten Sie die Daten des Admin Kontos
Log Out	Melden Sie sich sicher von der Appliance ab

User Information

Username	Benutzername bzw. E-Mail Adresse des Kontos
Name	Vorname des Administrators
Surname	Nachname des Administrators
Login Name	Loginname des Administrators
eMail Adress	E-Mail Adresses des Administrators
Alternative eMail Adress	Alternative E-Mail Adresse des Administrators
Picture	Profilbild
Phone Number	Telefonnummer des Administrators
Mobile Number	Handynummer des Administrators
Phone Extension	Durchwahl
Location	Standort
Position	Position im Unternehmen
Usergroup	Wählen Sie aus, welcher Usergruppe Sie das Admin-Konto zuordnen wollen
Comment	Fügen Sie einen Kommentar hinzu
Enter new password	Geben Sie zur Passwortänderung das neue Passwort
Repeat new password	Wiederholen Sie das neue Passwort zur Bestätigung

Bitte beachten Sie, dass der Administrationszugang auch als lokales Benutzerkonto im Hierarchiebaum hinterlegt wird. Ohne das Anlegen eines weiteren Administrators sollte dieser also nicht gelöscht werden!



Firmenverwaltung (Root-Verzeichnis) im Mobile Management

 ♥ Q Search here) 🐺 🔺 🕨 Gra	oup Profiles	
- E Root		Device Type	Device Property
Additions	*	iPhone	Corporate
	*	iPhone	Employee
	*	iPad	Corporate

Wenn Sie sich im Root-Verzeichnis befinden (erste Gruppe) können Sie diverse Einstellung für Ihr Unternehmen in Hinsicht auf das Mobile Management durchführen.

Create a Subgroup	Untergruppe erstellen
Rename Root Node	Umbenennen des Root-Verzeichnisses (z.B. Ihr Firmenname)
Mass Enrollment	Mehrere Geräte / User auf einmal enrollen
Mass Assignment	Profile für die jeweiligen Gruppen auf einen Blick zuweisen

Create a Subgroup

Mit Create a Subgroup können Sie eine weitere Untergruppe erstellen. Sie können festlegen unter welcher Gruppe sich die Untergruppe einreihen soll.

(Standardmäßig wird hier eine neue, dem Root-Verzeichnis untergeordnete, Gruppe erstellt).

Create Grou	p	×
Group Name	AppTec Test	
Parent Group	Root Node	~



Rename Root Node

An dieser Stelle können Sie Ihr Root-Verzeichnis umbenennen, häufig wird hier der Firmenname eingetragen.

Default Title		\times
Root Node Name	AppTec360	
		Lindate Name

Mass Enrollment

Mit "Mass Enrollment" können Sie auf einmal mehrere Geräte und User entrollen.



	Enrollmen	t											>	<
1	Name	ellail	Alternative eMail	Phone Number	eMail	alt, eMail	SMS	iOS	Android	Windows	Phone	Tablet	Emp.	Corp.
9 6	Consultants													
E 1	Lukas										V			
	Matthias		Concentration (1)						1			E	V	
E F	Felix													
F	Fabian Kola				V									
	Max Mustermann													
	Daniel												V	
	Admins													
	Tanja												V	
	Michael			1000 CONTRACTOR									V	
	Martina								(f)			100		
	Milan													
	Yasemin								[]				V	

Sie können direkt auswählen, in welcher Form der User das Enrollment erhalten soll (eMail; alternative eMail; SMS)

Je nachdem was der User für ein Gerät erhalten soll (iOS, Android, Windows Phone) können Sie dies direkt markieren.

Die Zuweisung ob es sich um ein Smartphone oder Tablet handelt kann ebenfalls direkt eingestellt werden, je nachdem müssen Sie hier die richtige Markierung mit einem Haken setzen.

Zuletzt können Sie bestimmen, ob es sich bei dem jeweiligen Gerät um ein Firmen-/ oder Privatgerät (BYOD) handelt.

Sie können mit "Export as CSV" die Informationen als CSV Tabelle exportieren, im Umkehrschluss können Sie mit "Import CSV" auch eine CSV Datei importieren, diese sollte wie im folgenden Beispiel aussehen:

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

Mass Assignment

Unter "Mass Assignment" können Sie allen Gruppen ein Profil zuweisen, dies ist unterteilt in iOS – Android – Windows



Prof	ile Assignmen	t							\times
Select Assign	Name	iPhone Corp.		Phone Em <mark>pl</mark> .		iPad Corp.		iPad Empl.	
Ξ	Consultants	Default iOS Phone Profile	~	Default iOS Phone Profile	~	Empty Profile	~	Profile US	~
Ξ	Admins	Default iOS Phone Profile	~	Default iOS Phone Profile	~	iOS Tablet Admin	~	Empty Profile	~
	Admins	Default iOS Phone Profile	~	Default iOS Phone Profile	~	iOS Tablet Admin	v	Empty Profile	



Gruppenverwaltung im Mobile Management

Ein Klick auf diese Gruppe zeigt eine Übersicht der verschiedenen Konfigurationsprofile für die entsprechenden Plattformen.

Ein Profil beinhaltet alle Einstellungsmöglichkeiten, die mit AppTec360 im Vornherein am Endgerät festgelegt werden können. Für jede Plattform können Profile für Firmengeräte (Corporate) oder Bring-Your-Own-Device Geräte (Employee) kreiert werden.

Um differenzierte Konfigurationen für Gerätegruppen, z.B. nach Standort oder Funktion, ermöglichen zu können, ist die Erstellung mehrerer Untergruppen empfohlen.

Beachten Sie die Profilverwaltung im Mobile Management.

🗸 🔍 Search here 🔪 🔅	< >	Group Profiles			👤 support@milanconsult.de 🗸
A 🚠 Root	-				
🔺 🧟 Admins		Device Type	Device Property	Selected Profile	Status
🕨 👤 Martina	*	iPhone	Corporate	Default iOS Phone Profile	V On
🕨 👤 Michael	*	iPhone	Employee	Default iOS Phone Profile	v On
🕨 👱 Tanja	*	iPad	Corporate	iOS Tablet Admin	v On
🕨 👤 Yasemin	*	iPad	Employee	Empty Profile	~ Он 🕥
	*	Android Phone	Corporate	Admin Android	✓ On On

Mit diesem Zahnradmenü können Sie diverse Einstellung für die jeweilige (Unter)gruppe vornehmen.

Create a Subgroup	Untergruppe für die jeweilige (Unter)gruppe vornehmen
Edit selected Group	Ausgewählte Gruppe editieren
Delete selected Group	Ausgewählte Gruppe löschen
Mass enrollment	Mehrere Geräte / User auf einmal für das ausgewählte Profil zu enrollen
Mass Assignment	Profile für die aktuell ausgewählte Gruppe verteilen
Create a User	User für die jeweilige (Unter)gruppe erstellen



Create a Subgroup

Mit Create a Subgroup können Sie eine weitere Untergruppe erstellen. Sie können festlegen unter welcher Gruppe sich die Untergruppe einreihen soll (standardmäßig gliedert sich die Untergruppe unter der aktuell ausgewählten Gruppe ein).

Create Group	ı.	\times
Group Name		
Parent Group	Admins	~
		Create group

Edit selected Group

Hier können Sie das Profil editieren – folgende Einstellungen sind hier möglich:

- Gruppenname kann geändert werden
- Übergeordnete Gruppe kann geändert werden

Update Group)	\times
Group Name	Admins	
Parent Group	Root Node	~
		Update group



Delete selected Group

Unter "delete selected Group" werden Ihnen alle User und Geräte in der jeweilig befinden Gruppe aufgelistet, Sie sind hier in der Lage diese zu löschen.

Für einen User können Sie folgende Löschbefehle durchführen:

Delete User	User wird gelöscht
Move User To Group:	Sie können den User in eine andere Gruppe (folgende Spalte, z.B. "Admins) verschieben

Für ein Gerät können Sie folgende Löschbefehle durchführen:

Wipe & Delete	Gerät zurücksetzen und löschen
Delete from System	Gerät nur aus AppTec entfernen

Verweis: Mass Enrollment

Verweis: Mass Assignment



<u>Create a User</u>

Mit "Create a User" können Sie einen neuen User hinzufügen.

Create	User	\times
Name	Pflichtfeld	Vorname des Users
Surname	Pflichtfeld	Nachname des Users
Login Name		Login Name des Users
eMail Address	Pflichtfeld	E-Mail Adresse des Users
Alternative eMail A	Address	Alternative E-Mail Adresse (des Users)
Picture		Click here to select a file Profilbild des Users
Phone Number		Telefonnummer (wichtig bei SMS Enrollment)
Mobile Number		Telefonnummer
Phone Extension		Durchwahl
Location		Standort
Position		Position
Usergroup		Admins Zugewiesene Gruppe ~
Comment		Hier können Sie einen Kommentar hinzufügen!
Comment		h.

Create User



Einen neuen Admin-User erstellen

Sie können einen Nutzer zum Admin-User machen. Dadurch hat dieser auch die Rechte sich in die Konsole einzuloggen und User/Gruppen/Geräte zu verwalten.

Erstellen Sie dazu einen normalen User oder wählen Sie einen bereits existierenden. Wählen sie den User an der die Rechte bekommen soll, klicken Sie auf das Zahnrad und dann auf "Edit User"

 ✓ Q Search here 	🗱 New Root
🔺 🗟 Root Node	💂 Edit User
🔺 🧟 Default Group	😛 Invite user to VPP
🕨 💄 New Root	

Weisen Sie dem Nutzer nun die "Super Root" Rolle zu und setzen Sie ein Passwort. Speichern Sie und der User kann sich mit seinem Username und dem eben vergebenen Passwort einloggen.

User Information		\times
Username	Sectors, egge at out	
Name	New	
Surname	Root	
Login Name		0
eMail Address	email@address.com	
Alternative eMail Address		
Picture	Click here to select a file	•
Phone Number		
Mobile Number		
Phone Extension		
Location		
Position		
Usergroup	Default Group	~
Assigned Roles	Super Root x	
Comment		h
Enter new password		0
Repeat new password		0
		Savo



Benutzerverwaltung im Mobile Management

Wenn Sie einen bestimmten User auswählen, erhalten Sie folgende Übersicht:



Sie erhalten einen Überblick über alle Informationen die Sie zuvor bei "Create a User" eingetragen haben.

Sie können mit dem obig angebrachten Zahnrad folgende Einstellungen vornehmen:

Edit User	User-Informationen bearbeiten
Delete user	User löschen → Delete from System = Das Gerät wird aus AppTec entfernt → Wipe & Delete = Das Gerät wird auf die Werkeinstellungen zurückgesetzt und aus AppTec entfernt
Add and enroll a Device	Ein Gerät für den ausgewählten User enrollen

Bitte beachten Sie, dass der Administrationszugang auch als lokales Benutzerkonto im Hierarchiebaum hinterlegt wird. Ohne das Anlegen eines weiteren Administrators sollte dieser also nicht gelöscht werden!



Add and enroll a Device

Hier können Sie für den ausgewählten User ein Gerät enrollen. Sie können alternativ ein Gerät auch auf Gruppenebene direkt einrollen. Wählen Sie dafür die Gruppe an, klicken auf das Zahnrad und wählen "Add and enroll a Device".

Folgende Übersicht sollten Sie erhalten:

Add Device		\times
Selected User	Max Mustermann	
Device name	Device of Max Mustermann	
Phone Number, e.g. +49160123456		
Alternative eMail		
Device Owner	Orporate Property Employee Property	
Choose operating system	 Android iOS Windows 	
Choose device type	 Phone Tablet 	
Send enroll request now ?	On	0
Send request to alternative eMail ?	Off	0
Send enrollment SMS ?	Off	0
	You have 10 SMS credits left	

Add Device



Je nachdem was Sie für ein Gerät enrollen möchten, müssen Sie folgende Einstellungen vornehmen:

Selected User	Ausgewählter User (wird automatisch befüllt)
Device Name	Wird automatisch ausgefüllt (Device of "Name des Users") – kann jedoch abgeändert werden
Phone Number	Telefonnummer, wird automatisch befüllt (sofern beim User angegeben) – kann jedoch hier hinzugefügt oder abgeändert werden
Alternative eMail	Alternative E-Mail Adresse, wird automatisch befüllt (sofern beim User angegeben) – kann jedoch hier hinzugefügt oder abgeändert werden
Device Owner	Corporate Property = Firmengerät Employee Property = BYOD Gerät
Choose operation System	Sie können hier zwischen Android, iOS und Windows Phone Geräte wählen
Send enroll request?	Die E-Mail wird sofort an die angegebene Haupt E-Mail Adresse verschickt und der User wird aufgefordert sein Gerät einzubinden
Send request to alternative eMail?	Die enroll E-Mail zusätzlich oder ausschließlich (falls "Send enroll request?" deaktiviert wurde) an die alternative E-Mail Adresse zu verschicken (E-Mail unterscheidet sich nicht im Gegensatz zur "normalen" enroll Request E-Mail)
Send enrollment SMS?	Ein enrollment request über SMS zu verschicken (die "Phone Number" muss eingetragen sein)

Nachdem der Enrollment Request verschickt wurde, wir bereits ein Gerät (rot markiert) angezeigt.

Sobald das Gerät erfolgreich eingebunden ist, wird das Gerät nach kurzer Zeit grün markiert und ist somit bereit diverse Restriktionen, Apps, etc. zu erhalten.



Profilverwaltung im Mobile Management

Nach einem Klick auf eine Gruppe erhalten Sie eine Übersicht aller zu konfigurierenden Geräteplattformen und der entsprechend zugewiesenen Profile.

🔺 🚠 Root		Device Type	Device Property	Selected Profile	Statue
🕨 🖄 Admins		Device Type	Device i toperty	Celected Frome	Otatus
🕨 🏯 Consultants	*	iPhone	Corporate	Default iOS Phone Profile V	On On
	*	iPhone	Employee	Default iOS Phone Profile	On
	*	iPad	Corporate	Default iOS Tablet Profile V	On On
	*	iPad	Employee	Default iOS Tablet Profile	On
	*	Android Phone	Corporate	Default Android Phone Profile	On On
	*	Android Phone	Employee	Default Android Phone Profile	On On
	*	Android Tablet	Corporate	Default Android Tablet Profile	On
	*	Android Tablet	Employee	Default Android Tablet Profile	On On
Group Profiles	*	Windows Phone	Corporate	Default Windows Phone Profile	On 💦
Content Management	*	Windows Phone	Employee	Empty Profile	On
				Inherit from parent group	

*	Nehmen Sie Einstellungen für das gerade ausgewählte Profil vor
Device Type	Gerätetyp bzw. Modell
Device Property	Eigentümer des Gerätes (Corporate = Firmeneigentum, Employee = Privatgerät d. Mitarbeiters)
Selected Profile	Ausgewähltes Profil (Das Zahnrad öffnet den Konfigurationsdialog des Profils)
Status	On/Off (Das Profil ist aktiviert/deaktiviert)

Wenn Sie das Zahnrad anwählen, erhalten Sie folgende Optionen:

Create a profile

Für jeden Eintrag bzw. Plattform können Sie ein neues Profil anlegen und konfigurieren. Nachdem Sie diesen Unterpunkt angeklickt haben, wird das Profil direkt erstellt und Sie können direkt mit der Konfiguration von iOS, Android und Windows Phone beginnen.



Edit Profile

Nach einem Klick auf "Edit Profile" gelangen Sie direkt in die Konfigurationsoberfläche für das entsprechende Profil und können die Einstellungen anpassen.


Copy Profile

Mit Hilfe der "Copy Profile" Funktion können Sie die Anpassungen/Einstellungen eines bereits vorhandenen Profils kopieren und in ein neues Profil einfügen.

Copy Group Prof	ile	\times
Source Profile Name	Default iOS Phone Profile	
New Profile Name	Copy of Default iOS Phone Profile	
Profile Type	Phone Profile	~
		Сору

Source Profile Name	Name des zu kopierenden Profils
New Profile Name	Name des neuen Profils
Profile Type	Typ des Profils (Phone/Tablet)

Wenn Sie nun auf "Copy" drücken, wird das Profil erstellt und kann nun der Gruppe zugewiesen werden

Delete Profile

Hier können Sie ein Profil endgültig löschen. Beachten Sie, dass bei der Löschung und nachfolgendem "Assign Now" des Profils die Konfiguration entsprechend auf den Endgeräten der betroffenen Gruppe verschwindet und nicht wiedergestellt werden kann!

Delete Group Profile		\times	
Profile to Delete	Default iOS Phone Profile		



Vererbung von Profilen

Bei der Auswahl der Profile steht auch die Option "Inherit from parent group" zur Verfügung.

milan Windows Phone	~
Default Windows Phone Profile	*
Empty Profile	
Inherit from parent group	
milan Windows Phone	*

Wenn dieses Profil aktiviert ist, dann wird für den entsprechend ausgewählten Gerätetyp das Profil der übergeordneten Gruppe (und jeweiligem Gerätetyp) verwendet. Beachten Sie also, dass Änderungen an diesem Profile durchaus mehrere Gruppen betreffen können.

Diese Einstellung ist auch als Standardwert eingestellt, wenn eine neue Untergruppe erstellt wird.

Ebenso ist die Einstellung "Empty Profile" vorhanden, welche einem leeren Profil entspricht, d.h. im Endeffekt werden keine Einstellungen am Endgerät vorgenommen.



Geräteverwaltung im Mobile Management

Wenn Sie ein Gerät auswählen, können Sie über das "Zahnrad" diverse Aktionen ausführen.

Diese unterscheiden sich je nach Betriebsplattform (Android, iOS, Windows Phone)

<u>Android</u>

*	Device of
ø	Edit Device
×	Clear Passcode
8	Lock Device
×	Delete Device
⊕	Wipe Device
戯	Enterprise Wipe
	Send Message
•	Send Enrollment Request

Edit Device	Geräte Informationen ändern
Clear Passcode	Passcode des Gerätes löschen
Lock Device	Gerät sperren (Sperrbildschirm)
Delete Device	Gerät aus AppTec entfernen
Wipe Device	Geräte auf die Werkseinstellungen zurücksetzen
Enterprise Wipe	Von AppTec zur Verfügung gestellte Informationen, Apps, Profile werden gelöscht (Gerät wird vom MDM getrennt)
Send Message	Push Benachrichtigung an das Gerät versenden Nachricht wird in der AppTec App angezeigt (Message Tab)
Send Enrollment Request	(erneuten) Enrollment request versenden



Edit Device

Hier können Sie diverse Informationen des Geräts anpassen.

Update Device		×
Selected User	Matthias	
Device name	Device of Matthias	
Phone Number, e.g. +491601234	56	
Device Owner	Corporate Property C Employee Property	
Choose device type	 Phone Tablet 	
		and the second sec

Selected User	Benutzer des Gerätes
Device name	Name des Gerätes
Phone Number	Telefonnummer des Gerätes
Device Owner	Corporate = Firmeneigentum Employee = Mitarbeitereigentum
Choose device typ	Typ des ausgewählten Gerätes

Clear Passcode

Hier können Sie das Gerätepasswort des ausgewählten Gerätes entfernen. Bei Android wird der Passcode standardmäßig auf "123456" gesetzt – dieses kann und sollte der User nachträglich wieder abändern.

Lock Device

Hier wird lediglich einen Sperrbefehl an das Endgerät verschickt (Sperrbildschirm).



Delete Device

Hier kann ein Löschbefehl durchgeführt werden, Sie könne erneut unterscheiden, ob das Gerät nur aus AppTec ("Delete from System") entfernt werden soll oder ob das Gerät aus AppTec entfernt werden soll und zusätzlich sich auf die Werkseinstellungen zurücksetzen soll ("Wipe & Delete).

Delet	te Device				\times
Are you sure	e to delete this device ?				
Device:	Device of Matthias	Delete from System	~	Root Node	~
			_		
				Proces	s Delete

Wipe Device

Unter "Wipe Device" können Sie einen vollständigen Wipe des Gerätes durchführen, das Gerät wird dann auf die Werkseinstellungen zurückgesetzt.

Zusätzlich können Sie, falls sich im Gerät eine SD Karte befindet, die SD Karte löschen, dies können Sie tun indem Sie "Wipe SD Card too?" auf "On" setzen.

Wipe Device	\times
Are you sure to wipe the device ?	
Wipe SD Card too ?	
No	Yes



Enterprise Wipe

Dies ist der empfohlene Weg um eine Trennung zum MDM durchzuführen.

Nur von AppTec zur Verfügung gestellte Informationen, Apps, Profile werden gelöscht, somit werden alle Firmendaten auf dem Endgerät nicht mehr zur Verfügung stehen, der private Bereich ist jedoch nicht betroffen und bleibt weiterhin auf dem Endgerät bestehen.

Enterprise Wipe device?	\times
Are you sure to Enterprise Wipe the device ?	
No	Yes

Send Message

Hier können Sie eine Push Benachrichtigung an das jeweilige Endgerät versenden.

Send a message		\times
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



Mit "Send Enrollment Request" können Sie (nochmals) ein Enrollment Request an den jeweiligen User schicken.

Bitte beachten Sie, dass nur der letzte Enrollment – Request gültig ist.

Send Enrollment Request			\times
Alternative eMail address	On On	com	•
Send to alt. eMail address ?	Он 🅥	com	0
Send enroll SMS ?	Off		0
			Enroll now



<u>iOS</u>

Wenn das Gerät eingebunden (grün) ist:

Device of Mix Edit Device Clear Passcode Lock Device Delete Device Wipe Device Enterprise Wipe Send Message Remove MDM

Wenn das Gerät nicht eingebunden (rot) ist:



Edit Device	Gerät editieren
Clear Passcode	Das Gerätepasswort wird gelöscht
Lock Device	Gerät sperren (Sperrbildschirm)
Delete Device	Gerät aus AppTec entfernen
Wipe Device	Geräte auf die Werkseinstellungen zurücksetzen
Enterprise Wipe	Von AppTec zur Verfügung gestellte Informationen, Apps, Profile werden gelöscht (Gerät wird vom MDM getrennt)
Send Message	Push Benachrichtigung an das Gerät versenden Nachricht wird in der AppTec App angezeigt (Message Tab)
Send Enrollment Request	(nochmaliger) Enrollment request versenden
Remove MDM	Das MDM vom Endgerät entfernen (gleicher Effekt wie der "Enterprise Wipe")



Edit Device

Hier können Sie diverse Informationen des Geräts anpassen.

Update Device		\times
Selected User	Matthias	
Device name	Device of Matthias	
Phone Number, e.g. +4916012345	6	
Device Owner	Orporate Property C Employee Property	perty
Choose device type	 Phone Tablet 	
		Save

Clear Passcode

Unter "Clear Passcode" können Sie das Gerätepasswort remote auf dem Endgerät entfernen, der User wird anschließend aufgefordert ein neues Passwort (je nach Passcode Richtlinien) zu vergeben.





Lock Device

Hier wird lediglich einen Sperrbefehl an das Endgerät verschickt (Sperrbildschirm).

Delete Device

Hier kann ein Löschbefehl durchgeführt werden, Sie könne erneut unterscheiden, ob das Gerät nur aus AppTec ("Delete from System") entfernt werden soll oder ob das Gerät aus AppTec entfernt werden soll und zusätzlich sich auf die Werkseinstellungen zurücksetzen soll ("Wipe & Delete).

Delet	te Device		X
Are you sure	e to delete this device ?		
Device:	Device of Matthias Mader	Delete from System	✓ Root Node ✓
			Process Delete

Wipe Device

Unter "Wipe Device" können Sie einen vollständigen Wipe des Gerätes durchführen, das Gerät wird dann auf die Werkseinstellungen zurückgesetzt.

Wipe Device	X
Are you sure to wipe the device ?	
No	Yes



Enterprise Wipe

Nur von AppTec zur Verfügung gestellte Informationen, Apps, Profile werden gelöscht, somit werden alle Firmendaten auf dem Endgerät nicht mehr zur Verfügung stehen, der private Bereich ist jedoch nicht betroffen und bleibt weiterhin auf dem Endgerät bestehen.

Enterprise Wipe device?	\times
Are you sure to Enterprise Wipe the device ?	
No	Yes

Send Message

Hier können Sie eine Push Benachrichtigung an das jeweilige Endgerät versenden.

Send a message		\times
Subject	Wichtig! Bitte bei Ihrer IT melden!	
Message	Sehr geehrter Herr Mustermann, bitte melden Sie sich umgehend bei Ihrer IT-Abteilung.	



Send Enrollment Request

Mit "Send Enrollment Request" können Sie (nochmals) ein Enrollment Request an den jeweiligen User schicken.

Send Enrollment Re	\times		
Send enroll request now ?	On On		0
Alternative eMail address	matthias	com	
Send to alt. eMail address ?	Off 🕥		0
Send enroll SMS ?	Off		0
			Enroll now

Remove MDM

Mit "Remove MDM" können Sie das MDM Profil und alles weitere von AppTec zur Verfügung gestellte auf dem Endgerät entfernen. Dieser Befehl führt dieselbe Aktion wie der "Enterprise Wipe" durch.







<u>Windows</u>

\$	Device of Max Mustermann
	Edit Device
8	Lock Device
	Delete Device
•	Wipe Device
	Enterprise Wipe
	Send Enrollment Request

Edit Device	Gerät editieren
Lock Device	Gerät sperren (Sperrbildschirm)
Delete Device	Gerät aus AppTec entfernen
Wipe Device	Geräte auf die Werkseinstellungen zurücksetzen
Enterprise Wipe	Von AppTec zur Verfügung gestellte Informationen, Apps, Profile werden gelöscht
Send Enrollment Request	(nochmaliger) Enrollment request versenden

Edit Device

Hier können Sie diverse Informationen des Geräts anpassen.

Update Device		\times
Selected User	Matthias	
Device name	Device of Matthias	
Phone Number, e.g. +4916012345	6	
Device Owner	Corporate Property Employee Property	
Choose device type	PhoneTablet	
	Save	



Lock Device

Hier wird lediglich einen Sperrbefehl an das Endgerät verschickt (Sperrbildschirm).

Delete Device

Hier kann ein Löschbefehl durchgeführt werden, Sie könne erneut unterscheiden, ob das Gerät nur aus AppTec ("Delete from System") entfernt werden soll oder ob das Gerät aus AppTec entfernt werden soll und zusätzlich sich auf die Werkseinstellungen zurücksetzen soll ("Wipe & Delete).

Delet	te Device			\times
Are you sure	e to delete this device ?			
Device:	Device of Matumas Mader	Delete from System	✓ Root Node	~
			Proc	cess Delete

Wipe Device

Unter "Wipe Device" können Sie einen vollständigen Wipe des Gerätes durchführen, das Gerät wird dann auf die Werkseinstellungen zurückgesetzt.





Enterprise Wipe

Nur von AppTec zur Verfügung gestellte Informationen, Apps, Profile werden gelöscht, somit werden alle Firmendaten auf dem Endgerät nicht mehr zur Verfügung stehen, der private Bereich ist jedoch nicht betroffen und bleibt weiterhin auf dem Endgerät bestehen.

Enterprise Wipe device?	\times
Are you sure to Enterprise Wipe the device ?	
No	Yes

Mit "Send Enrollment Request" können Sie (nochmals) ein Enrollment Request an den jeweiligen User schicken.

Send Enrollment Re	equest		\times
Send enroll request now ?	On On		0
Alternative eMail address	matthias	com	
Send to alt. eMail address ?	Off		0
Send enroll SMS ?	Off		0
			Enroll now

Send Enrollment Request



Content Management

Wenn Sie sich auf einer Gruppe befinden, können Sie mit dem "Content Management" die ContentBox von AppTec verwalten.

Mit der Content Box können Sie Dokumente und andere Firmendaten sicher auf die Endgeräte verteilen.

Group Files

"Group Files" stellt den zentralen Baustein der ContentBox dar, hier können Sie allerlei Einstellungen vornehmen, Ihre Dokumente hochladen, neue Ordner anlegen, etc.

🗸 🔍 Search here	Group Files File Explorer	Audit Trail Trash	External Storage	2	~
 Admins 会 Consultants 	Consultants				0
Danel Seban S	Root February 24, 2015, 10:09 am screenshols February 24, 2015, 4:57 pm Test March 2, 2015, 1:48 pm 1.png March 9, 2015, 2:51 pm	0 B 310.1 kB 249.5 kB 56.8 kB	Source: Group Root Permissions: RUCDS	Enable Group Folder Con Default group folder permissions Read / Update / Create Pass group folders on to subgroups Permissons for subgroups Read / Update / Create / Delete Allow sharing Con	9 9 9 9
Group Profiles	April 13, 2015, 10:26 am	557.3 kB			
Content Management	March 23, 2015, 1:44 pm	1.4 MB			

Mit dem Symbol oben rechts können Sie über "Add Folder" einen neuen Ordner anlegen, der der jeweiligen Gruppe zugeordnet werden soll.

Sie können den Ordner beliebig benennen.



Über "Upload Files" können Sie eine neue Datei hochladen, Ihr Standard-Explorer wird hier geöffnet. Selbstverständlich können Sie diese zwei Aktionen in jedem (Unter)Ordner durchführen.

Mit dem Symbol oben links kommen Sie immer wieder zurück ins Hauptverzeichnis.



Sie können mehrere Ordner und Dateien auswählen und sich diese per "Download" herunterladen oder Sie löschen diese indem Sie "Delete" anklicken.

✿ Consultants			
I 3 Files selected			Download × Delete
Root February 24, 2015, 10:09 am	0 B	Source: Permissions:	Group Root RUCDS
screenshots February 24, 2015, 4:57 pm	310.1 kB		
Test March 2, 2015, 1:48 pm	249.5 kB		
1.png March 9, 2015, 2:51 pm	56.8 kB		

Ebenfalls können Sie mit Select All alle Dateien und Ordner auswählen und die Befehle "Download" und "Delete" ausführen.

Wenn Sie den Mauszeiger über ein Ordner oder über einer Datei bewegen, erscheint Ihnen folgende Ansicht:

E Test				×
March 2, 2015, 1:48 pm	249.5 kB	🖋 Rename	Download	

- Mit "Rename" können Sie den Ordner / die Datei umbenennen
- Mit "Download" können Sie sich den Ordner / die Datei herunterladen
- Mit dem "x" können Sie den Ordner / die Datei löschen



Enable Group Folder	Falls aktiviert, alle Mitglieder in dieser Gruppe haben Zugriff auf den jeweiligen Ordner
Default group folder permissions	Berechtigung für die User in der ausgewählten Gruppe Read = nur Leseberechtigung Update = Update-Berechtigung Create = Erstell-Berechtigung Delete = Löschberechtigung
Pass group folders on to subgroups	Falls aktiviert, können die dementsprechenden Untergruppen auf die Dateien der übergeordnete Gruppe zugreifen
Permissions for subgroups	Berechtigung für die jeweilige Untergruppe Read = nur Leseberechtigung Update = Update-Berechtigung Create = Erstell-Berechtigung Delete = Löschberechtigung
Allow Sharing	Falls aktiviert, kann der User Dateien per Link teilen

Um Dateien hochzuladen, können Sie auch dieses Feld benutzen, indem Sie einfach per Drag & Drop eine Datei auf dieses Fenster ziehen, ebenfalls können Sie auf dieses Feld klicken, um mit Hilfe des Explorers eine Datei auszuwählen und hochzuladen.





File Explorer

Mit dem "File Explorer" können Sie alle Ordner und Dateien – unabhängig in welcher Gruppe Sie sich befinden – verwalten.

Sie finden die bereits schon beim "Group Files" gelernten Einstellungen und Knöpfe hier ebenfalls wieder.

File Root > AppTec Group Folders		0
Select All		
Root February 24, 2015, 10:09 am	0 B	
Admins April 30, 2015, 3:20 pm	4.3 MB	
Consultants June 16, 2015, 10:45 am	3.9 MB	
topCare May 12, 2015, 10:37 am	27.9 kB	
careCoach May 12, 2015, 11:04 am	0 B	
Test June 16, 2015, 11:31 am	0 B	

Audit Trail

Im "Audit Trail" können Sie eine Historie einsehen, welcher User etwas erstellt, gelöscht oder geteilt hat, somit können Sie zu jeder Zeit nachvollziehen was mit den Firmendaten gemacht wurde.

🗸 🔍 Search here	Group Files File Explorer Audit Trail Trash External Storage	👤 support@milanconsult.de 🗸
- 🛓 Root	Today	ſ
> 🗷 Admins	You enabled the provinciare Test	17 minutes ago
A A Consultants		
🕨 👤 Daniel Bezdecka	X You deleted Für Testzwecke	1 hour ago
🕨 👤 Fabian Kola	+ You created Für Testzwecke	1 hour ago
🕨 👤 Felix Alexa		
🕨 👤 Lukas Schreiber	Last month	
🕨 👤 Matthias Mader	You enabled the groupshare careCoach	last month
🕨 👤 Max Mustermann	+ You created group.jpg	last month
	You enabled the groupshare topCare	last month
	+ Lukas created IMG_0007.PNG	last month
Group Profiles	+ Martina created yasemin und martina	last month
	+ You created MDM vs. AS.docx	last month
Content Management	You shared 1.png via link	last month



Trash

Sollten Sie (ausversehen) etwas gelöscht haben, können Sie diese Ordner und Dateien unter "Trash" einsehen und bei Belieben wieder herstellen.

- Mit "Undelete" können Sie die Datei / den Ordner wiederherstellen.
- Mit "Delete" können Sie die Datei / den Ordner endgültig löschen Sie müssen den Löschvorgang nochmals bestätigen.

Bitte beachten Sie dass der sich im Papierkorb befindende belegte Speicherplatz vom "Total Space" abgezogen wird – dies ist seitens ownCloud bedingt.

Trash			
Name		Date	
Für Testzwecke) Undelete	1 hour ago	👕 Delete

External Storage

Unter dem Punkt "External Storage" können Sie einen externen Speicher anbinden.



Mit dem 💿 Symbol kann ein (weiterer) Speicher hinzugefügt werden.



Туре	Amazon S3, FTP, SFTP, ownCloud,	
	WebDAV, Windows Share, Sharepoint	
Amazon S3		
Display Name	Anzuzeigender Name	
Access Key	Zugangsschlüssel	
Secret Key	Sicherheitsschlüssel	
Bucket	Eindeutige Identität des Unterordners	
	der Ihnen zugewiesen ist	
Hostname (optional)	Hostname (optional)	
Port (optional)	Port (optional)	
Region	Region (optional)	
Enable SSL	Aktivierung von SSL	
Enable Path Style	Eindeutige Path Adresse die Ihnen	
	zugewiesen ist	
FTP		
Display Name	Anzuzeigender Name	
Host	Host-Adresse	
Username	Benutzername	
Password	Passwort	
Root	Hauptverzeichnis	
Secure ftps://		
SFTP		
Display Name	Anzuzeigender Name	
Host	Host-Adresse	
Username	Benutzername	
Password	Passwort	
Root	Hauptverzeichnis	
ownCloud	•	
Display Name	Anzuzeigender Name	
URL	ownCloud URL	
Username	Benutzername	
Password	Passwort	
Remote Subfolder	Standard Ordner	
Secure https://		
WebDAV		
Display Name	Anzuzeigender Name	
URL	WebDAV URL	
Username	Benutzername	
Password	Pasawart	
Password	Passwort	
Root	Hauptverzeichnis	
Secure https://		
Windows Share	Der Support für Windows Share wird	
Sharepoint	Der Support für Microsoft Sharepoint	
	wird demnächst erscheinen	



Konfiguration iOS

General

Je nachdem ob Sie aktuell eine Gruppe oder ein Gerät ausgewählt haben, unterscheiden sich die Darstellung und deren Unterpunkte – bitte beachten Sie dies sorgfältig!

Profile Information

Sollten Sie sich in einem Profil befinden, erhalten Sie hier einen kurzen Überblick über das Profil in Bezug auf Name, OS, Erstellungsdatum, Autor, etc.

Profile Name	Name des Profils – kann direkt hier umbenannt werden
Operating System	Für welches Betriebssystem das Profil gilt
Created At	Erstelldatum
Created By	Ersteller des Profils
Last Change	Datum und Uhrzeit an dem die letzten
	Änderungen vorgenommen wurden
Changed By	Anzeige darüber von wem die letzte
	Änderung vorgenommen wurde
Profile Revision	Anzahl wie oft das Profil bereits geändert
	wurde

General Information

Sollten Sie sich direkt auf einem Gerät befinden, erhalten Sie hier einen kurzen Überblick über Ihr ausgewähltes Gerät.

Device Name	Name des Geräts
Phone Number	Telefonnummer des Geräts
Model	Modellbezeichnung
Operating System	Betriebssystem
Serial Number	Seriennummer des Geräts
	Firmen- oder Privatgerät
Device Ownership	Corporate = Firmengerät
	Employee = Privatgerät
Device Type	Gerätetyp (Tablet oder Phone)
Jailbroken	Ob sich auf dem Gerät ein Jailbreak befindet
Supervised	Anzeige darüber ob es sich um ein Supervised
	Gerät handelt
Compliant	Ob gegen über irgendwelchen Richtlinien
	verstoßen wurde
Last Seen	Status wann sich das Gerät zuletzt am AppTec
	Server gemeldet hat



<u>Settings</u>

Diese Settings beinhaltet den Gerätename und einen vordefinierten Hintergrund.

Name device to system name	Der Name der in der AppTec Konsole vergeben wird (in der linken Strukturordnung), wird dann derselbe wie auf dem jeweiligen Endgerät (einsehbar in in den Geräte Einstellungen)
Use custom wallpaper (supervised devices only)	Hier können Sie einen Hintergrund vordefinieren, der auf dem Endgerät angezeigt warden soll (z.B. für eine Art Firmenbranding des Gerätes) Ist nur im Supervised Mode verfügbar!
Automatic OS updates	Erzwingt die OS Updates. Nur für DEP devices im supervised Modus.
Custom Fonts	Hier können eigene Schriftarten hinzugefügt werden.
Name	Optional. Der angezeigte Name für die Schriftart.
Font	Laden Sie die Datei für die Schriftart hier hoch (.otf or .ttf).

Config Revision

Hier erhalten Sie eine Übersicht welches Gruppenprofil dem Gerät zugewiesen ist.

Wenn sie auf das Gruppenprofil klicken, kommen Sie direkt zu diesem Profil und können Einstellungen vornehmen.

Mit dem Symbol können Sie die zugewiesenen Apps auf die Einstellung des Gruppenprofils zurücksetzen.

Mit dem O Symbol können Sie alle getätigten Apps auf die Einstellung des Gruppenprofils zurücksetzen.

Device Log

Unter diesem Punkt erhalten Sie eine Auflistung aller Aktionen, welche in Bezug auf das Endgerät stattgefunden haben, u.a. Erstellung, Löschung etc.

Administrationshandbuch AppTec360



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



Asset Management (nur auf Device Ebene)

Asset Management (nur auf Device Ebene)

Device Info

Model	Modellbezeichnung des Geräts
Operating System	Betriebssystem
OS Version	Betriebssystem Version
Serial Number	Seriennummer
UDID	UDID des Gerätes
Device Name	Gerätename
Supervised	Zeigt an, ob das Gerät supervised ist
Battery Status	Batterieanzeige

<u>Wi-Fi</u>

IP Address	IP Adresse des Gerätes
WiFi MAC	WiFi MAC Adresse

<u>Cellular</u>

Status	Status (SIM Karte vorhanden)
Phone Number	Telefonnummer
Roaming Status	Aktueller Roaming Status
Roaming (Voice/Data)	Roaming Status für Anrufe / Daten
IP Address	IP Adresse
IMEI	IMEI-Nummer
Operator/Carrier	Mobilfunk Anbieter
SIM Carrier Network	Mobilfunknetzwerk der SIM-Karte
Carrier Version	
Modem Firmware	Firmware des Modems
Current MCC/MNC	Siehe "SIM MCC/MNC"
	Der Mobile Country Code ist eine von der
	ITU im Standard E.212 festgelegte
	Länderkennung, die zusammen mit dem
	Mobile Network Code (MNC) zur
SIM MCC/MNC	Identifizierung eines Mobilfunknetzes
	verwendet wird (=Ländercode)
	Wenn man in ein anderes Mobilfunknetz
	geht ist deshalb der "Current MCC/MNC"
	und "SIM MCC/MNC" unterschiedlich.

<u>Bluetooth</u>

Bluetooth MAC	Bluetooth MAC Adresse



Security Management

Anti Theft (nur auf Device Ebene)

<u>GPS Information</u> (nur auf Device Ebene)

Hier können Sie den aktuellen / letzten Standort des Geräts ermitteln. Die Lokalisierung kann mit einem oder sogar zwei Passwörtern geschützt werden – Siehe: *General Settings – Privacy – GPS Access*



<u>Wipe & Lock</u> (nur auf Device Ebene)

Unter "Wipe & Lock" können Sie folgende Aktionen durchführen:

Full Wipe	Das Gerät wird auf die Werkseinstellungen zurückgesetzt (sowohl geschäftliche, als auch persönliche Daten werden gelöscht)
Enterprise Wipe	Nur die Firmendaten werden vom Endgerät entfernt (Alle Apps, Daten, etc. die von AppTec übergeben wurden)
Lock Screen	Bildschirmsperre wird aktiviert, es ist ausreichend das Gerät mit dem Geräte-Passwort/PIN wieder zu entsperren
Forensic Lockdown (Supervised Devices only)	Sollte diese Funktion mit dem Symbol aktiviert werden, wird das Gerät gesperrt, indem eine Meldung erscheint und es sich nicht mehr schließen lässt. Der Mitarbeiter kann das Gerät auch nicht entsperren.
	Nur der Administrator kann mit dem Entsperren (Symbol) das Gerät aus der Konsole heraus wieder entsperren.
Allow Activationlock (Supervised Devices Only)	Sollte die Funktion aktiviert werden, wird das Gerät gesperrt sobald "Find my iPhone" in den iCloud Einstellungen aktiviert wird



<u>Message</u> (nur auf Device Ebene)

Mit "Open Message Dialog" können Sie eine Push-Nachricht versenden.

Open Message Dialog

Anschließend sollte sich folgendes Fenster öffnen, dies können Sie mit einem Subject (Betreff) und einer Message (Nachricht) füllen und an das ausgewählte Endgerät versenden.

Send a message		\times
Subject	Test: Bitte bei Ihrer IT melden	
Harren	Diese Nachricht dient zur Testzwecken! Bitte melden Sie sich bei Ihrer EDV Abteilung.	1
Message	Mit freundlichen Grüßen Ihre IT-Abteilung	4

Send Message



Security Configuration

Passcode

Legen Sie hier die Einstellungen für das Gerätepasswort fest

Code deactivation allowed	Wenn diese Einstellung aktiviert ist, findet keine Aufforderung für das Setzen eines Passworts statt Sobald ein Passwort gesetzt ist, kann es nicht mehr deaktiviert werden
Allow simple value	Erlaube die Benutzung gleicher aufsteigender und absteigender Zeichenketten (z.B. 1234, 1111)
Require alphanumeric value	Passwörter müssen mindestens einen Buchstaben enthalten
Minimum passcode length	Minimale Länge des Passworts
Minimum number of complex characters	Minimale Anzahl alphanumerischer Zeichen im Passwort
Maximum passcode age	Anzahl der Tage, nach welchen das Passwort geändert werden muss
Maximum Auto-Lock	Maximale Dauer, nach welcher sich das Gerät sperrt
Maximum grace period for device lock	Dauer, nach welcher das Gerät in den gesperrten Stand-By geht
Maximum number of failed attempts	Legt fest, wie oft das Passwort falsch eingegeben werden darf, bis ein vollständiger Wipe des Gerätes durchgeführt wird
Maximum passcode age (1-730 days)	Maximale Passwortlebensdauer
Passcode history (1-50 passcodes)	Das Benutzen eines alten Passworts ist nach dieser Anzahl wieder erlaubt

Ein Klick auf den Papierkorb öffnet den Passwort-Reset Dialog, mit welchem ein vergessenes Gerätepasswort entfernt werden kann.



<u>Certificate</u> (nur auf Device Ebene)

Installed Certificates

Zeigt die auf dem Gerät verfügbaren Zertifikate an

•	►	Passcode	Certificate	Encryption	Single Sign On				support@mi	lanconsult.de	e 🗸
	Installed	d Certificates									
	Common	Name				\$ Is Identity	¢	valid to	\$	Show	\$
	33A1A2E	D1-CB30-E2D3-	C1D2-6D7FC50E7	352		YES		30.04.2017 - 13:25			

Encryption

Require storage encryption	Aktivieren Sie die eingebaute Verschlüsselungsfunktion des Gerätes

Single Sign-On

Unter dem Punkt "Single Sign-On" können Sie eine Kerberos Authentifizierung einstellen.

Hier legen Sie die Zugangsdaten und die jeweiligen URLs / Apps fest, die die Tokens des Kerberos benutzen dürfen.

Verfügbar im Supervised-Modus

Account Name	Account Name
Principal Name	Einzigartige Identität an welchem der Kerberos Tickets verteilen darf
Realm	Ihr zu benutzender Kerberos Realm (z.B. Ihre Domain)

Mit dem 💿 Symbol können Sie weitere URLs festlegen.

URL pattern used to limit this account	Festzulegende URLs an welche der
	Kerberos Tickets verteilen darf

Mit dem 💿 Symbol können Sie weitere Apps festlegen.



1	A nume to live it this associat	Cast-ularanda Anna an walaba dan
	Apps to limit this account	Festzulegende Apps an weiche der
		Kerberos Tickets verteilen darf



End of Life (nur auf Device Ebene)

<u>Wipe</u> (nur auf Device Ebene)

Unter "Wipe" können Sie das Gerät auf die Werkseinstellungen zurücksetzen, hier werden sowohl die geschäftlichen, als auch die privaten Daten auf dem Endgerät gelöscht



Wipe Device	X
Are you sure to wipe the device ?	
No	Yes

Mit "Yes" können Sie die Löschung durchführen.

Unter "Wipe Report" können Sie sich folgende Dinge anzeigen lassen

Wiped by	Historie von wem der Wipe ausgeführt wurde
Date	Datum
Status	Status (z.B. ob der Wipe erfolgreich durchgeführt wurde)



Restriction Settings

Device Functionality

Sperren Sie hier einzelne Funktionalitäten des Endgerätes

Allow installing apps	Installation von Apps zulassen
Allow camera	Verwendung der Kamera zulassen
Allow FaceTime	FaceTime zulassen
Allow screen capture	Bildschirmfoto erlauben
Allow auto sync while roaming	Automatische Synchronisierung beim Roaming
	zulassen
Allow Siri	Siri erlauben
Allow voice dialing	Sprachwahl erlauben
Allow in-app purchase	App-interne Käufe erlauben
Require iTunes Store	Es finden für alle Apps immer eine
password for all purchases	Passwortabfrage statt
Allow multiplayer gaming	Mehrspielermodus erlauben
Allow adding Come Contor	Hinzufügen von Come Conter Freunden
friends	
Allow open from managed to	Öffnen von Content in managed Apps in
unmanaged	unmanaged Apps zulassen
Allow open from unmanaged to	Öffnen von Content in unmanaged Apps in
managed	mangaged Apps zulassen
Allow today view in lock screen	Wenn diese Einstellung aktiv ist, wird die
	"Heute" Ansicht im Notification Center auf dem
	Sperrbildschirm angezeigt
Allow control center in lock	Control Center auf dem Sperrbildschirm
screen	erlauben
Allow TouchID	Touch ID zulassen
Allow over-the-air PKI updates	Over-the-air PKI Updates zulassen
Allow passbook while locked	Passbook bei Gerätesperre erlauben
	Diese Funktion deaktiviert das Ad Tracking (z.B.
Limit Ad Tracking	können Werbeanbieter das Ad Tracking nicht
	nutzen um personalisierte Werbung zu verteilen)
Allow Handoff	Handoff zulassen
Allow internet results in	Suchergebnisse in der Spotlight Suche zulassen
spotlight	(z.B. Bing od. Wikipedia)
Require passcode on first	Passwort bei erster AirPlay-Verbindung
AirPlay pairing	erfordern
	Falls aktiviert, wird die Apple Watch dazu
Force Watch Wrist Protection	
	Erkennung) zu nutzen
Allow ICloud Photo Library	Erlaubt die iCioud Fotopibliotnek, falls nicht
	enaupt werden alle Fotos die nicht vollstandig
	von der ICioud neruntergeladen Worden SINd
	vom lokalen Speicher gelöscht



Verfügbar im S	Supervised-Modus
Allow Account Modification	Änderungen an den "Mail, Kontakte,
	Kalender" Einstellungen zulassen
Allow AirDrop	AirDrop zulassen
Allow App Cellular Modification	Diese Einstellung blockiert die Änderung welche Apps mobile Daten nutzen darf Diese Einstellung kann z.B. zuerst am Endgerät händisch angelegt werden und anschließend diese Restriktion aktiviert
	Werden
content from the web	websuche auf bestimmten webseiten wird verhindert, z.B. Wikipedia weil hier jeder beliebige Änderungen vornehmen kann
Enable Siri profanity filter	Schimpfwörter, welche an Siri gerichtet sind, werden zensiert
Allow iBook Store	iBook Store erlauben
Allow iBook Store Erotica	iBook Store Erotika erlauben
Allow modifying Find my Friends	Änderungen der Find my Friends
settings	Einstellungen zulassen.
Allow Game Center	GameCenter erlauben
Allow Host Pairing	Verbindung zum Computer verbieten
Allow installing configuration profiles	Installation von Konfigurationsprofilen zulassen
Allow Remove App	Löschen von Apps verhindern
Allow iMessage	iMessage erlauben
Allow erase all contents and settings	Löschen aller Inhalte und Einstellungen zulassen
Allow configuring restrictions	Konfiguration von Einschränkungen zulassen
Allow Podcast	Podcasts erlauben
Allow Definition Lookup	Wörterbuch erlauben
Allow Predictive Keyboard	Personalisierte Tastaturvorschläge zulassen
Allow Auto Correction	Autokorrektur erlauben
Allow Spell Check	Rechtschreibüberprüfung erlauben
Allow UI App Installation	Falls deaktiviert, können keine Apps aus dem öffentlichen AppStore installiert werden (das Icon wird nicht mehr angezeigt), jedoch können noch Apps über iTunes und den Konfigurator installiert werden
Allow Keyboard Shortcuts	Erlauben der Keyboard Shortcuts, falls das Gerät mit einer mechanischen Tastatur verbunden ist
Allow Apple Watch pairing	Verbieten einer Kopplung zwischen Gerät und der Apple Watch, bereits vorhandene Verbindungen werden getrennt



Allow Passcode modification	Falls nicht zugelassen, kann kein Gerätepasswort hinzugefügt, geändert
Allow devicename modification	Richtlinie ob der Geratename geandert werden darf
Allow wallpaper modification	Richtlinie ob das Hintergrundbild
	geändert werden darf
Allow automatic app downloads	Falls deaktiviert, wird eine gekaufte App nicht automatisch auf anderen Geräten installiert, betrifft nicht das Update von bereits bestehenden Apps
Allow News	Erlauben von News auf dem iOS Gerät
Allow Enterprise app trust	Wenn auf "false" gesetzt ist, werden
	Enterprise Apps nicht vertraut.

<u>iCloud</u>

Sperren Sie bestimmte Funktionalitäten mit der iCloud Synchronisierung

Allow backup	Backups erlauben
Allow document sync	Dokumentsynchronisation erlauben
Allow Photo Stream	Photo Stream zulassen
Allow Shared Photo Stream	Geteilten Photo Stream zulassen
Allow Cloud Keychain Sync	Schlüsselbund Synchronisation zulassen
Allow managed apps to store data	Managed Apps erlauben, Daten zu
	speichern
Allow notes and highlights sync for	Synchronisierung von Markierungen &
enterprise books	Notizen in Enterprise Books zulassen
Allow backup of enterprise books	Backups für Enterprise Books erlauben

Security and Privacy

Sperren Sie Funktionalitäten im Zusammenhang mit diagnostischen Daten

Allow diagnostic data to be send to Apple	Übermittlung von diagnostischen Daten an Apple zulassen
Allow user to accept untrusted TLS certificates	User erlauben, nicht vertrauenswürdige TLS Zertifikate zu akzeptieren
Force encrypted backups	Verschlüsselte Backups erzwingen



BYOD Container

Built-In iOS Security (Container)

iOS war schon immer in der Lage, zwischen verwaltet (geschäftlich) und nicht verwaltet (privat) zu unterscheiden.

Alles, was aus dem MDM-System kommt, wird als verwaltet behandelt. z.B. wenn Sie eine App über MDM installieren oder ein Exchange-Konto einrichten, wird dies als vom iOS als verwaltet behandelt.

Alles andere, was manuell auf dem Gerät konfiguriert/installiert wird, wird als unmanaged behandelt. z.B. wenn der Benutzer WhatsApp selbst installiert oder ein Exchange-Konto hinzufügt.

Diese Trennung wirkte sich jedoch nie auf die Kontakte aus.. Aber seit iOS 11.3 (und höher) wurde dies auch für die Kontakte hinzugefügt.

Da es sich hierbei um eine Grundfunktionalität des Betriebssystems handelt, müssen Sie weder etwas installieren noch einen speziellen Container einrichten.

Setzen Sie den Schalter unter BYOD -> Built-In iOS Security auf "On" damit die Trennung aktiviert wird. Dies führt unter anderem auch dazu, dass einige Schalter in der Konsole ausgegraut werden, damit diese nicht versehentlich umgestellt werden und die Trennung wieder aufheben.

<u>Activation</u>

Aktivieren Sie die von AppTec360 unterstützten Container-Lösungen

Enable Google Divide Container	Aktivieren des Google Divide Containers
Enable SecurePIM Container	Aktivieren des SecurePim Containers

Sollten Sie den SecurePIM Container aktiviert haben finden Sie unter "Activation" noch folgenden Punkt, ebenfalls werden direkt oben vier weitere Tabs freigeschaltet die im Nachgang beschrieben werden.

Support Email Address	Support E-Mail Adresse an die sich die
	User bei Problemen wenden können

SecurePIM Password

Unter "SecurePIM Password" können Sie die Richtlinien für die Passwort-Stärke vornehmen.

Session Timeout	Hier können Sie festlegen nach wie viel Minuten das Passwort erneut eingeben
	werden muss, nachdem SecurePIM im Hintergrund läuft



Password Length	Passwortlänge um Zugang zum
5	SecurePIM Container zu erhalten
Upper Case Characters	Mindestanzahl an Großbuchstaben
Lower Case Characters	Mindestanzahl an Kleinbuchstaben
Special Characters	Mindestanzahl an Sonderzeichen
Digits	Mindestanzahl an Zahlen
	Anzahl wie oft das Passwort falsch
Wipe Application	eingegeben werden darf, bis der
	Soouro DIM Inholt golöopht wird
	Secure initial geloscht wird
	(Die App bleibt dennoch weiterhin auf
	dem Endgerät bestehen)


SecurePIM Security

Unter "SecurePIM Security" können Sie diverse Sicherheitseinstellungen vornehmen.

Detect Jailbroken Devices	Sollte diese Einstellung aktiv sein, wird der Zugang zum SecurePIM Container gesperrt, sobald das Gerät als jailbroken erkannt wird
Secure Text Fields	Der Inhalt der Eingabefelder wird verschlüsselt, keinerlei Informationen gelangen an das Betriebssystem (iOS) Hinweis: Sofern diese Einstellung aktiv ist, ist eine Auto-Korrektur nicht mehr möglich
Export Contact Data to Device	Sollte diese Einstellung aktiv sein, ist es dem User erlaubt die Exchange Kontakte auf sein lokales Gerät zu exportieren Hinweis: Nur der Name und die Telefonnummer werden exportiert
Show Event Location	Sollte diese Einstellung aktiv sein, wird der Ort des bevorstehenden Events in der Benachrichtigungsleiste angezeigt
Show Event Title	Sollte diese Einstellung aktiv sein, wird der Name des bevorstehenden Events in der Benachrichtigungsleiste angezeigt

SecurePIM Browser

On On		
Whitelisted URLs		0
http://www.apptec360.com/		•
Blacklisted URLs		0
www.facebook.com		•
Bookmark Title	Bookmark URL	0
AppTec English	http://www.apptec360.com/en_home.html	•

Hier können Sie den hauseigenen Browser von SecurePIM konfigurieren.

Mit dem 🖸 Symbol sind Sie in der Lage ein neue URL zu definieren.

Mit dem Symbol können Sie eine definierte URL wieder entfernen.



"Whitelisted URLs" sind URLs die aufgerufen werden dürfen.

"Blacklisted URLs" sind URLs die nicht aufgerufen werden und somit blockiert werden.

Beachten Sie bitte, dass die Whitelist Einträge höher priorisiert werden als die Blacklist Einträge.

Unter "Bookmark Title" können Sie einen Titel vergeben, anhand der "Bookmark URL" können Sie eine URL Adresse dem Bookmark Titel vergeben – somit können Sie individuell Lesezeichen an die jeweiligen User verteilen.

<u>Exchange</u>

Unter "Exchange" können Sie ein Exchange Konto konfigurieren.

ActiveSync Email Address	Exchange E-Mail Adresse (beachten Sie die "Placeholders")	
ActiveSync Exchange Login	Exchange Benutzernamen (beachten Sie die "Placeholders")	
ActiveSync Exchange Server	Exchange Server Adresse (FQDN)	
ActiveSync Exchange Domain	Exchange Domain Adresse	
User Certificate	Benutzerzertifikat	
Certificate based authentication	Benutzer authentifizieren sich anhand des Zertifikats	
Allow S/MIME Encryption	Erlaubt es dem User seine Mails zu verschlüsseln	
Allow S/MIME Signing	Erlaubt es dem User seine Mails zu signieren	
CRL Check	Falls aktiv wird das private Zertifikat mit der CRL (Certificate Revocation List) abgeglichen	



Connection Management

<u>Wifi</u>

Services Set Identifier (SSID)	SSID des zu verbindenden Netzwerks	
Auto Join	Automatischen Beitreten zum Netzwerk aktivieren	
Hidden Network	Aktivieren, falls der AP die SSID nicht broadcastet	
Proxy Setup	Konfigurieren eines Proxy für den Access Point	
None	Keinen Proxy festlegen	
Manual	Einen Proxy manuell festlegen	
Proxy Server URL	Adresse zum Abrufen der Proxy Settings	
Port	Port für den Proxy festlegen	
Authentication	Username zur Authentifizierung am Proxy	
Password	Passwort zur Authentifizierung am Proxy	
Automatic	Einen Proxy automatisch festlegen	
Proxy Server URL	URL zum Abrufen der Proxyeinstellungen	
Security Type	Sicherheitstyp des AP festlegen	
WEP		
Password	Passwort für den AP	
WPA/WPA2		
Password	Passwort für den AP	
WEP Enterprise – WPA / WPA2 Enterprise – Any Enterprise		
Protocols		
ILS	Aktivieren bzw. Deaktivieren	
TTLS	Aktivieren bzw. Deaktivieren	
LEAP	Aktivieren bzw. Deaktivieren	
PEAP	Aktivieren bzw. Deaktivieren	
EAP-FAST	Aktivieren bzw. Deaktivieren	
FAP-SIM	Aktivieren bzw. Deaktivieren	



Use PAC	Nutzung von PAC (Protected Access Controll)	
Provision PAC	Konfiguration von Provision PAC	
Provision PAC Anonymously	Anonyme Provisionierung von PAC	
Inner Authentications	Authentifizierungsprotokoll welches genutzt werden soll (ausschließlich bei TTLS): PAP, CHAP, MSCHAP, MSCHAPv2	
Authentication		
Username	Username zur Authentifizierung	
Don't use Per-Connection Password	Kein Per-Verbindung Passwort verwenden	
Identity Certificate	Zertifikat zur Authentifizierung hochladen / auswählen	
Outer Identity	Extern sichtbare Identität	
Trust		
Trusted Certificate 1	Erstes Vertrautes Zertifikat hochladen	
Trusted Certificate 2	Zweites Vertrautes Zertifikat hochladen	
Trusted Certificate 3	Drittes Vertrautes Zertifikat hochladen	
Trusted Server Certificate Names	Die Namen der zu erwartenden Serverzertifikate (in einer kommagetrennten Liste)	
None	Keine Sicherheit festlegen	



<u>VPN</u>

Connection Name	Name des VPN-Profils	
VPN Type		
VPN	Der gesamte Netzwerkverkehr des Gerätes wird über die VPN-Verbindung	
	delates with uper die VI N-Verbindung	
Connection Type	VPN-Verbindungstyp festlegen	
IPsec (cisco)	IPsec Protokoll von cisco	
PPTP	PPTP Protokoll	
I 2TP		
Cisco AnyConnect	AnyConnect Protokoll	
Juniper SSI	Juniper SSI Protokoll	
F5 SSI	E5 SSI Protokoll	
SonicWall mConnect	SonicWall Mobile Connect	
Aruba VIA	Aruba VIA Protokoll	
Custom SSI	Verbindung über Custom SSI	
Por-Ann VPN	Bei Öffnen einer bestimmten Ann wird	
	die VPN-Verbindung bergestellt	
Automatically start Per-App	Bei Start der App wird die VDN	
VPN connection	Verbindung automatisch bergestellt	
Connection Type	VPNLVerbindungstvp festlegen	
Cisco AnyConnect		
F5 SSI	F5 SSL Protokoll	
SonicWall mConnect	SonicWall Mebile Connect	
	Aruba VIA Protokoll	
Custom SSI	Verbindung über Custom SSI	
	Open//PN Protokoll	
Provy Setup	Konfigurieren eines Provy für die VPN	
	Verbindung	
None	Keinen Proxy festlegen	
Manual	Einen Proxy manuell festlegen	
Proxy Server URL	Adresse zum Abrufen der Proxy Settings	
Port	Port für den Proxy festlegen	
Authentication	Username zur Authentifizierung am	
	Proxv	
Password	Passwort zur Authentifizierung am Proxy	
Automatic	Finen Proxy automatisch festlegen	
Proxy Server URI	URI zum Abrufen der	
	Proxyeinstellungen	
Show Placeholders	Zeigt alle verfügbaren User-Variablen	
	an. welche AppTec benutzen kann	



<u>APN</u>

Access Point Name	Der Name des Access Points
Access Point User Name	Der Benutzername des AP User
Access Point Password	Password des AP Users
Proxy Server	Adresse des Proxy Servers
Port	Der entsprechende Proxy Port

<u>Cellular</u>

Enable Data Roaming	Aktivieren des Datenroamings
Enable Voice Roaming	Aktivieren des Sprachroamings
Enable Hotspot	Aktivieren des Hotspots erlauben

HTTP Proxy

Proxy Type	
Manual	Einen Proxy manuell festlegen
Proxy Server URL	Adresse zum Abrufen der Proxy
	Settings
Port	Port für den Proxy festlegen
Authentication	Username zur Authentifizierung am
	Proxy
Password	Passwort zur Authentifizierung am
	Proxy
Automatic	Einen Proxy automatisch festlegen
Proxy PAC URL	PAC URL des Proxy
Allow direct connection if PAC	Verbindung ohne VPN zulassen, falls
is unreachable	der PAC nicht erreichbar ist.
Allow bypassing proxy to access	Erlauben, an dem Proxy vorbei, sich zu
captive networks	internen Netzwerken zu verbinden.

<u>AirPrint</u>

IP Address	IP-Adresse des Druckers
Resource Path	Eindeutiger Pfad zum AirPrint Gerät

<u>AirPlay</u>

Device Name	Name des Gerätes	
Password	Passwort zum Verbinden	
	Definieren Sie eine Liste an Geräten,	
Whitelist	mit welchen sich das Gerät	
	ausschließlich verbinden darf	



PIM Management

Exchan	ge	Active	Sync
	-		

Account Name	Name des Email Accounts
Exchange ActiveSync Host	Adresse/FQDN des Servers
Allow Move	Das Bewegen von Mails zulassen
Use Only in Mail	Interaktionen dürfen nur in der nativen
	Mail App stattfinden
Use SSL	Benutze die SSL Verschlüsselung
Domain	Domäne des Servers
User	Benutzername
eMail Address	eMail Addresse (nur auf Device Ebene)
Password (nur auf Device Ebene)	Passwort des Benutzers
	Wählen Sie das entsprechende
Identity Certificate	Zertifikat zur Authentifizierung am
	Server aus
	Anzahl an Tagen, bis zu welchen die
Past Days of Mail to Sync	Mails zurücksynchronisiert werden
	sollen.
	No Limit = Keine Begrenzung
Enable S/MIME	S/MIME Verschlüsselung aktivieren
Signing Certificate	Das entsprechende Signing Certificate
	hochladen
Encryption Certificate	Das entsprechende Encryption
	Certificate hochladen

<u>eMail</u>

Einrichten von POP3 / IMAP Konten am Endgerät

Account Description	Name des Email Accounts
Account Type	
IMAP	
Path Prefix	Der Pfad Prefix für spezielle Ordner
POP	
User Display Name	Angezeigter Benutzername
Email Address	Email-Adresse des Benutzers
Allow Move	Das Bewegen von Mails zulassen
Enable S/MIME	S/MIME Verschlüsselung aktivieren
Signing Certificate	Das entsprechende Signing Certificate
	hochladen
Encryption Certificate	Das entsprechende Encryption
	Certificate hochladen

Inco	ming	Mail
	<u> </u>	

Eingehende Servereinstellungen



Mail Server Address	Adresse des Mail Servers	
Mail Server Port	Port des Mail Servers	
User Name	Entsprechender Benutzername	
Authentication Type	Authentifizierungsmethode	
None	Keine Authentifizierungsmethode	
Password (nur auf Device	Passwortabfrage	
Ebene)		
MDM Challenge-Response		
NTLM	NTLM-Authentifizierung	
HTTP MD5 Digest		
Use SSL	Aktivieren, falls SSL benötigt	

Outgoing Mail	Ausgehende Servereinstellungen		
Mail Server Adress	Adresse des Mailservers		
Mail Server Port	Port des Mail Server		
User Name	Entsprechender Benutzername		
Authentification Type			
None	Keine Authentifizierungsmethode		
Password (nur auf Device	Passwortabfrage		
Ebene)			
MDM Challenge-Response			
NTLM	NTLM-Authentifizierung		
HTTP MD5 Digest			
Use SSL	Aktivieren, falls SSL benötigt		
Outgoing password same as incoming	Ausgehendes Passwort entspricht dann dem eingehenden Passwort		
	Aktivieren, falls ausgehende		
Use only in mail	Nachrichten nur über die Mail-App		
	versendet werden sollen		

<u>CalDav</u>

Einrichtung und Verteilung eines CalDav Accounts konfigurieren

Account Description	Angezeigter Name des Accounts	
Hostname	Hostname bzw. IP Adresse	
Port	Port des CalDav Accounts	
Principal URL	Principal URL des Accounts	
Username	Entsprech. CalDav Benutzername	
Password (nur auf Device Ebene)	Entsprech. CalDav Passwort	
Use SSL	Aktivieren, falls SSL benötigt	

Subscribed Calendars

Einrichtung und Verteilung von Subscribed Calendars



Description	Angezeigter Name des Accounts	
URL	URL der Kalenderdatei	
Username	Benutzer des Kalenderabos	
Password (nur auf Device Ebene)	Passwort des Kalenderabos	
Use SSL	Aktivieren, falls SSL benötigt	

<u>LDAP</u>

Richten Sie an dieser Stelle eine LDAP-Verbindung ein, um einen dynamischen Zertifikatsaustausch zwischen Endgerät und Active Directory zu erlauben.

Beachten Sie, dass der benutzte User entsprechende Leseberechtigungen benötigt.

Account Description	Beschreibung des Accounts
Account Username	Benutzer für den LDAP-Zugriff
Account Password	Passwort für den LDAP-Zugriff
Account Hostname	Hostname/IP Adresse des LDAP Servers
Use SSL	Aktivieren, falls SSL benötigt

Im zweiten Abschnitt können Sie noch die einzelnen Filter zur Suche im LDAP Verzeichnis definieren.

Description	Scope	Search Base
Beschreibung des Filters	Suchlevel im LDAP Verzeichnis	Definieren der einzelnen Filter

Web Management

<u>Webclips</u>

Definieren Sie an dieser Stelle Lesezeichen mit Links zu Webseiten,



Intranetportalen etc, welche daraufhin als Applikation auf dem Endgerät zu sehen sein werden.

Label	Name der Verknüpfung auf dem		
	Endgerät		
URL	Link zur entsprechenden Website		
Removeable	Wenn aktiviert, kann der User den		
	Webclip entfernen		
Icon Laden Sie über diesen Dialog ein			
	Logo für die Verknüpfung hoch:		
	Maße 180x180, Format png		
	Wenn aktiviert, werden keine		
Precomposed Icon	zusätzlichen Effekte (Schatten,		
	Glanz) auf dem Icon angezeigt		
Full Screen Bei Öffnen des Webclips öffn			
	der Browser im Vollbildschirmmodus		

Web Content Filter

Der Web Content Filter ermöglicht es, Zugriff auf bestimmte Internetseiten zu begrenzen.

Allowed Websites	
Limit Adult Content	Es wird automatisch ein Webfilter für
	nicht jugendfreie Inhalte angewandt
Permitted URLs	Fügen Sie über das + Symbol
	entsprechende zugelassene Seiten
	hinzu
Blacklisted URLs	Fügen Sie über + Symbol
	entsprechende gesperrte Seiten
	hinzu
Specific Websites Only	Es können nur die definierten Inhalte
	angezeigt werden, welche Sie über
	das + Symbol hinzufügen können.



App Management

Enterprise App Manager

Installed Apps (nur auf Device Ebene)

* -	• •	Installed Apps	Mandatory Apps	Web Apps	suppor	t@milanconsult.de 🗸
		Application Na	ame	:	> Version	♦ VPN ♦ ●
	9	AppTec EMM			2.4	
	C	ContentBox			2.0	

Über das 💿 Symbol lassen sich direkt neue Apps auf das Endgerät pushen.

Sie können sowohl eine "Apple AppStore" App aus dem öffentlichen AppStore auf das Gerät pushen, als auch eine eigenentwickelte In-House App.

Oder Sie wählen unter der Kategorie "iOS In-House Apps" einer Ihrer unter den General Settings hochgeladene In-House App aus.

Bitte beachten Sie dass dies nur ein einmaliger Befehl ist, sollte dieser aus welchen Gründen auch immer an Endgerät nicht ankommen, findet keine Wiederholung statt!



Installations-Optionen

Keep up to date (nur für VPP im Device Mode)	Es wird binnen einer Woche überprüft, ob ein Update für die App vorhanden ist, falls ja wird dieses Update installiert Bei In-House Apps wird das Update Target, welches in den General Settings definiert ist, zur Aktualisierung verwendet.
Overtake when unmanaged	Ist die App bereits auf dem Gerät installiert, wird sie vom MDM übernommen und verwaltet
Remove app when MDM profile is removed	Bei Entfernung der Geräteverwaltung wird die App deinstalliert
Prevent backup of app data	Es wird kein Backup von app-spezifischen Daten erstellt
App Setting	Unter "App Settings" können Sie einer App (sofern die App das unterstützt, fragen Sie ggf. beim Hersteller der App nach) bestimmte Werte im Vorfeld mitgeben.

Sie können auch direkt über "Upload In-House App" eine ipa Datei auswählen und diese hochladen.

Upload an In-House App	\times
Upload Limit: max. size of ipa files is 50 MB	
Select the .ipa file of the iOS application which you want to upload	
Durchsuchen Keine Datei ausgewählt.	

Mandatory Apps

Unter den Mandatory Apps können Sie zwingend erforderliche Apps festlegen. Der User wird ständig dazu aufgefordert sich diese besagte App zu installieren.

Über das 💿 kann direkt eine zwingend erforderliche App definiert werden.





Dies kann wie bei den "Installed Apps" eine Apple App Store App sein, aber auch eine In-House App.

Sollte es sich um ein Supervised Gerät handeln, wird die App automatisch installiert.

Die Bedienung findet gleich statt wie beim Punkt Installed Apps.



Web Apps

Unter dem Punkt "Web Apps" können, ähnlich wie bei den "Web Clips" im Bereich Web Management, Internetseiten oder Intranetportale als Applikation auf das Endgerät gepusht werden, standardmäßig werden Web Apps im Vollbildschirm angezeigt, bei den Webclips ist dies einstellbar.

Installed Apps Mandat	ory Apps Web Apps		👤 support@milanconsult.de 🗸
On			0 0
Label		Test	0
URL		http://www.google.de	0
Removable		On On	0
Icon		9bc3b1b1501ea3f190efa6c83c429a91.png	
			@
Precomposed Icon		On On	0

Label	Name der Verknüpfung auf dem Endgerät
URL	Link zur entsprechenden Website
<u>Removeable</u>	Wenn aktiviert, kann der User den Webclip entfernen
Icon	Laden Sie über diesen Dialog ein Logo für die Verknüpfung hoch: Maße 180x180, Format png
Precomposed Icon	Wenn aktiviert, werden keine zusätzlichen Effekte (Schatten, Glanz) auf dem Icon angezeigt)



Restriction & Settings

Blacklisted / Whitelisted Apps

Hier können Sie, abhängig davon ob Sie in den General Settings Black- oder Whitelisted aktiviert haben, Apps hinzufügen die dann geblockt/erlaubt

werden. Ein Klick auf das Symbol bringt die gewohnte App-Suche hervor über diese Sie dann die gewünschte App suchen und hinzufügen können.

Beachten Sie, dass supervised Geräte für diese Funktion notwendig sind.

SysApp Restrictions

Sperren Sie hier einzelne Applikationen des Endgerätes

Allow use of YouTube	Benutzung von YouTube zulassen
Allow use of iTunes Store	Benutzung des iTunes zulassen
Allow use of Safari	Benutzung von Safari zulassen
Enable autofill	Automatisches Ausfüllen aktivieren
Force fraud warning	Betrugswarnung erzwingen
Enable JavScript	JavaScript aktivieren
Block pop-ups	Pop-Ups unterdrücken
Allow Cookies	Regelt, wann Safari Cookies akzeptiert



Available in supervised mode				
Allow Appstore	Erlaubt die Verwendung des Appsotres			
Allow Calculator	Erlaubt die Verwendung des Rechners			
Allow Calendar	Erlaubt die Verwendung des Kalenders			
Allow Clock	Erlaubt die Verwendung der Uhr			
Allow Compass	Erlaubt die Verwendung des Kompasses			
Allow Contacts	Erlaubt die Verwendung der Kontakte			
Allow Facetime	Erlaubt die Verwendung von Facetime			
Allow Find Friends	Erlaubt die Verwendung von Freunde			
Allow Find iPhone	Erlaubt die Verwendung der iPhone-Suche			
Allow Photos	Erlaubt die Verwendung von Fotos			
Allow Game Center	Erlaubt die Verwendung vom Game Center			
Allow Health	Erlaubt die Verwendung von Health			
Allow iBooks	Erlaubt die Verwendung von iBooks			
Allow iCloud Drive	Erlaubt die Verwendung von iCloud Drive			
Allow iTunes	Erlaubt die Verwendung iTunes			
Allow Mail	Erlaubt die Verwendung von Mail			
Allow Maps Erlaubt die Verwendung von Karten				
Allow Messages	Erlaubt die Verwendung von Nachrichten			
Allow Music	Erlaubt die Verwendung von Musik			
Allow Notes	Erlaubt die Verwendung von Notizen			
Allow Photo Booth	Erlaubt die Verwendung des Fotoautomaten			
Allow Podcasts	Erlaubt die Verwendung von Podcasts			
Allow Reminder	Erlaubt die Verwendung von Erinnerungen			
Allow Safari	Erlaubt die Verwendung von Safari			
Allow Stocks	Erlaubt die Verwendung von Aktien			
Allow Tipps	Erlaubt die Verwendung von Tipps			
Allow Videos	Erlaubt die Verwendung von Videos			
Allow Voice Memos	Erlaubt die Verwendung der Sprachmemos			
Allow Wallet	Erlaubt die Verwendung von Wallet			
Allow Watch	Erlaubt die Verwendung von AppleWatch			
Allow Weather	Erlaubt die Verwendung von Wetter			
Allow WebClips	Erlaubt die Verwendung von WebClips			



<u>App-VPN</u>

Über das 🕥 Symbol können Sie Applikationen definieren, welche beim Starten automatisch die ausgewählte VPN-Verbindung aufbauen.

•	►	Blacklisted Apps	SysApp Restrictions	App-VPN	App Setting	gs	S	upport@milanconsul	t.de 🗸
	S Or								
A	pplicatio	n				Per App VPN			0
	\$	Pulse Secure			*	none		~	•

App Settings

Unter "App Settings" können Sie einer App (sofern die App das unterstützt, fragen Sie ggf. beim Hersteller der App nach) bestimmte Werte im Vorfeld mitgeben.

Über das Symbol können Sie eine (weitere) App hinzufügen. Sie finden die gewohnte AppTec Darstellung eines App-Imports wieder.

Suchen Sie hier nach der App die Sie gerne konfigurieren möchten und wählen Sie diese aus. Diese Einstellungen werden nur auf Apps angewandt die vom MDM verwaltet werden.

Sollte der Import erfolgreich gewesen sein, erhalten Sie folgende Ansicht:

On				
Application		Set	tting	0
🔶 Div	ie 🗘	i.	8	•

Sie können nun mit einem Klick auf das diverse Anpassungen vornehmen.



Folgende Übersicht werden Sie dann erhalten:

App Settings	\times
PLIST Key / Value	
Show Diaceboilders	Sauo

Sollten Sie bereits eine vorhandene PLIST (Quelltext der Konfiguration) haben, können Sie diesen hier einfügen und mit "Save" das ganze abspeichern.

Unter "Key / Value" können Sie der App spezifische Konfigurationen mitgeben.

App Settings			\times
PLIST Key / Value			
Кеу	Value		Туре 🕒
Show Placeholders		Save	
Show Fracesholders		Gave	

Hier können Sie mit dem Symbol einen neuen Key und den dazu gehörigen Wert (Value) setzen.

Show Placeholders

App Settings		×
PLIST Key / Value		
Key	Value	Туре
email_address	%usermail%	String 🗸

Save



Selbstverständlich stehen Ihnen alle Platzhalter von AppTec zur Verfügung.

Erklärung der "Type":

String	Text
Boolean	True/False (wahr / falsch)
Number	Nummer

Mit dem 🗢 Symbol können Sie eine App wieder entfernen.

Enterprise App Store

iTunes Apps

Unter diesem Punkt können Sie optionale Apps für Ihre User verteilen. Sollte sich hier eine App befinden, wird automatisch auf dem Endgerät der AppTec Store installiert.

Dies sind lediglich Verlinkungen auf den offiziellen Apple App Store, aus diesem Grund muss auf jedem Endgerät eine Apple ID hinterlegt sein. Wir empfehlen an dieser Stelle, dass jeder User seine eigene Apple ID besitzt.

Mit dem 💿 können Sie weitere Apps hinzufügen.

Application Name	Version 🗘	0

Danach sollte Sich ein Fenster mit folgender Übersicht öffnen.

Bitte beachten Sie, dass nur kostenlose Apps angezeigt werden, kostenpflichtige Apps werden nur über das VPP angezeigt.

Select an application						\times
Apple iTunes						
Q Enter Searchterm here	Tablet	~	Germany	~	Search Now	

Bei "Enter Seachterm here …" können Sie nach einer sich im Apple App Store befindenden App suchen.



Install

Apple iTun	les		
Q db navi	igator	Tablet Germany Search Now	
DB Pev	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
DOTS	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_{\rm}	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

Wenn Sie nun auf das Icon oder auf den Name der App klicken, werden Sie nochmals gefragt, weitere Einstellungen vorzunehmen...

Install DB Navigator für iPa	\times	
Keep up to date	Off	
Remove app when MDM profile is removed.	On On	0
Prevent backup of the app data.	он 🕥	0
App VPN	none	~

Keep up to date	Es wird binnen einer Woche überprüft, ob ein Update für die App vorhanden ist, falls ja wird dieses Update installiert
Remove app when MDM profile is removed	Bei Entfernung der Geräteverwaltung wird die App deinstalliert
Prevent backup of app data	Es wird kein Backup von app- spezifischen Daten erstellt



App-VPN	VPN-Verbindung auswählen,
	welche bei Öffnen der App startet

Nach einem Klick auf "Install" wird die App in den Enterprise App Store hinzugefügt und kann dann vom Endgerät über den AppTec AppStore installiert werden

Sollte der App-Store Import erfolgreich gewesen sein, erhalten Sie folgende Übersicht:

<u>In-</u>	◄ ► iTunes Apps In-house		support@milanconsu	ult.de 🗸
		X		
	Application Name	\$	Version \$	0
	WordPress		4.9	

<u>House</u>

Unter dem Punkt "In-House" können Sie Ihre eigenentwickelten Apps hochladen und verteilen.

Mit dem 💿 können Sie weitere In-House Apps verteilen.



Sollten Sie bisher noch keine In-House App verteilt haben, erhalten Sie nun folgende Übersicht:



Klicken Sie hierzu auf "Upload In-House App", nun erhalten Sie folgende Übersicht:





Wählen Sie nun mit "Durchsuchen…" eine .ipa Datei aus und klicken Sie anschließend auf "Upload"



Ihre App

wird nun hochgeladen, in der Mitte des Kreises können Sie eine Prozentanzahl sehen wie weit Ihre App bereits hochgeladen ist.





Sollte ein Upload der In-House App erfolgreich gewesen sein, sehen Sie nun die eben hochgeladen App in ihrem App Katalog.

(•	Playstore	In-House			Support@	milanconsul	.de 🗸
		Application Na	ime	Version	\$ Size	\$ Package Name	\$	0
		IBM Notes T	raveler	9.0.1.3 201411210833-T7 2.0.0.34-170浙	6.35 MB	forgepond com lotus sync traveler		-

Der User ist nun in der Lage, auf seinem Endgerät diese App im AppTec Enterprise Store unter der Kategorie "In-House" sehen und installieren zu können.

Da es sich hierbei um keine öffentliche Apple AppStore App handelt, braucht der User an seinem jeweiligen Endgerät keine hinterlegte Apple ID.



<u>Kiosk Mode</u>

Der Kiosk Mode erlaubt es Ihnen eine App oder URL vorzudefinieren, dann ist es ausschließlich möglich diese App bzw. URL auszuführen/besuchen.

Ebenfalls können Sie im Kiosk Mode diverse Hardwaretasten deaktivieren.

Verfügbar im Supervised Modus				
Application Type	Package			
	URL			
Package	Wenn Sie eine App im Kiosk Mode starten möchten, wählen Sie unter "Application Type" "Package" aus			
Kiosk Application	Klicken Sie hier, um eine App die im Kiosk Mode gestartet werden soll auszuwählen Sie finden die gängige Übersicht vom App Management vor Sie können zwischen "Apple iTunes Apps", und "iOS In-House Apps" wählen			
URL	möchten, wählen Sie unter "Application Type" "URL" aus			
URL	Definieren Sie hier nun Ihre gewünschte URL Adresse			
Same Origin Policy	Sollte diese Funktion aktiviert sein, kann der User nur unter Unterseiten der vordefinieren URL surfen z.B. haben Sie folgende URL definiert: www.mypage.com der User kann dann auf www.mypage.com/subpage surfen			
Whitelisted URLs	Hier können Sie eine Whitelist pflegen, alle diese URLs sind zulässig Maximal 1 URL pro Linie Eine URL muss mit http:/ oder https:// beginnen			
Blacklisted URLs	Hier können Sie eine Blacklist pflegen, alle diese URLs sind unzulässig Maximal 1 URL pro Linie Eine URL muss mit http:/ oder https:// beginnen			
Clear Browser after inactivity	Nach Inaktivität wird der Browser Cache geleert			
Exit Password Enabled	Wenn Sie diese Funktion aktivieren, ist es dem User möglich, mit den von Ihnen vordefinierten Passwort den Kiosk Mode beenden zu können			
Exit Password	Dies ist das von Ihnen vordefinierte Passwort			



Scheduled Kiosk Mode	Sie können anhand der Uhrzeit den Kiosk Mode planen, dieser wird dann in der von Ihnen definierten Uhrzeit automatisch
Ctart Time	gestartet und beendet
Start Time	Zeit in Minuten, nach dem den Kiegk Mede
	wieder beendet werden soll
Disable Touch	Falls aktiviert, so wird der Touchscreen deaktiviert
Disable Device Rotation	Falls aktiviert, so wird die automatische Bildschirmanpassung deaktiviert
Disable Ringer Switch	Falls aktiviert, so wird der Ringer Switch deaktiviert. Das Verhalten ist daraufhin abhängig von der zuvor eingestellten Funktion
Disable volume buttons	Falls aktiviert, so werden die Lautstärkeknöpfe deaktiviert
Disable Sleep Wake Button	Falls aktiviert, so wird der An/Aus Schalter deaktiviert
Disable Auto Lock	Falls aktiviert, so wird das Gerät nicht automatisch in den Standby gesetzt
Enable Voice Over	Falls aktiviert, so wird der Voice Over Assistent aktiviert
Enable Zoom	Falls aktiviert, so wird der Zoom aktiviert
Enable Invert Colors	Falls aktiviert, so wird der invertierte Displaymodus aktiviert
Enable Assistive Touch	Falls aktiviert, so wird der AssistiveTouch aktiviert
Enable Speak Selection	Falls aktiviert, so wird die Sprachauswahl aktiviert
Enable Mono Audio	Falls aktiviert, so wird Mono Audio aktiviert
VoiceOver	Falls aktiviert, kann der User VoiceOver anpassen
Zoom	Falls aktiviert, kann der User den Zoom anpassen
Invert Colors	Falls aktiviert, kann der User die invertierten Farben anpassen
Assistive Touch	Falls aktiviert, kann der User Assistive Touch anpassen.

Content Management

<u>ContentBox</u>

Hier können Sie die ContentBox aktivieren bzw. deaktivieren

Enable ContentBox	ContentBox aktivieren



Konfiguration Android

Je nachdem ob Sie aktuell ein Profil oder ein Gerät ausgewählt haben, unterscheiden sich die Darstellung und deren Unterpunkte – bitte beachten Sie dies sorgfältig!

General

Profile Overview (nur auf Profil Ebene)

Sollten Sie sich in einem Profil befinden, erhalten Sie hier einen kurzen Überblick über das Profil in Bezug auf Name, OS, Erstellungsdatum, Autor, etc.

Profile Name	Name des Profils – kann direkt hier umbenannt werden
Operating System	Für welches Betriebssystem das Profil
	gilt
Created At	Erstelldatum
Created By	Ersteller des Profils
Profile Revision	Anzahl wie oft das Profil bereits
	geändert wurde

<u>Device Overview</u> (nur auf Device Ebene)

Sollten Sie sich auf einem Gerät befinden, erhalten Sie hier eine zusammenfassende Übersicht des ausgewählten Geräts, folgendes ist hier enthalten:

Device Name	Name des Geräts
Phone Number	Telefonnummer des Geräts
OS Version	OS Version des Geräts
Operating System	Betriebssystem (Android / iOS /
	Windows Phone)
Serial Number	Seriennummer des Geräts
Device Ownership	Firmen oder Privatgerät
Device Typ	Telefon oder Tablet
Rooted	Status ob das Gerät gerootet wurde
Compliant	Den Richtlinien entsprechend
Last Seen	Zeitpunkt an dem sich das Gerät zuletzt
	mit AppTec verbunden hat

Config Revision



Hier erhalten Sie eine Übersicht welches Gruppenprofil dem Gerät zugewiesen ist. Wenn sie auf das Gruppenprofil klicken, kommen Sie direkt zu diesem Profil und können Einstellungen vornehmen.

Mit dem Symbol können Sie die zugewiesenen Apps auf die Einstellung des Gruppenprofils zurücksetzen.

Mit dem Symbol können Sie alle getätigten Apps auf die Einstellung des Gruppenprofils zurücksetzen.

<u>Device Log</u>

Hier erhalten Sie diverse Gerätelogs.

Gegebenenfalls können Sie bei einem Fehler hier direkt die Ursache ausfindig machen.



Device Settings

Client Configuration

Hier können Sie folgende Einstellung für Ihr Android Gerät vornehmen:

Warning message after disabling Device Management	Festgelegte Warnmeldung, sobald der AppTec Geräteadministrator deaktiviert wird
Enforcement action after disabling Device Management	 Die Aktion die ausgeführt werden soll, sobald der Geräteadministrator deaktiviert wird: → do nothing = keine Aktion → Lock Device = Gerät sperren → Wipe Device = Gerät wird auf die Werkseinstellungen zurückgesetzt
Out of Compliance Time	Zeitlimit, nach welchem die "Enforcement Action after compliance" durchgeführt wird, falls das Gerät nicht compliant ist. Min. 1 Minute Max. 24 Stunden
Enforcement action after compliance timeout	 Die Aktion die ausgeführt werden soll, sobald ein Gerät nicht mehr compliant ist. → do nothing = keinerlei Aktionen → Lock Device = Gerät sperren → Wipe Device = Gerät wird auf die Werkseinstellungen zurückgesetzt
Data Collection Frequency	Frequenz in welcher Geräte- und GPS- Informationen gesammelt werden
Device Heartbeat Frequency	Intervall in welchem sich das Gerät beim AppTec Server meldet Min. 1 Minute Max. 24 Stunden
Enable Location Updates	Falls aktiviert, sendet das Gerät Standortinformationen an den AppTec Server
Location Update Time	Bestimmt, in welchem Zeitintervall das Gerät Standortinformationen an AppTec übermitteln soll
Use Network Location for Location Update	Wenn aktiviert, so wir die Netzwerklokalisierung zur Standortbestimmungen benutzt (falls dies unter "Restrictions" deaktiviert wurde, greift diese Einstellung nicht)
Use GPS Location for Location Update	Falls aktiviert, wird GPS für die Standortübermittlung benutzt
Allow Mock (Fake) Locations	Erlaubt das Fälschen der



Standortinformation durch Apps Dritter.

Asset Management (nur auf Device Ebene)

<u>Asset Management</u> (nur auf Device Ebene)

Device Info

Model	Modellbezeichnung des Geräts
Operating System	Betriebssystem
OS Version	Betriebssystem Version
Serial Number	Seriennummer
Device Name	Gerätename
Battery Status	Batterieanzeige
Free / Total Memory	Freier / insgesamter Speicherplatz
Samsung Safe	SAFE Schnittstelle von Samsung, nötig für diverse Einstellungsmöglichkeiten
SD Card Available	SD Karte verfügbar
SD Card Emulated	Emulierte SD Karte auf dem Gerät
SD Card Removable	SD Karte kann entfernt werden
SD Free / Total Memory	Freier / insgesamter Speicherplatz der SD Karte

<u>Wi-Fi</u>

IP Address	IP Adresse des Gerätes
WiFi MAC	WiFi MAC Adresse

<u>Cellular</u>

Status	Status (SIM Karte vorhanden)
Phone Number	Telefonnummer
Roaming (Voice / Data)	Roaming Status für Anrufe / Daten
Roaming Status	Aktueller Roaming Status
IP Address	IP Adresse
Operator/Carrier	Mobilfunk Anbieter
Cellular Technology	Genutzter Mobilfunkstandard
IMEI	IMEI Nummer



ICCID	Dies ist die ID der SIM-Chipkarte, oft auch als Smartcard oder Integrated Circuit Card (ICC)
IMSI	Die International Mobile Subscriber Identity (IMSI; deutsch Internationale Mobilfunk-Teilnehmerkennung) dient in GSM- und UMTS-Mobilfunknetzen der eindeutigen Identifizierung von Netzteilnehmern Die IMSI besteht aus maximal 15 Ziffern und setzt sich folgendermaßen zusammen: • <u>Mobile Country Code</u> (MCC), 3 Ziffern • <u>Mobile Network Code</u> (MNC), 2 oder 3 Ziffern • Mobile Subscriber Identification Number (MSIN) 1 10 Ziffern
Current MCC/MNC	Siehe "SIM MCC/MNC"
SIM MCC/MNC	Der Mobile Country Code ist eine von der ITU im Standard E.212 festgelegte Länderkennung, die zusammen mit dem Mobile Network Code (MNC) zur Identifizierung eines Mobilfunknetzes verwendet wird. Heißt das ist der Ländercode bzw. Mobile Network Code der Simkarte. Wenn man in ein anderes Mobilfunknetz geht ist deshalb logischerweise der "Current MCC/MNC" und "SIM MCC/MNC" unterschiedlich.

<u>Bluetooth</u>

Bluetooth MAC	Bluetooth MAC Adresse



Security Management

Anti Theft (nur auf Device Ebene)

GPS Information (nur auf Device Ebene)

Hier können Sie den aktuellen / letzten Standort des Geräts ermitteln. Die Lokalisierung kann mit einem oder sogar zwei Passwörtern geschützt werden – Siehe: *General Settings – Privacy – GPS Access*



<u>Wipe & Lock</u> (nur auf Device Ebene)

Unter "Wipe & Lock" können Sie folgende drei Aktionen durchführen:

Full Wipe	Das Gerät wird auf die Werkseinstellungen zurückgesetzt (sowohl geschäftliche, als auch persönliche Daten werden gelöscht)
Enterprise Wipe	Nur die Firmendaten werden vom Endgerät entfernt (Alle Apps, Daten, etc. die von AppTec übergeben wurden)
Lock Screen	Bildschirmsperre wird aktiviert, es ist ausreichend das Gerät mit dem Geräte- Passwort/PIN wieder zu entsperren



<u>Message</u> (nur auf Device Ebene)

Mit "Open Message Dialog" können Sie eine Push-Nachricht versenden.

Open Message Dialog

Anschließend sollte sich folgendes Fenster öffnen, dies können Sie mit einem Subject (Betreff) und einer Message (Nachricht) füllen und an das ausgewählte Endgerät versenden.

Send a message		\times
Subject	Test: Bitte bei Ihrer IT melden	
Message	Diese Nachricht dient zur Testzwecken! Bitte melden Sie sich bei Ihrer EDV Abteilung. Mit freundlichen Grüßen Ihre IT-Abteilung	it.

Send Message



Security Configuration

<u>Passcode</u>

Unter "Passcode" können Sie ein Gerätepasswort erzwingen, folgende Einstellungsmöglichkeiten stehen hier zur Verfügung:

Minimum Password length	Legt fest, aus wie vielen Zeichen das
Password quality	Passwortstärke Unspecified = nicht spezifiziert Every password is ok = jedes Passwort ist zulässig at least numeric characters = Mindestens Zahlen müssen enthalten sein at least complex characters = Mindestens komplexe (Sonderzeichen) müssen enthalten sein at least alphanumerical characters = mindestens alphanumerische Zeichen müssen enthalten sein at least alphabetic characters = mindestens alphabetische Zeichen müssen enthalten sein
Maximumg inactivity time look	Zeit der automatischen Tastensperre bei Inaktivität des Users
Minimum lowercase letters required in password	Mindestanzahl von kleingeschriebenen Buchstaben
Minimum uppercase letters required in password	Mindestanzahl von großgeschriebenen Buchstaben
Minimum non-letter characters required in password	Mindestanzahl wie viel "nicht- Buchstaben" Zeichen enthalten sein müssen
Minimum numerical digits required in password	Mindestanzahl wie viel Zaheln für das Passwort erforderlich sind
Minimum symbols required in password	Mindestanzahl wie viel Sonderzeichen enthalten sein müssen
Password expiration timeout	Legt fest, nach welchem Zeitraum das Passwort abläuft und ein neues Passwort vergeben werden muss
Password history restriction	Anzahl der wie viel zuletzt benutzten Passwörter nicht erlaubt sind
Maximum failed password attempts	Legt fest, wie oft das Passwort falsch eingegeben werden darf, bis ein vollständiger Wipe des Gerätes durchgeführt wird



Encryption

Unter diesem Punkt sind Sie in der Lage sowohl den internen Gerätespeicher, als auch den externen SD Kartenspeicher zu verschlüsseln.

Require Storage Encryption	Falls diese Einstellung aktiviert wird, ist der Gerätespeicher verschlüsselt, sofern das Gerät diese Funktionalität unterstützt. Sobald der Gerätespeicher einmalig verschlüsselt wird, ist es nicht mehr möglich diesen wieder zu entschlüsseln. Ebenfalls wird die Passwort Policy automatisch auf mindestens 6 alphanumerische Zeichen umgestellt
Require SD Card Enryption	Diese Einstellung gilt nur für Samsung Geräte! Falls diese Einstellung aktiviert wird, ist die externe SD Karte verschlüsselt und kann nur manuell auf dem Endgerät unter den Einstellungen wieder entschlüsselt werden. Ebenfalls wird dann die Passwort Policy automatisch auf mindestens 6 alphanumerische Zeichen umgestellt

<u>AntiVirus</u>

Scan Method	Quick = Nur Apps werden auf
	Schadcode / Viren untersucht
	Full = Das komplette System wird auf
	Schadcode / Viren untersucht
	Zeitraum in welchem Intervall eine
Scan Interval	Untersuchung (Quick / Full)
	durchgeführt werden soll
	Wie oft ein Update der App und deren
Update Check	Datenbank (Viren / Schadcode)
	durchgeführt werden soll
Protection Mode	Es wird die App beim Starten und
	Installieren auf Schadcode überprüft
	Falls aktiv, darf der User die
Self Configuration	Einstellungen selbst am Endgerät
_	vornehmen bzw. abändern
Connect During Roaming	Verbindungsaufbau während sich das
	Endgerät sich im Roaming befindet



End of Life (nur auf Device Ebene)

<u>Wipe</u> (nur auf Device Ebene)

Unter "Wipe" können Sie das Gerät auf die Werkseinstellungen zurücksetzen, hier werden sowohl die geschäftlichen, als auch die privaten Daten auf dem Endgerät gelöscht

Mit dem Klick auf das "Minussymbol" Sollten Sie folgende Meldung erhalten

Wine SD Card tee?	Ebonfalla dar SD Karton Spainhar wird
wipe SD Card too?	Ebenialis del SD-Kanen Speicher wird
	gelöscht

Wipe Device	X
Are you sure to wipe the device ? Wipe SD Card too ?	
No	Yes

Mit "Yes" können Sie die Löschung durchführen.

Unter "Wipe Report" können Sie sich folgende Dinge anzeigen lassen

Wiped by	Historie von wem der Wipe ausgeführt
	wurde
Date	Datum
Status	Status (z.B. ob der Wipe erfolgreich
	durchgeführt wurde)



Restriction Settings

<u>Restrictions</u>

Hier können diverse Dinge unterbunden und verhindert werden.

Enable Camera	Erlaubung der Kamera
Force Auto Sync	Betrifft die Schnelleinstellung "Sync" Sync On = Synchronisation ist permanent aktiviert Off = Synchronisation ist permanent
	deaktiviert User choice = Vom User selbst wählbar
Force Bluetooth	On = Bluetooth ist permanent aktiviert Off = Bluetooth ist permanent deaktiviert User choice = Vom User selbst wählbar
Force GPS	On = GPS ist permanent aktiviert Off = GPS ist permanent deaktiviert User choice = Vom User selbst wählbar
Force Network Location	On = Permanente Internet-Lokalisierung Off = Permanente Deaktivierung der Internet-Lokalisierung User choice = Vom User selbst wählbar

Für Samsung Geräte mit der SAFE 2.0 oder höher Schnittstelle sind zusätzlich folgende Einstellungsmöglichkeiten verfügbar.

Allow SD Card	Erlauben einer SD Karte
Allow SD Card Write	Erlauben das "Schreiben" auf der SD Karte
Allow Screen Capture	Erlauben von Screenshots
Allow Clipboard	Erlauben der Zwischenablage
Backup settings and app data in Google Cloud	Off = Google Backup deaktivieren On = Google Backup aktivieren User Choice = User Entscheidung


Allow USB Debugging	Erlauben des USB Debuggins (wird z.B. benötigt um Geräte-Logs (ADB) zu erstellen)
Allow Google Crash Report	Erlaubt es dem User Fehlerberichte von Apps an Google zu schicken
Allow Factory Reset	Erlaubt es dem User manuell das Gerät auf die Werkseinstellungen zurückzusetzen
Allow OTA Upgrade	Erlauben von "Over-The-Air" Updates
Allow USB host storage	Wenn aktiviert, kann ein externer USB Speicher in Form von einer HD oder einem SD Kartenleser angebunden werden
Allow USB Media Player (MTP,PTP)	Erlauben von USB Media Player (MTP,PTP)
Allow Microphone	On = Mikrofon für 3rd Party Apps erlauben Off = Mikrofon für 3rd Party Apps ist nicht erlaubt User Choice = Die Entscheidung des jeweiligen Users, ob die 3rd Party App auf das Mikrofon zugreifen darf
Allow NFC (Near Field Communication)	Erlauben von NFC
Allow Unknown Sources (APK Sideloading)	Erlaubt die Installation von Apps außerhalb des Appstores. Der Nutzer muss die Funktion manuell aktivieren wenn sie deaktiviert war und reaktiviert wurde.



AE Device Owner

(Gerät muss sich im Android	Enterprise Device	Owner Mode befinden)
-----------------------------	-------------------	----------------------

Security		
Disallow Share Location	Verbietet das Teilen der Standort Information	
Disallow Safe Boot	Verbietet das Starten im Safe Modus	
Disallow Network Reset	Verbietet das Zurücksetzen der Netzwerkeinstellungen	
Disallow Factory reset	Verbietet das Zurücksetzen auf Werkseinstellungen	
Enable ADB	Aktiviert die Anbindung an den PC via ADB	
Disable Keyguard	Deaktiviert Keyguard	
Device Owner Lockscreen Info	Zeigt den eingegeben Text auf dem Sperrbildschirm	
Compliance Enforcement	Wählt das Vorgehen zum Durchsetzen der Richtlinien Prompt User: Der Nutzer wird zum Durchführen der Aktionen aufgefordert Lock-Down Device: Alle Apps werden ausgeblendet bis alle notwendigen Aktionen ausgeführt wurden	
App Management		
Allow Cross Profile App Linking	Erlaubt das Verlinken von Apps zwischen Profilen	
Disallow App Control	Verbietet das Modifizieren von Apps in den Einstellungen oder dem Launcher	
Disallow App Installation	Verbietet die Deinstallation von Apps	
Disallow Uninstall Apps	Verbietet die Installation von Apps	
Runtime Permission Policy	Legen Sie fest, wie mit neu angeforderten Rechten von Apps verfahren werden soll.	
Allow Unknown Sources	Erlaubt die Installation von Apps von unbekannten Quellen	
Connectivity		
Disallow Mobile Network Config	Verbietet die Konfiguration von mobilen Netzen	
Disallow Tethering Config	Verbietet die Konfiguration von Tethering	
Disallow VPN Config	Verbietet die Konfiguration von VPN	
Disallow Wifi Config	Verbietet die Konfiguration von WiFi	
Disallow Outgoing NFC Beam	Verbietet ausgehende NFC Übertragung	



Lock WiFi Configuration	Sperrt die über das MDM angelegte WiFi Konfigurationen	
Enable Data Roaming	Aktiviert Daten Roaming	
Bluetooth		
Disallow Bluetooth	Verbietet Bluetooth (Android 8.0 oder höher)	
Disallow Bluetooth Sharing	Verbietet das Teilen über Bluetooth (Android 8.0 oder höher)	
Disallow Bluetooth Config	Verbietet die Konfiguration von Bluetooth	
Account Management		
Disallow adding managed profile	Verbietet das Hinzufügen von verwalteten Profilen (Android 8.0 oder höher)	
Disallow adding Users	Verbietet das Hinzufügen von Nutzern	
Disallow Remove Managed Profile	Verbietet das Entfernen von verwalteten Profilen (Android 8.0 oder höher)	
Disallow Remove User	Verbietet das Entfernen von Nutzern	
Disallow Account Modification	Verbietet die Modifikation von Accounts	
Telephony		
Disallow Outgoing Calls	Verbietet ausgehende Anrufe	
Disallow SMS	Verbietet SMS	
System		
Disallow Window Creation	Fenster, die nicht von Apps erstellt werden, werden unterbunden	
Disallow set User Icon	Verbietet das Ändern des Icons des Nutzers	
Disallow Set Wallpaper	Verbietet das Ändern des Hintergrundbildes	
Disable Status Bar	Deaktiviert die Statusleiste	
Enable Auto Time	Setzt die Uhrzeit automatisch	
Enable Auto Time Zone	Setzt die Zeitzone automatisch	
Stay on while plugged in	Das Gerät bleibt aktiv, während es mit einer Stromquelle verbunden ist	
Storage		
Disallow disable App Verification	Verbietet die Deaktivierung der Verifizierung von Apps	
Disallow Mount Physical Media	Verbietet das Anschließen externer Speichermedien	
Enable Backup Service		
	Aktiviert die Backup Dienste (Android 8.0 oder höher)	



Keyboard	
Disallow Autofill	Deaktiviert die Autovervollständigung (Android 8.0 oder höher)
Disallow Copy & Paste between Profiles	Deaktiviert das Kopieren & Einfügen zwischen Profilen
Sound	
Disallow Volume Adjustment	Verbietet das Ändern der Lautstärke
Disallow Unmute Microphone	Verbietet das Ändern der Lautstärke des Mikrofons
Mute Device	Schaltet das Gerät stumm.



BYOD Container

Android Enterprise

Android Enterprise

Enable Android Enterprise	Aktiviert Androd for Work (AE). AE wird seit Android 5.0 unterstützt, Aufgrund von technischen Problemen wird die Verwendung allerdings mit Geräten mit Android 5.1.1 oder höher empfohlen.
Runtime Permission Policy	Prompt user for new permission requests – User werden bezüglich neuen Berechtigungsanforderungen gefragt. Always grant new new permission requests – teilt immer benötigte Rechte zu. Always deny new permission requests – weißt alle Berechtigungsabfragen ab.
Allow Unknown Sources	Erlaubt die Installation von Apps über eine .apk Datei
Allow USB Debugging	Wenn aktiv, können Nutzer USB Debugging aktivieren.
Allow Cross profile Copy & Paste	Wenn aktiv, teilen sich Arbeitsprofil und privates Profil die Zwischenablage
Compliance Enforcement	Mode Prompt User – Der Nutzer wird dazu aufgefordert alle nötigen Schritte durchzuführen. Mode Lock-Down Container – Blendet alle Apps aus, bis alle Aktionen durchgeführt wurden.

Divide Exchange

Sie müssen die "Divide Productivity" App genehmigen bevor Sie Exchange Konten einrichten können.

Klicken Sie auf den Button "Divide Productivity" um die AE Store Seite zu öffnen und die App zu genehmigen.

eMail Address	Die Mitgegebene E-Mail Adresse des jeweiligen Users Beachten Sie hier die "Placeholders", anhand von diesen können Sie mit Credentials arbeiten und müssen nicht für jedes Gerät eine händische Änderung vornehmen Mit einem Klick auf Show Placeholders können Sie sich diese anzeigen lassen
Use AppTec Gateway	Wählen Sie die Apptec Gateway Konfiguration, welche Sie
	nutzen möchten.
Server Hostname	Hostname oder Adresse des Exchange Servers
Login Name	Der Name mit dem der Login am Exchange Server
	durchgeführt wird
Password	Das Passwort für den angegeben Exchange Nutzer
Signature	Die Signatur für eMails. Hinweis: Manche geräte
	benötigen eine HTML Formatierung.



Number of previous days to sync	Wieviele Tage rückwirkend synchronisiert werden
Device Identifier	Dieser muss ein String mit der EAS DeviceID sein. Dies ist Teil des EAS protocol, welches von manchen Umgebungen für die Erkennung benutzt wird.
Sync while Roaming	Wenn deaktiviert, werden keine Daten synchronisiert während man mobil im Ausland ist.
Use Secure Sockets Layer (SSL)	Aktiviert SSL
Accept all certificates	Akzeptiert alle Zertifikate. Nutzen Sie diese Option, wenn Ihr Exchange Server ein selbst-signiertes Zertifikat hat.
Enable Tasks	Wenn aktiv, werden die Aufgaben synchronisiert
Enable Notes	Wenn aktiv, werden die Notizen synchronisiert

System Apps

Hier können Sie System Apps für die Nutzung innerhalb des Containers aktivieren.

Samsung Knox

<u>Activation</u>

Unter dieser Einstellung können Sie einen PIM (Personal Information Manager) Container zur Verfügung stellen.

Sie können entweder den "Google Divide" Container oder den "SecurePIM" Container, sowie Samsung KNOX mit den On/Off Buttons freischalten.

Die jeweilig ausgewählte App wird dann automatisch auf dem Endgerät installiert.

Knox Passcode

Legen Sie Richtlinien fest, welche die Einstellungen für das Gerätepasswort betreffen

Minimum password length	Legt fest, aus wie vielen Zeichen das Passwort mindestens bestehen muss
Password quality	Passwortstärke Every password is ok = jedes Passwort ist zulässig At least numeric characters = Mindestens Zahlen müssen enthalten sein At least complex characters = Mindestens komplexe (Sonder-) Zeichen müssen enthalten sein At least alphanumerical characters = mindestens alphanumerische Zeichen müssen enthalten sein At least alphabetic characters = mindestens alphabetische Zeichen müssen enthalten sein



Minimum compley characters required	Mindestanzahl von komplexen Buchstaben
Maximum Inactivity Timeout	Zeit der automatischen Tastensperre bei
	Inaktivität des Users
Allow Fingerprint Authentication	Erlauben des Entsperrens via Fingerabdruck
Allow Iris Authentication	Erlauben des Entsperrens via
	Augenerkennung
Max Password Age	Legt fest, nach welchem Zeitraum das
	Passwort abläuft und ein neues Passwort
	vergeben werden muss
Stored Password History	Anzahl der wie viel zuletzt benutzten
	Passwörter nicht erlaubt sind
Maximum failed password	Legt fest, wie oft das Passwort falsch
attempts	eingegeben werden darf, bis ein vollständiger
	Wipe des Gerätes durchgeführt wird

Knox Security

Schränken Sie bestimmte Funktionalitäten des Gerätes ein

Enable Camera	Lasse das Benutzen der Kamera zu
Allow Samsung KNOX App Store	Erlaube die Benutzung des KNOX App Stores
Allow Google Play Services	Erlaube die Benutzung der Google Play Dienste
Allow Browser	Erlaube die Benutzung des nativen Browsers
Allow Screenshots	Erlaube das Erstellen von Bildschirmfotos
Allow Contact Import	Wenn aktiviert, so kann im KNOX Container auf die Gerätekontakte zugegriffen werden
Allow Contact Export	Wenn aktiviert, so kann vom Gerät aus auf die KNOX Kontakte zugegriffen werden
Allow Calendar Import	Wenn aktiviert, so kann im KNOX Container auf den Gerätekalender zugegriffen werden
Allow Calender Export	Wenn aktiviert, so kann vom Gerät aus auf den KNOX Kalender zugegriffen werden
Allow Non-Secure Keypad	Lasse das Benutzen einer nicht sicheren Tastatur zu
Enable File Import	Aktivieren Sie den Dateiimport in den KNOX Container
Enable File Export	Aktivieren Sie den Dateiexport aus dem KNOX Container



Knox Exchange

Hier können Sie ein Exchange-Profil für den KNOX Container konfigurieren.

eMail Address	Die Mitgegebene E-Mail Adresse des jeweiligen Users Beachten Sie hier die "Placeholders", anhand von diesen können Sie mit Credentials arbeiten und müssen nicht für jedes Gerät eine händische Änderung vornehmen
	Mit einem Klick auf Show Placeholders können Sie sich diese anzeigen lassen
Server Hostname	Serveradresse Ihres Exchange Servers
Login name	Der Login-Name für das jeweilige Endgerät, beachten Sie hier ebenfalls die "Placeholders
Domain	Domain Adresse
Password (nur auf Device Ebene)	Optional kann direkt für ein einzelnes Gerät ein Passwort mitgeben werden, sollte dies leer gelassen werden, wird der User aufgefordert sein Exchange Passwort einzugeben
Number of previous days to sync	Zeitraum wie viel Mails zurück- synchronisiert werden sollen
Signature	Es kann eine Signatur mitgegeben werden
Default Account	Legt fest, dass dieses Mailkonto das Standard Konto ist
Use Secure Sockets Layer (SSL)	Benutzung einer SSL Verbindung
Use Transport Layer Security (TLS)	Benutzung einer TLS Verbindung
Accept all certificates	Alle Zertifikate werden akzeptiert, bitte wählen Sie diese Option aus, falls Ihr Exchange Server self-signed Zertifikate nutzt



<u>Knox eMail</u>

eMail Address	Die mitgegebene E-Mail Adresse des jeweiligen Users Beachten Sie hier die "Placeholders", anhand von diesen können Sie mit Credentials arbeiten und müssen nicht für jedes Gerät eine händische Änderung vornehmen Mit einem Klick auf Show Placeholders Können Sie sich diese anzeigen lassen
Incoming server protocol	Eingehendes Server Protokoll → IMAP oder POP
Incoming server address	Eingehende Serveradresse
Incoming server port	Eingehender Serverport
Incoming server login/username	Eingehender Server Login / Benutzername
Incoming server password	Eingehendes Serverpasswort
Incoming server uses SSL	Eingehender Server benutzt SSL
Incoming server uses TLS	Eingehender Server benutzt TLS
Incoming server accept all certificates	Eingehender Server akzeptiert jegliche Art von Zertifiakten
Outgoing server protocol	Ausgehendes Server Protokoll → SMTP
Outgoing server port	Ausgehender Serverport
	Zusätzliche Daten für den ausgehenden
Outgoing Server uses extra	Server, wenn dies auf "off" steht, werden die
credentials	eingehenden Server Einstellungen verwendet
Outgoing server login/username	Ausgehender Server Login / Benutzername
Outgoing server password	Ausgehendes Serverpasswort
Outgoing server uses SSL	Ausgehender Server benutzt SSL
Outgoing server uses TLS	Ausgehender Server benutzt TLS
Outgoing server accept all certifiactes	Ausgehender Server akzeptiert jegliche Art von Zertifikaten
Signature	Hierüber kann eine Signatur mitgegeben werden
Notify user on receiving new eMail	User wird bei einer neuen Mail benachrichtigt

Knox Apps

Legen Sie hier Apps fest, welche Sie an die Endgeräte verteilen wollen. Diese werden daraufhin im KNOX-Container zur Verfügung stehen. Um eine App hinzuzufügen, gehen Sie bitte vor wie im Menüpunkt Mandatory Apps

Application Name	Name der Applikation
Mandatory Since	Zeitpunkt, wann die App hinzugefügt wurde
Source	Quelle der App (Play Store In-House)

Durch Klicken des Symbols kann die entsprechende App wieder entfernt werden



Connection Management

<u>Wifi</u>

Nehmen Sie an dieser Einstellung die Vorkonfiguration der Endgeräte für den Zugriff auf interne Access Points vor

Services Set Identifier (SSID)	SSID des zu verbindenden Netzwerks
Hidden Network	Aktivieren, falls der AP die SSID nicht
	broadcasted
Security Type	Sicherheitstyp des AP festlegen
WEP	
Password	Passwort für den AP
WPA/WPA2	
Password	Passwort für den AP
802.1x EAP	
EAP-Method	
PWD	Aktivieren bzw. Deaktivieren
PEAP	Aktivieren bzw. Deaktivieren
TTLS	Aktivieren bzw. Deaktivieren
TLS	Aktivieren bzw. Deaktivieren
Authentication	
PWD	
Identity	Identität
Password	Passwort
PEAP	
Phase 2 Authentication Protocol	Protokoll der 2nd Authentifizierung
none	Kein weiteres Protokoll
MSCHAPV2	MSCHAPV2 Protokoll
GTC	GTC Protokoll
CA Certificate	CA Zertifikat
Identity	Identität
Anonymous Identity	Anonyme Identität
Password	Passwort
TTLS	
Phase 2 Authentication Protocol	Protokoll der 2nd Authentifizierung
none	Kein weiteres Protokoll
PAP	PAP Protokoll
MSCHAP	MSCHAP Protokoll
MSCHAPV2	MSCHAPV2 Protokoll
GTC	GTC Protokoll
CA Certificate	CA Zertifikat
Identity	Identität
Anonymous Identity	Anonyme Identität
Password	Passwort
TLS	
CA Certificate	CA Zertifikat
Identity	Identität
Password	Passwort



<u>VPN</u>

Connection Type	VPN-Verbindungstyp festlegen
Cisco AnyConnect	
Connection Name	Verbindungsname der VPN
Server	Serveradresse
Certificate Mode	Disabled = deaktiviert
	Automatic = automatisch
L2TP (SAFE 2.x)	Nur für SAFE 2.x Geräte verfügbar
Connection Name	Verbindungsname
Server	Serveradresse
Enable L2TP Secret	
DNS Search Domains	DNS Suchdomainen
PPTP (SAFE 2.0+)	Nur für SAFE 2.0 oder höher verfügbar
Connection Name	Verbindungsname der VPN
Server	Serveradresse
Enable Encryption	Verschlüsselung aktivieren
DNS Search Domains	DNS Suchdomainen
L2TP / IPSec PSK (SAFE 2.0+)	Nur für SAFE 2.0 oder höher verfügbar
Connection Name	Verbindungsname der VPN
Server	Serveradresse
IPSec Pre-Shared Key	Pre-Shared Key zur Authentifizierung
Enable L2TP Secret	
L2TP Secret	
DNS Search Domains	DNS Suchdomainen
IPSec XAuth PSK (SAFE 3.0+)	Nur für SAFE 3.0 oder höher verfügbar
Connection Name	Verbindungsname der VPN
Server	Serveradresse
IPSec Identifier	Benutzername für die Verbindung
IPSec Pre-Shared Key	Passwort für die Verbindung
DNS Search Domains	DNS Suchdomainen
OpenVPN	
Connection Name	Verbindungsname
OpenVPN Profile	Hier wird der Inhalt der .ovpn Datei
	hineinkopiert
	Es gibt zwei unterschiedliche Apps für
	die Nutzung von OpenVPN
OpenVPN App	Wir empfehlen die "OpenVPN for
	Android" App, alternativ kann aber auch
	die "OpenVPN Connect" App genutzt
	werden



Restrictions

Hier können Sie diverse Restriktionen einstellen in der Hinsicht auf das Verbindungs-Management.

Allow Data Roaming	Das Erlauben von mobilen Daten im Roaming
Force Data Roaming	Falls aktiviert, ist Roaming für mobile Daten permanent aktiviert (nicht empfehlenswert!) Diese Einstellung überschreibt die "Allow Data Roaming" Einstellung!
Folgende Einstellung sind nur für SAFE 2.0 Geräte oder ggfs. höher verfügbar	
Allow Emergency Calls Only	Es können nur Notrufe getätigt werden
Allow WiFI	Erlauben von WiFi
WiFi Netwok Minimum Security Level	Mindestanforderung des Sicherheitslevels einer WiFi Verbindung Open = alle WiFi Typen sind zulässig
Forbid user to add WiFi networks	Der User darf selbst keine WiFi Netzwerke hinzufügen Diese Einstellung ist nur dann möglich, wenn ein WiFi Profil unter dem "Connection Management" definiert wurde
Allow SMS & MMS	All = Alles an SMS & MMS Verkehr ist erlaubt Incoming SMS Only = Nur eingehende SMS Nachrichten sind erlaubt Outgoing SMS Only = Nur ausgehende SMS Nachriten sind erlaubt None = Kein SMS / MMS Verkehr ist zulässig
Allow Sync during Romaing	Erlauben einer Synchronisation während das Gerät sich im Roaming befindet On = aktiviert Off = deaktiviert User choice = Entscheidung des Users
Allow Voice Roaming	Erlauben des Sprach-Roaming On = aktiviert Off = deakiviert User Choice = Entscheidung des Users
Use System http Proxy Server	Das Nutzen eines HTTP Proxy Servers, bereitgestellt durch Systemeinstellungen Einstellungen sind vom verbundenem Netzwerk (WiFi oder APN) abhängig



<u>APN</u>

Folgende Einstellungen sind nur für Samsung SAFE 2.0 oder ggf. höher verfügbar!	
APN Display Name	Anzeigender APN Name
Access Point Name	Name des APNs
Outgoing server protocol	
Not set	
None	
PAP	PAP Protokoll
CHAP	CHAP Protokoll
PAP or CHAP	Entweder das PAP oder CHAP Protokoll
	Hier wird der MCC eingetragen, lassen
MCC – Mobile Country Code	Sie dieses Feld leer falls der MCC der
	eingelegten SIM-Karte genutzt werden
	soll
MNC – Mobile Network Code	Hier wird der MNC eingetragen, lassen
	Sie dieses Feld leer falls der MNC der
	eingelegten SIM-Karte genutzt werden
	soll
Server address	Serveradresse
Server port number	Serverportnummer
Server proxy address	Serveradresse des Proxys
MMS server address	MMS Serveradresse, für Standard bitte
	freilassen
MMS prt number	MMS Portnummer
MMS proxy address	MMS Proxy Adresse
User name	Username
Password	Passwort
	Erlaubte Typen sind "default", "mms",
Access Point Type	"supl"
	Falls dieses Feld leer gelassen wird,
	wird "default, supl, mms" genutzt
Preferred APN	APN wird bevorzugt



<u>Bluetooth</u>

Hier können diverse Bluetooth Einstellung vorgenommen werden

Folgende Einstellungen sind nur für Samsung SAFE 2.0 oder höher verfügbar!		
Allow Device discovery via Bluetooth	Erlauben ob das Gerät hinsichtlich	
	Bluetooth sichtbar ist	
Allow Bluetooth Pairing	Erlaubt dem Gerät das Koppeln von	
	Bluetooth Geräten	
Allow Bluetooth Headset devices	Erlauben von Bluetooth Headsets	
Allow Bluetooth Hands-free devices	Erlauben von Freisprech-Bluetooth	
	Geräten	
Allow Bluetooth A2DP devices	Erlauben des Audio Streamings	
	Protokolls A2DP zwischen Geräten	
Allow Outgoing Calls	Erlaubt ausgehende Anrufe über BT	
Allow Data Transfer via Bluetooth	Erlaubt den Datenaustausch mithilfe von	
	Bluetooth	
Allow Bluetooth Tethering	Erlaubt die Nutzung des Gerät als	
	Modem (Bluetooth Internetverbindung)	
Allow connection to Computer via	Erlaubt es dem Gerät sich mit einem	
Bluetooth	Computer über Bluetooth zu verbinden	



PIM Management

Exchange

Nur für Samsung SAFE	1.0 oder höher verfügbar!
	Die Mitgegebene E-Mail Adresse des
	jeweiligen Users
	Beachten Sie hier die "Placeholders",
	anhand von diesen können Sie mit
eMail Address	Credentials arbeiten und müssen nicht
	für jedes Gerät eine händische
	Änderung vornehmen
	Show Placeholders
	Mit einem Klick auf
	konnen Sie sich diese anzeigen lassen
Server Hostname	Serveradresse Ihres Exchange Servers
	Der Login-Name für das jeweilige
Login name	Endgerät, beachten Sie hier ebenfalls
	die "Placeholders"
	Optional kann direkt für ein einzelnes
	Gerat ein Passwort mitgeben werden,
Password (nur auf Device Ebene)	solite dies leer gelassen werden, wird
	der User aufgefordert sein Exchange
Demosin	Passwort einzugeben
Domain	
Number of previous days to sync	Zeitraum wie viel Malis zuruck-
0: 1	synchronisiert werden sollen
Signature	Es kann eine Signatur mitgegeben
	werden
Default Account	Legt fest dass dieses Malikonto das
	Standard Konto Ist
Use Secure Sockets Layer (SSL)	Benutzung einer SSL verbindung
Use Transport Layer Security (TLS)	Benutzung einer ILS Verbindung
A + - 11 +: # + -	Alle Zertifikate werden akzeptiert, bitte
Accept all certificates	wanien Sie diese Option aus, falls Ihr
	Exchange Server self-signed Zertifikate
	nutzt



<u>eMail</u>

Hier können Sie IMAP und POP Konten an die jeweiligen Endgeräte verteilen.

Diese Einstellung ist nur für Samsung SAFE 2.0 oder höher verfügbar!		
	Die mitgegebene E-Mail Adresse des	
	jeweiligen Users	
	Beachten Sie hier die "Placeholders",	
	anhand von diesen können Sie mit	
eMail Address	Credentials arbeiten und müssen nicht	
	für jedes Gerät eine händische	
	Änderung vornehmen	
	Charry Direct alders	
	Mit einem Klick auf	
	können Sie sich diese anzeigen lassen	
Incoming server protocol	Eingehendes Server Protokoll	
	→ IMAP oder POP	
Incoming server address	Eingehende Serveradresse	
Incoming server port	Eingehender Serverport	
Incoming server login/username	Eingehender Server Login /	
	Benutzername	
Incoming server password (nur auf	Eingehendes Serverpasswort	
Device Ebene)		
Incoming server uses SSL	Eingehender Server benutzt SSL	
Incoming server uses TLS	Fingehender Server benutzt TI S	
Incoming server accept all certificates	Eingehender Server akzeptiert jegliche	
	Art von Zertifiakten	
Outgoing server protocol	Ausgehendes Server Protokoll	
	→ SMTP	
Outgoing server port	Ausgehender Serverport	
	Zusätzliche Daten für den ausgehenden	
Outgoing Server uses extra credentials	Server, wenn dies auf "off" steht,	
	werden die eingehenden Server	
	Einstellungen verwendet	
Outgoing server login/username	Ausgehender Server Login /	
	Benutzername	
Outgoing server password (nur auf	Ausgehendes Serverpasswort	
Device Ebene)		
Outgoing server uses SSL	Ausgehender Server benutzt SSL	
Outgoing server uses TLS	Ausgehender Server benutzt TLS	
Outgoing server accept all certifiactes	Ausgehender Server akzeptiert jegliche	
	Art von Zertifikaten	
Signature	Hierüber kann eine Signatur mitgegeben	
	werden	
Notify user on receiving new eMail	User wird bei einer neuen Mail	
	benachrichtigt	





AE Gmail Exchange

Hinweis: Diese Konfiguration wird in Gmail angelegt. Daher muss die G	mail
App erst freigegeben und installiert werden.	

eMail Address	Die Mitgegebene E-Mail Adresse des jeweiligen Users Beachten Sie hier die "Placeholders", anhand von diesen können Sie mit Credentials arbeiten und müssen nicht für iedes Gerät eine
	Mit einem Klick auf Show Placeholders können Sie sich diese anzeigen lassen
Server Hostname	Serveradresse Ihres Exchange Servers
	Der Login-Name für das jeweilige Endgerät,
Login name	beachten Sie hier ebenfalls die "Placeholders"
Signature	Es kann eine Signatur mitgegeben werden
Number of previous days to sync	Zeitraum wie viel Mails zurück-synchronisiert werden sollen
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)	Benutzung einer SSL Verbindung
	Alle Zertifikate werden akzeptiert, bitte wählen
Accept all certificates	Sie diese Option aus, falls Ihr Exchange
	Server self-signed Zertifikate nutzt



Touchdown Exchange

Sollten Sie Touchdown (3rd Party App) benutzen wollen, können Sie dies hier freischalten und im Vorfeld konfigurieren.

Hostname of the Exchange Server	Hostname Ihres Exchange Servers
	(FQDN oder IP Adresse)
	Die Mitgegebene E-Mail Adresse des
	jeweiligen Users
	Beachten Sie hier die "Placeholders",
eMail Address for the Exchange	anhand von diesen können Sie mit
Account	Credentials arbeiten und müssen nicht
	für jedes Gerät eine händische
	Änderung vornehmen
	Show Placeholders
	konnen Sie sich diese anzeigen lassen
	Der Username für das jeweilige
Username for the Exchange Account	Endgeral, beachten Sie nier ebenfalls
	Ontional kann direkt für ein einselner
	Opuonal kann ulrekt für ein einzeines
Descurred for the Evenerate Associat	Gerat ein Passwort mitgeben werden,
Password for the Exchange Account	der Lleer gelassen werden, wird
(nur auf Device Ebene)	Desewart sinzugeben
Allow Lloor to Change Email Signature	Passwort einzugeben
Allow User to Change Email Signature	Dem Oser enauden, dass er seine Signatur öndarn darf
	Touchdown muss senarat lizenziert
License Key	werden bier muss Ibr Lizenz-Code
	eingetragen werden
Device Type reported in Exchange	Legen Sie hier die Bezeichnung fest die
Server	vom Gerät an den Exchange Server
	mitgeteilt werden soll
Allow Backup if Emails and Settings	Erlauben eines Backups von Emails und
	Einstellungen
Allow Self signed certificates	Erlauben von selbst-signierten
5	Zertifikaten
Allow HTML Formatted Email	Erlauben von HTML formatierten E-
	Mails
Allow Attachments	Nutzung von Anhängen erlauben
	Sollte diese Einstellung aktiviert sein,
Enable TouchDown Widgets	kann der User die TouchDown Widgets
	auf seinem Endgerät nutzen
Maximum Attachment Size (KB)	Legt in KB fest, wie groß ein Anhang
	maximal sein darf
	Legt in KB fest, wie groß eine Mail sein
Maximum Email size (KB)	darf, sollte diese Grenze überschritten
	werden, wird diese Mail bis zur
	passenden Größe beschnitten
Signature	Vordefinierte Signatur



App Management

Enterprise App Manager

Installed Apps (nur auf Device Ebene)

Hier werden Ihnen alle Apps angezeigt, die aktuell auf dem jeweiligen Endgerät installiert sind.

	nstalled Apps System Apps	Mandatory Apps	Blacklisted	d Apps Sys App	Restrictions	support@milanconsul	t.de 💊
						ı 👰 I	
	Application Name	\$	Version 🗘	Size 🗘	Package Name	\$	C
9	Application Name	\$	Version ≎ 5.0.6	Size ≎ 2.5 MB	Package Name com.applec360.android.mdm	\$	C
>	Application Name AppTec MDM IKARUS mobile.security	\$	Version ≎ 5.0.6 1.8.4	Size	Package Name com.applec360.android.mdm com.ikarus.mobile.security.corporate	\$	0

Über das O_Symbol lassen sich direkt neue Apps auf das Endgerät pushen.

Sie können sowohl eine "Google Play Store" App aus dem öffentlich AppStore auf das Gerät pushen.



Select an application	1	
oogle Play Store Android In-House Apps		
९ db navigator	German V Free Apps V Search Now	
DB Navigator Deutsche Bahn free	App Berechtigungen - Datenschutz ist uns wichtig. Für Informationen über die Berechtigungen der App DB Navigator besuchen Sie bitte: www.bahn.de/androidrechteEgal 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	
DB Zugradar Deutsche Bahn free	Alle Züge auf einen Blick: Mit dem DB Zugradar/erfolgen 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	
Schallmessung : Sound Meter 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	
München Navigator Deutsche Bahn free	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 (MVV) bis kurz vor Fahrtbeginn kaufen und sich zusätzlich über die Position ihres Zuges oder eventuelle baubedingte Störungen i…	
Öffi - Fahrplanauskunft	All-in-one App für die Öffentlichen Verkehrsmittel:• Echtzeit-Abfahrtszeiten (inkl. Verspätungen), • nahedeledene Haltestellen (mit Karte). • Verbindunds-Abfraden (von Haustür zu Haustür) und •	

Oder Sie wählen unter der Kategorie "Android In-House Apps" einer Ihrer unter den General Settings hochgeladene In-House App aus.

Sele	ct an application			\times
Google Pla	ay Store Android In-House Apps			
Uploaded Ir	n-House Apps		Upload In-House App	
	IBM Notes Traveler Version:9.0.1.3 201411210833- T7.1.0.0.52-27IG forgepond.com.lotus.sync.traveler	No description available		0

Sie können auch direkt über "Upload In-House App" eine apk Datei auswählen und diese direkt hochladen.

Administrationshandbuch AppTec360







<u>System Apps</u> (nur auf Device Ebene)

Unter den "System Apps" werden Ihnen alle Apps und Dienste aufgeführt, die bereits von Ihrem Gerätehersteller aus auf dem Endgerät installiert sind.

 ▲ ▶ Ir 	stalled Apps System Apps	Mandatory Apps Blac	cklisted Apps S	ys App Res	trictions	support@milanconsu	ilt.de 🗸
	_		_	-			
	Application Name	\$	Version	\$	Size 🗘	Package Name	\$
ø	Adapt Sound		1.0		2.8 MB	com.sec.hearingadjust	
ø	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		4.3-19300XXUGNG	33	35 MB	android	
-	Application installer		1.0		39 kB	com.sec.android.preloadinstaller	
Ö	BadgeProvider		1.0		4 kB	com.sec.android.provider.badge	
-	BandService		1.42		518 kB	com.sec.android.band	
İ	Basic Daydreams		4.3-19300XXUGNG	33	32 kB	com.android.dreams.basic	
-	Benutzerhandbuch		1.0		23 kB	com.sec.android.widgetapp.webmanual	
- ģi	Best Face		20130529.1.0.0.46	6	199 kB	com.arcsoft.picturesbest.app	
ι.	Bevorzugte Apps		1.0		1.4 MB	com.sec.android.favoriteappwidget	



Mandatory Apps

Unter den Mandatory Apps können Sie zwingend erforderliche Apps festlegen. Der User wird ständig dazu aufgefordert sich diese besagte App zu installieren.

Über das 💿 kann direkt eine zwingend erforderliche App definiert werden.

Dies kann wie bei den "Installed Apps" eine Google Play Store App sein, aber auch eine In-House App.

Wenn Sie eine In-House App wählen, haben Sie zusätzlich die Möglichkeit "Keep up to date" zu aktivieren. Wenn diese Funktion aktiviert ist und Sie in der In-House App DB eine neuere Version als Update Target definieren, wird die App auf dem Gerät aktualisiert.



Die Bedienung funktioniert exakt gleich wie bei der Kategorie "Installed Apps".



Blacklisted Apps

Unter "Blacklisted Apps" können Sie Apps oder Dienste definieren, die nicht auf dem Endgerät installiert werden können bzw. diese werden deaktiviert und für den User unausführbar gemacht.

•	► I	nstalled Apps System Apps	Mandatory Apps	Blacklisted Apps Sys	App Restrictions	support@milanconsu	lt.de 🗸
		Application Name	> Packagename	:	Blacklisted Since	\$	0
	F	Flipboard	flipboard.app		March 27, 2015, 1:18 pm		•

Über das 💿 können Sie weitere blacklisted Apps oder Dienste hinzufügen.

Sie können entweder eine Google Play Store App auswählen.

Select an application					X	
Google Play Store Packagename						
Q Enter Searchterm here	German	~	Free Apps	~	Search Now	

Oder einen "Packagename" definieren.





Diesen Packagename finden Sie entweder unter den "Installed Apps" / "System Apps" unter "Package Name" oder Sie können ihn anhand des Google Play Store Links herausfinden.

Beispiel:

App Name: TV Spielfilm – TV Programm

Google Play Store Link: <u>https://play.google.com/store/apps/details?</u> id=de.tvspielfilm&hl=de

Der Packagename ist dann dieser ab dem "Gleichheitszeichen" und geht bis zu dem "Und-Zeichen".

Packagename: de.tvspielfilm

Dies ist bei allen Google Play Store Apps identisch.



Sys App Restrictions

Unter "Sys App Restrictions" können Sie unter anderem diverse vorinstallierte Apps und Dienste nach Ihren Wünschen blockieren.

Disable Browser	Deaktivierung des Standards Browsers
Disable Calendar	Deaktivierung vom nativen Kalender
Disable Calculator	Deaktivierung des Taschenrechners
Disable Chrome Browser	Deaktivierung des Chrome Browsers
Disable Clock	Deaktivierung der Uhr
Disable Contacts	Deaktivierung der Kontakte
Disable Dialer	Deaktivierung der nativen Telefon-App
Disable eMail	Deaktivierung von E-Mails
Disable Exchange	Deaktivierung von Exchange Konten
Disable Facebook	Deaktivierung der Facebook App
Disable Gallery	Deaktivierung der nativen Galerie-App
Disable Gmail	Deaktivierung von GMail
Disable Google Books	Deaktivierung von Google Books
Disable Google Play Kiosk	Deaktivierung von Google Play Kiosk
Disable Google Maps	Deaktivierung von Google Maps
Disable Google Music	Deaktivierung von Google Musik
Disable Google Movies	Deaktivierung von Google Movies
Disable Google Play Store	Deaktivierung des Google Play Stores (öffentlich App Store)
Disable Google Plus	Deaktivierung von Google Plus
Disable Google Search	Deaktivierung von der Google Suche
Disable Google Talk / Google Hangouts	Deaktivierung von Google Talk bzw.
	Google Hangouts
Disable Music Player	Deaktivierung der nativen Musik App
Disable Settings	Deaktivierung der Geräte-Einstellungen
Disable Sim Toolkit	Deaktivierung des Sim Toolkit Dienstes
Disable SMS / MMS	Deaktivierung von SMS und MMS
Disable Street View	Deaktivierung der Street View Dienste
Disable Youtube	Deaktivierung von YouTube



Samsung Apps

Unter "Samsung Apps" können Sie für Samsung Geräte noch folgende, zusätzliche Einstellungen bzw. Restriktionen definieren.

Disable AllShare Play / Samsung Link	Deaktivierung von AllShare Play /
	Samsung Link
Disable ChatON	Deaktivierung von ChatON
Disable Game Hub	Deaktivierung von Game Hub
Disable Group Play	Deaktivierung von Group Play
Disable Help	Deaktivierung der Samsung Hilfe
Disable KNOX	Deaktivierung des Samsung KNOX
	Containers
Disable Memo	Deaktivierung von Sprachmemos
Disable My Files	Deaktivierung von "Eigene Dateien"
Disable Optical Reader	Deaktivierung des Bild-Scanners
Disable Polaris Office	Deaktivierung von Polaris Office
Disable Readers Hub / Samsung Books	Deaktivierung von Readers Hub bzw.
	Samsung Books
Disable S Memo	Deaktivierung der Notiz-App von
	Samsung
Disalbe S Translator	Deaktivierung der Übersetzer App von
	Samsung
Disable S Voice	Deaktivierung des Sprachassistenten S
	Voice
Disable Samsung Apps	Deaktivierung des Samsung App Stores
Disable Samsung Hub	Deaktivierung des Entertainment Stores
	von Samsung
Disalbe Video Player	Deaktivierung des Video Players
Disable Voice Recorder	Deaktivierung der Sprachaufnahme
Disable WatchON	Deaktivierung von WatchON (simuliert
	eine Fernbedienung)

Huawei Apps

Unter "Huawei Apps" können Sie für Huawei Geräte noch folgende, zusätzliche Einstellungen bzw. Restriktionen definieren.

Disable DLNA	Deaktivierung von DLNA
Disable App Installer	Deaktivierung des App Installers
Disable File Manager	Deaktivierung des Datei Managers
Disable Backup Manager	Deaktivierung des Backup Managers
Disable System Updater	Deaktivierung des System Updaters
Disable Tool Box	Deaktivierung der Tool Box
Disable Weather	Deaktivierung des Wetterdienstes
Disable FM Radio	Deaktivierung von FM Radio



Enterprise App Store

<u>Playstore</u>

Unter diesem Punkt können Sie optionale Apps für Ihre User verteilen.

Dies sind lediglich Verlinkungen auf den offiziellen Google Play Store, aus diesem Grund muss auf jedem Endgerät eine Google ID hinterlegt sein. Wir empfehlen an dieser Stelle, dass jeder User seine eigene Google Play Store ID besitzt.

Mit dem 💿 können Sie weitere Apps hinzufügen.

Playstore In-House		l .		👤 support@milanconsult.de 🗸
Application Name	Version	\$ Size	Package Name	÷ 🕒

Danach sollte Sich ein Fenster mit folgender Übersicht öffnen.

Select an applicat	tion			X
Google Play Store				
Q Enter Searchterm here	German	✓ Free Apps	~	Search Now



Bei "Enter Seachterm here …" können Sie nach einer sich im Google Play Store befindenden App suchen.

Select an application		\times
Google Play Store		
Q db navi	German	
DB Navigator Deutsche Bahn free	App Berechtigungen - Datenschutz ist uns wichtig. Für Informationen über die Berechtigungen der App DB Navigator besuchen Sie bitte: www.bahn.de/androidrechteEgal 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	
DB Zugradar Deutsche Bahn free	Alle Züge auf einen Blick: Mit dem DB ZugradarVerfolgen 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	
Schallmessung : Sound Meter 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	
Meine Bank 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 …	
Ist mein Zug pünktlich?	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 oefahrene Züge speichern und so schnell und einfach auf "Ist	

Wenn Sie nun auf das Icon oder auf den Name der App klicken, werden Sich nochmals gefragt, ob Sie diese App dem App Katalog hinzufügen möchten – bestätigen Sie dies mit "yes".

Add app to AppTec App Store ?	X
Add DB Navigator to the device app catalog.	
	yes





Sollte der App-Store Import erfolgreich gewesen sein, erhalten Sie nun folgende Übersicht:



Somit ist der App-Store Import abgeschlossen und der User kann nun auf dem Endgerät den AppStore von AppTec sehen.

Wenn der User diesen Store öffnet, kann er Ihm alle zugewiesenen Apps sehen und installieren.



<u>In-House</u>

Unter dem Punkt "In-House" können Sie Ihre eigenentwickelten Apps hochladen und verteilen.

Mit dem 😳 können Sie weitere In-House Apps verteilen.

Wenn Sie eine In-House App wählen, haben Sie zusätzlich die Möglichkeit "Keep up to date" zu aktivieren. Wenn diese Funktion aktiviert ist und Sie in der In-House App DB eine neuere Version als Update Target definieren, wird die App auf dem Gerät aktualisiert.

◄ ► Playstore In-House				support@milanconsult.de 🗸
Application Name	Version	≎ Size	Package Name	÷ 🕒

Sollten Sie bisher noch keine In-House App verteilt haben, erhalten Sie nun folgende Übersicht:



Klicken Sie hierzu auf "Upload In-House App", nun erhalten Sie folgende





Wählen Sie nun mit "Durchsuchen…" eine .apk Datei aus und klicken Sie anschließend auf "Upload".

Upload an In-House App	\times
Unland Limit may aim of califiles is 64 UD	
Select the ank file of the Android application which you want to upload	
Durchsuchen IBMNotesTraveler_9.0.1.3_201411210833_7.2.0.0.34-170.p.apk	
	Upload

Ihre App wird nun hochgeladen, in der Mitte des Kreises können Sie eine Prozentanzahl sehen wie weit Ihre App bereits hochgeladen ist.

Upload an In-House App	\times
Upload Limit: max. size of apk files is 64 MB Select the .apk file of the Android application which you want to upload Durchsuchen. IBMNotesTraveler_9.0.1.3_201411210833_7.2.0.0.34	-170.p.apk
13%	
-7118-	
	Upload



Sollte ein Upload der In-House App erfolgreich gewesen sein, können Sie nun die eben hochgeladen App in ihrem App Katalog vorfinden.

•	•	Playstore In-House				🧕 supp	ort@milanconsult	.de 🗸
		Application Name	Version \$	Siz	е	\$ Package Name	\$	0
		IBM Notes Traveler	9013201411210833-T720034-170浙	6.3	5 MB	forgepond.com.lotus.svnc.traveler		

Der User ist nun in der Lage, auf seinem Endgerät diese App im AppTec Sore unter der Kategorie "In-House" sehen und installieren zu können.

Da es sich hierbei um keine öffentliche Google PlayStore App handelt, braucht der User an seinem jeweiligen Endgerät keine hinterlegte Google ID.

AE Playstore

Hier können Sie Apps zum eigenen Playstore im Android Enterprise Container hinzufügen. Beachten Sie, dass der Administrator diese Apps davor erst freigeben muss.



Kiosk Mode & Launcher

<u>Kiosk Mode</u>

Der Kiosk Mode erlaubt es Ihnen eine App oder URL vorzudefinieren, dann ist es ausschließlich möglich diese App bzw. URL auszuführen/besuchen.

Ebenfalls können Sie im Kiosk Mode diverse Hardware tasten deaktivieren.

Automatic Start	Startet den Kiosk Mode automatisch, sobald das Profil auf dem Endgerät angekommen ist				
Scheduled Kiosk Mode ?	Sie können anhand der Uhrzeit den Kiosk Mode planen, dieser wird dann in der von Ihnen definierten Uhrzeit automatisch gestartet und beendet				
Start Time	Startzeit				
Time in minutes	Zeit in Minuten, nachdem der Kiosk Mode wieder beendet werden soll				
Application Type	Single App				
	URL				
	Multi App				
Single App	Wenn Sie eine App im Kiosk Mode starten möchten, wählen Sie unter "Application Type" "Package" aus				
Kiosk Application	Klicken Sie hier, um eine App die im Kiosk Mode gestartet werden soll auszuwählen Sie finden die gängige Übersicht vom App Management vor Sie können zwischen "Google Play Store", "Android In-House Apps" und einem "Packagename" auswählen				
URL	Wenn Sie eine URL im Kiosk Mode starten möchten, wählen Sie unter "Application Type" "URL" aus				
URL	Definieren Sie hier nun Ihre gewünschte URL Adresse				
Clear browser after inactivity	Hier können Sie einen Zeitintervall in Minuten definieren, nachdem nach einer Inaktivität der Kiosk Mode neu gestartet werden soll				
Clear Web Cache and Cookies	Wenn Sie diese Funktion aktivieren, wird nach einem Neustart des Kiosk Modes der Web Cache (Cookies und cached Bilder) gelöscht				
Same Origin Policy	Sollte diese Funktion aktiviert sein, kann der User nur unter Unterseiten der vordefinieren URL surfen z.B. haben Sie folgende URL definiert:				


	www.mypage.com der User kann dann
	Hier können Sie eine Whiteliet aflegen
	alle diese LIDLe sind zulässig
VVNITEIISTED URLS	Maximal 1 URL pro Linie
	Eine URL muss mit http://oder https://
	beginnen
	Hier können Sie eine Blacklist pflegen,
	alle diese URLs sind unzulässig
Blacklisted URLs	Maximal 1 URL pro Linie
	Eine URL muss mit http:/ oder https://
	beginnen
Multi App	Wenn Sie den "Multi App" Kiosk Mode
	wählen, wird die Benutzung des AppTec
	Launchers erzwungen
Apps	Application: Wählen Sie eine Playstore
	oder Inhouse Ann. Sie können auch
	einen Packagename eintragen. Die
	ausgewählte Kiosk App muss auf dem
	Coröt installiort soin. Sotzon Sie die
	Kiesk Ann ele Mandeten Ann
	Klosk App als Mandatory App.
	Shortcut on Homescreen: Fine
	Verknüpfung wird auf dem Homescreen
	angelegt wenn diese Ontion auf "On"
	angelegt wenn diese Option auf Off
	yestelli wild. Welli dese auf Off Stellt,
	wild die App dennoch in der App Liste
Orne en Orientation	Dises Firstellus a hat iffedia
Screen Orientation	Diese Einstellung betrifft die
	Bliaschirmarenung
	Automatic = automatisch
	Portrait = Hochkant Format
	Landscape = Landschaftsmodus
	Wenn Sie diese Funktion aktivieren, ist
Exit Password Enabled	es dem User möglich, mit den von Ihnen
	vordefinierten Passwort den Kiosk Mode
	beenden zu können
Auto Collapse Status Bar	Wenn aktiviert, wird die Statusleiste
	automatisch geschlossen. Hiermit
	können auf die Informationen der
	Statusleiste zugegriffen warden, aber
	keine der Funktionen benutzt warden.
Disable Status Bar	Deaktiviert die Statusleiste vollständig
	Nur für Samsung Geräte mit S Δ FF 4 0
	oder höher
Exit Password	Dies ist das von Ihnen vordefinierte
	∣ r asswull Deaktivieren der Lautstärke Tasten (nur
Disable Voluma Kova	mit Someung Coröto mit SAEE 2.0 oder
Disable volume Neys	



Disable On / Off Switch	Deaktivierung des An-/ Ausschalters
	(nur mit Samsung Geräte mit SAFE 3.0
	oder höher verfügbar)
	Deaktivierung des Home Buttons, wenn
	diese Funktion aktiviert wurde, kann der
Disable Home Button	Kiosk Mode nur in der AppTec Console
	beendet werden
	(Nur mit Samsung Geräte mit SAFE 3.0
	oder höher verfügbar)
Disable Navigation Bar	Hiermit können Sie die Navigation Bar
	deaktivieren (Zurück / Menü)
	Wenn diese Funktion aktiviert wird, kann
	der Kiosk Mode nur in der AppTec
	Console beendet werden
	(Nur mit Samsung Geräte mit SAFE 3.0
	oder höher verfügbar)

AppTec Launcher

Enable AppTec Launcher	On: Aktiviert den AppTec Launcher. Der Nutzer muss diesen einmalig als Standard setzen.
	Info: Wenn der Kiosk Mode auf Multi-App eingestellt ist, wird der AppTec Launcher zwangsweise verwendet.
Large Icons	On: Eine größere Version der App Icons wird verwendet
Hide AppTec App Icon	On: Blendet die AppTec App aus
Hide AppTec Store Icon	On: Blendet den Enterpriste App Store aus

AppTec Settings

Enable AppTec Settings App	Die AppTec Settings App bietet Konfigurationen für WiFi und Bluetooth
Enable Settings in Multi App Kiosk Mode	Wenn aktiviert, ist die AppTec Settings App im Multi-Kiosk Mode
	verfügbar.



<u>Wallpaper</u>

Set custom Wallpaper	Aktivieren/Deaktivieren Sie den benutzerdefinierten Hintergrund
Wallpaper	Setzen Sie den Hintergrundmodus auf ein Bild oder Farbcode
Background Color	Geben Sie eine Hintergrundfarbe im Hex Forman an, bsp. #000000 für schwarz oder #fffffff für weiß
Wallpaper	Laden Sie hier das Bild hoch, welches Sie als Hintergrund verwenden wollen.



Content Management

<u>ContentBox</u>

Unter diesem Punkt können Sie die ContentBox aktivieren. Sobald Sie "Enable ContentBox" auf "On" geschaltet haben, wird eine separate ContentBox App automatisch auf dem Endgerät installiert.

ContentBox		support@milanconsult.de v
Enable ContentBox	💮 On	0



Konfiguration Windows Phone

Je nachdem ob Sie aktuell ein Profil oder ein Gerät ausgewählt haben, unterscheiden sich die Darstellung und deren Unterpunkte – bitte beachten Sie dies sorgfältig!

General

Profile Information (nur auf Profil Ebene)

Sollten Sie sich in einem Profil befinden, erhalten Sie hier einen kurzen Überblick über das Profil in Bezug auf Name, OS, Erstellungsdatum, Autor, etc.

Profile Name	Name des Profils – kann direkt hier umbenannt werden
Operating System	Für welches Betriebssystem das Profil gilt
Created At	Erstelldatum
Created By	Ersteller des Profils
Last Change	Datum und Uhrzeit wann die letzten Änderungen am Profil vorgenommen wurden
Changed By	Anzeige darüber wer die letzte Änderung vorgenommen hat
Profile Revision	Anzahl wie oft das Profil bereits geändert wurde

Device Overview (nur auf Device Ebene)

Eine zusammenfassende Übersicht des ausgewählten Geräts, folgendes ist hier enthalten:

Device Name	Name des Geräts
Phone Number	Telefonnummer des Geräts
OS Version	OS Version des Geräts
Operating System	Betriebssystem (Android / iOS /
	Windows Phone)
Device Ownership	Firmen oder Privatgerät
Device Typ	Telefon oder Tablet
Rooted	Status ob das Gerät gerootet wurde
Compliant	Den Richtlinien entsprechend
Last Seen	Zeitpunkt an dem sich das Gerät zuletzt
	mit AppTec verbunden hat



<u>Config Revision</u> (nur auf Device Ebene)

Hier erhalten Sie eine Übersicht welches Gruppenprofil dem Gerät zugewiesen ist.

Wenn sie auf das Gruppenprofil klicken, kommen Sie direkt zu diesem Profil und können Einstellungen vornehmen.

Mit dem Symbol können Sie die zugewiesenen Apps auf die Einstellung des Gruppenprofils zurücksetzen.

Mit dem O Symbol können Sie alle getätigten Apps auf die Einstellung des Gruppenprofils zurücksetzen.

<u>Device Log</u> (nur auf Device Ebene)

Hier erhalten Sie diverse Gerätelogs.

Gegebenenfalls können Sie bei einem Fehler hier direkt die Ursache ausfindig machen.



Asset Management (nur auf Geräte Ebene)

Asset Management (nur auf Geräte Ebene)

Device Info

Manufacturer	Gerätehersteller
Model	Modellbezeichnung des Geräts
Operating System	Betriebssystem
OS Version	Betriebssystem Version
Free / Total Memory	Freier / Gesamter Speicherplatz
Display Resolution	Bildschirmauflösung
Phone Language	Sprache des Gerätes
Firmware Version	Firmware Version
DM Client Revision	Device Management Client Version
Hardware Version	Version der Hardware im Gerät
CPU Architecture	CPU Architektur (Typ des Prozessors)

<u>Wi-Fi</u>

<u>Cellular</u>

SIM Carrier Network	Netzanbieter
	Die International Mobile Subscriber
	Identity (IMSI; deutsch Internationale
	Mobilfunk-Teilnehmerkennung) dient in
	GSM- und UMTS-Mobilfunknetzen der
	eindeutigen Identifizierung von
IMSI	Netzteilnehmern
	Die IMSI besteht aus maximal 15 Ziffern
	und setzt sich folgendermaßen
	zusammen: [1]
	 Mobile Country Code (MCC), 3
	Ziffern
	Mobile Network Code (MNC), 2
	oder 3 Ziffern
	Mobile Subscriber Identification Number
	(MSIN), 1-10 Ziffern
Modem Firmware	Modem Firmware



Synchronization Info

Instant DM Connection	Das Gerät soll sofort nach dem Einrollen eine Verbindung zu AppTec aufbauen
Inital Retry Time	Retry Zeit für diese erste Verbindung
Connection Retries	Anzahl der erneuten
	Verbindungsversuche nach einem
	Abbruch durch den Connection
	Manager oder einem WinInet-level
	Fehler
Maximum Sleep Time	Maximale Wartezeit nach package-
	sending Fehler
First Sync Retries	Zeit für die erste Stage nach dem
	Enrollment
First Retry Interval	Zeit für die erste Stage nach dem
	Enrollment
Second Retry Interval	Zeit für zweite Stage nach dem
	Enrollment
Regular Sync Retries	Zeit für weiteren Stage nach dem
	Enrollment
Regular Retry Interval	Zeit für weiteren Stage nach dem
	Enrollment



Security Management

Security Configuration

<u>Passcode</u>

Allow Simple Passwords	Erlauben von simplen Passwörtern, wie z.B. 1234 oder 1111
Minimum Password Length	Mindestanzahl an Zeichen des Passworts
Password Composition	Spezifizieren die Anzahl wie viel Charaktereigenschaften das Passwort besitzen muss Diese setzen sich aus Großbuchstaben, Kleinbuchstaben, Nummern und Sonderzeichen zusammen
Password Quality	Hier können Sie die Passwort Qualität einstellen Alphanumeric = Nur Zahlen und Buchstaben Numeric = Nur Zahlen Numeric or Alphanumeric = Zahlen oder Zahlen und Buchstaben
Maximum Inactivity Time Lock	Anzahl in Minuten, nachdem das Gerät ohne das Zutun des Users (Inaktivität) gesperrt werden soll Der User muss nach dieser Zeit das Gerät entsperren, indem er seine Gerätepasswort eingibt
Password Expiration	
Password History Restriction	Anzahl der wie viel zuletzt benutzten Passwörter nicht erlaubt ist
Maximum Failed Password Attempts	Anzahl wie oft das Passwort falsch eingegeben werden darf, bis ein vollständiger Wipe des Gerätes durchgeführt wird
Allow Password Grace Period Timer	Wenn aktiv, kann der User die Zeit zu erneute Passworteingabe einstellen. Wenn nicht, so wird das Passwort immer angefordert.



End of Life (nur auf Geräte Ebene)

<u>Wipe</u> (nur auf Geräte Ebene)

Unter "Wipe" können Sie das Gerät auf die Werkseinstellungen zurücksetzen, hier werden sowohl die geschäftlichen, als auch die privaten Daten auf dem Endgerät gelöscht



Wipe Device	X
Are you sure to wipe the device ?	
No	Yes

Mit "Yes" können Sie die Löschung durchführen.

Unter "Wipe Report" können Sie sich folgende Dinge anzeigen lassen

Wiped by	Historie von wem der Wipe ausgeführt wurde
Date	Datum
Status	Status (z.B. ob der Wipe erfolgreich durchgeführt wurde)



Restriction Settings

Device Functionality

Allow SD Card	Erlauben einer SD Karte
Allow Camera	Erlauben der Kamera
	Verschlüsselt die internen Daten auf
	dem Endgerät, falls diese Funktion
Enable Storage Encryption	einmal aktiviert wurde ist es nicht mehr
	möglich dies rückgängig zu machen
	SD Karten werden nicht verschlüsselt!
Allow USB Connection	Erlauben von USB Verbindungen
Allow Voice Recording	Erlauben von Sprachaufnahmen
Allow Location Service	Erlaubt die Lokalisierung des
	Endgerätes
Allow Screen Capture	Erlauben von Screenshots
Allow Developer Unlock	Erlaubt den Entwicklungsmodus
	Erlaubt es dem User "Mein Handy
	finden" zu nutzen, sollte diese Funktion
Allow AntiTheft Mode	bereits vor der Deaktivierung genutzt
	worden sein, muss sie zuerst manuell
	am Endgerät deaktiviert werden
Allow Cellular Data Roaming	Erlauben von mobilen Daten im im
	Roaming
Allow Cortana	Erlaubt den Sprachassistenten Cortana
Allow Appstore	Erlauben des offiziellen Appstores
Celluar App Download Limit	Maximal erlaubte App-Größe zum
	Download über das Mobilfunknetz
Allow Browser	Erlaubt den nativen Browser
Allow Task Switcher	Erlauben des Task-Managers
Allow Search to use Location	Erlaube der Suche, Lokalisierungsdaten
	zu verwenden
	Solle diese Funktion aktiviert werden,
Allow Moderate Search Filter	werden nicht jugendfrei Inhalte
	herausgefiltert und verhindert
Allow Storing Images From Vision	Mit dieser Einstellung können Sie
Search	verhindern, dass am Endgerät QR Code
	als Bilder gespeichert warden dürfen
	Ausschließlich der aktuell gescannte
	Code befindet sich auf dem Endgerat
Allow Save As Office Files	Erlaubt es dem User eine Datei als
	Office-Datei zu speichern
	Diese Policy betrifft nur den Office Hub
Allow Sharing OT Office Files	Erlaubt es dem User Office Dateien zu
	lellen Diese Delieu hetrifft zur den Office Llub
Allow Action Conton Notifician	Diese Policy Detrint nur den Office Hub
Allow Action Center Notificions	Erlaubt das Anzeigen von Nachrichten
	Im Action Center bei Sperrung



Allow Sync My Settings	Erlaubt die Synchronisierung von Einstellungen geräteübergreifend
Enable Email Data Encryption	Aktiviert die Datenverschlüsselung von E-Mails und deren Anhänge Das Gerätepasswort wird benötigt, um diese Dateien entschlüsseln zu können
Allow User Reset	Erlaubt es dem User sein Gerät in den Einstellungen oder mit den Hardware Tasten zurückzusetzen ACHTUNG! Diese Einstellung sollte nur dann deaktiviert werden, wenn es sich hierbei um ein Firmengerät handelt Sollte das Gerät aus welchen Gründen auch immer keine Verbindung mit dem AppTec Server mehr aufbauen können, muss das Gerät in einen Nokia Store geschickt werden, um das Gerät auf die Werkeinstellungen zurückzusetzen können Microsoft kann hierfür nicht für ein solches Problem verantwortlich gemacht werden
Allow User Unenrollment	Erlaubt es dem User den Unternehmensbereich zu entfernen und somit die Verbindung zu den AppTec Servern zu trennen, sollte dies geschehen ist es nicht mehr möglich das Geräte zu managen ACHTUNG! Diese Einstellung sollte nur dann deaktiviert werden, wenn es sich hierbei um ein Firmengerät handelt Sollte das Gerät aus welchen Gründen auch immer keine Verbindung mit dem AppTec Server mehr aufbauen können, muss das Gerät in einen Nokia Store geschickt werden, um das Gerät auf die Werkeinstellungen zurückzusetzen können Microsoft kann hierfür nicht für ein solches Problem verantwortlich gemacht werden



Connection Management

<u>Wifi</u>

Nehmen Sie an dieser Einstellung die Vorkonfiguration der Endgeräte für den Zugriff auf interne Access Points vor

Service Set Identifier (SSID)	SSID des zu verbindenden Netzwerks
Auto Join	Automatischen Beitreten zum Netzwerk aktivieren
Hidden Network	Aktivieren, falls der AP die SSID nicht broadcasted
Security Type	Sicherheitstyp des AP festlegen
WEP Open System	
Password	Passwort für den AP
WPA PSK	
Password	Passwort für den AP
WPA EAP	
Authentication Type	Authentifizierungsmöglichkeit, nur "PEAP-MSCAHPv2" möglich
Fast Reconnect	Geräte können zwischen den Access
	Points wechseln, ohne sich erneut
	authentifizieren zu müssen
Guest Access	Der User hat keinen Account und soll
	sich somit als Gast anmelden
Quarantine Checks	Der Client muss NAP (Network Access Protection) Checks ausführen und das Ergebnis dem System mitteilen, welches dann entscheidet ob sich der Client verbinden darf
Require Crypto Binding	Ausschließlich eine Authentifizierung über die Cryptobinding möglich
Server Validation	Der Client überprüft, ob das Server Zertifikat gültig ist, falls dies der Fall ist wird eine Verbindung hergestellt
Prompt for Certificates	Erlaubt dem Benutzer nicht vertrauenswürdige Zertifikate zu akzeptieren
Anonymous User Name	Der Client sendet seine Identität erst dann, sobald der RADIUS Server authentifiziert wurde Bis dahin nutzt er die hier angegebene Identität
Login Domain	Domaine zum Einloggen
User Name	Benutzername
Password	Passwort
Server Names	Bietet die Möglichkeit den Name des RADIUS-Servers anzugeben, der die Netzwerkauthentifizierung und –



	Autorioiorung boroitotollt
	Autonsierung bereitsteilt
WPA2-PSK	
Password	Passwort für den AP
WPA2 EAP	
Authentication Type	Authentifizierungsmöglichkeit, nur "PEAP-MSCAHPv2" möglich
Fast Reconnect	
Guest Access	
Quarantine Checks	Aktiviert den Netzwerk Zugriffsschutz NAP
Require Crypto Binding	Ausschließlich eine Authentifizierung mit Server die cryptobinding möglich
Server Validation	
Prompt for Certificates	Verlangt nach einem validierten Server- Zertifikat, Name oder einer Root Zertifikatsauthentifizierung (CA)
Anonymous User Name	
Logon Domain	
User Name	Benutzername
Password	Passwort
Server Names	Auflistung deren Server, deren Geräte vertraut werden soll
None	Keine Sicherheit festgelegt
Use Proxy Server	Das Benutzen eines Proxy Servers
Server Address	Serveradresse des Proxy Servers
Server Port	Server Port des Proxy Servers

Wifi Restrictions

Hier können Sie diverse Wifi Restriktionen definieren.

Allow WiFi	Erlauben bzw. verbieten von WiFi
Allow Internet Sharing	Erlauben eines Hotspots
Allow Auto Connect to WiFi Sense Hot	Erlauben von automatischen
Spots	Verbindungen zu einem WiFi Sense Hot
	Spots
	Erlauben das WiFi Hotspot
Allow WiFi Hot Spot Reporting	Informationen an Microsoft versendet
	werden dürfen
Allow Manual WiFi Configuration	Erlaubt es dem User sich mit nicht von
	AppTec definierten WiFi Netzwerken zu
	verbinden
WLAN Scan Frequency	Legt den WLAN-Scan Intervall fest,
	dabei verbessert ein höherer Wert die
	Erkennung von Wifi-Netzwerken



<u>VPN</u>

Nehmen Sie hier die entsprechenden Einstellungen vor, um die VPN Verbindungen zu konfigurieren

Connection Name	Angezeigte VPN Verbindungsname
Server	Serveradresse des VPN Servers
VPN Type	Typ der Verbindung
IKEv2 (native)	Es wird eine native VPN Verbindung
	genutzt
SSL-VPN (third-party)	Es wird eine 3rd Party App genutzt
Third-Party App	
	JunOS Pulse
	SonicWall Mobile Connect
	F5 Big-IP Edge Client
	Checkpoint Mobile VPN
Third-Party Configuration File	Hier muss der Inhalt der
	Konfigurationsdatei eingefügt werden
Authentication Type	Authentifizierungsmethode
Bypass Local Traffic	Bei Zugriff auf interne Ressourcen wird
	der Verkehr nicht über die VPN
	Verbindung geleitet
Connection Type	Manual = Der User muss manuell eine
	VPN Verbindung aufbauen / beenden
	Triggering = Die VPN Verbindung wird
	automatisch aufgebaut, sobald eine App
	sich zu einer geschützten oder internen
	Ressource verbinden mocnte
	Dies ist die emptoniene Einstellung
	Seitens Appilec um die bestmöglichste
	Monn diago Funktion aktiviart int wird
	koino VPN Vorbindung aufgebaut
	solange der User sich im Eirmen-WiFi
	befindet de deschützte Ressourcen
	direkt auf dem Endgerät erreichbar
	wären
	Sollte diese Funktion deaktiviert sein
	wird eine VPN Verbindung über das
Trusted Network Detection	Firmennetzwerk aufgebaut
	Es muss eine DNS Suffix eingerichtet
	werden, um zu definieren bei welchem
	WiFi es sich um eine Firmen-WiFi
	handelt
DNS Suffix	Hier können Sie den primären DNS
	Suffix eintragen
Use Proxy	Die Benutzung eines Proxys
Server Address	Serveradresse des Proxy Servers
Server Port	Server Port des Proxy Servers
Bypass Local Traffic	Bei Webanfragen ins lokale Intranet wird



der Verkehr nicht über den Proxy
geleitet.

VPN Restrictions

Hier können Sie diverse VPN Restriktionen definieren.

Allow Manual VPN Configuration	Diese Richtlinie erlaubt bzw. verbietet dem User die VPN Einstellungen zu deaktivieren und zu verändern
Allow VPN over Cellular	Verbietet bzw. erlaubt dem Gerät eine VPN Verbindung aufzubauen, falls sich das Gerät mobile Daten nutzt
Allow VPN Roaming over Cellular	Verbietet bzw. erlaubt dem Gerät eine VPN Verbindung aufzubauen, falls sich das Gerät im Roaming befindet

<u>Bluetooth</u>

Hier können Sie festlegen, ob Bluetooth erlaubt bzw. nicht erlaubt werden soll.

Allow Bluetooth	Bluetooth aktivieren / deaktivieren

<u>NFC</u>

Unter diesem Punkt können Sie festlegen, ob NFC erlaubt bzw. nicht erlaubt sein soll.

Allow NFC	NFC aktivieren / deaktivieren



PIM Management

Exchange Active Sync

Einrichten eines ActiveSync Kontos am Endgerät

Account Name	Name des Email Accounts
Server Host Name	Adresse/FQDN des Servers
Domain Name	Domäne des Servers
Email Address	E-Mail Adresse
User Name	Benutzername
User Password	Sie können hier optional bereits dem
	User ein Passwort mitgeben
Use SSL	Nutzung einer SSL Verbindung
	Hier kann das Intervall für die
	Synchronisation festgelegt werden
Sync Interval	Manual sync = Der User muss seine
	Mails aufrufen und eine manuell
	Synchronisation durchführen
Mail Age Filter	Zeitraum bis wann die Mails
	synchronisiert werden sollen
	No filter = unbegrenzt
Log Level	Festlegung der Logginglevels für den
	ActiveSync Verkehr
Sync Email	Aktiviert = Mails werden synchronisiert
Sync Contacts	Aktiviert = Kontakte werden
	synchronisiert
Sync Calendar	Aktiviert = Kalender wird synchronisiert
Sync Tasks	Aktiviert = Aufgaben werden
	synchronisiert



<u>eMail</u>

Einrichten von POP3/IMAP4 Konten am Endgerät.

Account Description	Name des Email Accounts
Sender Name	Angezeigter Name des Senders
Domain Name	Domain Name für den Email Account
Ν	E-Mail Adresse des Benutzers
User Name	Benutzername
User Password	Sie können hier optional bereits dem
	User ein Passwort mitgeben
	Hier kann definiert werden, falls für den
Alternative Outgoing Server Credentials	ausgehenden Server andere
	Credentials benötigt werden
Outgoing Domain Name	Ausgehende Domainname
Outgoing Server User Name	Ausgehender Benutzername
Outgoing Server Password	Ausgehendes Passwort
Email Protocol	POP3 oder IMAP4 kann als Protokoll
	genutzt werden
Incoming Mail Server Host Name	Eingehender Server Hostname
Use SSL for Incoming Mails	Benutzung von SSL bei eingehenden
	Mails
Outgoing Mail Server Host Name	Ausgehender Server Hostname
Use SSL for Outgoing Mails	Benutzung von SSL bei ausgehenden
	Mails
Outgoing Server Authentication	Eine ausgehende Server
	Authentifikation wird benötigt
	Hier kann das Intervall für die
	Synchronisation festgelegt werden
Sync Interval	Manual sync = Der User muss seine
	Mails aufrufen und eine manuell
	Synchronisation durchführen
	Zeitraum bis wann die Mails
Mail Age Filter	synchronisiert werden sollen
	No filter = unbegrenzt



App Management

Enterprise App Manager

Installed Apps (nur auf Geräte Ebene)

Hier werden Ihnen alle In-House Apps angezeigt.

Sie können direkt über das 🜑 Symbol eine neue In-House App (.xap Datei) dem Endgerät zuweisen.

Mandatory Apps

Hier werden Ihnen alle "Mandatory Apps", also sprich zwingend auf dem Endgerät erforderliche Apps angezeigt.

Sie können über das 💿 eine weitere Mandatory In-House App festlegen.

Whitelisted / Blacklisted Apps

Je nachdem ob Sie unter "General Settings" > "Black- & Whitelisting" > "Windows" > "Blacklisting" oder "Whitelisting" ausgewählt haben, können Sie hier blacklisted oder whitelisted Apps definieren.

Blacklisted Apps bedeutet dass all diese Apps nicht auf dem Endgerät installiert bzw. ausgeführt werden können, alle Apps die nicht hier definiert werden können installiert und ausgeführt werden

Whitelisted Apps bedeutet dass nur diese vordefinierten Apps installiert bzw. ausgeführt werden können.



Ebenfalls über das 💿 können weitere Windows Apps oder Product IDs festgelegt werden. Suchen Sie einfach nach einer App, in unserem Beispiel wäre dies Facebook.

Klicken Sie anschließend auf das App-Icon oder auf den Name der jeweiligen App.

Select an application			\times
Windows App Store Productid			
Q facebook	German (Germany)	Search Now	
Facebook Microsoft Corporation 0,00 €			
Facebook Star thanhtamBC 0,00 €			
Fast for Facebook Pro iexplore 1,29 €			
Instagram BETA Instagram			

Anschließend öffnet sich folgendes Fenster, bestätigen Sie dies mit "yes".





Sollte der App-Import erfolgreich gewesen sein, können Sie nun die eben definierte App in der Übersicht vorfinden.

< > I	nstalled Apps Mandatory	Apps Blacklisted Apps	support@milanconsul	t.de 🗸
	Application Name	Product Id 🗘	Blacklisted Since	0
(\mathfrak{O})	WhatsApp	218a0ebb-1585-4c7e-a9ec-054cf4569a79	March 23, 2015, 10:05 am	
	Angry Birds	5026b325-1461-4a4a-9ff9-4a5de698d58a	March 23, 2015, 10:20 am	
f	Facebook	82a23635-5bd9-df11-a844-00237de2db9e	May 26, 2015, 3:56 pm	•

In unserem Beispiel, da wir hier mit "Blacklisted Apps" arbeiten wäre es uns jetzt nicht möglich "Whatsapp", "Angry Birds" und "Facebook" zu installieren bzw. auszuführen, falls eine dieser Apps bereits vor dieser Regelung auf dem Endgerät installiert waren.



Enterprise App Store

<u>Windowsstore</u>

Hier sind Sie in der Lage Windows Apps an die User zu verteilen. Es handelt sich hierbei um öffentliche Windows Apps und können von dem jeweiligen User optional über den AppTec Enterprise AppStore installiert werden.

Über das Symbol lassen sich weitere Windows Apps hinzufügen. Über "Enter Searchterm here …" können Sie nach einer App aus dem Windows Store suchen. In unserem Beispiel handelt es sich hierbei um die "DB Navigator" App.

Select an appli	cation	X
Windows App Store		
Q db navigator	German (Germany)	Search Now
DB Navigator Deutsche Bahn 0,00 €		
FahrPlaner Verkehrsverbund Bre Niedersachsen 0,00 €	men	
DB Rent GmbH 0,00 €	g	
JDB for Facebook JDB Pocketware 0,00 €		
Navi S-Bahn Münche Deutsche Bahn	n	



Anschließend öffnet sich folgendes Fenster, bestätigen Sie dies mit "yes".



Sollte der App-Import erfolgreich gewesen sein, können Sie nun die eben definierte App in der Übersicht vorfinden.

•	►	Windowsstore	In-House			٩ 👤	support@milanconsult	.de 🗸
			&			×		
		Application Nat	me 💠	Version	≎ Size ≎	Package Name	\$	0
	DB	DB Navigator	r	2.1.0.94	3.9 MB	e2659b0e-f62a-e011-854c-00237de2db9e		٥
	8	GMaps 10.1		8.7.3.4	9.3 MB	73a03ef2-c494-4499-9577-81a38e9f5130		
	×	mytaxi		2.0.1.7	7.9 MB	1483c779-2edf-4d21-a221-9664ab7597f8		



<u>In-House</u>

Hier sind Sie in der Lage In-House Apps an die User zu verteilen. Es handelt sich hierbei um eigenentwickelte Windows Apps und können von dem jeweiligen User optional über den AppTec Enterprise AppStore installiert werden.

Über das 💿 Symbol lassen sich weitere In-House Windows Apps hinzufügen.

Klicken Sie im sich drauf öffnenden Fenster "Upload In-House App".

Select or upload an In-House App	X
Uploaded In-House Apps	Upload In-House App



Klicken Sie nun auf "Durchsuchen…" und wählen Sie eine .xap Datei aus.

Upload an In-House App	X
Upload Limit: max. size of xap files is 50 MB	
Select the .xap file of the windows phone application which you want to upload	
Durchsuchen Keine Datei ausgewählt.	

Nachdem Sie die xap Datei ausgewählt haben, können Sie mit "Upload" die App in Ihren AppTec Enterprise AppStore importieren.

Sollte der Upload erfolgreich gewesen sein, können Sie die App nun in der Übersicht vorfinden.



Kiosk Mode

<u>Kiosk Mode</u>

Unter dem Punkt "Kiosk Mode" können Sie eine App in den Vollbildmodus bringen, anschließend ist es nur noch möglich diese App zu nutzen.

•	►	Kiosk Mode	👤 support@milanconsult.de 🗸	r
		Dn		
	Produc	t ID	Click here to select an application or enter a Product ID	

ACHTUNG!

Der Kiosk Mode unter Windows Phone kann nur dann deaktiviert werden, indem das Gerät auf die Werkseinstellungen zurückgesetzt wird. Die App / Product ID die hier definiert wird, wird nach jedem Geräte Neustart automatisch im Vollbild ausgeführt.

Mit "Click here to select an application or entere a Product ID" können Sie eine öffentliche / In-House Windows App definieren oder Sie sind ebenfalls in der Lage eine Product ID festzulegen.

Select an application		×
Windows App Store Windows In-House Apps Pr	oductid	
Q db navigator	German (Germany)	Search Now
DB Navigator Deutsche Bahn 0,00 €		
FahrPlaner Verkehrsverbund Bremen Niedersachsen 0,00 €		
Elinkster - Carsharing DB Rent GmbH 0,00 €		
JDB for Facebook JDB Pocketware 0,00 €		
Navi S-Bahn München Deutsche Bahn		

Denken Sie daran die Kiosk Mode App ebenfalls unter "Mandatory App" festzulegen.

►	Kiosk Mode	Support@milanconsu	ilt.de 🗸
	Dn		
Produc	ct ID	e2659b0e-f62a-e011-854c-00237de2db9e	



Konfiguration Windows 10 PC

Je nachdem ob Sie aktuell ein Profil oder ein Gerät ausgewählt haben, unterscheiden sich die Darstellung und deren Unterpunkte – bitte beachten Sie dies sorgfältig!

General

Profile Information (nur auf Profil Ebene)

Sollten Sie sich in einem Profil befinden, erhalten Sie hier einen kurzen Überblick über das Profil in Bezug auf Name, OS, Erstellungsdatum, Autor, etc.

Profile Name	Name des Profils – kann direkt hier umbenannt werden
Operating System	Für welches Betriebssystem das Profil gilt
Created At	Erstelldatum
Created By	Ersteller des Profils
Last Change	Datum und Uhrzeit wann die letzten Änderungen am Profil vorgenommen wurden
Changed By	Anzeige darüber wer die letzte Änderung vorgenommen hat
Profile Revision	Anzahl wie oft das Profil bereits geändert wurde

<u>Device Overview</u> (nur auf Device Ebene)

Eine zusammenfassende Übersicht des ausgewählten Geräts, folgendes ist hier enthalten:

Device Name	Name des Gerätes in der Konsole
PC Name	Name des PC
PC UID	UID des PC
OS Edition	Installierte Windows Edition
OS Version	Installierte Windoes Version
OS Build	Derzeitiger Windows Build
Operating System	Derzeit installiertes Betriebssystem
Serial Number	Seriennummer des Gerätes
Device Ownership	Firmen oder Privatgerät
Device Type	Typ des Gerätes
Rooted	Anzeige ob das gerät gerooted ist
Compliant	Zeigt ob das Gerät den Richtlinien
	entspricht
Last Seen	Zeitpunkt an dem sich das Gerät zuletzt
	mit AppTec verbunden hat



<u>Settings</u>

Allow Auto Update	Erlaubt automatische Updates	

<u>Config Revision</u> (nur auf Device Ebene)

Hier erhalten Sie eine Übersicht welches Gruppenprofil dem Gerät zugewiesen ist.

Wenn sie auf das Gruppenprofil klicken, kommen Sie direkt zu diesem Profil und können Einstellungen vornehmen.

Mit dem Symbol können Sie die zugewiesenen Apps auf die Einstellung des Gruppenprofils zurücksetzen.

Mit dem Symbol können Sie alle getätigten Apps auf die Einstellung des Gruppenprofils zurücksetzen.

Device Log (nur auf Device Ebene)

Hier erhalten Sie diverse Gerätelogs.

Gegebenenfalls können Sie bei einem Fehler hier direkt die Ursache ausfindig machen.



Asset Management (only on device level)

Device Info

Manufacturer	Gerätehersteller
Model	Modellbezeichnung des Geräts
Model Number	Model Number
Operating System	Betriebssystem
OS Version	Betriebssystem Version
Serial Number	Seriennummer
ExchangeID	ExchangeID
Total RAM	Insgesamter Arbeitsspeicher
Display Resolution	Bildschirmauflösung
Phone Language	Sprache des Gerätes
Firmware Version	Firmware Version
DM Client Version	Device Management Client version
Hardware Version	Version der Hardware im Gerät
CPU Architecture	CPU Architektur (Typ des Prozessors)

<u>Cellular</u>

SIM Carrier Network	Netzanbieter
Modem Firmware	Modem Firmware

Synchronization Info

Instant DM Connection	Das Gerät soll sofort nach dem Einrollen eine Verbindung zu AppTec aufbauen
Inital Retry Time	Retry Zeit für diese erste Verbindung
Connection Retries	Anzahl der erneuten
	Verbindungsversuche nach einem
	Abbruch durch den Connection Manager
	oder einem WinInet-level Fehler
Maximum Sleep Time	Maximale Wartezeit nach package-
	sending Fehler
First Sync Retries	Zeit für die erste Stage nach dem
	Enrollment
First Retry Interval	Zeit für die erste Stage nach dem
	Enrollment
Second Retry Interval	Zeit für zweite Stage nach dem
	Enrollment
Regular Sync Retries	Zeit für weiteren Stage nach dem
	Enrollment
Regular Retry Interval	Zeit für weiteren Stage nach dem
	Enrollment



Security Management

Anti Theft (nur auf Device Ebene)

GPS Information (nur auf Device Ebene)

Hier können Sie den aktuellen / letzten Standort des Geräts ermitteln. Die Lokalisierung kann mit einem oder sogar zwei Passwörtern geschützt werden – Siehe: *General Settings – Privacy – GPS Access*



GPS Settings

Enable GPS Tracking	Aktiviert die Aufzeichnung der GPS Daten
Tracking Interval	Der Interval, in dem GPS Daten aufgezeichnet werden



Security Configuration

Passcode

Minimum Password Length	Mindestanzahl an Zeichen des Passworts
	Spezifizieren die Anzahl wie viel
	Charaktereigenschaften das Passwort besitzen
Password Composition	muss
	Diese setzen sich aus Großbuchstaben,
	Kleinbuchstaben, Nummern und Sonderzeichen
	zusammen
	Hier können Sie die Passwort Qualität einstellen
	Alphanumeric = Nur Zahlen und Buchstaben
Password Quality	Numeric = Nur Zahlen
	Numeric or Alphanumeric = Zahlen oder Zahlen
	und Buchstapen
	Anzani in Minuten, nachdem das Gerat onne das
Maximum Inactivity Time Look	Der Lleer muse nach dieser Zeit des Ceröt
	ontenerren indem er seine Gerätenesswert
	eingibt
Password Expiration	Setzt die Zeit nach der ein neues Passwort
	eingegeben werden muss
Password History Restriction	Anzahl der wie viel zuletzt benutzten Passwörter
,	nicht erlaubt ist
Maximum Failed Password	Anzahl wie oft das Passwort falsch eingegeben
Attempts	werden darf, bis ein vollständiger Wipe des
	Gerätes durchgeführt wird
Allow Password Grace Period	Wenn aktiv, kann der User die Zeit zu erneute
Timer	Passworteingabe einstellen. Wenn nicht, so wird
	das Passwort immer angefordert.



Restriction Settings

Device Functionality

Allow SD Card	Erlauben einer SD Karte
Allow Camera	Erlauben der Kamera
Allow Location Service	Erlaubt die Lokalisierung des Endgerätes
Allow Developer Mode	Erlaubt den Entwicklermodus
Allow Cellular Data	Erlauben von mobilen Daten im im Roaming
Roaming	
Allow Cortana	Erlaubt den Sprachassistenten Cortana
Allow Search to use	Erlaube der Suche, Lokalisierungsdaten zu verwenden
Location	
Allow Adding Non	Legt fest ob der Nutzer einen E-Mail Account anlegen
Microsoft Email	darf, der nicht von Microsoft kommt
Account	
Allow Microsoft	Legt fest ob der Microsoft für nicht-Email
Account Connection	Authentifizierungen genutzt werden darf
Allow Sync My	Erlaubt die Synchronisierung von Einstellungen
Settings	geräteübergreifend
Enterprise Protected	Gibt die Unternehmensdomänennamen an, welche durch
	, getternit sind
	mit den Herdware Testen zurückzusetzen
	Diago Einstellung collto nur dann docktiviert worden, wenn
	os sich hierbei um ein Eirmengeröt handelt
	Sollto das Coröt aus welshen Gründen aush immer keine
	Verbindung mit dem AnnTec Server mehr aufhauen
	können, muss das Gerät in einen Nokia Store geschickt
Allow User Reset	werden, um das Gerät auf die Werkeinstellungen
	zurückzusetzen können
	Microsoft kann hierfür nicht für ein solches Problem
	verantwortlich gemacht werden
	Frlaubt es dem User den Unternehmensbereich zu
	entfernen und somit die Verbindung zu den AppTec
	Servern zu trennen, sollte dies geschehen ist es nicht
	mehr möglich das Geräte zu managen
	ACHTUNG!
	Diese Einstellung sollte nur dann deaktiviert werden, wenn
	es sich hierbei um ein Firmengerät handelt
	Sollte das Gerät aus welchen Gründen auch immer keine
	Verbindung mit dem AppTec Server mehr aufbauen
Allow User	können, muss das Gerät in einen Nokia Store geschickt
Unenrollment	werden, um das Gerät auf die Werkeinstellungen
	zurückzusetzen können
	Microsoft kann hierfür nicht für ein solches Problem
	verantwortlich gemacht werden



Connection Management

<u>Wifi</u>

Nehmen Sie an dieser Einstellung die Vorkonfiguration der Endgeräte für den Zugriff auf interne Access Points vor

Service Set Identifier (SSID)	SSID des zu verbindenden Netzwerks
Auto Join	Automatischen Beitreten zum Netzwerk
	aktivieren
Hidden Network	Aktivieren, falls der AP die SSID nicht
	broadcasted
Security Type	Sicherheitstyp des AP festlegen
WEP Open System	
Password	Passwort für den AP
WPA PSK	
Password	Passwort für den AP
WPA EAP	
Authentication Type	Authentifizierungsmöglichkeit, nur "PEAP-MSCAHPv2" möglich
Fast Reconnect	Geräte können zwischen den Access
	Points wechseln, ohne sich erneut
	authentifizieren zu müssen
Guest Access	Der User hat keinen Account und soll
	sich somit als Gast anmelden
Quarantine Checks	Der Client muss NAP (Network Access
	Protection) Checks ausführen und das
	Ergebnis dem System mitteilen,
	welches dann entscheidet ob sich der
	Client verbinden darf
Require Crypto Binding	Ausschließlich eine Authentifizierung
	über die Cryptobinding möglich
Server Validation	Der Client überprüft, ob das Server
	Zertifikat gültig ist, falls dies der Fall ist
	wird eine Verbindung hergestellt
Prompt for Certificates	Erlaubt dem Benutzer nicht
	vertrauenswurdige Zertifikate zu
	akzepueren
Anonymous User Name	denn, achold der DADIUS Sonver
	authontifiziert wurde
	Ris dahin putzt or dia hier angogohono
	Identität
Login Domain	
Liser Name	Benutzername
Password	Passwort
Server Names	Rietet die Mödlichkeit den Name des
	RADIUS-Servers anzugeben der die
	Netzwerkauthentifizierung und -
	Autorisierung bereitstellt
WPA2-PSK	



Password	Passwort für den AP
WPA2 EAP	
Authentication Type	Authentifizierungsmöglichkeit, nur "PEAP-MSCAHPv2" möglich
Fast Reconnect	
Guest Access	
Quarantine Checks	Aktiviert den Netzwerk Zugriffsschutz NAP
Require Crypto Binding	Ausschließlich eine Authentifizierung mit Server die cryptobinding möglich
Server Validation	
Prompt for Certificates	Verlangt nach einem validierten Server- Zertifikat, Name oder einer Root Zertifikatsauthentifizierung (CA)
Anonymous User Name	
Logon Domain	
User Name	Benutzername
Password	Passwort
Server Names	Auflistung deren Server, deren Geräte vertraut werden soll
None	Keine Sicherheit festgelegt
Use Proxy Server	Das Benutzen eines Proxy Servers
Server Address	Serveradresse des Proxy Servers
Server Port	Server Port des Proxy Servers

Wifi Restrictions

Hier können Sie diverse Wifi Restriktionen definieren.

Allow WiFi	Erlauben bzw. verbieten von WiFi
Allow Internet Sharing	Erlauben eines Hotspots
Allow Auto Connect to WiFi Sense Hot	Erlauben von automatischen
Spots	Verbindungen zu einem WiFi Sense
	Hot Spots
Allow Manual WiFi Configuration	Erlaubt es dem User sich mit nicht von
	AppTec definierten WiFi Netzwerken zu
	verbinden
WLAN Scan Frequency	Legt den WLAN-Scan Intervall fest,
	dabei verbessert ein höherer Wert die
	Erkennung von Wifi-Netzwerken



<u>VPN</u>

Nehmen Sie hier die entsprechenden Einstellungen vor, um die VPN Verbindungen zu konfigurieren

Connection Name	Angezeigte VPN Verbindungsname	
Server	Serveradresse des VPN Servers	
VPN Type	Typ der Verbindung	
IKEv2 (native)	Es wird eine native VPN Verbindung genutzt	
Authentication Type	Authentifizierungsmethode	
Bypass Local Traffic	Bei Zugriff auf interne Ressourcen wird der Verkehr nicht über die VPN Verbindung geleitet	
Trusted Network Detection	Wenn diese Funktion aktiviert ist, wird keine VPN Verbindung aufgebaut, solange der User sich im Firmen-WiFi befindet, da geschützte Ressourcen direkt auf dem Endgerät erreichbar wären Sollte diese Funktion deaktiviert sein, wird eine VPN Verbindung über das Firmennetzwerk aufgebaut Es muss eine DNS Suffix eingerichtet werden, um zu definieren bei welchem WiFi es sich um eine Firmen- WiFi handelt	
DNS Suffix	Hier können Sie den primären DNS Suffix eintragen	
Use Proxy	Die Benutzung eines Proxys	
Server Address	Serveradresse des Proxy Servers	
URL to	URL über welche die Proxy Einstellungen	
automatically	automatisch bezogen werden	
retrieve the proxy		
settings		

VPN Restrictions

Hier können Sie diverse VPN Restriktionen definieren.

Allow Manual VPN Configuration	Diese Richtlinie erlaubt bzw. verbietet dem User die VPN Einstellungen zu deaktivieren und zu verändern
Allow VPN over Cellular	Verbietet bzw. erlaubt dem Gerät eine VPN Verbindung aufzubauen, falls sich das Gerät mobile Daten nutzt
Allow VPN Roaming over Cellular	Verbietet bzw. erlaubt dem Gerät eine VPN Verbindung aufzubauen, falls sich das Gerät im Roaming befindet

<u>Bluetooth</u>

Hier können Sie festlegen, ob Bluetooth erlaubt bzw. nicht erlaubt werden soll.



Allow Bluetooth

Bluetooth aktivieren / deaktivieren

PIM Management

Exchange Active Sync

Einrichten eines ActiveSync Kontos am Endgerät

Account Name	Name des Email Accounts
Server Host Name	Adresse/FQDN des Servers
Domain Name	Domäne des Servers
Email Address	E-Mail Adresse
User Name	Benutzername
User Password	Sie können hier optional bereits dem
	User ein Passwort mitgeben
Use SSL	Nutzung einer SSL Verbindung
	Hier kann das Intervall für die
	Synchronisation festgelegt werden
Sync Interval	Manual sync = Der User muss seine
	Mails aufrufen und eine manuell
	Synchronisation durchführen
Mail Age Filter	Zeitraum bis wann die Mails
	synchronisiert werden sollen
	No filter = unbegrenzt
Log Level	Festlegung der Logginglevels für den
	ActiveSync Verkehr
Sync Email	Aktiviert = Mails werden synchronisiert
Sync Contacts	Aktiviert = Kontakte werden
	synchronisiert
Sync Calendar	Aktiviert = Kalender wird synchronisiert
Sync Tasks	Aktiviert = Aufgaben werden
	synchronisiert


<u>eMail</u>

Einrichten von POP3/IMAP4 Konten am Endgerät.

Account Description	Name des Email Accounts	
Sender Name	Angezeigter Name des Senders	
Domain Name	Domain Name für den Email Account	
Email Adress	E-Mail Adresse des Benutzers	
User Name	Benutzername	
User Password	Sie können hier optional bereits dem	
	User ein Passwort mitgeben	
	Hier kann definiert werden, falls für den	
Alternative Outgoing Server Credentials	ausgehenden Server andere	
	Credentials benötigt werden	
Outgoing Domain Name	Ausgehende Domainname	
Outgoing Server User Name	Ausgehender Benutzername	
Outgoing Server Password	Ausgehendes Passwort	
Email Protocol	POP3 oder IMAP4 kann als Protokoll	
	genutzt werden	
Incoming Mail Server Host Name	Eingehender Server Hostname	
Use SSL for Incoming Mails	Benutzung von SSL bei eingehenden	
	Mails	
Outgoing Mail Server Host Name	Ausgehender Server Hostname	
Use SSL for Outgoing Mails	Benutzung von SSL bei ausgehenden	
	Mails	
Outgoing Server Authentication	Eine ausgehende Server	
	Authentifikation wird benötigt	
	Hier kann das Intervall für die	
	Synchronisation festgelegt werden	
Sync Interval	Manual sync = Der User muss seine	
	Mails aufrufen und eine manuell	
	Synchronisation durchführen	
	Zeitraum bis wann die Mails	
Mail Age Filter	synchronisiert werden sollen	
	No filter = unbegrenzt	



Konfiguration 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 (nur auf Profil Ebene)

Sollten Sie sich in einem Profil befinden, erhalten Sie hier einen kurzen Überblick über das Profil in Bezug auf Name, OS, Erstellungsdatum, Autor, etc.

Profile Name	Name des Profils – kann direkt hier umbenannt werden
Operating System	Für welches Betriebssystem das Profil
	gilt
Created At	Erstelldatum
Created By	Ersteller des Profils
Last Change	Datum und Uhrzeit an dem die letzten
	Änderungen vorgenommen wurden
Changed By	Anzeige darüber von wem die letzte
	Änderung vorgenommen wurde
Profile Revision	Anzahl wie oft das Profil bereits
	geändert wurde

<u>Device Overview</u> (nur auf Profil Ebene)

Sollten Sie sich direkt auf einem Gerät befinden, erhalten Sie hier einen kurzen Überblick über Ihr ausgewähltes Gerät.

Device Name	Name des Geräts
Model	Model
Operating System	Modellbezeichnung
Serial Number	Betriebssystem
Device Ownership	Seriennummer des Geräts
Device Type	Firmen- oder Privatgerät
	Corporate = Firmengerät
	Employee = Privatgerät
Compliant	Ob gegen über irgendwelchen
	Richtlinien verstoßen wurde
Last Seen	Status wann sich das Gerät zuletzt am
	AppTec Server gemeldet hat



Config Revision (nur auf Device Ebene)

Hier erhalten Sie eine Übersicht welches Gruppenprofil dem Gerät zugewiesen ist.

Wenn sie auf das Gruppenprofil klicken, kommen Sie direkt zu diesem Profil und können Einstellungen vornehmen.

Mit dem Symbol können Sie die zugewiesenen Apps auf die Einstellung des Gruppenprofils zurücksetzen.

Mit dem Symbol können Sie alle getätigten Apps auf die Einstellung des Gruppenprofils zurücksetzen.

<u>Device Log</u> (nur auf Device Ebene)

Hier erhalten Sie diverse Gerätelogs.

Gegebenenfalls können Sie bei einem Fehler hier direkt die Ursache ausfindig machen.



Asset Management (only on device level)

Device Info

Model Number	Modellbezeichnung des Geräts
Product Name	Produkt Name
Hostname	Hostname
Local Hostname	Lokaler Hostname
Operating System	Betriebssystem
OS Version	Betriebssystem Version
Serial Number	Seriennummer
UDID	UDID des Gerätes
Free / Total Memory	Freier / insgesamter Speicher

<u>User Info</u>

UserID	UserID
Username	Username

<u>WiFi</u>

IP Address	IP Addresse
WiFi MAC	WiFi MAC

<u>Cellular</u>

Phone Number	Telefonnummer
Roaming Status	Aktueller Roaming Status
Roaming (Voice / Data)	Roaming Status für Anrufe / Daten
IP Address	IP Adresse
Operator/Carrier	Mobilfunk Anbieter
SIM Carrier Network	Mobilfunknetzwerk der SIM-Karte
Carrier Version	Carrier Version
ICCID	ICCID
Current MCC/MNC	Siehe "SIM MCC/MNC"
SIM MCC/MNC	Der Mobile Country Code ist eine von der ITU im
	Standard E.212 festgelegte Länderkennung, die
	zusammen mit dem Mobile Network Code (MNC) zur
	Identifizierung eines Mobilfunknetzes verwendet wird
	(=Ländercode)
	Wenn man in ein anderes Mobilfunknetz geht ist
	deshalb der "Current MCC/MNC" und "SIM MCC/MNC"
	unterschiedlich.

<u>Bluetooth</u>



Bluetooth MAC Security Management

Bluetooth MAC

Security Configuration

Passcode

Legen Sie hier die Einstellungen für das Gerätepasswort fest

Code deactivation allowed	Wenn diese Einstellung aktiviert ist, findet keine Aufforderung für das Setzen eines Passworts statt Sobald ein Passwort gesetzt ist, kann es nicht mehr deaktiviert werden
Allow simple value	Erlaube die Benutzung gleicher aufsteigender und absteigender Zeichenketten (z.B. 1234, 1111)
Require alphanumeric value	Passwörter müssen mindestens einen Buchstaben enthalten
Minimum passcode length	Minimale Länge des Passworts
Minimum number of complex characters	Minimale Anzahl alphanumerischer Zeichen im Passwort
Maximum passcode age	Anzahl der Tage, nach welchen das Passwort geändert werden muss
Maximum Auto-Lock	Maximale Dauer, nach welcher sich das Gerät sperrt
Maximum grace period for device lock	Dauer, nach welcher das Gerät in den gesperrten Stand-By geht
Maximum passcode age (1- 730 days, or none)	Maximale Passwortlebensdauer
Passcode history (1-50 passcodes, or none)	Das Benutzen eines alten Passworts ist nach dieser Anzahl wieder erlaubt

Certificate

PKCS#1	
Description	Beschreibung für das Zertifikat
Credential	Laden Sie eine pkcs1 Datei

PKCS#12	
Description	Beschreibung für das Zertifikat
Credential	Laden Sie eine pkcs12 Datei



Restriction Settings

Device Functionality

Allow Camera	Verwendung der Kamera zulassen
Allow Game Center	Erlaubt Game Center
Allow multiplayer	Erlaubt die Verwendung von Multiplayer im Game Center
gaming	
Allow adding Game	Erlaubt das Hinzufügen von Freunden im Game Center
Center friends	
Allow iCloud Photo	Erlaubt die iCloud Fotobibliothek, falls nicht erlaubt
Library	werden alle Fotos die nicht vollständig von der iCloud
	heruntergeladen worden sind vom lokalen Speicher
	gelöscht
Allow Touch ID	Touch ID zulassen

<u>iCloud</u>

Sperren Sie bestimmte Funktionalitäten mit der iCloud Synchronisierung

Allow document sync	Dokumentsynchronisation erlauben
Allow iCloud Keychain Sync	Schlüsselbund Synchronisation zulassen
Allow iCloud Notes	Erlaubt iCloud Notes
Allow iCloud BTMM	Erlaubt iCloud BTMM
Allow iCloud FMM	Erlaubt iCloud FMM
Allow iCloud Bookmarks	Erlaubt Lesezeichen
Allow iCloud Mail	Erlaubt iCloud Mail
Allow iCloud Calender	Erlaubt iCloud Kalender
Allow iCloud Reminders	Erlaubt iCloud Erinnerungen
Allow iCloud Addressbook	Erlaubt iCloud Addressbuch



Media Management

Eject at Logout	Wirft alle entfernbaren Wechseldatenträger beim
	Logout
Allow Network	Erlaubt Zugriff auf Netzwerkdatenträger
Allow Internal Disk	Erlaubt Zugriff auf den internen Datenträger
Require Authentication	Erfordere Authentifizierung für die Verwendung dieses Datenträger
Read Only	Der Nutzer kann von diesem Datenträger nur lesen
Allow External Disk	Erlaubt Zugriff auf externe Datenträger
Require Authentication	Erfordere Authentifizierung für die Verwendung dieses
	Datenträger
Read Only	Der Nutzer kann von diesem Datenträger nur lesen
Allow Disk Images	Erlaubt Zugriff auf Datenträger Abbilder
Require Authentication	Erfordere Authentifizierung für die Verwendung dieses
	Datenträger
Read Only	Der Nutzer kann von diesem Datenträger nur lesen
Allow DVD-RAM	Erlaubt Zugriff auf DVD-RAM
Require Authentication	Erfordere Authentifizierung für die Verwendung dieses Datenträger
Read Only	Der Nutzer kann von diesem Datenträger nur lesen
Allow DVD	Erlaubt Zugriff auf DVD
Require Authentication	Erfordere Authentifizierung für die Verwendung dieses
	Datenträger
Allow CD	Erlaubt Zugriff auf CD
Require Authentication	Erfordere Authentifizierung für die Verwendung dieses
	Datenträger



Connection Management

<u>Wifi</u>

Nehmen Sie an dieser Einstellung die Vorkonfiguration der Endgeräte für den Zugriff auf interne Access Points vor

Service Set Identifier (SSID)	SSID des zu verbindenden Netzwerks
Auto Join	Automatischen Beitreten zum Netzwerk
	aktivieren
Hidden Network	Aktivieren, falls der AP die SSID nicht
	broadcastet
Proxy Setup	Konfigurieren eines Proxy für den Access Point
None	Keinen Proxy festlegen
Manual	Einen Proxy manuell festlegen
Proxy Server URL	Adresse zum Abrufen der Proxy Settings
Port	Port für den Proxy festlegen
Authentication	Username zur Authentifizierung am Proxy
Password	Passwort zur Authentifizierung am Proxy
Automatic	Einen Proxy automatisch festlegen
Proxy Server URL	URL zum Abrufen der Proxyeinstellungen
Security Type	Sicherheitstyp des AP festlegen
WEP	
Password	Passwort für den AP
WPA/WPA2	
Password	Passwort für den AP
WEP Enterprise – WPA /	
WPA2 Enterprise – Any	
Enterprise	
Protocols	
TLS	Aktivieren bzw. Deaktivieren
TTLS	Aktivieren bzw. Deaktivieren
LEAP	Aktivieren bzw. Deaktivieren
PEAP	Aktivieren bzw. Deaktivieren
EAP-FAST	Aktivieren bzw. Deaktivieren
EAP-SIM	Aktivieren bzw. Deaktivieren
Use PAC	Nutzung von PAC (Protected Access Controll)
Provision PAC	Konfiguration von Provision PAC
Provision PAC	Anonyme Provisionierung von PAC
Anonymously	
	Authentifizierungsprotokoll welches genutzt
Inner	werden soll (ausschließlich bei TTLS): PAP,
Authentications	CHAP, MSCHAP, MSCHAPv2
Username	
Don't use Per-	Username zur Authentifizierung
Connection	
Password	
Identity Certificate	Kein Per-Verbindung Passwort verwenden
Outer Identity	Zertifikat zur Authentifizierung hochladen /



		auswählen
	Trust	Extern sichtbare Identität
	Trusted Certificate	
1		
	Trusted Certificate	Erstes Vertrautes Zertifikat hochladen
2		
	Trusted Certificate	Zweites Vertrautes Zertifikat hochladen
3		
	Trusted Server	Drittes Vertrautes Zertifikat hochladen
Certificate		
Name	es	
None		Die Namen der zu erwartenden Serverzertifikate
		(in einer kommagetrennten Liste)
		Keine Sicherheit festlegen

<u>VPN</u>

Connection Name	Name des VPN-Profils
VPN Type	
VPN	Der gesamte Netzwerkverkehr des Gerätes wird über die VPN-Verbindung geleitet.
Connection Type	VPN-Verbindungstyp festlegen
IPsec (cisco)	IPsec Protokoll von cisco
PPTP	PPTP Protokoll
L2TP	L2TP Protokoll
Cisco AnyConnect	AnyConnect Protokoll
Juniper SSL	Juniper SSL Protokoll
F5 SSL	F5 SSL Protokoll
SonicWall mConnect	SonicWall Mobile Connect
Aruba VIA	Aruba VIA Protokoll
Custom SSL	Verbindung über Custom SSL
OpenVPN	OpenVPN Protokoll
Proxy Setup	Konfigurieren eines Proxy für die VPN- Verbindung
None	Keinen Proxy festlegen
Manual	Einen Proxy manuell festlegen
Proxy Server URL	Adresse zum Abrufen der Proxy Settings
Port	Port für den Proxy festlegen
Authentication	Username zur Authentifizierung am Proxy
Password	Passwort zur Authentifizierung am Proxy
Automatic	Einen Proxy automatisch festlegen
Proxy Server URL	URL zum Abrufen der Proxveinstellungen



HTTP Proxy

Proxy Type	
Manual	Einen Proxy manuell festlegen
Proxy Server URL	Adresse zum Abrufen der Proxy Settings
Port	Port für den Proxy festlegen
Authentication	Username zur Authentifizierung am
	Proxy
Password	Passwort zur Authentifizierung am Proxy
Automatic	Einen Proxy automatisch festlegen
Proxy PAC URL	PAC URL des Proxy
Allow direct connection if PAC	Verbindung ohne VPN zulassen, falls
is unreachable	der PAC nicht erreichbar ist.
Allow bypassing proxy to access captive	Erlauben, an dem Proxy vorbei, sich zu
networks	internen Netzwerken zu verbinden.

<u>AirPrint</u>

IP Address	IP-Adresse des Druckers
Resource Path	Eindeutiger Pfad zum AirPrint Gerät

<u>AirPlay</u>

Device Name	Name des Gerätes
Password	Passwort zum Verbinden
	Definieren Sie eine Liste an Geräten, mit
Whitelist	welchen sich das Gerät ausschließlich
	verbinden darf



PIM Management

Exchange Active Sync

Account Name	Name des Email Accounts
eMail Address	eMail Addresse
Server Hostname	Adresse/FQDN des Servers
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 Applec Gateway will
	authenticate the device with the following name
Decoword	Domain Login Name
Passworu Deet Deve of Meil to Sure	Das Passwort für den einan Account
Past Days of Mail to Sync	Anzani an Tagen, bis zu weichen die Malis
	zurucksynchronisiert werden sollen.
	No Limit = Keine Begrenzung
Use SSL	Benutze die SSL Verschlüsselung
Advanced Option	Zeigt erweiterte Optionen
Server Port	Interner Port
Server Path	Interner Pfad
External Hostname	Externer Host
External Port	Externer Host
External Path	Externer Pfad
Use SSL for External	Benutzt SSL für den externen Exchange Host
Exchange Host	

<u>eMail</u>

Einrichten von POP3 / IMAP Konten am Endgerät

Account Description	Name des Email Accounts
Account Type	
IMAP	
Path Prefix	Der Pfad Prefix für spezielle Ordner
POP	
User Display Name	Angezeigter Benutzername
Email Address	Email-Adresse des Benutzers



Incoming Mail	Eingehende Servereinstellungen
Mail Server Address	Adresse des Mail Servers
Mail Server Port	Port des Mail Servers
User Name	Entsprechender Benutzername
Authentication Type	Authentifizierungsmethode
None	Keine Authentifizierungsmethode
Password (only on device level)	Passwortabfrage
MDM Challenge-Response	
NTLM	NTLM-Authentifizierung
HTTP MD5 Digest	
Use SSL	Aktivieren, falls SSL benötigt

Outgoing Mail	Ausgehende Servereinstellungen
Mail Server Address	Adresse des Mailservers
Mail Server Port	Port des Mail Server
User Name	Entsprechender Benutzername
Authentication Type	
None	Keine Authentifizierungsmethode
Password (only on device level)	Passwortabfrage
MDM Challenge-Response	
NTLM	NTLM-Authentifizierung
HTTP MD5 Digest	
Use SSL	Aktivieren, falls SSL benötigt
Outgoing password same as incoming	Ausgehendes Passwort entspricht dann
	dem eingehenden Passwort
	Aktivieren, falls ausgehende
Use only in mail	Nachrichten nur über die Mail-App
	versendet werden sollen

<u>CalDav</u>

Einrichtung und Verteilung eines CalDav Accounts konfigurieren

Account Description	Angezeigter Name des Accounts
Hostname	Hostname bzw. IP Adresse
Port	Port des CalDav Accounts
Principal URL	Principal URL des Accounts
Username	Entsprech. CalDav Benutzername
Password (only on device level)	Entsprech. CalDav Passwort
Use SSL	Aktivieren, falls SSL benötigt



<u>CardDav</u>

Einrichtung und Verteilung eines CardDav Accounts konfigurieren

Account Description	Angezeigter Name des Accounts
Hostname	Hostname bzw. IP Adresse
Port	Port des CardDav Accounts
Principal URL	Principal URL des Accounts
Username	Entsprech. CardDav Benutzername
Password (only on device level)	Entsprech. CardDav Passwort
Use SSL	Aktivieren, falls SSL benötigt

<u>LDAP</u>

Richten Sie an dieser Stelle eine LDAP-Verbindung ein, um einen dynamischen Zertifikatsaustausch zwischen Endgerät und Active Directory zu erlauben.

Beachten Sie, dass der benutzte User entsprechende Leseberechtigungen benötigt.

Account Description	Beschreibung des Accounts
Account Username	Benutzer für den LDAP-Zugriff
Account Password	Passwort für den LDAP-Zugriff
Account Hostname	Hostname/IP Adresse des LDAP Servers
Use SSL	Aktivieren, falls SSL benötigt

Im zweiten Abschnitt können Sie noch die einzelnen Filter zur Suche im LDAP Verzeichnis definieren.

Description	Scope	Search Base
Beschreibung des Filters	Suchlevel im LDAP Verzeichnis	Definieren der einzelnen Filter



V. Dashboard & Reporting

Dashboard

Das "Dashboard" zeigt Ihnen grundlegende Informationen auf einen Blick an:

- Meist installierten Apps
- Aktueller Status der Endgeräte
- Übersicht der aktuellen Plattformen
- Geräte die Roaming aktiviert haben
- Genutzter Netzanbieter
- Neue Registrationen / ausstehende Registrationen





Extended Reporting

Das "Extended Reporting" bringt detaillierte und informationsreiche Ansichten, Grafiken und Übersichten mit.

In der Regel finden Sie in den Unterpunkten folgende Tabs:

- All (Alle Geräte)
- iOS (nur iOS Geräte)
- Android (nur Android Geräte)
- ggfs. Windows (nur Windows Phone Geräte)
- Bei Ausnahmenfällen wird dies explizit in dem jeweiligen Unterpunkt erwähnt

Unter dem jeweiligen Unterpunkt können Sie sich mit 🖆 (Export Data) die aktuelle Übersicht als .csv Datei exportieren lassen.

Sollte der Unterpunkt eine Grafik enthalten, können Sie mit 🔽 (Hide Chart) die Grafik ausblenden, bzw. mit 🔼 (Show Chart) die Grafik (wieder) einblenden.

Folgende Punkte sind standardmäßig vorzufinden:

Device Alias	Gerätename
Device Owner	Besitzer des Gerätes
eMail	E-Mail Adresse des Gerätes
Phone	Telefonnummer
OS	Betriebssystem
Last Seen	Zuletzt beim AppTec Server gemeldet



Compliance Reports

Rooted Devices

Übersicht aller Geräte die gerootet / gejailbreakt wurden.

Zusätzlicher Punkt in dieser Kategorie:

			All	i	OS Android					S	upport@milan	consult.de 🗸
Root		< 1										
The second se	Compliance Reports	~	Rooted Devices						Ē	🛨 Gen	erated: 08:43:0	9 20 Mar 2015
Ē	Rooted Devices		Device Alias	\$	Device Owner	\$ eMail	\$ Phone	\$ Manufacturer	\$	0S -	Last Seen	\$
<u>(4</u>)	Roaming Devices											
യ്യ	Roaming Enabled Devices											
2	Supervised Devices											
	Inactive Devices											
	Device Reports	~										
•	App Reports	~										

Roaming Devices

Übersicht aller Geräte die sich im Roaming befinden.

Zusätzlicher Punkt in dieser Kategorie:

Phone	Telefonnummer
-------	---------------

	All	iOS And	roid Windows			suppo	rt@milanconsult.de 🗸
Root 🗸							
Compliance Reports							~
Rooted Devices							
Roaming Devices							
Roaming Enabled Devices							
Supervised Devices							
Inactive Devices							
Device Reports 🗸							
App Reports 🗸 🗸	Roaming Devices				12	Generate	d: 08:43:03 20 Mar 2015
	Device Alias	Device Owner	r 🗘 eMail	\$	Phone 🗘	05 \$	Last Seen 🗘
	Device of Fabian	Fabian	fabian.	de		iOS	03 Mar 2015
	Device of Lukas	Lukas	lukas.s	Lde	-	iOS	20 Mar 2015



Roaming Enabled Devices

Übersicht aller Geräte die Roaming aktiviert haben.

			∢ ▶	All	iOS	Android	Windows					support@mil	anconsult.de 🗸
Root		~											
P	Compliance Reports	~	Roaming E	Enabled Device	S						12	Generated: 08:4	3:12 20 Mar 2015
B	Rooted Devices		Device Alia	IS	\$	Device Owner	<	e Mail	Phone	\$ OS	\$	Last Seen	\$
(1)	Roaming Devices												
യ്യ	Roaming Enabled Device	s											
2	Supervised Devices												
	Inactive Devices												
	Device Reports	~											
	App Reports	~											

Supervised Devices

Alle Geräte die Supervised sind (ausschließlich iOS Geräte)

Inactive Devices

Übersicht aller inaktiven Geräte.



Device Reports

Devices by Ownership

			< ►							l s	upport@milanconsult.de	~
Root	· · · · · · · · · · · · · · · · · · ·											
W h	Compliance Reports	^	Supervised Devices						≌	Gen	erated: 08:43:14 20 Mar 2	2015
			Device Alias	\$ Device Owner	\$ eMail		\diamond	Phone		\$	Last Seen	\$
	Rooted Devices		Device of Felix	Felix	felix.	de					05 Mar 2015	
<u>(</u>)	Roaming Devices											
യ്യ	Roaming Enabled Devices											
1	Supervised Devices											
	Inactive Devices											
	Device Reports	~										
	App Reports	~										

Hier können Sie sehen wie viel Geräte aktuell Corporate (Firmengeräte) und Employee (Privatgeräte) im Einsatz sind.

Zusätzlicher Punkt:

Ownership	Corporate = Firmengerät
	Employee = Privatgerät





All Devices

Hier finden Sie eine Übersicht von allen Geräten mit den wichtigsten Informationen.

Zusätzliche Punkte:

	AII	iOS Androi	d Window	S		support@rr	ilanconsult.de 🗸							
Root 🗸														
Compliance Reports 🗸			20%				~							
Device Reports			20 /0											
Levices by Ownership														
All Devices		20%												
Device Carriers														
SAFE Devices														
App Reports 🗸 🗸														
	All Devices					Generated: 08	43:21 20 Mar 2015							
	Device Alias	Contraction Device Owner	Ownership 🗘	os 💠	Serial	IMEI 🗘	Last Seen 🗘							
	Device of Fabian	Fabian I	Corporate	ios	DLXG3N72DKNY	01 279900 266046 5	03 Mar 2015							
	Device of Felix.	Felix	Corporate	IOS	DMPG65KRDFJ1	01 280200 992256 3	05 Mar 2015							
	Device of Matthias	Matthias	Corporate	Android	542a975e	353726060748731	10 Mar 2015							
	Device of Max Mustermann	Max Mustermann	Corporate	Windows	um:uuld:BFD6EC34- B1B6-5561-8B12-14F06891EE21		01 Feb 2015							
	Device of Lukas	Lukas	Corporate	IOS	DMPK56KGF18P	99 000289 227034 7	20 Mar 2015							

Ownership	Corporate = Firmengerät
	Employee = Privatgerät
Serial	Serialnummer des Gerätes
IMEI	IMEI Nummer des Gerätes



Device Carriers

Hier erhalten Sie eine Übersicht in Hinsicht auf den Carrier (Mobilfunkanbieter).

Zusätzliche Punkte:

Carrier	Mobilfunkanbieter
	z.B. Telekom, Vodafone

SAFE Devices

Hier erhalten Sie eine Übersicht welche Geräte welche SAFE Version nutzen. Da diese Übersicht bzw. SAFE nur für Samsung Geräte verfügbar ist, sehen Sie in diesem Punkt nicht die üblichen Tabs.

Zusätzliche Punkte in dieser Kategorie:

Phone	Telefonnummer
SAFE Version	SAFE Version



App Reports

Hier erhalten Sie alle möglichen Übersichten in der Hinsicht auf Apps.

Installed Apps

Hier erhalten Sie eine Übersicht aller Apps die installiert worden sind.

Sie können dies anhand folgender Kriterien sortieren:

- All Apps (Es werden alle Apps berücksichtigt)
- System Apps (Es werden ausschließlich vom Gerätehersteller kommende Apps angezeigt)
- User Apps (Es werden ausschließlich die manuell installierten Apps angezeigt, offizieller AppStore und AppTec Enterprise Store)

Name	Name der jeweiligen App bzw. Dienst
Identifier	Eindeutige ID der App / eines Dienstes
Total Count	Anzahl wie oft diese App / dieser Dienst
	auf den Endgeräten installiert ist

	All iOS Android		👤 support@milanconsult.de 🗸
Root 🗸			
Compliance Reports	4		•
Device Reports 🗸	3		
App Reports			
installed Apps	2		
Most Installed Apps	1		
Mandatory Apps			
Blacklisted Apps			
NX .			
	Installed Apps V		Generated: 09:07:37 20 Mar 2015
	Name O	ldentifier	
	AirDraid	com.sec.android.app.tourviewer	1
	AirDiolo	com comound endroid ann ainvakeumiew	1
		com soc apdroid app taskmanager	1
	Aktive Anwendungen	com sec android vidaetana activo application videet	1
	AllPhare EilePhare Sension	com compute android allabara contras fileshara	1
	Andraid System WebView	com google apdroid webview	1
	Android System	android	1
	ANT HAI Service	com dei ant senier	1
	ANT Radio Service	com dsi ant service socket	1
	ANT+ Plugins Service	com dei ant plugins antplus	1
	Application installer	com.sec.android.preloadinstaller	1
	AppTec MDM	com.apptec360.android.mdm	1
	Assistentenmenü	com.samsung.android.app.assistantmenu	1
	AudioConnectionService	com.samsung.android.sdk.professionalaudio.app.audi	1
		· · · · · · · · · · · · · · · · · · ·	



Most Installed Apps

Hier erhalten Sie eine Übersicht der meist installierten Apps.

Sie können dies anhand folgender Kriterien sortieren:

- All Apps (Es werden alle Apps berücksichtigt)
- System Apps (Es werden ausschließlich vom Gerätehersteller kommende Apps angezeigt)
- User Apps (Es werden ausschließlich die manuell installierten Apps angezeigt, offizieller AppStore und AppTec Enterprise Store)

Name	Name der jeweiligen App bzw. Dienst
Identifier	Eindeutige ID der App / eines Dienstes
Total Count	Anzahl wie oft diese App / dieser Dienst
	∣ aut den Endgeraten installiert ist





Mandatory Apps

Hier erhalten Sie eine Übersicht von allen Mandatory (zwingend erforderlichen) Apps.

Es kann zwischen folgenden Kriterien unterschieden werden:

- All Apps (Alle Apps)
- InHouse Apps (selbst hochgeladene / eigenentwickelte Apps)
- Store Apps (offizielle AppStore Apps)

Name	Name der jeweiligen App bzw. Dienst
Identifier	Eindeutige ID der App / eines Dienstes
	Für welchen AppStore es sich handelt:
App Source	- Google PlayStore
	- iTunes AppStore (iOS)
	- Microsoft Store (Windows Phone=
Total Count	Anzahl wie oft diese App / dieser Dienst
	auf den Endgeräten installiert ist

			All	iOS	Andr	oid		support@milar	iconsult.de	~
All Grou	ps	~								
P	Compliance Reports		Mandatory Apps	All Apps	~		Ľ	Generated: 04:04:	09 20 Mar 20)15
	Device Reports	~	Name	All Apps	\$	Identifier 🗘	App Source	\$	OS	\$
		·	DB Navigator für iPad	Store Apps		com.deutschebahn.navigator.ipad	iTunes		iOS	
-	App Reports									
	Installed Apps									
G	Most Installed Apps									
Ŷ	Mandatory Apps									
	Blacklisted Apps									

Blacklisted Apps

Hier erhalten Sie eine Übersicht über alle definierten Blacklsited Apps.

Name	Name der jeweiligen App bzw. Dienst
Identifier	Eindeutige ID der App / eines Dienstes
OS	Um welche Plattform (Android, iOS,
	Windows Phone) es sich handelt

			< ►	All			support@mila	inconsult.de 🗸
All Grou	ps	~						
P	Compliance Reports	~	Blacklis	sted Apps			Generated: 09:20	:25 20 Mar 2015
			Name		\$	Identifier	\$ OS	\$
	Device Reports	~	Whats/	App Messenger		com.whatsapp	Android	
-		^						
6	Installed Apps							
G	Most Installed Apps							
	Mandatory Apps							
\$	Blacklisted Apps							



VI. Mandanten Management

Im Mandanten-Portal können weitere AppTec Lizenzen hochgeladen werden, welche daraufhin als neue AppTec-Instanz (genannt "Client") fungieren. Im Endeffekt können also mehrere Clients mit einer Installation verwaltet und zur Verfügung gestellt werden.

Um die entsprechende Oberfläche zu öffnen, melden Sie sich bitte auf der Appliance mit den "Server Admin Credentials" an, welche Sie während des Installationsvorgangs festgelegt haben ("STEP THREE" der Appliance Config).

Oberfläche

List all clients

												۲		
🚚 List all clients											 	 		-
APNS expiry dates	Client Id¢	Company Name	0	eMail	0	Country	٥	Ref¢	Devices\$	Registration Date	\$ Last Login	\$ License\$	CB License\$	s
Upload Client License														1
Durchsuchen														
υριοκα														
Import Client Data														
Max mesize is 64 megabyte														
Overwrite existing Client Data														
Durchsuchen														
Upload														
·														

Client ID	Client ID
Company Name	Firmenname
eMail	E-Mail Adresse der Kontaktperson
Country	Land
Ref	Ref
Devices	Anzahl an registrierten Geräten
Registration Date	Zeitpunkt der Lizenzeinspielung
Last Login	Letzter Login des Admin Accounts
License	Anzeige des Lizenztyps (Free Paid)
CB License	Typ der ContentBox Lizenz (Free Paid)
Status	Aktueller Status des AppTec-Clients
Expired	Zeigt an, ob die Lizenz abgelaufen ist



Hier wird Ihnen eine Übersicht aller eingespielten AppTec-Clients angezeigt. <u>APNS expiry dates</u>

				۲			~
List all clients	Client Id	Company Name	0	Expire Date	Ó	Info	Ó
APNS expiry dates					~		
Upload Client License							
Durchsuchen Keine Datei ausgewählt.							
Upload							
Import Client Data							
Max filesize is 64 Megabyte							
Overwrite existing Client Data							
Keine Datei ausgewählt.							
Upload							

Client ID	Client ID
Company Name	Firmenname
Expire Date	Ablaufdatum für das Apple APNS-
	Zertifikat
Info	Weitere Informationen

Auf dieser Übersichtsseite sind alle Ablaufzeitpunkte für die APNS Zertifikate notiert.



Account Information

				٢	~
List all clients	Company Name	AppTec GmbH			
APRIS expiry dates	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			
Upload Client License	Database Name	apptec_account8880275090			
Durchsuchen bau-fritz_license_5551a3ff80d08_	Root User				E
Upload	Root Login				
Import Client Data	ContenBox	Free License, limited to 25 devices (Purchase License)			
Max filesize is 64 Megabyte	ContenBox Quota	250MB			
Overwrite existing Client Data					. 1
Durchsuchen	With the Button below you can delete the Account of AnnTec GmbH				
Upload					-
	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	Firmenname
Registration Date	Zeitpunkt der Lizenzeinspielung
License Type	Anzeige des Lizenztyps (Free Paid)
License Expiration Date	Ablaufdatum der Lizenz
Account Status	Status des Accounts (Enabled Disabled)
Devices	Anzahl an registrierten Geräten
Contact Person	Kontaktperson
Phone	Telefonnummer der Kontaktperson
eMail	Email Adresse der Kontaktperson
Client Identifier	Kennnummer des AppTec-Clients
Database name	Datenbankname der AppTec-Clients
Root User	Vollständiger Name des Root Users
Root Login	Loginname des Root Users (Email)
ContentBox	Lizenzinformationen bzgl. der Content
	Box
ContentBox Quota	Verfügbarer ContentBox-Speicherplatz

Block Account / Unblock Account	Nach einem Klick auf "Block Account" ist kein Zugriff auf den AppTec-Client mehr möglich
Delete Account	Hier können Sie die AppTec-Client löschen



Einspielen einer weiteren AppTec-Lizenz

			6	9		*
List all clients			-	~	-	~
APNS expiry dates	Client Id 🗢	Company Name	Expire Date	\$	info	¢
Upload Client License						
Durchsuchen Keine Datei ausgewählt.						
upioad						
Import Client Data						
Max filesize is 64 Megabyte						
Overwrite existing Client Data						
Durchsuchen Keine Datei ausgewählt.						
upload						

Nachdem Sie eine weitere AppTec-Lizenz erhalten haben, können Sie diese im Mandanten-Portal hochladen.

Klicken Sie hierzu auf "Durchsuchen", wählen Sie die entsprechende Lizenzdatei aus und klicken danach auf "Upload". Der neue AppTec-Client ist damit erfolgreich eingespielt.



Nach einem Klick auf "Renew Cache", was ein Aktualisieren der Liste bewirkt, wird der neu eingespielte Client angezeigt.



KONTAKT

Noch fragen? Kontaktieren Sie uns einfach unter:

Für allgemeine technische Fragen support@apptec360.com +41 61 511 3210

Für Fragen bzgl. der Installation einer virtuellen Appliance consulting@apptec360.com +41 61 511 3214

DISCLAIMER

© AppTec GmbH

Diese Dokumentation ist urheberrechtlich geschützt. Alle Rechte liegen bei der AppTec GmbH. Jede andere Nutzung, insbesondere die Weitergabe an Dritte, Speicherung innerhalb eines Datensystems, Verbreitung, Bearbeitung, Vortrag, Aufführung und Vorführung sind untersagt. Dies gilt sowohl für das gesamte Dokument als auch Teile davon. Änderungen vorbehalten.

Andere, an dieser Stelle nicht ausdrücklich aufgeführte, Firmen-, Marken- und Produktnamen sind Marken oder eingetragene Marken ihrer jeweiligen Inhaber und unterliegen dem Markenschutz. Änderungen und Irrtümer vorbehalten.