AppTec360 Enterprise Mobile Manager & ContentBox

Verwaltungshandbuch | Version 5.0 (202110)

Inhaltsverzeichnis

- SecurePIM Sicherheit
- SecurePIM-Browser
- Tauschen Sie

Verbindungsmanagement

- Wi-Fi
  - Proxy-Einrichtung
  - Sicherheit Typ
- VPN
  - VPN-Typ
    - VPN
    - Pro-App VPN
  - Proxy-Einrichtung
- APN
- Zellulär
- HTTP-Proxy
- AirPrint
- AirPlay

PIM-Verwaltung

- Exchange Active Sync
- eMail
  - Eingehende Post
  - Ausgehende Post
- CalDav
- Abo-Kalender
- LDAP

Web Management

- Webclips
- Web-Inhaltsfilter

App Verwaltung

- Enterprise App Manager
  - Installierte Apps (nur auf Geräteebene)
  - Obligatorische Apps
    - Installations-Optionen
  - Web Apps

- Einschränkung & Einstellungen
  - Auf der schwarzen Liste / Whitelist stehende Apps
  - SysApp-Einschränkungen
  - App-VPN
  - App-Einstellungen
- Enterprise App Store
  - iTunes Apps
  - Hausintern
- Kiosk-Modus
  - Anwendungstyp
    - Paket
    - URL
  - Einstellungen für den Kioskmodus

Android Enterprise – Vollständig verwaltete Gerätekonfiguration

Allgemein

- Gruppenprofilübersicht (nur auf Gruppenebene)
- Geräteübersicht (nur auf Geräteebene)
- Config Revision (nur auf Geräteebene)
- Geräteprotokoll (nur auf Geräteebene)
  - Befehl Log
  - Mögliche Befehlszustände
- Geräteeinstellungen
  - Client-Konfiguration
  - Tapete

Asset Management (nur auf Geräteebene)

- Geräte-Infos
  - Wi-Fi
- Zellulär
- Bluetooth

Sicherheitsmanagement

- Anti-Diebstahl (nur auf Geräteebene)
  - GPS-Informationen (nur auf Geräteebene)
  - Wischen & Sperren (nur auf Geräteebene)
  - Nachricht (nur auf Geräteebene)

- Sicherheitskonfiguration
  - Geräte-Passcode
  - AntiVirus
- Ende der Lebensdauer (nur auf Geräteebene)
  - Wischen (nur auf Geräteebene)
- Einstellungen zur Einschränkung
  - Beschränkungen
- Zertifikat Management

Verbindungsmanagement

- Wifi
  - Sicherheit Typ
    - WEP
    - WPA/WPA2
    - 802.1x EAP
- VPN
  - VPN-Typ
    - VPN
    - Pro-App VPN
- Beschränkungen

PIM-Verwaltung

- Google Mail Austausch

App Verwaltung

- Enterprise App Manager
  - Installierte Apps (nur auf Geräteebene)
  - System-Apps (nur auf Geräteebene)
  - Obligatorische Apps
  - Black- & Whitelisting
  - AE System Apps
- Beschränkungen & Einstellungen
  - App Management Einstellungen
- Enterprise App Store
  - Hausintern
- Enterprise Play Store
  - AE Play Store
- Kiosk-Modus & Launcher

- Tapete
- Asset Management (nur auf Geräteebene)
  - Geräte-Infos
    - Wi-Fi
  - Zellulär
  - Bluetooth
- Sicherheitsmanagement
  - Anti-Diebstahl (nur auf Geräteebene)
    - GPS-Informationen (nur auf Geräteebene)
    - Wischen & Sperren (nur auf Geräteebene)
    - Nachricht (nur auf Geräteebene)
  - Sicherheitskonfiguration
    - Geräte-Passcode
    - Container Passcode
    - AntiVirus
  - Ende der Lebensdauer (nur auf Geräteebene)
    - Wischen (nur auf Geräteebene)
  - Einstellungen zur Einschränkung
    - Beschränkungen
  - Zertifikat Management
- Verbindungsmanagement
  - Wifi
    - Sicherheit Typ
      - WEP
      - WPA/WPA2
      - 802.1x EAP
  - VPN
    - VPN-Typ
      - VPN
      - Pro-App VPN
  - Beschränkungen
- PIM-Verwaltung
  - Google Mail Austausch
- App Verwaltung
  - Enterprise App Manager

- Nachricht (nur auf Geräteebene)
- Sicherheitskonfiguration
  - Passcode
  - Verschlüsselung
  - AntiVirus
- Ende der Lebensdauer (nur auf Geräteebene)
  - Wischen (nur auf Geräteebene)
- Einstellungen zur Einschränkung
  - Beschränkungen
  - AE Geräteeigentümer

BYOD Container

- Android Unternehmen
  - Android Unternehmen
  - Google Mail Austausch
  - AE System Apps
  - Container Passcode
- Samsung KNOX
  - Aktivierung
  - Knox Passcode
  - Knox Sicherheit
  - Knox Börse
  - Knox eMail
  - Knox Apps

Verbindungsmanagement

- Wifi
  - Sicherheit Typ
    - WEP
    - WPA/WPA2
    - 802.1x EAP
- VPN
- Beschränkungen
- APN
- Bluetooth

PIM-Verwaltung

- Tauschen Sie

- eMail
- AE Gmail Exchange

App Verwaltung

- Enterprise App Manager
  - Installierte Apps (nur auf Geräteebene)
  - System-Apps (nur auf Geräteebene)
  - Obligatorische Apps
  - AE System Apps
- Beschränkungen & Einstellungen
  - Black- & Whitelisting
  - Sys App-Einschränkungen
    - Samsung Apps
    - Huawei Apps
  - App Management Einstellungen
- Enterprise App Store
  - Playstore
  - Hausintern
- Enterprise Play Store
- Kiosk-Modus & Launcher
  - Kiosk-Modus
  - AppTec360-Startprogramm
  - AppTec360 Einstellungen

Fernsteuerung

- Splashtop
- Teamviewer

Content Management

- Inhaltsbox
- Sicherer Browser

Konfiguration Windows 10 PC

Allgemein

- Gruppenprofilübersicht (nur auf Gruppenebene)
- Geräteübersicht (nur auf Geräteebene)
- Einstellungen
- Config Revision (nur auf Geräteebene)

- Geräteprotokoll (nur auf Geräteebene)
  - Befehl Log
  - Mögliche Befehlszustände
- Asset Management (nur auf Geräteebene)
  - Geräte-Infos
  - Zellulär
  - Informationen zur Synchronisierung
- Sicherheitsmanagement
  - Anti-Diebstahl (nur auf Geräteebene)
    - GPS-Informationen (nur auf Geräteebene)
    - GPS-Einstellungen
  - Sicherheitskonfiguration
    - Passcode
    - Antivirus
    - Sicherheitszentrum
    - Firewall-Konfiguration
    - Firewall-Regeln
  - Einstellungen zur Einschränkung
    - Gerätefunktionalität
  - BitLocker
    - BitLocker-Konfiguration
    - BitLocker-Status
  - Zertifikat Management
    - Zertifikat Liste
    - Zertifikat Konfiguration
    - SCEP
- Verbindungsmanagement
  - Wifi
    - Sicherheit Typ
    - Proxy-Server verwenden
  - Wifi-Einschränkungen
  - VPN
    - Verbindungstyp
    - Allgemeine VPN-Konfigurationen
  - VPN-Einschränkungen
  - Bluetooth
- PIM-Verwaltung

- Exchange Active Sync
- eMail
- App Verwaltung
  - Enterprise App Manager
    - Installierte Apps
    - Obligatorische Apps
    - Sys App-Einschränkungen
    - Black- & Whitelisting

MacOS Konfiguration

Allgemein

- Gruppenprofilübersicht (nur auf Gruppenebene)
- Geräteübersicht (nur auf Geräteebene)
- Config Revision (nur auf Geräteebene)
- Geräteprotokoll (nur auf Geräteebene)
  - Befehl Log
  - Mögliche Befehlszustände

Asset Management (nur auf Geräteebene)

- Geräte-Infos
- WiFi
- Zellulär
- Bluetooth

Update Management (nur auf Geräteebene)

- Infos aktualisieren

Sicherheitsmanagement

- Anti-Diebstahl
  - Wischen & Sperren
- Sicherheitskonfiguration
  - Passcode
  - Zertifikat
- Einstellungen zur Einschränkung
  - Gerätefunktionalität
  - iCloud
  - Medienmanagement

Verbindungsmanagement

Allgemeiner Überblick

Einführung in AppTec360

Die Enterprise-Mobile-Management-Lösung von AppTec bietet die Möglichkeit, alle mobilen Geräte über eine intuitive Management-Konsole zu verwalten und zu konfigurieren. In diesem Szenario kann der EMM-Server entweder in Ihrer eigenen Umgebung laufen oder Sie können unsere Cloud-basierte Lösung nutzen.

Auch wenn es um die zentrale Installation von Unternehmensanwendungen auf Smartphones geht, sind Sie bei uns an der richtigen Adresse. Mit dem Enterprise Mobile Manager können Sie Unternehmensanwendungen und -dokumente innerhalb von Sekunden auf Geräte verteilen oder unerwünschte Anwendungen mit White/Blacklisting blockieren.

Die Verwendung privater Geräte in Unternehmen stellt eine neue Herausforderung für die Sicherung von Smartphones und Tablets dar. Da die Mitarbeiter ihre Smartphones immer häufiger nutzen wollen, müssen IT-Administratoren eine große Anzahl verschiedener Gerätetypen schützen. Wir helfen Ihnen bei der Sicherung aller Geräte und der darauf gespeicherten sensiblen Daten und verwalten sie über eine intuitive Konsole.

Unterstützte Gerätebetriebssysteme

AppTec360 bietet Unterstützung für iOS-, Android- und Windows-Geräte. Bitte beachten Sie, dass der Funktionsumfang der genannten Plattformen von einem Betriebssystem zum anderen unterschiedlich sein kann.

- Apple iOS 11.0 oder höher*
- Apple macOS 10.11 oder höher
- Google Android 4.4 oder höher** in der Cloud-Version
- Google Android 4.1 oder höher** auf der OnPrem Version
- MS Windows 10 oder höher*** (Desktop-Computer, Notebook und Tablet)

**Bitte beachten Sie, dass Geräte mit iOS 10 oder früher aufgrund drastischer Änderungen von Apple im Registrierungsprozess nicht registriert werden können.*

***Geräte können verbunden und konfiguriert werden, auch wenn sie eine Version verwenden, die vom Hersteller nicht mehr unterstützt wird. Bitte beachten Sie, dass es Funktionen geben kann, die eine bestimmte Android-Version erfordern. In Supportfällen folgen wir dem offiziellen Support des Herstellers. Bei Problemen oder Fehlern, die durch eine veraltete Version verursacht werden, die vom Hersteller nicht mehr unterstützt wird, behalten wir uns das Recht vor, nur begrenzten Support anzubieten.*

****Home Version von Windows wird aufgrund von Einschränkungen des Betriebssystems nicht unterstützt. Wir empfehlen dringend, eine Betriebssystemversion zu verwenden, die noch vom Hersteller unterstützt wird. Nicht nur aus Kompatibilitätsgründen, sondern auch aus Sicherheitsgründen. Wir empfehlen daher iOS 12 oder höher und Android 9 oder höher.*

Unterstützte LDAP-Verzeichnisse

- Microsoft Active Directory
- LDAP öffnen

Aktuelle Informationen über "Unterstützte Gerätebetriebssysteme" und "Unterstützte LDAP-Verzeichnisse" finden Sie hier:

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

Erläuterung des „Überwachungsmodus“ auf Apple-Geräten

Der Supervised-Mode stellt eine erweiterte Schnittstelle für iOS-Geräte dar.

Auf dem entsprechend konfigurierten Gerät können zusätzliche Einschränkungen, die sich auf die Funktionalität des Endgeräts beziehen, vorgenommen werden. Diese sind auch im Verwaltungshandbuch enthalten und mit einem Banner gekennzeichnet.

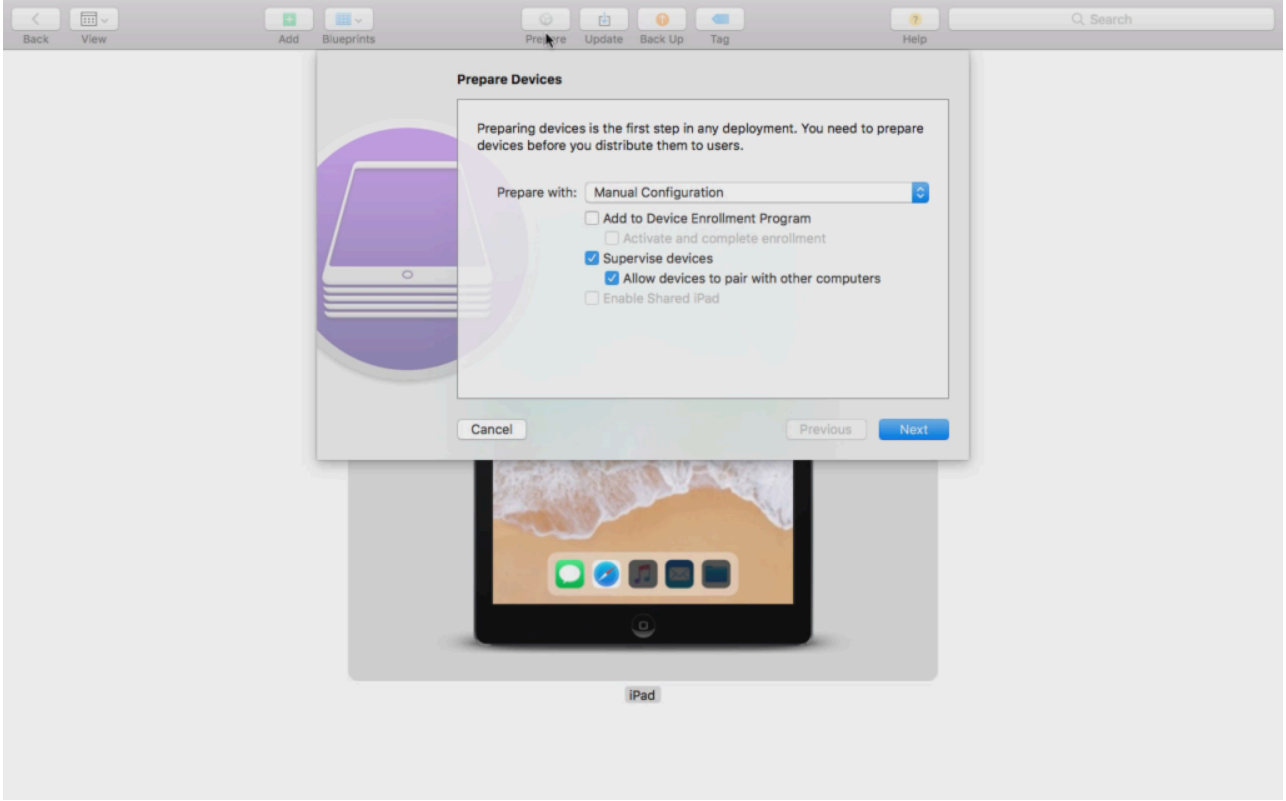
Verfügbar im Überwachungsmodus

Der "Supervised-Mode" kann mit dem Programm "Apple Configurator" aktiviert werden. Der Apple Configurator kann als Konfigurationstool (über die USB-Schnittstelle) die Standardeinstellungen auf neuen iOS-Geräten festlegen.

Das Tool kann nicht nur Konfigurationsprofile, sondern auch Anwendungen installieren. Es ist kostenlos, erfordert aber einen Mac Computer.

Aktivieren Sie den überwachten Modus

1. Öffnen Sie den Apple-Konfigurator



2. Klicken Sie auf das Gerät und wählen Sie "Vorbereiten".
3. Wählen Sie "Manuelle Konfiguration" und "Geräte überwachen".
4. Klicken Sie auf "Weiter"
5. (Fakultativ) Jetzt können Sie einen MDM-Server hinzufügen, auf dem das Gerät registriert werden soll. Den Link dazu finden Sie unter "Allgemeine Einstellungen - iOS Konfiguration - Konfigurator & URL" Wählen Sie Ihre Organisation oder erstellen Sie eine neue
6. Wählen Sie Ihre Organisation oder erstellen Sie eine neue
7. Wählen Sie aus, welche Schritte bei der Ersteinrichtung übersprungen werden sollen und klicken Sie auf "Weiter" (ACHTUNG: Wenn Sie fortfahren, wird Ihr Gerät gelöscht!)

Ihr Gerät wird nun in den überwachten Modus versetzt. Dies kann einige Minuten dauern. Danach wird das Gerät neu gestartet.

Jetzt wird Ihr Gerät überwacht!

Hinzufügen eines Geräts zur DEP

Sie können Geräte auch über den Apple Configurator zum DEP (Device Enrollment Programm) hinzufügen, wenn Ihre Geräte mit iOS 11 oder höher arbeiten.

Mehr Informationen über DEP: https://www.apple.com/business/dep/

Führen Sie die gleichen Schritte aus wie bei der Überwachung eines Geräts und markieren Sie zusätzlich die Option "Zum Programm für die Geräteanmeldung hinzufügen". Sie werden nach Ihren DEP-Anmeldedaten gefragt, wenn Sie sich noch nie mit dem Apple Configurator bei DEP angemeldet haben.

Nachdem der Prozess abgeschlossen ist, finden Sie das Gerät im DEP Server unter "Von Apple Configurator 2 hinzugefügte Geräte". Sie können nun diesen Server verwenden und ihn mit der Verwaltungskonsole verbinden oder das Gerät auf einen bereits vorhandenen Server übertragen.

Sie haben nun erfolgreich ein Gerät zur DEP hinzugefügt!

Erläuterung von Android Enterprise

Was ist Android Enterprise?

Android Enterprise bietet eine bessere Kontrolle über Arbeitsgeräte, die mit einem MDM verwaltet werden. Dies ermöglicht es Administratoren, entweder die volle Kontrolle über ihre Android-Geräte zu haben oder die Unternehmensdaten von den privaten Daten auf den Container-Geräten zu trennen. Außerdem ermöglicht Android Enterprise eine einfachere Registrierung der Geräte und eine einfache App-Verteilung.

Was sind die Voraussetzungen für die Verwendung von Android Enterprise?

Android Enterprise kann von jedem kostenlos genutzt werden. Sie müssen nur ein Google-Konto mit dem MDM verbinden, um alle Android Enterprise-Funktionen zu aktivieren. Mehr dazu finden Sie im Abschnitt Android Enterprise.

Android Enterprise kann auf Geräten mit Android 5.1 oder höher verwendet werden, mit Ausnahme des Enhanced Work Profile (siehe unten). Wir empfehlen mindestens Android 7 oder höher für eine einfachere Anmeldung oder Android 11, um alle verfügbaren Funktionen nutzen zu können.

Welche Modi sind bei Android Enterprise verfügbar?

Bei der Verwendung von Android Enterprise stehen Ihnen 3 verschiedene Modi zur Verfügung.

AE Vollständig verwaltetes Gerät (Work Managed): Ein vollständig verwaltetes Gerät, das nur für die Arbeit verwendet wird. Dies ermöglicht dem Administrator die volle Kontrolle über das Gerät. Eine private Nutzung des Geräts ist damit nicht möglich. Um Geräte in diesem Modus zu registrieren, müssen die Geräte zurückgesetzt und mit einem QR-Code registriert werden (siehe AE-Registrierung) oder über Knox Enrollment oder Zero Touch registriert werden.

AE BYOD Container: Der BYOD-Container (bring your own device) ermöglicht es Benutzern, auf Unternehmensdaten auf ihrem privaten Telefon in einem separaten Container zuzugreifen. In diesem Modus können private Apps keine Unternehmensdaten und -Apps sehen und umgekehrt. Um Geräte in diesem Modus zu registrieren, muss die AppTec App heruntergeladen und ein QR-Code gescannt werden. Erstellen Sie ein Gerät in der Konsole und wählen Sie "AE Container (BYOD & Enahnced Work Profile)" als Gerätetyp. Klicken Sie auf den QR-Code auf dem neu erstellten Gerät, um den QR-Code zu erhalten und stellen Sie den ersten Schalter auf "Legacy & BYOD".

AE Enhanced Work Profile: (erfordert Android 11 oder höher) Während der oben erwähnte BYOD-Container Unternehmensdaten auf ein privates Gerät bringt, tut das Enhanced Work Profile dasselbe, aber für ein unternehmenseigenes Gerät. Es erstellt denselben Container, gibt dem Administrator aber

etwas mehr Kontrolle über das Gerät, so dass der Benutzer das MDM nicht einfach vom Gerät entfernen kann. Erstellen Sie ein Gerät in der Konsole und wählen Sie "AE Container (BYOD & Enahnced Work Profile)" als Gerätetyp. Klicken Sie auf den QR-Code auf dem neu erstellten Gerät, um den QR-Code zu erhalten und stellen Sie den ersten Schalter auf "Erweitertes Arbeitsprofil". Dieser QR-Code kann gescannt werden, nachdem Sie das Gerät zurückgesetzt und 6 Mal auf den Bildschirm getippt haben, wie in Methode 1 in AE Enrollment beschrieben.

Wie kann ich Android Enterprise-Geräten Apps zuweisen?

Zuerst müssen Sie die Apps, die Sie verwenden möchten, unter Allgemeine Einstellungen → App-Verwaltung → AE Play Store → Play Store Apps genehmigen. Nachdem Sie eine App genehmigt haben, können Sie sie der obligatorischen App-Liste → Ihres Profils zuweisen, indem Sie auf das "+" klicken und die App auf der Registerkarte "AE Play Store" auswählen. Dadurch wird die App automatisch heruntergeladen und installiert. Es ist kein Google-Konto auf dem Gerät erforderlich und der Benutzer muss dies nicht bestätigen oder zulassen.

Laden Sie Ihre eigenen Apps in den Google Play Store hoch

Es ist möglich, Ihre Inhouse Apps in den Google Play Store hochzuladen. Auf diese Weise können Sie von verschiedenen Vorteilen wie dem Update-Mechanismus des Play Store profitieren.

Dazu benötigen Sie ein Google-Entwicklerkonto. Melden Sie sich über die Google Play Console an(https://play.google.com/apps/publish)

Klicken Sie auf "Anwendung erstellen". Wählen Sie Ihre Standardsprache und den Titel der App.

Create application

Default language *

English (United Kingdom) – en-GB ▾

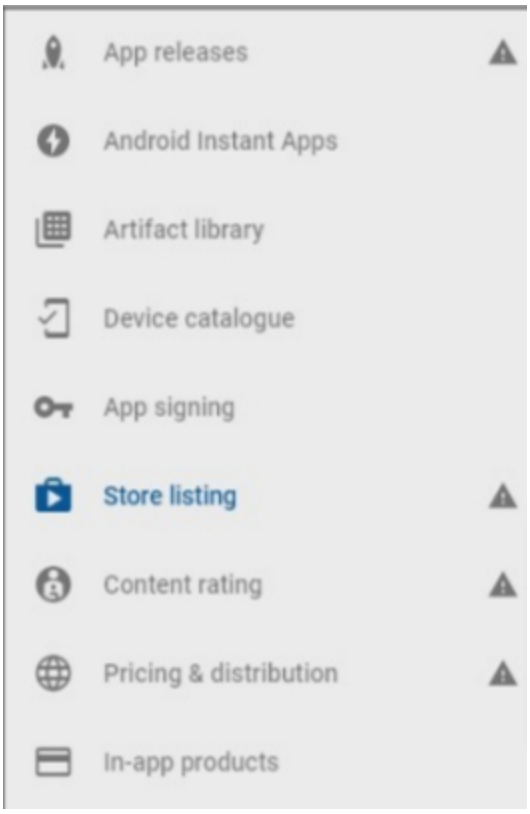
Title *

AppTec Demo App

15/50

CANCEL CREATE

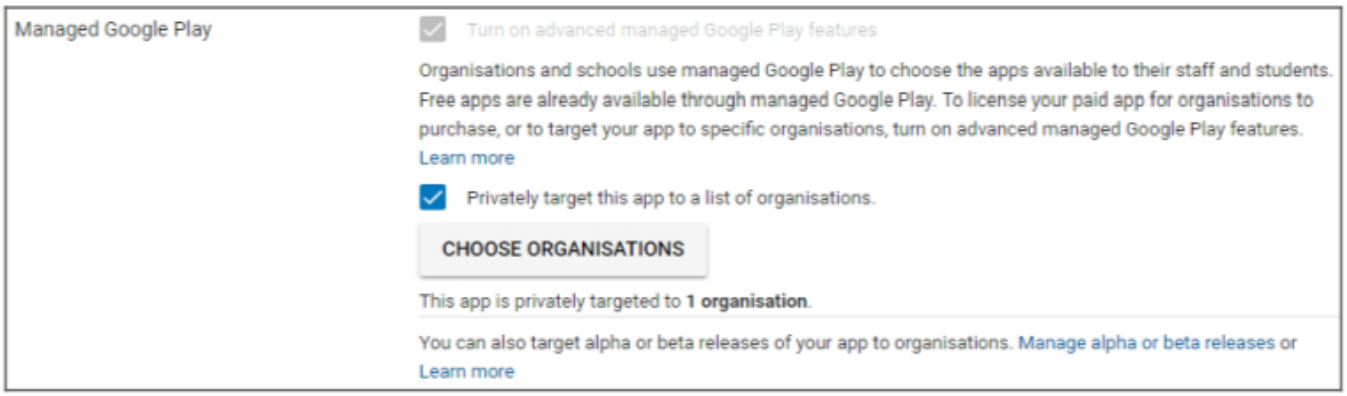
Auf der folgenden Seite werden Sie aufgefordert, verschiedene Details zu Ihrer App einzugeben.



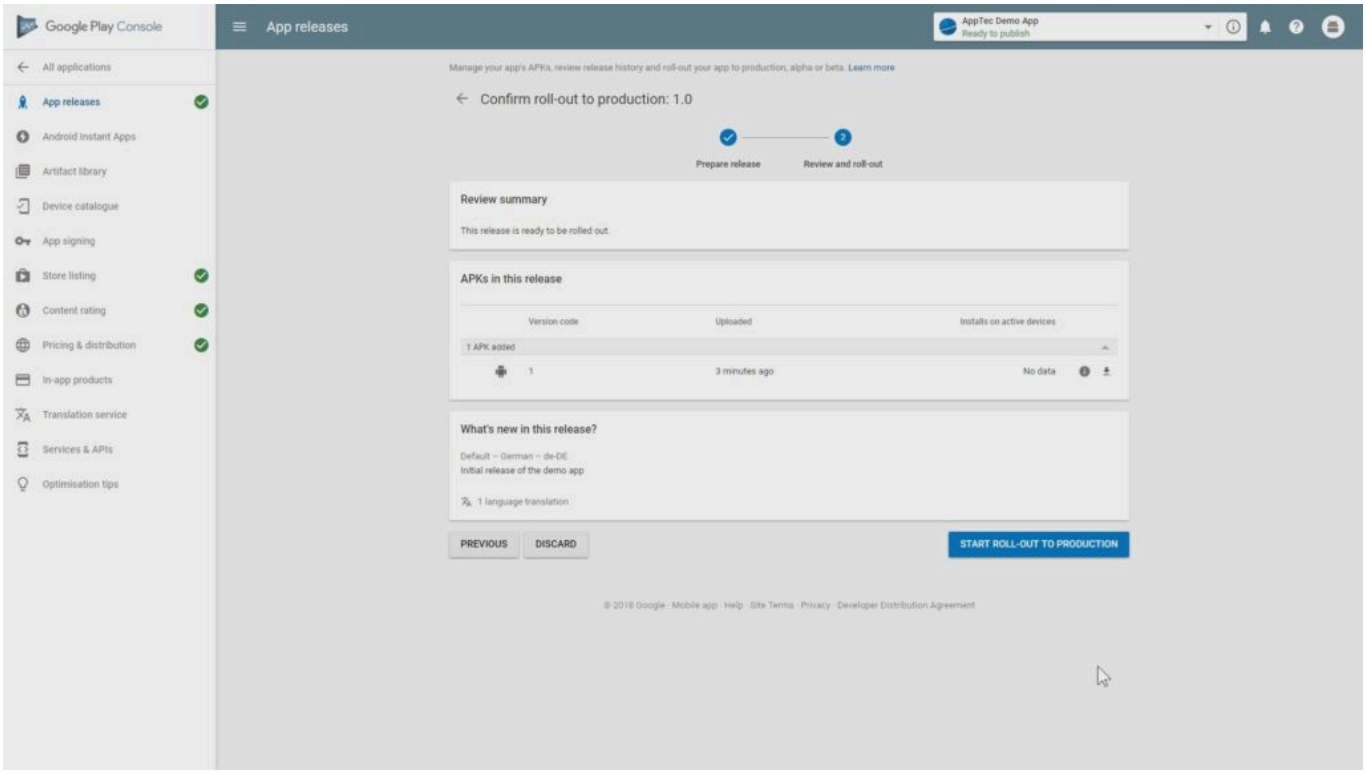
Nachdem Sie alle Details eingegeben haben, werden auf der linken Seite verschiedene Hinweis-Symbole angezeigt.

Fahren Sie mit dem Mauszeiger darüber, um zu sehen, welche Schritte noch übrig sind, und folgen Sie diesen in beliebiger Reihenfolge.

Hinweis: Vergewissern Sie sich, dass Sie die beiden Kontrollkästchen bei "Managed Google Play" unter "Preisgestaltung & Vertrieb" aktiviert haben. Andernfalls ist die App öffentlich und kann von jedem eingesehen werden. Achten Sie auch darauf, das Land für die Verteilung zu wählen.



Nachdem Sie alle Schritte abgeschlossen haben, können Sie zu "App-Veröffentlichungen" gehen. Klicken Sie auf "Review" und "Start Roll-Out to Production", um Ihren Entwurf fertig zu stellen und die App zu veröffentlichen.



Es kann einige Zeit dauern, bis die App im Play Store verfügbar ist. Nachdem der Prozess abgeschlossen ist, können Sie Ihre App im Play for Work-Store suchen und sie genehmigen. Danach können Sie die App einfach über die EMM-Konsole den Geräten zuweisen, so wie Sie es bei anderen Apps auch tun.

Anforderungen und Installation

Anforderungen

Systemanforderungen

Die virtuelle Appliance ist im Open Virtualization Format (VMWare, VirtualBox, Citrix Xen Server) und als komprimierte .vhdx (Hyper-V) Datei* verfügbar.

*Hinweis: Bei Verwendung von Hyper-V muss die Maschine mit Generation 1 erstellt werden.

Die virtuelle Festplatte hat eine Zielgröße von 20 GB und die Maschine benötigt 4 GB RAM.

Die Appliance basiert auf Debian 9 64bit

Aktualisieren Sie die importierte Maschine auf die neueste Kompatibilität (z.B. in VMWare) und stellen Sie sicher, dass der Betriebssystemtyp der Maschine in Ihrem Hypervisor korrekt eingestellt ist.

Lizenzschlüssel

Um den Server erfolgreich aktivieren und installieren zu können, benötigen Sie eine gültige Lizenzdatei. Diese können Sie direkt bei AppTec360 und/oder bei Ihrem jeweiligen Händler erhalten.

IP-Adresse und DNS-Auflösung

Die AppTec360 Appliance muss von dem Gerät unter dem Hostnamen, für den die Lizenz ausgestellt wurde, erreichbar sein.

Um Windows 10-Geräte zu registrieren, müssen Sie außerdem eine zusätzliche Subdomäne in Form von "enterpriseenrollment." einrichten, die auf die Appliance verweist.

SSL-Zertifikat

Da alle Verbindungen zu und von den Geräten mit SSL gesichert werden müssen, benötigen Sie ein gültiges Zertifikat für den Hostnamen, das von einer Zertifizierungsstelle ausgestellt wurde, der das Gerät vertraut. Der private Schlüssel für das Zertifikat muss ohne Passwortschutz hochgeladen werden. In den meisten Fällen ist ein Zwischenzertifikat für die CA erforderlich, damit die Geräte das Serverzertifikat erkennen.

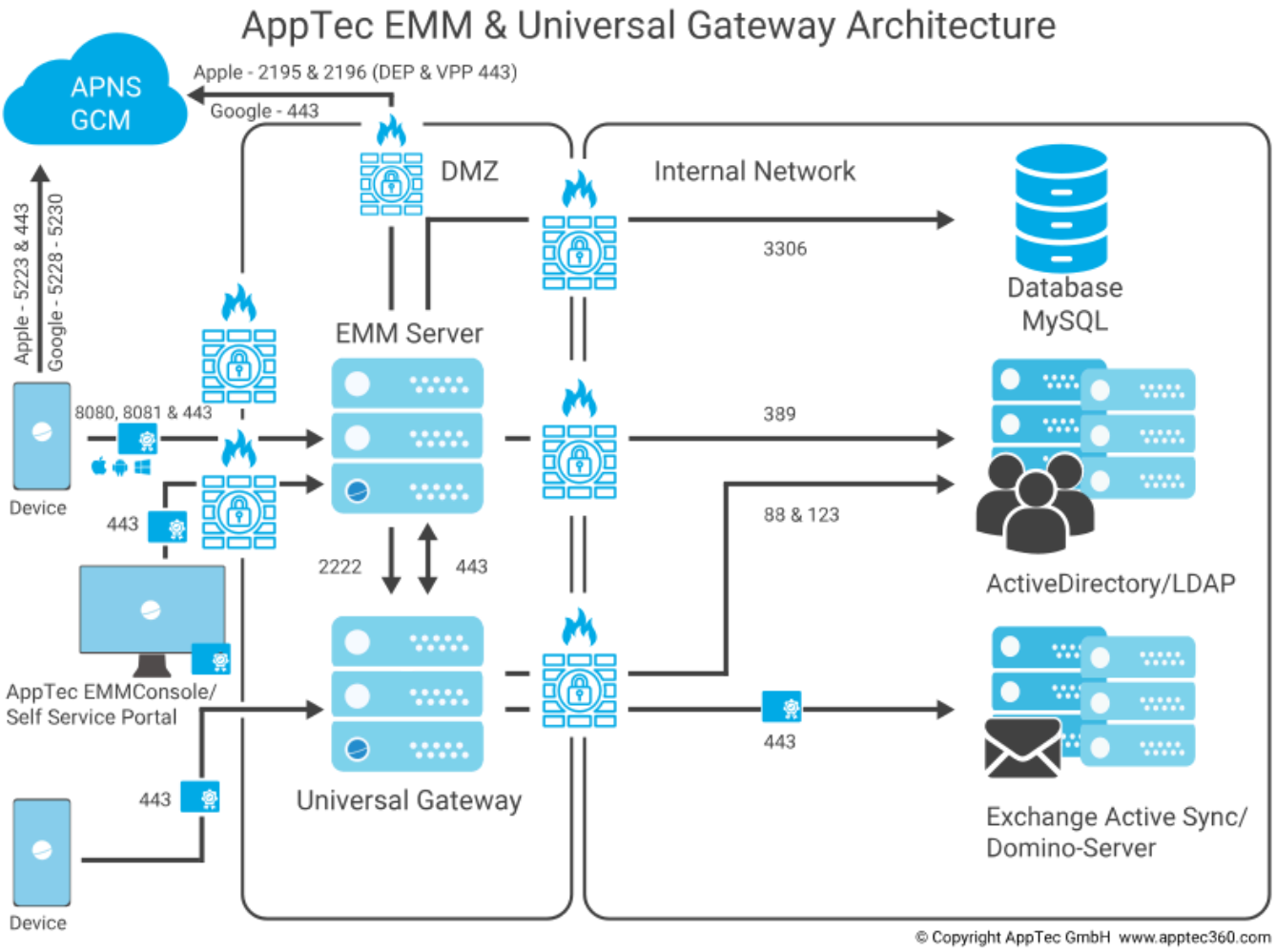
Windows 10-Geräte benötigen ein spezielles Zertifikat für Ihre Subdomäne für die Unternehmensregistrierung.

Ab der Appliance-Version 202104 können Sie auch Let's Encrypt-Zertifikate verwenden, die automatisch generiert werden (beschrieben in Schritt Zwei - SSL-Zertifikat).

SMTP-Server

Ein E-Mail-Server und/oder ein E-Mail-Relay ist erforderlich, damit der AppTec360 EMM E-Mails versenden kann (z.B. für die Geräteregistrierung und Kontoprüfung).

Firewall-Regeln



Dieses Diagramm zeigt, welche Verbindung benötigt wird, je nachdem, welche Dienste Sie nutzen möchten.

Eine genauere Beschreibung finden Sie in der Tabelle auf der nächsten Seite.

Beliebig (extern/Geräte)	→	**AppTec360 Appliance / emmconsole.com**
Häfen	443	Verwaltung, Enterprise AppStore & Windows Phone Kommunikation
	8080	Android & iOS Kommunikation
	80	Erstmalige Einrichtung von Let's Encrypt. Verwendet danach 443.
Beliebig (Geräte)	→	**Beliebig (extern)**
Häfen	5223, 443	Apple Push Service, muss ohne Proxy erreichbar sein, 443 als Fallback, siehe https://support.apple.com/en-us/HT203609
	5228-5230	Android Push Service (FCM), muss ohne Proxy erreichbar sein
AppTec360 Appliance	→	**Domänencontroller**
Häfen	389, (LDAPS 636)	Benutzer-Synchronisierung mit LDAP
AppTec360 Appliance	→	**Jede**
Hafen	443	Wird für den Android-Push-Dienst (GCM) verwendet. AppStore / Play Store Suche
AppTec360 Appliance	→	**emmconsole.com**
Häfen	443	AppTec360 Appliance Updates, APNS-Zertifikatserstellung
AppTec360 Appliance	→	**Apple Netzwerk (17.0.0.0/8)**
Häfen	2195, 2196	Apple Push-Dienst & Feedback-Dienst
	443	DEP & VPP

Sicherheits-Updates

Das Debian-Betriebssystem sollte regelmäßig aktualisiert werden, um die neuesten Sicherheitskorrekturen zu erhalten. Stellen Sie jedoch sicher, dass Sie nicht manuell auf eine neuere Hauptversion von Debian aktualisieren. Wenn AppTec360 EMM mit einer neueren Hauptversion kompatibel ist, werden wir in einem Appliance-Update eine Möglichkeit zum Upgrade hinzufügen.

Standardkennwörter der virtuellen Appliance

Login User (Root-Login ist deaktiviert. Verwenden Sie "sudo" für Administrationsaufgaben)

apptec

Login-Passwort

apptec

MySQL Root-Benutzer

Wurzel

MySQL Root-Passwort

apptec

MySQL-Standardbenutzer

AppTec

MySQL Standard-Benutzerpasswort

AppTec

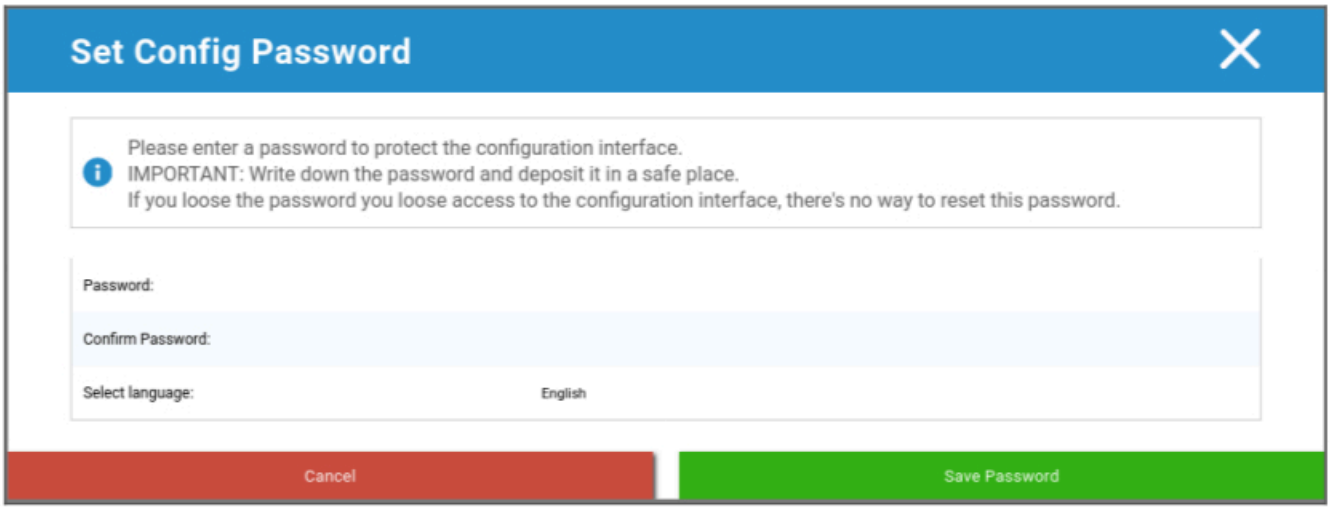
Konfiguration der virtuellen Appliance

Wichtig: Bevor Sie mit der Konfiguration der Virtual Appliance beginnen, sollte die Bildschirmauflösung auf mindestens 1280 x 800 Pixel eingestellt sein.

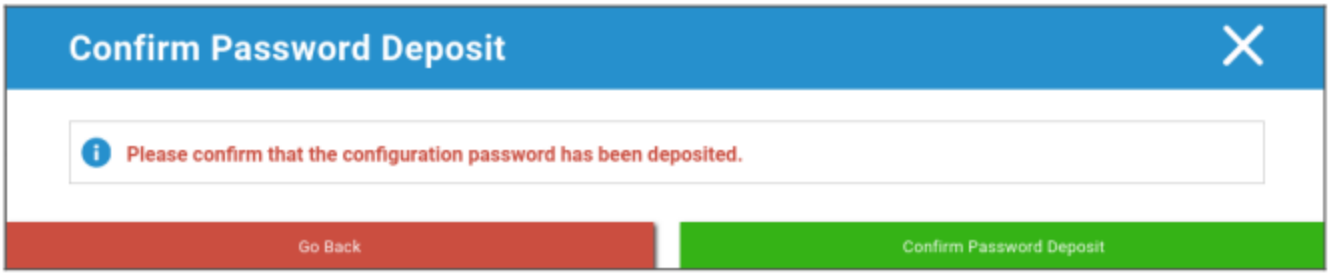
Nachdem Sie sich in die Appliance eingeloggt haben, sollte Firefox automatisch gestartet werden und die Konfigurationsoberfläche anzeigen.

Vorbereitung

Zunächst müssen Sie ein Passwort für die Konfigurationsschnittstelle angeben. Dieses Passwort wird verwendet, um alle Informationen und Dateien zu verschlüsseln, die in die Konfigurationsoberfläche eingegeben werden. Hier können Sie auch die Sprache einstellen, in der die Oberfläche angezeigt werden soll (kann später geändert werden).

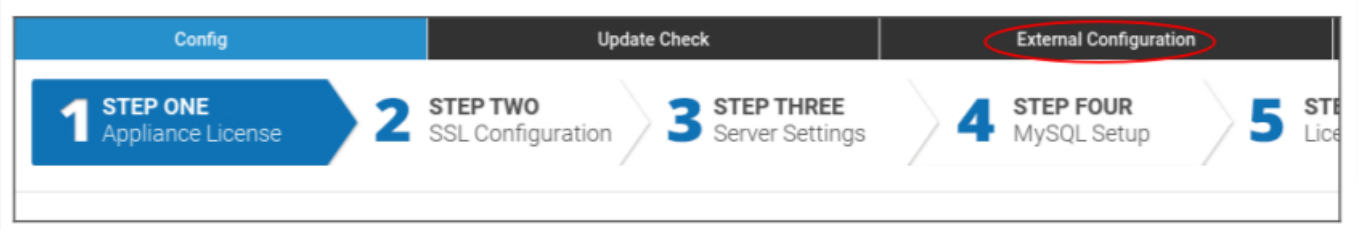


Das Passwort kann nur vom AppTec360-Support zurückgesetzt werden. Stellen Sie also sicher, dass Sie es an einem sicheren Ort hinterlegen und das kommende Popup bestätigen.



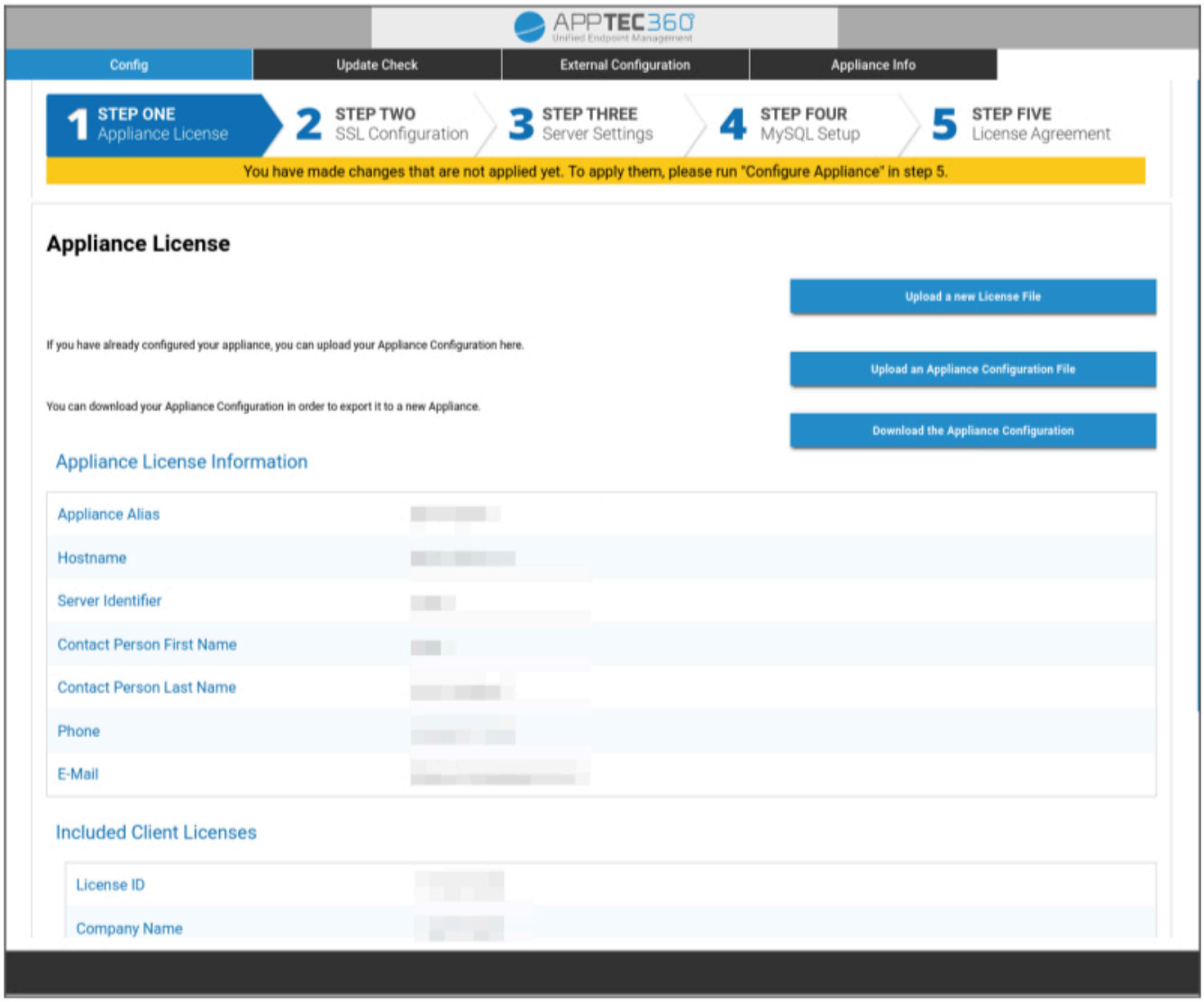
Von externem Host aus konfigurieren

Um den Einrichtungsprozess zu vereinfachen, können Sie die Konfigurationsseite aus der Ferne zugänglich machen. Folgen Sie dazu den Schritten unter "Von externem Host aus konfigurieren".



Schritt Eins – Appliance-Lizenz

1. Bitte laden Sie die Lizenzdatei hoch, die Sie von AppTec erhalten haben.
2. Wenn die Lizenzdatei erfolgreich hochgeladen wurde, sehen Sie die Lizenzinformationen der Appliance wie im folgenden Screenshot.



Schritt Zwei – SSL-Zertifikat

Sie können entweder die automatische Zertifikatseinrichtung mit Let's Encrypt verwenden oder die Zertifikate selbst bereitstellen (siehe SSL-Zertifikat für weitere Informationen).

Automatisch

Das Zertifikat wird automatisch mit Hilfe des Let's Encrypt-Dienstes erstellt.

Der AppTec360 EMM verwendet die HTTP-01-Challenge zur Validierung der Domäne, was bedeutet, dass der HTTP-Port für die erste Anforderung eines Zertifikats aus dem Internet geöffnet sein muss. Spätere Verlängerungsanfragen können über HTTPS validiert werden.

Schalten Sie die Optionsfelder auf "Automatisch (Let's Encrypt)" um und drücken Sie auf "WERT SICHERN". Das Zertifikat wird automatisch angefordert, wenn Sie die Konfiguration in Schritt Fünf - Lizenzvereinbarung anwenden. Das Zertifikat wird bei Bedarf automatisch erneuert und Sie erhalten eine E-Mail, wenn das Zertifikat bald abläuft (was bedeutet, dass die Erneuerung möglicherweise fehlgeschlagen ist).

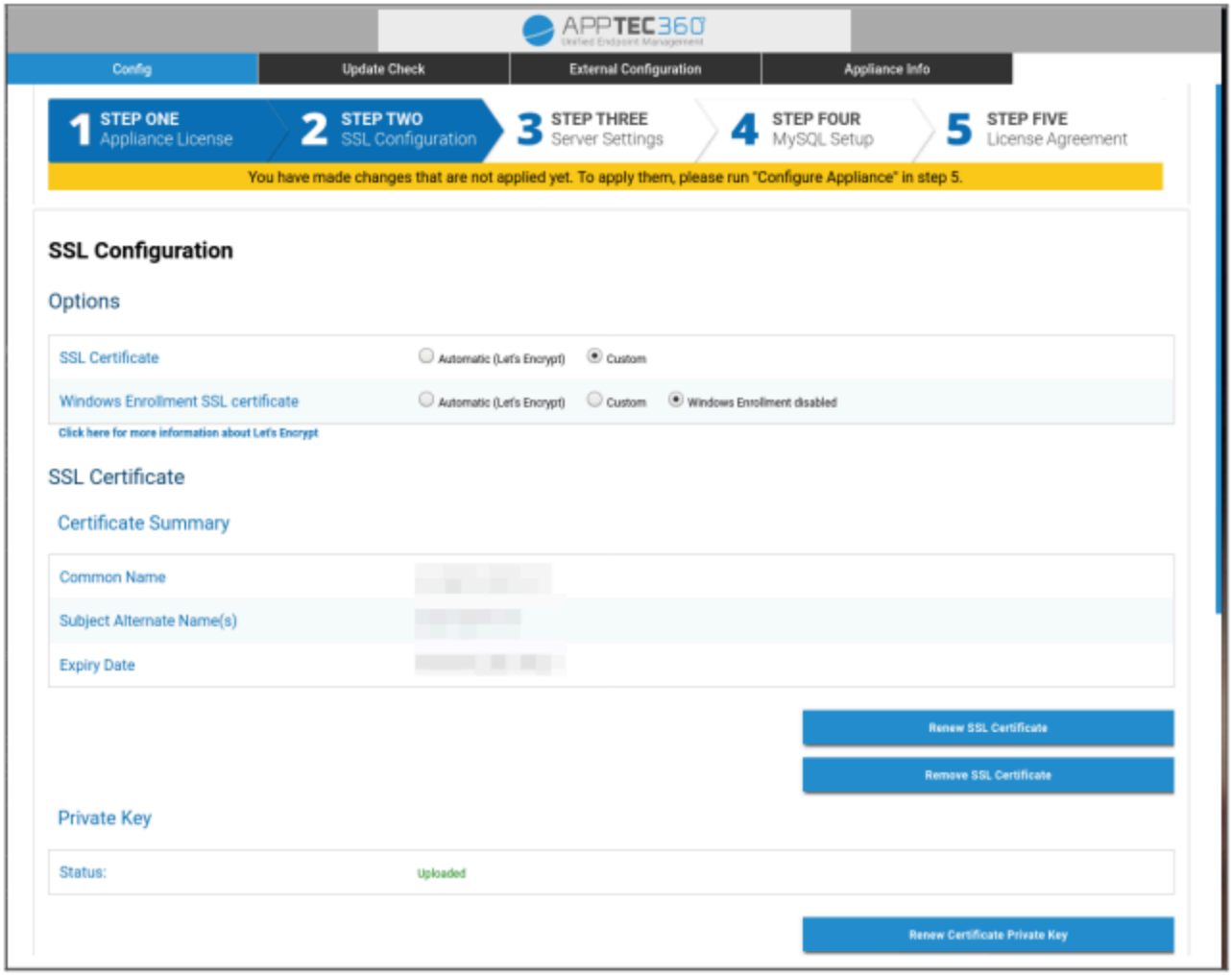
Benutzerdefiniert

1. Laden Sie das SSL-Zertifikat für Ihren lizenzierten Hostnamen hoch. Sie können den Hostnamen in Schritt Eins - Appliance-Lizenz sehen.

2. Bitte laden Sie auch den privaten Schlüssel für das Zertifikat und ggf. das Zwischenzertifikat hoch.

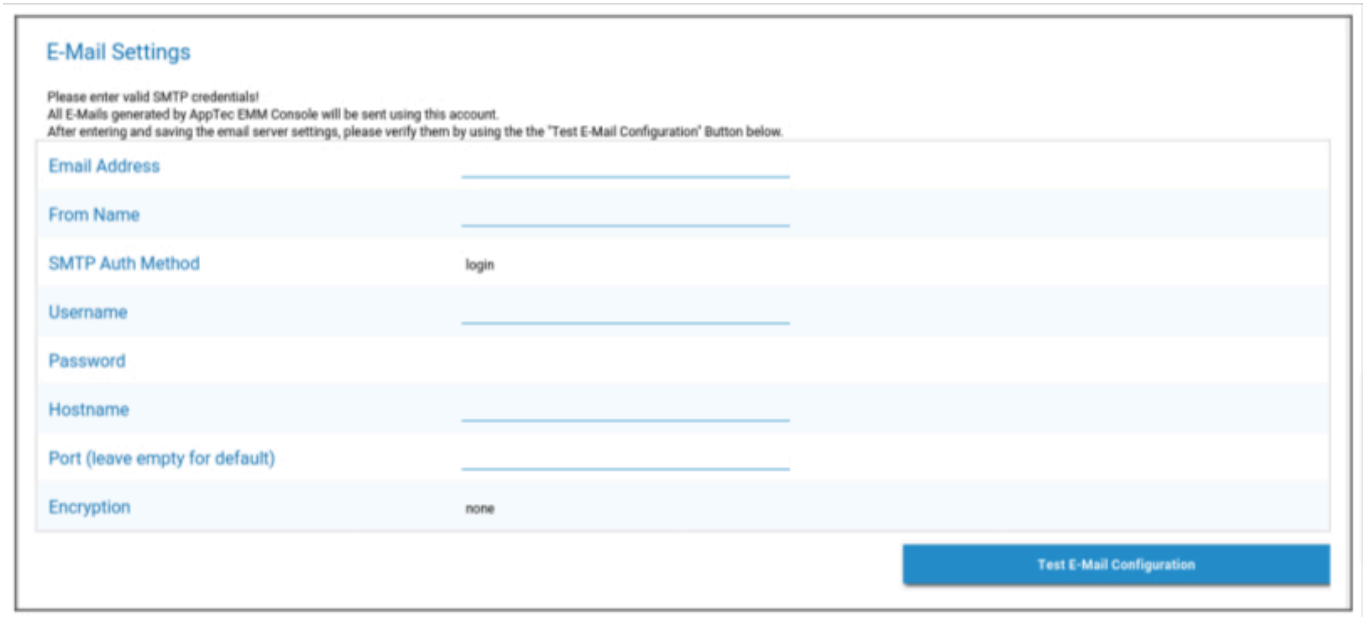
Wichtig: Der Schlüssel darf nicht passwortgeschützt sein. Wenn dies der Fall ist, entfernen Sie bitte das Passwort, bevor Sie es hochladen.

Tipp: Wenn Sie auch Windows 10-Geräte verwenden möchten, müssen Sie "Windows Enrollment SSL-Zertifikat" aktivieren und das Zertifikat, den privaten Schlüssel und das Zwischenzertifikat für Ihre Subdomain hochladen (wie unter IP-Adresse und DNS-Auflösung beschrieben) unten auf der Seite hochladen.



Schritt Drei – Servereinstellungen

1. Bitte geben Sie eine globale Support-E-Mail-Adresse ein. Diese Adresse wird in E-Mails an Ihre Benutzer verwendet, damit diese wissen, an wen sie sich bei Problemen mit ihrem Gerät wenden können.
2. Geben Sie die E-Mail-Einstellungen an, die das System für den Versand von E-Mails verwenden soll. Die Einstellungen werden verwendet, um E-Mails an den Benutzer zu senden und auch um Fehlerberichte und Feature Requests an"support@apptec360.com"zu senden. Nachdem Sie Ihre E-Mail-Einstellungen gespeichert haben, müssen Sie sie überprüfen, indem Sie auf "E-Mail-Konfiguration testen" klicken und den Anweisungen folgen.



Schritt Vier – MySQL-Einrichtung

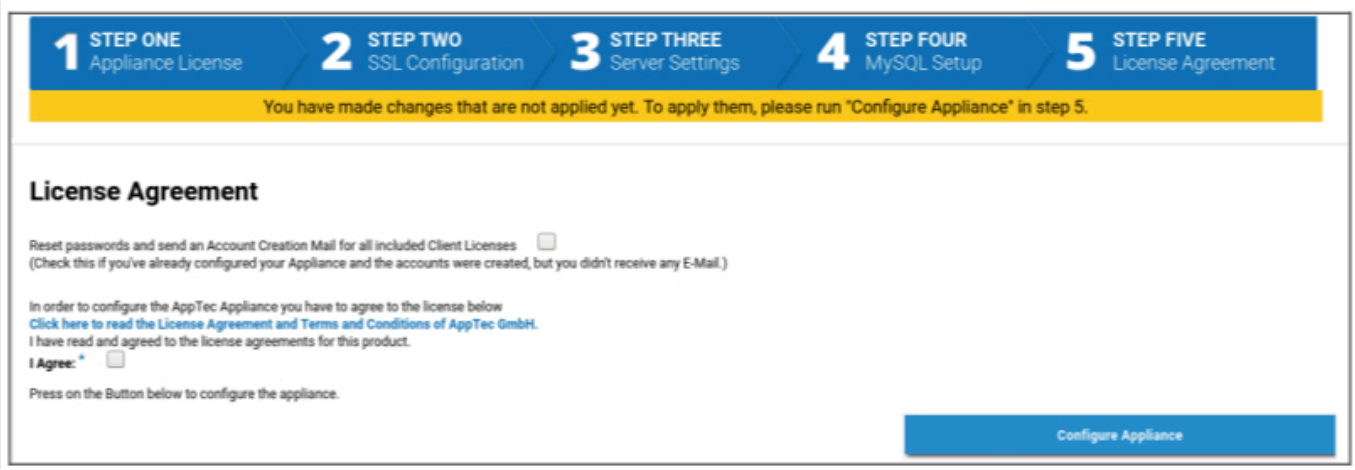
1. Wenn Sie die interne Datenbank verwenden möchten, können Sie diesen Schritt überspringen. Andernfalls können Sie die Verbindungsinformationen für Ihren externen Datenbankserver eingeben.


1 STEP ONE Appliance License
2 STEP TWO SSL Configuration
3 STEP THREE Server Settings
4 STEP FOUR MySQL Setup
5 STEP FIVE License Agreement
You have made changes that are not applied yet. To apply them, please run "Configure Appliance" in step 5.
MySQL Setup
The MySQL connection has been successfully tested at April 7, 2021, 8:45 am.
If you change the settings after the initial configuration, you have to reconfigure your appliance by clicking on "Configure now" in step 5.
IP Address or Hostname
127.0.0.1
(Default: 127.0.0.1)
Username
AppTec
(Default: AppTec)
Password
(Default: AppTec)
Port
3306
(Default: 3306)

Schritt Fünf – Lizenzvertrag

1. Bitte lesen Sie die Lizenzvereinbarung.
2. Markieren Sie "Ich stimme zu" und klicken Sie auf die Schaltfläche "Appliance konfigurieren", um die Einstellungen zu übernehmen.

Hinweis: Sie müssen jedes Mal, wenn Sie die Einstellungen in den 5 Schritten ändern, "Appliance konfigurieren" ausführen, um die Einstellungen zu übernehmen.



Herzlichen Glückwunsch!

Sie haben die Konfiguration der virtuellen Appliance abgeschlossen.

Eine E-Mail mit Ihrem Passwort wurde an die Adresse gesendet, die Sie für die Lizenz angegeben haben (sichtbar unter "Enthaltene Client-Lizenzen" in Schritt Eins - Appliance-Lizenz).

Sie können sich nun mit diesem Passwort und der E-Mail-Adresse, mit der Sie es erhalten haben, bei der Konsole anmelden.

Um sich bei der Konsole anzumelden, geben Sie bitte den Hostnamen der Konsole in die Adresszeile Ihres Browsers ein.

Sie finden den Hostnamen Ihrer Appliance in Schritt Eins - Appliance-Lizenz.

Fehlersuche

1. Sie haben bei der Konfiguration der Appliance in Schritt Fünf - Lizenzvereinbarung keine E-Mail erhalten:

Stellen Sie sicher, dass Ihre E-Mail-Einstellungen in Schritt Drei - Servereinstellungen korrekt sind. Um das Passwort erneut zu senden, aktivieren Sie "Passwörter zurücksetzen und eine E-Mail zur Kontoerstellung für alle enthaltenen Client-Lizenzen senden" in Schritt Fünf - Lizenzvereinbarung, bevor Sie "Appliance konfigurieren" erneut ausführen.

2. Sie haben während der Konfiguration in Schritt Fünf - Lizenzvereinbarung einen Fehler in Bezug auf Let's Encrypt erhalten:

Stellen Sie sicher, dass die Appliance über ihren Domänennamen auf Port 80 erreichbar ist. Let's encrypt schreibt auch ein Protokoll nach "/var/log/letsencrypt", das bei der weiteren Fehlersuche helfen kann.

Sicherheitsempfehlungen

Es wird empfohlen, die folgenden Schritte durchzuführen, um Ihre AppTec360 Appliance zu sichern.

Dies ist keine vollständige Anleitung, sondern nur eine Empfehlung für eine Grundkonfiguration.

- Ändern Sie das Passwort für den AppTec360-Benutzer
- Ändern Sie das Passwort für die MySQL-Benutzer "root" und "AppTec" und aktualisieren Sie Schritt Vier - MySQL-Einrichtung entsprechend
- Ändern Sie den Standard-Port des SSH-Servers
- Blockieren Sie Port 80 in Ihrer Konsole und lassen Sie eingehenden HTTP-Verkehr nicht zu, verwenden Sie nur HTTPS. Einmal konfiguriert, ist auch eine externe Konfiguration über HTTPS möglich.
- Schränken Sie den Zugriff auf die Verwaltungsoberfläche nur auf bestimmte Benutzer ein, und zwar am Ende von Schritt Drei - Servereinstellungen
- Konfigurieren Sie die Firewall

Allgemeine Einstellungen

Konto Übersicht

Konto-Informationen

Übersicht

Hier sehen Sie eine Übersicht über Ihr AppTec360-Konto.

Name des Unternehmens	Ihr Firmenname
Erstellungsdatum	Erstellungsdatum Ihres Kontos
Lizenz-Typ	Bezahlt = bezahlte Lizenz Kostenlos = unbezahlte Lizenz Hinweis: Konten auf einer OnPremise Appliance werden aus technischen Gründen immer als bezahlt angezeigt.
Kennung des Kunden	Kennung Ihres Kontos (Dies ist NICHT Ihre Kundennummer)
Ablaufdatum der Lizenz	Ablaufdatum Ihrer AppTec360 Lizenz
ContentBox-Lizenz	Kostenlos = kostenlose Lizenz für 25 Geräte Bezahlt = bezahlte Lizenz für x Geräte
Barkasse	Zeigt an, ob Sie den benutzerdefinierten Launcher für Android verwenden können oder nicht
Geräte	Anzahl der derzeit verwendeten / Gesamtlizenzen
Kontaktperson	Bereitgestellte Kontaktperson
Telefon	Angegebene Telefonnummer
eMail*	Angegebene E-Mail Adresse
Root-Benutzer	Root-Benutzer, die sich anmelden können
Software Version	Aktuelle Software Version

**Hinweis: Die hier angezeigte E-Mail-Adresse ist die, die Sie bei der Registrierung des Kontos angegeben haben. Auf dieser Grundlage wird ein Benutzer in der Benutzer/Geräte-Struktur erstellt und kann geändert werden. Durch die Bearbeitung dieses Benutzers wird die E-Mail-Adresse geändert, mit der Sie sich anmelden müssen, nicht aber die Informationen in der Kontoübersicht..*

Fehlerbericht

Ein Fehlerbericht kann direkt an den Support gesendet werden, um Probleme oder Fehler zu melden und enthält Informationen und Protokolle über Ihr Konto und Ihre Einrichtung.

Thema	Der Gegenstand des Fehlerberichts. Geben Sie eine Ticketnummer an, wenn Sie dies zu einem bestehenden Support-Ticket hinzufügen möchten.
Erwartetes Verhalten	Beschreiben Sie im Detail, was Sie getan haben und was Sie erwartet haben
Tatsächliches Verhalten	Beschreiben Sie im Detail, was genau passiert ist. Bitte zitieren Sie Fehlermeldungen EXAKT. Es hilft auch, wenn Sie dem Anhang Screenshots beifügen.
Zu welchem Zeitpunkt trat das Problem auf?	Bitte geben Sie den genauen Zeitpunkt an, zu dem Sie eine bestimmte Fehlermeldung/ein bestimmtes Problem erhalten haben. Im besten Fall geben Sie auch Sekunden an, z.B. 18:55:27
Kann das Problem reproduziert werden? Wenn ja, wie (im Detail)?	Beschreiben Sie, wie Sie das Problem im Detail reproduzieren können.
Hat diese Funktion bisher so funktioniert, wie Sie es erwartet haben? Wenn ja, bis wann?	Lassen Sie leer, wenn Sie es nicht wissen.
Wurden bestimmte Änderungen am System vorgenommen, bevor dieses Problem auftrat? Wenn ja, welche Änderungen (im Detail)?	Erwähnen Sie immer, was Ihre letzte Änderung oder Aktion vor dem Auftauchen des Problems war, auch wenn Sie denken, dass es irrelevant ist.
Falls zutreffend: Welche Gerätemodelle und Betriebssystemversionen sind betroffen?	Bitte geben Sie immer die genaue OS-Version an (z.B. iOS 14.7.1 oder Android 11)
Falls zutreffend: Wie lautet die öffentliche IP-Adresse oder/und die Seriennummer des Geräts?	Nennen Sie mindestens eines, auch wenn alle Geräte betroffen sind.
Logdateien einbeziehen	Aktivieren Sie diese Option, um die Protokolldatei mit dem Fehlerbericht zu senden. Es wird empfohlen, dies zu tun.
Aktuellen VPP-Status von Apple abrufen und in den Bugreport aufnehmen	Enthält Informationen über VPP-Lizenzzuweisungen. Aktivieren Sie dies nur, wenn Sie vom Support dazu aufgefordert werden oder wenn Ihr Problem mit VPP zu tun hat.

Anhang	Fügen Sie jede Datei an, die nützlich sein könnte (z.B. Screenshots einer Fehlermeldung)

Feature Anfrage

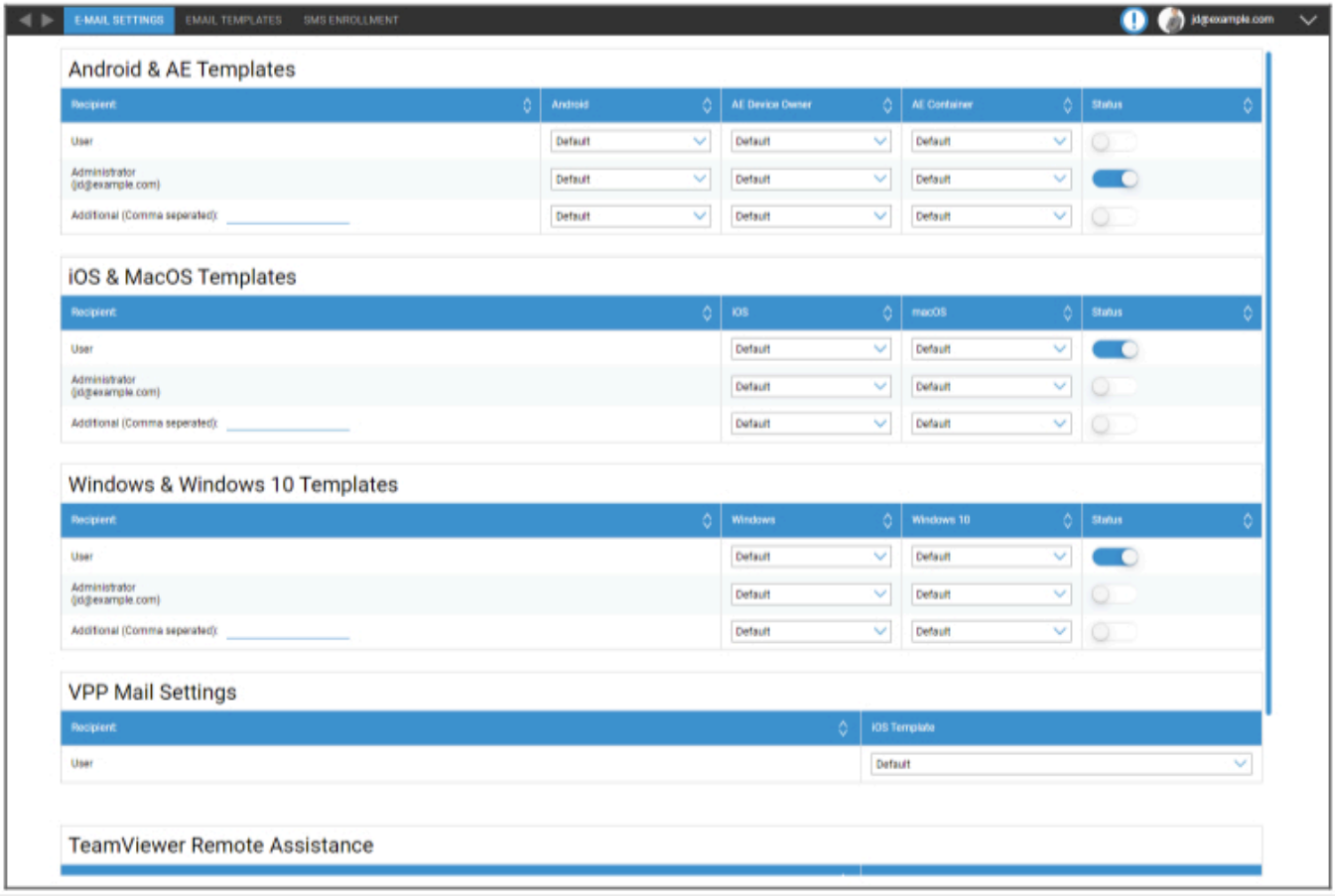
Sie können eine Funktionsanfrage direkt an den Support senden. Dies kann eine Anfrage für eine bestimmte Funktion oder eine Verbesserung für

Zusammenfassung	Eine kurze Zusammenfassung Ihres Problems
Beschreibung	Eine detaillierte Beschreibung Ihres Problems, bitte so genau wie möglich
Anhang	Dateien an den Fehlerbericht anhängen

Globale Konfiguration

eMail-Einstellungen

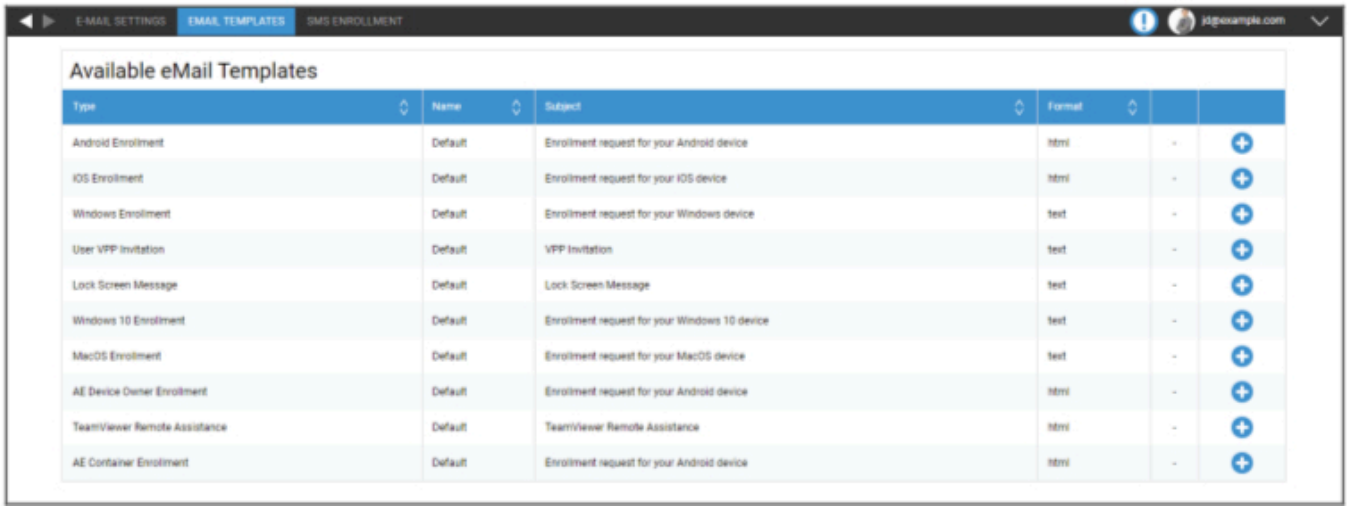
Hier können Sie festlegen, wer eine E-Mail erhält, wenn eine Registrierungsanfrage erstellt wird, und welche Textvorlage für diese E-Mail verwendet wird.



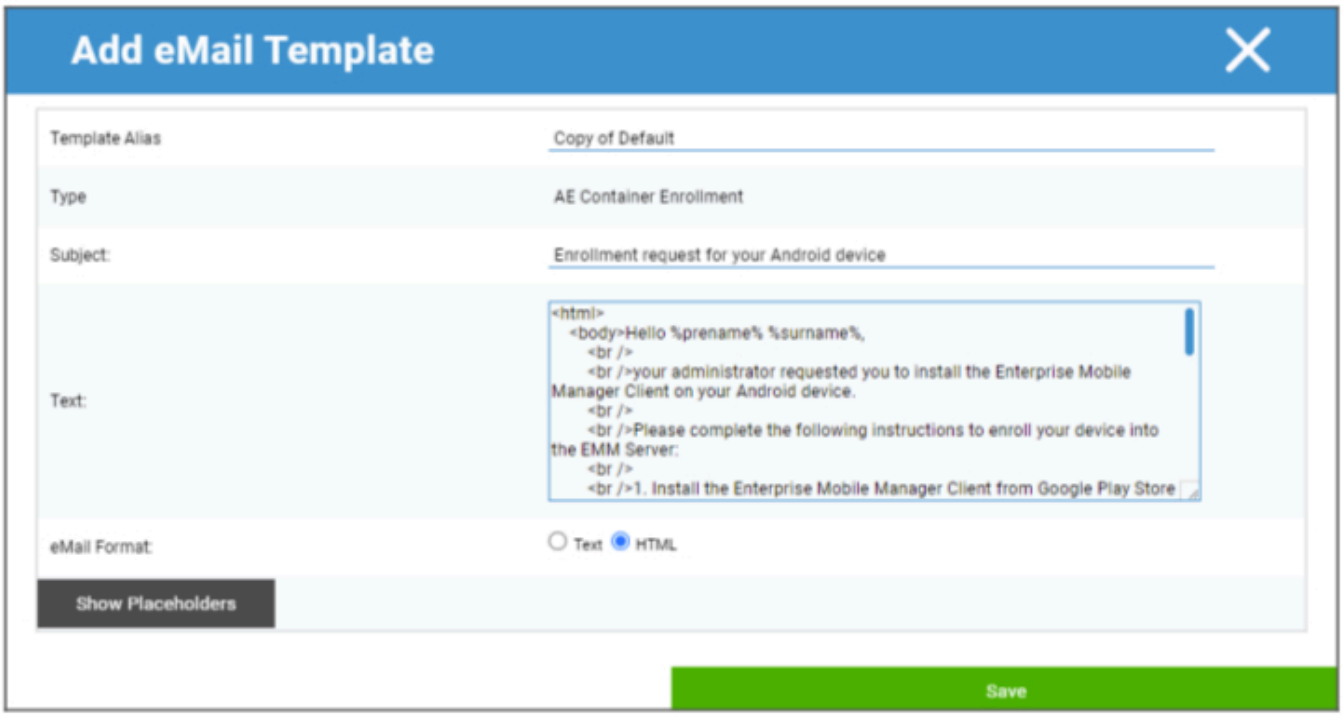
eMail-Vorlagen

Hier können Sie Ihre Vorlagen für verschiedene Szenarien erstellen und bearbeiten. Diese können in normaler Textform oder in HTML sein. Mit HTML können Sie die Formatierung Ihres Textes besser kontrollieren.

Die Standardvorlagen können nicht bearbeitet oder gelöscht werden.



Sie können auch Platzhalter als Variable verwenden, die automatisch ersetzt werden. Klicken Sie während der Bearbeitung auf "Platzhalter anzeigen", um die verfügbaren Platzhalter zu sehen. Verschiedene Kategorien haben unterschiedliche Platzhalter.



SMS-Registrierung

Hier können Sie den SMS-Anmeldeprozess aktivieren.

(Standard: deaktiviert)

Sie sehen auch eine Anzeige, wie viele SMS-Credits noch verfügbar sind.

SMS-Credits müssen gesondert erworben werden.

Datenschutz

GPS Zugang

Hier können Sie die GPS-Ansicht für jedes Gerät mit 1 oder 2 Passwörtern schützen (Vier-Augen-Prinzip). Jedes Mal, wenn Sie versuchen, auf den Standort eines Geräts zuzugreifen, werden Sie aufgefordert, Ihr(e) Passwort(e) einzugeben.

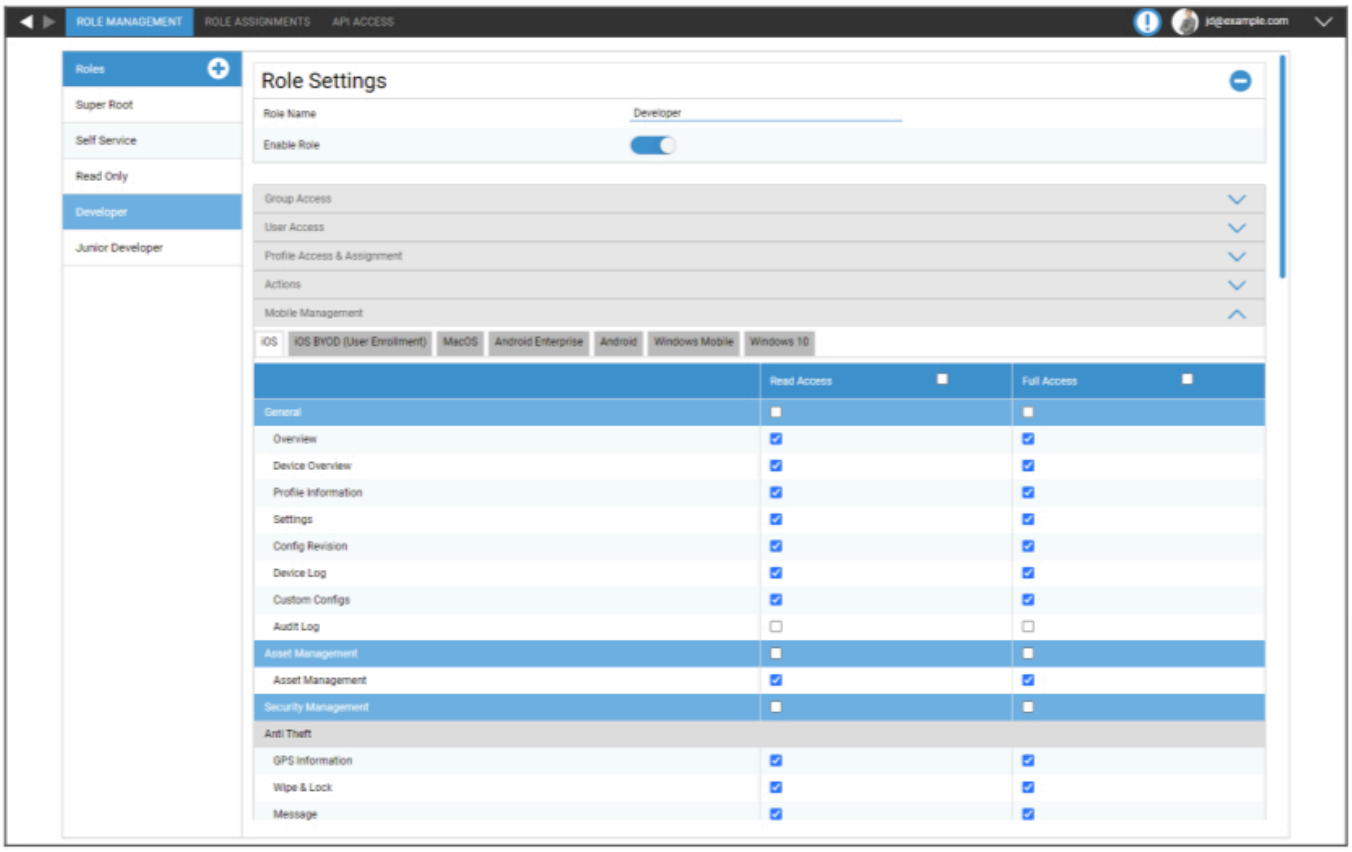
Zugriff auf GPS-Einstellungen einschränken	Aus = Die Funktion ist ausgeschaltet und es ist kein Passwort für die Lokalisierung erforderlich.
	Ein = Funktion ist eingeschaltet und ein Passwort ist für die Lokalisierung erforderlich
Schutz Methode	Ein Passwort verwenden = ein Passwort für die Lokalisierung verwenden
	Zwei Passwörter verwenden = zwei Passwörter für die Lokalisierung verwenden
Passwort eingeben (1)	Gewähltes Passwort eingeben
Passwort wiederholen (1)	Gewähltes Passwort erneut eingeben
optional: Passwort eingeben 2	2. gewähltes Passwort eingeben
optional: Wiederholen Sie Passwort 2	Geben Sie das 2. gewählte Passwort erneut ein

Hinweis: Nachdem Sie den/die Passcode(s) eingestellt haben, müssen Sie ihn noch einmal eingeben, bevor er vollständig aktiviert wird.

Rollenbasierter Zugriff

Rollenmanagement

Die Rollen definieren, was ein Benutzer sehen und tun kann, wenn er sich bei der Verwaltungskonsole anmeldet. Damit können Sie Benutzer anlegen, die sich zwar anmelden können, aber nur über eingeschränkte Funktionen verfügen.



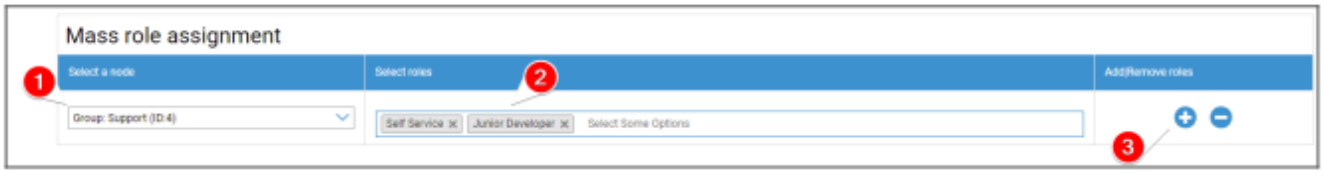
Die Super Root-Rolle ist eine Standardrolle, die immer alles sehen und ändern kann. Sie kann nicht geändert oder gelöscht werden. Die Self-Service-Rolle kann nur ihre eigenen Benutzer und Geräte sehen. Sie können Self Service und eine benutzerdefinierte Rolle kombinieren, um z.B. Benutzern die Möglichkeit zu geben, sich anzumelden und Geräte allein und nur für ihren Benutzer zu registrieren.

Benutzerdefinierte Rollen können manuell aktiviert oder deaktiviert werden. Neue Rollen sind standardmäßig deaktiviert. Benutzer mit einer deaktivierten Rolle arbeiten so, als ob sie die Rolle nicht hätten. So können Sie z.B. die Aktionen einer bestimmten Rolle vorübergehend einschränken.

Alle Berechtigungen sind zwischen "Lesezugriff" und "Vollzugriff" unterteilt. Wenn Sie einer Rolle Lesezugriff gewähren, kann sie einen bestimmten Teil der Konsole sehen. Wenn Sie ihnen Vollzugriff gewähren, kann die Rolle den entsprechenden Teil der Konsole sehen und ändern.

Rollenzuweisungen

Hier erhalten Sie einen Überblick über alle Benutzer, die eine Rolle haben und sehen, welche Rolle sie haben. Sie können hier auch Benutzern oder ganzen Gruppen eine Rolle zuweisen:

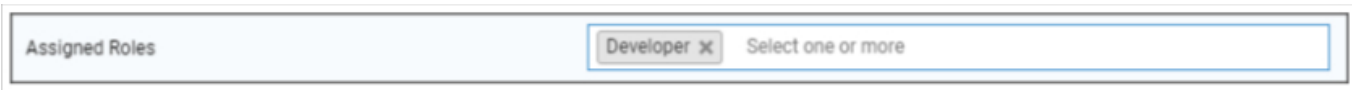


1. Wählen Sie aus, für welche Gruppe oder welchen Benutzer Sie Rollen hinzufügen oder entfernen möchten. Sie können entweder einen einzelnen Benutzer oder eine Gruppe auswählen. Wenn Sie eine Gruppe auswählen, wirkt sich Ihre Änderung auf alle Benutzer innerhalb dieser Gruppe und alle Benutzer von Untergruppen innerhalb der ausgewählten Gruppe aus.
2. Wählen Sie die Rolle, die Sie hinzufügen oder entfernen möchten. Sie können eine oder mehrere Rollen auswählen.
3. . Wählen Sie aus, welche Operation Sie durchführen möchten. Wenn Sie auf das "+" klicken, werden die ausgewählten Rollen hinzugefügt, falls der/die Benutzer sie noch nicht hatten. Wenn Sie auf das "-" klicken, werden die ausgewählten Rollen von dem/den Benutzer(n) entfernt. Wenn Sie einem Benutzer, der noch keine Rolle hatte, Rollen hinzufügen, wird automatisch "Kann sich anmelden" für den Benutzer aktiviert.
4. Speichern Sie, um den Vorgang abzuschließen. Benutzer, die bisher keine Rolle hatten und bei denen "Anmelden können" deaktiviert war, erhalten automatisch eine E-Mail mit einem Link, über den sie ein Passwort festlegen können.

Unterhalb der Massenrollenzuweisung finden Sie die Übersicht über die zugewiesenen Rollen. Sie können dort auch manuell Rollen für bestimmte Benutzer ändern.

Zuweisung einer Rolle

Um einem Benutzer eine Rolle zuzuweisen, müssen Sie zum Mobile Management gehen, wo Sie den Baum Ihrer Gruppen, Benutzer und Geräte finden. Bearbeiten Sie den Benutzer, um ihm eine Rolle zuzuweisen. Alternativ können Sie die oben beschriebene Methode auch nur für einzelne Benutzer verwenden.



API-Zugang

Zugang zur AppTec360 REST API

Die AppTec360 REST API benötigt ein Authentifizierungs-Token (API-Schlüssel) und einen privaten Schlüssel, die in der Verwaltungskonsole generiert werden müssen.

Melden Sie sich dazu in AppTec360 EMM an und gehen Sie zu

Allgemeine Einstellungen → Rollenbasierter Zugriff → API-Zugriff und fügen Sie einen neuen Schlüssel hinzu.

Sie müssen einen Benutzer auswählen, dessen Berechtigungen für den API-Schlüssel gelten sollen.

Der private Schlüssel kann nur einmal heruntergeladen werden. Nachdem der Download begonnen hat, wird der Schlüssel gelöscht, und die Schaltfläche "Download" verschwindet.

Wenn Sie Ihren privaten Schlüssel verlieren, müssen Sie einen neuen API-Schlüssel generieren.

Allgemeine Regeln

- Die REST-API ist unterhalb der Basis-URL verfügbar:

/public/external/api

- Alle Anfragen müssen per POST gesendet werden.
- Die REST-API unterstützt nur Anfragen über HTTPS.
- Die Anfragen müssen die folgenden Kopfzeilen enthalten:

Kopfzeile Name	Kopfzeile Wert	Beschreibung
Inhaltstyp	anwendung/json	fest
auth	123...xyz	API-Schlüssel auf der Registerkarte "API-Zugang".
Unterschrift	Base64 kodierte Signatur	Signatur der Nutzdaten, die mit dem privaten Schlüssel auf der Registerkarte "API-Zugang

- Der Request Body muss ein json kodiertes Objekt sein, das die folgenden Werte enthält:

Feld	Feld Beispielwert	Beschreibung
api	v2/Gerät/ListeGeräte	Name der API
Zeit	1529662725	Unix-Zeitstempel (UTC) des Client-Rechners. Die maximal zulässige Zeitdifferenz zwischen dem Client und dem Server beträgt 30 Minuten.

- Bei Erfolg gibt die API die angeforderten Daten (siehe die Abfragen unten) und einen HTTP-Statuscode 200 zurück.
- Wenn ein Fehler auftritt, ist der HTTP-Statuscode je nach Fehler zwischen 4xx und 5xx und das Antwortobjekt enthält ein Array mit dem Schlüssel "errors", das eine Liste von menschenlesbaren Fehlermeldungen enthält.
- Wenn es keine passenden Daten für ein Gerät gibt, wird ein leeres Array zurückgegeben.
- Wenn eine Geräte-ID nicht existiert, sind die Rückgabedaten Null.

Beispiel anfordern

POST /public/external/api HTTP/1.1
Host: myapptecemm.com
Accept: /
Content-Type: application/jsonauth: 1234567890abcdefghijklmnopqrstuvwxyz
signature: a/bnOV466a0SiyVfsbpspZ+NxiTpmeF18NkfnOIq+OrEZDu9+VW7ESKziPXvw
kTM5B9j/t1WGN1mRcIKe80m8fDKPj+lr3BqoMJe7wGXift+uy6iS7Chpdz2iZA4KPxxU9Z
GU2cdQ/SQceX57pi+ch7ApxBeVX2+lJapTwA6CfB0mJFaf4MPcg/
7LZWkzKxKF7LNzNJHiy/vSpZcqjbXjpC4HWrX6j2uZG5eSP8kYcTR
9VQfGtkX9pcyaNAwguR7zOOwMu/8L0oKq21/19rkabE4ZgUjtKS2+
+q+rh6mrP1g4BCZ7Xq/wvgZkaP
b0CStBdMRvj46i3enxCXcLQQ==
Content-Length: 74
{"api":"v2/device/listposition","time":1529665112,"params":{"ids": [10]}}

Abfragen

Alle Geräte auflisten

Funktionsweise: Gibt eine Liste aller Geräte zurück, die die Geräte-ID, IMEI und Seriennummer enthält
API URI: v2/Gerät/ListeGeräte
Obligatorische Parameter: keine
Optionale Parameter: keine

Beispiel-Anfragetext

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

Beispiel Antwortkörper

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

Liste der (GPS-)Positionen abrufen

Funktionsweise: Gibt eine Liste aller gespeicherten Positionsprotokolleinträge für Geräte-IDs zurück
API URI: v2/Gerät/Listenposition
Obligatorische Parameter: "ids" - Array von Geräte-IDs
Optionale Parameter: keine

Beispiel-Anfragetext


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


Beispiel Antwortkörper


```
{
"errors": [],
"list":[
"10":[
{"time":"1529632725","pos":"47.5572,7.5967"},
{"time":"1529642725","pos":"47.5572,7.5968"},
{"time":"1529652725","pos":"47.5573,7.5969"},
],
"88":[],
]
}
```

Asset-Map abrufen

Funktionsweise:
Gibt eine Liste aller gespeicherten möglichen Assets zurück, die mit Get any asset data angefordert werden können.
Sie können entweder das menschenlesbare Formular oder das Asset-Tag verwenden, um die Daten abzufragen.
API URI: v2/device/getassetmap
Obligatorische Parameter: keine
Optionale Parameter: keine

Beispiel-Anfragetext

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

Beispiel Antwortkörper

Diese Antwort wurde zur besseren Lesbarkeit gekürzt.

{
"AssetKeys": {
"UDID": "AT001",
"Device Alias": "AT002",
"OS Version WinMobile iOS MacOS": "AT003",
"Model Name": "AT004",
"Serial Number": "AT005",
"Total Storage": "AT006",
"Free Storage": "AT007",
"IMEI": "AT008",
…
"apptecID": "APPTECID"
},
"errors": []
}

Alle Asset-Daten abrufen

Funktionsweise: Gibt eine Liste der angeforderten Asset-Daten für Geräte-IDs zurück
API URI: v2/device/getassetdata
Obligatorische Parameter: "ids" - Array von Geräte-IDs
Optionale Parameter:
"assetkeys" - Asset-Datenschlüssel, die zurückgegeben werden sollen. Wenn nicht angegeben, werden alle verfügbaren Asset-Daten
zurückgegeben. Eine Liste der Asset-Schlüssel erhalten Sie mit Get asset map.

Beispiel-Anfragetext


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


Beispiel Antwortkörper


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

Beispielcode in Python3

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

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

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

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

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

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

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

Apple Konfiguration

APNS-Zertifikat

Hier können Sie ein APNS-Zertifikat hochladen. Dies ist erforderlich, um iOS- und MacOS-Geräte zu verwalten.

Hinweis: Das APNS-Zertifikat ist nur ein Jahr lang gültig. Diese muss erneuert werden, bevor sie abläuft. Der Erneuerungsprozess ist identisch mit der Erstellung (siehe unten) und dauert nur wenige Minuten.

Sollten Sie vergessen, diese rechtzeitig zu erneuern, können Sie keine Änderungen an Ihren bereits registrierten Geräten vornehmen **und Sie müssen alle Geräte erneut registrieren.** .

Schritt 1

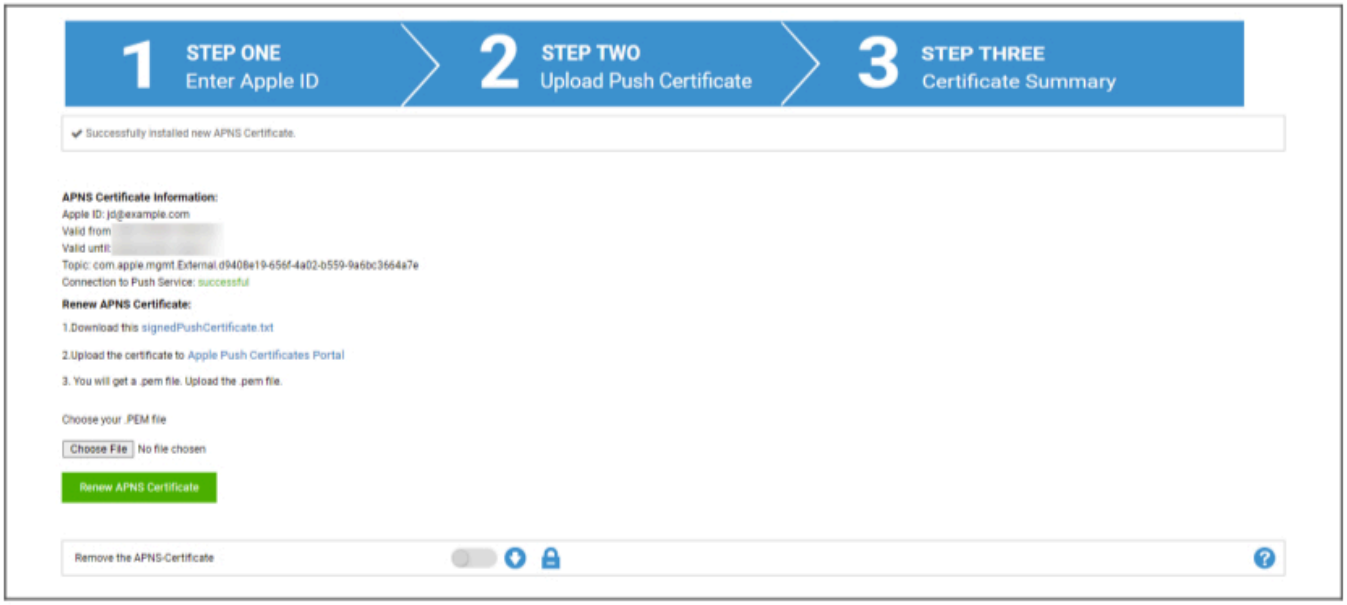
- Geben Sie zunächst Ihre Apple ID ein, die Sie für die Erstellung des APNS-Zertifikats verwenden möchten.

Hinweis: Diese Apple ID wird nur für die Erstellung des APNS-Zertifikats verwendet. Diese Apple ID hat nichts mit den Geräten zu tun und die Geräte werden nichts von dieser Apple ID wissen. Außerdem benötigen Sie Zugang zu dieser Apple ID, um das APNS-Zertifikat zu erneuern. Es wird daher empfohlen, eine generische Apple ID zu verwenden und die Anmeldedaten zu dokumentieren. Bevor das APNS-Zertifikat abläuft, wird eine Erinnerung an die verwendete Mail-Adresse der Apple ID gesendet.

- Klicken Sie auf "Nächster Schritt", um fortzufahren.
- (optional) Sie können auch das zuvor gelöschte APNS-Zertifikat wiederherstellen, wenn Sie es versehentlich gelöscht haben

Schritt 2

- Laden Sie die Datei signedPushCertificate.txt herunter
- Gehen Sie zu https://identity.apple.com/pushcert/ und melden Sie sich mit Ihrer Apple ID aus Schritt 1 an.
- Klicken Sie auf "Ein Zertifikat erstellen".
- (optional) geben Sie eine Notiz ein. Dies kann hilfreich sein, wenn Sie mehrere Mieter verwalten, um sie leicht identifizieren zu können.
- Klicken Sie auf "Datei auswählen", um die zuvor heruntergeladene Datei signedPushCertificate.txt auszuwählen.
- Klicken Sie auf "Hochladen".
- Sie sehen nun die Bestätigung, dass Sie ein APNS-Zertifikat erstellt haben.
- Klicken Sie auf "Download" und speichern Sie es.
- Gehen Sie zurück zur Verwaltungskonsole.
- Klicken Sie auf "Datei auswählen" und wählen Sie das APNS-Zertifikat, das Sie hochladen möchten.
- Klicken Sie auf "Hochladen".



Schritt 3

Sie haben nun das APNS-Zertifikat erfolgreich eingerichtet und können nun iOS- und MacOS-Geräte verwalten.

In Schritt 3 sehen Sie eine Übersicht über Ihr aktuell verwendetes APNS-Zertifikat.

Sie haben auch die Möglichkeit, das APNS-Zertifikat zu erneuern, indem Sie die auf dem Bildschirm angezeigten Schritte befolgen. Denken Sie daran, diese zu erneuern, bevor sie abläuft.

Denken Sie bei der Erneuerung des APNS-Zertifikats daran, sich mit der in Schritt 3 angegebenen Apple ID anzumelden und das zuvor verwendete Zertifikat zu erneuern und KEIN neues zu erstellen. Sie sehen das "Thema" des APNS-Zertifikats in Schritt 3 und beim Klicken auf das "i" im Apple Push Certificate Portal. Dies ist die eindeutige ID, die das Zertifikat identifiziert. Dies wird Ihnen helfen, den richtigen zu identifizieren und den richtigen zu erneuern.

Wenn Sie die Meldung "Fehler: Das Push-Zertifikat hat ein anderes Thema!" während der Erneuerung erhalten, bedeutet dies, dass Sie ein anderes Zertifikat erneuert oder ein neues Zertifikat erstellt haben.

Wenn Sie ein neues Zertifikat hochladen möchten, z.B. wenn Sie keinen Zugriff mehr auf die zuvor verwendete Apple ID haben, müssen Sie zunächst das aktuell hochgeladene Zertifikat löschen.

In jedem Fall bedeutet das Löschen des APNS-Zertifikats, dass Sie für die derzeit registrierten Geräte keine Änderungen mehr vornehmen können, bis Sie sie erneut registrieren. Stellen Sie also sicher, dass Sie darauf vorbereitet sind und entfernen Sie das Zertifikat nur, wenn es keine andere Möglichkeit gibt.

Verwalteter Zugang

Hier können Sie die Benutzeranmeldung für iOS-Geräte und die iPad-Freigabe für iOS-Geräte aktivieren.

Benutzerregistrierung

Die Option 'Benutzerregistrierung' ermöglicht einen speziellen Modus für BYOD-Geräte.

Für jeden Benutzer muss eine verwaltete Apple-ID im Apple Business Portal erstellt werden.

Während des Anmeldevorgangs werden die Benutzer nach ihren Apple-ID-Anmeldedaten gefragt.

Die 'Benutzeranmeldung' garantiert maximale Sicherheit für den Benutzer, da nur eine begrenzte Anzahl von Einstellungen und Einschränkungen vom MDM konfiguriert werden kann.

Verwaltete Domäne:

Die Domäne, die verwendet wird, um die E-Mail-Adresse des Benutzers der verwalteten Apple-ID zuzuordnen (muss im Format '@appleid.company.com' angegeben werden). john.doe@example.com wird z.B. john.doe@appleid.company.com zugeordnet.

Überprüfen Sie den Apple Business Manager, um Ihre Managed Domain zu sehen

Gemeinsames iPad

Ein freigegebenes iPad ist ein DEP-Gerät, das mit einem speziellen DEP-Profil konfiguriert ist.

Dies ermöglicht es mehreren Benutzern, sich mit ihrer verwalteten Apple-ID auf dem Gerät anzumelden.

Die verwaltete Apple-ID muss im Apple Business Portal oder im Apple School Manager erstellt werden.

Benutzer, die sich bei einem gemeinsam genutzten iPad anmelden, werden nach ihren verwalteten Apple-ID-Anmeldedaten gefragt.

Verwaltete Domäne:

Die Domäne, die verwendet wird, um die E-Mail-Adresse des Benutzers der verwalteten Apple-ID zuzuordnen (muss im Format '@appleid.company.com' angegeben werden). john.doe@example.com wird z.B. john.doe@appleid.company.com zugeordnet.

Überprüfen Sie den Apple Business Manager, um Ihre Managed Domain zu sehen

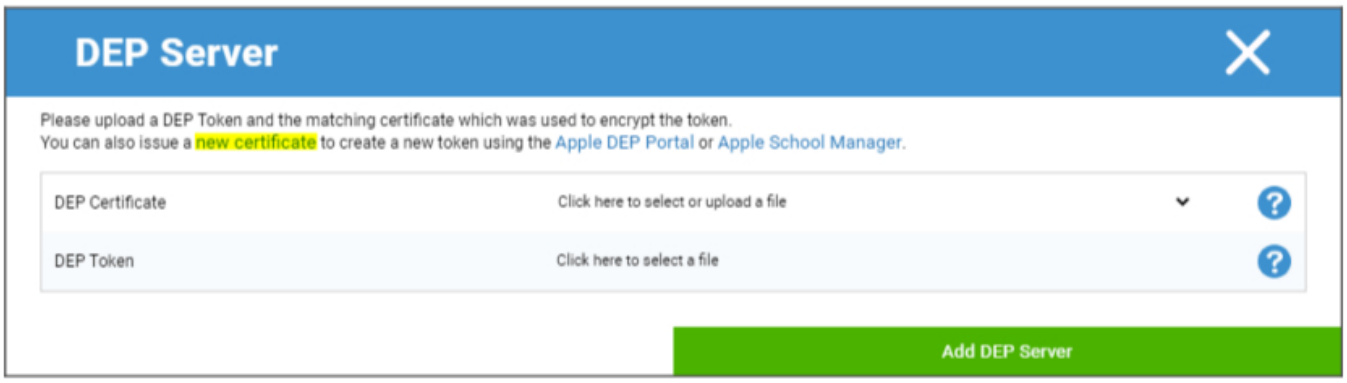
DEP

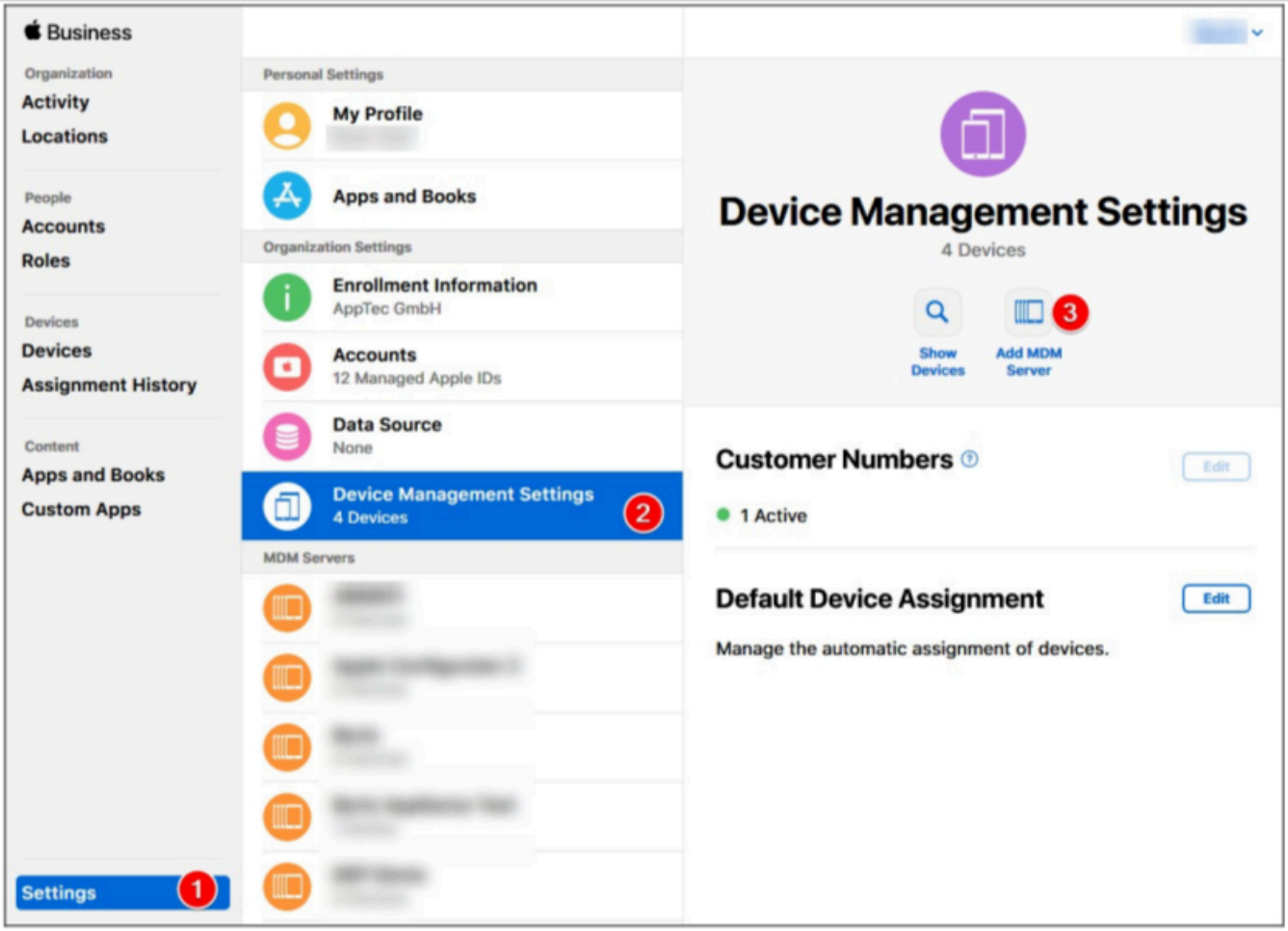
Mit DEP (Device Enrollment Program) können Sie Geräte ganz einfach in das MDM einschreiben. Wenn Sie DEP verwenden, werden die Geräte beim Einrichten automatisch mit dem MDM verbunden. Sie können auch fast alle Einrichtungsschritte überspringen, die bei iOS normalerweise obligatorisch sind.

Denken Sie daran, dass Sie die Geräte bei einem Händler kaufen müssen, der DEP unterstützt. Weitere Informationen erhalten Sie bei Ihrem Fachhändler oder bei Apple.

Mehr Informationen über DEP: https://www.apple.com/business/dep/

Klicken Sie auf das "+", um ein DEP-Token hinzuzufügen. Klicken Sie im Popup auf den Text "neues Zertifikat" (in der Abbildung unten gelb markiert). Dadurch wird ein DEP-Zertifikat erstellt und heruntergeladen. Gehen Sie anschließend zum Apple Business Manager(https://business.apple.com/) oder Apple School Manager(https://school.apple.com/).

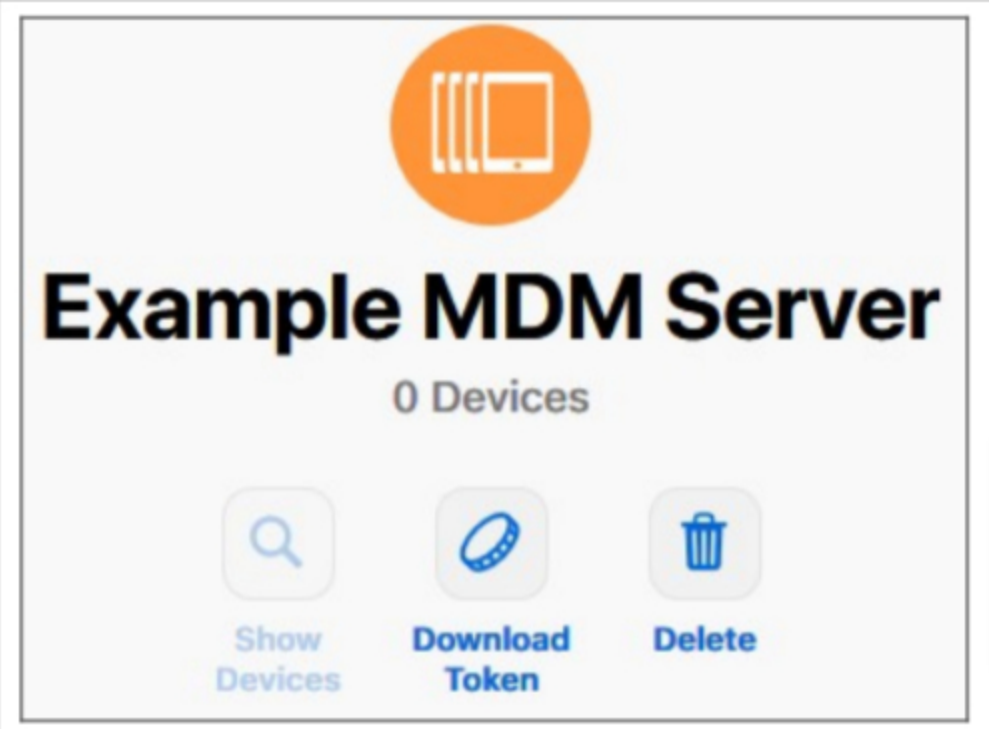




Führen Sie im Apple Business Manager die Schritte aus, die in der Abbildung oben gezeigt werden. Einstellungen → Geräteverwaltungseinstellungen → MDM-Server hinzufügen.

Geben Sie dem Server einen beliebigen Namen und laden Sie das zuvor heruntergeladene DEP-Zertifikat unter MDM Server Settings → Upload Public Key hoch und klicken Sie auf "Save".

Sie erhalten nun die Option "Token herunterladen". Klicken Sie hierauf und speichern Sie es. Der Token ist nur 1 Jahr lang gültig. Wenn Sie jedoch erneut auf "Token herunterladen" klicken, erhalten Sie einen neuen Token, was die Erneuerung des Tokens sehr einfach macht.



Sie können nun zum MDM zurückkehren, wo Sie zuvor das DEP-Zertifikat heruntergeladen haben. Wenn Sie die Registerkarte nicht geschlossen haben, sollte das Popup-Fenster zum Hinzufügen eines DEP-Servers noch geöffnet sein und das DEP-Zertifikat bereits ausgewählt sein. Sie können nun Ihren Token in das Feld "DEP Token" hochladen und auf DEP Server klicken.

In der Spalte "**Geräte**" sehen Sie die Anzahl der Geräte, die diesem DEP-Server zugewiesen sind. Geräte, die zu diesem DEP-Server hinzugefügt werden, werden automatisch im DEP-Pool in der Mobilen Verwaltung angelegt.

Sie können auf diese Nummer klicken, um einen Überblick über alle Ihre DEP-Geräte und deren Status zu erhalten.

Hinweis: Je nach Ihrem Arbeitsablauf oder Ihrer Konfiguration im Business Manager kann es sein, dass Sie diese Geräte dem DEP Server manuell zuweisen müssen. Sie können auch einen Standard-DEP-Server im Apple Business Manager für neue Geräte festlegen.

In der Spalte "**Profile**" sehen Sie die Anzahl der DEP-Profile, die Sie haben. Sie können auch auf diese Nummer klicken, um Details zu Ihren DEP-Profilen zu sehen, und Sie können hier alte/unbenutzte Profile löschen. Es ist derzeit nicht möglich, diese zu ändern. Wenn Sie eine Änderung vornehmen möchten, müssen Sie eine neue erstellen.

In der Spalte "**Letzte Synchronisierung**" können Sie den DEP Server manuell synchronisieren (z.B. wenn Sie gerade ein neues Gerät zu DEP hinzugefügt haben) und das Datum der letzten erfolgreichen Synchronisierung sehen.

In der Spalte "**Auto-Profil**" können Sie ein DEP-Profil als automatischen Standard festlegen. Dieses Profil wird neuen Geräten automatisch zugewiesen. Wenn Sie kein Auto-Profil einstellen, müssen Sie neuen Geräten jedes Mal manuell ein Profil zuweisen.

In der Spalte "**Profil hinzufügen**" können Sie ein neues DEP-Profil hinzufügen. Das Gerät erhält dies zu Beginn der Einrichtung des Geräts. Das DEP-Profil legt fest, wie das Gerät eingerichtet wird und welche Einrichtungsschritte übersprungen werden sollen.

Hinweis: Nachdem ein Gerät registriert wurde, können diese Einstellungen nur geändert werden, indem Sie das Gerät auf die Werkseinstellungen zurücksetzen und mit einem neuen Profil registrieren. Dies gilt insbesondere für "**Entfernbar**" und "**Kopplung zulassen**". Im Falle von "**Kopplung zulassen**" wird empfohlen, diese Option zu aktivieren, da sie über MDM-Einschränkungen deaktiviert werden kann, aber nicht wieder aktiviert werden kann, wenn sie im DEP-Profil deaktiviert wurde.

In der Spalte "**Bearbeiten**" können Sie einen neuen Token hochladen, z.B. wenn Sie den Token erneuern.

Konfigurator & URL

Pool-Anmelde-URL’s

Hier können Sie eine Anmelde-URL und einen Anmelde-QR-Code erstellen, die für eine bestimmte Anzahl von Anmeldungen und bis zu einem bestimmten Datum gültig sind. So können Sie mehrere Geräte mit nur einem Link oder QR-Code registrieren.

Geräte, die mit dieser URL oder diesem QR-Code registriert werden, befinden sich im Pool in der Mobilen Verwaltung und müssen anschließend manuell einer Gruppe oder einem Benutzer zugewiesen werden.

Hinweis: Dies gilt nur für die manuelle Einschreibung. Verwenden Sie diese URL nicht, wenn Sie die Geräte über Apple Configurator registrieren

MDM-Profil – Apple-Konfigurator

Hier erhalten Sie die URL, die Sie benötigen, wenn Sie Geräte über Apple Configurator registrieren. Während Sie die Geräte mit dem Apple Configurator vorbereiten, können Sie die Geräte im selben Prozess zum MDM hinzufügen. Der Apple Configurator benötigt dazu diese URL.

Geräte, die über den Apple Configurator hinzugefügt werden, befinden sich im Pool in der Mobilen Verwaltung und müssen anschließend manuell einer Gruppe oder einem Benutzer zugewiesen werden.

Hier finden Sie auch eine .mobileconfig-Datei, mit der Sie die Geräte über den Apple Configurator anmelden können. Es wird jedoch empfohlen, die URL zu verwenden.

Android-Konfiguration

Android-Konfiguration

Schutz deinstallieren	Wenn diese Funktion aktiviert ist, kann der Benutzer den Geräteadministrator nicht deaktivieren, ohne das vom MDM-Administrator festgelegte Passwort einzugeben. Das Passwort wird bei der Registrierung festgelegt, so dass die Geräte erneut registriert werden müssen, um das Passwort zu aktualisieren. Es gibt zwei Möglichkeiten, die Geräteadministratoren zu entfernen: 1. Manuell auf dem Gerät ◦ Öffnen Sie die EMM App auf dem Gerät ◦ Wechseln Sie zur Registerkarte Status ◦ Tippen Sie auf "Schutz deinstallieren". ◦ Geben Sie das Passwort ein. Sie können die Revision verwenden, um das richtige Passwort aus der "Passwort-Historie" in der Konsole zu erhalten. ◦ Scrollen Sie nach unten und tippen Sie auf den neu hinzugefügten Punkt "Tippen Sie auf "AppTec360 MDM App deinstallieren" (Sie haben 20 Sekunden Zeit, um diese Aufgabe auszuführen). ◦ Bestätigen Sie den Dialog "AppTec360 MDM App deinstallieren" mit "ok". Dadurch wird das Gerät von der Konsole abgemeldet. ◦ Um die App vom Gerät zu entfernen, bestätigen Sie den Dialog "AppTec360 MDM wird deinstalliert" mit "UNINSTALL". 2. die Automatik (Konsole) ◦ Wählen Sie das Gerät in der Konsole ◦ Klicken Sie auf das blaue Zahnradsymbol und wählen Sie "Enterprise Wipe".

	Hinweis: Nur verfügbar mit Android 4.x und niedrigeren Versionen oder auf Geräten mit der KNOX API (Samsung Geräte)
Passwort deinstallieren (Revision x)	Das festgelegte Passwort, mit dem der Benutzer den Geräteadministrator entfernen kann Revision x = Zähler, wie oft das Passwort bereits geändert wurde Es ist wichtig, welches Passwort der Benutzer benötigt, da es möglich ist, dass das Gerät noch nicht mit dem AppTec360 Server kommuniziert hat und daher das neueste Passwort noch nicht übermittelt wurde
Passwortverlauf	Wenn Sie auf die blaue Schaltfläche ("Verlauf anzeigen") klicken, können Sie die zuvor eingerichteten Passwörter einsehen
Erweiterter Deinstallationsschutz	Diese Option bietet Schutz vor Nicht-SAFE-Geräten Solange diese Einstellung aktiviert ist, ist es nicht möglich, den Geräteadministrator einfach zu deaktivieren.
Den Benutzer auffordern, blockierte Apps zu deinstallieren?	Wenn möglich, werden blockierte Apps nicht nur blockiert, sondern auch automatisch deinstalliert. Der Benutzer wird aufgefordert, blockierte Apps zu deinstallieren, wenn keine automatische Deinstallation möglich ist.
Intelligentes System App-Blockierung	Wenn Whitelisting aktiviert ist, blockiert der Android MDM Client alle vom Benutzer installierten Apps. Aktivieren Sie diese Einstellung, um alle startbaren System-Apps im Whitelisting-Modus zu blockieren.

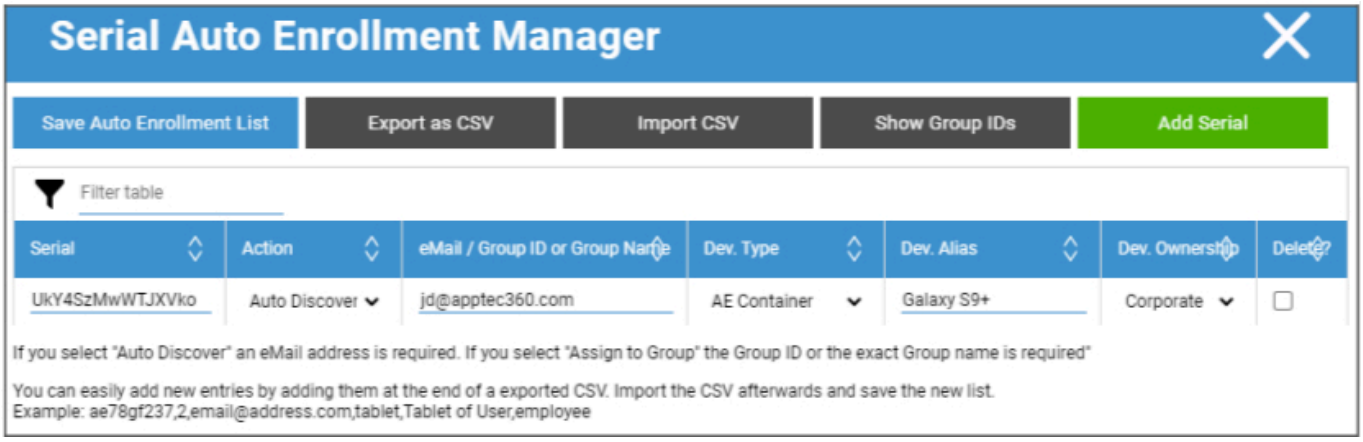
Automatische Einschreibung

Hier können Sie die Funktion Auto-Enrollment aktivieren, um Ihre Geräte automatisch zu registrieren, wenn der AppTec360 MDM Client auf dem Gerät geöffnet wird.

Wichtig: Diese Anmeldemethode ist veraltet und funktioniert nicht mehr unter Android 10 oder höher. Wenn Sie Android 7 oder höher verwenden, sollten Sie die Geräte ohnehin als vollständig verwaltetes Android Enterprise registrieren. Wenn Sie den Android Enterprise BYOD-Container verwenden möchten und Android 10 oder höher verwenden, müssen Sie das Gerät manuell über Anmeldeinformationen, QR-Code oder SMS registrieren. Die Auto-Enrollment-Liste wird dennoch verwendet, um den Registrierungsprozess für z.B. AE Enrollment, Knox Enrollment, etc. zu automatisieren.

Die Auto-Enrollment-Liste wird dennoch verwendet, um den Registrierungsprozess für z.B. AE Enrollment, Knox Enrollment, etc. zu automatisieren.

Indem Sie entweder auf "Serienmanager" oder "IMEI-Manager" klicken, können Sie die Seriennummer bzw. IMEI Ihrer Geräte hinzufügen. Sie müssen nicht beides für Ihre Geräte tun, eines reicht aus.



Aktion legt fest, ob die Geräte in den Pool, einen Benutzer oder eine Gruppe aufgenommen werden sollen.

Sie können auch eine .csv-Datei exportieren und importieren und Ihre Einträge nach Stichworten filtern.

Android Unternehmen

Hier können Sie Android Enterprise einrichten. Dies ist notwendig, um alle Funktionen von Android Enterprise zu nutzen.

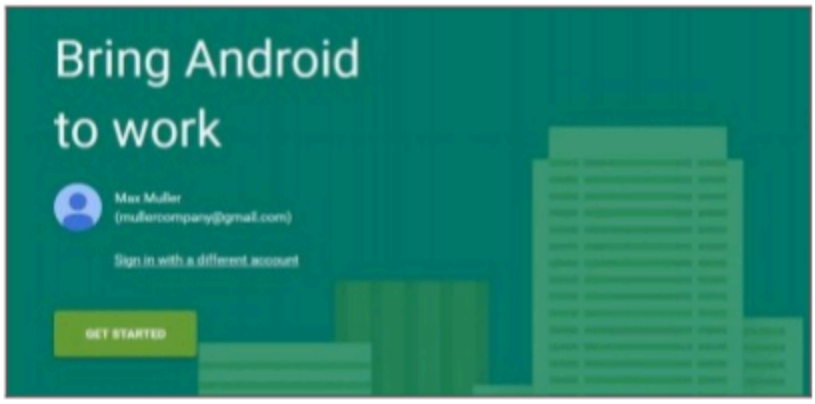
Erste Methode: Android-Unternehmenskonto (Google-Konto)

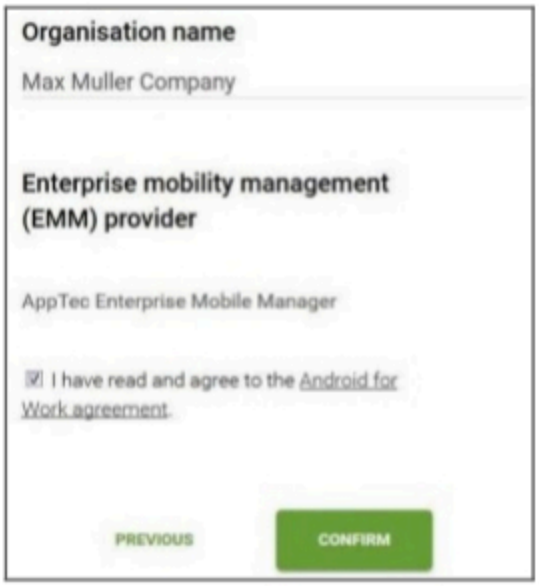
Drücken Sie zunächst auf "Setup vorbereiten", dann sollte nach einem kurzen Moment die Schaltfläche "Setup starten" erscheinen.

Dies bringt Sie zur Google Android Enterprise Setup-Seite.

Melden Sie sich mit dem Google-Konto an, das Sie verwenden möchten, falls Sie noch nicht angemeldet sind, und klicken Sie auf "Starten".

Jetzt können Sie den Namen Ihres Unternehmens eingeben. Aktivieren Sie anschließend das Kontrollkästchen und klicken Sie auf "Bestätigen".





Im letzten Schritt können Sie Ihre Registrierung abschließen und sollten zur Konsole zurückkehren. Wenn alles funktioniert hat, sollte es so aussehen:

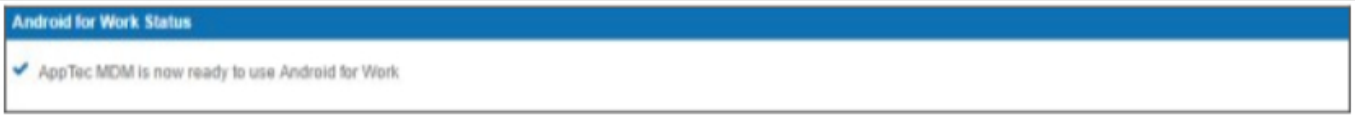
Jetzt können Sie damit beginnen, Ihren Android Enterprise Container zu konfigurieren.

Zweite Methode: G-Suite Konto

Klicken Sie auf "G-Suite verwenden" und melden Sie sich bei Ihrem Google Admin-Konto an. Dort gehen Sie auf "Sicherheit" -> "Mehr anzeigen" -> "EMM-Anbieter für Android verwalten" und generieren ein Token. Hinweis: Wenn Sie die Android Enterprise Settings in Ihrem G-Suite-Konto nicht sehen, müssen Sie zu "Weitere Apps und Dienste" gehen und die Android-Geräteverwaltung hinzufügen. Geben Sie nun den Token und Ihre primäre Domain in unsere Konsole ein und klicken Sie auf "Änderungen speichern". Wenn Sie fertig sind, klicken Sie auf "Android Enterprise-Konto verwenden".

Jetzt sollten Sie die Schaltfläche "Servicekonto erstellen" sehen. Klicken Sie darauf. Dieser Vorgang kann einige Augenblicke dauern.

Wenn alles funktioniert hat, sollte es so aussehen:



Jetzt können Sie damit beginnen, Ihren Android Enterprise Container zu konfigurieren.

Schutz vor Werksreset

Mit dem Schutz vor dem Zurücksetzen auf die Werkseinstellungen können Sie Ihr Gerät an ein Google-Konto Ihrer Wahl binden, das auch eine bestehende Bindung an ein Google-Konto außer Kraft setzt. Um den Schutz vor dem Zurücksetzen auf die Werkseinstellungen zu verwenden, müssen Sie ihn zunächst hier einrichten und anschließend in Ihren Profilen aktivieren.

Um den Schutz vor dem Zurücksetzen auf die Werkseinstellungen einzurichten, klicken Sie auf "FRP Setup" und folgen Sie den Anweisungen auf dem Bildschirm.

HINWEIS: Lesen Sie die Schritte sorgfältig durch und führen Sie sie aus. Wir empfehlen, dies in einem neuen Inkognito-Browser-Fenster zu tun, um zu vermeiden, dass Sie sich automatisch beim falschen Google-Konto anmelden. Sie können sich komplett aus dem Gerät aussperren, falls Sie eine falsche ID eingeben oder den Zugriff auf das verwendete Google-Konto verlieren sollten!

AE Einschreibung

Hier können Sie das Android Enterprise Ernollment aktivieren. Mit dieser Methode werden Ihre Geräte für den Android Enterprise Device Owner Mode angemeldet. In diesem Modus haben Sie die volle Kontrolle über das Gerät.

AE-Registrierung aktivieren	Aktiviert die AE-Registrierung Vorsicht: Wenn Sie AE Enrollment deaktivieren, funktionieren vorhandene QR-Codes und bereits konfigurierte NFC-Programmiergeräte nicht mehr. Wenn Sie AE Enrollment wieder aktivieren, müssen Sie erneut NFC-Push-Konfigurationen senden / neue QR-Codes generieren.
Automatische Erkennung aktivieren	Wenn sich ein Gerät über "AE Enrollment" anmeldet, versucht das System, es auf der Grundlage der in der Serien-/IMEI-Whitelist ("Allgemeine Einstellungen" > "Android-Konfiguration" > "Auto Enrollment") festgelegten Informationen einem Benutzer zuzuordnen.
Unbekannte Geräte blockieren	Nur Geräte, die in der Serien-/IMEI-Whitelist ("Allgemeine Einstellungen" > "Android-Konfiguration" > "Auto-Enrollment") aufgeführt sind, können sich anmelden.

Hinweis zu Methode 1 & 2: "Willkommensbildschirm" bezieht sich auf den ersten Bildschirm, den Sie nach dem Zurücksetzen auf die Werkseinstellungen sehen. Dies kann je nach Android-Version und/oder Gerätemodell, das Sie verwenden, unterschiedlich aussehen.

Methode 1: QR-Code-Anmeldung

(erfordert Android 7.0 oder höher) Wir empfehlen, diese Methode immer zu verwenden, wenn Sie Android 7 oder höher verwenden.

1. Das Gerät auf die Werkseinstellungen zurücksetzen
2. Generieren Sie den QR-Code für die Anmeldung mit einer der beiden folgenden Methoden:
   - Klicken Sie unter "Allgemeine Einstellungen -> Android-Konfiguration -> AE-Registrierung" auf "QR-Code generieren". Wählen Sie, ob Sie die Speicherverschlüsselung überspringen möchten und/oder ob alle Systemanwendungen entfernt werden sollen.
   - (alternativ) Wählen Sie ein vorhandenes Gerät. Klicken Sie in der "Geräteübersicht" auf den dort angezeigten QR-Code. Wählen Sie, ob Sie die Speicherverschlüsselung überspringen möchten und/oder ob alle Systemanwendungen entfernt werden sollen.
3. Tippen Sie nun 6 Mal auf den Willkommensbildschirm Ihres Geräts. Dies sollte den QR-Registrierungsmodus starten.
4. Verbinden Sie sich nun mit einem drahtlosen Netzwerk und warten Sie eine kurze Zeit, bis der QR-Code-Reader installiert ist
5. Scannen Sie jetzt den QR-Code

6. Das war's. Ihr Gerät ist jetzt für den Android Enterprise Device Mode angemeldet.
    - a. Wenn Sie den QR-Code in den "Allgemeinen Einstellungen" verwendet haben, finden Sie Ihr Gerät unter "Pool -> AE-Geräteeigentümergeräte". (Hinweis: Es ist möglich, dass Sie die Seite neu laden müssen, um die Geräte zu sehen). Wenn Sie die Option "Automatische Erkennung aktivieren" aktiviert haben, finden Sie das Gerät unter Ihrem Benutzer für die automatische Erkennung.
    - Wenn Sie den QR-Code eines bestehenden Geräteprofils verwendet haben, wird das Gerät in diesem Profil registriert.

Methode 2: NFC-Registrierung

(erfordert NFC und Android 6.0 oder höher)

Vorbereitung: Geben Sie Ihre WiFi-Informationen unter "Allgemeine Einstellungen -> Android Konfiguration -> AE Enrollment -> Daten für die NFC-Bereitstellung" ein. Verwenden Sie nun "NFC-Gerät", um nach dem Gerät zu suchen, das das Programmiergerät werden soll. Dieses Gerät wird verwendet, um die Anmeldeinformationen über NFC an die anderen Geräte zu senden.

1. Ihr Gerät auf die Werkseinstellungen zurücksetzen
2. Öffnen Sie die NFC-Pairing-App von AppTec360 auf Ihrem Programmiergerät
3. Wählen Sie, ob Sie die Speicherverschlüsselung überspringen möchten und/oder ob alle Systemanwendungen entfernt werden sollen.
4. Halten Sie beide Geräte Rücken an Rücken
5. Jetzt sollte die Android Enterprise Enrollment stark
6. Sie finden Ihr Gerät jetzt in der Konsole
    - a. Wenn Sie im Pool keine automatische Erkennung konfiguriert haben
    - b. Innerhalb des Benutzers, den Sie für die automatische Erkennung konfiguriert haben
    - c. Hinweis: Es kann sein, dass Sie die Seite neu laden müssen, um die Geräte zu sehen

Methode 3: Google-Konto

(erfordert Android 5.1 oder höher)

(Hinweis: Wenn Sie diese Methode verwenden, wird das Gerät nicht automatisch registriert. Stattdessen müssen Sie es manuell registrieren oder den Prozess mit der automatischen Registrierung automatisieren).

1. Ihr Gerät auf die Werkseinstellungen zurücksetzen
2. Gehen Sie durch die Einrichtungsschritte, bis Sie sich mit einem Google-Konto anmelden können
3. Geben Sie "afw#apptec" als Benutzername/E-Mail ein
4. Tippen Sie auf "Weiter"

5. Ihr Gerät ist jetzt ein Android Enterprise-Gerät

KNOX Immatrikulation

Hier können Sie das KNOX Enrollment aktivieren und finden die Informationen, die Sie benötigen, um ein KNOX Enrollment Profil im KNOX Deployment Portal zu erstellen. Sie benötigen ein Konto beim KNOX Deployment Portal, um dies zu konfigurieren und zu nutzen.

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

KNOX-Registrierung aktivieren	Aktiviert die KNOX-Anmeldung. Vorsicht! Wenn Sie KNOX Enrollment deaktivieren, funktionieren bestehende MDM-Profile nicht mehr. Wenn Sie KNOX Enrollment wieder aktivieren, müssen Sie das Feld "Custom JSON Data" in Ihrem MDM-Profil aktualisieren.
Automatische Erkennung aktivieren	Wenn sich ein Gerät über "KNOX Enrollment" anmeldet, versucht das System, es anhand der in der Serien-/IMEI-Whitelist ("Allgemeine Einstellungen" > "Android-Konfiguration" > "Auto Enrollment") festgelegten Informationen einem Benutzer zuzuordnen.

1. Melden Sie sich beim Samsung KNOX Mobile Enrollment Portal https://eukme.samsungknox.com/itadmin an.
2. Gehen Sie zu "MDM-Profile".
3. Klicken Sie auf "Hinzufügen".
4. Wählen Sie "Server-URI für mein MDM nicht erforderlich" und klicken Sie auf "Weiter".
5. Erstellen Sie nun ein Profil mit den Informationen, die in der Verwaltungskonsole angezeigt werden

Jetzt kann dieses KNOX Enrollment Profile direkt von Samsung auf dem Gerät installiert werden, wenn Sie die Geräte direkt von Samsung erwerben.

Alternativ können Sie auch die KNOX Deployment App herunterladen, sich mit Ihrem KNOX Deployment Account anmelden und das KNOX Enrollment Profile per NFC an andere Geräte senden.

Wenn auf dem Gerät ein KNOX-Anmeldeprofil installiert ist, lädt es unsere App herunter und meldet das Gerät an, sofern es über eine funktionierende Internetverbindung verfügt.

Die Registrierung von Geräten über KNOX Enrollment finden Sie unter "Pool -> KNOX Enrollment", oder innerhalb des Benutzers, den Sie in der automatischen Erkennung angegeben haben.

Zero-Touch

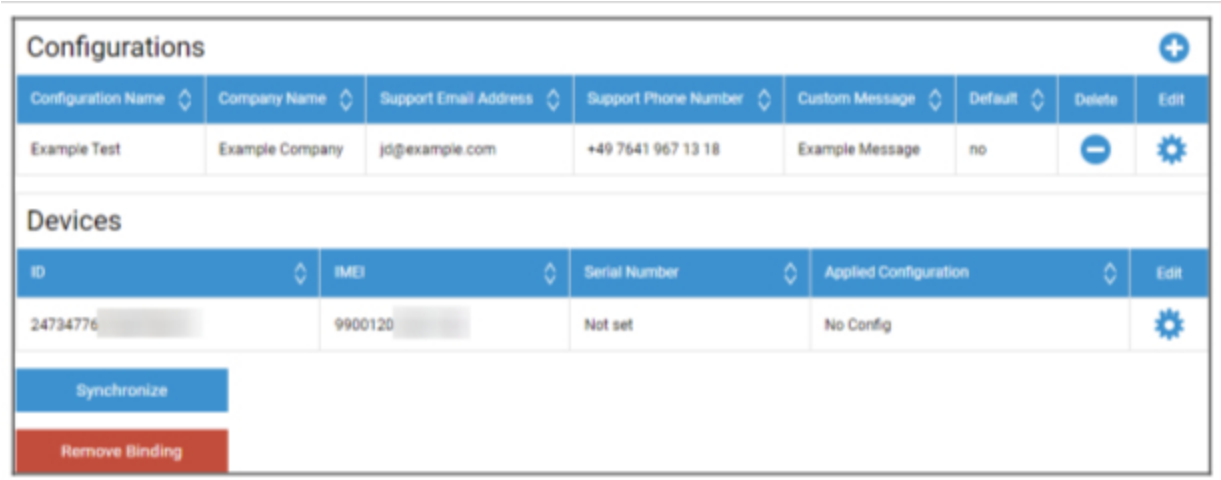
Mit Zero-Touch können Sie Ihre Geräte ganz einfach anmelden, ohne sie zu berühren oder etwas auf dem Gerät selbst zu konfigurieren. Sie müssen es nur einschalten, die Konfiguration wie gewohnt durchführen und das Gerät erhält alle Informationen zur Einrichtung und Verbindung mit dem MDM völlig automatisch.

Um Zero-Touch zu verwenden, müssen Sie Ihre Geräte bei einem Händler kaufen, der Zero-Touch unterstützt. Derselbe Wiederverkäufer erstellt auch ein Konto für Sie im Zero-Touch-Portal. Wenden Sie sich an Ihren Händler, um weitere Informationen über das Verfahren zu erhalten oder wenn Sie Probleme beim Zugriff auf das Zero-Touch Portal haben.

Klicken Sie auf "Einrichtung starten", um die Einrichtung zu beginnen. Sie werden zu einer Anmeldeseite weitergeleitet, auf der Sie Ihr Google-Konto auswählen müssen, das Zugriff auf das Zero-Touch Portal hat.

HINWEIS: Es ist möglich, JEDES Konto auszuwählen. Stellen Sie also sicher, dass Sie in diesem Schritt das richtige Konto auswählen. Wenn Sie Ihre Geräte/Konfigurationen nicht sehen, haben Sie höchstwahrscheinlich das falsche Konto verwendet.

Nach der Anmeldung sieht die Seite wie folgt aus:



Klicken Sie auf das "+", um eine Konfiguration hinzuzufügen, und füllen Sie die auf dem Bildschirm angezeigten Felder aus. Wenn Sie die Konfiguration als Standardkonfiguration aktivieren, wird sie den neuen Geräten automatisch zugewiesen. Durch das Erstellen oder Festlegen einer Standardkonfiguration wird diese nicht den bereits vorhandenen Geräten zugewiesen.

Wenn einem Gerät keine Konfiguration zugewiesen wurde, wird es wie ein normales Gerät eingerichtet und nicht mit dem MDM verbunden. Stellen Sie daher sicher, dass Ihren Geräten eine Konfiguration zugewiesen ist.

Nachdem Sie Ihr Konto verbunden haben, Ihre Geräte sichtbar sind und Sie ihnen eine Konfiguration zugewiesen haben, können Sie mit dem Einrichten der Geräte beginnen.

Sie können die Geräte zur Liste für die automatische Registrierung hinzufügen, so dass sie automatisch in eine bestimmte Gruppe oder einen bestimmten Benutzer eingetragen werden. Wenn Sie in der Liste Auto-Enrollment nichts konfiguriert haben, werden die Geräte in den Pool aufgenommen.

Windows-Konfiguration

Windows-Konfiguration

Hier haben Sie die Möglichkeit, die folgenden Konfigurationen auf Ihrem Windows 10 PC zu aktivieren:

Sofortige DM-Verbindung	
Erste Wiederholungsversuche	Stellt den ersten Verbindungsversuch zum Gerät her, dieser Wert steigt exponentiell an
Wiederholte Verbindungsversuche	Gibt an, wie viele Verbindungsversuche der DM-Client bei einem Verbindungsfehler durchführen soll
Maximale Schlafdauer	Gibt die maximale Schlafzeit nach einem Verbindungsfehler an
Erste Sync-Wiederholungen	Intervalle, in denen das Gerät mit dem Server kommunizieren soll, nach der ersten Verbindung
Intervall für den ersten Wiederholungsversuch	Bezieht sich auf "Erste Sync-Wiederholungen". Hier sind die Zeiten in Minuten angegeben Zum Beispiel ist unter "First Sync Retries" der Wert "2" und unter "First Retry Interval" der Wert "4 Minutes" aufgeführt. Auf diese Weise kommuniziert das Gerät nach der ersten Verbindung alle 4 Minuten 2 Mal.
Zweite Sync-Wiederholungen	Intervalle, in denen das Gerät mit dem Server kommunizieren soll, nachdem es die "Ersten Sync-Wiederholungen" abgeschlossen hat
Zweiter Wiederholungsversuch Intervall	Gleiches Prinzip wie bei "Erstes Wiederholungsintervall" - nur dass es hier für "Zweite Sync-Wiederholungen" gilt.
Regelmäßige Wiederholungen der Synchronisation	Intervalle, wie oft das Gerät in Zukunft mit dem Server kommunizieren soll Standard: "Unendlich" Wir empfehlen, diesen Wert nicht zu ändern, denn wenn Sie "10" eingeben, wird das Gerät 10x mit dem Server kommunizieren und dann aufhören. Die Kommunikation mit dem AppTec360-Server wird also unterbrochen!
Regelmäßiges Wiederholungsintervall	Gleiches Prinzip wie bei "Erstes/Zweites Wiederholungsintervall" - nur dass hier die Einstellungen für die Zukunft übernommen werden

Regelmäßiges Wiederholungsintervall	Gleiches Prinzip wie bei "Erstes/Zweites Wiederholungsintervall" - nur dass hier die Einstellungen für die Zukunft übernommen werden

ContentBox

Konfiguration

Hier können Sie die ContentBox konfigurieren. Sie können Dateien für Gruppen in der ContentBox ablegen, auf die Sie mit der ContentBox App auf dem Gerät zugreifen können.

ContentBox aktivieren	Aktivieren Sie ContentBox. Wenn Sie diese Funktion deaktivieren, wenn Sie die ContentBox nicht verwenden, können Sie auf OnPremise-Rechnern Ressourcen sparen.
Externe ContentBox-Installation verwenden	Die ContentBox kann auch mit Ihrer eigenen Nextcloud betrieben werden.
URL	Vollständige URL der Nextcloud-Entität
Root-Benutzer	Root-Benutzer des Nextcloud-Kontos
Root-Passwort	Root-Passwort für das Nextcloud-Konto
Standardberechtigungen für Gruppenordner	Standardberechtigungen für Gruppenordner, können von der Gruppe individuell geändert werden (in Mobile Management)
Gruppenordner für Untergruppen freigeben	Wenn aktiv, kann jede Untergruppe alle Ordner der Hauptgruppe lesen, kann aber auch für jede Gruppe individuell konfiguriert werden (Mobile Management)
Berechtigungen für Untergruppen	Berechtigungen für Untergruppen kann für jede Gruppe individuell konfiguriert werden (Mobile Management)
Gemeinsame Nutzung zulassen	Ermöglicht es dem Benutzer, den Inhalt über Links zu teilen, kann für jede Gruppe individuell konfiguriert werden
Maximale Größe der hochgeladenen Datei in MB	Maximale Größe einer Datei Standard: 512 MB Maximale Konfiguration: 2048
WebDAV-Anmeldeinformationen	
WebDAV-URL	Sie können die ContentBox auch mit WebDAV öffnen. Bitte löschen Sie unter keinen Umständen die folgenden Ordner: /apptecgroups /apptecgroups/AppTecGroup-X
Root-Benutzer	Name des Root Users
Passwort	Passwort der Root-Benutzer

Die Synchronisierung mit der ContentBox erfolgt automatisch. Sie können jedoch eine manuelle Synchronisierung mit "ContentBox synchronisieren" durchführen.

Außerdem können Sie hier die ContentBox auf jedem einzelnen Gerät aktivieren/deaktivieren.

Dies ist nur relevant, wenn Sie die ContentBox nicht zusätzlich lizenziert haben, dann haben Sie noch Zugriff auf 25 Geräte, mit denen Sie die ContentBox testen können - hier können Sie dies für die jeweiligen Geräte aktivieren.

LDAP-Konfiguration

LDAP-Übersicht

Hier können Sie eine Verbindung zu Ihrem Active Directory über LDAP herstellen, um Benutzer und Gruppen massenhaft zu importieren. Die Synchronisierung muss manuell durchgeführt werden. Sie können mehrere LDAP-Verbindungen zu verschiedenen Systemen oder mit unterschiedlichen Konfigurationen/Filtern konfigurieren.

Server Name	Der Anzeigename des Servers
Typ	Derzeit werden nur Active Directories unterstützt, die LDAP unterstützen
LDAP-Domäne	Die primäre LDAP-Domäne (z. B. example.com)
LDAP-Host	Nur erforderlich, wenn der LDAP-Host nicht unter der angegebenen LDAP-Domäne erreichbar ist.
Hafen	Leer lassen, um den Standard-Port zu verwenden (389 oder 636 für SSL)
Benutzername	Z.B. CN=John,OU=Users,DC=EXAMPLE,DC=COM Hinweis: Die meisten Systeme verlangen den Benutzernamen in diesem Format und akzeptieren nicht "John" als Benutzernamen
Passwort	
Bestätigen Sie Ihr Passwort	
Sicherheit der Verbindung	Hinweis: Wenn Sie SSL oder TLS verwenden, wird das Zertifikat des Active Directory überprüft. Wenn diese selbstsigniert ist, müssen Sie die Root-CA zum Vertrauensspeicher des OnPremise-Rechners hinzufügen. Wenn Sie eine Cloud verwenden, muss Active Directory ein vertrauenswürdiges Zertifikat bereitstellen, sonst funktioniert die Verbindung nur ohne Verschlüsselung.
Automatische Synchronisation.	Aktiviert die automatische Synchronisierung des LDAP-Verzeichnisses in dem Zeitintervall, das in den allgemeinen LDAP-Einstellungen angegeben ist.
Basis-DN	Wenn Sie nicht das gesamte Verzeichnis synchronisieren möchten, können Sie hier eine OU angeben, z.B. OU=AndroidUsers,OU=Users,DC=EXAMPLE,DC=COM
Mitglied von	Alle importierten Benutzer werden der ausgewählten Gruppe hinzugefügt.
Nur aktivierte Benutzer?	Wenn diese Option aktiviert ist, wird das Attribut userAccountControl berücksichtigt, Benutzer ohne dieses Attribut werden nicht importiert.

LDAP-Filter	Sie können LDAP-Filter verwenden, um zu filtern, welche Benutzer importiert werden
Regex-Filter	Sie können Regex-Filter verwenden, um zu filtern, welche Benutzer importiert werden.
Verbindung testen	Testet die Verbindung beim Speichern der Konfiguration
Verzeichnisstruktur bei Synchronisierung zurücksetzen?	Bei true werden alle LDAP-Einträge an ihre ursprüngliche Position im LDAP-Baum zurückgeschoben. Es wird empfohlen, sie zu aktivieren.
Gelöschte Benutzer und Gruppen wieder importieren?	Wenn diese Option aktiviert ist, werden gelöschte Benutzer und Gruppen neu erstellt. Es wird empfohlen, sie zu aktivieren.
Synchronisierte Löschungen?	Wenn diese Option aktiviert ist, werden Gruppen und Benutzer gelöscht, wenn sie auf dem LDAP-Server gelöscht werden. Auch die Geräte von gelöschten Benutzern werden gelöscht.

Unterhalb der Liste Ihrer LDAP-Konfigurationen können Sie den Zeitraum festlegen, in dem sich das System automatisch synchronisiert. Verwendet nur die LDAP-Konfigurationen für die automatische Synchronisierung, bei denen die entsprechende Option aktiviert ist.

App Verwaltung

Hausinterne App DB

Android

Hier können Sie die Android-Apps, die Ihr Unternehmen entwickelt hat, hochladen und sie später in Mobile Management in Geräte- oder Gruppenprofilen verteilen.

Bitte beachten Sie, dass wir empfehlen, nur Apps auf diese Weise zu vertreiben, die nicht im Google Play Store erhältlich sind.

Klicken Sie auf das "+", um die APK einer App hochzuladen, die Sie hochladen möchten. Derzeit wird nur das APK-Format unterstützt.

Das Upload-Limit auf OnPremise Appliances kann in Schritt 3 der Appliance-Konfiguration erhöht werden. Wenn Sie das Upload-Limit für die Cloud erhöhen möchten, wenden Sie sich bitte an den Support, um weitere Informationen zu erhalten.

Beachten Sie, dass APKs normalerweise etwas kleiner sind als ihr Inhalt. Es ist möglich, dass ein Upload deswegen fehlschlägt, da die APK dabei entpackt wird. Es ist z.B. möglich, dass eine 95MB APK bei einem 100MB Upload-Limit nicht funktioniert. Erhöhen Sie in diesem Fall das Upload-Limit wie oben beschrieben.

Wir raten Ihnen auch, die APK zunächst manuell auf ein Testgerät zu übertragen (z.B. über USB) und zu versuchen, sie manuell mit der Dateien-App des Geräts zu installieren. Wenn dies aus irgendeinem Grund nicht funktioniert, wird es auch über MDM fehlschlagen.

Ziel aktualisieren

Mit der Funktion "Ziel aktualisieren" können Sie wählen, welche Version einer App installiert werden soll oder auf welche Version eine App aktualisiert werden soll, wenn Sie "Auf dem neuesten Stand halten" für eine App aktiviert haben.

Wenn Sie kein Aktualisierungsziel ausgewählt haben, wird die höchste Version verwendet.

Beachten Sie, dass Android kein Downgrade von Apps durchführen kann. Beachten Sie auch, dass der "Versionscode" bestimmt, ob eine Version höher, niedriger oder gleich ist oder nicht. Stellen Sie also sicher, dass Sie diese Version in Ihrer App korrekt erhöhen, wenn Sie ein Update erstellen.

iOS

Hier können Sie die von Ihnen entwickelten iOS-Apps hochladen und sie später in Mobile Management in Ihrem Geräte- oder Gruppenprofil verteilen.

Klicken Sie auf das "+", um die IPA einer App hochzuladen, die Sie hochladen möchten. Ab sofort wird nur noch das IPA-Format unterstützt.

Das Upload-Limit auf OnPremise Appliances kann in Schritt 3 der Appliance-Konfiguration erhöht werden. Wenn Sie das Upload-Limit für die Cloud erhöhen möchten, wenden Sie sich bitte an den Support, um weitere Informationen zu erhalten.

Ziel aktualisieren

Mit der Funktion "Ziel aktualisieren" können Sie wählen, welche Version einer App installiert werden soll oder auf welche Version eine App aktualisiert werden soll, wenn Sie "Auf dem neuesten Stand halten" für eine App aktiviert haben.

Wenn Sie kein Aktualisierungsziel ausgewählt haben, wird die höchste Version verwendet.

MacOS

Hier können Sie die von Ihnen entwickelten MacOS-Apps hochladen und sie später in Mobile Management in Ihrem Geräte- oder Gruppenprofil verteilen.

Klicken Sie auf das "+", um die PKG einer App hochzuladen, die Sie hochladen möchten. Ab sofort wird nur noch das PKG-Format unterstützt.

Das Upload-Limit auf OnPremise Appliances kann in Schritt 3 der Appliance-Konfiguration erhöht werden. Wenn Sie das Upload-Limit für die Cloud erhöhen möchten, wenden Sie sich bitte an den Support, um weitere Informationen zu erhalten.

Ziel aktualisieren

Mit der Funktion "Ziel aktualisieren" können Sie wählen, welche Version einer App installiert werden soll oder auf welche Version eine App aktualisiert werden soll, wenn Sie "Auf dem neuesten Stand halten" für eine App aktiviert haben.

Wenn Sie kein Aktualisierungsziel ausgewählt haben, wird die höchste Version verwendet.

Windows 10

Hier können Sie die Windows 10 Apps hochladen und später in Mobile Management in Ihrem Geräte- oder Gruppenprofil verteilen.

Klicken Sie auf das "+", um das APPX, APPXBUNDLE oder MSI einer App hochzuladen, die Sie hochladen möchten. Ab sofort wird nur noch das APPX-, APPXBUNDLE- oder MSI-Format unterstützt.

Sie können auch Abhängigkeiten für eine App hochladen und definieren, die dann automatisch verteilt und installiert werden, bevor Sie die gewünschte App installieren.

Das Upload-Limit auf OnPremise Appliances kann in Schritt 3 der Appliance-Konfiguration erhöht werden. Wenn Sie das Upload-Limit für die Cloud erhöhen möchten, wenden Sie sich bitte an den Support, um weitere Informationen zu erhalten.

Ziel aktualisieren

Mit der Funktion "Ziel aktualisieren" können Sie wählen, welche Version einer App installiert werden soll oder auf welche Version eine App aktualisiert werden soll, wenn Sie "Auf dem neuesten Stand halten" für eine App aktiviert haben.

Wenn Sie kein Aktualisierungsziel ausgewählt haben, wird die höchste Version verwendet.

Win32-Paket (.exe)

Sie können auch .exe-Dateien/Installationsprogramme auf Ihre Geräte verteilen.

Name des Pakets	Der Name, der im MDM angezeigt werden soll
Beschreibung	Im MDM angezeigte Beschreibung
Paket Datei	Es sind nur .zip-Dateien erlaubt. Legen Sie die Dateien, die Sie bereitstellen möchten, in diese Zip-Datei.
Kontext des Einsatzes	**System**: Der Installationsbefehl wird mit Systemprivilegien ausgeführt, die höher sind als "Benutzer". Auch bei der Verwendung von "System" hat der Prozess keine Benutzeroberfläche, d.h. er ist still und das Benutzerprofil, z.B. Umgebungsvariablen wie %AppDat%, ist nicht zugänglich. **Benutzer**: Der Installationsbefehl hat Zugriff auf das Benutzerprofil und kann bei Bedarf die Benutzeroberfläche anzeigen. Hinweis: Einige Prozesse funktionieren möglicherweise nur in einem Kontext. Wenn sich z.B. eine Software in AppData installiert, funktioniert sie nur, wenn Sie "Benutzer" auswählen.
Befehl installieren	Der Befehl, mit dem Sie das Programm installieren. Der Installationsbefehl für eine Zip-Datei, die "setup.exe" in ihrem Stammverzeichnis enthält und den Parameter "/s" für eine stille Installation unterstützt, lautet beispielsweise "setup.exe /s". Beachten Sie, dass verschiedene Software unterschiedliche Parameter haben kann.
Befehl deinstallieren	Der auszuführende Befehl zur Deinstallation der Software über MDM. Normalerweise verweist dies auf das Deinstallationsprogramm. Zum Beispiel "C:\Programme\BeispielSoftware\uninstall.exe".
Anforderungen	
Hinweis: Damit die Software installiert werden kann, müssen alle festgelegten Anforderungen erfüllt sein. Andernfalls wird es nicht installiert. Einige Felder können obligatorisch sein. Wenn für eine Anforderung kein Wert festgelegt wird, wird die Anforderung ignoriert.	
OS-Architektur	OS-Architektur
Min OS Version	Min OS Version
Min. freier Festplattenspeicher (MB)	Min. freier Festplattenspeicher (MB)
Minimaler physischer Speicher (MB)	Minimaler physischer Speicher (MB)
Minimale Anzahl von logischen	Minimale Anzahl von logischen Prozessoren

Prozessoren	
Minimale CPU-Geschwindigkeit (MHz)	Minimale CPU-Geschwindigkeit (MHz)
Zusätzliche Anforderungen	Sie können hier auch manuell Regeln definieren oder ein Skript hochladen, um zusätzliche Anforderungsprüfungen durchzuführen, wenn Sie dies wünschen.
Erkennungsregeln	
Methode zur Erkennung	Hier können Sie festlegen, wie erkannt werden soll, ob die App auf dem Gerät installiert ist. Die Installationsbefehle werden nur ausgeführt, wenn diese Regeln feststellen, dass die App NICHT installiert ist. Deinstallationsbefehle werden nur ausgeführt, wenn diese Regeln feststellen, dass die App nicht installiert ist. **Regeln manuell definieren**: Ermöglicht es Ihnen, eine oder mehrere Regeln manuell zu definieren, um z.B. zu prüfen, ob eine bestimmte Datei, ein Ordner, eine MSI oder ein Registrierungsschlüssel vorhanden ist. Wenn alle angegebenen Erkennungsregeln zutreffen, wird die App als vorhanden betrachtet. **Skript verwenden**: Laden Sie Ihr eigenes Skript mit Ihren eigenen Prüfungen hoch. Wenn das Skript "$TRUE" zurückgibt, wird die App als vorhanden betrachtet.
Regeln zur Erkennung	

App-Einstellungen

iOS App Einstellungen

Hier können Sie die Standardeinstellungen für das Hinzufügen einer App zu den obligatorischen Apps oder zum Enterprise App Store festlegen.

Hinweis: Hier wird nur festgelegt, was beim Hinzufügen von Apps standardmäßig ausgewählt ist. Dies ändert NICHT die bestehenden Einstellungen für Apps, die bereits in den obligatorischen Apps oder im Enterprise App Store hinzugefügt wurden.

Auf dem Laufenden bleiben	Hält die App automatisch auf dem neuesten Stand. Bitte beachten Sie, dass es bis zu 7 Tage nach Veröffentlichung eines Updates dauern kann, bis die App aktualisiert wird.
Überholen, wenn nicht verwaltet	Wenn eine App bereits als nicht verwaltet (durch den Benutzer) installiert ist, wird die App vom MDM übernommen und verwaltet.
App entfernen, wenn MDM-Profil entfernt wird	Deinstalliert die App, wenn das MDM entfernt wird.
Verhindern Sie die Sicherung der App-Daten	Verhindert die Sicherung der App-Daten.

Android App Einstellungen

Hier können Sie die Standardeinstellungen für das Hinzufügen einer App zu den obligatorischen Apps oder zum Enterprise App Store festlegen.

Hinweis: Hier wird nur festgelegt, was beim Hinzufügen standardmäßig ausgewählt ist. Dies ändert NICHT die Einstellungen für Apps, die bereits in den obligatorischen Apps oder im Enterprise App Store hinzugefügt wurden.

Auf dem Laufenden bleiben	Hält die App automatisch auf dem neuesten Stand. Nur für InHouse Apps verfügbar.
Kontrolliertes AppTec360 EMM Client Update	Wenn diese Option aktiviert ist, können Administratoren das Updateziel für den AppTec360 EMM Client festlegen. Eine Liste aller verfügbaren Versionen des AppTec360 EMM Clients finden Sie unter "Allgemeine Einstellungen" → "App-Verwaltung" → "In-House App DB" → "Android".

Apps von Drittanbietern

Android

Hier können Sie Ihren Aktivierungscode für Ikarus eingeben.

Stellen Sie dies auf "Aktivierungscode verwenden" und geben Sie hier Ihren Aktivierungscode ein.

Hinweis: Nachdem Sie den Code eingegeben und gespeichert haben, ist der Code noch nicht dem Profil hinzugefügt, das an das Gerät gesendet wird. Sie müssen eine Änderung in Ihrem Profil vornehmen, damit der Code dem Profil hinzugefügt werden kann. Ändern Sie z.B. einen beliebigen Schalter im Profil von Aus → Ein → Aus - Speichern → Jetzt zuweisen.

iOS

Hier können Sie Ihre SecurePIM-Lizenz eingeben. Nachdem Sie die Lizenz eingegeben haben, drücken Sie auf "Änderungen speichern" und Sie können die SecurePIM-Optionen nutzen.

VPP / KNOX Premium

Apples Volume Purchase Program (VPP) ermöglicht es Ihnen, kostenpflichtige und kostenlose Apps ganz einfach auf Ihre Geräte zu verteilen. Dies ist sehr empfehlenswert, da Sie keine Apple ID auf den Geräten benötigen, die Benutzer die Installation nicht bestätigen müssen (überwacht), die Benutzer das Passwort der Apple ID nicht eingeben müssen und Sie bezahlte Apps einfach verteilen können, ohne sie auf jedem Gerät erneut zu kaufen.

Um VPP zu nutzen, müssen Sie sich im Apple Business Manager registrieren.

VPP-Lizenzen

Hier können Sie sich einen Überblick über Ihre VPP Apps verschaffen, wie viele Lizenzen verwendet werden und wie viele noch verfügbar sind.

Wenn Sie auf das Rad klicken, können Sie sehen, welchen Geräten eine Lizenz zugewiesen ist und welchen Status diese Zuweisung hat.

Wenn Sie auf klicken, wird der VPP-Cache aktualisiert, der die im MDM zugewiesenen Lizenzen mit den auf Apples Seite zugewiesenen Lizenzen vergleicht. Dies kann in einigen Fällen Lizenzprobleme beheben.

VPP Token

Hier können Sie Ihren VPP Token hochladen, den Sie im Apple Business Manager unter Einstellungen → Apps & Bücher finden. Sie können mehrere VPP-Tokens hochladen.

Sie können einen Token erneuern, indem Sie einfach einen neuen Token im Apple Business Manager herunterladen, auf das Rad "Bearbeiten" klicken und den neuen Token hochladen.

Der "VPP-Modus" bestimmt, wie die Lizenzzuweisung gehandhabt wird. Abhängig von Ihrem Szenario müssen Sie verschiedene Modi verwenden:

"Gerätebasiert" muss verwendet werden, wenn die Geräte über QR-Code, Link, Apple Configurator oder DEP angemeldet werden.

"Benutzerbasiert" ist erforderlich, wenn die Geräte mit der Benutzerregistrierung oder als Shared iPad registriert sind.

Wenn Sie "Automatisches Lizenzmanagement" aktivieren, werden Benutzern, die von einer Gruppe in eine andere verschoben werden, automatisch Apple VPP-Lizenzen auf der Grundlage des Gruppenprofils, in das sie verschoben werden, zugewiesen.

Bestehende Apple VPP-Lizenzen aus der Gruppe, aus der sie gewechselt haben, werden nicht widerrufen.

Neuen Benutzern, die einer Gruppe hinzugefügt werden, werden automatisch Apple VPP-Lizenzen auf der Grundlage des jeweiligen Gruppenprofils zugewiesen.

KNOX Premium Schlüssel

Hier können Sie Ihren KNOX Premium Key eingeben, um den Samsung KNOX Container zu nutzen.

Bitte beachten Sie, dass dies seit Android 10 nicht mehr unterstützt wird. Verwenden Sie stattdessen den Android Enterprise Container.

App Store Einstellungen

Region & Sprache

Hier können Sie die Standardsprache und -region für die App-Suche in der App-Verwaltung festlegen.

Bitte beachten Sie, dass die Einstellung für iTunes auch festlegt, wie das System Informationen über bestimmte Apps abruft. Wenn Sie in Ihren Listen auf Apps stoßen, die auf seltsame Weise angezeigt werden (z.B. fehlendes Symbol), haben Sie möglicherweise eine Region festgelegt, in der die betreffende App nicht verfügbar ist.

AE Play Store

Hier finden Sie alle Optionen für den Play Store für Android-Unternehmensgeräte, um Apps zu genehmigen, eigene Apps in den Play Store hochzuladen oder Ihre eigenen Web-Apps zu erstellen.

Zugelassene Apps

Hier erhalten Sie einen Überblick über alle Apps, die Sie genehmigt haben.

Play Store Apps

Dadurch wird ein iFrame geladen, der den Play Store anzeigt. Suchen Sie nach einer beliebigen App, klicken Sie sie an und genehmigen Sie sie. Während Sie die App genehmigen, können Sie auch festlegen, dass die Genehmigung widerrufen wird, wenn sich die erforderlichen Berechtigungen ändern. Wir empfehlen, diese Einstellungen bei der Genehmigung von Apps standardmäßig zu belassen.

Nachdem eine App genehmigt wurde, können Sie sie zu Ihren Profilen hinzufügen.

Die Schaltfläche "Genehmigen" ändert sich nach der Genehmigung in "Genehmigung widerrufen", so dass Sie die Apps jederzeit entfernen können, wenn Sie sie nicht mehr benötigen.

Private Apps

Hier können Sie Ihre eigene App als private App in den Google Play Store hochladen. Dies ermöglicht Ihnen, die App über Googles Dienste zu verbreiten und sie über diese zu aktualisieren. Dies hat auch

den Vorteil, dass Ihre eigenen Apps ohne die normalerweise erforderliche Bestätigung des Benutzers installiert werden können.

Web Apps

Hier können Sie Web Apps erstellen, d.h. Links zu bestimmten Webseiten, die wie Apps zugewiesen werden können.

Sie können auch ein benutzerdefiniertes Symbol verwenden und festlegen, wie genau es angezeigt wird.

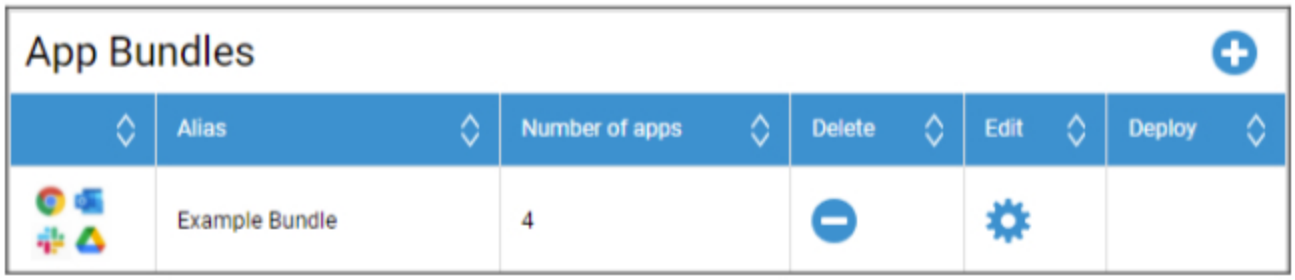
Laden-Layout

Das Store-Layout bestimmt, wie Apps im Play Store angezeigt werden oder ob sie überhaupt angezeigt werden.

Denken Sie daran, wenn Sie Apps im Play Store anzeigen möchten, die der Benutzer manuell installieren kann, müssen diese hier im Layout hinzugefügt werden **UND** im Profil zum Enterprise Play Store hinzugefügt werden. Wenn Sie eine App nur zu einer von ihnen hinzufügen, wird sie nicht angezeigt.

App-Bündel

Mit App-Bundles können Sie Gruppen von Apps definieren, die mit einem Klick Geräte- oder Gruppenprofilen zugewiesen werden können.



Klicken Sie auf das "+", um ein neues App-Bundle zu erstellen. Nachdem Sie ein App-Bundle erstellt haben, können Sie auf "Bearbeiten" klicken, um Apps aus verschiedenen Quellen zu dem Bundle hinzuzufügen.

Ein Bundle kann wie jede andere App zu Profilen hinzugefügt werden. Beim Hinzufügen von Apps haben Sie eine zusätzliche Registerkarte mit dem Namen "App-Bundles", auf der Sie Ihre Bundles haben.

Wenn Sie eine Änderung an einem App-Bundle vornehmen, wird eine Schaltfläche in der Spalte "Bereitstellen" angezeigt. Damit können Sie diese Änderungen an alle Profile weitergeben, die dieses Bundle enthalten. Denken Sie also daran, dass Sie dies nach dem Hinzufügen oder Entfernen von Apps in einem Bundle manuell tun müssen.

Fernsteuerung

TeamViewer

TeamViewer-Anschluss

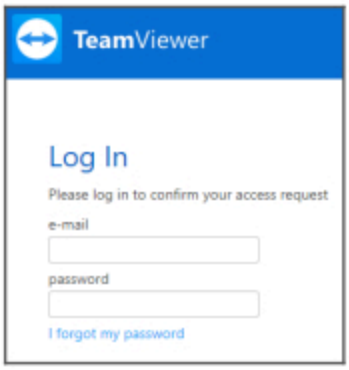
Hinweis: In der kostenlosen Testversion unserer Cloud-Version können Sie Ihr TeamViewer-Konto nicht verbinden. Stattdessen wird automatisch ein kostenloses Demokonto für Sie eingerichtet.

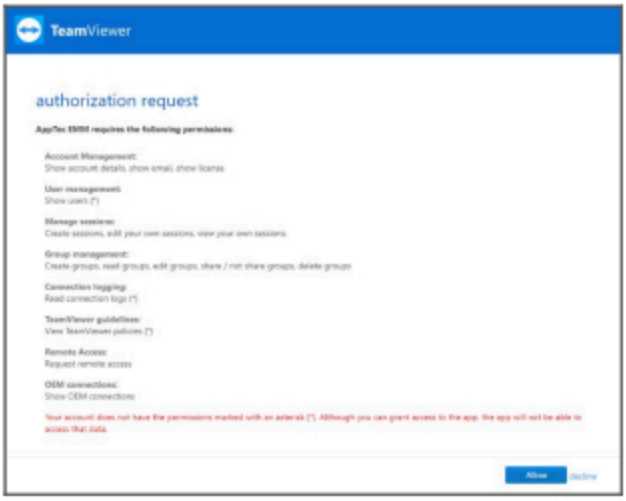
Gehen Sie zu Allgemeine Einstellungen -> Fernsteuerung -> TeamViewer. Hier können Sie Ihr TeamViewer-Konto mit der Konsole verknüpfen oder Informationen über Ihr derzeit verbundenes Konto einsehen. Sie können auch alle derzeit aktiven Sitzungen einsehen, wenn Sie auf "Aktive Sitzungen" gehen.

Um Ihr Konto zu verknüpfen, klicken Sie auf "Einrichtung starten".

Daraufhin werden Sie auf eine neue Seite weitergeleitet, auf der Sie sich mit Ihrem TeamViewer-Konto anmelden müssen.

Nach der Anmeldung haben Sie das AppTec360 MDM autorisiert, dieses Konto zu verwenden. Nachdem Sie dies bestätigt haben, müssen Sie ein paar Sekunden warten und das Konto ist verbunden.


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


TeamViewer
authorization request

TeamViewer QuickSupport installieren

Fügen Sie die App "TeamViewer QuickSupport" zu den obligatorischen Apps Ihres Geräte- oder Gruppenprofils hinzu und klicken Sie auf "Jetzt zuweisen". Warten Sie, bis die App auf dem Gerät installiert ist.

Wenn Sie versuchen, auf ein Gerät zuzugreifen, auf dem die App nicht installiert ist, wird sie installiert oder Sie werden aufgefordert, sie zu installieren, je nach Gerätekonfiguration.

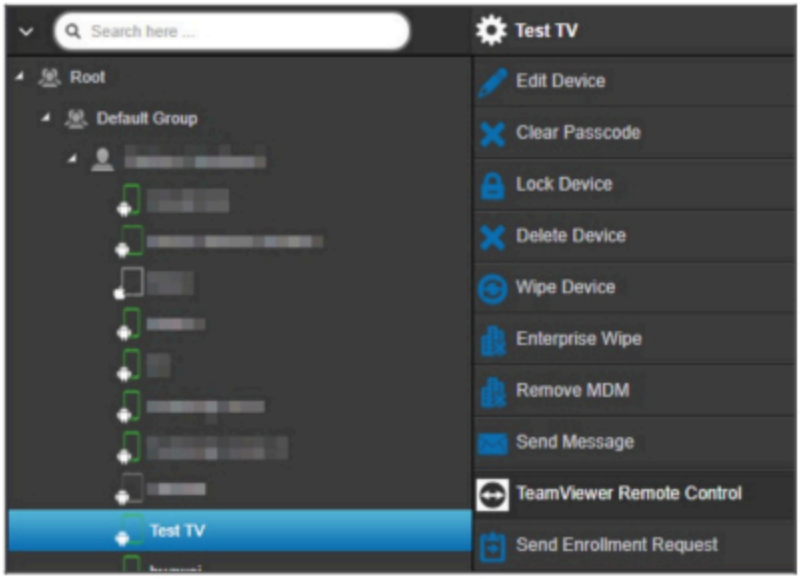
Ihr Gerät fernsteuern

Um Ihr Gerät fernzusteuern, wählen Sie das Gerät aus, klicken Sie auf das Rad und wählen Sie "TeamViewer Remote Control".

Wenn es bereits eine aktive Sitzung gibt, können Sie entweder die alte Sitzung verwenden oder eine neue erstellen.

Bestätigen Sie, dass Sie eine neue TeamViewer-Sitzung erstellen möchten.

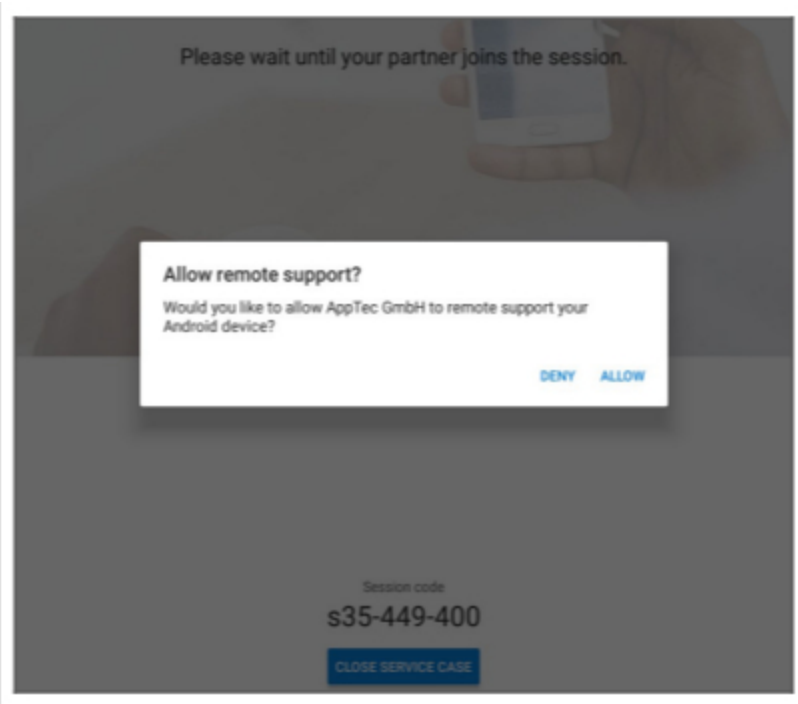
Nach ein paar Sekunden erhalten Sie einen Link für Ihre TeamViewer-Sitzung. Sie können auf "Start" klicken, um diesen Link in einem neuen Fenster zu öffnen.


Search here ...
Root
Default Group
Test TV
Test TV
Edit Device
Clear Passcode
Lock Device
Delete Device
Wipe Device
Enterprise Wipe
Remove MDM
Send Message
TeamViewer Remote Control
Send Enrollment Request


Remote Control
Supporter URL: https://get.teamviewer.com/v13/
Click on "Start" to open the TeamViewer Remote Control in a new window.
Cancel
Start

Dieser Link öffnet Ihr installiertes TeamViewer und verbindet Sie mit Ihrem Gerät.

Jetzt müssen Sie die Verbindung auf dem Gerät selbst bestätigen, um es fernzusteuern.

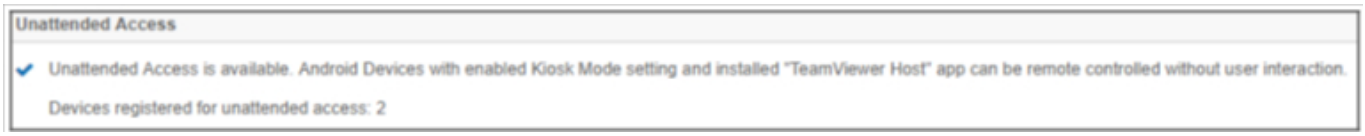


Wenn Sie iOS verwenden, erhalten Sie eine Meldung im AppTec360 MDM Client. Mit dieser Verbindung wird das Gerät der Fernsitzung beitreten. Je nach den Benachrichtigungseinstellungen des Geräts ist es möglich, dass Sie keine Benachrichtigung erhalten und den AppTec360 MDM Client manuell öffnen müssen.

Auf einigen Android-Geräten (z.B. Samsung) ist es erforderlich, eine zusätzliche App als Addon zu installieren. Die TeamViewer-App auf dem Gerät wird Sie darüber informieren, wenn dies auf Ihrem Gerät erforderlich ist.

Unbeaufsichtigter Zugang

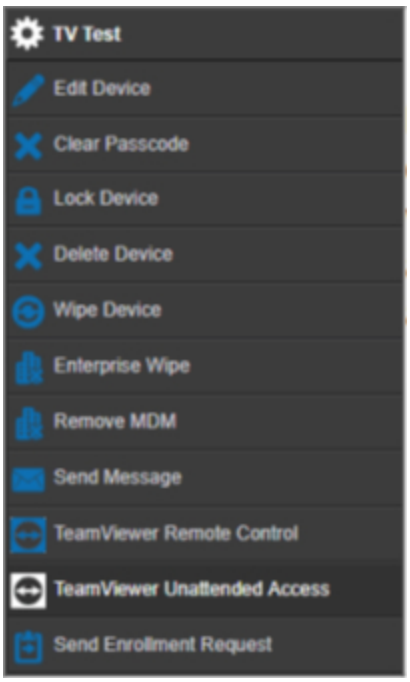
Hinweis: Unbeaufsichtigter Zugriff ist nur auf Android-Geräten möglich.



Sie können sich nur dann mit Ihren Geräten verbinden, ohne die Verbindung auf dem Gerät zu akzeptieren, wenn Ihr TeamViewer-Konto eine "Tensor" oder "Corporate" Lizenz verwendet.

Sie können dies, nachdem Sie Ihr Konto verknüpft haben, unter "Allgemeine Einstellungen" überprüfen.

Um den unbeaufsichtigten Zugriff zu nutzen, müssen Sie die App "TeamViewer Host" installieren und in Ihrem Profil unter "Kioskmodus & Launcher" die Option "Unbeaufsichtigten Zugriff aktivieren" aktivieren. Bitte beachten Sie, dass dies nur möglich ist, wenn Sie den Kioskmodus verwenden.



Jetzt können Sie den unbeaufsichtigten Zugriff auswählen, indem Sie Ihr Gerät auswählen und auf das Rad klicken. Dadurch werden Sie mit Ihrem Gerät verbunden, ohne dass eine Bestätigung auf dem Gerät selbst erforderlich ist. Bitte beachten Sie, dass es einige Augenblicke dauern kann, bis Sie den Link zum Zugriff auf Ihr Gerät erhalten.

Splashtop

Wenn Sie die Option Splashtop aktivieren, sehen Sie die Splashtop-Konfigurationsoptionen in Ihren Profilen.

Um Splashtop zu verwenden, müssen Sie den Splashtop Streamer (com.splashtop.streamer.csrs) als obligatorische App in Ihrem Profil festlegen. Danach können Sie die Splashtop-Konfiguration in Ihrem Profil unter "Fernsteuerung" aktivieren. Wenn Sie dies aktivieren, wird die Splashtop Streamer-App konfiguriert. Wenn Sie Splashtop Streamer verwenden, aber nicht in Kombination mit dem MDM, sollten Sie dies auslassen.

In Ihrem Profil unter "Fernsteuerung" müssen Sie auch einen Einsatzcode festlegen. Gehen Sie zu https://my.splashtop.com und melden Sie sich bei Ihrem Splashtop-Konto an. Klicken Sie auf "Computer hinzufügen" und kopieren Sie den 12-stelligen Bereitstellungscode von der angezeigten Seite.

Ohne den Deploy Code ist die Fernsteuerung NICHT möglich.

Danach können Sie mit der rechten Maustaste auf Ihr Gerät klicken und eine Remote Session starten, indem Sie auf "Splashtop Remote Control" klicken.

Sim Karten Verwaltung

CSV-Massenimport

Hier erhalten Sie einen Überblick über die Ihnen zugewiesenen Sim-Karten und alle Informationen zu diesen Karten. Dies hilft Ihnen, alle Informationen, nicht nur über Ihre Geräte, sondern auch über Ihre Sim-Karten in einem System zu haben.

HINWEIS: Dies ist eine manuelle Verwaltung/Dokumentation. Aufgrund der Datenschutz-/Sicherheitsmechanismen der Betriebssysteme ist es nicht möglich, diese Daten automatisch von den Geräten zu erhalten.

Sie können diese Liste auch ex- und importieren als CSV.

Transportunternehmen & Tarif

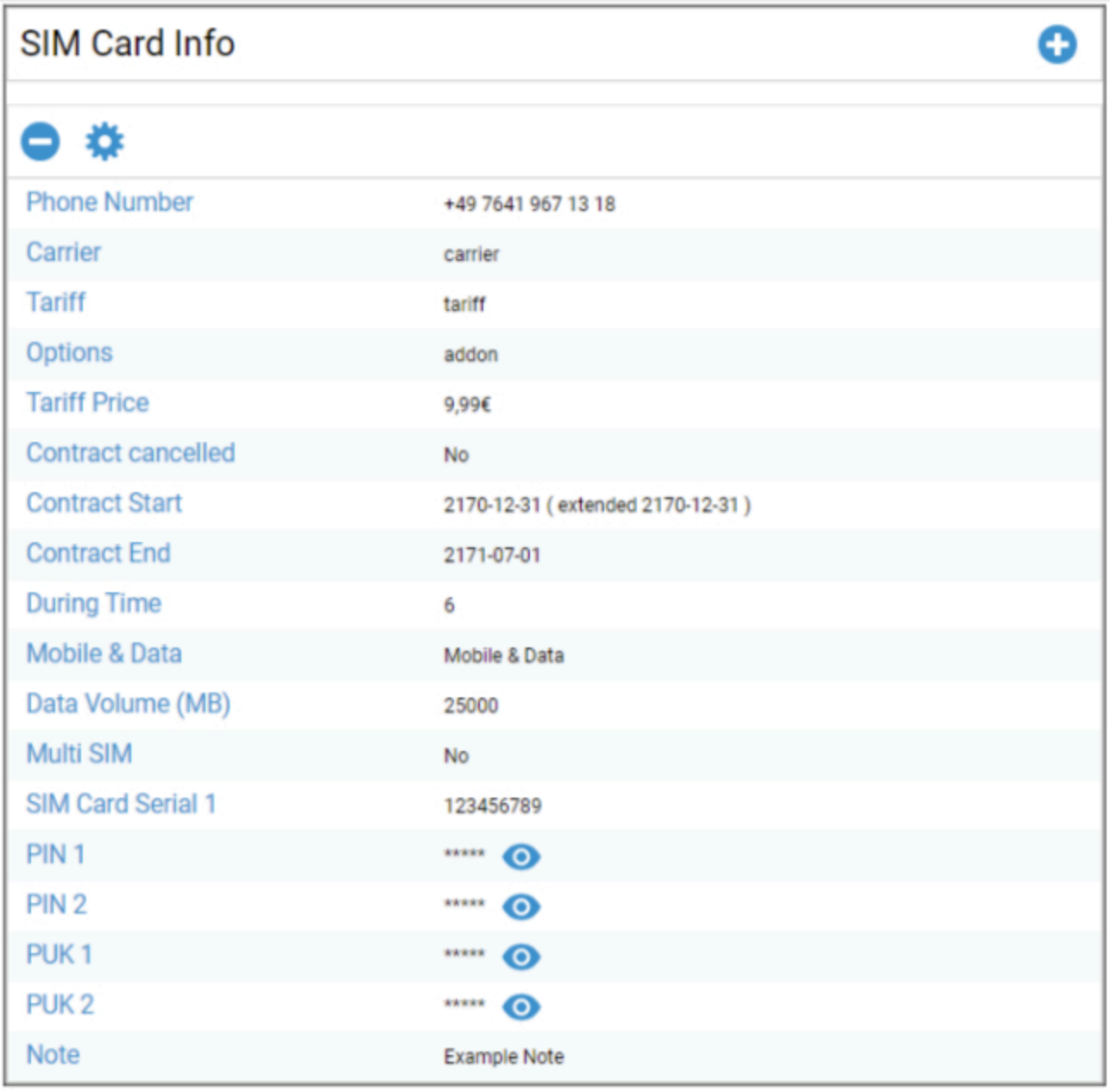
Um eine Sim-Karte hinzuzufügen, klicken Sie zunächst auf die Schaltfläche zum Hinzufügen eines oder mehrerer Anbieter.

Klicken Sie anschließend auf das "+" bei "Tarifinformationen", um einen Tarif zu einem Anbieter hinzuzufügen.

Optional können Sie unten optionale Add-Ons hinzufügen, wenn Sie so etwas haben.

Damit ist alles vorbereitet, was Sie zum Hinzufügen einer Sim-Karte benötigen. Sim-Karten sind derzeit einem Benutzer zugewiesen. Gehen Sie daher zur Mobilen Verwaltung, wählen Sie einen Benutzer aus und gehen Sie zu "Simkartenübersicht".

Hier sehen Sie die Sim-Karten dieser Benutzer. Wenn es einen gibt, können Sie ihn bearbeiten oder entfernen. Benutzer können mehrere Sim-Karten haben.

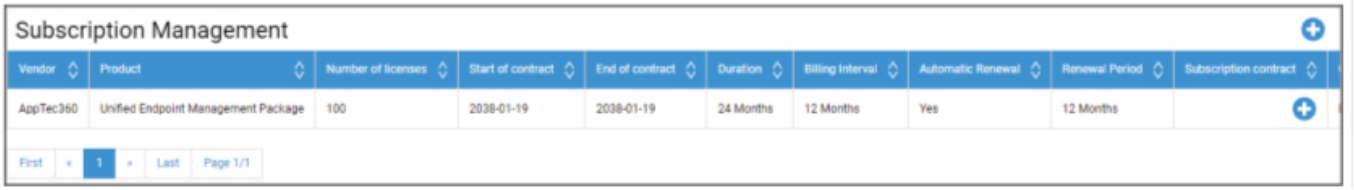


Klicken Sie auf das "+", um eine Sim-Karte hinzuzufügen und fügen Sie alle erforderlichen Informationen hinzu. Diese Sim-Karten werden auch in der Liste all Ihrer Sim-Karten unter Allgemeine Einstellungen → Sim-Kartenverwaltung aufgeführt.

Abonnement-Verwaltung

Abonnement-Verwaltung

Hier können Sie laufende Abonnements und deren Details dokumentieren und auch verschiedene Dateien speichern, z.B. den unterzeichneten Vertrag, das Kündigungsschreiben, usw. Sie können auch Erinnerungen einrichten, die Sie per E-Mail vor Ablauf des Abonnements daran erinnern und sich vielleicht automatisch verlängern.



Klicken Sie auf das "+" am oberen Rand, um ein Abonnement hinzuzufügen. Sie können so viele Abonnements hinzufügen, wie Sie möchten.

Klicken Sie auf das "+" in den verschiedenen Feldern, um Dateien zu diesem Abonnement hochzuladen. Sie können technisch gesehen jeden Dateityp hochladen, aber beachten Sie, dass nicht jeder Dateityp im Browser angezeigt werden kann.

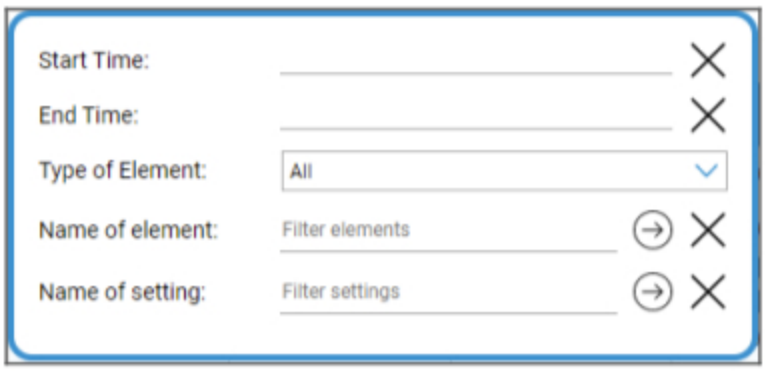
Allgemeines Audit-Protokoll

Audit-Protokoll

Hier finden Sie ein allgemeines Audit-Protokoll, das alle vorgenommenen Änderungen anzeigt. Während das Audit-Protokoll eines Benutzers oder einer Gruppe nur Änderungen anzeigt, die diesen Benutzer oder diese Gruppe betreffen, wird hier JEDE Änderung angezeigt, die irgendwo in der Konsole vorgenommen wurde.

Sie können sehen, was geändert wurde, von wem, wann und wo. In einigen Fällen können Sie den Eintrag auch erweitern, um weitere Details zu sehen.

Sie können auf den Benutzer oder auf den Eintrag in "Pfad / Typ" klicken, um zu dem Ort zu gelangen, an dem die Änderung vorgenommen wurde.



Oben rechts können Sie auch einen Filter definieren, der Ihnen helfen kann, bestimmte Änderungen in einer Umgebung zu finden, in der viele Änderungen stattfinden.

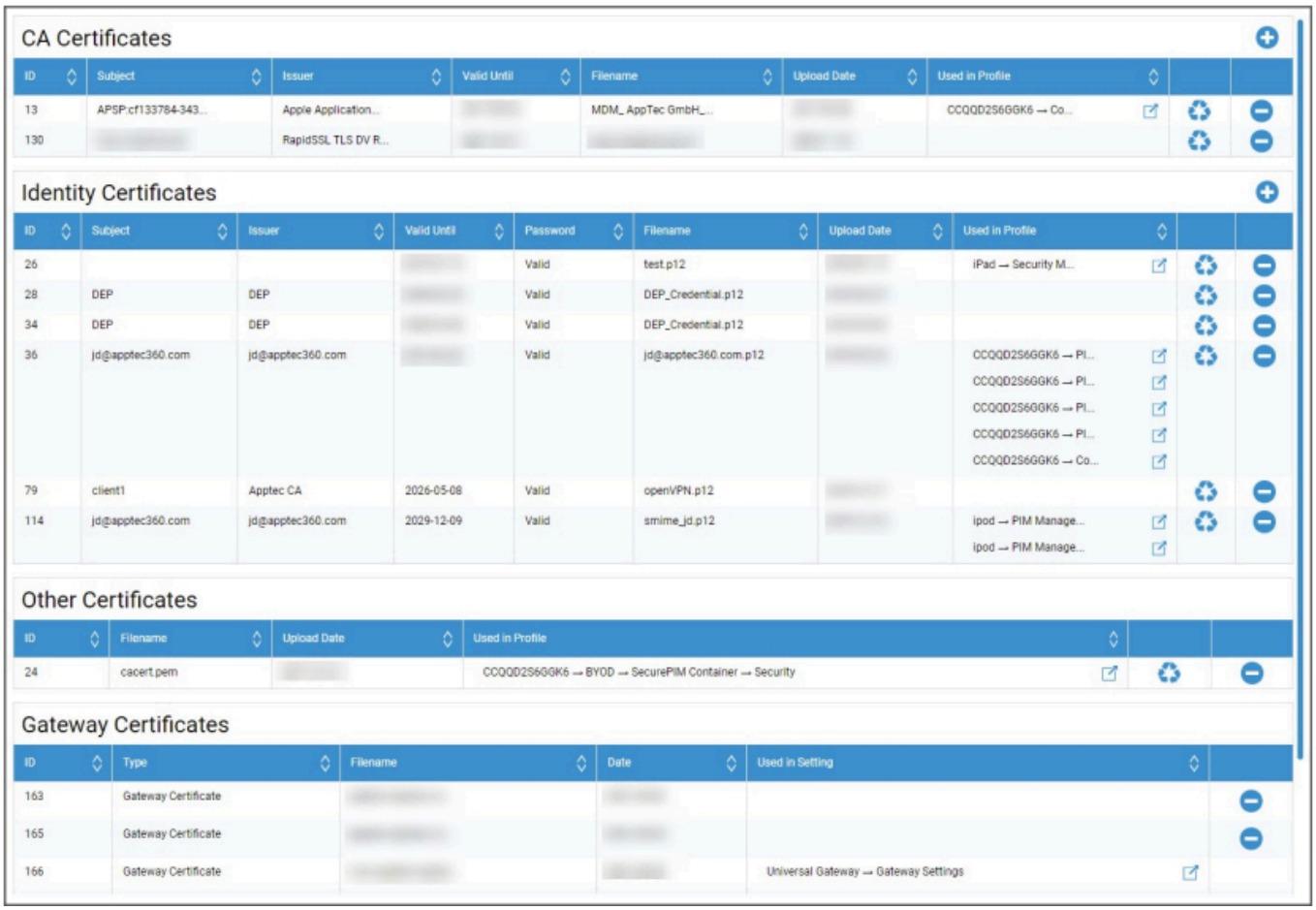
Audit Log Einstellungen

Die "Aufbewahrungsfrist für Audit-Protokolle" legt fest, wie lange die Audit-Protokolle aufbewahrt werden sollen, bevor sie gelöscht werden.

Zertifikat Management

Hier erhalten Sie einen Überblick über alle hochgeladenen und in der Konsole verwendeten Zertifikate. Dies ist nur ein Überblick. Die eigentliche Konfiguration für z.B. Wi-Fi-Zertifikate erfolgt weiterhin im Profil an der entsprechenden Stelle.

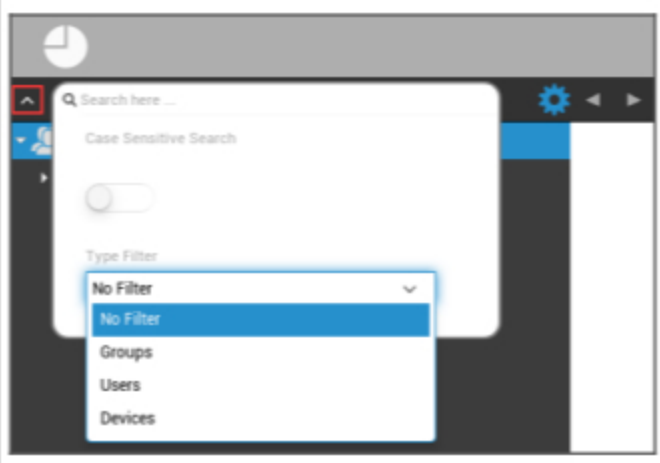
Hier können Sie auch Zertifikate entfernen oder aktualisieren, was sich automatisch auf die betroffenen Profile auswirkt. Klicken Sie auf die Info unter "Im Profil verwendet", um zu sehen, wo genau ein Zertifikat noch zugewiesen ist.



Mobile Management

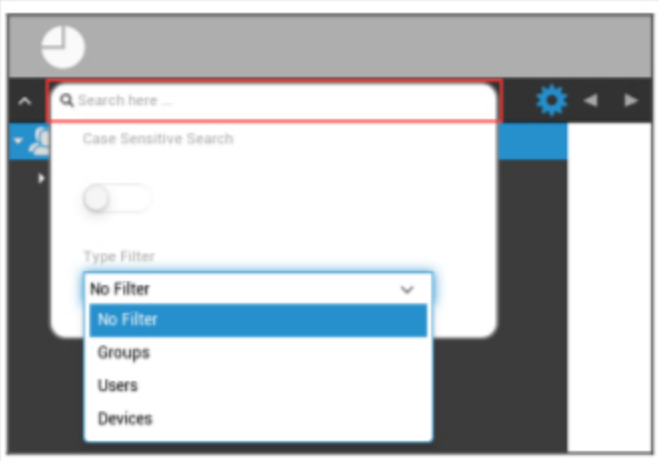
Bildschirm für die mobile Verwaltung

Gerätefilter



Mit einem Klick in der oberen linken Ecke des Bildschirms finden Sie eine Vielzahl von Filtern für die Anzeige von Geräten.

Suchfenster



Im Suchfenster können Sie alle Geräte und/oder Benutzer mit einem bestimmten Schlüsselwort suchen.

Optionen Getriebe

Nachdem Sie auf das entsprechende Symbol geklickt haben, wird eine Liste der Optionen angezeigt, die Ihnen zur Verfügung stehen.

Diese ändern sich mit jedem aktuellen Fenster und werden in den jeweiligen Kapiteln erläutert.

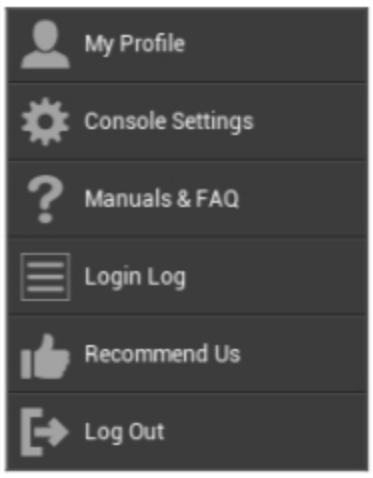
Navigationspfeile

Mit einem Klick auf den Pfeil nach links gelangen Sie auf die vorherige Seite.

Danach gelangen Sie mit einem Klick auf den Pfeil nach rechts zu der Seite, die Sie gerade verlassen haben.

Verwaltung Konto-Einstellungen

Wenn Sie wie oben auf die E-Mail-Adresse klicken, wird das folgende Menü angezeigt:



Mein Profil	Bearbeiten Sie die Details des Administratorkontos
Konsolen-Einstellungen	Konfigurieren Sie die Konsoleneinstellungen für das Admins-Konto
Handbücher & FAQ	Sehen Sie sich die Seite "Handbücher & FAQ" unter "Allgemeine Einstellungen" an.
Login-Logbuch	Zugriff auf das "Login Log"
Empfehlen Sie uns	Sehen Sie sich die Seite "Uns empfehlen" unter "Allgemeine Einstellungen" an.
Abmelden	Melden Sie sich von der MDM-Konsole ab

Benutzerinformationen

Hier können Sie die Kontodaten des aktuell angemeldeten Administrators bearbeiten.

Benutzername	Nutzername und/oder E-Mail-Adresse des Kontos
Name	Vorname des Administrators
Nachname	Nachname des Administrators
Login-Name	Anmeldename des Administrators
eMail-Adresse	E-Mail Adresse des Administrators
Alternative eMail-Adresse	Alternative E-Mail-Adresse des Administrators
Bild	Profilbild
Telefon Nummer	Telefonnummer des Administrators
Mobilnummer	Handynummer des Administrators
Telefon Durchwahl	Telefon-Durchwahl
Standort	Standort
Position	Position im Unternehmen
Benutzergruppe	Wählen Sie, welcher Benutzergruppe Sie das Administratorkonto zuweisen möchten
Kommentar	Einen Kommentar eingeben
Neues Passwort eingeben	Geben Sie das Passwort für eine Änderung des Passworts ein
Wiederholen Sie das neue Passwort	Wiederholen Sie das neue Passwort zur Bestätigung

Bitte beachten Sie, dass der Administrationszugang auch als lokales Benutzerkonto in der Hierarchiestruktur abgelegt werden kann. Ohne die Einrichtung eines zusätzlichen Administrators sollte dieser nicht gelöscht werden!

Konsolen-Einstellungen

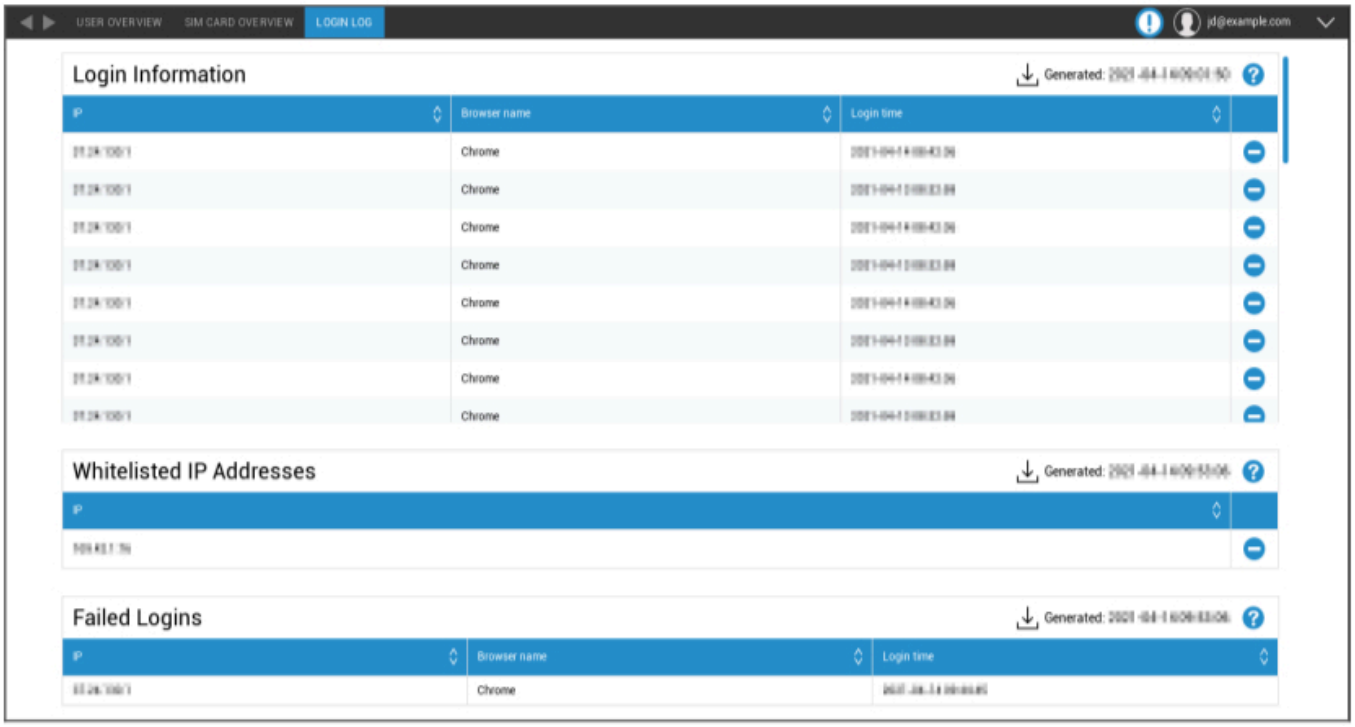
Hier können Sie die folgenden Konsoleneinstellungen für das Admins-Konto konfigurieren:

Verzeichnis Benutzeranzeigeoptionen	Definieren Sie, wie Benutzer in der Baumstruktur gekennzeichnet werden sollen
Verzeichnis Geräteanzeigeoptionen	Legen Sie fest, wie Geräte in der Baumstruktur beschriftet werden sollen
Zeitüberschreitung der Sitzung	Wenn der Benutzer in der angegebenen Zeit nichts unternimmt, wird er abgemeldet. Der Standardwert ist 60 Minuten. Bitte loggen Sie sich aus und melden Sie sich erneut an, nachdem Sie diese Einstellung geändert haben.
Zeitzone	Wählen Sie die verwendete Zeitzone
Zeitformat	Wählen Sie, wie Zeitstempel angezeigt werden sollen
Konsolensprache	Wählen Sie die Sprache, in der die Konsole angezeigt werden soll. Englisch und Deutsch sind verfügbar.
Hauptfarbe	Sie können eine Farbe festlegen, die als Basis für das Farbschema der Konsole verwendet werden soll. Sie können entweder den Farbwähler verwenden oder eine Farbe in HTML HEX-Notation eingeben. RGB-Formatoren wie 'rosa', 'gelb' funktionieren ebenfalls.
Befehl speichern	Die Tastenkombination zum Auslösen eines Speichervorgangs, ohne die Schaltfläche "Speichern" zu drücken.
Verwenden Sie die Zwei-Faktor-Authentifizierung	Aktivieren Sie die Verwendung der Zwei-Faktor-Authentifizierung bei der Anmeldung. Sie erhalten nach der Anmeldung eine E-Mail mit einem Code, den Sie eingeben müssen, um sich einzuloggen.
Zeitüberschreitung bei der Zwei-Faktoren-Authentifizierung	Legen Sie eine Zeitspanne fest, in der Sie nach einer bereits erfolgreichen Authentifizierung nicht nach einer Zwei-Faktor-Authentifizierung gefragt werden.
Verifizierungscode senden über	Der Verifizierungscode wird an die ausgewählten Optionen gesendet. Die Gerätemeldung wird in der AppTec360 MDM App auf allen Android- und iOS-Geräten, die Ihnen gehören, angezeigt.
Login-Nachricht nach dem Login senden	Wenn diese Option aktiviert ist, wird bei jeder Anmeldung von einer IP-Adresse, die nicht auf der Whitelist steht, eine E-Mail gesendet.

	Die E-Mail enthält Informationen über die Anmeldung (z.B. IP, Browser).

Login-Logbuch

Hier sehen Sie Informationen zu den Anmeldungen des aktuell angemeldeten Administratorkontos.



Informationen zur Anmeldung	Eine Liste mit den Logins des aktuell angemeldeten Administratorkontos, die von der Konsole aufgezeichnet wurden. Diese Liste zeigt alle Ihre erfolgreichen Anmeldungen der letzten 30 Tage.
IP-Adressen auf der Whitelist	Dies ist die Liste aller Ihrer IP-Adressen auf der Whitelist. Wenn Sie sich von einer IP einloggen, die hier aufgelistet ist, erhalten Sie die Login-Nachricht nicht. Sie können eine IP-Adresse zu dieser Liste hinzufügen, indem Sie auf die Schaltfläche neben einem Eintrag in der Liste "Anmeldeinformationen" oben klicken. Sie können eine IP-Adresse aus dieser Liste entfernen, indem Sie auf die Schaltfläche neben einem Eintrag in dieser Liste oder in der Liste "Anmeldeinformationen" oben klicken.
Fehlgeschlagene Anmeldungen	Dies ist eine Liste aller fehlgeschlagenen Anmeldeversuche der letzten 30 Tage. Wenn Sie innerhalb von 20 Minuten mindestens 3 Mal nicht das richtige Passwort eingegeben haben, erscheint ein Eintrag in dieser Liste. Sie werden auch über fehlgeschlagene Anmeldeversuche per E-Mail informiert.

Unternehmensverwaltung (Root-Node) in Mobile Management

Wenn Sie den Root-Node (erste Gruppe) erreicht haben, können Sie eine Reihe von Einstellungen für Ihr Unternehmen in Bezug auf die mobile Verwaltung vornehmen.

Eine Untergruppe erstellen	Erstellen Sie eine Untergruppe
Wurzelknoten umbenennen	Umbenennung des Root-Knotens (z. B. Ihr Firmenname)
Massenimmatrikulation	Registrieren Sie mehrere Geräte/Benutzer gleichzeitig
Massenzuweisung	Weisen Sie den jeweiligen Gruppen ein Profil zu, mit einem Blick
Schnelle App-Verwaltung	Senden Sie (Un-)Installationsanfragen für eine Anwendung an die Geräte der jeweiligen Gruppen
CSV-Benutzer-Import	Benutzer aus CSV in die jeweilige Gruppe importieren

Eine Untergruppe erstellen

Mit "Eine Untergruppe erstellen" können Sie eine zusätzliche Untergruppe erstellen.

Sie können festlegen, unter welcher Gruppe die Untergruppe zugeordnet werden soll.

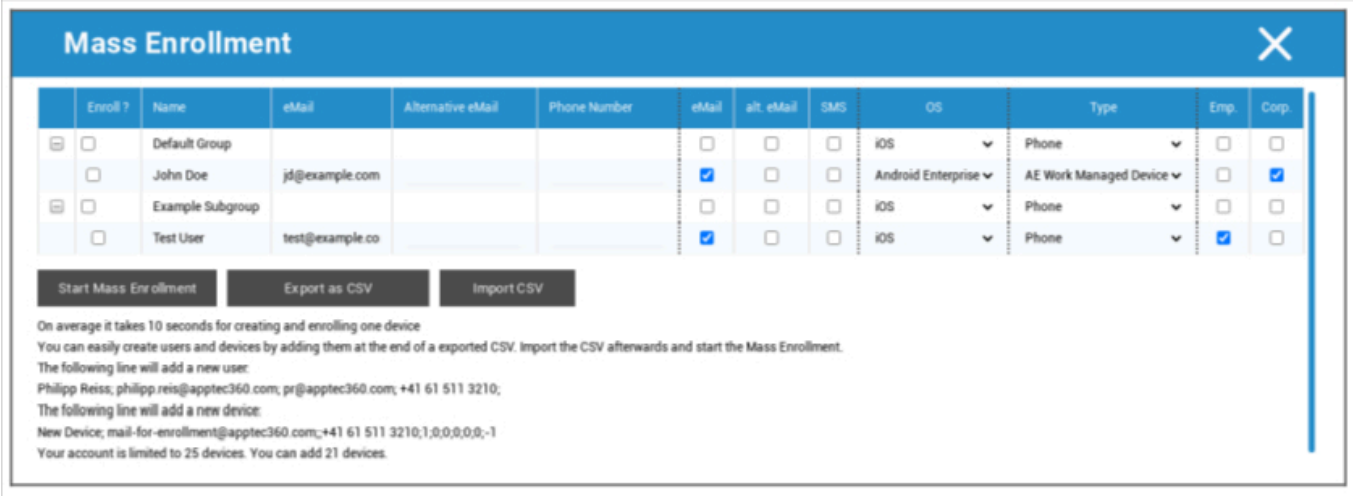
(Standardmäßig wird eine neue Gruppe erstellt, die als Untergruppe im Stammknoten zugewiesen wird)

Wurzelknoten umbenennen

Hier können Sie Ihren Root-Namen umbenennen. Es ist üblich, dass in diesem Fall der Firmenname verwendet wird.

Massenimmatrikulation

Mit der "Massenregistrierung" können Sie mehrere Geräte und Benutzer registrieren.



Sie können direkt auswählen, auf welche Weise der Benutzer die Anmeldung erhalten soll (eMail; alternative eMail; SMS)

Je nachdem, welches Gerät der Benutzer erhalten wird (iOS, Android, Windows Phone), können Sie das hier direkt markieren.

Auch die Unterscheidung, ob es sich um ein Smartphone oder ein Tablet handelt, kann hier konfiguriert werden, was Sie mit einem Häkchen korrekt auswählen müssen.

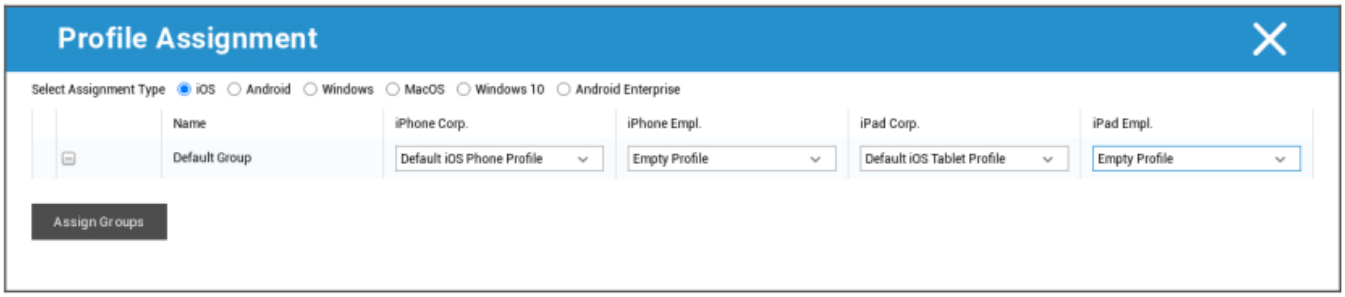
In einem letzten Schritt können Sie feststellen, ob es sich um ein Firmengerät oder ein privates Gerät (BYOD) handelt.

Mit der Option "Als CSV exportieren" können Sie die Informationen als CSV-Datei exportieren. Im Gegenzug können Sie die CSV-Datendatei auch mit "CSV importieren" importieren. Die Datei sollte wie das folgende Beispiel aussehen:

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

Massenzuweisung

Unter Massenzuweisung können Sie allen Gruppen ein Profil zuweisen, dies ist unterteilt in iOS - Android - Windows - MacOS - Windows 10 - Android Enterprise

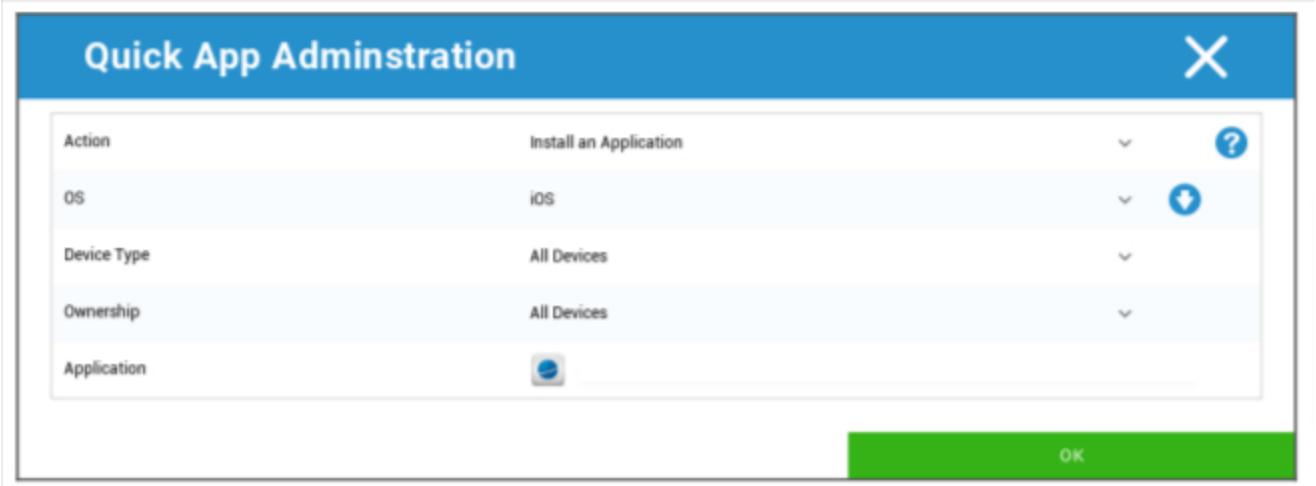


Windows - MacOS - Windows 10 - Android Enterprise

Schnelle App-Verwaltung

Unter App-Schnellverwaltung können Sie Installations- oder Deinstallationsanfragen für eine bestimmte Anwendung an ein Betriebssystem Ihrer Wahl senden.

Sie können auch festlegen, ob die Anfrage an alle Gerätetypen des ausgewählten Betriebssystems oder nur an einen bestimmten Gerätetyp gesendet werden soll.



CSV-Benutzer-Import

Importieren Sie Benutzer aus CSV in die jeweilige Gruppe.

Mit "CSV-Vorlage herunterladen" können Sie eine CSV-Vorlagendatei exportieren, die Sie ausfüllen können (oder als Referenz verwenden können).

Sie können auch die Optionen "Rollen-IDs anzeigen" und "Gruppen-IDs anzeigen" als Referenz verwenden, um Ihre eigene CSV-Datei zu erstellen.

Die CSV-Datei kann mit "CSV hochladen" in das MDM hochgeladen werden.

Als letzten Schritt können Sie den Import starten, indem Sie auf "Import starten" klicken.

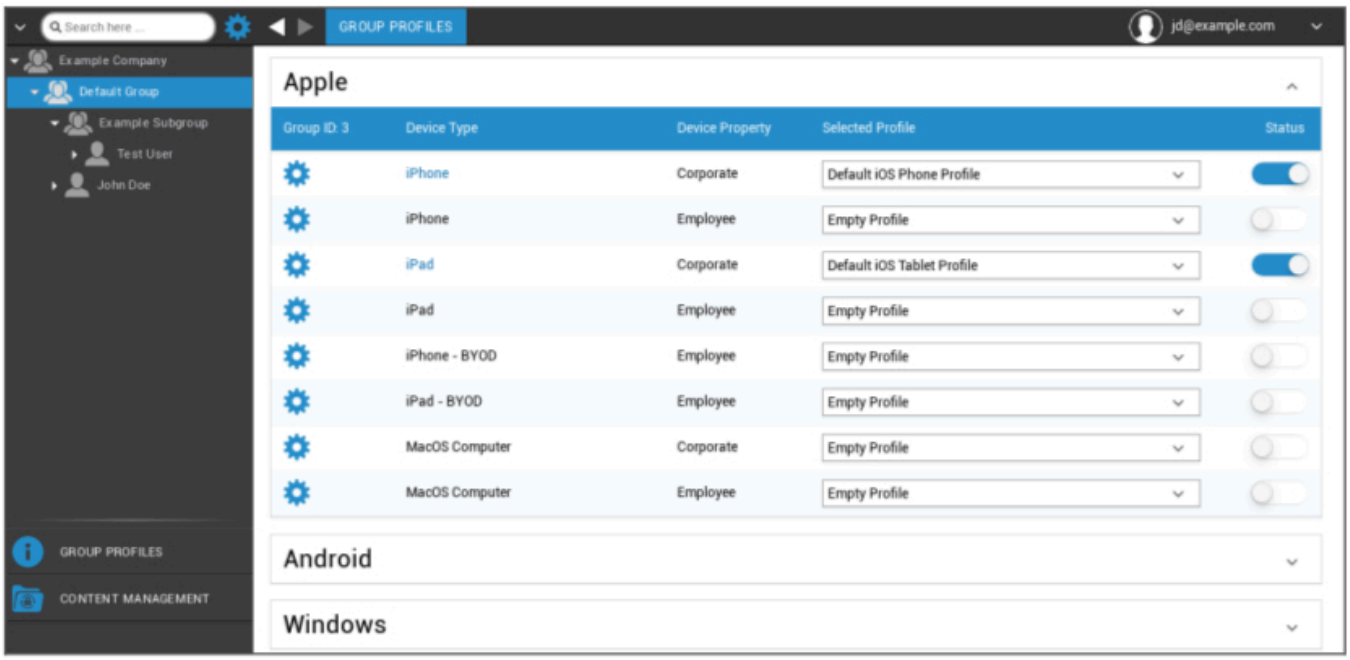
Gruppenverwaltung in Mobile Management

Ein Klick auf die Übersicht zeigt die verschiedenen Konfigurationsprofile für die jeweiligen Plattformen an.

Ein Profil enthält alle Einstellungsmöglichkeiten, die mit AppTec360 im Vorfeld auf dem Endgerät eingerichtet werden können. Auf jeder Plattform können Sie Profile für Firmengeräte (Corporate) oder Bring-Your-Own-Device-Geräte (Employee) erstellen.

Um Konfigurationen für Gerätegruppen zu unterscheiden, zum Beispiel nach Standort oder Funktion, empfiehlt es sich, mehrere Untergruppen zu erstellen.

Bitte beachten Sie die Profilverwaltung in Mobile Management



Mit dem Zahnradmenü richten Sie eine Vielzahl von Einstellungen für die jeweilige (Unter-)Gruppe ein.

Eine Untergruppe erstellen	Untergruppe für die jeweilige (Unter-)Gruppe erstellen
Ausgewählte Gruppe bearbeiten	Ausgewählte Gruppe bearbeiten
Ausgewählte Gruppe löschen	Ausgewählte Gruppe löschen
Massenimmatrikulation	Registrieren Sie viele Geräte/Benutzer auf einmal für das ausgewählte Profil
Massenzuweisung	Profile der aktuell ausgewählten Gruppe zuweisen
Eine Untergruppe erstellen	Untergruppe für die jeweilige (Unter-)Gruppe erstellen

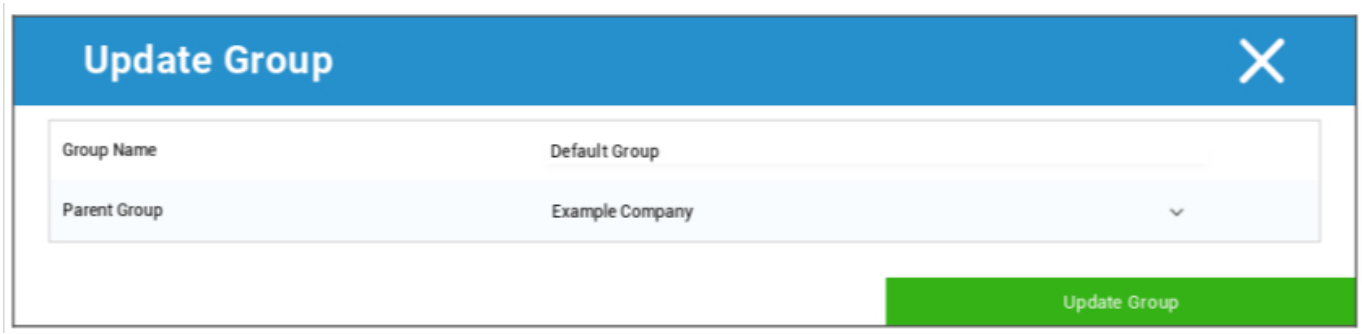
Einen Benutzer erstellen	Erstellen Sie einen Benutzer für die jeweilige (Unter-)Gruppe

Eine Untergruppe erstellen

Mit "Eine Untergruppe erstellen" können Sie eine zusätzliche Untergruppe erstellen.

Sie können festlegen, welcher Gruppe die Untergruppe zugewiesen werden soll (standardmäßig wird die Untergruppe der Gruppe zugewiesen, die gerade ausgewählt ist).

Ausgewählte Gruppe bearbeiten



Hier können Sie das Profil bearbeiten - hier sind die folgenden Einstellungen möglich:

- Gruppenname kann geändert werden
- Übergeordnete Gruppe kann geändert werden

Ausgewählte Gruppe löschen

Unter "Ausgewählte Gruppe löschen" werden Ihnen alle Benutzer und Geräte aufgelistet, die sich in der jeweiligen Gruppe befinden. Hier haben Sie die Möglichkeit, sie zu löschen.

Für einen Benutzer können Sie die folgenden Löschbefehle ausführen:

Benutzer löschen	Benutzer wird gelöscht
Benutzer in Gruppe verschieben:	Sie können den Benutzer in eine andere Gruppe verschieben (folgende Spalte, z.B. "Admins")

Für ein Gerät können Sie die folgenden Löschbefehle ausführen:

Wischen & Löschen	Gerät wischen und löschen
Aus dem System löschen	Gerät nur aus AppTec entfernen

Referenz: Massenimmatrikulation

Referenz: Massenzuweisung

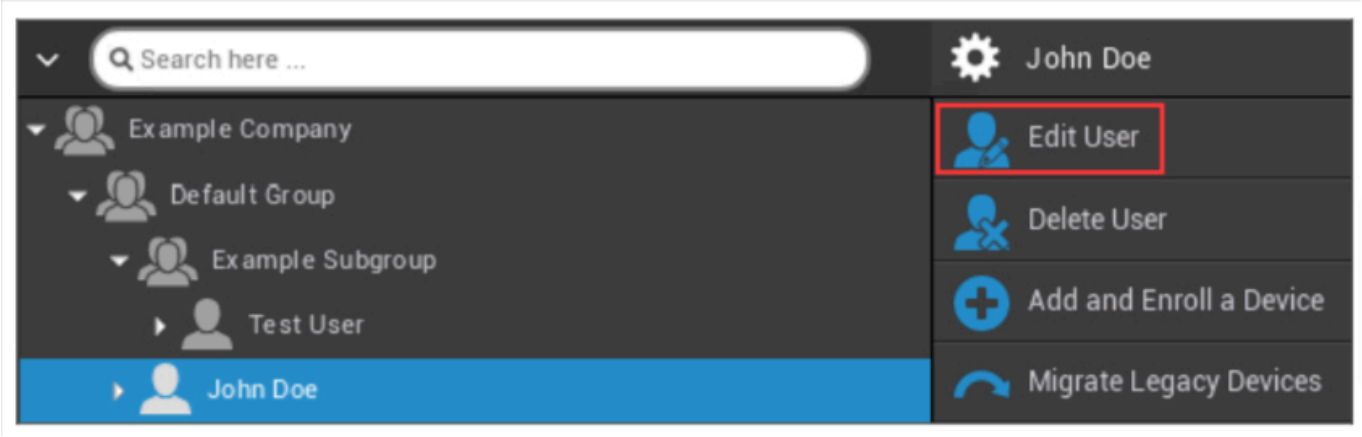
Einen Benutzer erstellen

Mit "Einen Benutzer erstellen" können Sie einen neuen Benutzer hinzufügen.

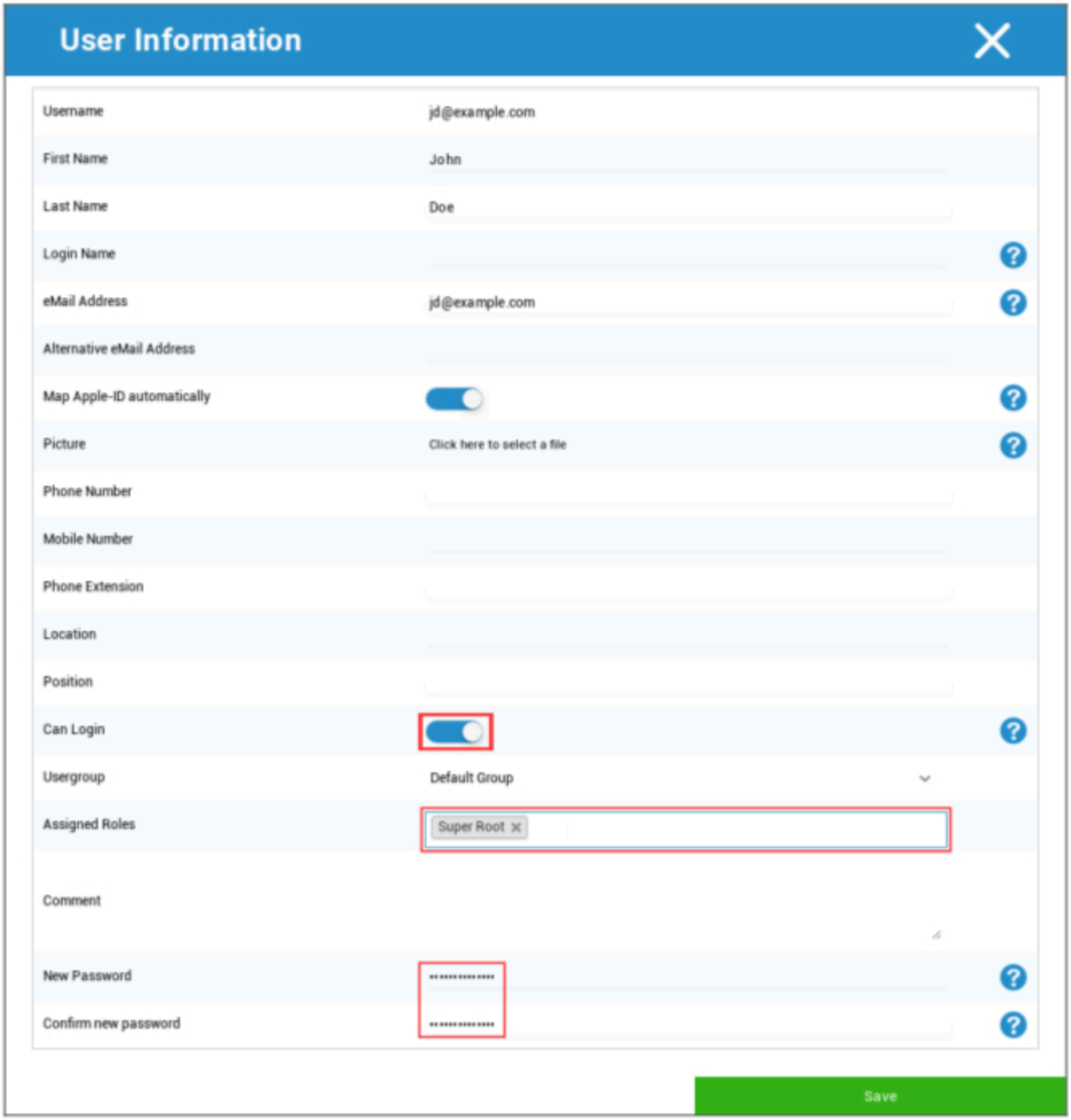
Erstellen Sie einen neuen Admin-Benutzer

Sie können einen Benutzer als Admin-Benutzer festlegen. Dadurch erhält er die Berechtigung, sich an der Konsole anzumelden und auch Benutzer/Gruppen/Geräte zu ändern.

Erstellen Sie einen normalen Benutzer oder verwenden Sie einen vorhandenen Benutzer. Wählen Sie den Benutzer, dem Sie Administratorrechte erteilen möchten, klicken Sie auf das Rad und wählen Sie "Benutzer bearbeiten":



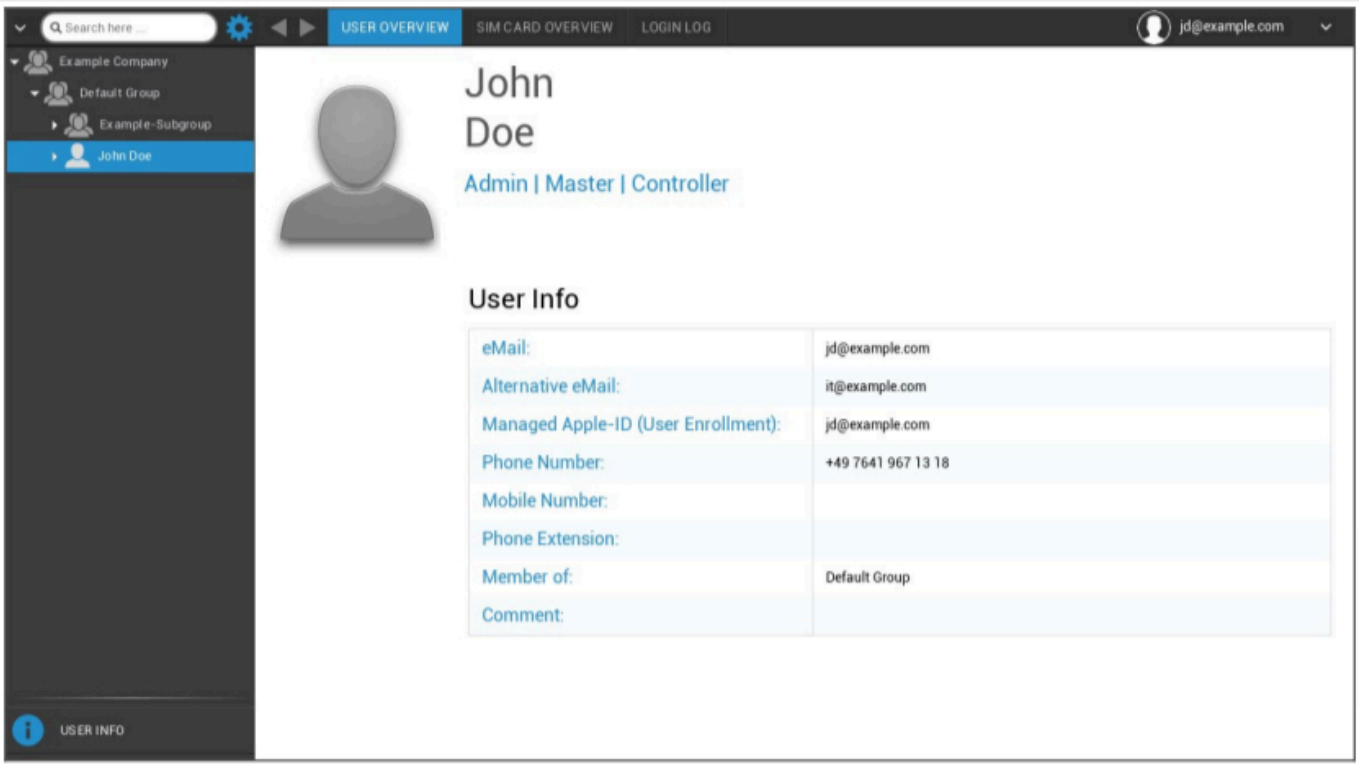
Aktivieren Sie den Schalter für "Kann sich anmelden", weisen Sie dem Benutzer die Rolle "Super-Root" zu und legen Sie ein Passwort fest.



Speichern Sie dies und der Benutzer kann sich nun mit seinem Benutzernamen und Passwort anmelden.

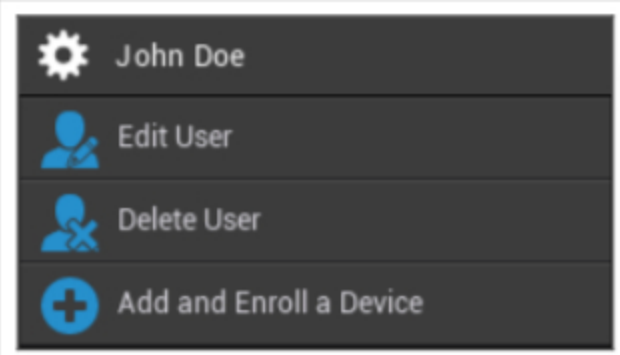
Benutzerverwaltung in Mobile Management

Wenn Sie einen bestimmten Benutzer auswählen, sehen Sie die folgende Übersicht:



Sie erhalten eine Übersicht über alle Informationen, die Sie zuvor unter "Benutzer erstellen" eingegeben haben.

Mit dem oben installierten Getriebe können Sie die folgenden Konfigurationen vornehmen:



Benutzer Name	Benutzername des ausgewählten Benutzers
Benutzer bearbeiten	Benutzer-Informationen bearbeiten
Benutzer löschen	Benutzer löschen

	• Aus dem System löschen = Das Gerät wird aus AppTec entfernt. • Wipe & Delete = Das Gerät wird auf die Werkseinstellungen zurückgesetzt und aus AppTec entfernt.
Hinzufügen und Registrieren eines Geräts	Registrieren Sie ein Gerät für den ausgewählten Benutzer

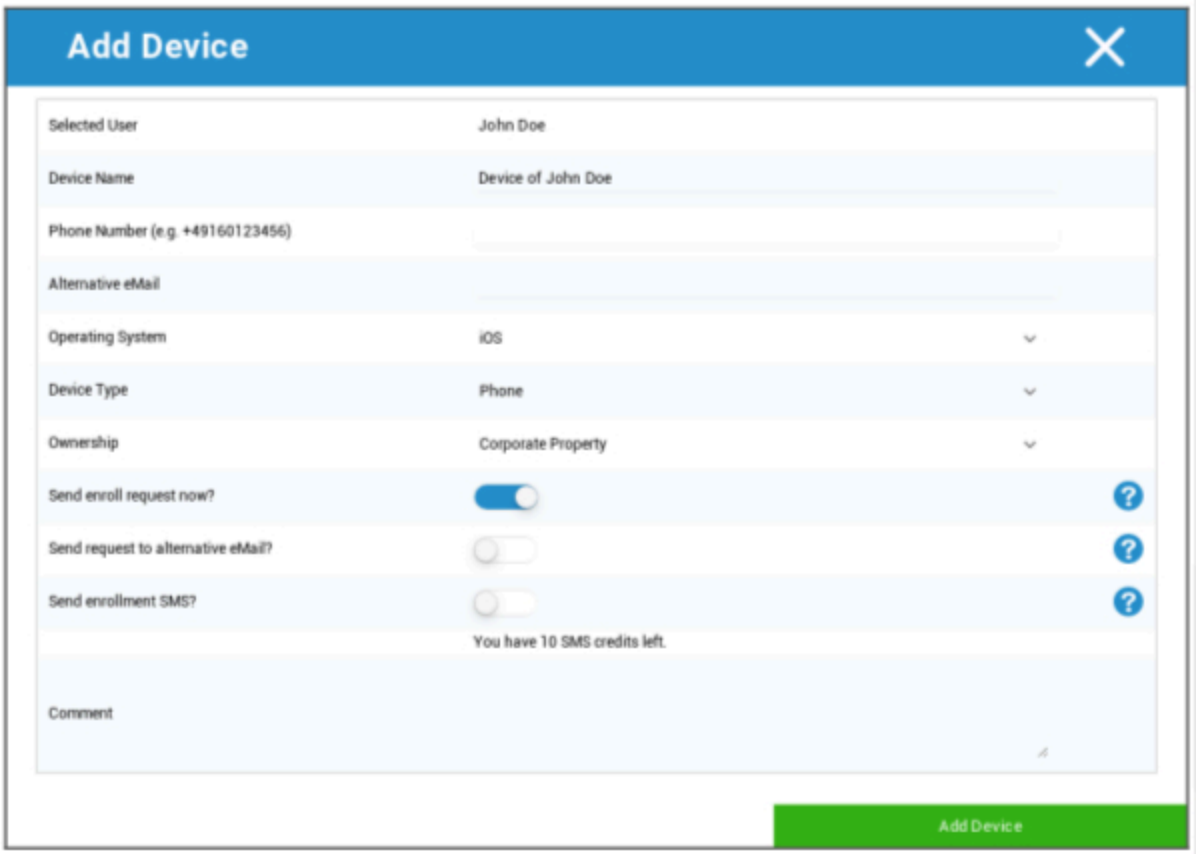
Bitte beachten Sie, dass der Administrationszugang auch als lokales Benutzerkonto in der Hierarchiestruktur abgelegt werden kann. Ohne die Einrichtung eines zusätzlichen Administrators sollte dieser nicht gelöscht werden!

Hinzufügen und Registrieren eines Geräts

Hier können Sie ein Gerät für die gewählte Verwendung auswählen.

Alternativ können Sie Geräte auch direkt in eine Gruppe aufnehmen. Klicken Sie dazu auf die Gruppe, klicken Sie auf das Rad und wählen Sie "Gerät hinzufügen und registrieren".

Sie sollten die folgende Übersicht sehen:



Je nachdem, welche Art von Gerät Sie registrieren möchten, müssen Sie die folgenden Konfigurationen vornehmen:

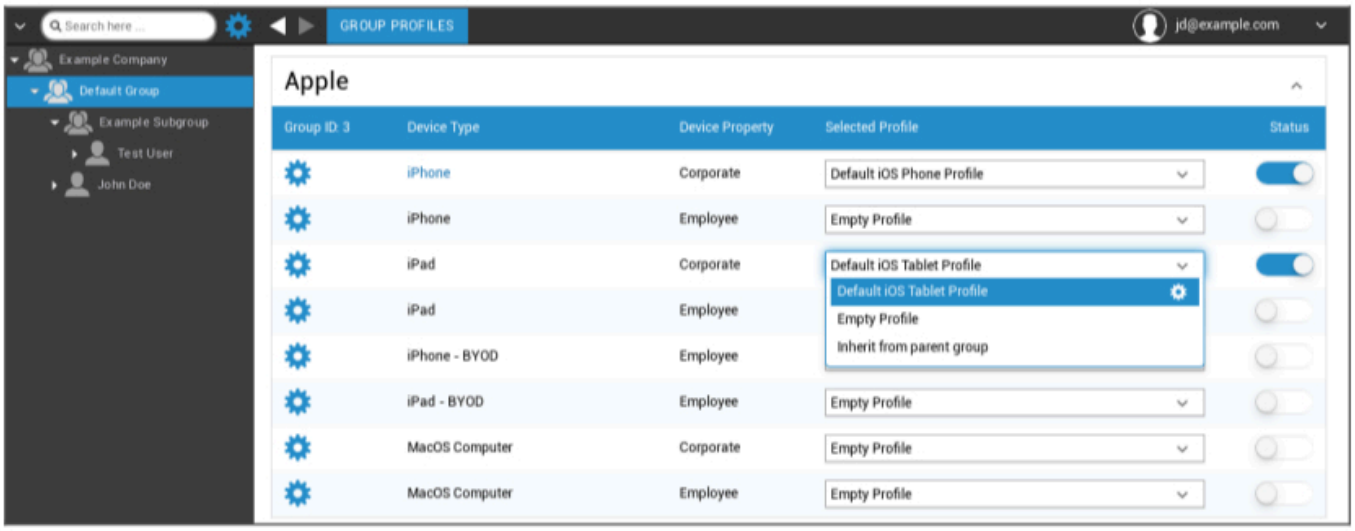
Ausgewählter Benutzer	Ausgewählter Benutzer (wird automatisch ausgefüllt)
Gerät Name	Wird automatisch ausgefüllt (Gerät für "Name des Benutzers") - kann aber geändert werden
Telefon Nummer	Telefonnummer, wird automatisch ausgefüllt (sofern sie vom Benutzer angegeben wurde) - hier kann sie jedoch hinzugefügt oder geändert werden
Alternative eMail	Alternative E-Mail, wird automatisch ausgefüllt (sofern sie vom Benutzer angegeben wurde) - hier kann sie jedoch hinzugefügt oder geändert werden
Besitzer des Geräts	Firmeneigentum = Firmengerät Eigentum des Mitarbeiters = BYOD-Gerät
Wählen Sie Operation System	Hier können Sie zwischen den folgenden Betriebssystemen wählen: • iOS • iOS BYOD (Benutzerregistrierung) • MacOS • Android Unternehmen • Android • Windows Mobile • Windows 10
Anfrage zur Registrierung senden?	Die E-Mail wird sofort an die Haupt-E-Mail-Adresse gesendet und der Benutzer wird aufgefordert, sein Gerät zu verbinden
Anfrage an alternative eMail senden?	Senden Sie die E-Mail zusätzlich oder ausschließlich (falls "Send enroll request?" deaktiviert wurde) an die alternative E-Mail-Adresse (die E-Mail unterscheidet sich von der "normalen" enroll Request E-Mail)
Anmelde-SMS senden?	Senden Sie eine Registrierungsanfrage per SMS (die "Telefonnummer" muss eingegeben werden)

Nachdem die Registrierungsanfrage gesendet wurde, wird das Gerät sofort angezeigt (rot markiert).

Sobald das Gerät erfolgreich verbunden wurde, wird es kurz darauf grün markiert und ist damit bereit, Einschränkungen, Apps usw. zu empfangen.

Profilverwaltung in Mobile Management

Nachdem Sie auf eine Gruppe geklickt haben, erhalten Sie eine Übersicht über alle zu konfigurierenden Geräteplattformen und die jeweils zugeordneten Profile.



	Führen Sie die Konfiguration für das ausgewählte Profil durch
Gerätetyp	Gerätetyp und/oder Modell
Geräteeigenschaft	Eigentümer des Geräts (Unternehmen = Firmeneigentum, Mitarbeiter = privates Mitarbeitergerät)
Ausgewähltes Profil	Ausgewähltes Profil (das Zahnrad öffnet den Konfigurationsdialog des Profils)
Status	Ein/Aus (das Profil ist aktiviert/deaktiviert)

Wenn Sie den Gang wählen, erhalten Sie die folgenden Optionen:

Ein Profil erstellen

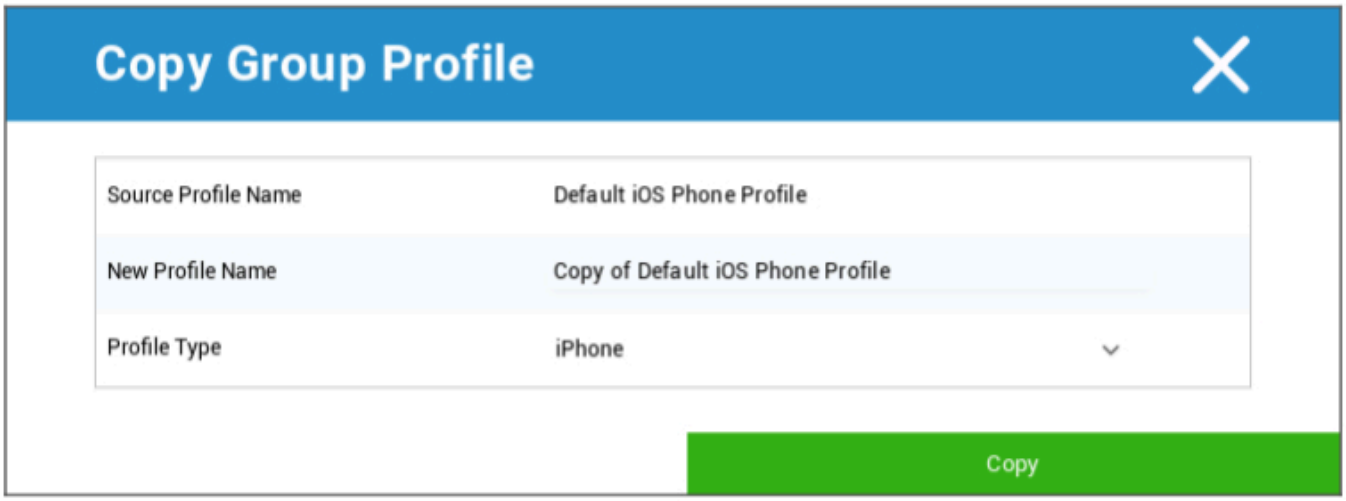
Sie können für jeden Eintrag und/oder jede Plattform ein neues Profil erstellen und konfigurieren. Nachdem Sie auf diesen Unterpunkt geklickt haben, wird das Profil sofort erstellt und Sie können sofort mit der Konfiguration des iOS, Android und Windows Phone beginnen.

Profil bearbeiten

Nachdem Sie auf "Profil bearbeiten" geklickt haben, gelangen Sie zur Konfigurationsanzeige für das jeweilige Profil, wo Sie die Konfigurationen einstellen können.

Profil kopieren

Mit Hilfe der Funktion "Profil kopieren" können Sie die Einstellungen/Konfigurationen aus einem bereits vorhandenen Profil kopieren und einem neuen Profil hinzufügen.

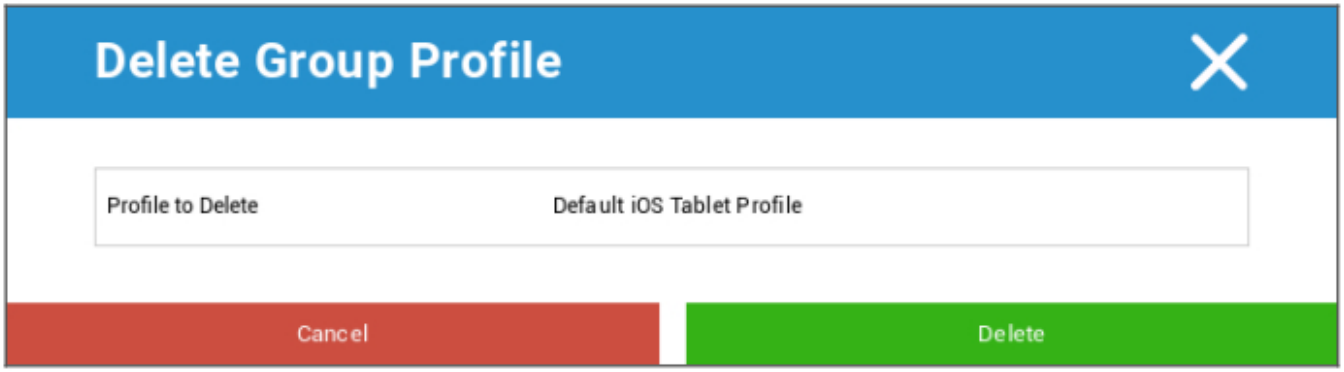


Quelle Profil Name	Name des Profils, das kopiert werden soll
Neuer Profilname	Name des neuen Profils
Profil Typ	Profiltyp (Telefon/Tablet)

Sobald Sie auf "Kopieren" klicken, wird das Profil erstellt und kann nun der Gruppe zugewiesen werden

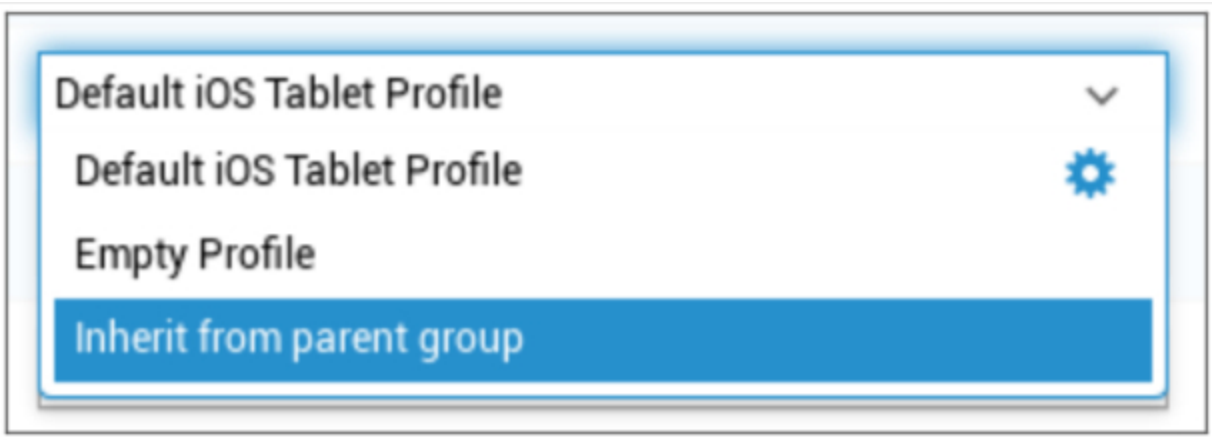
Profil löschen

Hier können Sie ein Profil dauerhaft löschen. Bitte beachten Sie, dass während des Löschvorgangs und des anschließenden "Jetzt zuweisen"-Prozesses für das Profil die Konfiguration auf den jeweiligen Geräten einer betroffenen Gruppe verschwindet und nicht wiederhergestellt werden kann!


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

Vererbung von Profilen

Bei der Auswahl der Profile ist die Option "Von der übergeordneten Gruppe erben" verfügbar.



Wenn das Profil aktiviert ist, wird das Profil der übergeordneten Gruppe für das jeweils ausgewählte Gerät (und den entsprechenden Gerätetyp) verwendet. Bitte beachten Sie auch, dass Änderungen an diesem Profil möglicherweise zahlreiche Gruppen betreffen können.

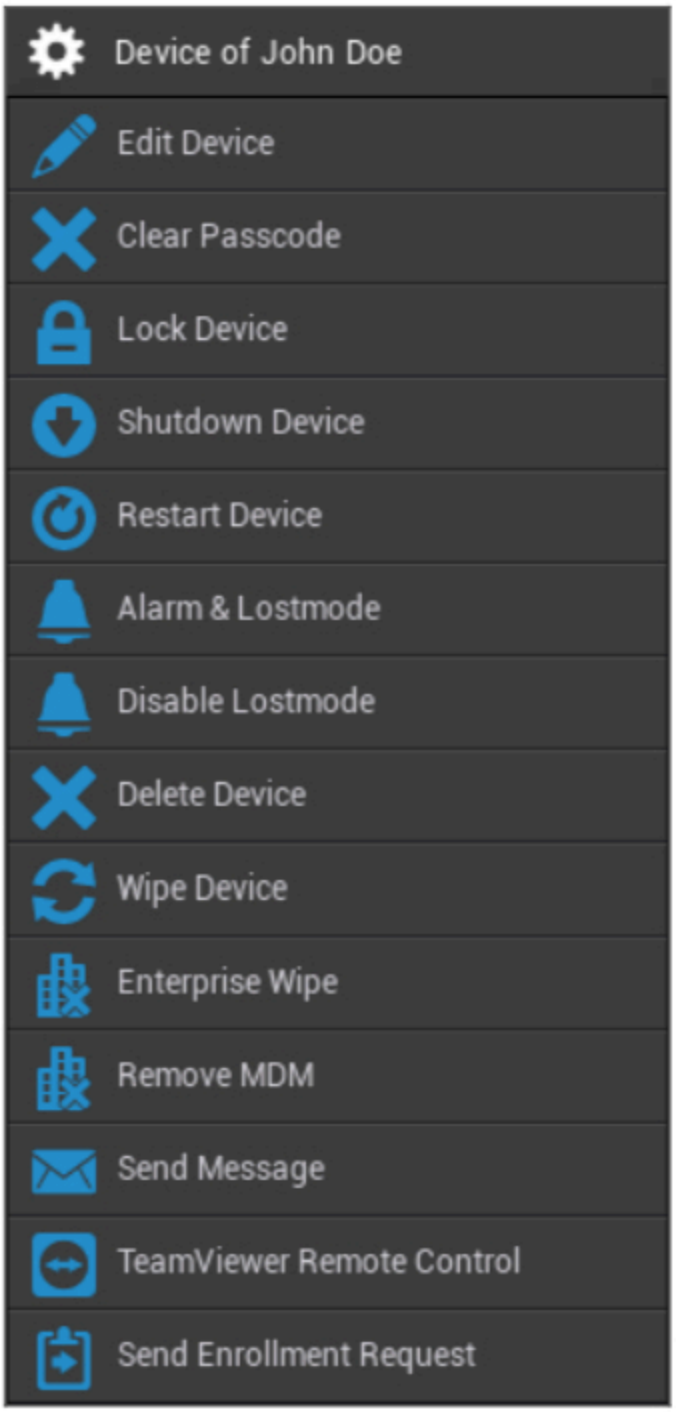
Diese Konfiguration wird als Standardwert festgelegt, wenn eine neue Untergruppe erstellt wird.

Es gibt auch die Konfiguration "Leeres Profil", die einem leeren Profil entspricht, was bedeutet, dass auf dem Endbenutzergerät keine neuen Konfigurationen vorgenommen werden.

Geräteverwaltung in Mobile Management

Wenn Sie ein Gerät auswählen, können Sie über das "Zahnrad" eine Reihe von Aufgaben ausführen. Diese sind je nach Betriebssystemplattform (iOS, Android Enterprise, Android, Windows Mobile, Windows 10) unterschiedlich.

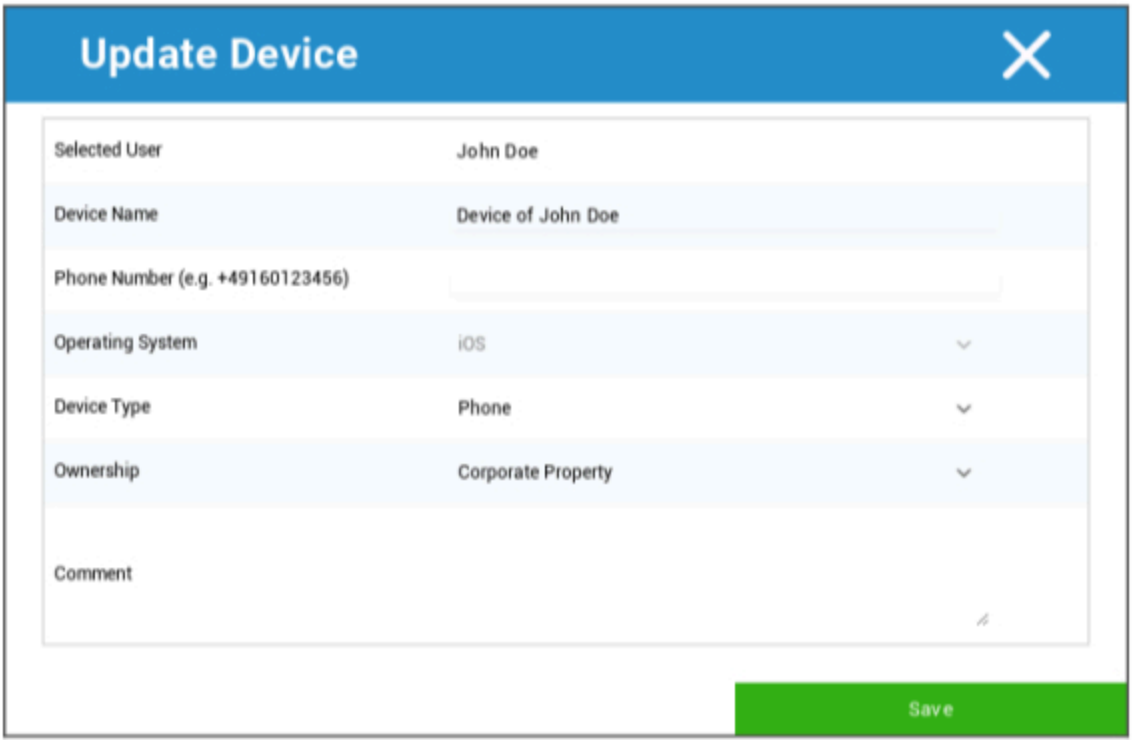
IOS



Gerät bearbeiten	Gerät bearbeiten
Passcode löschen	Der Passcode des Geräts wird gelöscht
Gerät sperren	Gerät sperren (Sperrbildschirm)
Abschaltvorrichtung	Gerät zum Herunterfahren

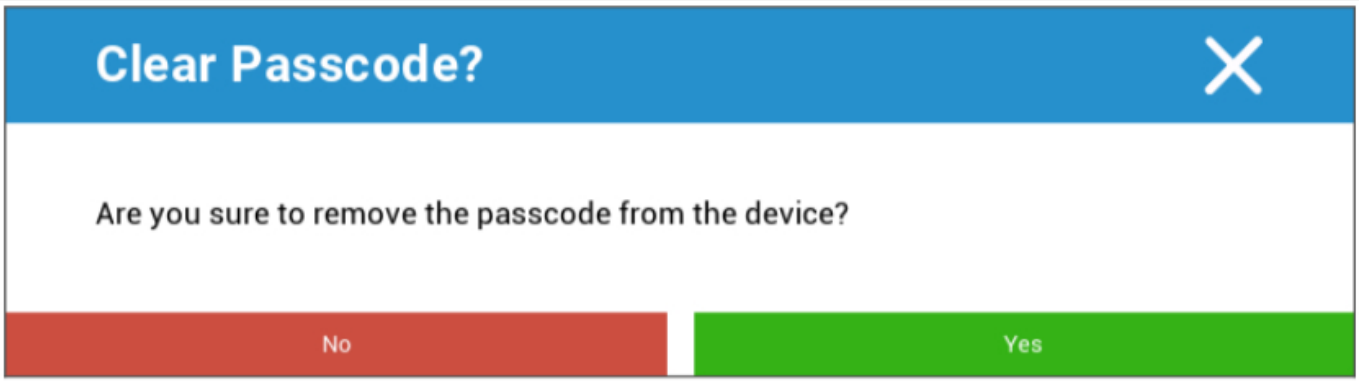
Gerät neu starten	Gerät neu starten
Alarm & Verlustmodus	Start Alarm & Lostmode
Lostmode deaktivieren	Lostmode deaktivieren
Gerät löschen	Gerät aus AppTec entfernen
Gerät wischen	Gerät auf Werkseinstellungen zurücksetzen
Enterprise Wipe	Die von AppTec360 bereitgestellten Informationen, Apps und Profile werden gelöscht (Gerät wird vom MDM getrennt)
MDM entfernen	
Nachricht senden	Push-Benachrichtigungen an das Gerät senden Die Nachricht wird in der AppTec360 App (Registerkarte Nachricht) angezeigt.
TeamViewer Fernsteuerung	Fernsteuerungssitzung mit TeamViewer starten
Antrag auf Einschreibung senden	(Wiederholte) Anmeldeanfrage senden

Gerät bearbeiten



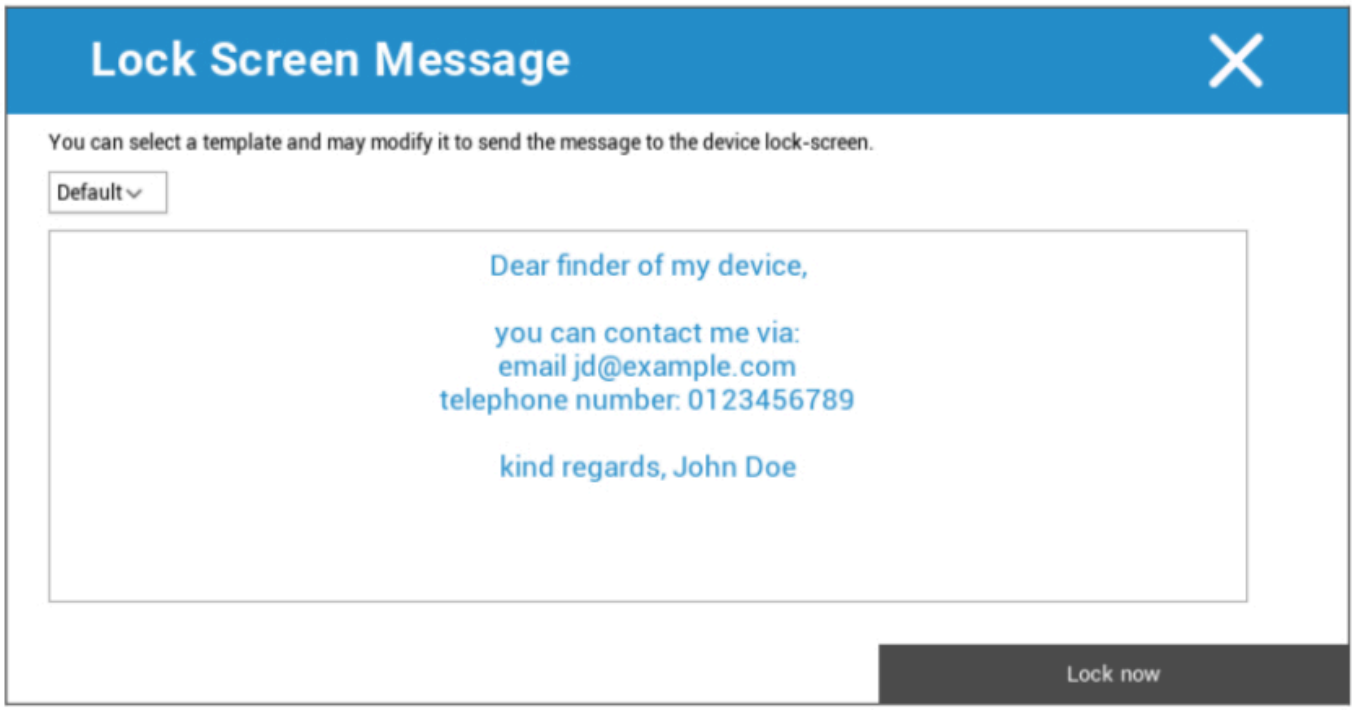
Hier können Sie eine Vielzahl von Informationen über das Gerät aktualisieren.

Passcode löschen



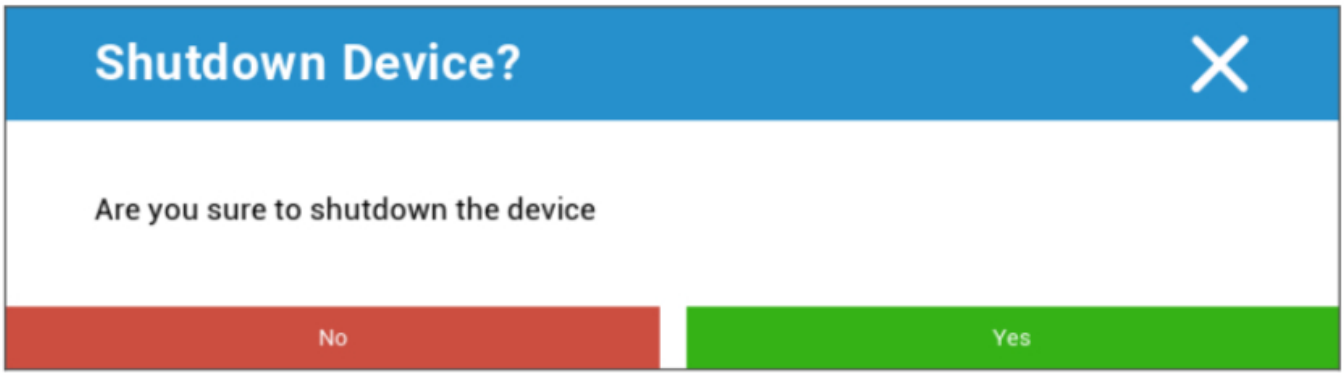
Unter "Passcode löschen" können Sie den Passcode aus der Ferne vom Gerät entfernen. Anschließend wird der Benutzer aufgefordert, ein neues Passwort zu vergeben (abhängig von den Passcode-Richtlinien).

Gerät sperren



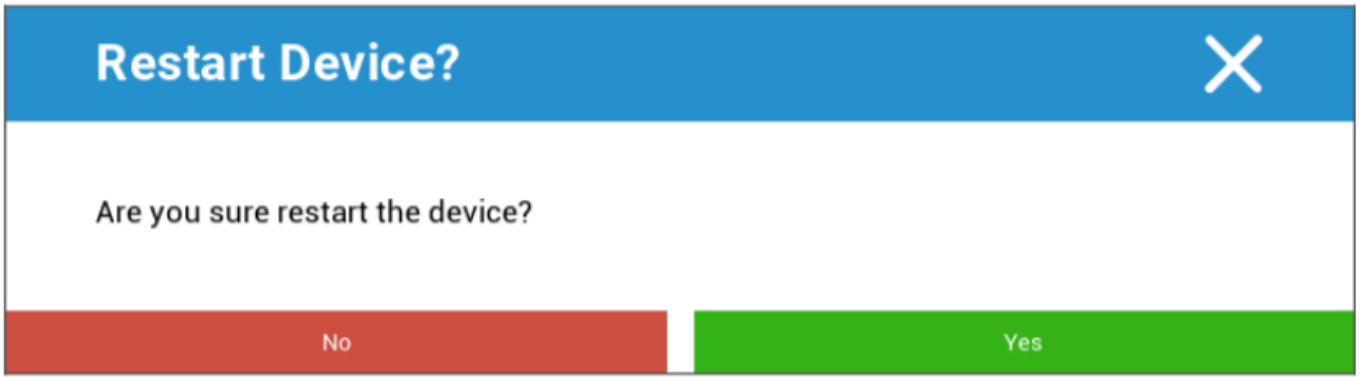
Hier wird ein Sperrbefehl an das Endgerät des Benutzers gesendet (Sperrbildschirm).

Abschaltvorrichtung



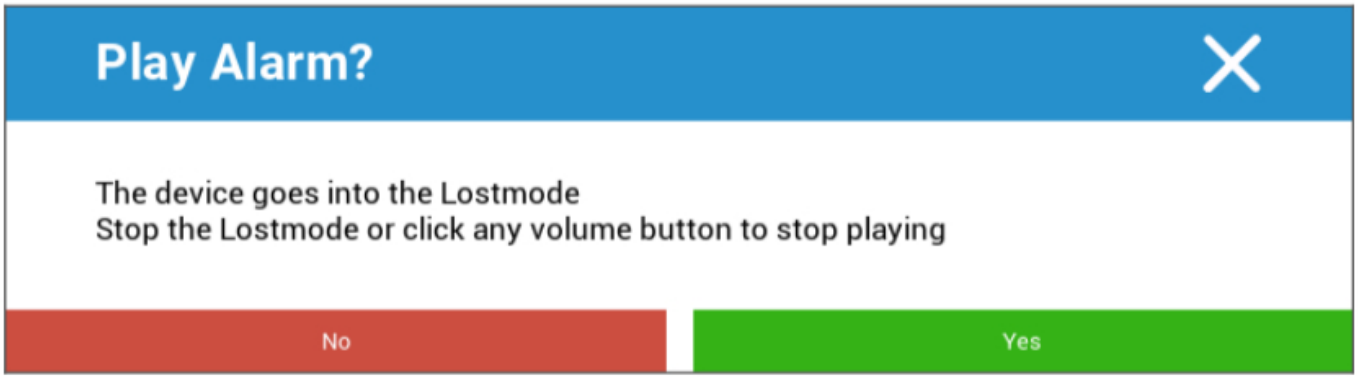
Hier wird ein Befehl zum Herunterfahren an das Endgerät gesendet.

Gerät neu starten

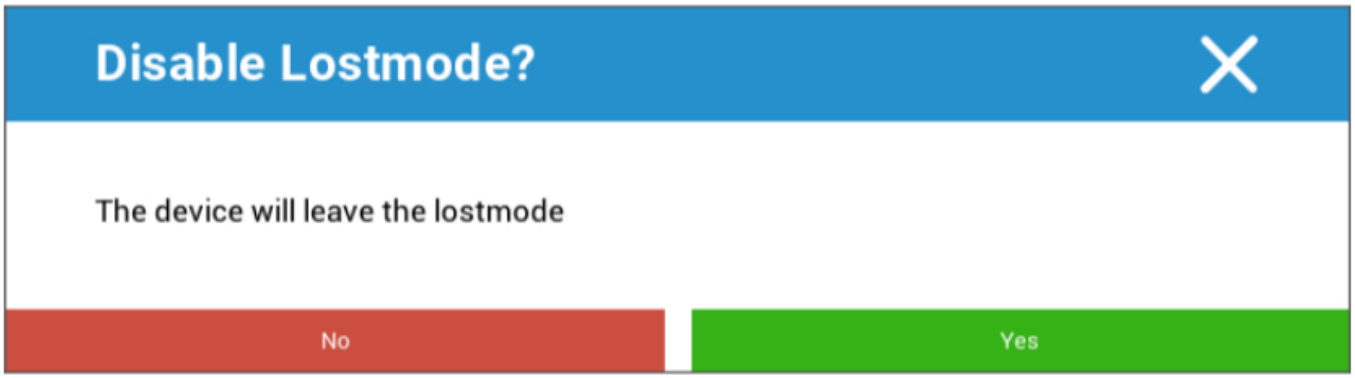


Hier wird ein Neustart-Befehl an das Endgerät des Benutzers gesendet.

Alarm & Verliermodus | Verliermodus deaktivieren



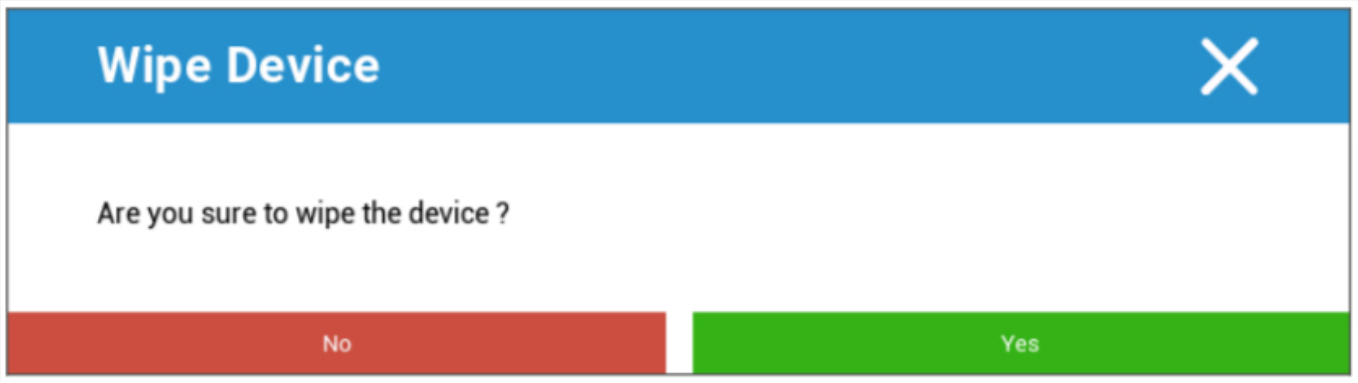
Hier können Sie das Gerät in den Lostmode versetzen, der das Gerät so einstellt, dass es ständig einen Alarmton abspielt. Der Lostmode kann durch Drücken einer beliebigen Lautstärketaste des Geräts oder aus der Ferne durch Klicken auf "Lostmode deaktivieren" beendet werden:



Gerät löschen

Hier kann der Löschbefehl ausgeführt werden. Sie können noch einmal entscheiden, ob das Gerät nur aus AppTec360 entfernt werden soll ("Aus dem System löschen") oder ob das Gerät aus AppTec360 entfernt und zusätzlich in den Auslieferungszustand zurückgesetzt werden soll ("Wipe & Delete").

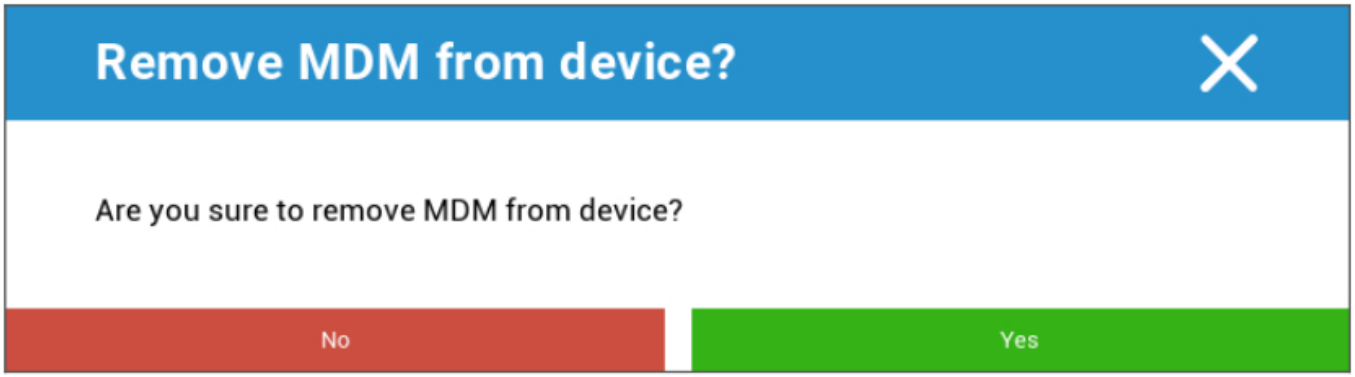
Gerät wischen



Unter "Gerät löschen" können Sie eine vollständige Löschung des Geräts durchführen. Das Gerät wird auf seine Werkseinstellungen zurückgesetzt.

Enterprise Wipe | MDM entfernen

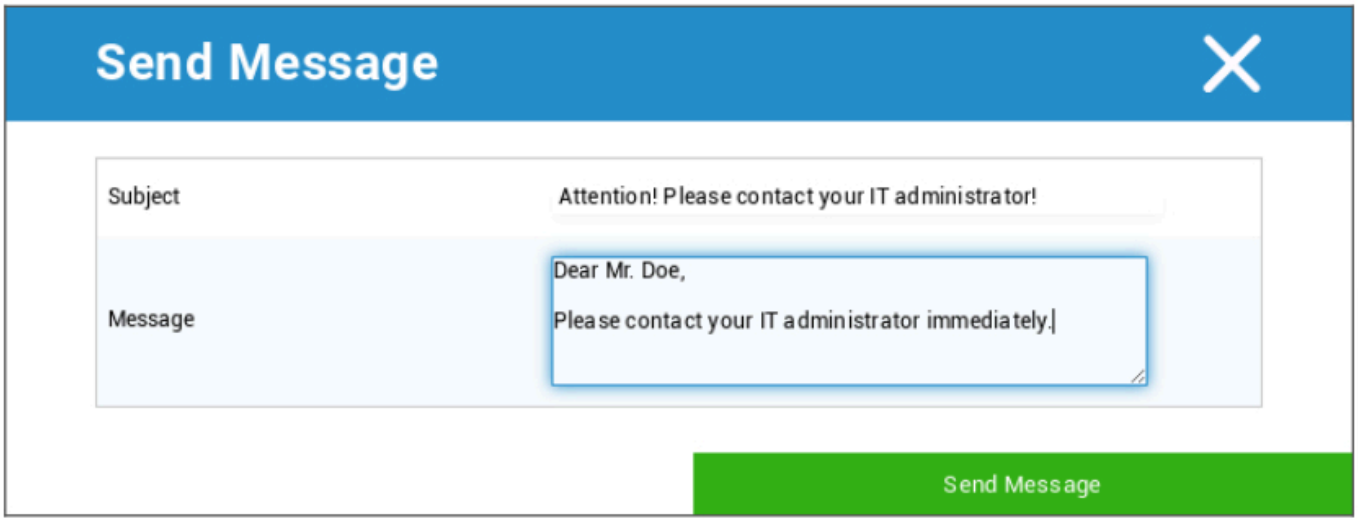
Nur die von AppTec360 bereitgestellten Informationen, Apps und Profile werden gelöscht. Auf diese Weise sind die Unternehmensdaten nicht mehr auf dem Gerät des Endbenutzers verfügbar. Der private Bereich ist davon nicht betroffen und verbleibt weiterhin auf dem Endbenutzergerät.



Mit "MDM entfernen" können Sie das MDM-Profil auf dem Endbenutzergerät und alle anderen von AppTec bereitgestellten Elemente entfernen.

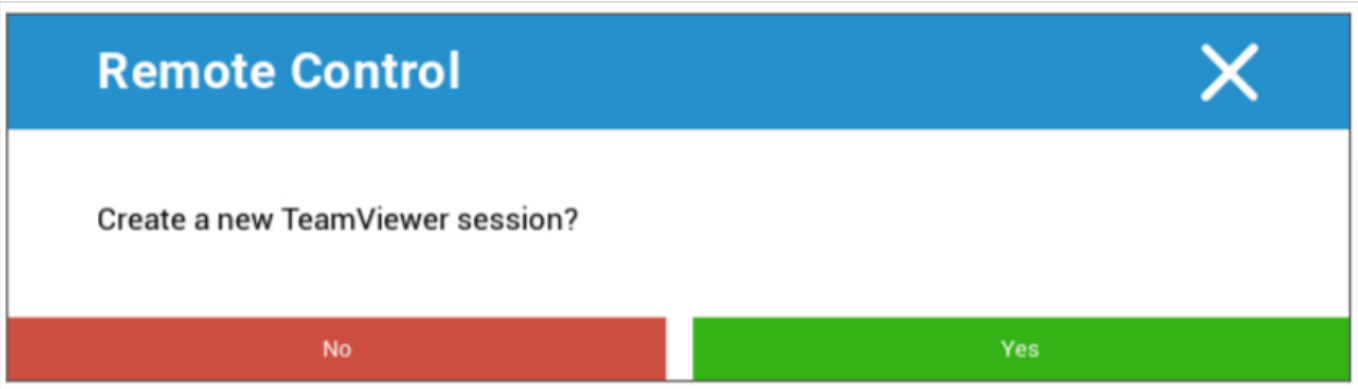
Dieser Befehl führt die gleiche Aktion aus wie "Enterprise Wipe".

Nachricht senden



Hier können Sie eine Push-Benachrichtigung an das entsprechende Gerät senden.

TeamViewer Fernsteuerung



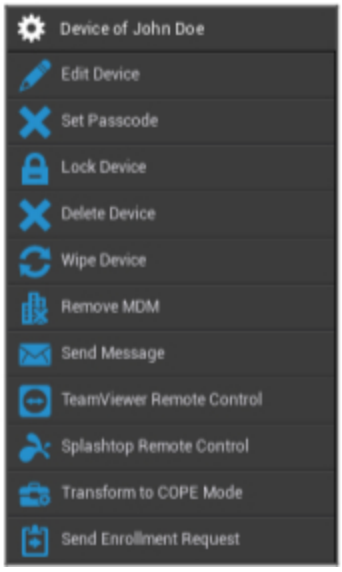
Hier können Sie eine Teamviewer-Fernsteuerungssitzung starten.

Antrag auf Einschreibung senden

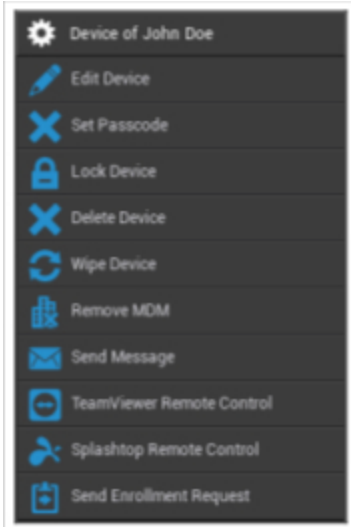
Mit "Registrierungsanfrage senden" können Sie (erneut) eine Registrierungsanfrage an den betreffenden Benutzer senden.

Android

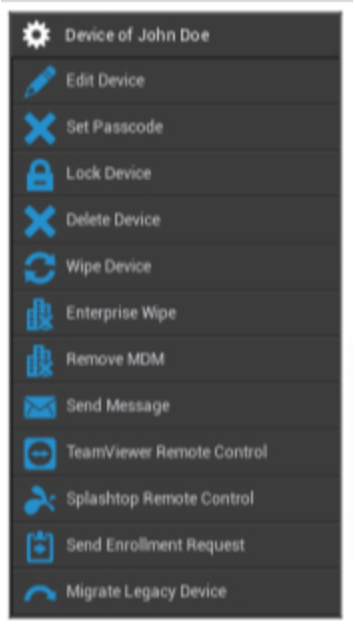
AE Vollständig verwaltetes Gerät (Work Managed)



AE Arbeitsprofil (Container)



Android Telefon | Tablet

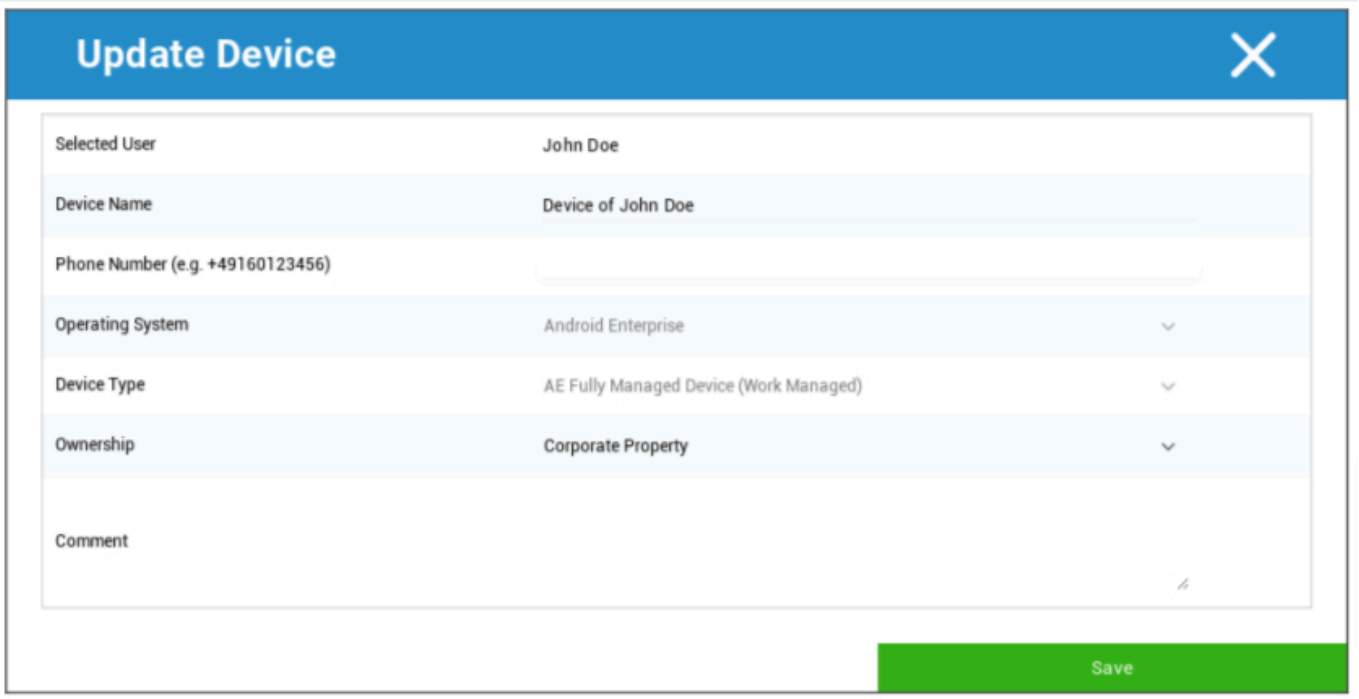


Gerät bearbeiten	Geräteinformationen bearbeiten
Passcode einstellen	Passcode für das Gerät festlegen
Gerät sperren	Gerät sperren (Sperrbildschirm)
Gerät löschen	Gerät aus AppTec löschen
Gerät wischen	Gerät auf Werkseinstellungen zurücksetzen
Enterprise Wipe	Informationen, Apps und Profile, die von AppTec360 bereitgestellt werden, werden gelöscht (das Gerät wird vom MDM getrennt)
MDM entfernen	
Nachricht senden	Push-Benachrichtigungen an das Gerät senden Die Nachricht wird in der AppTec360 App (Registerkarte Nachricht) angezeigt.
TeamViewer Fernsteuerung	Starten Sie eine Fernsteuerungssitzung für dieses Gerät mit TeamViewer
Splashtop-Fernbedienung	Starten Sie eine Fernsteuerungssitzung für dieses Gerät mit Splashtop
In den COPE-Modus umwandeln (nur bei AE Fully Managed Device (Work Managed))	Erstellen Sie ein Arbeitsprofil auf diesem AE Fully Managed (Work Managed) Gerät
Antrag auf Einschreibung senden	Senden Sie eine (wiederholte) Registrierungsanfrage
Legacy-Gerät migrieren (nur auf Android-Telefonen/Tablets, wenn Sie sich mit der	Migrieren Sie das Profil für Android-Telefone/Tablets in das AE-Profil für vollständig

Provisionierung im Modus "Gerätebesitzer" angemeldet haben)	verwaltete Geräte (Work Managed)

Gerät bearbeiten

Hier können Sie eine Vielzahl von Geräteinformationen aktualisieren.



Ausgewählter Benutzer	Benutzer des Geräts
Gerät Name	Name des Geräts
Telefon Nummer	Telefonnummer des Geräts
Betriebssystem	Android Unternehmen Android
Gerätetyp	Android Enterprise: • AE Vollständig verwaltetes Gerät (Work Managed) • AE Arbeitsprofil-Modus (nur Container) • AE Vollständig verwaltetes Gerät mit Arbeitsprofil (COPE) Android: • Telefon • Tablette
Eigentümerschaft	Corporate = Unternehmenseigentum

	Mitarbeiter = Mitarbeiter Eigenschaft
Kommentar	Zusätzliche Beschreibungen für das Gerät

Passcode löschen

Hier können Sie den Gerätepasscode auf dem ausgewählten Gerät entfernen. Unter Android ist der Passcode standardmäßig auf "123456" eingestellt - dies kann und sollte vom Benutzer nachträglich geändert werden.

Gerät sperren

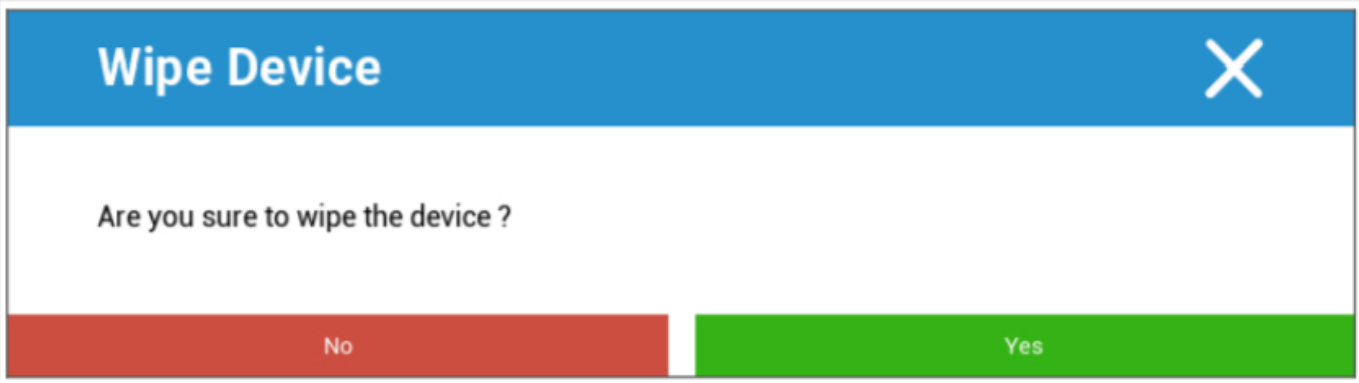
Hier wird ein Befehl zum Sperren des Geräts an das Gerät gesendet (Sperrbildschirm).

Gerät löschen

Hier kann ein Löschbefehl ausgeführt werden. Sie können noch einmal entscheiden, ob das Gerät nur aus AppTec360 entfernt werden soll ("Aus dem System löschen") oder ob das Gerät aus AppTec360 entfernt und zusätzlich auf die Werkseinstellungen zurückgesetzt werden soll ("Wipe & Delete").

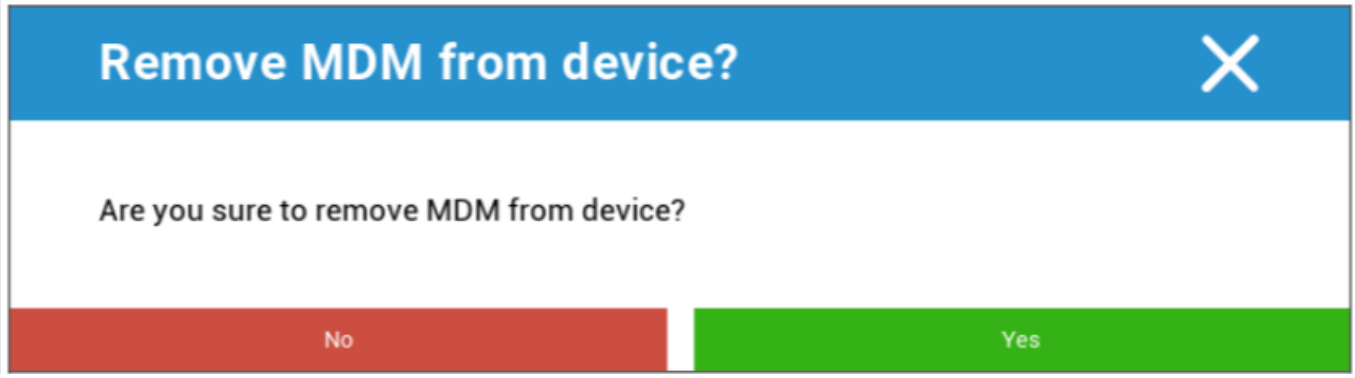
Gerät wischen

Unter "Gerät löschen" können Sie eine vollständige Löschung des Geräts durchführen. Das Gerät wird dann auf seine Werkseinstellungen zurückgesetzt.



Wenn das Gerät eine SD-Karte enthält, können Sie außerdem die SD-Karte löschen. Sie können dies erreichen, indem Sie die Option "SD-Karte auch löschen? " auf "Ein".

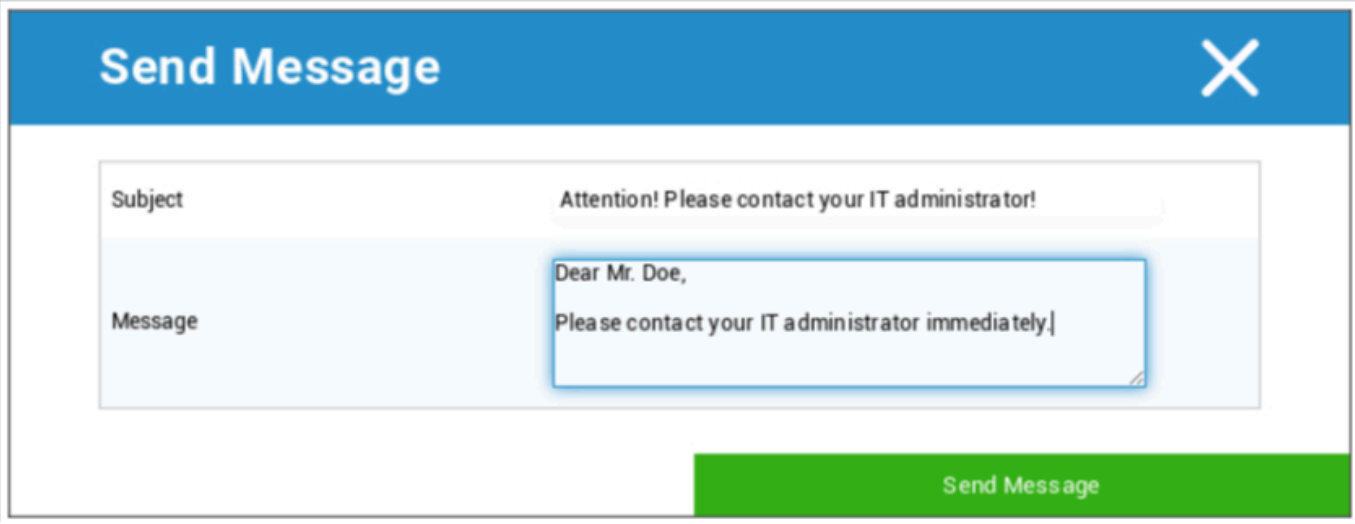
MDM entfernen



Dies ist die empfohlene Methode, um eine Trennung von MDM zu erreichen.

Nur die von AppTec360 bereitgestellten Informationen, Apps und Profile werden gelöscht. Das bedeutet, dass alle Unternehmensdaten nicht mehr auf dem Endgerät des Benutzers verfügbar sind. Die private Sphäre ist davon jedoch nicht betroffen und verbleibt weiterhin auf dem Gerät des Endbenutzers.

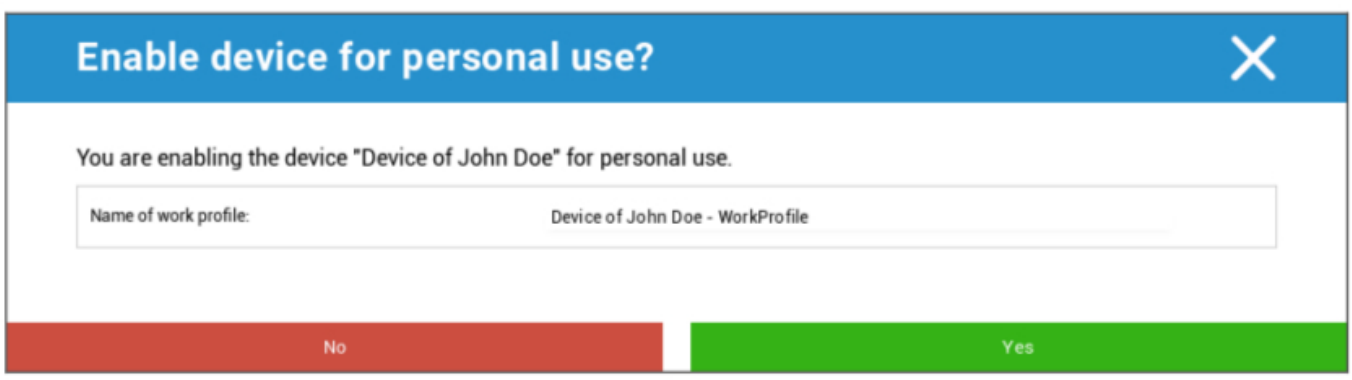
Nachricht senden



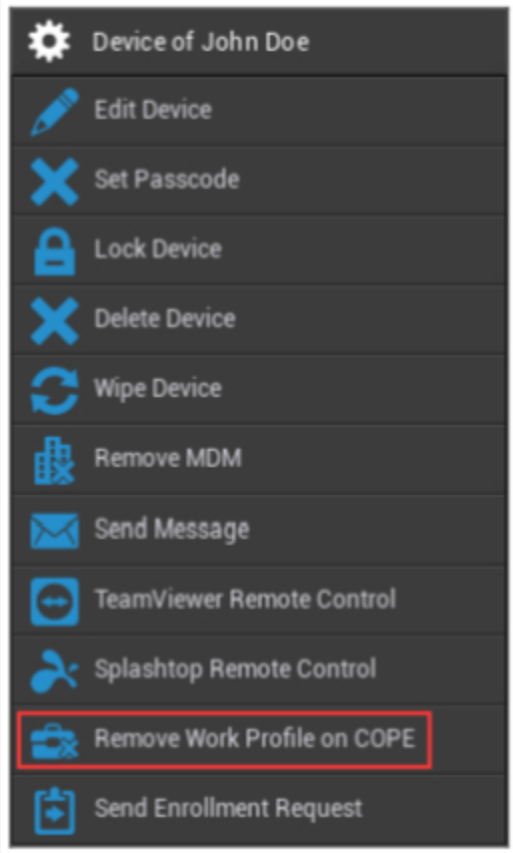
Hier können Sie eine Push-Benachrichtigung an das jeweilige Endgerät des Benutzers senden.

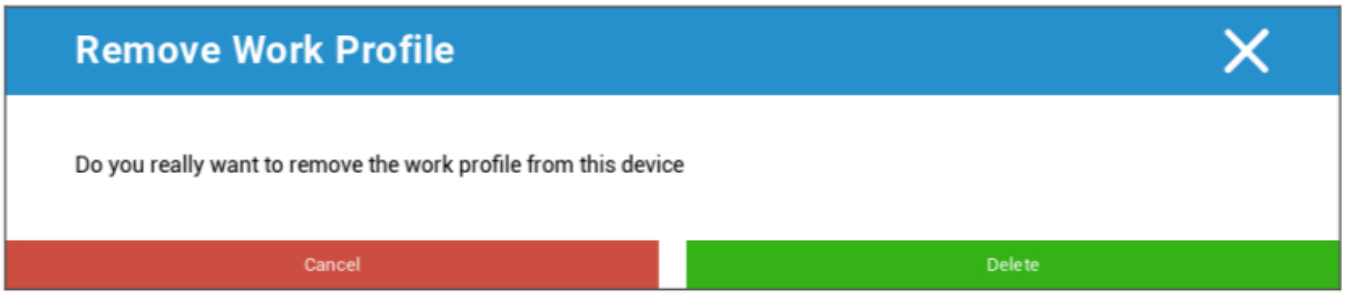
In den COPE-Modus wechseln

Erstellen Sie ein Arbeitsprofil auf diesem AE Fully Managed (Work Managed) Gerät



Nachdem Sie das Gerät in den COPE-Modus versetzt haben, können Sie das Arbeitsprofil entfernen, indem Sie auf die Zahnradoption **Arbeitsprofil entfernen auf COPE** klicken **:**




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

Antrag auf Einschreibung senden

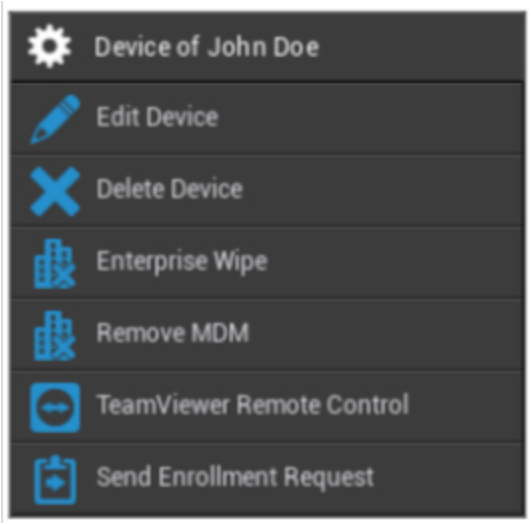
Mit "Registrierungsanfrage senden" können Sie (erneut) eine Registrierungsanfrage an den betreffenden Benutzer senden.

Bitte beachten Sie, dass nur der neueste Enrollment - Antrag gültig ist.

Älteres Gerät migrieren

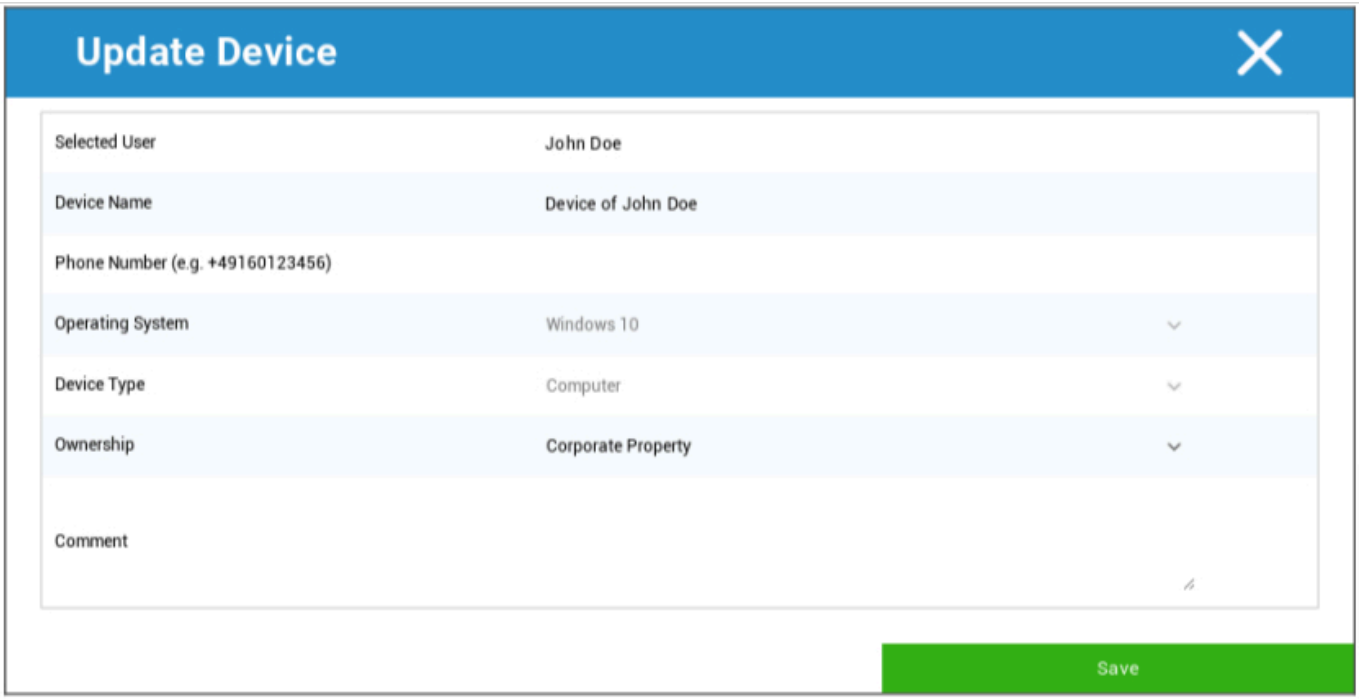
Migrieren Sie das Profil für Android-Telefone/Tablets in das AE-Profil für vollständig verwaltete Geräte (Work Managed)

Windows



Gerät Name	Name des ausgewählten Geräts
Gerät bearbeiten	Gerät bearbeiten
Gerät löschen	Gerät aus AppTec entfernen
Enterprise Wipe	Von AppTec360 bereitgestellte Informationen, Apps und Profile werden gelöscht
MDM entfernen	
TeamViewer Fernsteuerung	Fernsteuerung des Geräts mit TeamViewer
Antrag auf Einschreibung senden	Registrierungsanfrage (erneut) senden

Gerät bearbeiten

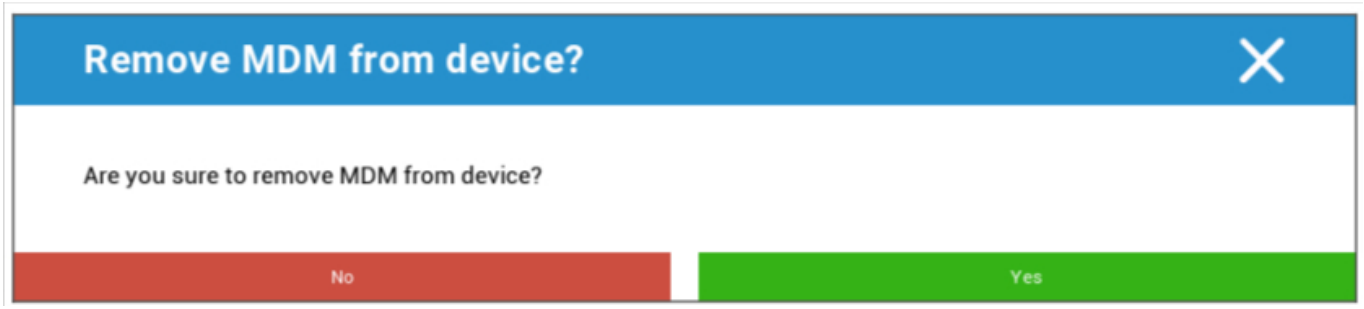


Hier können Sie eine Vielzahl von Informationen über das Gerät aktualisieren.

Gerät löschen

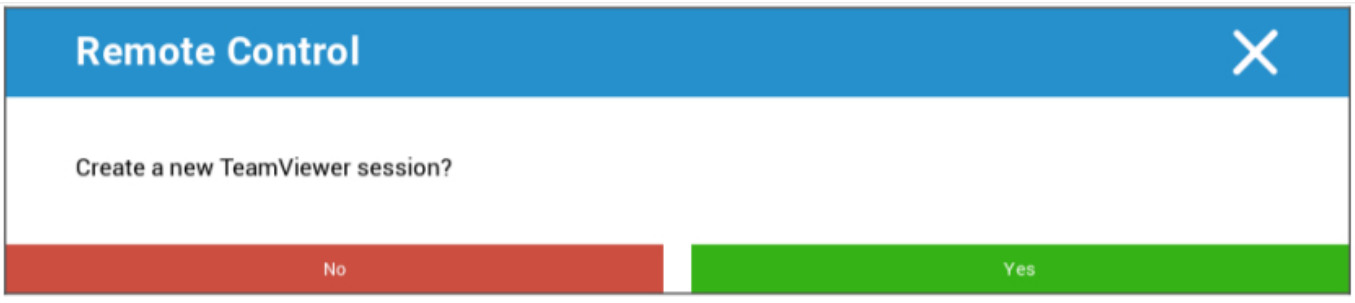
Hier können Sie den Löschbefehl ausführen, der das Gerät nur aus AppTec360 entfernt.

Enterprise Wipe | MDM entfernen



Nur die von AppTec360 bereitgestellten Informationen, Apps und Profile werden gelöscht. Auf diese Weise sind die Unternehmensdaten nicht mehr auf dem Gerät des Endbenutzers verfügbar. Der private Bereich ist davon nicht betroffen und verbleibt weiterhin auf dem Endbenutzergerät.

TeamViewer Fernsteuerung



Hier können Sie eine TeamViewer-Fernsteuerungssitzung für dieses Gerät starten.

Antrag auf Einschreibung senden

Mit "Registrierungsanfrage senden" können Sie (erneut) eine Registrierungsanfrage an den betreffenden Benutzer senden.

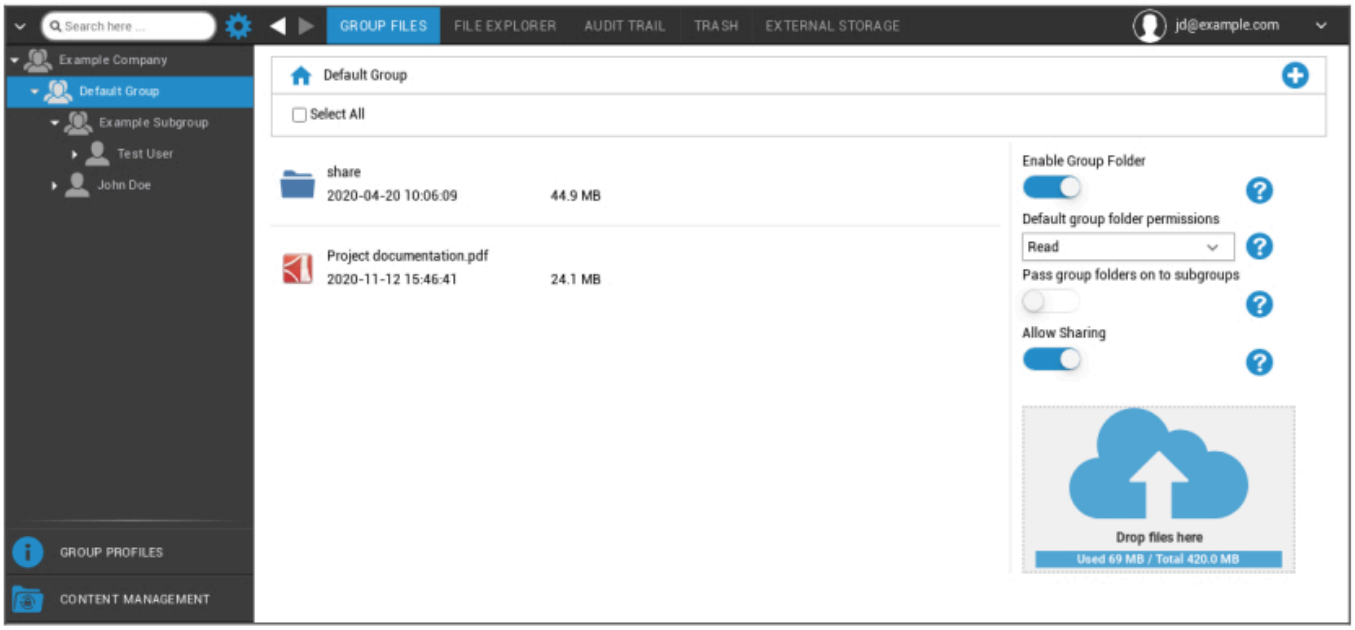
Content Management

Wenn Sie in einer Gruppe sind, können Sie die AppTec ContentBox mit "Content Management" verwalten.

Mit der Content Box können Sie Dokumente und andere Unternehmensdaten sicher an die Geräte der Endbenutzer verteilen.

Gruppendateien

"Gruppendateien" ist ein wesentlicher Bestandteil von ContentBox. Hier können Sie Einstellungen vornehmen, Dokumente hochladen, neue Ordner erstellen usw.



Mit dem Symbol in der oberen rechten Ecke können Sie neue Ordner erstellen, die der jeweiligen Gruppe mit "Ordner hinzufügen" zugeordnet werden.

Mit dem Symbol in der oberen rechten Ecke können Sie über "Ordner hinzufügen" einen neuen Ordner erstellen, der der jeweiligen Gruppe zugeordnet werden soll.

Sie können den Ordner benennen, wie Sie möchten.

Über "Dateien hochladen" können Sie Daten hochladen. Hier wird Ihr Standard-Explorer geöffnet. Diese beiden Aktionen können Sie natürlich auch in jedem (Unter-)Ordner durchführen.

Mit dem Symbol in der oberen linken Ecke können Sie zum Hauptmenü zurückkehren.

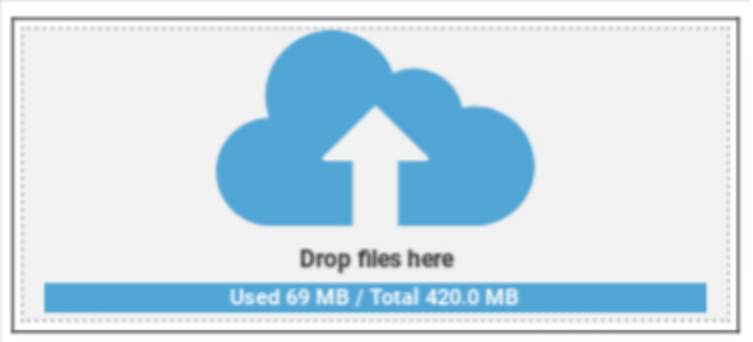
Sie können mehrere Ordner und Dateien auswählen und sie mit "Herunterladen" herunterladen oder sie mit "Löschen" löschen.

Sie können auch alle Dateien und Ordner mit auswählen und die Befehle "Herunterladen" und "Löschen" ausführen.

Wenn Sie Ihre Maus über einen Ordner oder eine Datei bewegen, sehen Sie die folgende Übersicht:

- Mit "Umbenennen" können Sie den Ordner/die Datei umbenennen
- Mit "Download" können Sie den Ordner/die Datei herunterladen
- Mit "Löschen" können Sie den Ordner/die Datei löschen

Gruppenordner aktivieren	Wenn aktiviert, haben alle Mitglieder der Gruppe Zugriff auf den jeweiligen Ordner
Standardberechtigungen für Gruppenordner	Berechtigungen der Benutzer in der ausgewählten Gruppe: Lesen = nur Leseberechtigung Update = Erlaubnis zum Aktualisieren Erstellen = Erlaubnis zum Erstellen Löschen = Erlaubnis zum Löschen
Gruppenordner an Untergruppen weitergeben	Wenn aktiviert, können die jeweiligen Untergruppen auf die übergeordneten Dateien zugreifen
Berechtigungen für Untergruppen	Berechtigungen der Benutzer in der ausgewählten Untergruppe: Lesen = nur Leseberechtigung Update = Erlaubnis zum Aktualisieren Erstellen = Erlaubnis zum Erstellen Löschen = Erlaubnis zum Löschen
Freigabe erlauben	Wenn aktiviert, kann der Benutzer Dateien über einen Link teilen



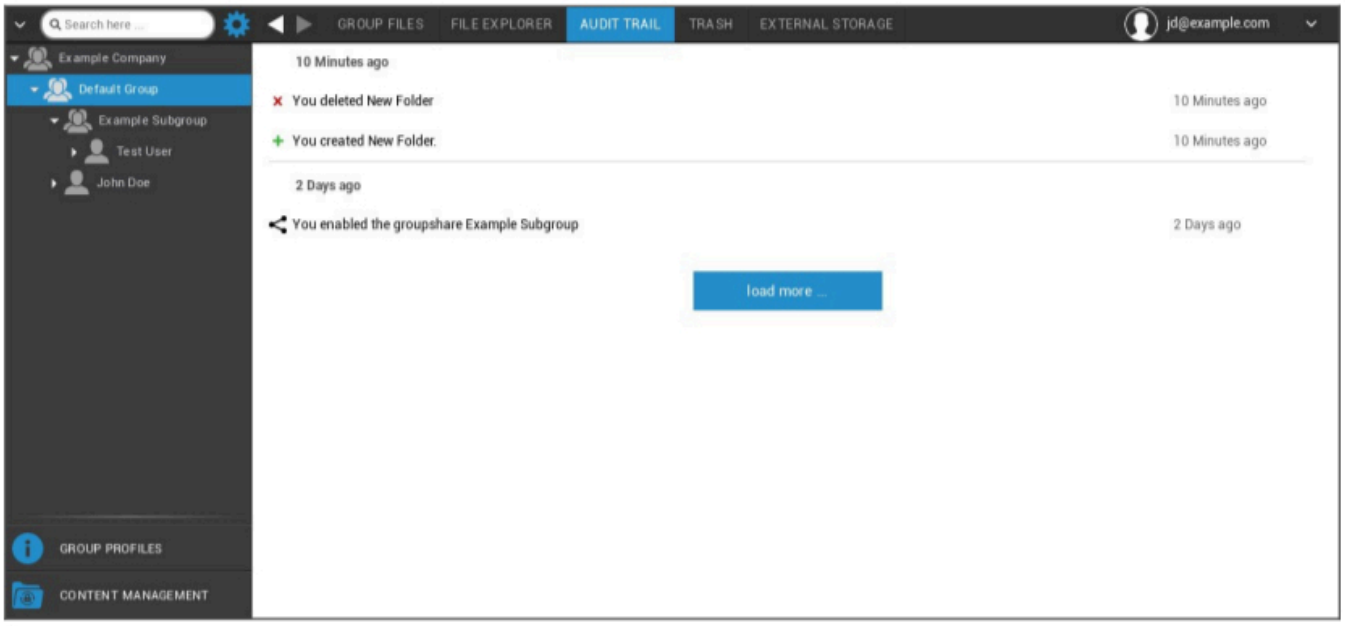
Um Dateien hochzuladen, können Sie dieses Feld verwenden, indem Sie eine Datei per Drag & Drop in dieses Fenster ziehen. Sie können auch auf dieses Feld klicken, um eine Datei mit Hilfe des Internet Explorers auszuwählen und hochzuladen.

Datei-Explorer

Mit dem "Datei-Explorer" können Sie alle Ordner und Dateien verwalten - unabhängig davon, in welcher Gruppe sie abgelegt sind.

Hier finden Sie auch die Einstellungen und Schaltflächen, die Sie unter "Gruppendateien" kennen gelernt haben.

Prüfpfad



Unter "Audit Trail" können Sie in der Historie sehen, welcher Benutzer was erstellt, gelöscht oder freigegeben hat. Auf diese Weise können Sie jederzeit feststellen, was mit den Unternehmensdaten gemacht wurde.

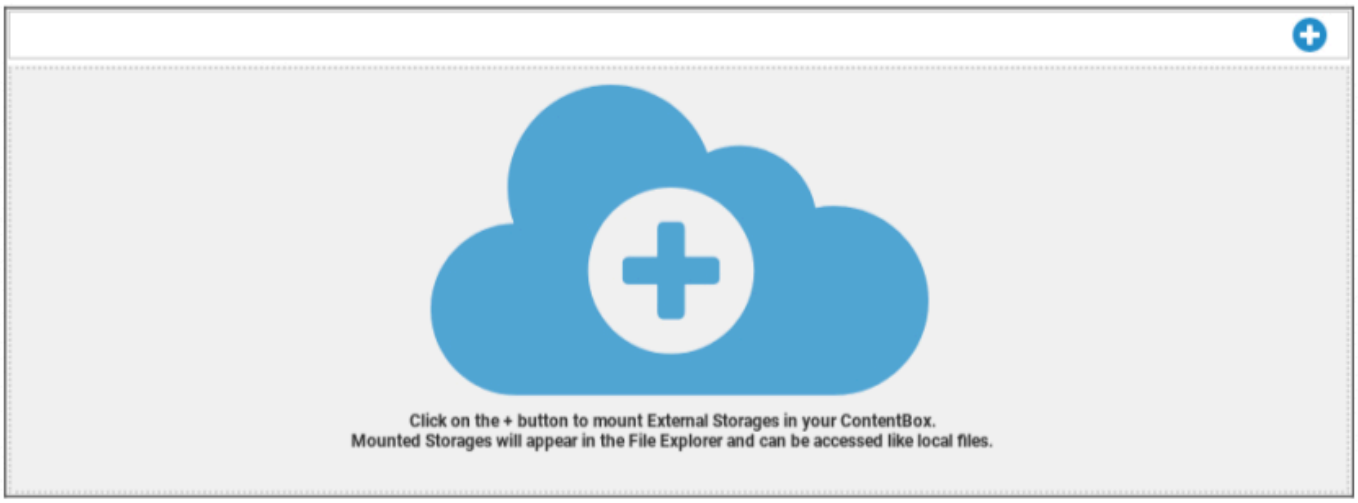
Papierkorb

Sollten Sie etwas (versehentlich) gelöscht haben, können Sie die Ordner und Dateien unter "Papierkorb" einsehen und sie nach Ihren Wünschen wiederherstellen.

- Mit "Undelete" können Sie die Daten/Ordner wiederherstellen.
- Mit "Löschen" können Sie die Daten/Ordner dauerhaft löschen - Sie müssen den Löschbefehl noch einmal bestätigen.

Bitte beachten Sie, dass die Speicherkapazität, die im Papierkorb genutzt wird, den verfügbaren "Gesamtspeicherplatz" reduziert - dies ist eine Anforderung von ownCloud.

Externer Speicher



Unter der Überschrift "Externer Speicher" können Sie einen externen Speicher anschließen.

Mit dem Symbol können Sie (zusätzlichen) Speicherplatz hinzufügen.

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

Amazon S3	
Name anzeigen	Name anzeigen
Zugangsschlüssel	Zugangsschlüssel
Geheimschlüssel	Sicherheitsschlüssel
Eimer	Eindeutige Identität des Unterordners, der Ihnen zugewiesen wurde
Hostname (optional)	Hostname (optional)
Anschluss (optional)	Anschluss (optional)
Region	Region (optional)
SSL aktivieren	SSL aktivieren
Pfadstil aktivieren	Pfadadresse löschen, die Ihnen zugewiesen wurde

FTP	
Name anzeigen	Name anzeigen
Gastgeber	Host-Adresse
Benutzername	Benutzername
Passwort	Passwort
Wurzel	Hauptmenü
Sicher ftps://	

SFTP	
Name anzeigen	Name anzeigen
Gastgeber	Host-Adresse
Benutzername	Name des Benutzers
Passwort	Passwort
Wurzel	Hauptmenü

ownCloud	
Name anzeigen	Name anzeigen
URL	ownCloud URL
Benutzername	Benutzername
Passwort	Passwort
Entfernter Unterordner	Standard-Ordner
Sicher https://	

WebDAV	
Name anzeigen	Name anzeigen
URL	WebDAV-URL
Benutzername	Name des Benutzers
Passwort	Passwort
Wurzel	Hauptmenü
Sicher https://	
Windows-Aktie	Unterstützung für Windows Share wird bald verfügbar sein
SharePoint	Unterstützung für Microsoft SharePoint wird bald verfügbar sein

Audit-Protokoll

Hier finden Sie ein Protokoll, das Informationen über Aktionen aufzeichnet, die in der MDM-Konsole durchgeführt werden.

Mit dem Filtersymbol können Sie Filter auf die angezeigte Liste anwenden.

Mit dem Dropdown-Menü **Artikel pro Seite**: können Sie die Anzahl der Artikel auswählen, die auf einer Seite der Liste angezeigt werden sollen.

Ergriffene Maßnahme / Einstellung geändert	Die Aktion, die durchgeführt wurde / Die Einstellung, die geändert wurde
Wert	Der Wert der durchgeführten Aktion / geänderten Einstellung
Benutzer	Der Name des Benutzers, der die Aktion durchgeführt / die Einstellung geändert hat
Datum	Der Zeitstempel, wann diese Aktion durchgeführt / diese Einstellung geändert wurde
Pfad / Typ	Der Pfad zu dem Ort, an dem diese Aktion durchgeführt / diese Einstellung geändert wurde

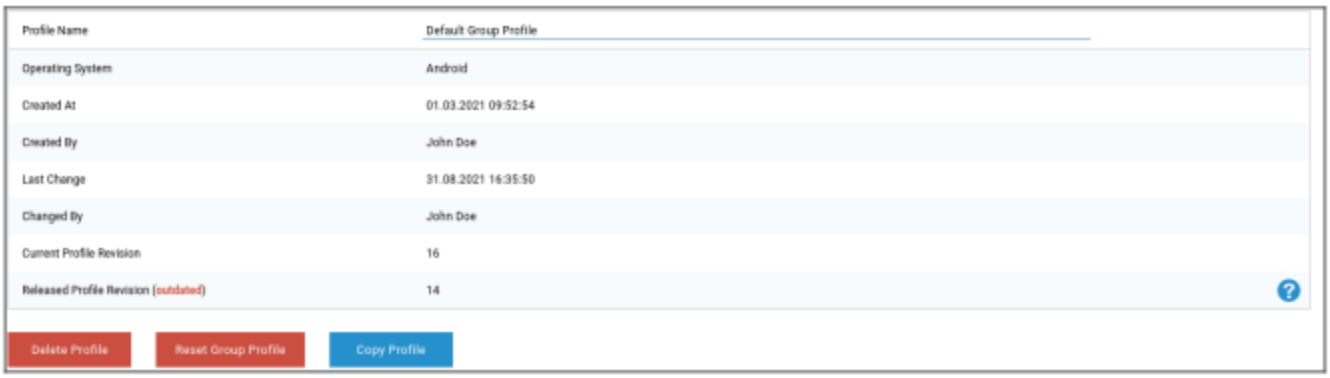
iOS Konfiguration

Allgemein

Je nachdem, ob Sie gerade eine Gruppe oder ein Gerät ausgewählt haben, sind die Anzeige und ihre Unterpunkte unterschiedlich - bitte beachten Sie dies genau!

Gruppenprofilübersicht (nur auf Gruppenebene)

Wenn Sie ein Gruppenprofil öffnen, erhalten Sie einen schnellen Überblick über das Profil



Profil Name	Name des Profils (kann hier geändert werden)
Betriebssystem	Betriebssystem, für das das Profil bestimmt ist
Erstellt am	Zeitpunkt der Erstellung
Erstellt von	Der Ersteller des Profils
Letzte Änderung	Zeitpunkt der letzten Änderung des Profils
Geändert von	Konto, das die letzten Änderungen vorgenommen hat
Aktuelle Profilüberarbeitung	Revision des gespeicherten Profilstatus
Freigegebene Profil-Revision	Zugewiesene Profilrevision ("Jetzt zuweisen"). Wenn das Etikett hinter dem Text "(veraltet)" anzeigt, bedeutet dies, dass Sie das Profil zwar gespeichert, aber noch nicht zugewiesen haben, so dass die Geräte noch eine ältere Version erhalten.

Allgemeine Informationen

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

Gerät Name	Name des Geräts
Telefon Nummer	Telefonnummer des Geräts
Modell	Modellnummer
Betriebssystem	OS
Seriennummer	Seriennummer des Geräts
Geräteeigentum	Firmen- oder Privatgerät Unternehmen = Unternehmensgerät Mitarbeiter = privates Gerät
Gerätetyp	Gerätetyp (Tablet oder Telefon)
Jailbroken	Wenn ein Jailbreak auf dem Gerät vorhanden ist
Beaufsichtigt	Zeigt an, ob dies ein überwachtes Gerät ist
Konform	Wenn gegen Richtlinien verstoßen wurde
Zuletzt gesehen	Status, wann das Gerät zuletzt mit dem AppTec360 Server kommuniziert hat

Einstellungen

Diese Einstellungen enthalten den Gerätenamen und einen vordefinierten Hintergrund.

Gerät in Systemname umbenennen	Der Name, der in der AppTec360-Konsole (in der linken Hierarchiestruktur) ausgegeben wird, ist derselbe wie auf dem jeweiligen Endgerät (kann in den Geräteeinstellungen eingesehen werden)
Benutzerdefiniertes Hintergrundbild verwenden (nur überwachte Geräte)	Hier können Sie den Hintergrund vordefinieren, der auf dem Endgerät angezeigt werden soll (z.B. für eine Art Corporate Branding für das Gerät) Ist nur im überwachten Modus verfügbar!
Automatische OS-Updates	Erzwingt Betriebssystem-Updates, falls verfügbar. Nur für DEP-Geräte im überwachten Modus.
Benutzerdefinierte Schriftarten	Hier können Sie benutzerdefinierte Schriftarten hinzufügen.
Name	Optional. Der für den Benutzer sichtbare Name für die Schriftart. Dieses Feld wird nach der Installation durch den tatsächlichen Namen der Schriftart ersetzt.
Schriftart	Laden Sie die Schriftartdatei (.otf oder .ttf) hoch.

Konfig-Revision

Hier erhalten Sie einen Überblick darüber, welches Gruppenprofil dem Gerät zugewiesen ist.

Wenn Sie auf das Gruppenprofil klicken, haben Sie direkten Zugriff auf das Profil und können Einstellungen vornehmen.

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

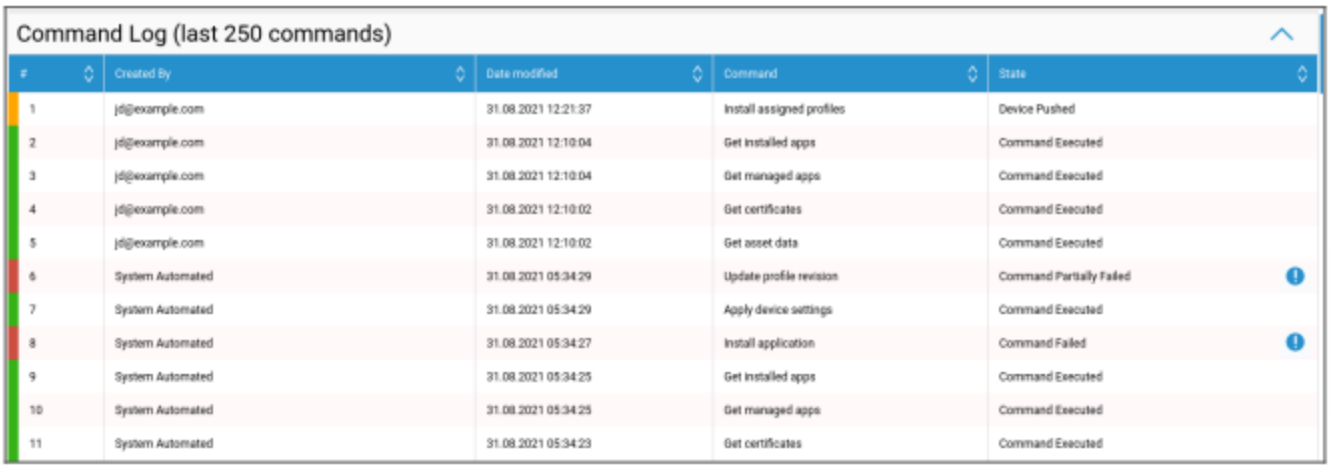
Mit dem Symbol können Sie das Geräteprofil so zurücksetzen, dass es keinerlei Einstellungen enthält.

"Neuere Revision verfügbar" bedeutet, dass das Gruppenprofil geändert und gespeichert, aber nicht zugewiesen wurde. Das Gruppenprofil muss mit "Jetzt zuweisen" auf Gruppenebene zugewiesen werden, um die Änderungen auf die Geräte anzuwenden.

Geräteprotokoll (nur auf Geräteebene)

Befehl Log

Hier können Sie sehen, welche Befehle für das Gerät erteilt wurden und welchen Status sie haben.



Mit "System Automated" erstellte Befehle werden automatisch vom System erstellt.

Mögliche Befehlszustände

Gerät geschoben	Eine Push-Anfrage wurde an den Push-Dienst (z.B. APNS) gesendet, um das Gerät anzuweisen, sich wieder mit dem EMM-Server zu verbinden.
Befehl erstellt	Der Befehl wurde im System erstellt.
Befehl gesendet	Der Befehl wurde an das Gerät gesendet, nachdem es sich mit dem Server verbunden hat.
Befehl Ausgeführt	Der Befehl wurde erfolgreich ausgeführt.
Befehl fehlgeschlagen	Der Befehl ist fehlgeschlagen. *
Befehl Teilweise fehlgeschlagen	Je nach Betriebssystem des Geräts können einige Befehle in Gruppen zusammengefasst werden. Dabei sind einige Teile dieser Befehlsgruppe fehlgeschlagen. *
Befehl ausgeführt, eventuell fehlgeschlagen	Der Befehl wurde ausgeführt, aber vielleicht auch nicht.
Kommando zurückgeschoben	Der Befehl wurde von einem Benutzer erneut gesendet.
Weggeworfen	Der Befehl wurde verworfen. Zum Beispiel, weil er durch einen anderen Befehl ersetzt wurde oder das Gerät neu registriert wurde und alte Befehle entfernt wurden

Wenn sich hinter der Nachricht ein Ausrufezeichen befindet, können Sie weitere Informationen erhalten, indem Sie mit dem Mauszeiger über das Symbol fahren.

Asset Management (nur auf Geräteebene)

Asset Management (nur auf Geräteebene)

Geräte-Infos

Modell	Modellnummer des Geräts
Betriebssystem	OS
OS Version	OS-Version
Seriennummer	Seriennummer
UDID	Gerät UDID
Gerät Name	Name des Geräts
Beaufsichtigt	Zeigt an, ob das Gerät beaufsichtigt wird
Akku-Status	Status der Batterie

Wi-Fi

IP-Adresse	Geräte-IP-Adresse
WiFi MAC	WiFi MAC-Adresse

Zellulär

Status	Status (SIM-Karte vorhanden)
Telefon Nummer	Telefon Nummer
Roaming-Status	Aktueller Roaming-Status
Roaming (Sprache/Daten)	Roaming-Status für Sprache/Daten
IP-Adresse	IP-Adresse
IMEI	IMEI-Nummer
Betreiber/Transporteur	Anbieter von Mobilfunkdiensten
SIM-Betreiber Netzwerk	SIM-Betreibernetz
Carrier Version	Träger-Version
Modem-Firmware	Modem-Firmware
Aktuelle MCC/MNC	Siehe "SIM MCC/MNC".
SIM MCC/MNC	Der Mobile Country Code ist eine von der ITU festgelegte Länderkennung gemäß der E.212 Standard, der in Verbindung mit dem Mobile Network Code (MNC) zur Identifizierung eines Mobilfunknetzes (=Ländercode) verwendet wird Wenn Sie in ein anderes Mobilfunknetz wechseln, sind "Aktuelle MCC/MNC" und "SIM MCC/MNC" daher unterschiedlich.

Bluetooth

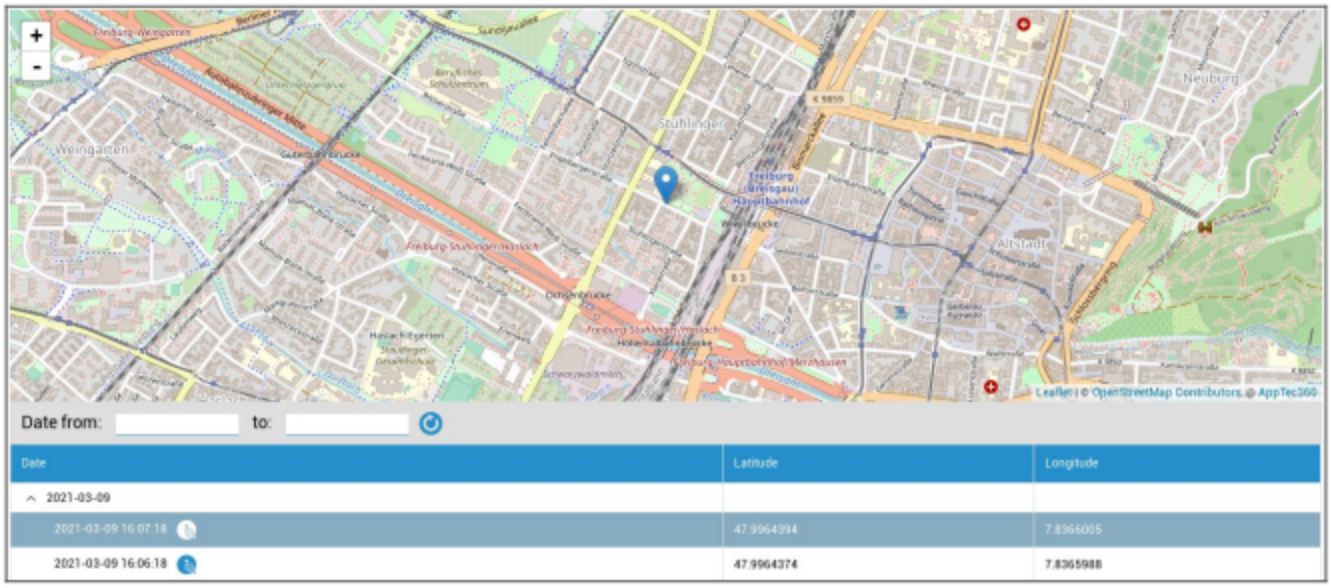
Bluetooth MAC	Bluetooth MAC-Adresse

Sicherheitsmanagement

Anti-Diebstahl (nur auf Geräteebene)

GPS-Informationen (nur auf Geräteebene)

Hier können Sie den aktuellen/letzten Standort des Geräts ermitteln. Die Lokalisierung kann entweder mit einem oder sogar zwei Passwörtern geschützt werden - siehe: Allgemeine Einstellungen - Datenschutz - GPS-Zugriff



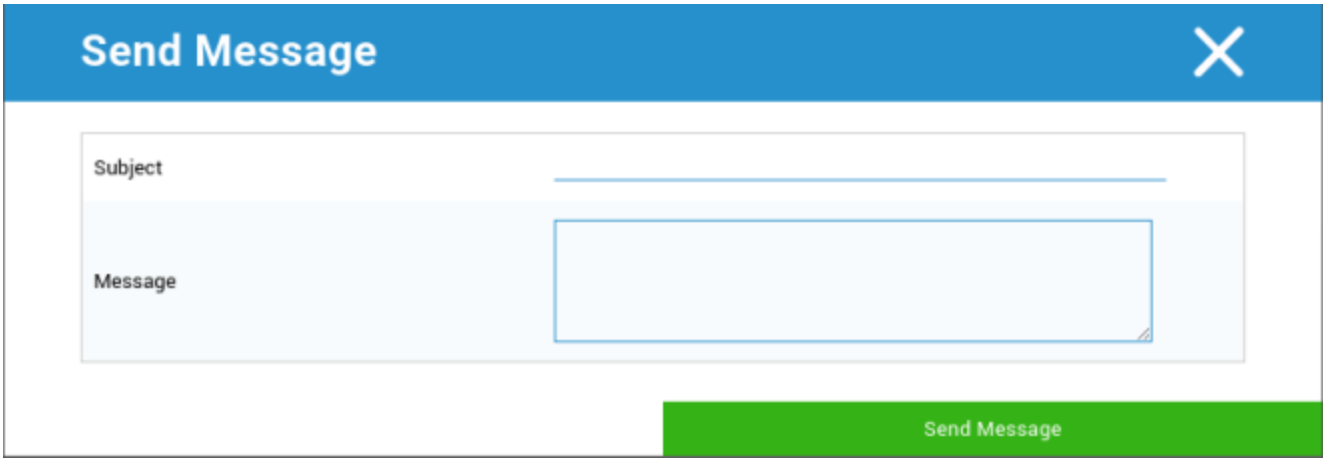
Wischen & Sperren (nur auf Geräteebene)

Unter "Wischen & Sperren" können Sie die folgenden drei Aktionen durchführen:

Vollständig abwischen	Das Gerät wird auf die Werkseinstellungen zurückgesetzt (Unternehmens- und persönliche Daten werden gelöscht)
Enterprise Wipe	Nur Unternehmensdaten werden vom Endbenutzergerät entfernt (alle Apps, Daten usw., die von AppTec bereitgestellt wurden)
Sperrbildschirm	Wenn die Bildschirmsperre aktiviert ist, reicht es aus, das Gerät mit dem Geräte-Passwort/PIN zu entsperren
Forensische Sperrung (nur überwachte Geräte)	Sollte diese Funktion mit dem Symbol  aktiviert werden, wird das Gerät gesperrt, indem eine Meldung angezeigt wird, die nicht geschlossen werden kann. Der Mitarbeiter kann das Gerät auch nicht entsperren. Nur der Administrator kann das Gerät in der Konsole mit dem Symbol zum Entsperren  entsperren.
Aktivierungssperre zulassen (nur überwachte Geräte)	Sollte diese Funktion aktiviert sein, wird das Gerät gesperrt, sobald "Mein iPhone suchen" in den iCloud-Einstellungen aktiviert ist.

Nachricht (nur auf Geräteebene)

Im folgenden Fenster können Sie den Betreff und eine Nachricht eingeben und an ein Endgerät senden:



Sicherheitskonfiguration

Passcode

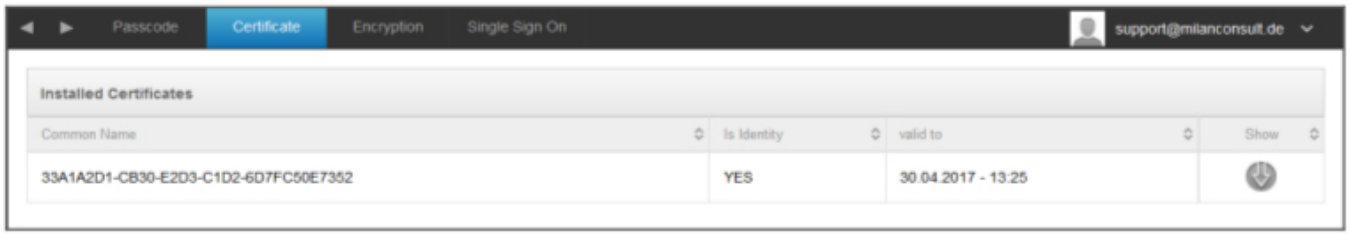
Hier legen Sie die Einstellungen für das Gerätepasswort fest

Code-Deaktivierung erlaubt	Wenn diese Einstellung aktiviert ist, gibt es keine Aufforderung zur Eingabe eines Passworts Sobald ein Passwort eingerichtet ist, kann es nicht mehr deaktiviert werden.
Einfachen Wert zulassen	Erlauben Sie dem Benutzer, die gleichen, eskalierenden und reduzierenden Nummernfolgen zu verwenden (z.B. 1234, 1111)
Alphanumerischer Wert erforderlich	Passwörter müssen mindestens einen Buchstaben enthalten
Mindestlänge des Passcodes	Minimale Passwortlänge
Mindestanzahl von komplexen Zeichen	Minimale Anzahl von alphanumerischen Symbolen im Passwort
Maximales Alter des Passcodes	Anzahl der Tage, nach denen das Passwort geändert werden muss
Maximum Auto-Lock	Maximale Zeit, nach der das Gerät gesperrt wird
Maximale Karenzzeit für die Gerätesperre	Zeit, nach der das Gerät in den gesperrten Stand-By
Maximale Anzahl von Fehlversuchen	Legt fest, wie oft ein Passwort falsch eingegeben werden kann, bevor ein komplettes Löschen des Geräts durchgeführt wird.
Maximales Alter des Passcodes (1-730 Tage)	Maximales Alter des Passworts
Passcode-Historie (1-50 Passcodes)	Die Verwendung eines alten Passworts ist nach dieser Zahl erlaubt

Ein Klick auf den Papierkorb öffnet den Passwort-Rücksetzungsdialog, mit dem ein vergessenes Gerätepasswort gelöscht werden kann.

Zertifikat (nur auf Geräteebene)

Zeigt die Zertifikate an, die auf dem Gerät verfügbar sind


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

Verschlüsselung

Verschlüsselung des Speichers verlangen	Aktivieren Sie die Verschlüsselungsfunktion des installierten Geräts

Einzelanmeldung

Unter dem Punkt "Single Sign-On" können Sie die Kerberos-Authentifizierung konfigurieren.

Hier legen Sie die Zugangsdaten und die entsprechenden URLs / Apps fest, die die Kerberos-Tokens verwenden dürfen.

Verfügbar im Überwachungsmodus	
Konto Name	Konto Name
Hauptperson Name	Eindeutige Identität, an die Kerberos-Tickets verteilt werden können
Reich	Ihr Kerberos-Realm, der verwendet werden soll (z.B. Ihre Domain)

Mit dem Symbol können Sie zusätzliche URLs einrichten.

URL-Muster, um dieses Konto einzuschränken	Noch zu bestimmende URLs, an die Kerberos-Tickets verteilt werden können

Mit dem Symbol können Sie zusätzliche Apps einrichten.

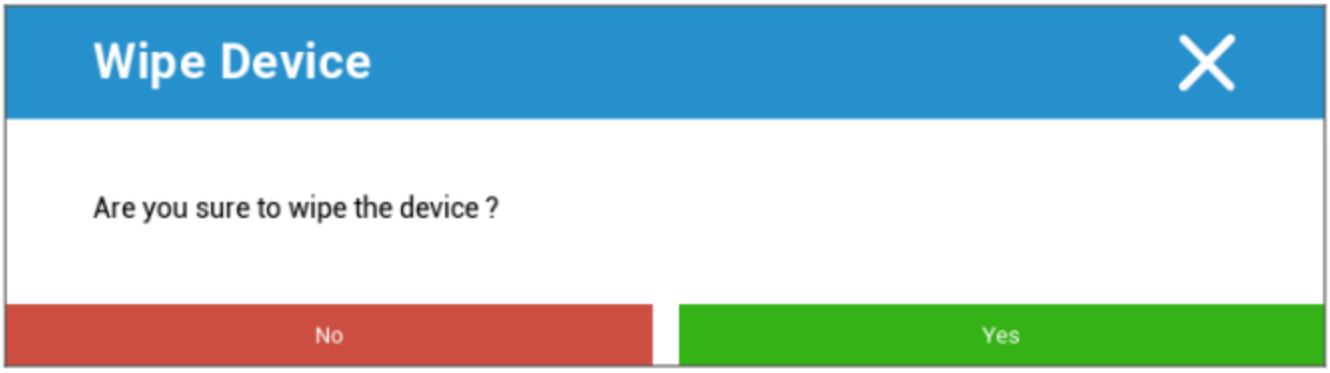
Apps zum Einschränken dieses Kontos	Noch zu bestimmende Apps, an die Kerberos-Tickets verteilt werden können

Ende der Lebensdauer (nur auf Geräteebene)

Wischen (nur auf Geräteebene)

Unter "Löschen" können Sie das Gerät auf seine Werkseinstellungen zurücksetzen. Hier werden sowohl die Unternehmensdaten als auch die privaten Daten auf dem Endgerät des Benutzers gelöscht.

Mit einem Klick auf das "Minus-Symbol" sollten Sie die folgende Meldung erhalten



Mit "Ja" können Sie die Löschung durchführen.

Unter "Wischbericht" können die folgenden Punkte angezeigt werden

Abgewischt von	Historie der Person, die den Wisch durchgeführt hat
Datum	Datum
Status	Status (z.B. ob der Löschvorgang erfolgreich durchgeführt wurde)

Einstellungen zur Einschränkung

Gerätefunktionalität

Hier können Sie einzelne Funktionen des Endgeräts sperren

Installation von Apps zulassen	Erlauben Sie die Installation von Apps
Kamera zulassen	Erlauben Sie die Verwendung der Kamera
FaceTime zulassen	FaceTime zulassen
Bildschirmaufnahme zulassen	Bildschirmaufnahme zulassen
Automatische Synchronisierung beim Roaming zulassen	Automatische Synchronisierung beim Roaming zulassen
Siri zulassen	Siri zulassen
Sprachanwahl zulassen	Sprachanwahl zulassen
In-App-Käufe zulassen	In-App-Käufe zulassen
iTunes Store-Passwort für alle Einkäufe erforderlich machen	iTunes Store-Passwort für alle Einkäufe erforderlich machen
Erlauben Sie Multiplayer-Spiele	Erlauben Sie Multiplayer-Spiele
Hinzufügen von Game Center Freunden zulassen	Hinzufügen von Game Center Freunden zulassen
Öffnen von verwaltet zu nicht verwaltet zulassen	Öffnen von Inhalten aus verwalteten Anwendungen in nicht verwalteten Anwendungen zulassen
Öffnen von nicht verwaltet zu verwaltet zulassen	Erlauben Sie das Öffnen von Inhalten in nicht verwalteten Anwendungen in verwalteten Anwendungen
Heute-Ansicht im Sperrbildschirm zulassen	Wenn diese Einstellung aktiviert ist, wird die Ansicht "Heute" im Benachrichtigungscenter auf dem Sperrbildschirm angezeigt.
Control Center auf dem Sperrbildschirm zulassen	Control Center auf dem Sperrbildschirm zulassen
TouchID zulassen	TouchID zulassen
Erlauben Sie Over-the-Air PKI-Updates	Erlauben Sie Over-the-Air PKI-Updates
Sparbuch bei Sperre zulassen	Sparbuch zulassen, während das Gerät gesperrt ist
Anzeigenverfolgung einschränken	Diese Funktion deaktiviert das Ad Tracking (z.B. können Werbetreibende Ad Tracking nicht verwenden, um personalisierte

	Werbung zu schalten)
Übergabe zulassen	Übergabe zulassen
Internet-Ergebnisse im Spotlight zulassen	Internet-Ergebnisse im Spotlight zulassen (z.B. Bing oder Wikipedia)
Bei der ersten AirPlay-Kopplung einen Passcode verlangen	Bei der ersten AirPlay-Kopplung einen Passcode verlangen
Force Watch Schutz für das Handgelenk	Wenn aktiviert, wird die Apple Watch gezwungen, den "Handgelenkschutz" (Handgelenkserkennung) zu verwenden
iCloud-Fotomediathek zulassen	Erlaubt die iCloud-Fotomediathek. Wenn Sie dies nicht zulassen, werden alle Bilder, die nicht vollständig aus iCloud heruntergeladen wurden, auf dem lokalen Speicher gelöscht.
Verfügbar im Überwachungsmodus	
Kontomodifikation zulassen	Änderung von "Mail, Kontakte, Kalender" zulassen
AirDrop zulassen	AirDrop zulassen
App Cellular Modification zulassen	Diese Einstellung blockiert die Einstellung, welche Apps mobile Daten verwenden dürfen Diese Einstellung kann z.B. manuell auf dem Endgerät des Benutzers vorgenommen werden und dann kann diese Einschränkung aktiviert werden
Erlauben Sie Siri die Abfrage von nutzergenerierten Inhalten aus dem Web	Die Websuche auf bestimmten Websites ist blockiert, z. B. Wikipedia, weil jeder nach Belieben Änderungen vornehmen kann
Siri-Schimpfwortfilter aktivieren	Schimpfwörter, die an Siri gerichtet sind, werden zensiert.
iBook Store zulassen	iBook Store zulassen
iBook Store Erotik zulassen	iBook Store Erotik zulassen
Ändern der Einstellungen von "Meine Freunde suchen" zulassen	Ändern der Einstellungen von "Meine Freunde suchen" zulassen
Game Center zulassen	Game Center zulassen
Host-Paarung zulassen	Computer koppeln
Erlauben Sie die Installation von Konfigurationsprofilen	Erlauben Sie die Installation von Konfigurationsprofilen
App entfernen zulassen	Entfernen von Kontroll-Apps

iMessage zulassen	iMessage zulassen
Erlauben Sie das Löschen aller Inhalte und Einstellungen	Erlauben Sie das Löschen aller Inhalte und Einstellungen
Erlauben Sie die Konfiguration von Einschränkungen	Erlauben Sie die Konfiguration von Einschränkungen
Podcast zulassen	Podcast zulassen
Nachschlagen von Definitionen zulassen	Nachschlagen von Definitionen zulassen
Prädiktive Tastatur zulassen	Prädiktive Tastatur zulassen
Auto-Korrektur zulassen	Automatische Korrektur zulassen
UI App Installation zulassen	Wenn diese Funktion deaktiviert ist, können keine Apps aus dem öffentlichen AppStore installiert werden (das Symbol wird nicht mehr angezeigt). Apps können jedoch weiterhin über iTunes und den Configurator installiert werden.
Tastaturkürzel zulassen	Tastaturkürzel zulassen, wenn das Gerät an eine physische Tastatur angeschlossen ist
Kopplung der Apple Watch zulassen	Verhindert eine Kopplung zwischen dem Gerät und der Apple Watch, bestehende Verbindungen werden abgebrochen
Änderung des Passcodes zulassen	Wenn nicht erlaubt, kann kein Gerätepasswort hinzugefügt, geändert oder entfernt werden.
Änderung des Devicenamens zulassen	Leitfaden zur Bestimmung, ob der Gerätename geändert werden kann
Änderung des Hintergrundbildes zulassen	Leitfaden zur Bestimmung, ob das Hintergrundbild geändert werden kann
Automatische App-Downloads zulassen	Wenn Sie diese Funktion deaktivieren, wird eine gekaufte App nicht automatisch auf anderen Geräten installiert. Gilt nicht für Updates für bestehende Apps
Nachrichten zulassen	Nachrichten auf dem iOS-Gerät zulassen
Vertrauen in Enterprise-Apps zulassen	Bei der Einstellung false wird das Vertrauen in Unternehmensanwendungen verhindert.

iCloud

Blockieren bestimmter Funktionen während der iCloud-Kopplung

Sicherung zulassen	Sicherung zulassen
Synchronisierung von Dokumenten zulassen	Synchronisierung von Dokumenten zulassen
Fotostream zulassen	Fotostream zulassen
Gemeinsamen Fotostream zulassen	Gemeinsamen Fotostream zulassen
Cloud-Schlüsselbund-Synchronisierung zulassen	Cloud-Schlüsselbund-Synchronisierung zulassen
Erlauben Sie verwalteten Anwendungen, Daten zu speichern	Erlauben Sie verwalteten Anwendungen, Daten zu speichern
Synchronisierung von Notizen und Markierungen für Unternehmensbücher zulassen	Synchronisierung von Notizen und Hervorhebungen für Unternehmensbücher zulassen
Erlauben Sie die Sicherung von Unternehmensbüchern	Erlauben Sie die Sicherung von Unternehmensbüchern

Sicherheit und Datenschutz

Blockieren Sie diese mit Diagnosedaten verbundenen Funktionen

Senden von Diagnosedaten an Apple zulassen	Erlauben Sie das Senden von Diagnosedaten an Apple
Dem Benutzer erlauben, nicht vertrauenswürdige TLS-Zertifikate zu akzeptieren	Dem Benutzer erlauben, nicht vertrauenswürdige TLS-Zertifikate zu akzeptieren
Verschlüsselte Backups erzwingen	Verschlüsselte Backups erzwingen

BYOD

Integrierte iOS-Sicherheit (Container)

iOS konnte schon immer zwischen verwalteten (geschäftlichen) und nicht verwalteten (privaten) Systemen unterscheiden. Alles, was aus dem MDM-System kommt, wird als verwaltet behandelt. Wenn Sie z.B. eine App über MDM installieren oder ein Exchange-Konto konfigurieren, wird dies als von iOS verwaltet behandelt.

Alles andere, was manuell auf dem Gerät konfiguriert/installiert wird, wird als nicht verwaltet behandelt. Zum Beispiel, wenn der Benutzer WhatsApp selbst installiert oder wenn er ein Exchange-Konto hinzufügt. Diese Trennung hat die Kontakte jedoch nie beeinträchtigt. Aber seit iOS 11.3 (und höher) wurde dies auch für die Kontakte hinzugefügt.

Da dies eine Grundfunktion des Betriebssystems ist, müssen Sie nichts installieren oder einen speziellen Container einrichten.

Aktivieren Sie die integrierte Funktion zur Trennung von privaten und geschäftlichen Anwendungen/Informationen/Dateien. Mit dieser Einstellung werden auch einige andere Funktionen deaktiviert, die sonst versehentlich Teile dieser Trennung ausschalten könnten.

Aktivierung

Aktivieren Sie die Container-Lösungen, die von AppTec360 unterstützt werden

Aktivieren Sie Google Divide Container	Aktivieren Sie Google Divide Container
SecurePIM Container einschalten	SecurePIM Container einschalten

Sollten Sie den SecurePIM Container aktiviert haben, finden Sie unter "Aktivierung" auch den folgenden Punkt. Außerdem werden sofort vier weitere Registerkarten geöffnet, die im Folgenden beschrieben werden.

Support-E-Mail-Adresse	Support-E-Mail-Adresse, an die sich ein Benutzer bei Problemen wenden kann

SecurePIM Kennwort

Unter "SecurePIM-Passwort" können Sie die Richtlinien für die Sicherheitsstärke des Passworts festlegen.

Zeitüberschreitung der Sitzung	Hier können Sie festlegen, nach wie vielen Minuten ein neues Passwort eingegeben werden muss, sobald SecurePIM im Hintergrund läuft
Passwort Länge	Passwortlänge für den Zugriff auf den SecurePIM Container
Großbuchstaben	Minimum Großbuchstaben
Kleinbuchstaben	Minimum Kleinbuchstaben
Besondere Zeichen	Minimum Sonderzeichen
Ziffern	Minimale Ziffern
Wischen Anwendung	Anzahl der Male, die ein Passwort falsch eingegeben werden kann, bevor der SecurePIM-Inhalt gelöscht wird (Die App verbleibt jedoch weiterhin auf dem Endgerät des Benutzers)

SecurePIM Sicherheit

Unter "SecurePIM-Sicherheit" können Sie eine Reihe von Sicherheitseinstellungen vornehmen.

Jailbroken-Geräte erkennen	Sollte diese Einstellung aktiviert sein, wird der Zugriff auf den SecurePIM Container blockiert, sobald das Gerät als jailbroken erkannt wird
Sichere Textfelder	Der Inhalt der Eingabefelder wird verschlüsselt, keine Information erreicht das Betriebssystem (iOS) Hinweis: Solange diese Einstellung aktiv ist, ist die Autokorrektur nicht mehr verfügbar.
Kontaktdaten auf das Gerät exportieren	Wenn diese Einstellung aktiviert ist, kann der Benutzer die Exchange-Kontakte auf sein lokales Gerät exportieren. Hinweis: Es werden nur der Name und die Telefonnummer exportiert.
Veranstaltungsort anzeigen	Wenn diese Einstellung aktiviert ist, wird der Ort der kommenden Ereignisse in der Benachrichtigungsleiste angezeigt
Veranstaltungstitel anzeigen	Wenn diese Einstellung aktiviert ist, wird der Ort des bevorstehenden Ereignisses in der Benachrichtigungsleiste angezeigt

SecurePIM-Browser

Hier können Sie den Browser von SecurePIM konfigurieren.

Mit dem Symbol können Sie eine neue URL definieren.

Mit dem Symbol können Sie eine definierte URL wieder entfernen.

"Whitelisted URLs" sind URLs, die geladen werden können.

"URLs auf der schwarzen Liste" sind URLs, die nicht geladen werden können und daher gesperrt sind.

Bitte beachten Sie, dass die Einträge auf der Whitelist eine höhere Priorität haben als die Einträge auf der Blacklist. Unter "Lesezeichentitel" können Sie einen Titel vergeben. Mit "Lesezeichen-URL" können Sie die URL-Adresse mit dem Titel des Lesezeichens verknüpfen - auf diese Weise können Sie individualisierte Lesezeichen an die jeweiligen Benutzer verteilen.

Tauschen Sie

Unter "Exchange" können Sie ein Exchange-Konto konfigurieren.

ActiveSync E-Mail Adresse	Exchange-E-Mail-Adresse (beachten Sie die "Platzhalter")
ActiveSync Exchange Anmeldung	Benutzernamen austauschen (beachten Sie die "Platzhalter")
ActiveSync Exchange Server	Exchange Server-Adresse (FQDN)
ActiveSync Exchange-Domäne	Exchange Domain-Adresse
Benutzer-Zertifikat	Benutzerzertifikat
Zertifikatsbasierte Authentifizierung	Benutzer authentifiziert sich mit einem Zertifikat
S/MIME-Verschlüsselung zulassen	Ermöglicht es dem Benutzer, seine E-Mails zu verschlüsseln
S/MIME-Signierung zulassen	Ermöglicht es dem Benutzer, seine E-Mails zu signieren
CRL-Prüfung	Falls aktiv, wird das private Zertifikat mit der CRL (Certificate Revocation List) verglichen.

Verbindungsmanagement

Wi-Fi

Services Set Identifier (SSID)	SSID des Netzwerks, mit dem eine Verbindung hergestellt werden soll
Auto Join	Aktivieren Sie den automatischen Beitritt beim Beitritt zu einem Netzwerk
Verborgenes Netzwerk	Aktivieren, für den Fall, dass der AP die SSID nicht sendet

Proxy-Einrichtung

Konfigurieren eines Proxys für jeden Access Point

Keine	Keine Vollmacht einrichten
Handbuch	Einen manuellen Proxy einrichten
Proxy-Server-URL	Adresse für den Zugriff auf die Proxy-Einstellungen
Hafen	Legen Sie den Port für den Proxy fest
Authentifizierung	Benutzernamen für die Authentifizierung auf dem Proxy
Passwort	Passwort für die Authentifizierung auf dem Proxy
Automatisch	Automatisch einen Proxy einrichten
Proxy-Server-URL	URL für den Zugriff auf die Proxy-Einstellungen

Sicherheit Typ

Sicherheitstyp für den AP einrichten

WEP	
Passwort	Passwort für den AP

WPA/WPA2	
Passwort	Passwort für den AP

WEP Unternehmen - WPA / WPA2 Unternehmen - Jedes Unternehmen			
	Protokolle		
	TLS	Aktivieren/Deaktivieren	
	TTLS	Aktivieren/Deaktivieren	
	LEAP	Aktivieren/Deaktivieren	
	PEAP	Aktivieren/Deaktivieren	
	EAP-FAST	Aktivieren/Deaktivieren	
	EAP-SIM	Aktivieren/Deaktivieren	
	PAC verwenden		Verwendung von PAC (Protected Access Controll)
	Rückstellung PAC	Konfiguration der Provision PAC	
	Anonyme Bereitstellung von PAC	Anonyme Bereitstellung von PAC	
	Innere Authentifizierungen	Authentifizierungsprotokoll, das verwendet werden soll: PAP, CHAP, MSCHAP, MSCHAPv2	
	Benutzername	Benutzername für die Authentifizierung	
	Verwenden Sie kein Passwort pro Verbindung	Verwenden Sie kein Passwort pro Verbindung	
	Identitätszertifikat	Authentifizierungszertifikat hochladen/auswählen	
	Äußere Identität	Identität, die von außen sichtbar ist	
	Vertrauen Sie		
	Vertrauenswürdiges Zertifikat 1	Erstes vertrauenswürdiges Zertifikat hochladen	
	Vertrauenswürdiges Zertifikat 2	Zweites vertrauenswürdiges Zertifikat hochladen	
	Vertrauenswürdiges Zertifikat 3	Drittes vertrauenswürdiges Zertifikat hochladen	
	Namen von Zertifikaten für vertrauenswürdige Server	Die Namen der erwarteten Serverzertifikate	

		(in einer durch Komma getrennten Liste)	

Keine	Keine Sicherheit einrichten

VPN

Name der Verbindung	Name des VPN-Profils

VPN-Typ

VPN

Der gesamte Netzwerkverkehr des Geräts wird über eine VPN-Verbindung geleitet.

Verbindungstyp	VPN-Verbindungstyp einrichten
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
Benutzerdefiniertes SSL	Verbindung über Custom SSL
OpenVPN	OpenVPN-Protokoll

Pro-App VPN

Wenn Sie eine bestimmte App öffnen, wird eine VPN-Verbindung aufgebaut

Automatischer Start einer Per-App VPN-Verbindung	Automatischer Start einer Per-App VPN-Verbindung
Verbindungstyp	VPN-Verbindungstyp einrichten
Cisco AnyConnect	AnyConnect-Protokoll
Juniper SSL	Juniper SSL-Protokoll
F5 SSL	F5 SSL-Protokoll
SonicWall mConnect	SonicWall mobile Connect
Aruba VIA	Aruba VIA-Protokoll
Benutzerdefiniertes SSL	Verbindung über Custom SSL
OpenVPN	OpenVPN-Protokoll

Proxy-Einrichtung

Konfigurieren eines Proxys für die VPN-Verbindung

Keine	Keine Vollmacht einrichten
Handbuch	Manuelles Einrichten eines Proxys
Proxy-Server-URL	Adresse für den Zugang zu den Proxy-Einstellungen
Hafen	Legen Sie den Port für den Proxy fest
Authentifizierung	Benutzername für die Authentifizierung beim Proxy
Passwort	Passwort für die Authentifizierung beim Proxy
Automatisch	Automatisch einen Proxy einrichten
Proxy-Server-URL	URL für den Zugriff auf die Proxy-Einstellungen

Platzhalter anzeigen	Zeigt alle verfügbaren Benutzervariablen an, die AppTec360 verwenden kann.

APN

Name des Zugangspunkts	Name des Zugangspunkts
Benutzername für den Zugangspunkt	Benutzername des Access Point
Passwort für den Zugangspunkt	Passwort für den Zugangspunkt
Proxy-Server	Proxy Server Adresse
Hafen	Der jeweilige Proxy-Port

Zellulär

Daten-Roaming aktivieren	Daten-Roaming aktivieren
Aktivieren Sie Voice Roaming	Aktivieren Sie Voice Roaming
Hotspot aktivieren	Hotspot aktivieren

HTTP-Proxy

Proxy Typ	
Handbuch	Einen Proxy manuell einrichten
Proxy-Server-URL	Adresse für den Zugriff auf die Proxy-Einstellungen
Hafen	Proxy-Port einrichten
Authentifizierung	Benutzername für die Authentifizierung beim Proxy
Passwort	Passwort für die Authentifizierung beim Proxy
Automatisch	Automatisch einen Proxy einrichten
Proxy PAC URL	Proxy PAC URL
Direkte Verbindung zulassen, wenn PAC nicht erreichbar ist	Direkte Verbindung (ohne VPN) zulassen, wenn PAC nicht erreichbar ist
Erlaubt die Umgehung des Proxys für den Zugriff auf firmeneigene Netzwerke	Erlauben Sie die Umgehung des Proxys für den Zugriff auf firmeninterne Netzwerke

AirPrint

IP-Adresse	IP-Adresse des Druckers
Ressource Pfad	Eindeutiger Pfad zum AirPrint-Gerät

AirPlay

Gerät Name	Name des Geräts
Passwort	Passwort für die Kopplung
Whitelist	Definieren Sie eine Liste von Geräten, mit denen sich das Gerät exklusiv koppeln kann

PIM-Verwaltung

Exchange Active Sync

Konto Name	Name des E-Mail-Kontos
Exchange ActiveSync-Host	Adresse/FQDN des Servers
Verschieben zulassen	Erlauben Sie das Verschieben von E-Mails
Nur in der Post verwenden	Interaktionen können nur in der nativen Mail-App auftreten
SSL verwenden	Verwenden Sie SSL-Verschlüsselung
Domain	Server-Domäne
Benutzer	Benutzername
eMail-Adresse	E-Mail Adresse (nur auf Geräteebene)
Passwort (nur auf Geräteebene)	Benutzer-Passwort
Identitätszertifikat	Wählen Sie das entsprechende Zertifikat für die Authentifizierung am Server
Vergangene Tage von Mail to Sync	Anzahl der Tage, bis die E-Mails zurück synchronisiert werden sollen. Kein Limit = unbegrenzt
Aktivieren Sie S/MIME	Aktivieren Sie die S/MIME-Verschlüsselung
Zertifikat signieren	Laden Sie das entsprechende Signierzertifikat hoch
Verschlüsselungszertifikat	Laden Sie das entsprechende Verschlüsselungszertifikat hoch

eMail

Einrichtung von POP3 / IMAP-Konten auf dem Endgerät des Benutzers

Konto Beschreibung	Name des E-Mail-Kontos		
Konto Typ	IMAP	Pfad-Präfix	Das Pfadpräfix für spezielle Ordner
	POP		
Benutzer Display Name	Anzeigename des Benutzers		
E-Mail Adresse	Benutzer-E-Mail-Adresse		
Verschieben zulassen	Erlauben Sie das Verschieben von E-Mails		
Aktivieren Sie S/MIME	Aktivieren Sie die S/MIME-Verschlüsselung		
Zertifikat signieren	Laden Sie das entsprechende Signierzertifikat hoch		
Verschlüsselungszertifikat	Laden Sie das entsprechende Verschlüsselungszertifikat hoch		

Eingehende Post

Einstellungen für eingehende Server

Mail Server Adresse	Mail Server Adresse
Mail Server Port	Mail-Server-Port
Benutzer Name	Entsprechender Nutzername
Art der Authentifizierung	Art der Authentifizierung
Keine	Kein Authentifizierungstyp
Passwort (nur auf Geräteebene)	Passwortabfrage
MDM-Herausforderung-Antwort	
NTLM	NTLM-Authentifizierung
HTTP MD5-Digest	
SSL verwenden	Verwenden Sie SSL, falls erforderlich

Ausgehende Post

Einstellungen für den Ausgangsserver

Mail Server Adresse	Mail Server Adresse
Mail Server Port	Mail Server Port
Benutzer Name	Entsprechender Benutzername
Art der Authentifizierung	
Keine	Keine Authentifizierungsmethode
Passwort (nur auf Geräteebene)	Passwortabfrage
MDM-Herausforderung-Antwort	
NTLM	NTLM-Authentifizierung
HTTP MD5-Digest	
SSL verwenden	Verwenden Sie SSL, falls erforderlich
Ausgehendes Passwort gleich wie eingehendes	Ausgehendes Passwort gleich wie eingehendes
Nur in der Post verwenden	Aktivieren Sie diese Option, wenn alle ausgehenden E-Mails über die Mail-App versendet werden sollen.

CalDav

Konfigurieren Sie die Einrichtung und Verteilung eines CalDav-Kontos

Konto Beschreibung	Anzeigename des Kontos
Hostname	Hostname und/oder IP-Adresse
Hafen	Port des CalDav-Kontos
Haupt-URL	Haupt-URL des Kontos
Benutzername	Entsprechender CalDav-Benutzername
Passwort (nur auf Geräteebene)	Entsprechendes CalDav-Passwort
SSL verwenden	Verwenden Sie SSL, falls erforderlich

Abo-Kalender

Einrichten und Verteilen von abonnierten Kalendern

Beschreibung	Anzeigename des Kontos
URL	URL der Kalenderdatenbank
Benutzername	Benutzername des Kalenderabonnements
Passwort (nur auf Geräteebene)	Passwort des Kalenderabonnements
SSL verwenden	Verwenden Sie SSL, falls erforderlich

LDAP

Richten Sie in diesem Bereich eine LDAP-Verbindung ein, um einen dynamischen Zertifikatsaustausch zwischen dem Endbenutzergerät und dem Active Directory zu ermöglichen.

Bitte beachten Sie, dass der ausgewählte Benutzer die entsprechende Leseberechtigung benötigt.

Konto Beschreibung	Konto Beschreibung
Konto-Benutzername	Benutzer für LDAP-Zugang
Konto-Passwort	Passwort für LDAP-Zugang
Konto Hostname	LDAP Server Hostname/IP-Adresse
SSL verwenden	Verwenden Sie SSL, falls erforderlich

Im zweiten Teil können Sie individuelle Filter für die Suche in der LDAP-Registrierung definieren.

Beschreibung	Umfang	Basis durchsuchen
Filter Beschreibung	Suchebene in der LDAP-Registrierung	Definieren Sie den individuellen Filter

Web Management

Webclips

Hier können Sie Lesezeichen mit Links zu Webseiten, Intranetportalen usw. definieren, die auf dem Endgerät des Benutzers als Anwendung angezeigt werden.

Etikett	Name der Verbindung auf dem Endbenutzergerät
URL	Link zur jeweiligen Website
Abnehmbar	Wenn aktiviert, kann der Benutzer den Webclip entfernen
Ikone	Über diesen Dialog können Sie ein Logo für die Verbindung hochladen: Abmessungen 180x180, png-Format
Vorgefertigte Ikone	Wenn aktiviert, werden keine zusätzlichen Effekte (Schatten, Reflexion) auf dem Symbol angezeigt.
Vollbild	Wenn Sie Webclips öffnen, öffnet sich der Browser im Vollbildmodus

Web-Inhaltsfilter

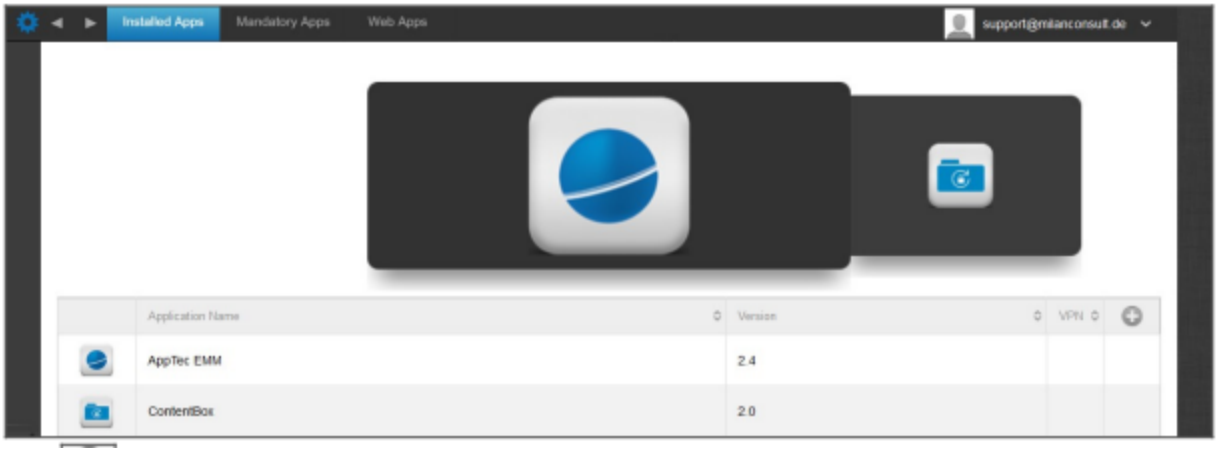
Der Web Content Filter ermöglicht es, den Zugriff auf bestimmte Internetseiten zu beschränken.

Erlaubte Websites	
Inhalte für Erwachsene einschränken	Webfilter wird automatisch auf nicht jugendfreie Inhalte angewendet
Erlaubte URLs	Mit dem Symbol + fügen Sie zulässige Seiten hinzu
Auf der schwarzen Liste stehende URLs	Mit dem Symbol + fügen Sie gesperrte Seiten hinzu
Nur bestimmte Websites	Es können nur bestimmte Inhalte angezeigt werden, die Sie mit dem Symbol + hinzufügen können.

App Verwaltung

Enterprise App Manager

Installierte Apps (nur auf Geräteebene)



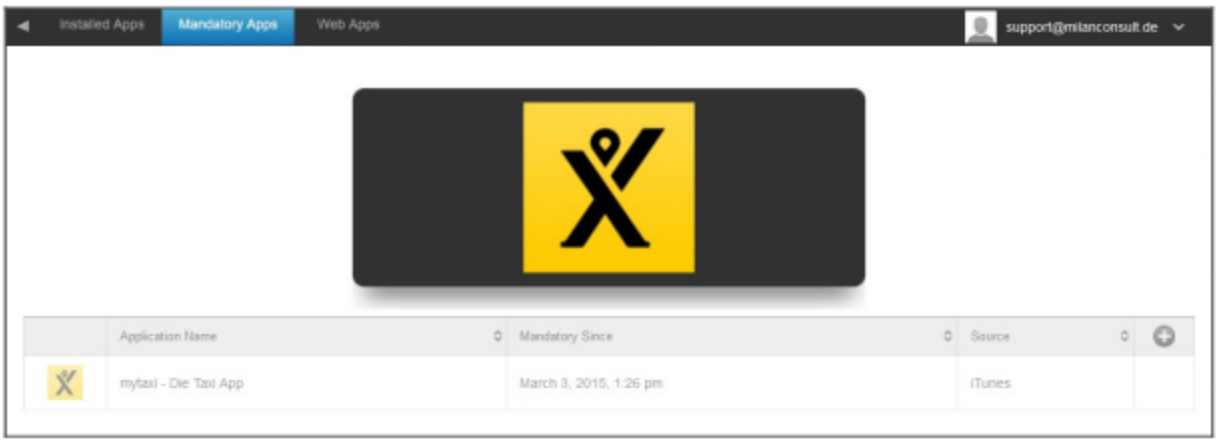
Hier können Sie die Apps sehen, die derzeit auf dem Gerät installiert sind.

Obligatorische Apps

Unter Obligatorische Apps können Sie notwendige Apps festlegen.

Der Benutzer wird ständig daran erinnert, diese App zu installieren.

Über die kann die mandatierte App definiert werden.



Dies kann eine Apple App Store App sein, aber auch eine In-House App.

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

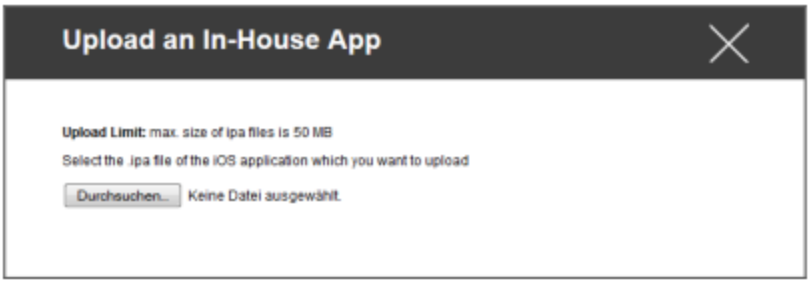
Sie können sowohl eine "Apple AppStore" App aus dem öffentlichen AppStore als auch eine intern entwickelte In-House App auf das Gerät übertragen.

Oder Sie können aus der Kategorie "iOS In-House Apps" eine In-House App auswählen, die Sie unter Allgemeine Einstellungen hochgeladen haben.

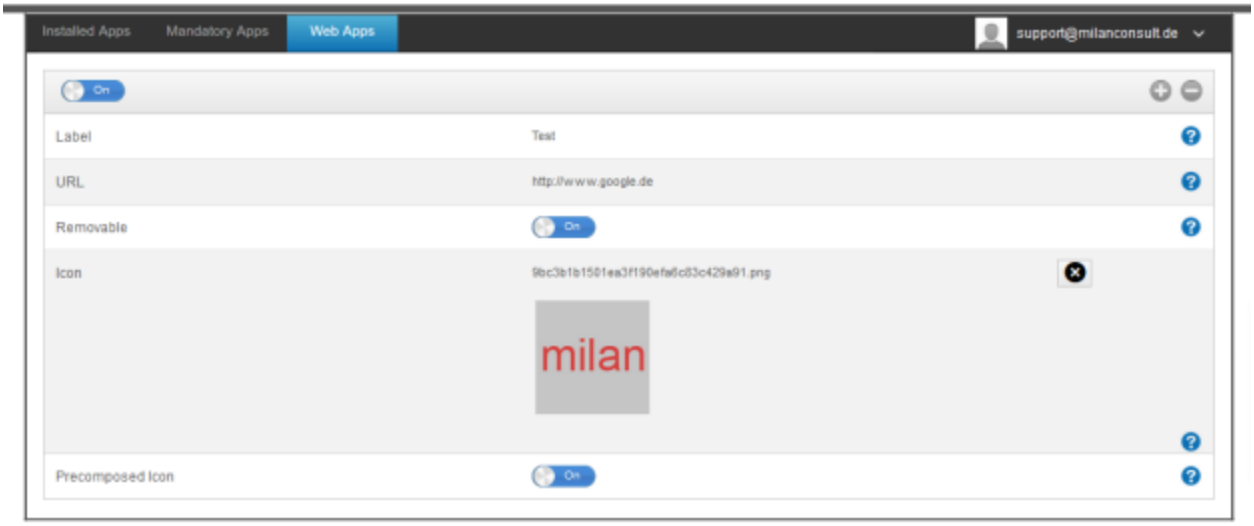
Installations-Optionen

Auf dem neuesten Stand halten (nur für VPP pro Gerät unterstützt)	Einmal pro Woche wird ermittelt, ob es ein Update für die App gibt. Wenn ja, wird dieses Update installiert Für In-House Apps wird das Update-Ziel, das Sie in den Allgemeinen Einstellungen konfiguriert haben, für den Update-Prozess verwendet.
Überholen, wenn nicht verwaltet	Wenn die App bereits installiert ist, übernimmt das MDM die App und verwaltet sie
App entfernen, wenn MDM-Profil entfernt wird	Im Falle einer Entfernung durch die Geräteverwaltung wird die App deinstalliert.
Verhindern Sie die Sicherung von App-Daten	Ein Backup der app-spezifischen Daten wird nicht erstellt
App Einstellung	Unter "App-Einstellungen" können Sie der App bestimmte Werte in den Vordergrund stellen (sofern die App dies unterstützt, fragen Sie ggf. den Entwickler der App).

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



Web Apps



Unter dem Punkt "Web Apps" können Sie, ähnlich wie bei "Web Clips", im Bereich Web Management Internetseiten oder Intranetportale als Anwendung auf das Endgerät des Benutzers schieben. Web-Apps werden standardmäßig im Vollbildmodus angezeigt, der unter Webclips konfiguriert werden kann.

Etikett	Name der Verbindung auf dem Endbenutzergerät
URL	Link zur jeweiligen Website
Abnehmbar	Wenn aktiviert, kann der Benutzer den Webclip entfernen
Ikone	Über diesen Dialog können Sie ein Logo für die Verbindung hochladen: Abmessungen 180x180, png-Format
Vorgefertigte Ikone	Wenn aktiviert, werden keine zusätzlichen Effekte (Schatten, Reflexion) auf dem Symbol angezeigt.

Einschränkung & Einstellungen

Auf der schwarzen Liste / Whitelist stehende Apps

Hier können Sie die Apps festlegen, die abhängig von Ihren Einstellungen unter "Allgemeine Einstellungen" blockiert (oder erlaubt) werden. Ein Klick darauf öffnet die bekannte App-Suche. Dort können Sie nach den Apps suchen, die Sie hinzufügen möchten.

Beachten Sie, dass für diese Funktion ein überwachtes Gerät erforderlich ist

SysApp-Einschränkungen

Blockieren Sie bestimmte Apps oder Funktionen Ihres Geräts

Erlauben Sie die Nutzung von YouTube	Erlauben Sie die Nutzung von YouTube
Verwendung des iTunes Store zulassen	Verwendung des iTunes Store zulassen
Verwendung von Safari zulassen	Verwendung von Safari zulassen
Autofill aktivieren	Erlaubt das automatische Ausfüllen
Warnung vor Betrug	Erzwingt die Betrugswarnung
JavScript aktivieren	Ermöglicht die Verwendung von JavaScript
Pop-ups blockieren	Blockiert alle Arten von Verpuppungen
Cookies zulassen	Legen Sie fest, wann Safari Cookies akzeptieren soll

App-VPN

Über das Symbol können Sie Anwendungen definieren, die beim Start automatisch die ausgewählte VPN-Verbindung starten.

App-Einstellungen

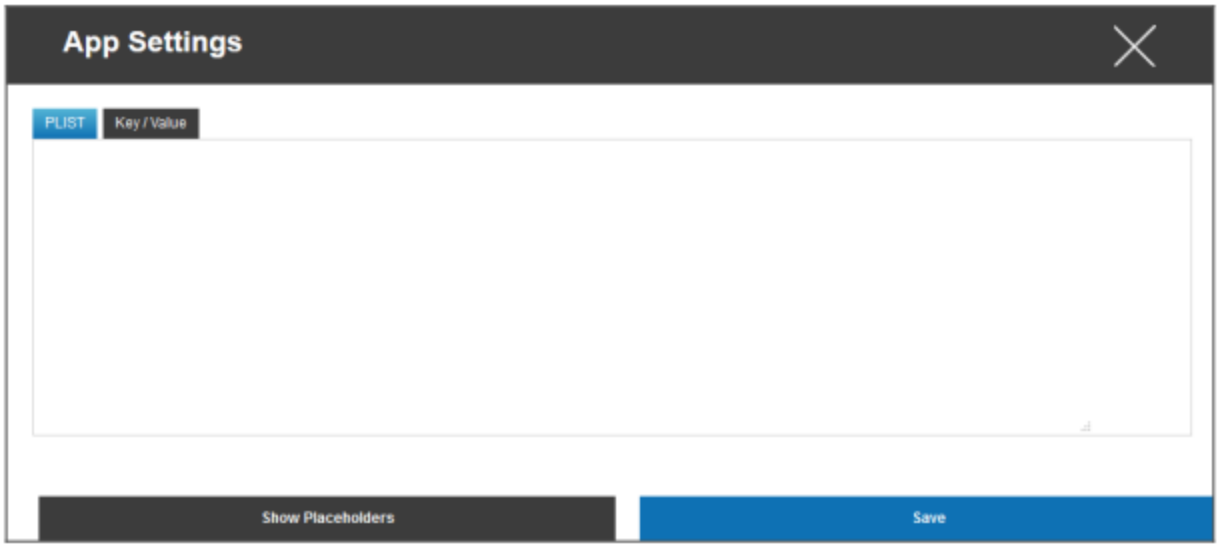
Unter "App-Einstellungen" können Sie der App bestimmte Werte in den Vordergrund stellen (sofern die App dies unterstützt, fragen Sie ggf. den Entwickler der App).

Über das Symbol fügen Sie eine (zusätzliche) App hinzu. Hier finden Sie wieder die bekannte AppTec360-Darstellung eines App-Imports.

Suchen Sie hier nach der App, die Sie konfigurieren möchten, und wählen Sie sie aus. Die Einstellungen gelten nur für verwaltete Apps.

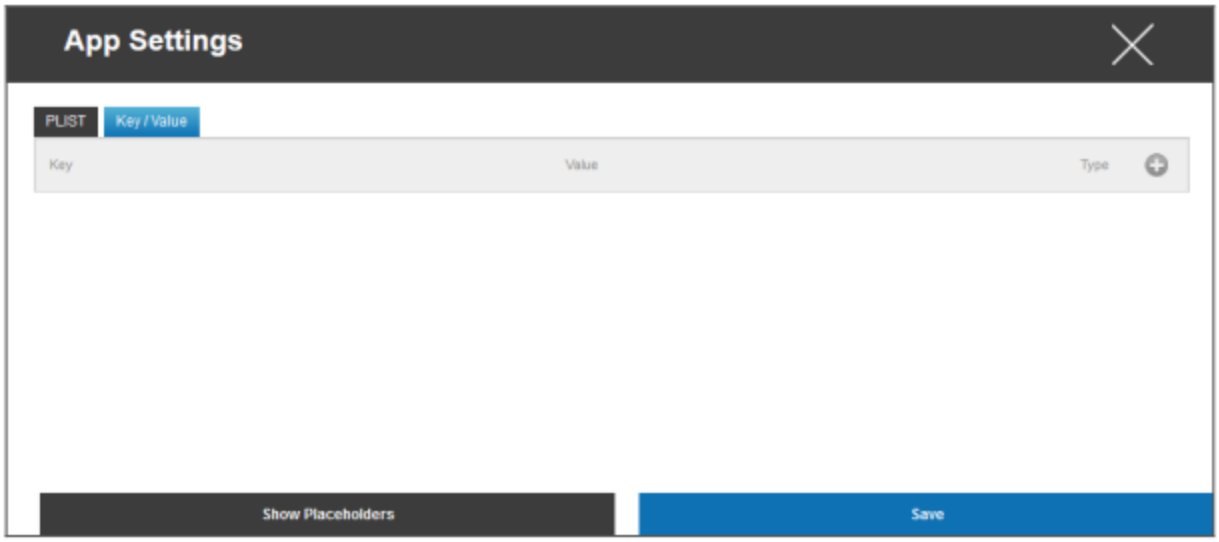
Sollte der Import erfolgreich gewesen sein, sehen Sie die folgende Anzeige:

Mit einem Klick auf können Sie nun eine Vielzahl von Konfigurationen vornehmen. Sie erhalten dann die folgende Übersicht:

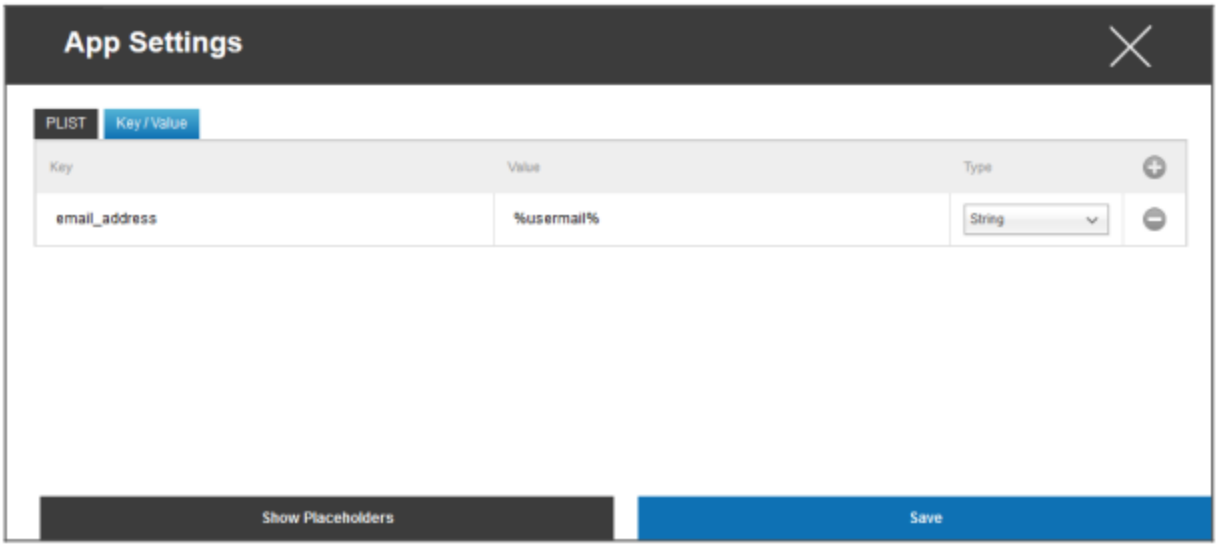


Sollten Sie bereits eine PLIST (Quelltext der Konfiguration) haben, können Sie diese hier hinzufügen und alles mit "Speichern" speichern.

Unter "Schlüssel / Wert" können Sie der App bestimmte Konfigurationen zuordnen



Hier können Sie einen neuen Schlüssel und seinen Wert mit dem Symbol festlegen.



Natürlich stehen Ihnen alle Platzhalter von AppTec zur Verfügung

Erklärung "Typ":

String	Text
Boolesche	Richtig/Falsch
Nummer	Nummer

Mit dem Symbol können Sie eine App wieder entfernen.

Enterprise App Store

iTunes Apps

Unter diesem Punkt können Sie optionale Apps für Ihren Benutzer verteilen.

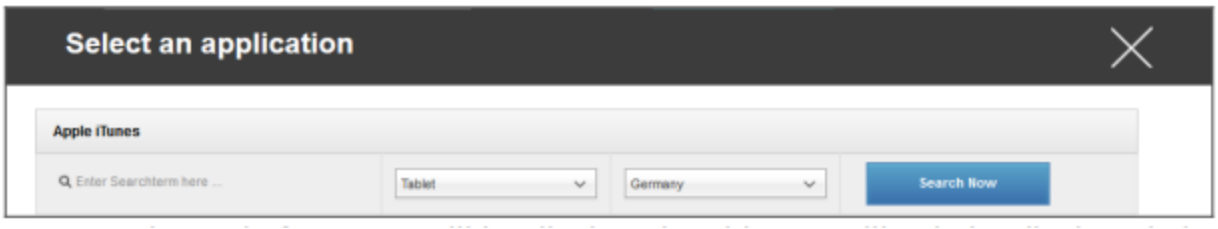
Sollte sich hier eine App befinden, wird sie automatisch auf dem Endgerät des AppTec360 Store installiert.

Dies sind lediglich Links zum offiziellen Apple App Store. Aus diesem Grund muss jedes Endgerät mit einer Apple ID ausgestattet sein.

An dieser Stelle empfehlen wir, dass jeder Benutzer seine eigene Apple ID hat.

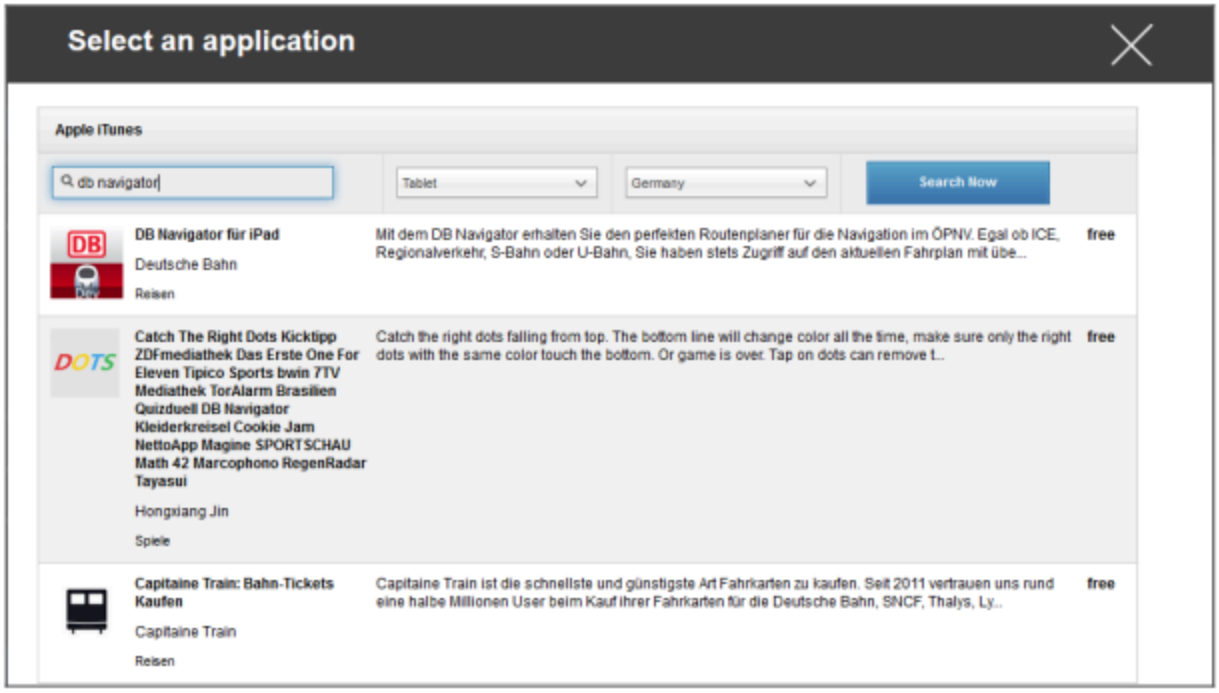
Mit dem Symbol können Sie zusätzliche Apps hinzufügen.

Daraufhin sollte sich ein Fenster mit der folgenden Übersicht öffnen.



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

Unter "Suchbegriff hier eingeben ..." können Sie nach einer App suchen, die sich im Apple App Store befindet.



Sobald Sie auf das Symbol oder den Namen der App klicken, werden Sie erneut aufgefordert, zusätzliche Konfigurationen vorzunehmen.

Auf dem Laufenden bleiben	Einmal pro Woche wird ermittelt, ob es ein Update für die App gibt. Wenn ja, wird dieses Update installiert
App entfernen, wenn MDM-Profil entfernt wird	Im Falle einer Entfernung durch die Geräteverwaltung wird die App deinstalliert.
Verhindern Sie die Sicherung von App-Daten	Ein Backup der app-spezifischen Daten wird nicht erstellt
App-VPN	Wählen Sie eine VPN-Verbindung, die beim Öffnen der App gestartet wird

Nach einem Klick auf "Installieren" wird die App dem Enterprise App Store hinzugefügt und kann dann über den AppTec360 AppStore auf dem Endgerät des Benutzers installiert werden.

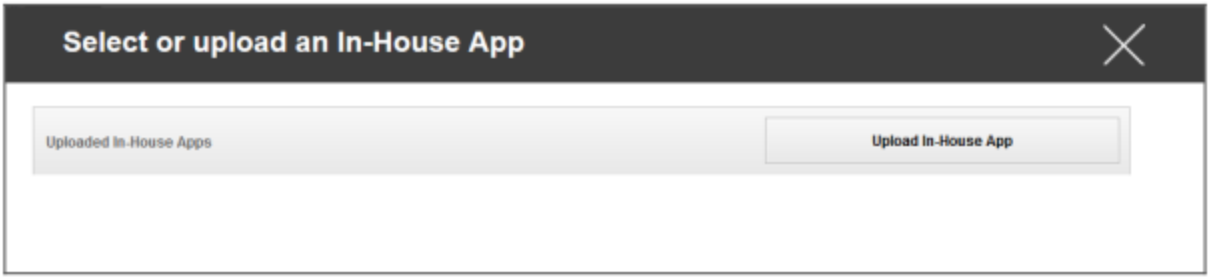
Wenn der App-Store-Import erfolgreich durchgeführt wurde, erhalten Sie die folgende Übersicht:

Hausintern

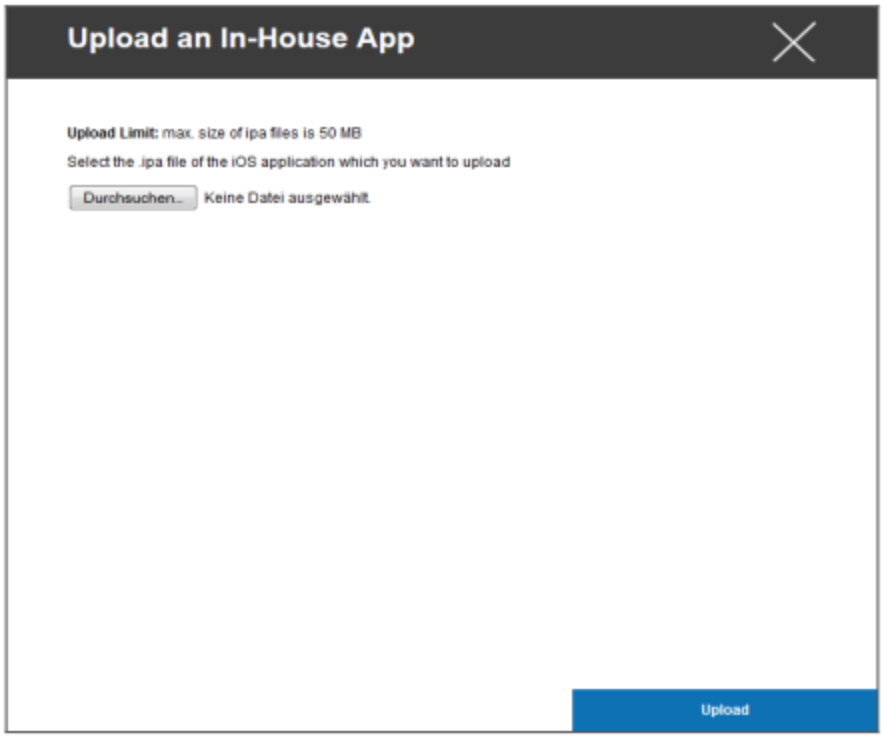
Unter dem Punkt "In-House" können Sie intern entwickelte Apps hochladen und vertreiben.

Mit dem Symbol können Sie zusätzliche In-House Apps vertreiben.

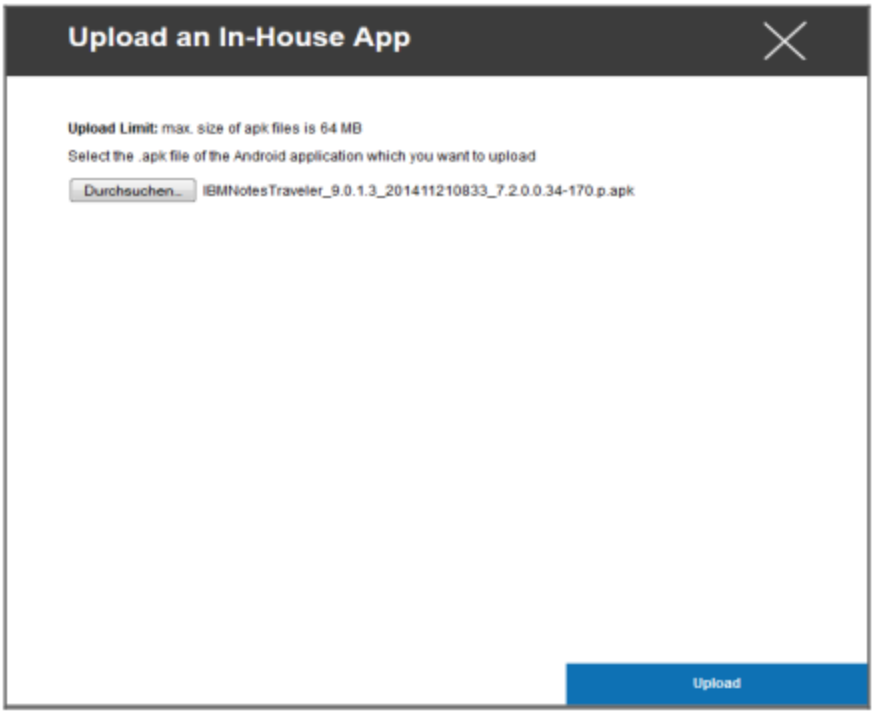
Wenn Sie noch nie eine In-House App vertrieben haben, erhalten Sie anschließend die folgende Übersicht:



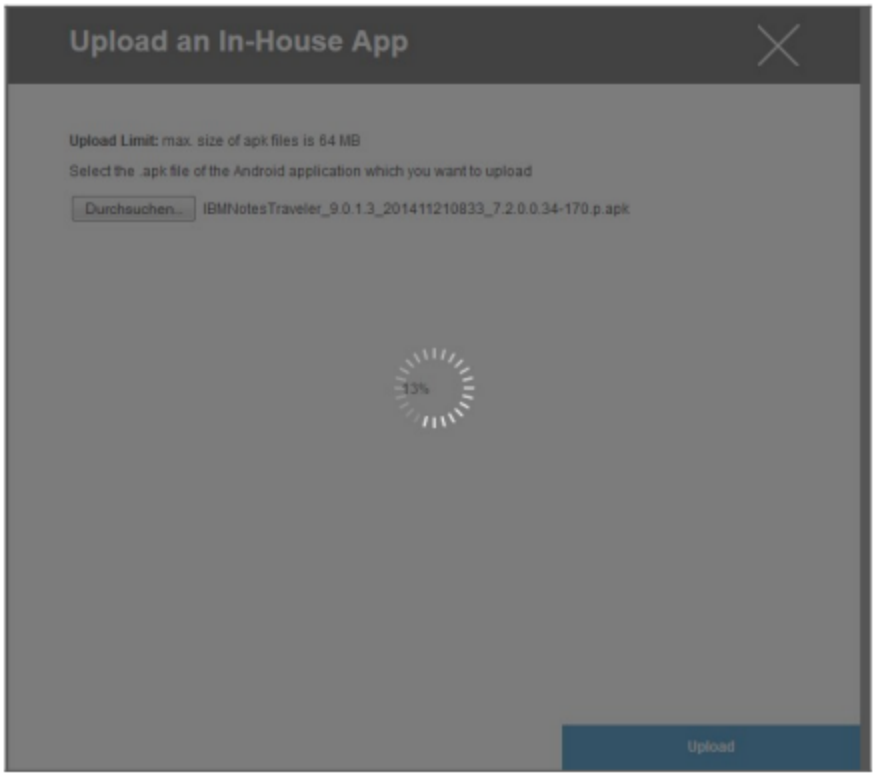
Klicken Sie dazu auf "In-House App hochladen", Sie erhalten dann die folgende Übersicht:



Wählen Sie nun mit "Suchen..." eine .ipa-Datei aus und klicken Sie dann auf "Hochladen".



Ihre App wird nun hochgeladen. In der Mitte des Kreises sehen Sie den Prozentsatz, wie viel von Ihrer App bereits hochgeladen wurde.



Sollte der Upload der In-House App erfolgreich durchgeführt worden sein, sehen Sie die neu hochgeladene App in Ihrem App-Katalog.

Der Benutzer hat nun die Möglichkeit, diese App im AppTec360 Store auf dem Endgerät unter der Kategorie "In-House" zu sehen und zu installieren.

Da es sich hierbei nicht um eine öffentliche Apple AppStore App handelt, benötigt der Benutzer keine gespeicherte Apple ID auf dem Endgerät.

Kiosk-Modus

Der iOS Kiosk-Modus ist nur im überwachten Modus verfügbar

Im Kioskmodus können Sie eine App oder eine URL vordefinieren, so dass es möglich ist, ausschließlich diese App/URL auszuführen/zu besuchen.

Außerdem können Sie im Kioskmodus verschiedene Hardwaretasten deaktivieren.

Anwendungstyp

Paket

Wenn Sie die App im Kioskmodus starten möchten, wählen Sie unter "Anwendungstyp" die Option "Paket".

Kiosk-Anwendung	Klicken Sie hier, um eine App auszuwählen, die im Kioskmodus starten soll Sie finden die aktuelle Übersicht der App-Verwaltung Sie können zwischen "Apple iTunes Apps" und "iOS In-House Apps" wählen.

URL

Wenn Sie eine URL im Kioskmodus starten möchten, wählen Sie unter "Anwendungstyp" die Option "URL".

URL	Definieren Sie nun die gewünschte URL-Adresse
Politik der gleichen Herkunft	Wenn diese Funktion aktiviert ist, kann der Benutzer nur auf den Unterseiten der vordefinierten URL surfen Wenn Sie zum Beispiel die folgende URL definiert haben: www.mypage.com, dann kann der Benutzer auf www.mypage.com/subpage surfen.
URLs auf der Whitelist	Hier können Sie eine Whitelist pflegen, alle diese URLs sind erlaubt Maximal 1 URL pro Zeile Eine URL muss mit http:/ oder https:// beginnen.
Auf der schwarzen Liste stehende URLs	Hier können Sie eine Schwarze Liste führen, in der alle diese URLs nicht zugelassen sind Maximal 1 URL pro Zeile Eine URL muss mit http:/ oder https:// beginnen.
Browser nach Inaktivität löschen	Nach Inaktivität wird der Browser-Cache geleert
Exit-Passwort Aktiviert	Wenn Sie diese Funktion aktivieren, hat der Benutzer die Möglichkeit, den Kioskmodus mit einem von Ihnen vordefinierten Passwort zu beenden
Exit-Passwort	Dies ist das von Ihnen vordefinierte Passwort

Einstellungen für den Kioskmodus

Geplanter Kiosk-Modus	Basierend auf der Tageszeit können Sie den Kioskmodus so einstellen, dass der Modus automatisch zu einer vorher festgelegten Zeit gestartet und beendet wird.
Startzeit	Startzeit
Zeit in Minuten	Zeit in Minuten, nach der der Kioskmodus wieder beendet werden soll
Touch deaktivieren	Falls aktiviert, ist der Touchscreen deaktiviert
Gerätedrehung deaktivieren	Falls aktiviert, ist die automatische Bildschirmanpassung deaktiviert
Ruftonschalter deaktivieren	Falls aktiviert, wird der Ruftonschalter dann deaktiviert. Von da an ist das Verhalten abhängig von der zuvor eingestellten Funktion
Lautstärketasten deaktivieren	Falls aktiviert, werden die Lautstärketasten deaktiviert
Deaktivieren der Sleep Wake Taste	Falls aktiviert, wird der Ein/Aus-Schalter deaktiviert
Automatische Sperre deaktivieren	Falls aktiviert, wird das Gerät nicht in den Standby-Modus versetzt.
Aktivieren Sie Voice Over	Falls aktiviert, wird der Voice Over Assistant aktiviert
Zoom aktivieren	Falls aktiviert, wird der Zoom aktiviert
Farben invertieren aktivieren	Falls aktiviert, wird der invertierte Anzeigemodus aktiviert
Assistive Touch aktivieren	Falls aktiviert, wird das AssistiveTouch aktiviert
Aktivieren Sie die Sprachauswahl	Falls aktiviert, wird die Sprachauswahl aktiviert
Mono-Audio aktivieren	Falls aktiviert, wird Mono-Audio aktiviert.
VoiceOver	Falls aktiviert, kann der Benutzer VoiceOver aktivieren
Zoomen	Falls aktiviert, kann der Benutzer Zoom aktivieren
Farben invertieren	Wenn aktiviert, kann der Benutzer invertierte Farben aktivieren
Assistive Touch	Falls aktiviert, kann der Benutzer die Berührungsunterstützung aktivieren

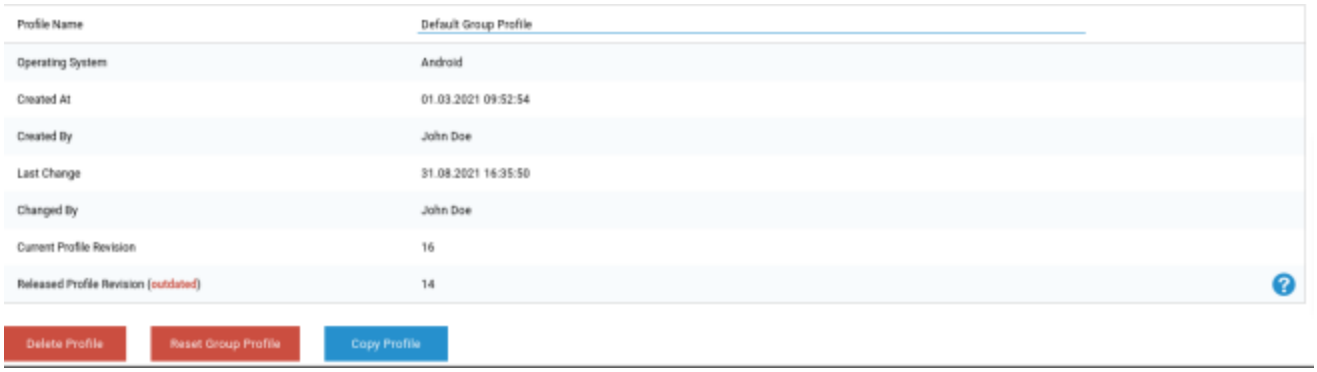
Android Enterprise – Vollständig verwaltete Gerätekonfiguration

Je nachdem, ob Sie gerade ein Gruppenprofil oder ein Gerät ausgewählt haben, unterscheiden sich die Übersicht und ihre Unterpunkte - bitte beachten Sie dies sorgfältig!

Allgemein

Gruppenprofilübersicht (nur auf Gruppenebene)

Wenn Sie ein Gruppenprofil öffnen, erhalten Sie einen schnellen Überblick über das Profil.



Profil Name	Name des Profils (kann hier geändert werden)
Betriebssystem	Betriebssystem, für das das Profil bestimmt ist
Erstellt am	Zeitpunkt der Erstellung
Erstellt von	Der Ersteller des Profils
Letzte Änderung	Zeitpunkt der letzten Änderung des Profils
Geändert von	Konto, das die letzten Änderungen vorgenommen hat
Aktuelle Profilüberarbeitung	Revision des gespeicherten Profilstatus
Freigegebene Profil-Revision	Zugewiesene Profilrevision ("Jetzt zuweisen"). Wenn das Etikett hinter dem Text "(veraltet)" anzeigt, bedeutet dies, dass Sie das Profil zwar gespeichert, aber noch nicht zugewiesen haben, so dass die Geräte noch eine ältere Version erhalten.

Geräteübersicht (nur auf Geräteebene)

Sollten Sie sich auf einem Gerät befinden, erhalten Sie eine Übersicht über das gewählte Gerät, die folgendes enthält:

Gerät Name	Name des Geräts
Standort	Standort-Koordinaten
Telefon Nummer	Rufnummer
Zugewiesene obligatorische Apps	Anzahl der zugewiesenen obligatorischen Apps
OS Version	OS-Version des Geräts
Betriebssystem	Betriebssystem (Android Enterprise)
Seriennummer	Seriennummer des Geräts
Geräteeigentum	Firmen- oder Privatgerät
Gerätetyp	AE Work Managed Device
Verwurzelt	Status, der anzeigt, ob das Gerät gerootet wurde
Konform	Konform mit der Richtlinie
IP-Adresse	IP-Adresse des Geräts
Zuletzt gesehen	Zeitpunkt, zu dem sich das Gerät zuletzt mit AppTec verbunden hat
Letzter Schub	Zeitpunkt, zu dem der letzte Push an das Gerät gesendet wurde
AE Geräteeigentümer-Modus	Ja
Benutzerzuordnung	Der Benutzer oder die Gruppe, der dieses Gerät zugewiesen ist

Config Revision (nur auf Geräteebene)

Hier erhalten Sie einen Überblick darüber, welches Gruppenprofil dem Gerät zugewiesen ist.

Wenn Sie auf das Gruppenprofil klicken, erhalten Sie direkten Zugriff auf dieses Profil und können Einstellungen vornehmen.

Mit diesem Symbol können Sie die verteilten Apps auf die Einstellungen des Gruppenprofils zurücksetzen.

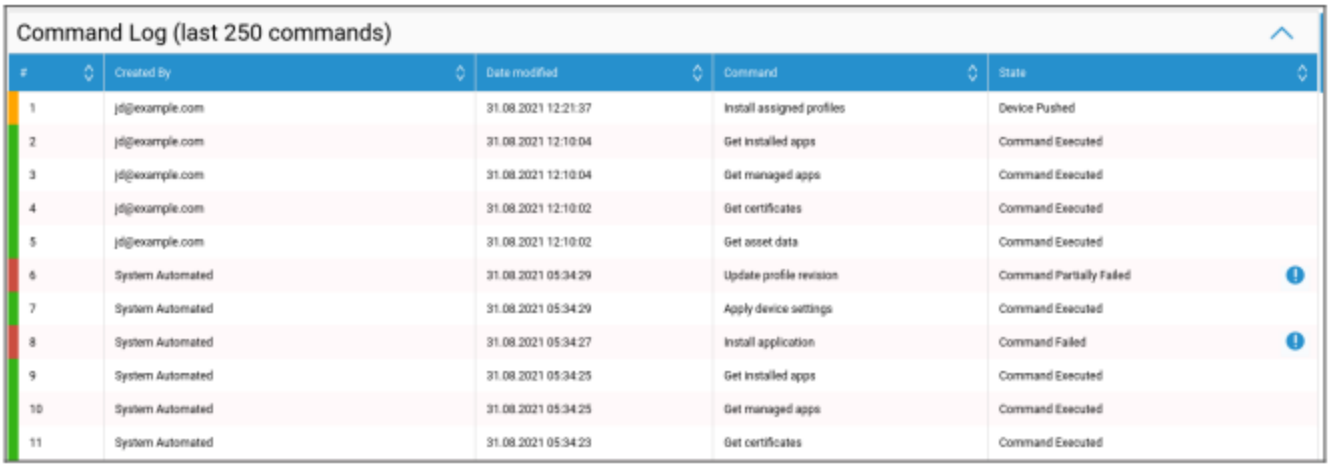
Mit diesem Symbol können Sie alle verwendeten Apps auf die Einstellungen des Gruppenprofils zurücksetzen.

"Neuere Revision verfügbar" bedeutet, dass das Gruppenprofil geändert und gespeichert, aber nicht zugewiesen wurde. Das Gruppenprofil muss mit "Jetzt zuweisen" auf Gruppenebene zugewiesen werden, um die Änderungen auf die Geräte anzuwenden.

Geräteprotokoll (nur auf Geräteebene)

Befehl Log

Hier können Sie sehen, welche Befehle für das Gerät erteilt wurden und welchen Status sie haben.



Mit "System Automated" erstellte Befehle werden automatisch vom System erstellt.

Mögliche Befehlszustände

Gerät geschoben	Eine Push-Anfrage wurde an den Push-Dienst (z.B. APNS) gesendet, um das Gerät anzuweisen, sich wieder mit dem EMM-Server zu verbinden.
Befehl erstellt	Der Befehl wurde im System erstellt.
Befehl gesendet	Der Befehl wurde an das Gerät gesendet, nachdem es sich mit dem Server verbunden hat.
Befehl Ausgeführt	Der Befehl wurde erfolgreich ausgeführt.
Befehl fehlgeschlagen	Der Befehl ist fehlgeschlagen. *
Befehl Teilweise fehlgeschlagen	Je nach Betriebssystem des Geräts können einige Befehle in Gruppen zusammengefasst werden. Dabei sind einige Teile dieser Befehlsgruppe fehlgeschlagen. *
Befehl ausgeführt, eventuell fehlgeschlagen	Der Befehl wurde ausgeführt, aber vielleicht auch nicht.
Kommando zurückgeschoben	Der Befehl wurde von einem Benutzer erneut gesendet.
Weggeworfen	Der Befehl wurde verworfen. Zum Beispiel, weil er durch einen anderen Befehl ersetzt wurde oder das Gerät neu registriert wurde und alte Befehle entfernt wurden

Wenn sich hinter der Nachricht ein Ausrufezeichen befindet, können Sie weitere Informationen erhalten, indem Sie mit dem Mauszeiger über das Symbol fahren.

Geräteeinstellungen

Client-Konfiguration

Hier können Sie die folgenden Konfigurationen auf Ihrem Android-Gerät vornehmen:

Zeit der Nichteinhaltung	Das Zeitlimit für die Benutzerantwort, nach dem die Durchsetzungsmaßnahme angewendet wird.
Durchsetzungsmaßnahmen nach Ablauf der Einhaltungsfrist	Durchsetzungsmaßnahmen, wenn ein Benutzer keine Aktionen durchführt, die zu einem konformen Gerätestatus führen
Häufigkeit der Datenerhebung	Häufigkeit, mit der Geräte-/GPS-Informationen gesammelt werden sollen
Herzschlagfrequenz des Geräts	Intervall, in dem das Gerät den AppTec360 Server kontaktieren soll Min. 1 Minute Max. 24 Stunden
Standortaktualisierungen aktivieren	Wenn aktiviert, sendet das Gerät Standortaktualisierungen an den AppTec360 Server
Standort Aktualisierungszeit	Legt fest, in welchen Zeitabständen das Gerät Standortaktualisierungen an AppTec360 sendet.
Verwenden Sie Google Location Accuracy für die Standortaktualisierung	Wenn aktiviert, wird der Netzwerkstandort für Standortaktualisierungen verwendet (wenn dies unter "Einschränkungen" deaktiviert wurde, hat diese Einstellung keine Auswirkungen).
GPS-Standort für Standortaktualisierung verwenden	Falls aktiviert, wird das GPS für Standortaktualisierungen verwendet.
Attraktive (gefälschte) Standorte zulassen	Ermöglicht das Fälschen von Standortinformationen über Apps von Drittanbietern
Aktion "Verlorene Verbindung	Wenn diese Option aktiviert ist, können Sie eine Aktion für den Fall festlegen, dass ein Gerät innerhalb des Heartbeat-Intervalls keine Verbindung zum MDM-Server erhält. Wenn das Gerät zum Beispiel eine Heartbeat-Zeit von 5 Minuten hat, verbindet es sich um 10:35 Uhr mit dem Server. Danach verlässt das Gerät die Wi-Fi-Reichweite. Der nächste Heartbeat um 10:40 Uhr wird fehlschlagen und die angegebene Aktion wird ausgeführt.
Aktion	Die Maßnahmen, die zu ergreifen sind, sobald ein Gerät nicht mehr konform ist.

		• Gerät sperren = Gerät sperren • Gerät löschen = Das Gerät wird auf die Werkseinstellungen zurückgesetzt. • Gerät und SD-Karte löschen = Das Gerät wird auf die Werkseinstellungen zurückgesetzt und der Speicher der SD-Karte wird gelöscht.
	Schwellenwert	Sie können einen Schwellenwert für fehlgeschlagene Heartbeats angeben, die notwendig sind, um die angegebene Aktion auszulösen.

Modus zur Durchsetzung von Richtlinien	Standard:	Die Benutzer werden in regelmäßigen Abständen aufgefordert, ausstehende Aktionen auszuführen
	Faule Durchsetzung von Richtlinien:	Die Benutzer werden nie aufgefordert, ausstehende Aktionen auszuführen. Alle offenen Aktionen werden im AppTec360 Client angezeigt
	Aggressive Durchsetzung von Richtlinien:	Benutzer werden ununterbrochen aufgefordert, ausstehende Aktionen auszuführen
AppTec360 Versionssperre	Wenn aktiviert, kann ein Versionscode für den AppTec360 MDM Client angegeben werden. Der AppTec360-Client wird nur auf die angegebene Version aktualisiert. Neuere Versionen werden ignoriert. Ein Downgrade ist NICHT möglich.	
Version Code	Versionscode für den AppTec360 MDM Client, auf den gesperrt werden soll.	
AppTec360-Benachrichtigung deaktivieren	Wenn diese Option deaktiviert ist, zeigt der AppTec360 Client keine Benachrichtigung in der Benachrichtigungsleiste an. So können Benutzer den AppTec360-Client über den Task-Manager schließen. Wenn der AppTec360-Client geschlossen ist, funktionieren verschiedene Funktionen wie der Kioskmodus und das Black-/Whitelisting von Apps nicht richtig. Samsung Geräte bieten einen Schutzmechanismus für den AppTec360 Client. Die Benachrichtigung ist auf Samsung-Geräten, die die KNOX-APIs unterstützen, standardmäßig deaktiviert. Die Benachrichtigung sollte bei Geräten mit Android 8.0 oder höher nicht deaktiviert werden.	

Tapete

Benutzerdefiniertes Hintergrundbild einstellen	Aktivieren/Deaktivieren des benutzerdefinierten Hintergrundbildes
Tapete	Stellen Sie den Hintergrundmodus so ein, dass ein Farbcode oder ein Bild verwendet wird.
Eine Farbe angeben	Geben Sie eine Hintergrundfarbe als Hex-Wert an, z.B. #000000 für Schwarz oder #ffffff für Weiß.
Bild als Hintergrundbild festlegen	Laden Sie die Bilddatei hoch, die Sie als Hintergrundbild verwenden möchten

Asset Management (nur auf Geräteebene)

Geräte-Infos

Modell	Bezeichnung des Gerätemodells
Betriebssystem	OS
OS Version	OS-Version
Seriennummer	Seriennummer
Gerät Name	Name des Geräts
Akku-Status	Status der Batterie
Freier / Gesamter Speicher	Freier / Gesamter Speicher
Samsung Safe	Samsung SAFE-Schnittstelle, erforderlich für eine Vielzahl von Einstellungsmöglichkeiten
SD-Karte verfügbar	SD-Karte verfügbar
Emulierte SD-Karte	SD-Karte emuliert
SD-Karte herausnehmbar	SD-Karte herausnehmbar
SD Freier / Gesamter Speicher	SD Freier / Gesamter SD-Kartenspeicher

Wi-Fi

IP-Adresse	IP-Adresse des Geräts
WiFi MAC	WiFi MAC-Adresse

Zellulär

Status	Status (SIM-Karte installiert)
Telefon Nummer	Telefon Nummer
Roaming (Sprache/Daten)	Roaming für Sprache/Daten
Roaming-Status	Aktueller Roaming-Status
IP-Adresse	IP-Adresse
Betreiber/Transporteur	Betreiber/Transporteur
Zellulare Technologie	Zellulare Technologie
IMEI	IMEI-Nummer
ICCID	Dies ist die ID für die SIM-Karte, oft auch eine Smartcard oder Integrated Circuit Card (ICC)
IMSI	Die International Mobile Subscriber Identity (IMSI) bietet in GSM- und UMTS-Mobilfunknetzen eine eindeutige Identifizierung der Netznutzer Die IMSI besteht aus maximal 15 Ziffern und wird auf folgende Weise konfiguriert: • Mobiler Ländercode (MCC), 3-stellig • Mobile Network Code (MNC), 2 oder 3 Ziffern • Mobile Subscriber Identification Number (MSIN), 1-10 Ziffern
Aktuelle MCC/MNC	Siehe "SIM MCC/MNC".
SIM MCC/MNC	Der Mobile Country Code ist eine etablierte Länderkennung, die von der ITU gemäß E.212 festgelegt wurde. Standard. Dieser funktioniert in Verbindung mit dem Mobile Network Code (MNC) zur Identifizierung des Mobilfunknetzes. Bedeutet den Länder-/Mobilfunknetzcode der SIM-Karte. Wenn Sie in ein anderes Mobilfunknetz roamen, sind die "Aktuelle MCC/MNC" und die "SIM MCC/MNC" logischerweise unterschiedlich.

Bluetooth

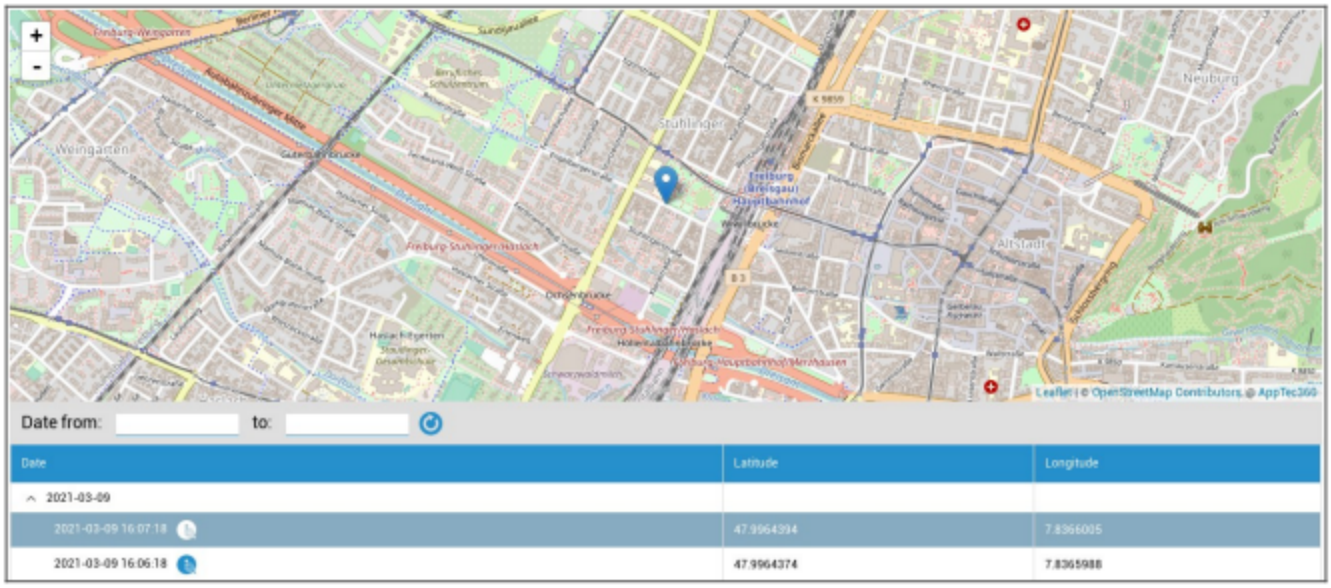
Bluetooth MAC	Bluetooth MAC-Adresse

Sicherheitsmanagement

Anti-Diebstahl (nur auf Geräteebene)

GPS-Informationen (nur auf Geräteebene)

Hier können Sie den aktuellen/letzten Standort des Geräts festlegen. Die Lokalisierung kann mit einem oder sogar zwei Passwörtern geschützt werden - Siehe: Allgemeine Einstellungen - Datenschutz - GPS-Zugang



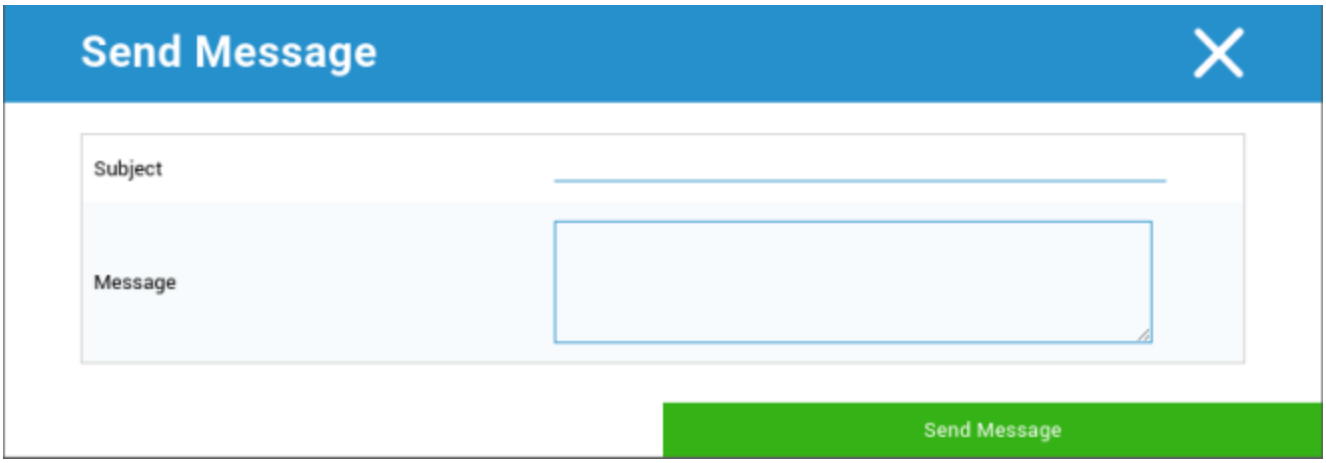
Wischen & Sperren (nur auf Geräteebene)

Unter "Wischen & Sperren" können Sie die folgenden drei Aktionen durchführen:

Vollständig abwischen	Das Gerät wird auf die Werkseinstellungen zurückgesetzt (Unternehmens- und persönliche Daten werden gelöscht)
Enterprise Wipe	Nur Unternehmensdaten werden vom Endbenutzergerät entfernt (alle Apps, Daten usw., die von AppTec360 bereitgestellt wurden)
Sperrbildschirm	Wenn die Bildschirmsperre aktiviert ist, reicht es aus, das Gerät mit dem Geräte-Passwort/PIN zu entsperren

Nachricht (nur auf Geräteebene)

Hier können Sie den Betreff und eine Nachricht eingeben und sie an ein Endgerät senden.



Sicherheitskonfiguration

Geräte-Passcode

Unter "Passcode" können Sie ein Gerätepasswort vergeben. Folgende Einstellungsmöglichkeiten stehen Ihnen zur Verfügung

Minimale Passwortlänge	Legt fest, wie viele Symbole ein Passwort mindestens enthalten muss	
Passwort Qualität	Nicht spezifiziert	Diese Richtlinie enthält keine Anforderungen an das Passwort.
	Biometrisch Schwach	Diese Richtlinie ermöglicht eine biometrische Erkennungstechnologie mit geringer Sicherheit. Dies setzt Technologien voraus, die die Identität einer Person bis auf eine etwa 3-stellige PIN erkennen können (die Falscherkennung liegt bei weniger als 1 zu 1.000).
	Etwas	Diese Richtlinie erfordert die Festlegung eines Kennworts oder Musters, erzwingt aber keine spezifischen Regeln.
	Alphabetisch	Der Benutzer muss ein Passwort eingegeben haben, das mindestens Buchstaben (oder andere Symbole) enthält.
	Alphanumerisch	Der Benutzer muss ein Passwort eingegeben haben, das mindestens sowohl numerische als auch alphabetische Zeichen (oder andere Symbole) enthält.
	Komplexe	Der Benutzer muss ein Passwort eingegeben haben, das standardmäßig mindestens einen Buchstaben, eine Ziffer und ein Sonderzeichen enthält. Mit dieser Passwortqualität können Passwörter auf verschiedene Zeichengruppen beschränkt werden, z. B. mindestens einen Großbuchstaben usw.
Minimale Passwortlänge	Legen Sie die erforderliche Anzahl von Zeichen für das Passwort fest. Sie können zum Beispiel verlangen, dass PINs oder Passwörter mindestens sechs Zeichen haben müssen.	
Mindestens erforderliche numerische Ziffern im Passwort	Mindestens erforderliche numerische Ziffern im Passwort	

Mindestens Kleinbuchstaben im Passwort erforderlich	Mindestens Kleinbuchstaben im Passwort erforderlich
Mindestens Großbuchstaben im Passwort erforderlich	Mindestens Großbuchstaben im Passwort erforderlich
Mindestens erforderliche Nicht-Buchstaben-Zeichen im Passwort	Mindestens erforderliche Nicht-Buchstaben-Zeichen im Passwort
Mindestens erforderliche Symbole im Passwort	Mindestens erforderliche Symbole im Passwort

Sperre für maximale Inaktivitätszeit	Maximale Benutzerinaktivität bis zur Zeitsperre
Zeitlimit für den Ablauf des Passworts	Legt fest, nach welchem Zeitintervall das Passwort abläuft und ein neues Passwort vergeben werden muss
Einschränkung des Passwortverlaufs	Anzahl der zuvor verwendeten Passwörter, die nicht erlaubt sind
Maximale Anzahl fehlgeschlagener Passwortversuche	Legt fest, wie oft ein Passwort falsch eingegeben werden kann, bevor ein komplettes Löschen des Geräts durchgeführt wird.
Biometrische Authentifizierung zulassen	Ermöglicht die Authentifizierung per Fingerabdruck oder Irisscan. Nur für Samsung KNOX 2.1 und höher

AntiVirus

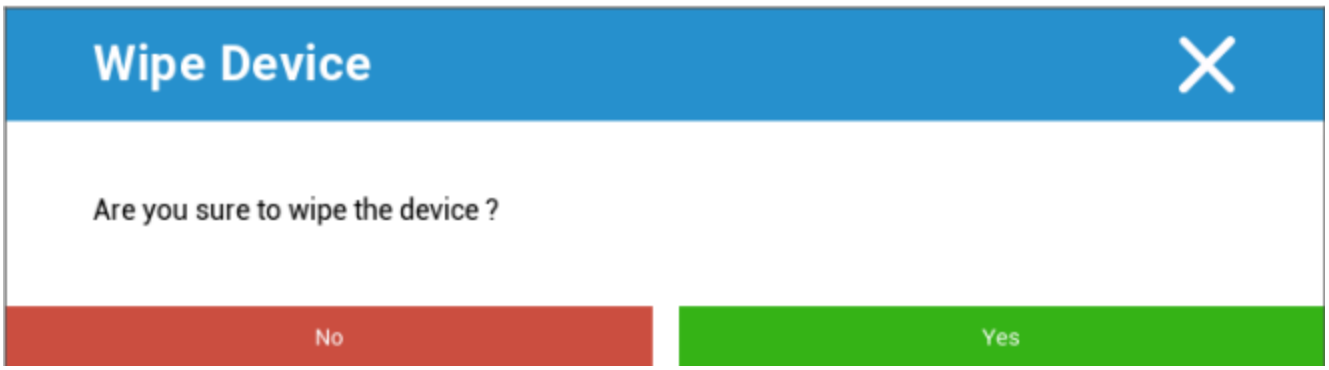
Automatischer Scan	Regelmäßige automatische Scans aktivieren
Scan-Intervall	Intervall für die Untersuchung (Schnell / Vollständig)
Vollständiger automatischer Scan	Vollständige automatische Scans aktivieren
Automatische Updates	Aktivieren Sie automatische Updates
Intervall der Aktualisierungsprüfung	Wie oft die App und ihre Datenbank aktualisiert werden sollten (Viren / beschädigter Code)
App-Schutz	Automatischen App-Scan aktivieren
SD-Karten Schutz	Automatischen SD-Karten-Scan einschalten
Nur Wi-Fi Update	Wenn diese Option aktiviert ist, werden Updates nur dann angewendet, wenn das Gerät erfolgreich mit einem Wi-Fi-Netzwerk verbunden ist.

Ende der Lebensdauer (nur auf Geräteebene)

Wischen (nur auf Geräteebene)

Unter "Löschen" können Sie das Gerät auf seine Werkseinstellungen zurücksetzen. Hier werden sowohl die Unternehmensdaten als auch die privaten Daten auf dem Endgerät des Benutzers gelöscht.

Mit einem Klick auf das "Minus-Symbol" erhalten Sie die folgende Meldung:



Mit "Ja" können Sie die Löschung durchführen.

Unter "Wischbericht" können die folgenden Punkte angezeigt werden

Abgewischt von	Historie der Person, die den Wisch durchgeführt hat
Datum	Datum
Status	Status (z.B. ob der Löschvorgang erfolgreich durchgeführt wurde)

Einstellungen zur Einschränkung

Beschränkungen

Hier kann eine Vielzahl von Dingen eingeschränkt und blockiert werden.

Kamera einschalten	Verwendung der Kamera zulassen	
Auto-Synchronisation erzwingen	Auf	Die Synchronisierung ist permanent aktiviert
	Aus	Die Synchronisierung ist dauerhaft deaktiviert
	Wahl des Benutzers	Vom Benutzer ausgewählt
Bluetooth erzwingen	Auf	Bluetooth ist permanent aktiviert
	Aus	Bluetooth ist dauerhaft deaktiviert
	Wahl des Benutzers	Vom Benutzer ausgewählt
GPS erzwingen	Auf	GPS ist permanent aktiviert
	Aus	GPS ist dauerhaft deaktiviert
	Wahl des Benutzers	Vom Benutzer ausgewählt
Force Network Standort	Auf	Permanente Internet-Lokalisierung
	Aus	Dauerhafte Deaktivierung der Internet-Lokalisierung
	Wahl des Benutzers	Vom Benutzer ausgewählt

Sicherheit		
Freigabeort verbieten	Gibt an, ob ein Benutzer die Standortfreigabe nicht einschalten darf.	
Abgesicherten Start nicht zulassen	Gibt an, ob der Benutzer das Gerät nicht in den abgesicherten Bootmodus neu starten darf.	
Netzwerk-Reset nicht zulassen	Gibt an, ob ein Benutzer die Netzwerkeinstellungen nicht über die Einstellungen zurücksetzen darf.	
Werksreset nicht zulassen	Gibt an, ob ein Benutzer das Gerät nicht zurücksetzen darf.	
ADB aktivieren	Ermöglicht die Verbindung mit einem PC über ADB	
Schlüsselschutz deaktivieren	Deaktiviert den Schlüsselschutz	
Informationen zum Sperrbildschirm des Gerätebesitzers	Legt die Informationen zum Besitzer des Geräts fest, die auf dem Sperrbildschirm angezeigt werden sollen.	
Durchsetzung der Compliance	Modus Eingabeaufforderung Benutzer	Der Benutzer wird aufgefordert, die erforderlichen Aktionen auszuführen.
	Modus Lock-Down Container	Alle Anwendungen ausblenden, bis alle Anforderungen erfüllt sind

App Verwaltung	
Profilübergreifende App-Verknüpfung zulassen	Ermöglicht es Anwendungen im übergeordneten Profil, Weblinks aus dem verwalteten Profil zu verarbeiten.
App-Steuerung verbieten	Legt fest, ob ein Benutzer keine Anwendungen in den Einstellungen oder Launchern ändern darf.
App-Installation verbieten	Gibt an, ob einem Benutzer die Installation von Anwendungen untersagt ist.
Deinstallieren von Apps verbieten	Gibt an, ob ein Benutzer keine Anwendungen deinstallieren darf.
Richtlinie für Laufzeitberechtigungen	Legt fest, wie neue Berechtigungsanfragen von Anwendungen behandelt werden.
Unbekannte Quellen zulassen	Wenn diese Funktion aktiviert ist, können Benutzer Apps durch die Installation einer .apk-Datei sideloaden.

Konnektivität	
Mobile Netzwerkkonfiguration nicht zulassen	Gibt an, ob es einem Benutzer nicht erlaubt ist, mobile Netzwerke zu konfigurieren.
Tethering verbieten Konfig.	Gibt an, ob es einem Benutzer nicht erlaubt ist, Tethering und mobile Hotspots zu konfigurieren.
VPN-Konfiguration verbieten	Gibt an, ob einem Benutzer die Konfiguration eines VPN untersagt ist.
Wifi-Konfiguration verbieten	Gibt an, ob ein Benutzer die WiFi-Zugangspunkte nicht wechseln darf.
Ausgehenden NFC-Strahl verbieten	Legt fest, ob der Benutzer NFC nicht zum Beamen von Daten aus Apps verwenden darf.
WiFi-Konfiguration sperren	Diese Einstellung steuert, ob von einer App des Gerätebesitzers erstellte WiFi-Konfigurationen gesperrt werden sollen (d.h. nur von der App des Gerätebesitzers bearbeitet oder entfernt werden können, nicht einmal von der App Einstellungen).
Daten-Roaming aktivieren	Aktiviert Daten-Roaming

Bluetooth	
Bluetooth deaktivieren	Gibt an, ob Bluetooth auf dem Gerät nicht erlaubt ist. Benötigt Android 8.0
Bluetooth-Freigabe deaktivieren	Gibt an, ob die ausgehende Bluetooth-Freigabe auf dem Gerät nicht erlaubt ist. Benötigt Android 8.0
Bluetooth-Konfiguration nicht zulassen	Gibt an, ob einem Benutzer die Konfiguration von Bluetooth untersagt ist.

Kontoführung	
Hinzufügen eines verwalteten Profils nicht zulassen	Gibt an, ob einem Benutzer das Hinzufügen von verwalteten Profilen untersagt ist. Benötigt Android 8.0
Hinzufügen von Benutzern verbieten	Gibt an, ob einem Benutzer das Hinzufügen neuer Benutzer untersagt ist.
Nicht zulassen Verwaltetes Profil entfernen	Gibt an, ob verwaltete Profile dieses Benutzers entfernt werden können, außer von seinem Profileigentümer. Benötigt Android 8.0
Kontomodifikation verbieten	Gibt an, ob einem Benutzer das Hinzufügen und Entfernen von Konten untersagt ist, es sei denn, sie werden von Authenticator programmatisch hinzugefügt.

Telefonie	
Ausgehende Anrufe verbieten	Legt fest, dass der Benutzer keine ausgehenden Telefonanrufe tätigen darf.
SMS verbieten	Legt fest, dass der Benutzer keine SMS-Nachrichten senden oder empfangen darf.

System	
Fenstererstellung verbieten	Legt fest, dass neben den Anwendungsfenstern keine weiteren Fenster erstellt werden sollen.
Eingestelltes Benutzersymbol nicht zulassen	Gibt an, ob ein Benutzer sein Symbol nicht ändern darf.
Hintergrundbild einstellen verbieten	Benutzerbeschränkung, um das Einstellen eines Hintergrundbildes zu verbieten.
Statusleiste deaktivieren	Die Deaktivierung der Statusleiste blockiert Benachrichtigungen, Schnelleinstellungen und andere Bildschirmüberlagerungen, die das Verlassen eines Einweggeräts ermöglichen.
Auto Zeit aktivieren	Stellt die Uhrzeit automatisch ein.
Automatische Zeitzone aktivieren	Stellt die Zeitzone automatisch ein.
Bleibt eingeschaltet, wenn der Stecker eingesteckt ist	Das Gerät bleibt aktiv, solange es an eine Stromquelle angeschlossen ist.

Lagerung	
Deaktivieren Sie die App-Verifizierung	Gibt an, ob ein Benutzer die Anwendungsüberprüfung nicht deaktivieren darf.
Einhängen physischer Medien verbieten	Gibt an, ob es einem Benutzer nicht erlaubt ist, physische externe Medien einzuhängen.
Sicherungsdienst aktivieren	Der Backup-Dienst verwaltet alle Sicherungs- und Wiederherstellungsmechanismen auf dem Gerät. Wenn Sie diesen Wert auf false setzen, werden die Daten nicht gesichert oder wiederhergestellt. Der Backup-Dienst ist standardmäßig deaktiviert. Benötigt Android 8.0
Aktivieren Sie den USB-Massenspeicher	Ermöglicht die Verwendung des USB-Massenspeichers.

Tastatur	
Autofill deaktivieren	Gibt an, ob ein Benutzer die Autofill Services nicht verwenden darf. Benötigt Android 8.0
Kopieren und Einfügen zwischen Profilen verbieten	Gibt an, ob das, was in die Zwischenablage dieses Profils kopiert wird, in verwandte Profile eingefügt werden kann.

Ton	
Volumenanpassung nicht zulassen	Gibt an, ob ein Benutzer die Master-Lautstärke nicht verändern darf.
Mikrofon stummschalten nicht zulassen	Legt fest, ob ein Benutzer die Mikrofonlautstärke nicht verändern darf.
Gerät stummschalten	Gerät stummschalten.

Zertifikat Management

Hier können Sie vertrauenswürdige Zertifikate und Identitätszertifikate an Ihre Geräte verteilen.

Android 8 oder höher ist erforderlich, um vertrauenswürdige Zertifikate zu verteilen und Android 9 oder höher ist erforderlich, um Identitätszertifikate zu verteilen.

Mit dem "+" können Sie mehrere Zertifikate hinzufügen.

Vertrauenswürdige Zertifikate müssen im PEM-Format vorliegen.

Identitätszertifikate müssen im PKCS12-Format vorliegen

Verbindungsmanagement

Wifi

Führen Sie für diese Einstellung die Vorkonfiguration der Endbenutzergeräte durch, für den Zugriff auf den internen Access
Punkte

Services Set Identifier (SSID)	SSID für das Netzwerk, mit dem eine Verbindung hergestellt werden soll
Verborgenes Netzwerk	Aktivieren, für den Fall, dass der AP die SSID nicht sendet

Sicherheit Typ

Legen Sie den Sicherheitstyp des APs fest

WEP

Passwort	Passwort für den AP

WPA/WPA2

Passwort	Passwort für den AP

802.1x EAP

EAP-Methode

PWD	Identität	Identität
	Passwort	Passwort

PEAP	Phase 2 Authentifizierungsprotokoll	keine	Kein zusätzliches Protokoll
		MSCHAPV2	MSCHAPV2-Protokoll
		GTC	GTC-Protokoll
	CA-Zertifikat	CA-Zertifikat	
	Identität	Identität	
	Anonyme Identität	Anonyme Identität	
	Passwort	Passwort	

TTLS	Phase 2 Authentifizierungsprotokoll	keine	Kein zusätzliches Protokoll
		PAP	PAP-Protokoll
		MSCHAP	MSCHAP-Protokoll
		MSCHAPV2	MSCHAPV2-Protokoll
		GTC	GTC-Protokoll
	CA-Zertifikat	CA-Zertifikat	
	Identität	Identität	
	Anonyme Identität	Anonyme Identität	
	Passwort	Passwort	

TLS	CA-Zertifikat	CA-Zertifikat
	Identität	Identität
	Passwort	Passwort

VPN

Name der Verbindung	Name der VPN-Verbindung

VPN-Typ

VPN

VPN-Client

AppTec360 VPN-Client	
Gateway-Konfiguration	Wählen Sie die Gateway-VPN-Konfiguration (siehe **Allgemeine Einstellungen > Universal Gateway > VPN-Einstellungen**)
Immer eingeschaltetes VPN	Native Abriegelung aktivieren
AppTec360 Lockdown aktivieren	AppTec360 Lockdown aktivieren

Eingebaut (nur auf Samsung-Geräten verfügbar)			
Verbindungstyp	PPTP	Server	Server
		PPTP-Verschlüsselung aktivieren	PPTP-Verschlüsselung aktivieren
	L2TP / IPSec PSK	Server	Server
		IPSec Pre-Shared Key	IPSec Pre-Shared Key
		L2TP-Geheimnis aktivieren	L2TP-Geheimnis aktivieren
		L2TP Geheimnis	L2TP Geheimnis
	IPSec XAuth PSK	Server	Server
		IPSec-Bezeichner	IPSec-Bezeichner
		IPSec Pre-Shared Key	IPSec Pre-Shared Key
DNS-Suchdomänen	DNS-Suchdomänen		
Experten-Einstellungen	DNS-Server	DNS-Server	
	Weiterleitungsrouten	Weiterleitungsrouten	

VPN öffnen		
Server	Server	
OpenVPN-Profil	OpenVPN-Profil	
OpenVPN-App	OpenVPN für Android (empfohlen)	
	OpenVPN-Verbindung	
Experten-Einstellungen	DNS-Server	DNS-Server
	Weiterleitungsrouten	Weiterleitungsrouten

Samsung / Starker Schwan			
Verbindungstyp	PPTP	Server	Server
		Benutzername	Benutzername
		Passwort	Passwort
		PPTP-Verschlüsselung aktivieren	PPTP-Verschlüsselung aktivieren
	L2TP / IPSec PSK	Server	Server
		IPSec Pre-Shared Key	IPSec Pre-Shared Key
		Benutzername	Benutzername
		Passwort	Passwort
		L2TP-Geheimnis aktivieren	L2TP Geheimnis
	IPSec XAuth PSK	Server	Server
		IPSec-Bezeichner	IPSec-Bezeichner
		IPSec Pre-Shared Key	IPSec Pre-Shared Key
		Benutzername	Benutzername
		Passwort	Passwort
Experten-Einstellungen	DNS-Server	DNS-Server	
	Weiterleitungsrouten	Weiterleitungsrouten	

Cisco Any Connect		
Server	Server	
Zertifikat-Modus	Behinderte	Behinderte
	Automatisch	Automatisch
Experten-Einstellungen	DNS-Server	DNS-Server
	Weiterleitungsrouten	Weiterleitungsrouten

Pro-App VPN

VPN-Client

AppTec360 VPN-Client		
Gateway-Konfiguration	Wählen Sie die Gateway-VPN-Konfiguration (siehe **Allgemeine Einstellungen > Universal Gateway > VPN-Einstellungen**)	
VPN-Apps	VPN-Apps	
Immer eingeschaltetes VPN	Native Abriegelung aktivieren	Immer eingeschaltetes VPN
AppTec360 Lockdown aktivieren	AppTec360 Lockdown aktivieren	

Samsung / Starker Schwan			
Verbindungstyp	PPTP	Server	Server
		VPN-Apps	VPN-Apps
		Benutzername	Benutzername
		Passwort	Passwort
		PPTP-Verschlüsselung aktivieren	PPTP-Verschlüsselung aktivieren
	L2TP / IPSec PSK	Server	Server
		VPN-Apps	VPN-Apps
		IPSec Pre-Shared Key	IPSec Pre-Shared Key
		Benutzername	Benutzername
		Passwort	Passwort
		L2TP-Geheimnis aktivieren	L2TP Geheimnis
	IPSec XAuth PSK	Server	Server
		VPN-Apps	VPN-Apps
		IPSec-Bezeichner	IPSec-Bezeichner
		IPSec Pre-Shared Key	IPSec Pre-Shared Key
		Benutzername	Benutzername
		Passwort	Passwort
Experten-Einstellungen	DNS-Server	DNS-Server	
	Weiterleitungsrouten	Weiterleitungsrouten	

Beschränkungen

Hier können Sie die Einschränkungen in Bezug auf die Verbindungsverwaltung festlegen.

Daten-Roaming zulassen	Mobile Daten beim Roaming zulassen
Daten-Roaming erzwingen	Falls aktiviert, ist das Roaming für mobile Daten dauerhaft aktiviert (nicht empfohlen!) Diese Einstellung überschreibt die Einstellung "Datenroaming zulassen"!
Die folgenden Einstellungen sind nur auf SAFE 2.x oder höher verfügbar	
Nur Notrufe zulassen	Nur Notrufe zulassen
WiFi zulassen	WiFi zulassen
WiFi Netzwerk Mindest-Sicherheitsstufe	Minimale Sicherheitsstufe des WiFi-Netzwerks Offen = alle Arten von WiFi sind erlaubt
Verbieten Sie dem Benutzer, WiFi-Netzwerke hinzuzufügen	Der Benutzer kann nicht selbst ein WiFi-Netzwerk hinzufügen Diese Einstellung ist nur möglich, wenn unter "Verbindungsverwaltung" ein WiFi-Profil definiert wurde.
SMS & MMS zulassen	Alle = Der gesamte SMS- und MMS-Verkehr ist erlaubt Nur eingehende SMS = Nur eingehende SMS-Nachrichten sind erlaubt Nur ausgehende SMS = Nur ausgehende SMS-Nachrichten sind erlaubt Keine = Kein SMS / MMS-Verkehr ist erlaubt
Synchronisierung beim Roaming zulassen	Synchronisierung beim Roaming zulassen Ein = aktiviert Aus = Deaktiviert Wahl des Benutzers = Wahl des Benutzers
Sprachroaming zulassen	Sprachroaming zulassen Ein = aktiviert Aus = Deaktiviert User Choice = die Wahl des Benutzers
System http Proxy Server verwenden	Die Verwendung eines HTTP-Proxyservers, der von den Systemeinstellungen in den Einstellungen bereitgestellt wird, ist abhängig vom verbundenen Netzwerk (WiFi oder APN)

PIM-Verwaltung

Google Mail Austausch

Info: Diese Konfiguration wird auf die Google Mail-App angewendet. Sie müssen also Gmail genehmigen und installieren.

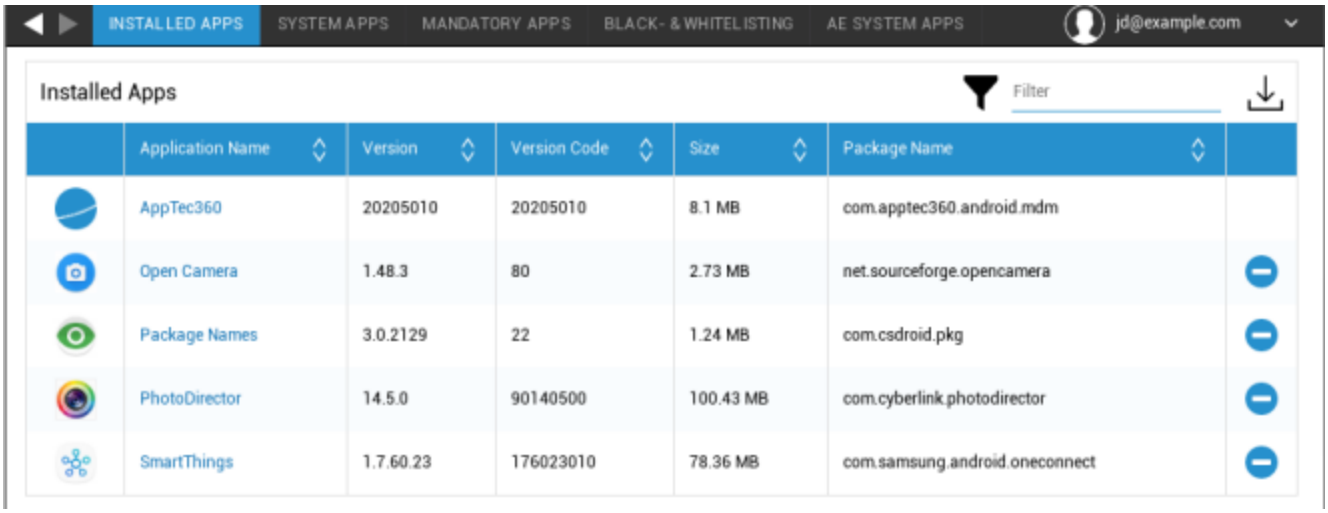
eMail-Adresse	Die angegebene E-Mail-Adresse des Benutzers Bitte beachten Sie die "Platzhalter", die Sie für die Arbeit mit Anmeldeinformationen verwenden können und die Sie nicht auf jedem Gerät manuell ändern müssen Mit einem Klick auf können Sie sie sich selbst anzeigen lassen
Server-Hostname	Serveradresse Ihres Exchange Servers
Login-Name	Der Login-Name für das jeweilige Endgerät, bitte beachten Sie auch die "Platzhalter hier
Unterschrift	Eine Signatur kann angehängt werden (Hinweis: Einige Geräte erfordern eine HTML-Formatierung für die Signatur)
Anzahl der zu synchronisierenden Vortage	Anzahl der Tage, die bestimmen, wann die E-Mails wieder synchronisiert werden
Geräte-Identifikator	Ein String der die EAS DeviceID enthält. Dies ist Teil des EAS Protokols und wird in einigen Umgebungen benötigt
Verwenden Sie Secure Sockets Layer (SSL)	Verwenden Sie eine SSL-Verbindung
Alle Zertifikate akzeptieren	Alle Zertifikate werden akzeptiert. Bitte wählen Sie diese Option, wenn Ihr Exchange Server ein selbstsigniertes Zertifikat verwendet

App Verwaltung

Enterprise App Manager

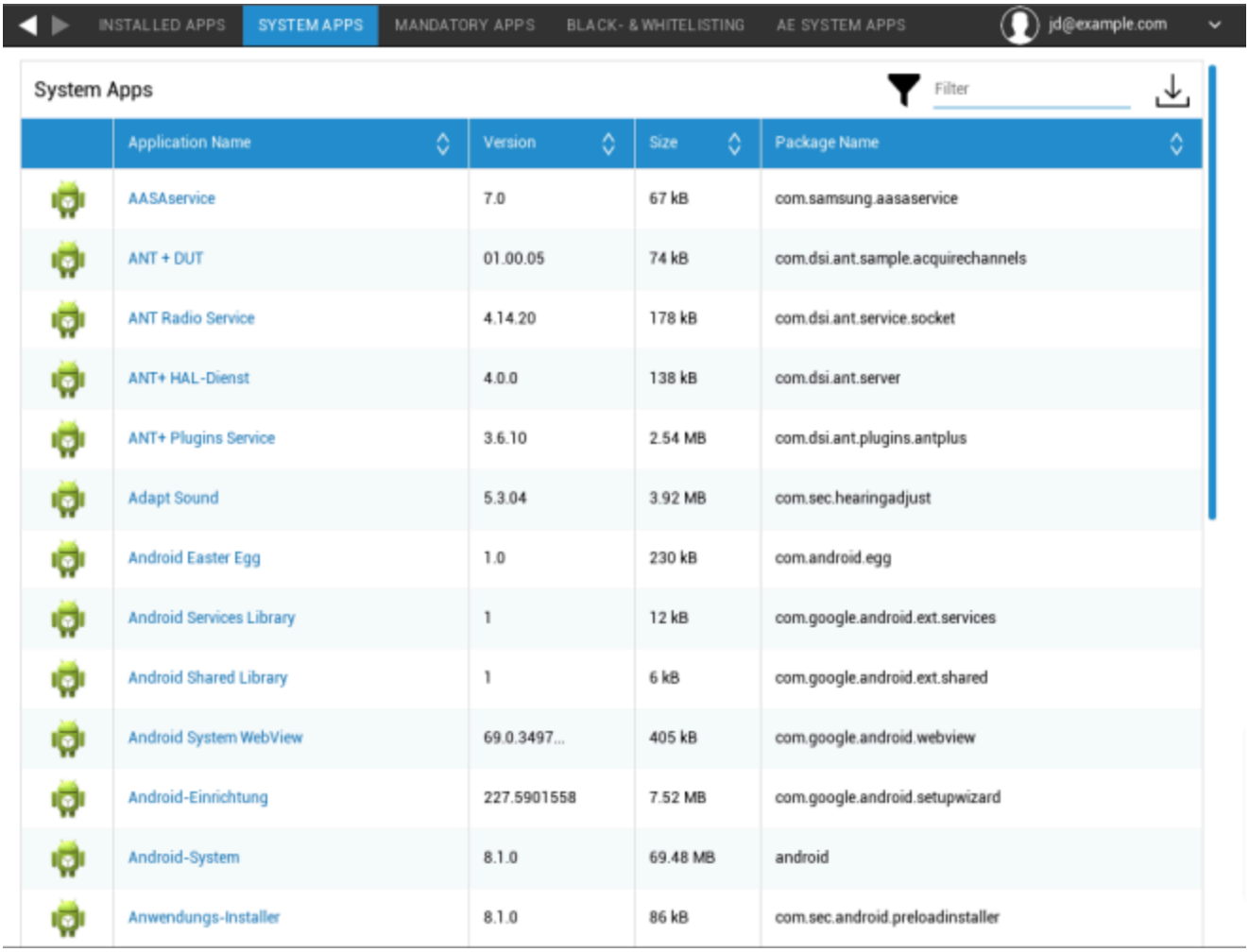
Installierte Apps (nur auf Geräteebene)

Hier werden Ihnen alle Apps angezeigt, die derzeit auf dem Endbenutzergerät installiert sind.



System-Apps (nur auf Geräteebene)

Unter "System-Apps" werden alle Apps und Dienste aufgelistet, die bereits von Ihrem Gerätehersteller auf dem Endgerät installiert wurden.

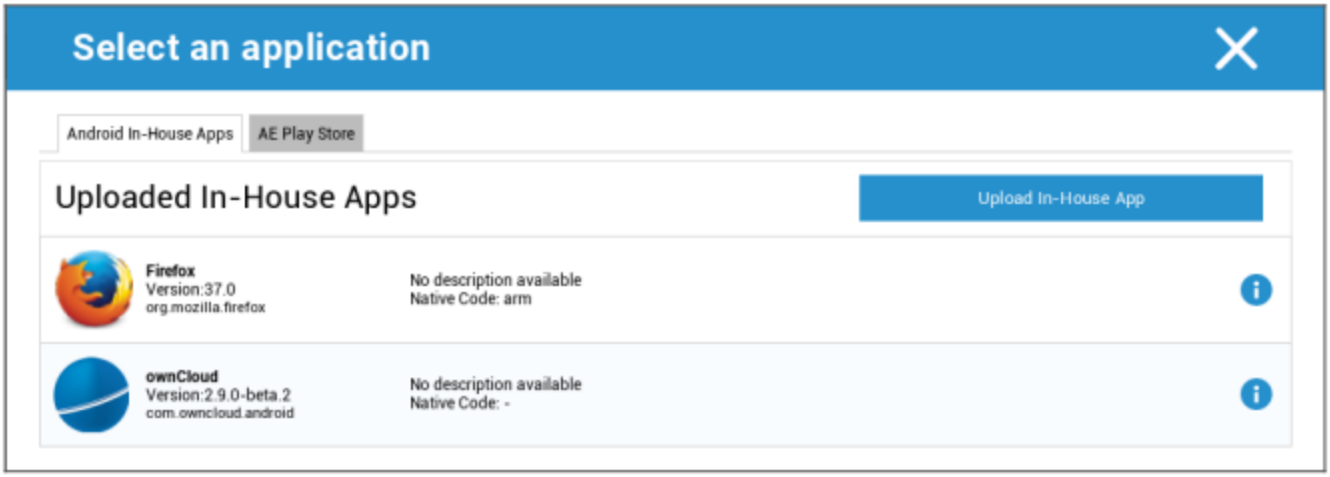


Obligatorische Apps

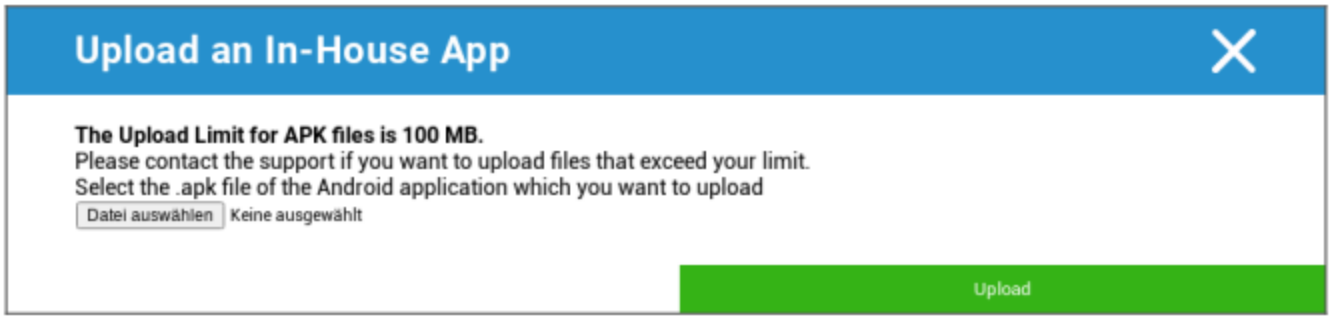
Unter den obligatorischen Apps können Sie die obligatorisch erforderlichen Apps festlegen. Der Benutzer wird ständig aufgefordert, diese bestimmte App zu installieren.

Über die können Sie die obligatorisch benötigte App definieren.

Dies kann eine In-House App aus den "Android In-House Apps" sein, die Sie in den Allgemeinen Einstellungen hochgeladen haben.

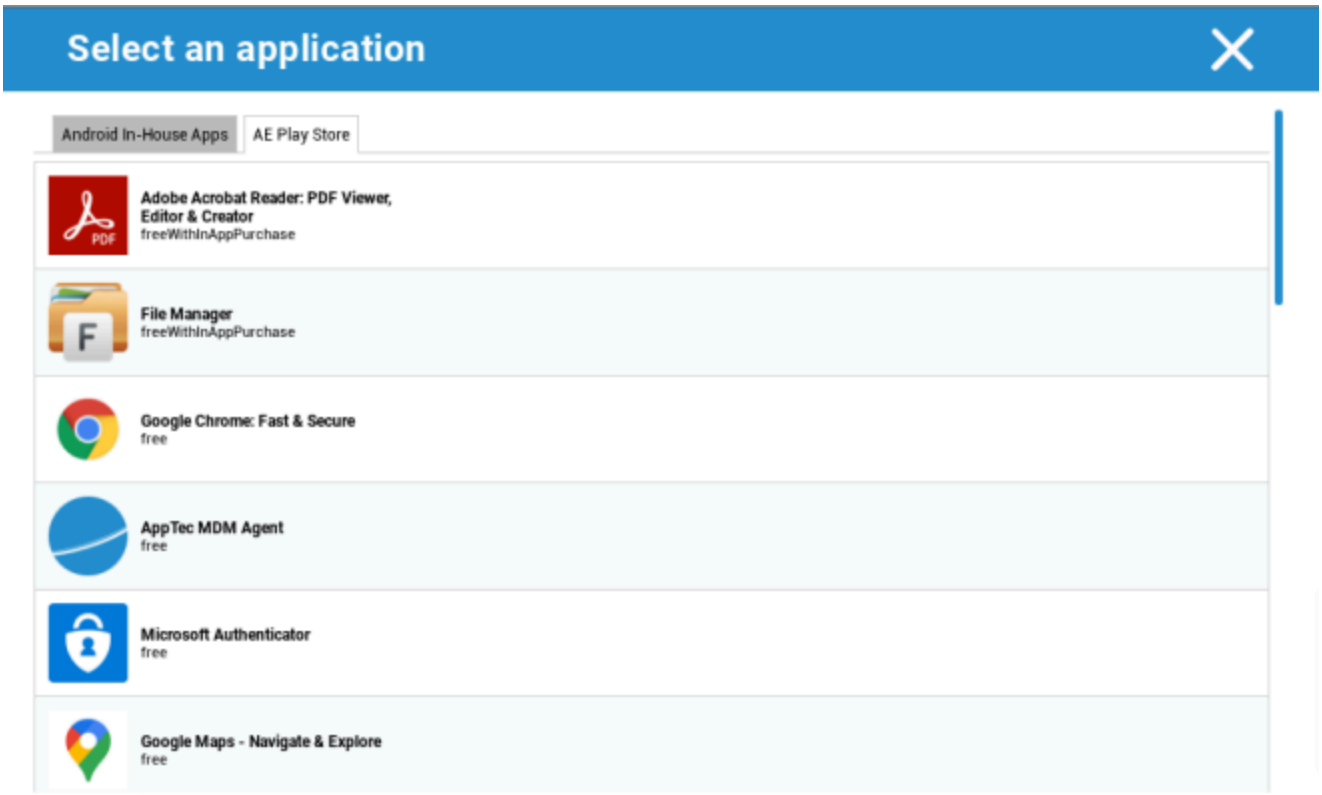


Sie können auch direkt eine apk-Datei mit "In-House App hochladen" auswählen und hochladen.



Wenn Sie eine In-House App installieren, haben Sie die Möglichkeit, "Auf dem Laufenden halten" zu aktivieren. Wenn dies aktiviert ist und Sie eine neuere Version in der In-House App DB definiert haben, wird die App auf dem Gerät aktualisiert.

Oder es kann eine "AE Play Store" App aus dem Google Work Play Store sein.



Nur genehmigte "AE Play Store Apps" werden in dieser Registerkarte angezeigt.

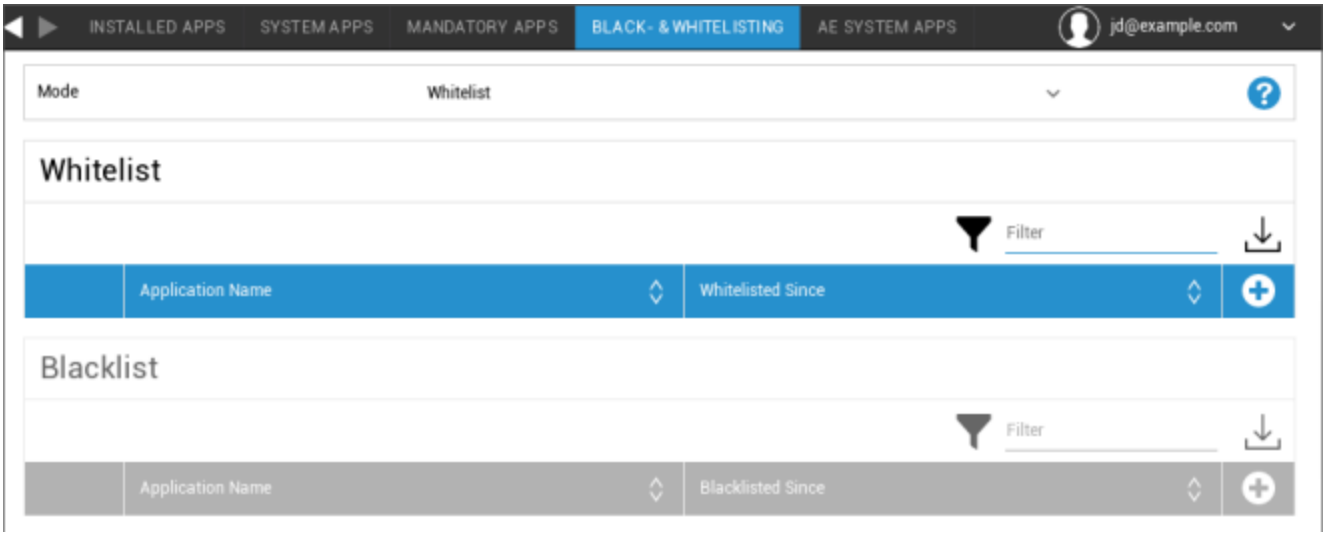
Um eine "AE Play Store App" zu genehmigen, gehen Sie bitte zu "Allgemeine Einstellungen" > "App Management" > "AE Play

Store" und fügen Sie eine App über die Schaltfläche hinzu, die Sie zur Registerkarte "Play Store Apps" weiterleitet (oder Sie
können Sie direkt zur Registerkarte "Play Store Apps" gehen).

Auf der Registerkarte "Play Store Apps" können Sie nach Apps suchen. Wenn Sie auf eine App klicken, öffnet sich die App-Seite
und hier können Sie die App genehmigen, indem Sie auf "Genehmigen" klicken.

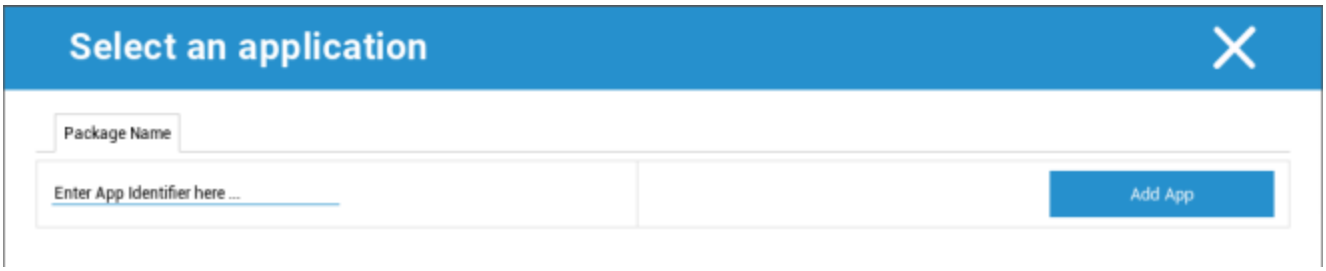
Black- & Whitelisting

Unter "Black- & Whitelisting" können Sie zwischen dem Modus "Whitelist" und dem Modus "Blacklist" wählen.



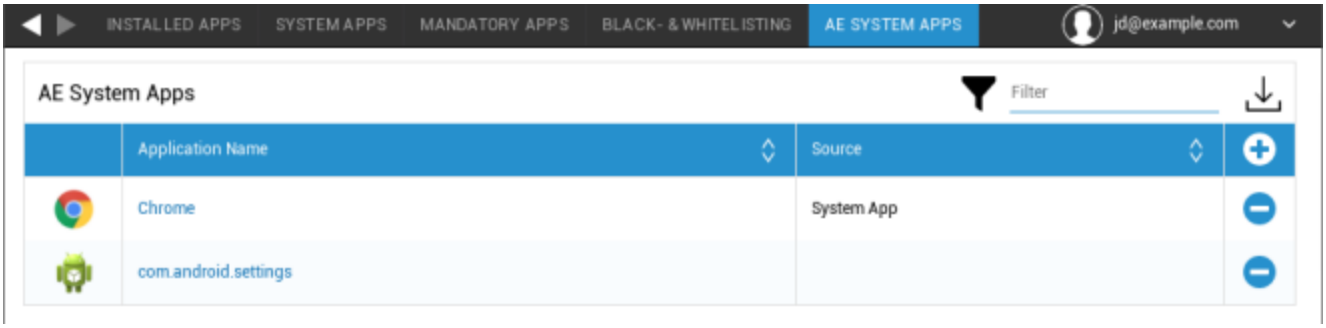
Whitelist	Nur Apps und Dienste, die der Liste hinzugefügt werden, können auf dem Endgerät des Benutzers installiert werden. Wenn diese bereits auf dem Endbenutzergerät vorinstalliert sind, werden sie aktiviert und so eingestellt, dass der Benutzer sie ausführen kann.
	Alle anderen Apps, die nicht zur Liste hinzugefügt werden, können nicht auf dem Endgerät des Benutzers installiert werden. Wenn diese bereits auf dem Endbenutzergerät vorinstalliert sind, werden sie deaktiviert und so eingestellt, dass der Benutzer sie nicht ausführen kann.
Schwarze Liste	Apps und Dienste, die der Liste hinzugefügt werden, können nicht auf dem Endgerät des Benutzers installiert werden. Wenn diese bereits auf dem Endbenutzergerät vorinstalliert sind, werden sie deaktiviert und so eingestellt, dass der Benutzer sie nicht ausführen kann.
	Alle anderen Apps, die nicht zur Liste hinzugefügt werden, können auf dem Endgerät des Benutzers installiert werden. Wenn diese bereits auf dem Endbenutzergerät vorinstalliert sind, werden sie aktiviert und so eingestellt, dass der Benutzer sie ausführen kann.

Über die Taste , fügen Sie der aktuell verwendeten Liste weitere Apps oder Dienste hinzu.
Über die Taste , fügen Sie der derzeit inaktiven Liste weitere Apps oder Dienste hinzu.
Sie können einen "Packagennamen" definieren:

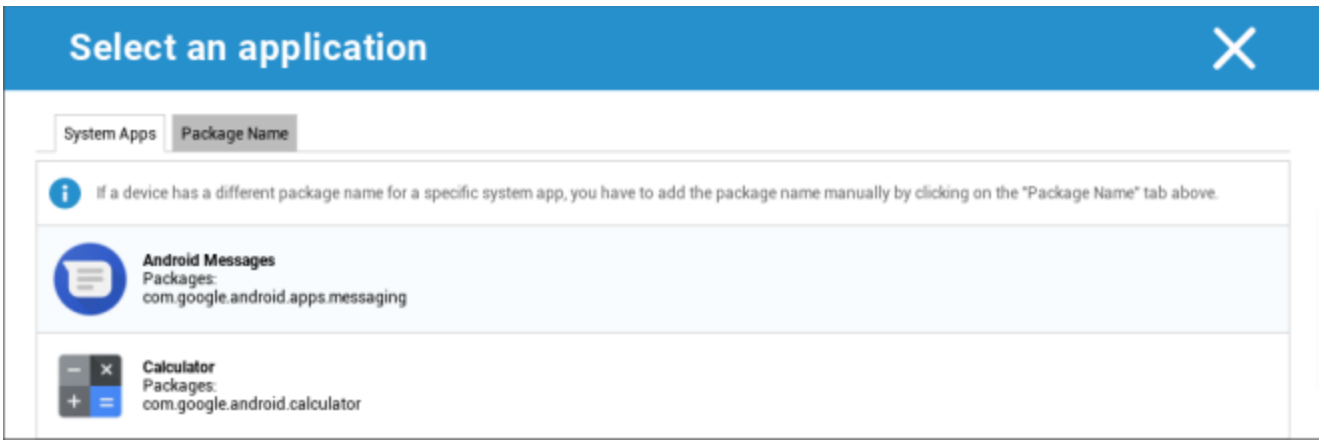

Select an application
Package Name
Enter App Identifier here ...
Add App

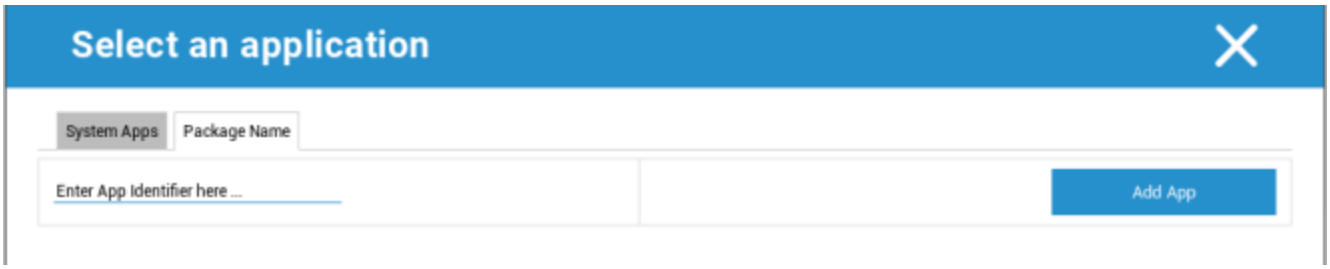
AE System Apps

Hier können Sie eine Liste definieren, die bestimmte System-Apps enthält, die auf den Geräten aktiviert werden sollen.



Wenn Sie auf die Schaltfläche klicken, können Sie aus einer von Google bereitgestellten Liste möglicher System-Apps wählen oder direkt den Paketnamen einer System-App eingeben, die aktiviert werden soll.





Bitte beachten Sie, dass die System-Apps in der von Google bereitgestellten Liste nur Apps sind, die System-Apps sein können, aber nicht unbedingt System-Apps auf Ihren Geräten sein müssen.

Diese Liste betrifft jedoch nur Apps, die bereits vorinstalliert sind.

Das Hinzufügen von Apps, die nicht auf Ihren Geräten vorinstalliert sind, wirkt sich nicht auf Ihre Geräte aus, unabhängig davon, ob die App aus der von Google bereitgestellten Liste stammt oder der

Paketname der App direkt eingegeben wird.

Beschränkungen & Einstellungen

App Management Einstellungen

Hier können Sie das Verhalten des Geräts in Bezug auf App-Updates konfigurieren.

Häufigkeit der Aktualisierungsprüfung	Legen Sie fest, in welchem Intervall der AppTec360 Client nach App-Updates suchen soll. Der Standardwert ist 24 Stunden.
Wi-Fi Schwellenwert	Apps, die größer als die angegebene Größe sind, werden über Wi-Fi heruntergeladen. Wenn "Nur Wi-Fi" ausgewählt ist, werden alle Apps über Wi-Fi heruntergeladen.

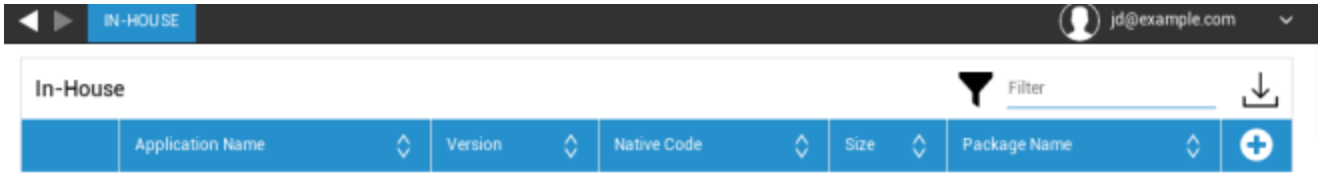
Enterprise App Store

Hausintern

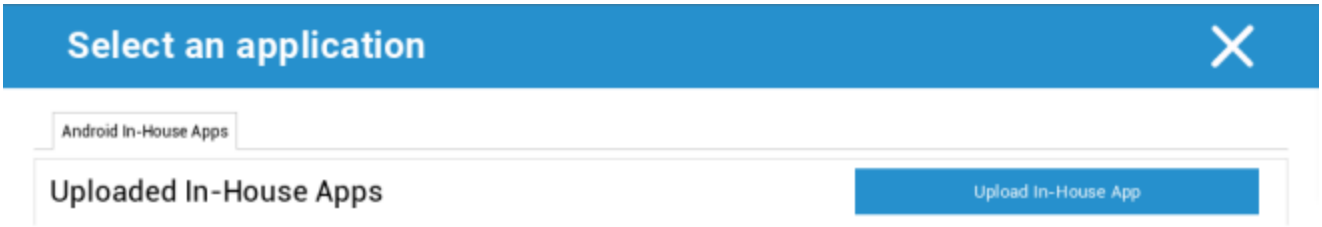
Unter dem Punkt "In-House" können Sie intern entwickelte Apps hochladen und verbreiten.

Mit dem Symbol können Sie zusätzliche In-House Apps vertreiben.

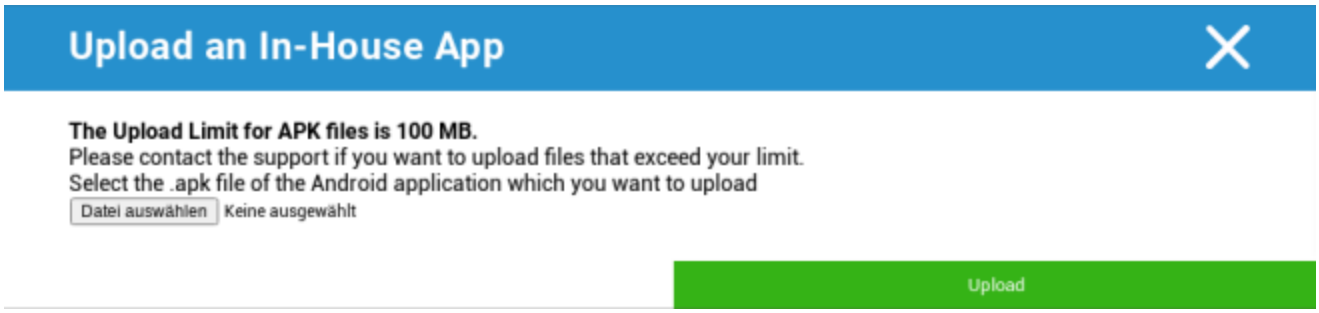
Wenn Sie eine In-House App installieren, haben Sie die Möglichkeit, "Auf dem Laufenden halten" zu aktivieren. Wenn
aktiviert ist und Sie eine neuere Version in der In-House App DB definiert haben, wird die App
auf dem Gerät aktualisiert.



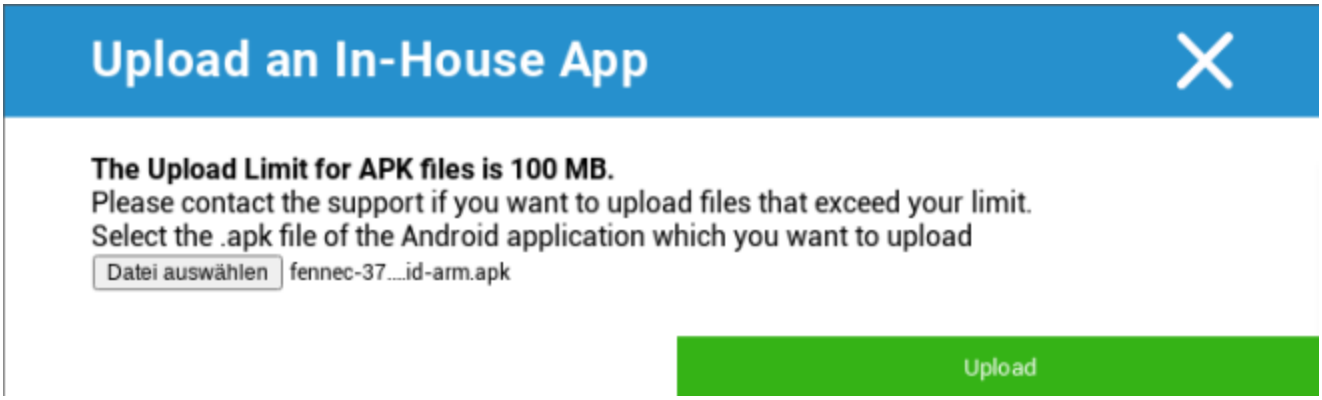
Sollten Sie keine In-House Apps verteilt haben, erhalten Sie dann die folgende Übersicht:



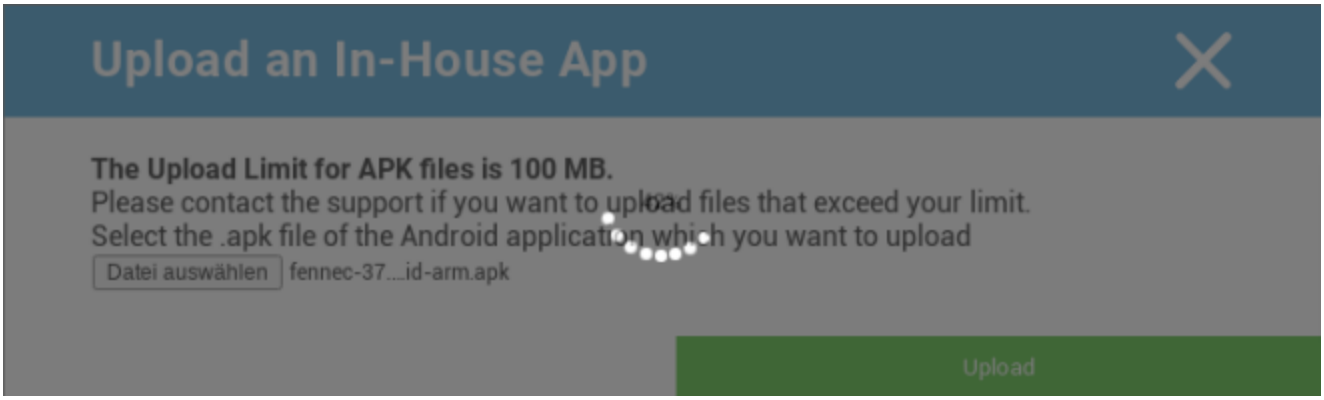
Klicken Sie dazu auf "In-House App hochladen", Sie erhalten dann die folgende Übersicht:



Wählen Sie nun mit "Suchen..." eine .apk-Datei aus und klicken Sie dann auf "Hochladen".



Ihre App wird nun hochgeladen. In der Mitte des Kreises sehen Sie eine Prozentanzeige, zeigt an, wie viel von Ihrer App bereits hochgeladen wurde.



Sollte der Upload Ihrer In-House App erfolgreich gewesen sein, finden Sie die hochgeladene App dann
in Ihrem App-Katalog.

Der Benutzer hat nun die Möglichkeit, diese App im AppTec360 Store auf dem Endbenutzer zu sehen und zu installieren
Gerät, unter der Kategorie "In-House".

Da es sich nicht um eine Google PlayStore App handelt, benötigt der Benutzer keine gespeicherte Google
ID auf ihrem jeweiligen Endbenutzergerät.

Enterprise Play Store

AE Play Store

Hier können Sie Apps zum Android Enterprise Playstore hinzufügen. Bitte beachten Sie, dass Sie Folgendes genehmigen müssen
Apps mit Ihrem AE Administrator-Konto, bevor Sie sie hinzufügen können.

Um eine App zu genehmigen, lesen Sie bitte die Anweisungen unter Obligatorische Apps.

Kiosk-Modus & Launcher

Kiosk-Modus

Der Kioskmodus ermöglicht es Ihnen, eine App oder eine URL vorzudefinieren. Dann wird es ausschließlich möglich sein
diese App und oder URL ausführen/besuchen.

Ebenso können verschiedene Hardware-Tasten im Kioskmodus deaktiviert werden.

Automatischer Start	Startet automatisch den Kioskmodus, sobald das Profil das Endgerät des Benutzers erreicht
Geplanter Kiosk-Modus?	Sie können eine Zeit für den Kioskmodus planen. Dieser startet und endet dann automatisch zu einer von Ihnen festgelegten Zeit.
Startzeit	Startzeit
Zeit in Minuten	Zeit in Minuten, nach der der Kioskmodus wieder beendet werden soll

Anwendungstyp

Einzelne App	Wenn Sie die App im Kioskmodus starten möchten, wählen Sie unter "Anwendungstyp" die Option "Paket".
Kiosk-Anwendung	Klicken Sie hier, um eine Anwendung auszuwählen, die im Kioskmodus gestartet werden soll Hier finden Sie die übliche Übersicht der App-Verwaltung Sie können zwischen einem "Google Play Store", "Android In-House Apps" und einem "Packagename" wählen.

Anwendungstyp

URL		Wenn Sie eine URL im Kioskmodus starten möchten, wählen Sie unter "Anwendungstyp" die Option "URL". Definieren Sie dann die gewünschte URL-Adresse
	Browser nach Inaktivität löschen	Hier können Sie ein Zeitintervall in Minuten festlegen, nach dem der Kioskmodus neu gestartet werden soll
	Web-Cache und Cookies löschen	Wenn Sie diese Funktion aktivieren, wird nach einem Neustart des Kioskmodus der Web-Cache (Cookies und zwischengespeicherte Bilder) gelöscht.
	Politik der gleichen Herkunft	Wenn diese Funktion aktiv ist, kann der Benutzer nur auf den Unterseiten einer bestimmten URL surfen Sie haben zum Beispiel die folgende URL definiert:www.mypage.com Dann kann der Benutzer weitersurfen: www.mypage.com/subpage
	URLs auf der Whitelist	Hier können Sie eine Whitelist pflegen, alle diese URLs sind erlaubt Maximal 1 URL pro Zeile Eine URL muss mit http:/ oder https:// beginnen.
	Auf der schwarzen Liste stehende URLs	Hier können Sie eine Blacklist pflegen, in der alle diese URLs nicht erlaubt sind Maximal 1 URL pro Zeile Eine URL muss mit http:/ oder https:// beginnen.
	Bildschirmausrichtung	Diese Einstellung bezieht sich auf die Bildschirmeinstellungen Automatisch = automatisch Hochformat = vertikales Format Landscape = Querformat

Multi-App		Wenn Sie den Kioskmodus "Multi App" auswählen, wird die Verwendung des AppTec360 Launcher erzwungen.
	Apps	Anwendung: Wählen Sie eine Playstore- oder eine hauseigene App als Kioskanwendung. Es ist auch möglich, einen Packungsnamen einzugeben. Die ausgewählte Kioskanwendung muss auf dem Gerät installiert sein. Denken Sie daran, die Kiosk-Anwendung als obligatorisch einzustellen. Verknüpfung auf dem Homescreen: Wenn Sie diese Option auf "Ein" setzen, wird eine Verknüpfung auf dem Homescreen erstellt. Wenn Sie die Option "Aus" wählen, wird die App trotzdem in der App-Liste angezeigt.

Exit-Passwort Aktiviert	Wenn Sie diese Funktion aktivieren, ist es dem Benutzer möglich, den Kioskmodus mit einem von Ihnen festgelegten Passwort zu beenden.
Exit-Passwort	Dies ist das Passwort, das Sie selbst festgelegt haben
Statusleiste automatisch einklappen	Wenn diese Option aktiviert ist, wird die Statusleiste automatisch kollabiert. Mit dieser Option können Benutzer die Informationen in der Statusleiste sehen, aber nicht auf ihre Funktionen zugreifen
Statusleiste deaktivieren	Die Statusleiste enthält Benachrichtigungen, Shortcuts und Informationen. Nur verfügbar für Samsung-Geräte mit SAFE 4.0 oder höher.
Lautstärketasten deaktivieren	Lautstärketasten deaktivieren (nur verfügbar auf Samsung-Geräten mit SAFE 3.0 oder höher)
Ein/Aus-Schalter deaktivieren	Ein/Aus-Schalter deaktivieren (nur bei Samsung-Geräten mit SAFE 3.0 oder höher verfügbar)
Home-Taste deaktivieren	Deaktivieren Sie die Home-Taste. Wenn diese Funktion aktiviert ist, kann der Kioskmodus nur in der AppTec360 Konsole beendet werden. (nur verfügbar auf Samsung-Geräten mit SAFE 3.0 oder höher)
Navigationsleiste deaktivieren	Damit können Sie die Navigationsleiste (Zurück / Menü) deaktivieren. Wenn diese Funktion aktiviert ist, kann der Kioskmodus nur in der AppTec360 Konsole beendet werden. (nur verfügbar auf Samsung-Geräten mit SAFE 3.0 oder höher)

AppTec360-Startprogramm

Aktivieren Sie AppTec360 Launcher	Ein: Aktiviert den AppTec360 Launcher. Der Benutzer muss ihn einmalig als Standard-Startprogramm festlegen. Hinweis: Wenn der Kioskmodus aktiviert ist und der Kioskmodus auf "Multi App" eingestellt ist, wird die Verwendung des AppTec360 Launcher erzwungen.
Große Icons	Ein: Zeigt eine größere Version der App-Symbole im Launcher an
AppTec360 App-Symbol ausblenden	Ein: Blendet die AppTec360 App vollständig aus
AppTec360 Store-Symbol ausblenden	Ein: Blendet den AppTec360 Enterprise AppStore vollständig aus.

AppTec360 Einstellungen

AppTec360 Einstellungen App aktivieren	Die AppTec360 Settings App ermöglicht die Kontrolle über WiFi- und Bluetooth-Verbindungen
Einstellungen in Multi-App aktivieren Kiosk-Modus	Wenn aktiviert, können Benutzer auf die AppTec360 Settings App zugreifen, während der Multi App Kiosk Modus aktiv ist.

Fernsteuerung

Splashtop

Um eine Fernsteuerungssitzung für Ihr Gerät zu starten, muss die App "Splashtop Streamer" auf dem Gerät installiert werden, indem Sie die App zu **App Management** → **Enterprise App Manager** → **Obligatorische Apps** hinzufügen.

Konfigurieren Sie anschließend die folgenden Einstellungen für Splashtop:

Splashtop aktivieren	Wenn diese Option aktiviert ist, konfiguriert AppTec360 die Splashtop-App so, dass eine Fernsteuerung möglich ist.
Code bereitstellen	Gehen Sie zu https://my.splashtop.com und melden Sie sich bei Ihrem Splashtop-Konto an. Klicken Sie auf "Computer hinzufügen" und kopieren Sie den 12-stelligen Bereitstellungscode von der angezeigten Seite.
Benutzerdefiniertes Bereitstellungs-Gateway einstellen?	Gateway bereitstellen
Gateway-Domäne/Host bereitstellen	Gateway bereitstellen
Zertifikat-Überprüfung	Zertifikat-Überprüfung

Dann können Sie über die Option Splashtop Remote Control im Kontextmenü (Zahnrad neben der Suchleiste, wenn das Gerät ausgewählt ist oder Rechtsklick auf das Gerät in der Baumstruktur) die Fernsteuerungssitzung starten.

TeamViewer

Um eine Fernsteuerungssitzung für Ihr Gerät zu starten, muss die App "TeamViewer QuickSupport" auf dem Gerät installiert werden, indem Sie die App zu **App Management** → **Enterprise App Manager** → **Obligatorische Apps** hinzufügen.

Dann können Sie die Option **TeamViewer Remote Control** im Kontextmenü (Zahnrad neben der Suchleiste, wenn das Gerät ausgewählt ist oder Rechtsklick auf das Gerät in der Baumstruktur) verwenden, um die Fernsteuerungssitzung zu starten.

Content Management

ContentBox

Hier können Sie die ContentBox aktivieren.

Sobald Sie "Enable ContentBox" auf "On" stellen, wird eine separate ContentBox App installiert automatisch auf dem Endbenutzergerät.

Sicherer Browser

Hier können Sie Einstellungen für den AppTec360 Secure Browser vornehmen.

Sobald Sie den Abschnitt unter "Sicherer Browser" auf "Ein" stellen, wird eine separate Browser-App automatisch auf dem Endbenutzergerät installiert.

Passwort anfordern	Verlangen Sie vom Benutzer die Einrichtung und Verwendung eines Passworts für den Zugriff auf den Browser.
Minimal erforderliche Passwortlänge	Legen Sie die erforderliche Anzahl von Zeichen für das Passwort fest
Erforderliche Passwortqualität	Legen Sie die erforderliche Passwortqualität fest
Downloads einschränken / Öffnen in	
Uploads einschränken	
Whitelist hochladen	Eine Liste von URLs, für die das Hochladen immer erlaubt ist.
Kopieren zulassen	Erlauben Sie das Kopieren, Ausschneiden oder Teilen von Text innerhalb der Webseiten.
Bildschirmaufzeichnung zulassen	Erlauben Sie die Aufnahme von Bildschirmfotos.
Häufigkeit der Datenbereinigung	Wählen Sie, wie oft ALLE Benutzerdaten (Verlauf, Cache usw.) automatisch gelöscht werden sollen.
Lesezeichen für Unternehmen	Die Lesezeichen werden im Ordner "Firmenlesezeichen" in den Lesezeichen des Browsers angezeigt. Sie können vom Benutzer nicht bearbeitet werden.
Adressleiste ausblenden	
In-Browser Whitelisting (ohne Universal Gateway)	Aktiviert das URL-Whitelisting auf der Client-Seite. • Firmen-Lesezeichen sind immer auf der Whitelist • Wird nur für 100 URLs unterstützt • Bitte verwenden Sie den Universal Gateway für unbegrenztes Black- und Whitelisting
URLs auf der Whitelist	Eine Liste der erlaubten URLs.

Gateway-basiertes Black- und Whitelisting	Für die Aufnahme in die Schwarze Liste gelten die folgenden Voraussetzungen: • Ein funktionierendes AppTec360 Universal Gateway ("Allgemeine Einstellungen" → "Universal Gateway") • Eine funktionierende VPN-Konfiguration mit einem angegebenen DNS-Server ("Allgemeine Einstellungen" → "Universal Gateway" → "VPN-Einstellungen") • Eine Blacklist-Konfiguration ("Allgemeine Einstellungen" → "Universal Gateway" → "Domain Blacklist") • Eine gültige VPN-Verbindung im Profil ("Verbindungsverwaltung" → "VPN")

Zusätzliche API

Samsung KNOX

Beschränkungen

SD-Karte zulassen	
Schreiben auf SD-Karte zulassen	
Bildschirmaufzeichnung zulassen	
Zwischenablage zulassen	
Einstellungen und Anwendungsdaten in Google Cloud sichern	
Einstellungen aus der Google Cloud wiederherstellen, wenn Sie eine App neu installieren	
USB-Debugging zulassen	
Google Crash Report zulassen	
Werksreset zulassen	
OTA-Upgrade zulassen	
USB-Host-Speicher zulassen	Wenn diese Funktion aktiviert ist, kann der Benutzer einen beliebigen USB-Speicher, eine externe Festplatte oder einen Secure Digital (SD)-Kartenleser anschließen, der dann als Speicherlaufwerk auf dem Gerät eingebunden wird.
USB Media Player zulassen (MTP,PTP)	
Mikrofon zulassen	Deaktiviert das Mikrofon für Anwendungen von Drittanbietern
NFC (Nahfeldkommunikation) zulassen	
Unbekannte Quellen zulassen (APK Sideloading)	Wenn diese Option aktiviert ist, ist das Nebenbei-Laden von Apps (APK-Dateien) erlaubt. Sobald diese Einstellung deaktiviert ist, muss der Benutzer sie manuell aktivieren, wenn Sie die Installation von APKs aus unbekannten Quellen wieder zulassen.
Benutzererstellung zulassen	Wenn diese Option aktiviert ist, können Benutzer mehrere Konten auf dem Gerät erstellen, z.B. Gastkonten.

E-Mail

eMail-Adresse	
Protokoll des eingehenden Servers	
Adresse des eingehenden Servers	
Port des eingehenden Servers	
Login/Benutzername des Eingangsservers	
Passwort für den Posteingangsserver	
Eingehender Server verwendet SSL	
Eingehender Server verwendet TLS	
Eingehender Server akzeptiert alle Zertifikate	
Protokoll des ausgehenden Servers	
Adresse des ausgehenden Servers	
Port des ausgehenden Servers	
Ausgehender Server verwendet zusätzliche Anmeldeinformationen	Wenn diese Option deaktiviert ist, verwendet das System die eingehenden Anmeldeinformationen auch für den ausgehenden Server.
Anmeldung/Benutzername des Ausgangsservers	
Passwort für den Ausgangsserver	
Ausgehender Server verwendet SSL	
Ausgehender Server verwendet TLS	
Ausgehender Server akzeptiert alle Zertifikate	
Unterschrift setzen	
Unterschrift	Hinweis: Bei einigen Geräten muss die Signatur im HTML-Format angegeben werden.
Benutzer bei Erhalt einer neuen eMail benachrichtigen	

Tauschen Sie

eMail-Adresse	
Server-Hostname	Der Hostname des Exchange Servers
Login-Name	Der Benutzername, der für die Anmeldung beim Exchange Server verwendet wird
Domain	Wenn eine ACL-Gateway-Konfiguration aktiviert ist und das Feld Domain nicht leer ist, authentifiziert das AppTec360 Universal Gateway das Gerät mit folgendem Namen "Domain\Login Name
Passwort	
Anzahl der zu synchronisierenden Vortage	
Häufigkeit der eMail-Synchronisation	
Synchronisieren beim Roaming	
Unterschrift setzen	
Unterschrift	Hinweis: Bei einigen Geräten muss die Signatur im HTML-Format angegeben werden.
Standard-Konto	
Verwenden Sie Secure Sockets Layer (SSL)	
Verwenden Sie Transport Layer Security (TLS)	
Alle Zertifikate akzeptieren	

APN

APN-Anzeigename	
Name des Zugangspunkts	Name des APN
Protokoll des ausgehenden Servers	
MCC - Mobiler Ländercode	Leer lassen, um mmc der installierten SIM zu verwenden
MNC - Mobile Network Code	Leer lassen, um mnc der installierten SIM zu verwenden
Server Adresse	
Server-Portnummer	
Server-Proxy-Adresse	
MMS-Server-Adresse	Leer lassen für Standard
MMS-Anschlussnummer	Leer lassen für Standard
MMS-Proxy-Adresse	Leer lassen für Standard
Benutzername	
Passwort	
Zugangspunkt-Typ	Akzeptierte Typen sind "default", "mms", "supl".
	Wenn null oder leer übergeben wird, wird standardmäßig "default,supl,mms" verwendet.
	Leer lassen für Standard.
Bevorzugter APN	

Bluetooth

Geräteerkennung über Bluetooth zulassen	
Bluetooth-Kopplung zulassen	
Bluetooth-Headset-Geräte zulassen	
Bluetooth-Freisprecheinrichtungen zulassen	
Bluetooth A2DP-Geräte zulassen	A2DP, Advanced Audio Distribution Profile ermöglicht Audio-Streaming zwischen Geräten
Ausgehende Anrufe zulassen	
Datenübertragung über Bluetooth zulassen	
Bluetooth-Tethering zulassen	
Verbindung zum Computer über Bluetooth zulassen	

Verbindung

Nur Notrufe zulassenWi-Fi zulassen	
Wi-Fi Netzwerk Mindest-Sicherheitsstufe	
Verbieten Sie dem Benutzer, Wi-Fi-Netzwerke hinzuzufügen	Diese Einschränkung kann nur aktiviert werden, wenn unter Verbindungsverwaltung mindestens ein aktives Wi-Fi-Profil definiert ist.
SMS & MMS zulassen	
Synchronisierung beim Roaming zulassen	
Sprachroaming zulassen	

Android Enterprise – Vollständig verwaltetes Gerät mit Arbeitsprofil (COPE)

Allgemeine Erläuterung zu COPE

COPE ist eine Abkürzung für **Corporate Owned Personally Enabled**.

Der COPE-Modus ermöglicht es, ein Android-Gerät als **Android Enterprise - Fully Managed Device** mit integriertem **Android Enterprise - Container** Profil zu registrieren.

Dabei kann es sich entweder um ein Android-Gerät handeln, das bereits als **Android Enterprise - Fully Managed Device** registriert ist und auf dem zusätzlich der **Android Enterprise - Container** eingerichtet ist, oder um ein neu registriertes Android-Gerät, das direkt als **Android Enterprise - Fully Managed Device** zusammen mit dem darauf befindlichen **Android Enterprise - Container** registriert wird.

Der COPE-Modus ist nur für Geräte mit Android 8, 9 und 10 verfügbar

Konfiguration von Profilen für COPE-Geräte

Da es für den COPE-Modus selbst kein Konfigurationsprofil gibt, wird die Konfiguration von **Android Enterprise - Fully Managed Device** und **Android Enterprise - Container** in zwei Profile innerhalb des COPE-Profils aufgeteilt. Sie können bei der Konfiguration eines jeden Profils zwischen den beiden Profilen wechseln, indem Sie auf die entsprechende Schaltfläche auf der linken Seite der Konsole klicken:

Beide Profile können wie für jedes einzelne Profil beschrieben konfiguriert werden:

Android Enterprise - Vollständig verwaltetes Gerät

Android Enterprise - Container

Zurückkehren zu AE Vollständig verwaltetes Gerät

Das **Android Enterprise - Container-Profil** kann wie in **Mobile Management** beschrieben entfernt werden.

Wenn Sie das Container-Profil entfernen, wird das COPE-Profil in ein **Android Enterprise - Fully Managed Device-Profil** umgewandelt.

Android Enterprise – Container-Konfiguration

Je nachdem, ob Sie gerade ein Gruppenprofil oder ein Gerät ausgewählt haben, unterscheiden sich die Übersicht und ihre Unterpunkte - bitte beachten Sie dies sorgfältig!

Allgemein

Profilübersicht (nur auf Profilebene)

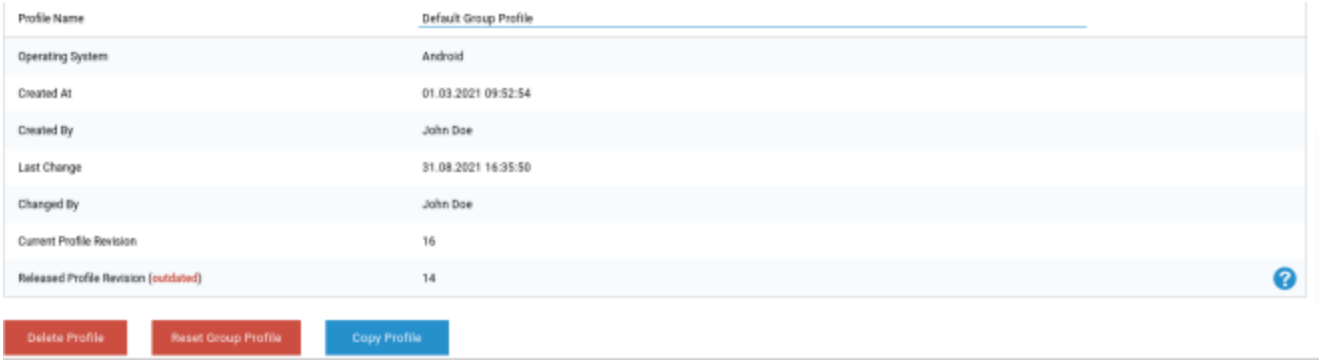
Wenn Sie sich in einem Profil befinden, erhalten Sie einen kurzen Überblick über das Profil, z.B. über Name, Betriebssystem, Erstellungsdatum, Autor usw.

Profil Name	Profilname - kann hier direkt umbenannt werden
Betriebssystem	Gültiges Betriebssystem für das Profil
Erstellt am	Erstellungsdatum
Erstellt von	Erstellt von
Letzte Änderung	Datum der letzten Änderung
Geändert von	Der Benutzer, der die letzten Änderungen an diesem Profil vorgenommen hat
Aktuelle Profilüberarbeitung	Anzahl der Aktualisierungen, die das Profil bereits erfahren hat
Freigegebene Profil-Revision	Anzahl der Aktualisierungen des Profils, denen bereits Geräte zugewiesen wurden

Profil löschen	Profil löschen
Gruppenprofil zurücksetzen	Gruppenprofil zurücksetzen
Profil kopieren	Profil kopieren

Gruppenprofilübersicht (nur auf Gruppenebene)

Wenn Sie ein Gruppenprofil öffnen, erhalten Sie einen schnellen Überblick über das Profil.



Profil Name	Name des Profils (kann hier geändert werden)
Betriebssystem	Betriebssystem, für das das Profil bestimmt ist
Erstellt am	Zeitpunkt der Erstellung
Erstellt von	Der Ersteller des Profils
Letzte Änderung	Zeitpunkt der letzten Änderung des Profils
Geändert von	Konto, das die letzten Änderungen vorgenommen hat
Aktuelle Profilüberarbeitung	Revision des gespeicherten Profilstatus
Freigegebene Profil-Revision	Zugewiesene Profilrevision ("Jetzt zuweisen"). Wenn das Etikett hinter dem Text "(veraltet)" anzeigt, bedeutet dies, dass Sie das Profil zwar gespeichert, aber noch nicht zugewiesen haben, so dass die Geräte noch eine ältere Version erhalten.

Geräteübersicht (nur auf Geräteebene)

Sollten Sie sich auf einem Gerät befinden, erhalten Sie eine Übersicht über das gewählte Gerät, die folgendes enthält:

Gerät Name	Name des Geräts
Standort	Standort-Koordinaten
Telefon Nummer	Rufnummer
Zugewiesene obligatorische Apps	Anzahl der zugewiesenen obligatorischen Apps
OS Version	OS-Version des Geräts
Betriebssystem	Betriebssystem (Android Enterprise)
Seriennummer	Seriennummer des Geräts
Geräteeigentum	Firmen- oder Privatgerät
Gerätetyp	AE Work Managed Device
Verwurzelt	Status, der anzeigt, ob das Gerät gerootet wurde
Konform	Konform mit der Richtlinie
IP-Adresse	IP-Adresse des Geräts
Zuletzt gesehen	Zeitpunkt, zu dem sich das Gerät zuletzt mit AppTec verbunden hat
Letzter Schub	Zeitpunkt, zu dem der letzte Push an das Gerät gesendet wurde
Benutzerzuordnung	Der Benutzer oder die Gruppe, der dieses Gerät zugewiesen ist

Konfig-Revision

Hier erhalten Sie einen Überblick darüber, welches Gruppenprofil dem Gerät zugewiesen ist.

Wenn Sie auf das Gruppenprofil klicken, erhalten Sie direkten Zugriff auf dieses Profil und können Einstellungen vornehmen.

Mit diesem Symbol können Sie die verteilten Apps auf die Einstellungen des Gruppenprofils zurücksetzen.

Mit diesem Symbol können Sie alle verwendeten Apps auf die Einstellungen des Gruppenprofils zurücksetzen.

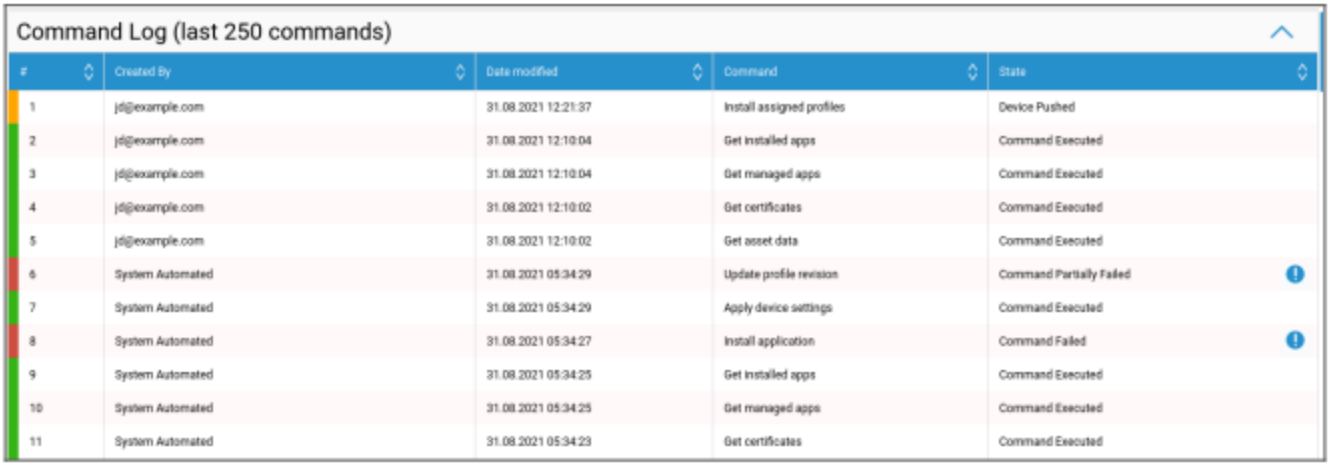
"Neuere Revision verfügbar" bedeutet, dass das Gruppenprofil geändert und gespeichert, aber nicht zugewiesen wurde. Das Gruppenprofil muss mit "Jetzt zuweisen" auf Gruppenebene zugewiesen werden, um die Änderungen auf die Geräte anzuwenden.

Geräteprotokoll (nur auf Geräteebene)

Hier erhalten Sie verschiedene Geräteprotokolle. Bei Bedarf können Sie hier direkt die Ursache eines Fehlers herausfinden.

Befehl Log

Hier können Sie sehen, welche Befehle für das Gerät erteilt wurden und welchen Status sie haben.



Mögliche Befehlszustände

Gerät geschoben	Eine Push-Anfrage wurde an den Push-Dienst (z.B. APNS) gesendet, um das Gerät anzuweisen, sich wieder mit dem EMM-Server zu verbinden.
Befehl erstellt	Der Befehl wurde im System erstellt.
Befehl gesendet	Der Befehl wurde an das Gerät gesendet, nachdem es sich mit dem Server verbunden hat.
Befehl Ausgeführt	Der Befehl wurde erfolgreich ausgeführt.
Befehl fehlgeschlagen	Der Befehl ist fehlgeschlagen. *
Befehl Teilweise fehlgeschlagen	Je nach Betriebssystem des Geräts können einige Befehle in Gruppen zusammengefasst werden. Dabei sind einige Teile dieser Befehlsgruppe fehlgeschlagen. *
Befehl ausgeführt, eventuell fehlgeschlagen	Der Befehl wurde ausgeführt, aber vielleicht auch nicht.
Kommando zurückgeschoben	Der Befehl wurde von einem Benutzer erneut gesendet.
Weggeworfen	Der Befehl wurde verworfen. Zum Beispiel, weil er durch einen anderen Befehl ersetzt wurde oder das Gerät neu registriert wurde und alte Befehle entfernt wurden

*Wenn sich hinter der Nachricht ein Ausrufezeichen befindet, erhalten Sie weitere Informationen, indem Sie mit dem Mauszeiger über das Symbol fahren.

Geräteeinstellungen

Client-Konfiguration

Hier können Sie die folgenden Konfigurationen auf Ihrem Android-Gerät vornehmen:

Zeit der Nichteinhaltung	Das Zeitlimit für die Benutzerantwort, nach dem die Durchsetzungsmaßnahme angewendet wird.
Durchsetzungsmaßnahmen nach Ablauf der Einhaltungsfrist	Durchsetzungsmaßnahmen, wenn ein Benutzer keine Aktionen ausführt, die zu einem konformen Gerätestatus führen
Häufigkeit der Datenerhebung	Häufigkeit, mit der Geräte-/GPS-Informationen gesammelt werden sollen
Herzschlagfrequenz des Geräts	Intervall, in dem das Gerät den AppTec Server kontaktieren soll Min. 1 Minute Max. 24 Stunden
Standortaktualisierungen aktivieren	Wenn aktiviert, sendet das Gerät Standortaktualisierungen an den AppTec Server
Standort Aktualisierungszeit	Legt fest, in welchen Zeitabständen das Gerät Standortaktualisierungen an AppTec sendet.
Verwenden Sie Google Location Accuracy für die Standortaktualisierung	Wenn aktiviert, wird der Netzwerkstandort für Standortaktualisierungen verwendet (wenn dies unter "Einschränkungen" deaktiviert wurde, hat diese Einstellung keine Auswirkungen).
GPS-Standort für Standortaktualisierung verwenden	Falls aktiviert, wird das GPS für Standortaktualisierungen verwendet.
Attraktive (gefälschte) Standorte zulassen	Ermöglicht das Fälschen von Standortinformationen über Apps von Drittanbietern

Aktion "Verlorene Verbindung	Wenn diese Option aktiviert ist, können Sie eine Aktion für den Fall festlegen, dass ein Gerät innerhalb des Heartbeat-Intervalls keine Verbindung zum MDM-Server erhält. Wenn das Gerät zum Beispiel eine Heartbeat-Zeit von 5 Minuten hat, verbindet es sich um 10:35 Uhr mit dem Server. Danach verlässt das Gerät die Wi-Fi-Reichweite. Der nächste Heartbeat um 10:40 Uhr wird fehlschlagen und die angegebene Aktion wird ausgeführt.
Aktion	Die Maßnahmen, die zu ergreifen sind, sobald ein Gerät nicht mehr konform ist. • Lock Gerät = Gerät sperren • Gerät löschen = Das Gerät wird auf die Werkseinstellungen zurückgesetzt. • Gerät und SD-Karte löschen = Das Gerät wird auf die Werkseinstellungen zurückgesetzt und der Speicher der SD-Karte wird gelöscht.
Schwellenwert	Sie können einen Schwellenwert für die Anzahl der fehlgeschlagenen Heartbeats festlegen, die erforderlich sind, um die angegebene Aktion auszulösen.

Modus zur Durchsetzung von Richtlinien	Standard:	Die Benutzer werden in regelmäßigen Abständen aufgefordert, ausstehende Aktionen auszuführen
	Faule Durchsetzung von Richtlinien:	Die Benutzer werden nie aufgefordert, ausstehende Aktionen auszuführen. Alle offenen Aktionen werden im AppTec Client angezeigt
	Aggressive Durchsetzung von Richtlinien:	Benutzer werden ununterbrochen aufgefordert, ausstehende Aktionen auszuführen
AppTec Version Lock	Falls aktiviert, kann ein Versionscode für die AppTec App angegeben werden. Der AppTec Client wird nur auf die angegebene Version aktualisiert. Neuere Versionen werden ignoriert. Ein Downgrade ist NICHT möglich.	
Version Code	Versionscode für die AppTec-App, auf die Sie sich festlegen möchten.	
AppTec-Benachrichtigung deaktivieren	Wenn diese Option deaktiviert ist, zeigt der AppTec Client keine Benachrichtigung in der Benachrichtigungsleiste an. So können Benutzer den AppTec-Client über den Task-Manager schließen. Wenn der AppTec Client	

	geschlossen ist, funktionieren verschiedene Funktionen wie der Kioskmodus und das Black-/Whitelisting von Apps nicht richtig. Samsung Geräte bieten einen Schutzmechanismus für den AppTec Client. Die Benachrichtigung ist auf Samsung-Geräten, die die KNOX-APIs unterstützen, standardmäßig deaktiviert. Die Benachrichtigung sollte bei Geräten mit Android 8.0 oder höher nicht deaktiviert werden.

Tapete

Benutzerdefiniertes Hintergrundbild einstellen	Aktivieren/Deaktivieren des benutzerdefinierten Hintergrundbildes
Tapete	Stellen Sie den Hintergrundmodus so ein, dass ein Farbcode oder ein Bild verwendet wird.
Eine Farbe angeben	Geben Sie eine Hintergrundfarbe als Hex-Wert an, z.B. #000000 für Schwarz oder #ffffff für Weiß
Bild als Hintergrundbild festlegen	Laden Sie die Bilddatei hoch, die Sie als Hintergrundbild verwenden möchten

Asset Management (nur auf Geräteebene)

Geräte-Infos

Modell	Bezeichnung des Gerätemodells
Betriebssystem	OS
OS Version	OS-Version
Seriennummer	Seriennummer
Gerät Name	Name des Geräts
Akku-Status	Status der Batterie
Freier / Gesamter Speicher	Freier / Gesamter Speicher
Samsung Safe	Samsung SAFE-Schnittstelle, erforderlich für eine Vielzahl von Einstellungsmöglichkeiten
SD-Karte verfügbar	SD-Karte verfügbar
Emulierte SD-Karte	SD-Karte emuliert
SD-Karte herausnehmbar	SD-Karte herausnehmbar
SD Freier / Gesamter Speicher	SD Freier / Gesamter SD-Kartenspeicher

Wi-Fi

IP-Adresse	IP-Adresse des Geräts
WiFi MAC	WiFi MAC-Adresse

Zellulär

Status	Status (SIM-Karte installiert)
Telefon Nummer	Telefon Nummer
Roaming (Sprache/Daten)	Roaming für Sprache/Daten
Roaming-Status	Aktueller Roaming-Status
IP-Adresse	IP-Adresse
Betreiber/Transporteur	Betreiber/Transporteur
Zellulare Technologie	Zellulare Technologie
IMEI	IMEI-Nummer
ICCID	Dies ist die ID für die SIM-Karte, oft auch eine Smartcard oder Integrated Circuit Card (ICC)
IMSI	Die International Mobile Subscriber Identity (IMSI) bietet in GSM- und UMTS-Mobilfunknetzen eine eindeutige Identifizierung der Netznutzer Die IMSI besteht aus maximal 15 Ziffern und wird auf folgende Weise konfiguriert: • Mobiler Ländercode (MCC), 3-stellig • Mobile Network Code (MNC), 2 oder 3 Ziffern • Mobile Subscriber Identification Number (MSIN), 1-10 Ziffern
Aktuelle MCC/MNC	Siehe "SIM MCC/MNC".
SIM MCC/MNC	Der Mobile Country Code ist eine etablierte Länderkennung, die von der ITU gemäß E.212 festgelegt wurde. Standard. Dieser funktioniert in Verbindung mit dem Mobile Network Code (MNC) zur Identifizierung des Mobilfunknetzes. Bedeutet den Länder-/Mobilfunknetzcode der SIM-Karte. Wenn Sie in ein anderes Mobilfunknetz roamen, sind die "Aktuelle MCC/MNC" und die "SIM MCC/MNC" logischerweise unterschiedlich.

Bluetooth

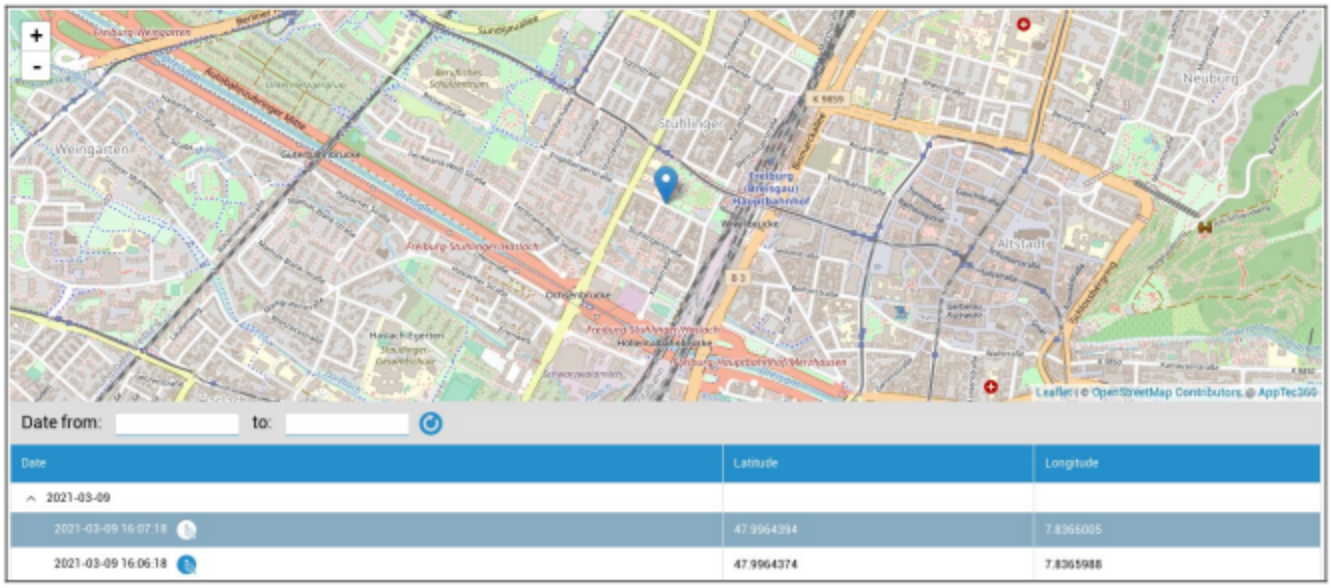
Bluetooth MAC	Bluetooth MAC-Adresse

Sicherheitsmanagement

Anti-Diebstahl (nur auf Geräteebene)

GPS-Informationen (nur auf Geräteebene)

Hier können Sie den aktuellen/letzten Standort des Geräts festlegen. Die Lokalisierung kann mit einem oder sogar zwei Passwörtern geschützt werden - Siehe: Allgemeine Einstellungen - Datenschutz - GPS-Zugang



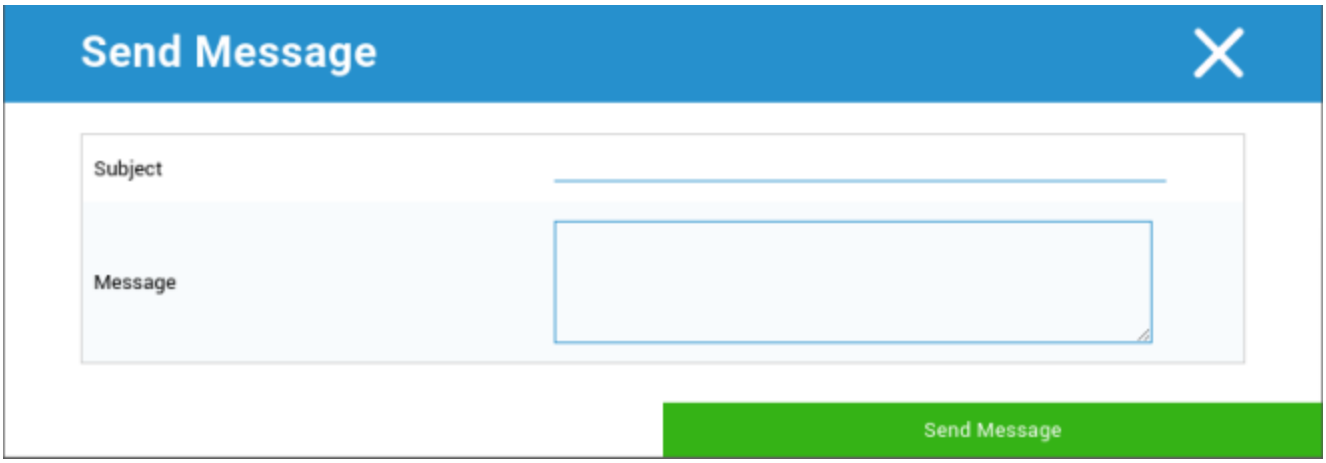
Wischen & Sperren (nur auf Geräteebene)

Unter "Wischen & Sperren" können Sie die folgenden drei Aktionen durchführen:

Vollständig abwischen	Das Gerät wird auf die Werkseinstellungen zurückgesetzt (Unternehmens- und persönliche Daten werden gelöscht). Funktioniert nur für Erweitertes Arbeitsprofil
Enterprise Wipe	Nur Unternehmensdaten werden vom Endbenutzergerät entfernt (alle Apps, Daten usw., die von AppTec bereitgestellt wurden)
Sperrbildschirm	Wenn die Bildschirmsperre aktiviert ist, reicht es aus, das Gerät mit dem Geräte-Passwort/PIN zu entsperren

Nachricht (nur auf Geräteebene)

Hier können Sie den Betreff und eine Nachricht eingeben und sie an ein Endgerät senden.



Sicherheitskonfiguration

Geräte-Passcode

Unter "Passcode" können Sie ein Gerätepasswort vergeben. Folgende Einstellungsmöglichkeiten stehen Ihnen zur Verfügung

Minimale Passwortlänge	Legt fest, wie viele Symbole ein Passwort mindestens enthalten muss	
Passwort Qualität	Nicht spezifiziert	Diese Richtlinie enthält keine Anforderungen an das Passwort.
	Biometrisch Schwach	Diese Richtlinie ermöglicht eine biometrische Erkennungstechnologie mit geringer Sicherheit. Dies setzt Technologien voraus, die die Identität einer Person bis auf eine etwa 3-stellige PIN erkennen können (die Falscherkennung liegt bei weniger als 1 zu 1.000).
	Etwas	Diese Richtlinie erfordert die Festlegung eines Kennworts oder Musters, erzwingt aber keine spezifischen Regeln.
	Alphabetisch	Der Benutzer muss ein Passwort eingegeben haben, das mindestens Buchstaben (oder andere Symbole) enthält.
	Alphanumerisch	Der Benutzer muss ein Passwort eingegeben haben, das mindestens sowohl numerische als auch alphabetische Zeichen (oder andere Symbole) enthält.
	Komplexe	Der Benutzer muss ein Passwort eingegeben haben, das standardmäßig mindestens einen Buchstaben, eine Ziffer und ein Sonderzeichen enthält. Mit dieser Passwortqualität können Passwörter auf verschiedene Zeichengruppen beschränkt werden, z. B. mindestens einen Großbuchstaben usw.
Minimale Passwortlänge	Legen Sie die erforderliche Anzahl von Zeichen für das Passwort fest. Sie können zum Beispiel verlangen, dass PINs oder Passwörter mindestens sechs Zeichen haben müssen.	
Mindestens erforderliche numerische Ziffern im Passwort	Mindestens erforderliche numerische Ziffern im Passwort	

Mindestens Kleinbuchstaben im Passwort erforderlich	Mindestens Kleinbuchstaben im Passwort erforderlich
Mindestens Großbuchstaben im Passwort erforderlich	Mindestens Großbuchstaben im Passwort erforderlich
Mindestens erforderliche Nicht-Buchstaben-Zeichen im Passwort	Mindestens erforderliche Nicht-Buchstaben-Zeichen im Passwort
Mindestens erforderliche Symbole im Passwort	Mindestens erforderliche Symbole im Passwort

Sperre für maximale Inaktivitätszeit	Maximale Benutzerinaktivität bis zur Zeitsperre
Zeitlimit für den Ablauf des Passworts	Legt fest, nach welchem Zeitintervall das Passwort abläuft und ein neues Passwort vergeben werden muss
Einschränkung des Passwortverlaufs	Anzahl der zuvor verwendeten Passwörter, die nicht erlaubt sind
Maximale Anzahl fehlgeschlagener Passwortversuche	Legt fest, wie oft ein Passwort falsch eingegeben werden kann, bevor ein komplettes Löschen des Geräts durchgeführt wird.
Biometrische Authentifizierung zulassen	Ermöglicht die Authentifizierung per Fingerabdruck oder Irisscan. Nur für Samsung KNOX 2.1 und höher

Container Passcode

Unter "Passcode" können Sie ein Container-Passwort vergeben, die folgenden Einstellungsmöglichkeiten sind
verfügbar für Sie

Minimale Passwortlänge	Legt fest, wie viele Symbole ein Passwort mindestens enthalten muss	
Passwort Qualität	Nicht spezifiziert	Diese Richtlinie enthält keine Anforderungen an das Passwort.
	Biometrisch Schwach	Diese Richtlinie ermöglicht eine biometrische Erkennungstechnologie mit geringer Sicherheit. Dies setzt Technologien voraus, die die Identität einer Person bis auf eine etwa 3-stellige PIN erkennen können (die Falscherkennung liegt bei weniger als 1 zu 1.000).
	Etwas	Diese Richtlinie erfordert die Festlegung eines Kennworts oder Musters, erzwingt aber keine spezifischen Regeln.
	Alphabetisch	Der Benutzer muss ein Passwort eingegeben haben, das mindestens Buchstaben (oder andere Symbole) enthält.
	Alphanumerisch	Der Benutzer muss ein Passwort eingegeben haben, das mindestens sowohl numerische als auch alphabetische Zeichen (oder andere Symbole) enthält.
	Komplexe	Der Benutzer muss ein Passwort eingegeben haben, das standardmäßig mindestens einen Buchstaben, eine Ziffer und ein Sonderzeichen enthält. Mit dieser Passwortqualität können Passwörter auf verschiedene Zeichengruppen beschränkt werden, z. B. mindestens einen Großbuchstaben usw.
Minimale Passwortlänge	Legen Sie die erforderliche Anzahl von Zeichen für das Passwort fest. Sie können zum Beispiel verlangen, dass PINs oder Passwörter mindestens sechs Zeichen haben müssen.	
Mindestens erforderliche numerische Ziffern im Passwort	Mindestens erforderliche numerische Ziffern im Passwort	
Mindestens Kleinbuchstaben im	Mindestens Kleinbuchstaben im Passwort erforderlich	

Passwort erforderlich	
Mindestens Großbuchstaben im Passwort erforderlich	Mindestens Großbuchstaben im Passwort erforderlich
Mindestens erforderliche Nicht-Buchstaben-Zeichen im Passwort	Mindestens erforderliche Nicht-Buchstaben-Zeichen im Passwort
Mindestens erforderliche Symbole im Passwort	Mindestens erforderliche Symbole im Passwort

Sperre für maximale Inaktivitätszeit	Maximale Benutzerinaktivität bis zur Zeitsperre
Zeitlimit für den Ablauf des Passworts	Legt fest, nach welchem Zeitintervall das Passwort abläuft und ein neues Passwort vergeben werden muss
Einschränkung des Passwortverlaufs	Anzahl der zuvor verwendeten Passwörter, die nicht erlaubt sind
Maximale Anzahl fehlgeschlagener Passwortversuche	Legt fest, wie oft ein Passwort falsch eingegeben werden kann, bevor ein komplettes Löschen des Geräts durchgeführt wird.

AntiVirus

Automatischer Scan	Regelmäßige automatische Scans aktivieren
Scan-Intervall	Intervall für die Untersuchung (Schnell / Vollständig)
Vollständiger automatischer Scan	Vollständige automatische Scans aktivieren
Automatische Updates	Aktivieren Sie automatische Updates
Intervall der Aktualisierungsprüfung	Wie oft die App und ihre Datenbank aktualisiert werden sollten (Viren / beschädigter Code)
App-Schutz	Automatischen App-Scan aktivieren
SD-Karten Schutz	Automatischen SD-Karten-Scan einschalten
Nur Wi-Fi Update	Wenn diese Option aktiviert ist, werden Updates nur dann angewendet, wenn das Gerät erfolgreich mit einem Wi-Fi-Netzwerk verbunden ist.

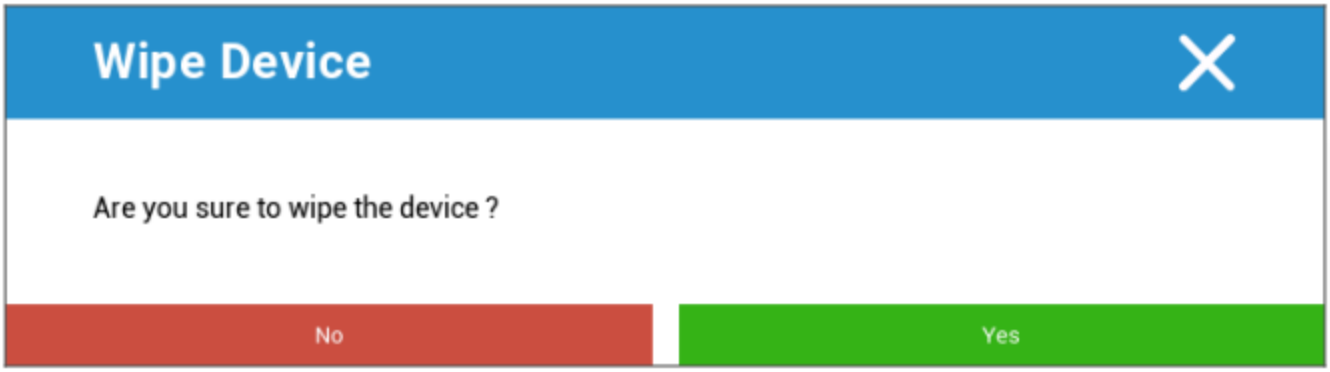
Ende der Lebensdauer (nur auf Geräteebene)

Wischen (nur auf Geräteebene)

Unter "Wischen" können Sie das Gerät auf die Werkseinstellungen zurücksetzen (nur bei erweitertem Arbeitsprofil).

Hier werden sowohl die Unternehmensdaten als auch die privaten Daten auf dem Endgerät des Benutzers gelöscht.

Mit einem Klick auf das "Minus-Symbol" erhalten Sie die folgende Meldung:



Mit "Ja" können Sie die Löschung durchführen.

Unter "Wischbericht" können die folgenden Punkte angezeigt werden

Abgewischt von	Historie der Person, die den Wisch durchgeführt hat
Datum	Datum
Status	Status (z.B. ob der Löschvorgang erfolgreich durchgeführt wurde)

Einstellungen zur Einschränkung

Beschränkungen

Hier kann eine Vielzahl von Dingen eingeschränkt und blockiert werden.

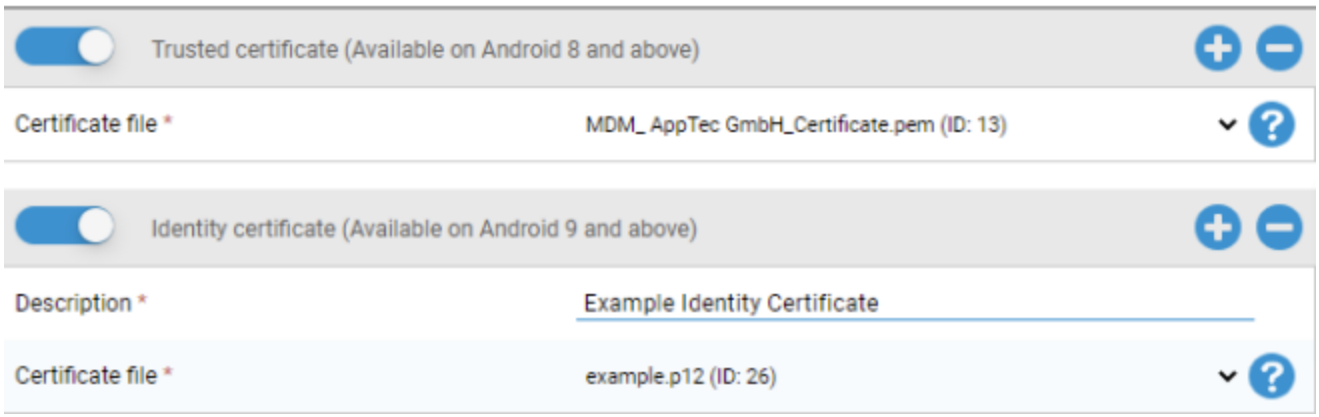
Durchsetzung der Compliance	Modus Benutzer auffordern - Der Benutzer wird aufgefordert, die notwendigen Aktionen durchzuführen. Mode Lock-Down Container - Blenden Sie alle Anwendungen aus, bis alle Anforderungen erfüllt sind
Richtlinie für Laufzeitberechtigungen	Aufforderung an den Benutzer für neue Berechtigungsanfragen Neue Genehmigungsanfragen immer gewähren Neue Genehmigungsanfragen immer ablehnen Warnung: Einige Apps haben Probleme, die Berechtigungen zu erkennen, wenn diese automatisch eingestellt sind. Wenn Sie immer Berechtigungen erteilen und Probleme mit Apps auftreten, die behaupten, dass Berechtigungen fehlen, setzen Sie dies auf "Benutzer auffordern" und installieren Sie die App neu.
Ausgehende Zwischenablage zulassen	Ermöglicht das Kopieren und Einfügen aus dem Inneren des Containers nach außen
Auflösung der Anrufer-ID zulassen	Zeigt den Namen für einen eingehenden Anruf basierend auf den Kontakten im Container an
Auflösung der Kontaktsuche zulassen	Ermöglicht die Suche nach Namen in den Containerkontakten bei Anrufen
Bluetooth-Kontaktfreigabe zulassen	Ermöglicht den Zugriff auf den Containerkontakt in einem Auto
Ausgehenden NFC-Strahl verbieten	Deaktiviert NFC für den Container
Unbekannte Quellen zulassen	Wenn diese Funktion aktiviert ist, können Benutzer Apps durch die Installation einer .apk-Datei sideloaden.
USB-Debugging zulassen	Wenn diese Option aktiviert ist, können Sie das USB-Debugging aktivieren.
Kontomodifikation verbieten	Verbietet die Erstellung, Löschung und Änderung von Konten im Container Beachten Sie, dass einige Anwendungen Konten erstellen oder ändern müssen, damit sie wie erwartet funktionieren.

Einschränkungen des Arbeitsprofils. Nur auf Geräten mit Android 11 und höher verfügbar, mit Enhanced Work Profile	
Kamera verbieten	Gibt an, ob die Kamera im Arbeitsprofil nicht zugelassen ist.
Bluetooth deaktivieren	Gibt an, ob Bluetooth im Arbeitsprofil nicht erlaubt ist.
Schutz vor Werksreset aktivieren	Aktivieren Sie dies, um den Schutz vor dem Zurücksetzen auf die Werkseinstellungen von Android auf das Google-Konto zu übertragen, das Sie unter "Allgemeine Einstellungen" → "Android-Konfiguration" → "Android Enterprise" → "Schutz vor dem Zurücksetzen auf die Werkseinstellungen" definiert haben. Wenn dies aktiviert ist und Sie das Gerät zurücksetzen, müssen Sie das konfigurierte Google-Konto angeben, um das Gerät erneut einzurichten.
OS-Update steuern	Aktivieren Sie diese Option, um das Aktualisierungsverhalten auf automatisch, in einem Fenster oder zeitversetzt einzustellen.
Politik aktualisieren	Automatisch: Automatisch installieren, sobald ein Update verfügbar ist. Mit Fenster: Automatische Installation innerhalb eines täglichen Wartungsfensters. Dadurch werden auch die Play-Apps so konfiguriert, dass sie innerhalb des Fensters aktualisiert werden. Dies wird für Kiosk-Geräte dringend empfohlen, denn nur so können Apps, die dauerhaft in den Vordergrund gepinnt sind, von Play aktualisiert werden. Aufschieben: Verschieben Sie die automatische Installation bis zu maximal 30 Tage.

Persönliche Profileinschränkungen. Nur auf Geräten mit Android 11 und höher verfügbar, mit Enhanced Work Profile	
Kamera verbieten	Gibt an, ob die Kamera im persönlichen Profil nicht erlaubt ist.
Bluetooth deaktivieren	Gibt an, ob Bluetooth im persönlichen Profil nicht erlaubt ist.
Unbekannte Quellen zulassen	Wenn diese Option aktiviert ist, können Benutzer von Arbeitsprofilen Apps durch die Installation einer .apk-Datei sideloaden.

Zertifikat Management

Hier können Sie vertrauenswürdige Zertifikate und Identitätszertifikate an Ihre Geräte verteilen. Android 8 oder höher ist erforderlich, um vertrauenswürdige Zertifikate zu verteilen und Android 9 oder höher ist erforderlich, um Identitätszertifikate zu verteilen.



Mit dem "+" können Sie mehrere Zertifikate hinzufügen.

Vertrauenswürdige Zertifikate müssen im PEM-Format vorliegen.

Identitätszertifikate müssen im PKCS12-Format vorliegen.

Verbindungsmanagement

Wifi

Führen Sie für diese Einstellung die Vorkonfiguration der Endbenutzergeräte durch, für den Zugriff auf den internen Access
Punkte

Services Set Identifier (SSID)	SSID für das Netzwerk, mit dem eine Verbindung hergestellt werden soll
Verborgenes Netzwerk	Aktivieren, für den Fall, dass der AP die SSID nicht sendet

Sicherheit Typ

Legen Sie den Sicherheitstyp des APs fest

WEP

Passwort	Passwort für den AP

WPA/WPA2

Passwort	Passwort für den AP

802.1x EAP

EAP-Methode

PWD	Identität	Identität
	Passwort	Passwort

PEAP	Phase 2 Authentifizierungsprotokoll	keine	Kein zusätzliches Protokoll
		MSCHAPV2	MSCHAPV2-Protokoll
		GTC	GTC-Protokoll
	CA-Zertifikat	CA-Zertifikat	
	Identität	Identität	
	Anonyme Identität	Anonyme Identität	
	Passwort	Passwort	

TTLS	Phase 2 Authentifizierungsprotokoll	keine	Kein zusätzliches Protokoll
		PAP	PAP-Protokoll
		MSCHAP	MSCHAP-Protokoll
		MSCHAPV2	MSCHAPV2-Protokoll
		GTC	GTC-Protokoll
	CA-Zertifikat	CA-Zertifikat	
	Identität	Identität	
	Anonyme Identität	Anonyme Identität	
	Passwort	Passwort	

TLS	CA-Zertifikat	CA-Zertifikat
	Identität	Identität
	Passwort	Passwort

VPN

Name der Verbindung	Name der VPN-Verbindung

VPN-Typ

VPN

VPN-Client

AppTec VPN-Client	
Gateway-Konfiguration	Wählen Sie die Gateway-VPN-Konfiguration (siehe **Allgemeine Einstellungen > Universal Gateway > VPN-Einstellungen**)
Immer eingeschaltetes VPN	Native Abriegelung aktivieren
Aktivieren Sie AppTec Lockdown	Aktivieren Sie AppTec Lockdown

Eingebaut (nur auf Samsung-Geräten verfügbar)			
Verbindungstyp	PPTP	Server	Server
		PPTP-Verschlüsselung aktivieren	PPTP-Verschlüsselung aktivieren
	L2TP / IPSec PSK	Server	Server
		IPSec Pre-Shared Key	IPSec Pre-Shared Key
		L2TP-Geheimnis aktivieren	L2TP-Geheimnis aktivieren
		L2TP Geheimnis	L2TP Geheimnis
	IPSec XAuth PSK	Server	Server
		IPSec-Bezeichner	IPSec-Bezeichner
		IPSec Pre-Shared Key	IPSec Pre-Shared Key
DNS-Suchdomänen	DNS-Suchdomänen		
Experten-Einstellungen	DNS-Server	DNS-Server	
	Weiterleitungsrouten	Weiterleitungsrouten	

VPN öffnen		
Server	Server	
OpenVPN-Profil	OpenVPN-Profil	
OpenVPN-App	OpenVPN für Android (empfohlen)	
	OpenVPN-Verbindung	
Experten-Einstellungen	DNS-Server	DNS-Server
	Weiterleitungsrouten	Weiterleitungsrouten

Samsung / Starker Schwan			
Verbindungstyp	PPTP	Server	Server
		Benutzername	Benutzername
		Passwort	Passwort
		PPTP-Verschlüsselung aktivieren	PPTP-Verschlüsselung aktivieren
	L2TP / IPSec PSK	Server	Server
		IPSec Pre-Shared Key	IPSec Pre-Shared Key
		Benutzername	Benutzername
		Passwort	Passwort
		L2TP-Geheimnis aktivieren	L2TP Geheimnis
	IPSec XAuth PSK	Server	Server
		IPSec-Bezeichner	IPSec-Bezeichner
		IPSec Pre-Shared Key	IPSec Pre-Shared Key
		Benutzername	Benutzername
		Passwort	Passwort
Experten-Einstellungen	DNS-Server	DNS-Server	
	Weiterleitungsrouten	Weiterleitungsrouten	

Cisco Any Connect		
Server	Server	
Zertifikat-Modus	Behinderte	Behinderte
	Automatisch	Automatisch
Experten-Einstellungen	DNS-Server	DNS-Server
	Weiterleitungsrouten	Weiterleitungsrouten

Pro-App VPN

VPN-Client

AppTec VPN-Client		
Gateway-Konfiguration	Wählen Sie die Gateway-VPN-Konfiguration (siehe **Allgemeine Einstellungen > Universal Gateway > VPN-Einstellungen**)	
VPN-Apps	VPN-Apps	
Immer eingeschaltetes VPN	Native Abriegelung aktivieren	Immer eingeschaltetes VPN
Aktivieren Sie AppTec Lockdown	Aktivieren Sie AppTec Lockdown	

Samsung / Starker Schwan			
Verbindungstyp	PPTP	Server	Server
		VPN-Apps	VPN-Apps
		Benutzername	Benutzername
		Passwort	Passwort
		PPTP-Verschlüsselung aktivieren	PPTP-Verschlüsselung aktivieren
	L2TP / IPSec PSK	Server	Server
		VPN-Apps	VPN-Apps
		IPSec Pre-Shared Key	IPSec Pre-Shared Key
		Benutzername	Benutzername
		Passwort	Passwort
		L2TP-Geheimnis aktivieren	L2TP Geheimnis
	IPSec XAuth PSK	Server	Server
		VPN-Apps	VPN-Apps
		IPSec-Bezeichner	IPSec-Bezeichner
		IPSec Pre-Shared Key	IPSec Pre-Shared Key
		Benutzername	Benutzername
		Passwort	Passwort
Experten-Einstellungen	DNS-Server	DNS-Server	
	Weiterleitungsrouten	Weiterleitungsrouten	

Beschränkungen

Hier können Sie die Einschränkungen in Bezug auf die Verbindungsverwaltung festlegen

Daten-Roaming zulassen	Mobile Daten beim Roaming zulassen
Daten-Roaming erzwingen	Falls aktiviert, ist das Roaming für mobile Daten dauerhaft aktiviert (nicht empfohlen!) Diese Einstellung überschreibt die Einstellung "Datenroaming zulassen"!
System http Proxy Server verwenden	Die Verwendung eines HTTP-Proxyservers, der von den Systemeinstellungen in den Einstellungen bereitgestellt wird, ist abhängig vom verbundenen Netzwerk (WiFi oder APN)

PIM-Verwaltung

Google Mail Austausch

Info: Diese Konfiguration wird auf die Google Mail-App angewendet. Sie müssen also Gmail genehmigen und installieren.

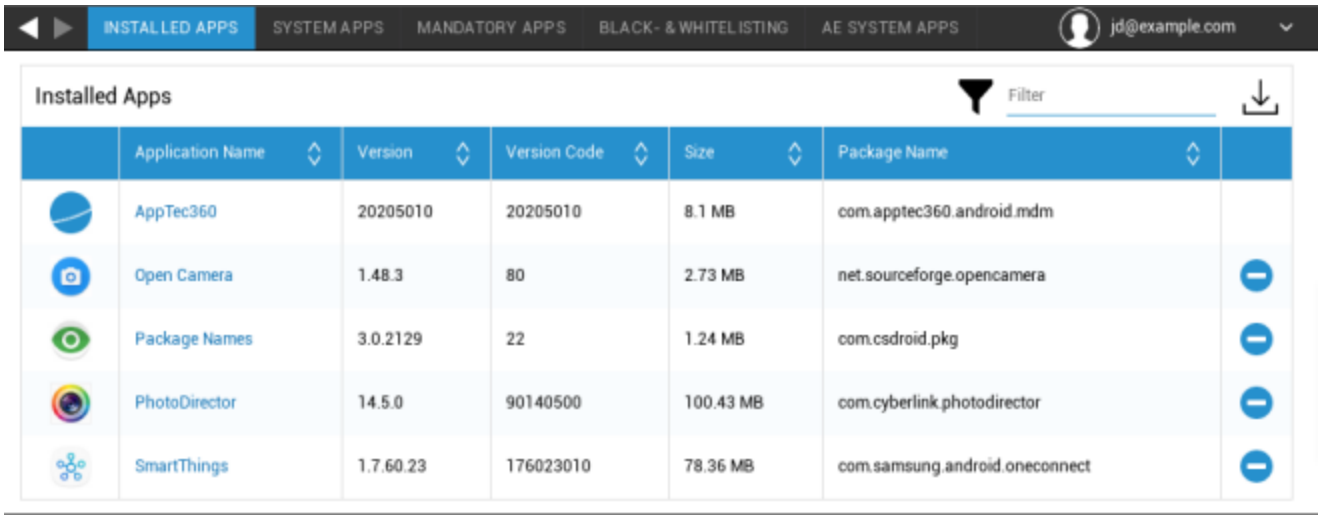
eMail-Adresse	Die angegebene E-Mail-Adresse des Benutzers Bitte beachten Sie die "Platzhalter", die Sie für die Arbeit mit Anmeldeinformationen verwenden können und die Sie nicht auf jedem Gerät manuell ändern müssen Mit einem Klick auf können Sie sie sich selbst anzeigen lassen
Server-Hostname	Serveradresse Ihres Exchange Servers
Login-Name	Der Login-Name für das jeweilige Endgerät, bitte beachten Sie auch die "Platzhalter hier
Unterschrift	Eine Signatur kann angehängt werden (Hinweis: Einige Geräte erfordern eine HTML-Formatierung für die Signatur)
Anzahl der zu synchronisierenden Vortage	Anzahl der Tage, die bestimmen, wann die E-Mails wieder synchronisiert werden
Geräte-Identifikator	Ein String der die EAS DeviceID enthält. Dies ist Teil des EAS Protokols und wird in einigen Umgebungen benötigt
Verwenden Sie Secure Sockets Layer (SSL)	Verwenden Sie eine SSL-Verbindung
Alle Zertifikate akzeptieren	Alle Zertifikate werden akzeptiert. Bitte wählen Sie diese Option, wenn Ihr Exchange Server ein selbstsigniertes Zertifikat verwendet
Nicht verwaltete Konten zulassen	Erlauben Sie Benutzern, jedes beliebige Exchange-Konto hinzuzufügen oder zu entfernen, außer dem in dieser verwalteten Konfiguration angegebenen Konto. Wenn diese Einstellung aktiviert ist, können Sie nicht verhindern, dass Benutzer andere Exchange-Konten zu Google Mail hinzufügen. Außerdem können Sie die gemeinsame Nutzung von Daten durch andere Anwendungen und Exchange-Konten, die von Benutzern hinzugefügt wurden, nicht kontrollieren. Diese Einstellung sollte nur aktiviert werden, wenn Ihre Benutzer mehr als ein Arbeits-Exchange-Konto in Google Mail unterhalten müssen.
Kundenzertifikat	Client-Zertifikat. Nur erforderlich, wenn Ihr Mailserver diese Angabe erwartet.

App Verwaltung

Enterprise App Manager

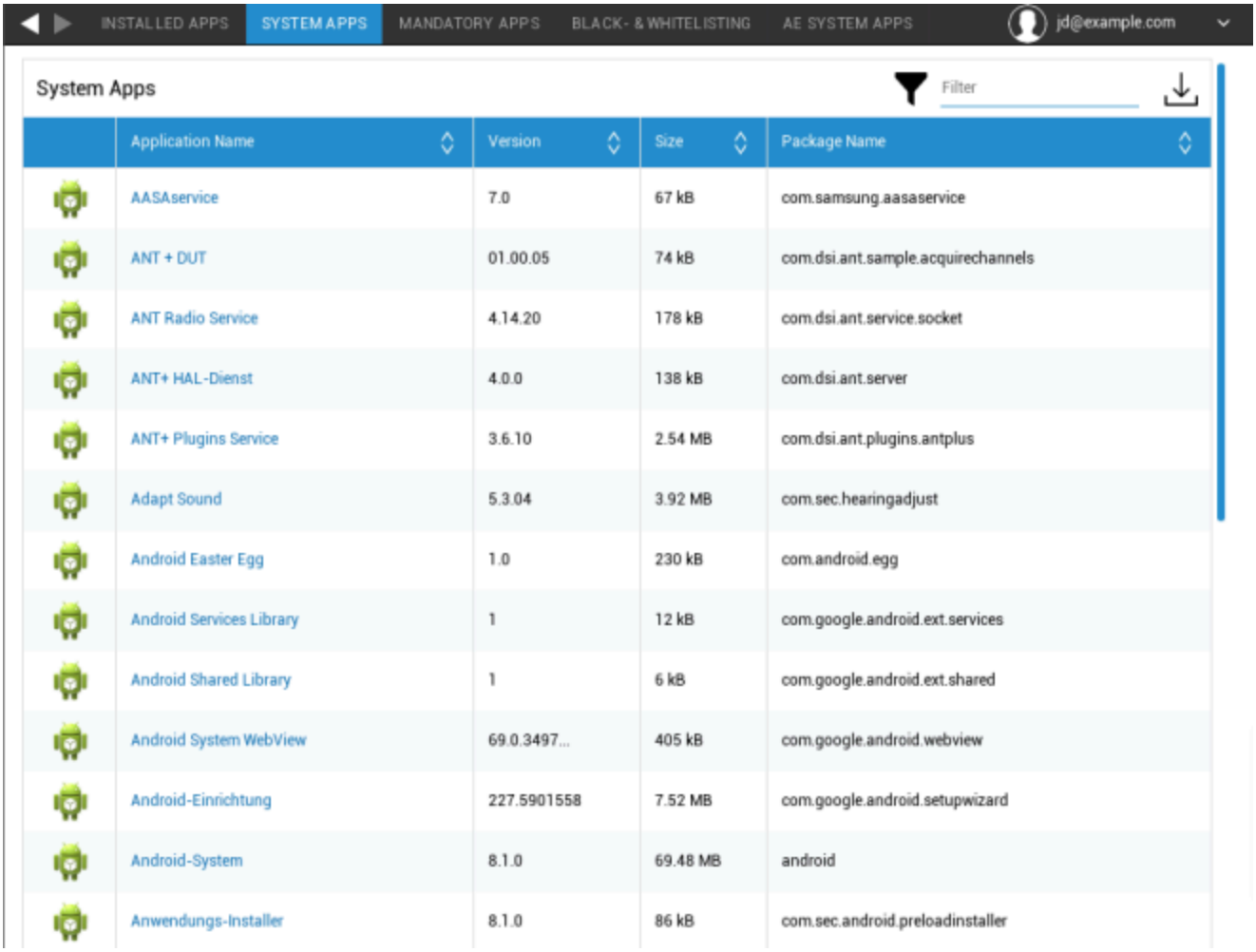
Installierte Apps (nur auf Geräteebene)

Hier werden Ihnen alle Apps angezeigt, die derzeit im Container installiert sind.



System-Apps (nur auf Geräteebene)

Unter "System-Apps" werden alle Apps und Dienste aufgelistet, die bereits von Ihrem Gerätehersteller auf dem Endgerät installiert wurden.

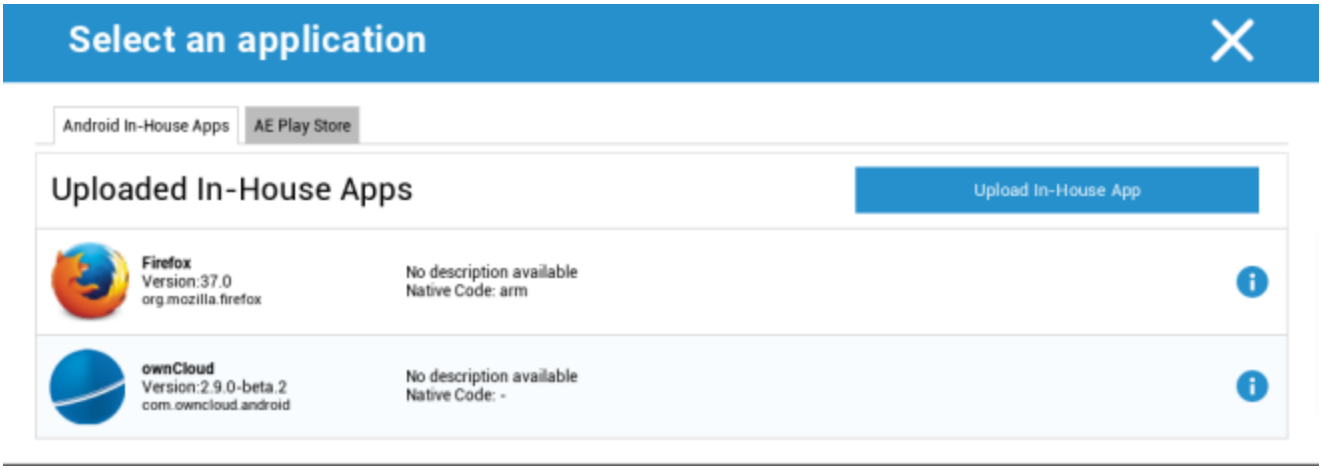


Obligatorische Apps

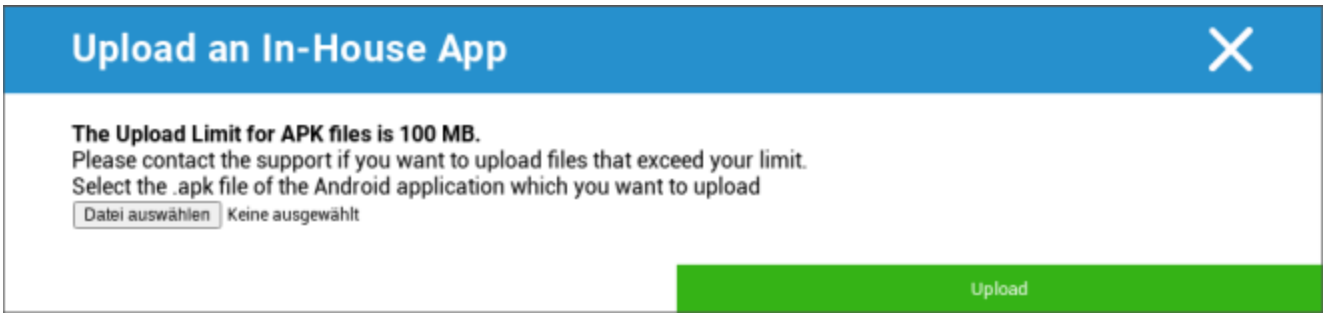
Unter den obligatorischen Apps können Sie die obligatorisch erforderlichen Apps festlegen. Wenn es sich um eine InHouse App handelt, wird der Benutzer ständig aufgefordert, diese App zu installieren. Die Play Store-Apps werden automatisch installiert.

Über die können Sie die obligatorisch benötigte App definieren.

Dies kann eine In-House App aus den "Android In-House Apps" sein, die Sie in den Allgemeinen Einstellungen hochgeladen haben.

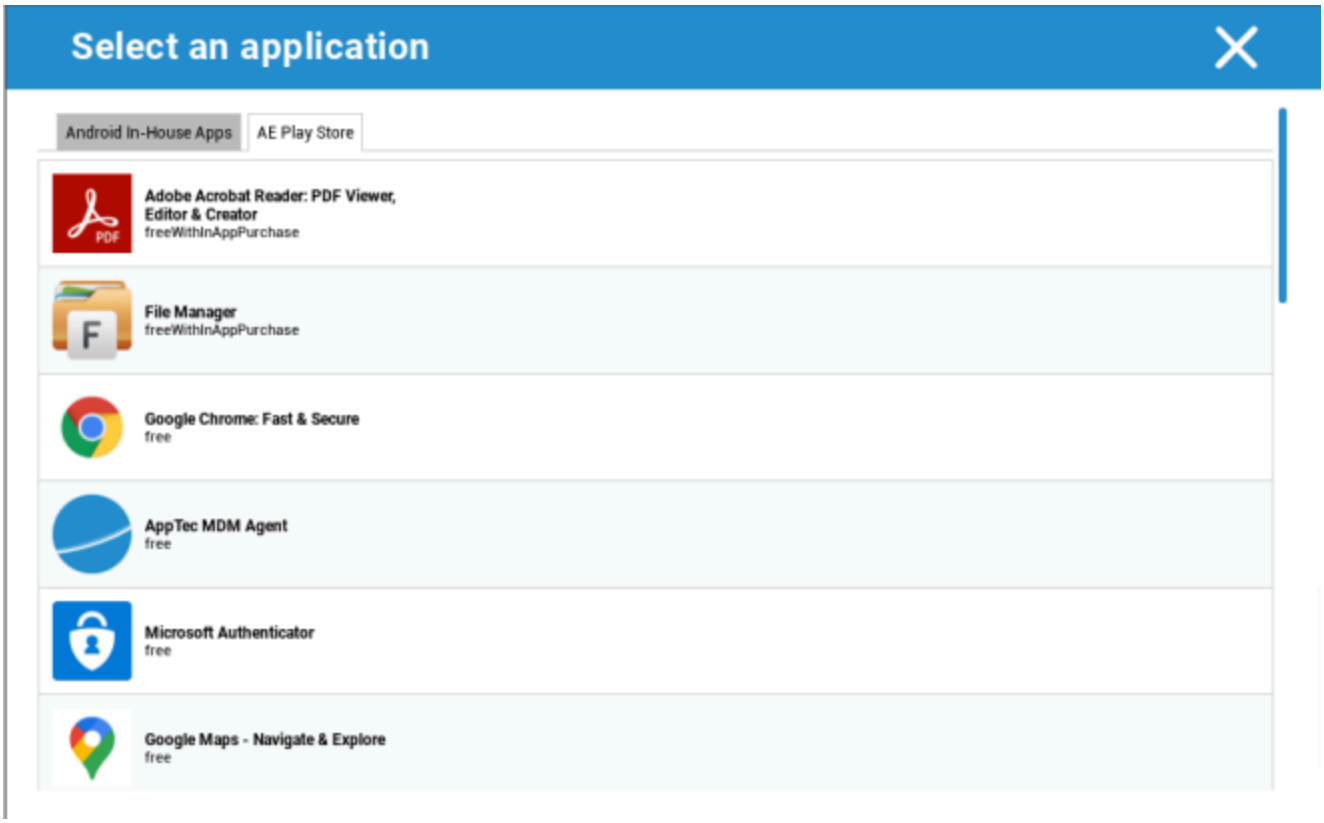


Sie können auch direkt eine apk-Datei mit "In-House App hochladen" auswählen und hochladen.



Wenn Sie eine In-House App installieren, haben Sie die Möglichkeit, "Auf dem Laufenden halten" zu aktivieren. Wenn dies aktiviert ist und Sie eine neuere Version in der In-House App DB definiert haben, wird die App auf dem Gerät aktualisiert.

Oder es kann eine "AE Play Store" App aus dem Google Work Play Store sein.



Nur genehmigte "AE Play Store Apps" werden in dieser Registerkarte angezeigt.

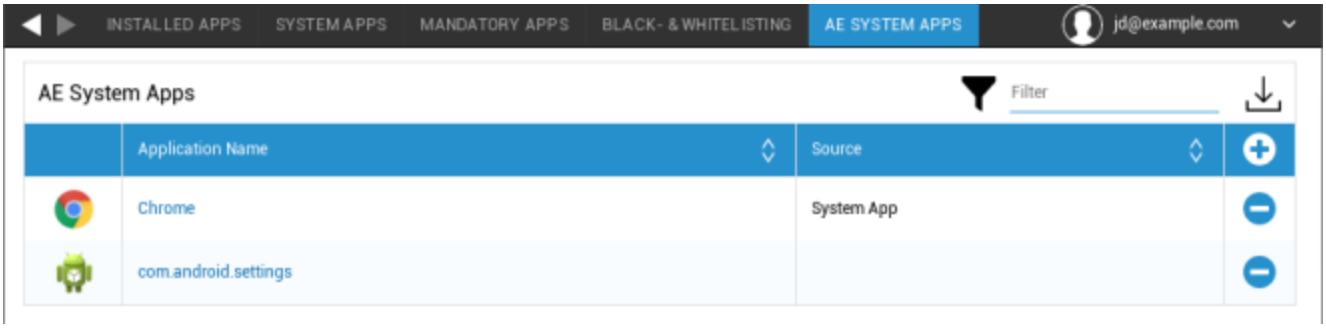
Um eine "AE Play Store App" zu genehmigen, gehen Sie bitte zu "Allgemeine Einstellungen" > "App Management" > "AE Play

Store" und fügen Sie eine App über die Schaltfläche hinzu, die Sie zur Registerkarte "Play Store Apps" weiterleitet (oder Sie können direkt zur Registerkarte "Play Store Apps" gehen).

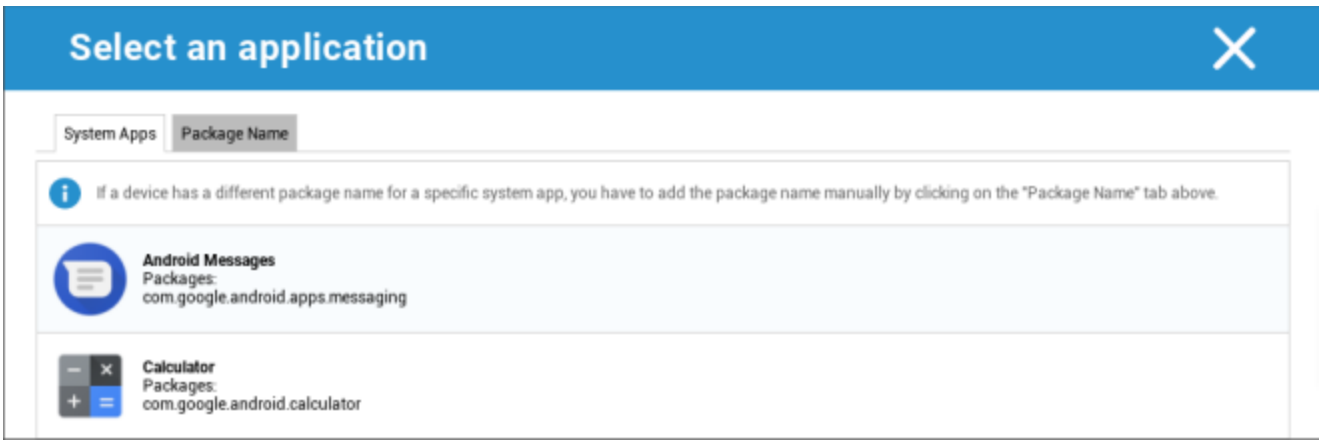
Auf der Registerkarte "Play Store Apps" können Sie nach Apps suchen. Wenn Sie auf eine App klicken, öffnet sich die App-Seite und hier können Sie die App genehmigen, indem Sie auf "Genehmigen" klicken.

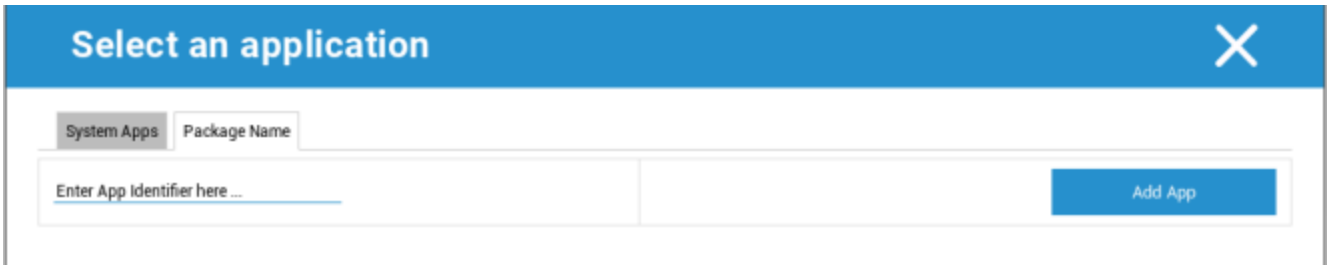
AE System Apps

Hier können Sie eine Liste definieren, die bestimmte System-Apps enthält, die auf den Geräten aktiviert werden sollen.



Wenn Sie auf die Schaltfläche klicken, können Sie aus einer von Google bereitgestellten Liste möglicher System-Apps wählen oder direkt den Paketnamen einer System-App eingeben, die aktiviert werden soll.





Bitte beachten Sie, dass die System-Apps in der von Google bereitgestellten Liste nur Apps sind, die System-Apps sein können, aber nicht unbedingt System-Apps auf Ihren Geräten sein müssen.

Diese Liste betrifft jedoch nur Apps, die bereits vorinstalliert sind.

Das Hinzufügen von Apps, die nicht auf Ihren Geräten vorinstalliert sind, wirkt sich nicht auf Ihre Geräte aus, unabhängig davon, ob die App aus der von Google bereitgestellten Liste stammt oder der

Paketname der App direkt eingegeben wird.

Beschränkungen & Einstellungen

App Management Einstellungen

Hier können Sie das Verhalten des Geräts in Bezug auf App-Updates konfigurieren.

Häufigkeit der Aktualisierungsprüfung	Legen Sie fest, in welchem Intervall der AppTec Client nach App-Updates suchen soll. Der Standardwert ist 24 Stunden.
Wi-Fi Schwellenwert	Apps, die größer als die angegebene Größe sind, werden über Wi-Fi heruntergeladen. Wenn "Nur Wi-Fi" ausgewählt ist, werden alle Apps über Wi-Fi heruntergeladen.

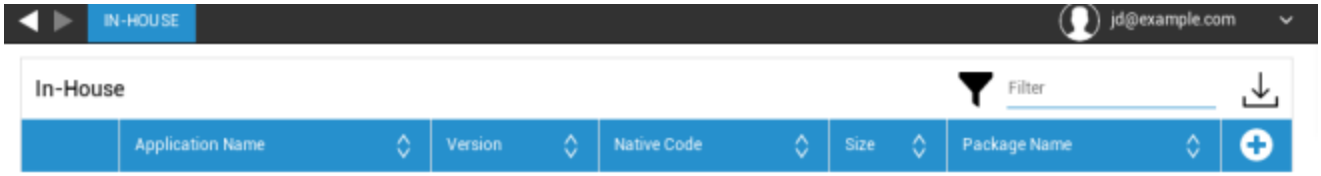
Enterprise App Store

Hausintern

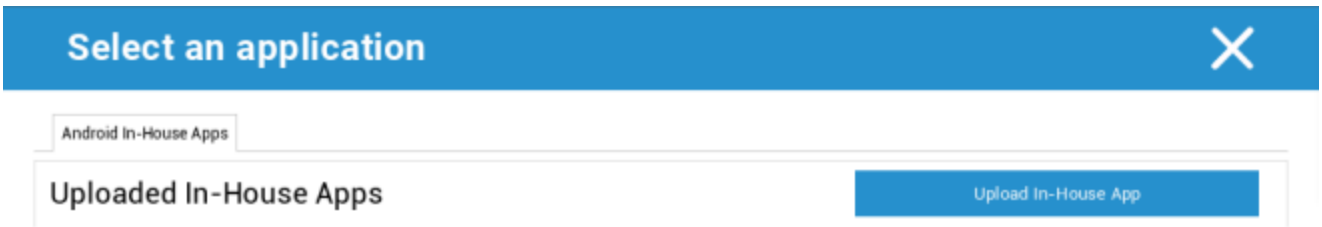
Unter dem Punkt "In-House" können Sie intern entwickelte Apps hochladen und verbreiten.

Mit dem Symbol können Sie zusätzliche In-House Apps vertreiben.

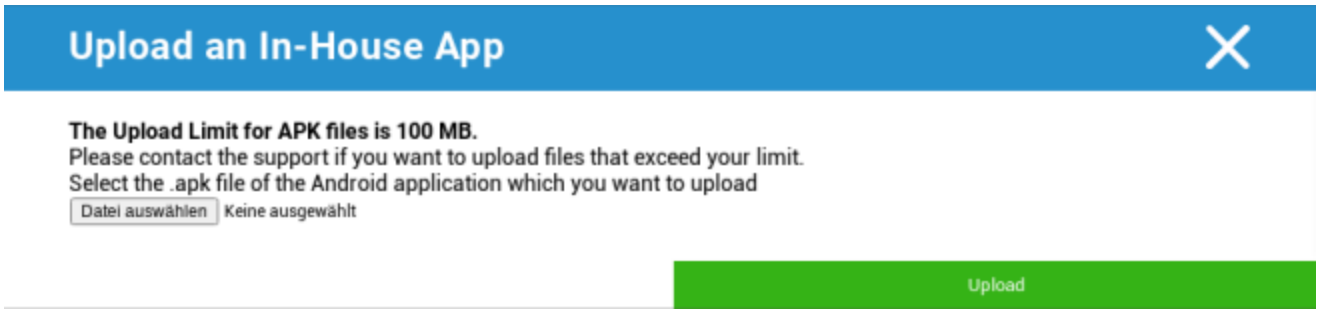
Wenn Sie eine In-House App installieren, haben Sie die Möglichkeit, "Auf dem Laufenden halten" zu aktivieren. Wenn dies aktiviert ist und Sie eine neuere Version in der In-House App DB definiert haben, wird die App auf dem Gerät aktualisiert.



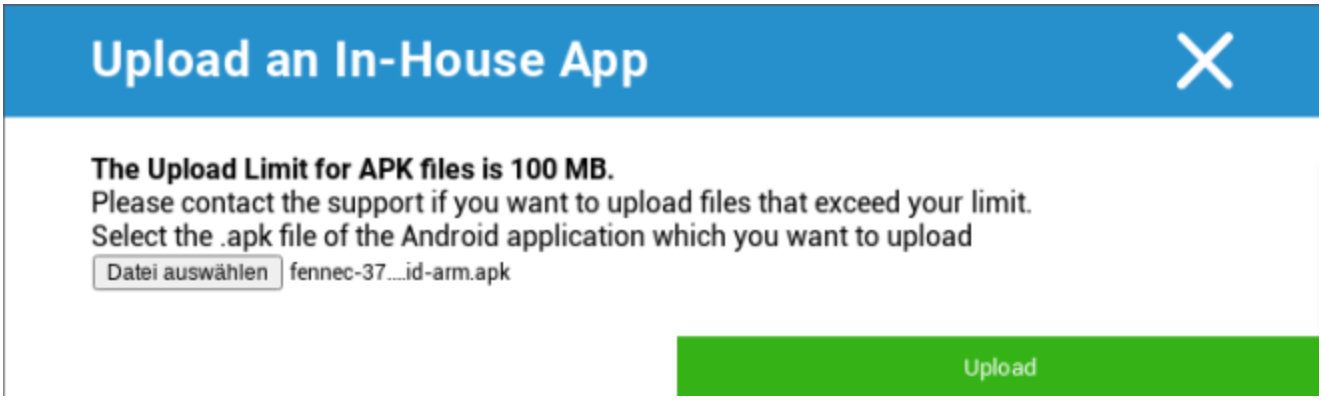
Sollten Sie keine In-House Apps verteilt haben, erhalten Sie dann die folgende Übersicht:



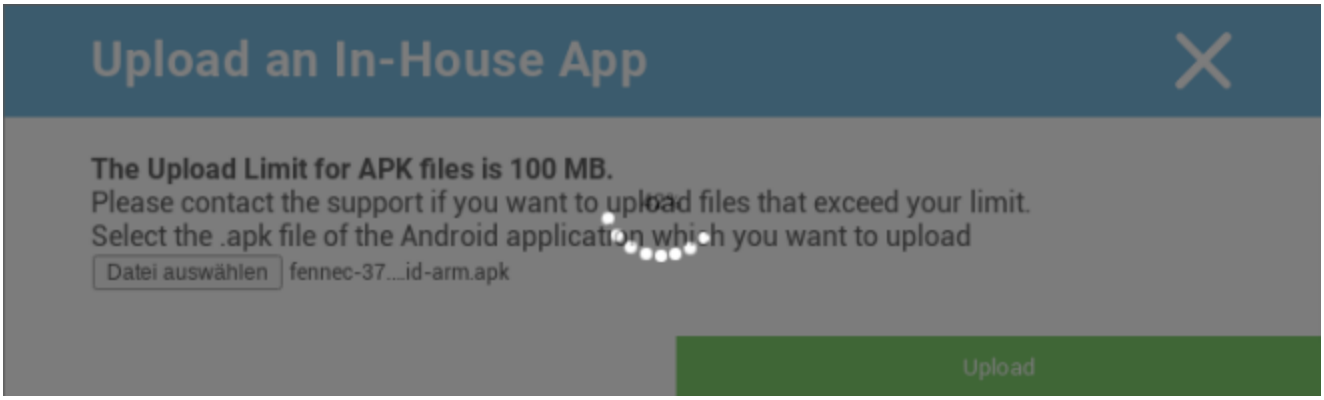
Klicken Sie dazu auf "In-House App hochladen", Sie erhalten dann die folgende Übersicht:



Wählen Sie nun mit "Suchen..." eine .apk-Datei aus und klicken Sie dann auf "Hochladen".



Ihre App wird nun hochgeladen. In der Mitte des Kreises sehen Sie eine Prozentanzeige, die angibt, wie viel von Ihrer App bereits hochgeladen wurde.



Sollte der Upload Ihrer In-House App erfolgreich gewesen sein, finden Sie die hochgeladene App in Ihrem App-Katalog.

Der Benutzer hat nun die Möglichkeit, diese App im AppTec Store auf dem Endgerät unter der Kategorie "In-House" zu sehen und zu installieren.

Da es sich hierbei nicht um eine Google PlayStore App handelt, benötigt der Benutzer keine gespeicherte Google ID auf seinem jeweiligen Endgerät.

Enterprise Play Store

AE Play Store

Hier können Sie Apps zum Android Enterprise Playstore hinzufügen. Bitte beachten Sie, dass Sie Apps mit Ihrem AE Administrator-Konto genehmigen müssen, bevor Sie sie hinzufügen können.

Um eine App zu genehmigen, lesen Sie bitte die Anweisungen unter Obligatorische Apps.

Content Management

ContentBox

Hier können Sie die ContentBox aktivieren.

Sobald Sie "Enable ContentBox" auf "On" schalten, wird automatisch eine separate ContentBox App auf dem Endgerät des Benutzers installiert.

Sicherer Browser

Hier können Sie Einstellungen für den AppTec Secure Browser vornehmen.

Sobald Sie den Abschnitt unter "Sicherer Browser" auf "Ein" stellen, wird automatisch eine separate Browser-App auf dem Endgerät des Benutzers installiert.

Passwort anfordern	Verlangen Sie vom Benutzer die Einrichtung und Verwendung eines Passworts für den Zugriff auf den Browser.
Minimal erforderliche Passwortlänge	Legen Sie die erforderliche Anzahl von Zeichen für das Passwort fest
Erforderliche Passwortqualität	Legen Sie die erforderliche Passwortqualität fest
Downloads einschränken / Öffnen in	
Uploads einschränken	
Whitelist hochladen	Eine Liste von URLs, für die das Hochladen immer erlaubt ist.
Kopieren zulassen	Erlauben Sie das Kopieren, Ausschneiden oder Teilen von Text innerhalb der Webseiten.
Bildschirmaufzeichnung zulassen	Erlauben Sie die Aufnahme von Bildschirmfotos.
Häufigkeit der Datenbereinigung	Wählen Sie, wie oft ALLE Benutzerdaten (Verlauf, Cache usw.) automatisch gelöscht werden sollen.
Lesezeichen für Unternehmen	Die Lesezeichen werden im Ordner "Firmenlesezeichen" in den Lesezeichen des Browsers angezeigt. Sie können vom Benutzer nicht bearbeitet werden.
Adressleiste ausblenden	
In-Browser Whitelisting (ohne Universal Gateway)	Aktiviert das URL-Whitelisting auf der Client-Seite. • Firmen-Lesezeichen sind immer auf der Whitelist • Wird nur für 100 URLs unterstützt • Bitte verwenden Sie den Universal Gateway für unbegrenztes Black- und Whitelisting
URLs auf der Whitelist	Eine Liste der erlaubten URLs.

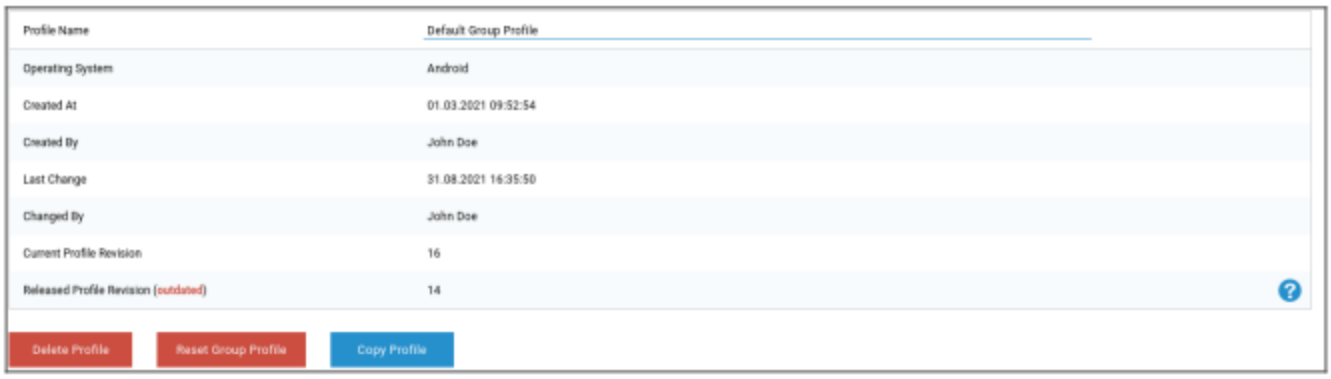
Gateway-basiertes Black- und Whitelisting	Für die Aufnahme in die Schwarze Liste gelten die folgenden Voraussetzungen: • Ein funktionierendes AppTec Universal Gateway ("Allgemeine Einstellungen" → "Universal Gateway") • Eine funktionierende VPN-Konfiguration mit einem angegebenen DNS-Server ("Allgemeine Einstellungen" → "Universal Gateway" → "VPN-Einstellungen") • Eine Blacklist-Konfiguration ("Allgemeine Einstellungen" → "Universal Gateway" → "Domain Blacklist") • Eine gültige VPN-Verbindung im Profil ("Verbindungsverwaltung" → "VPN")

Android-Konfiguration

Allgemein

Gruppenprofilübersicht (nur auf Gruppenebene)

Wenn Sie ein Gruppenprofil öffnen, erhalten Sie einen schnellen Überblick über das Profil.



Profil Name	Name des Profils (kann hier geändert werden)
Betriebssystem	Betriebssystem, für das das Profil bestimmt ist
Erstellt am	Zeitpunkt der Erstellung
Erstellt von	Der Ersteller des Profils
Letzte Änderung	Zeitpunkt der letzten Änderung des Profils
Geändert von	Konto, das die letzten Änderungen vorgenommen hat
Aktuelle Profilüberarbeitung	Revision des gespeicherten Profilstatus
Freigegebene Profil-Revision	Zugewiesene Profilrevision ("Jetzt zuweisen"). Wenn das Etikett hinter dem Text "(veraltet)" anzeigt, bedeutet dies, dass Sie das Profil zwar gespeichert, aber noch nicht zugewiesen haben, so dass die Geräte noch eine ältere Version erhalten.

Geräteübersicht (nur auf Geräteebene)

Sollten Sie sich auf einem Gerät befinden, erhalten Sie eine Übersicht über das gewählte Gerät, die folgendes enthält:

Gerät Name	Name des Geräts
Letzter bekannter Standort	Die letzten bekannten GPS-Koordinaten
Telefon Nummer	Rufnummer
Zugewiesene obligatorische Apps	Die Anzahl der zugewiesenen Pflichtanwendungen
OS Version	OS-Version des Geräts
Betriebssystem	Betriebssystem (Android / iOS / Windows Phone)
Seriennummer	Seriennummer des Geräts
Geräteeigentum	Firmen- oder Privatgerät
Gerätetyp	Telefon oder Tablet
Verwurzelt	Status, der anzeigt, ob das Gerät gerootet wurde
Konform	Konform mit der Richtlinie
IP-Adresse	IP-Adresse
Zuletzt gesehen	Zeitpunkt, zu dem sich das Gerät zuletzt mit AppTec verbunden hat
Letzter Schub	Zeitpunkt, zu dem der Server einen Push an das Gerät gesendet hat
Benutzerzuordnung	Ein Dropdown-Menü, um das Gerät einem anderen Benutzer zuzuweisen

Config Revision (nur auf Geräteebene)

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

Wenn Sie auf das Gruppenprofil klicken, haben Sie direkten Zugriff auf das Profil und können Einstellungen vornehmen.

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

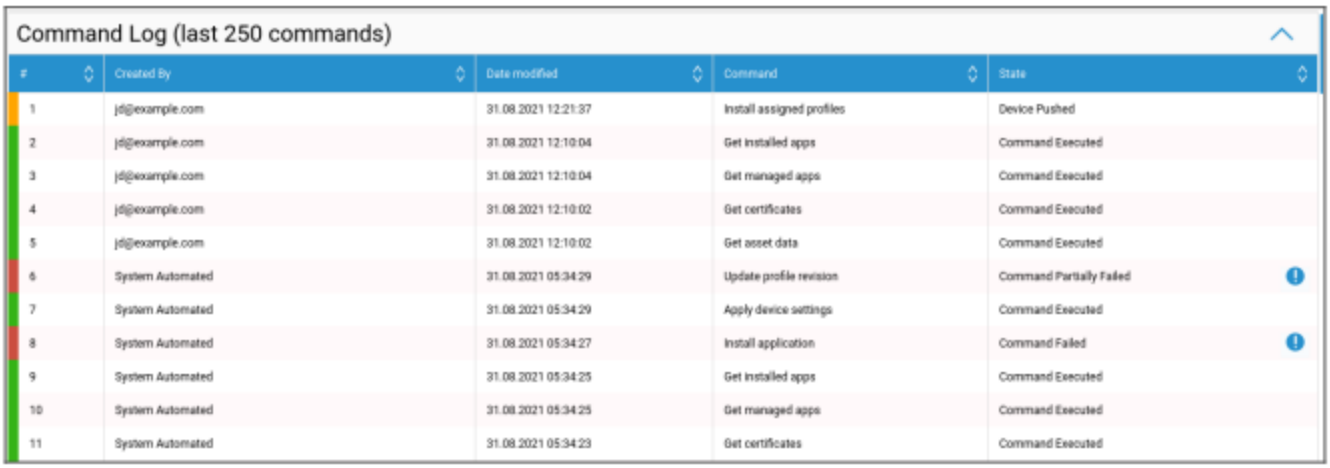
Mit dem Symbol können Sie das Geräteprofil so zurücksetzen, dass es keinerlei Einstellungen enthält.

"Neuere Revision verfügbar" bedeutet, dass das Gruppenprofil geändert und gespeichert, aber nicht zugewiesen wurde. Das Gruppenprofil muss mit "Jetzt zuweisen" auf Gruppenebene zugewiesen werden, um die Änderungen auf die Geräte anzuwenden.

Geräteprotokoll (nur auf Geräteebene)

Befehl Log

Hier können Sie sehen, welche Befehle für das Gerät erteilt wurden und welchen Status sie haben.



Mit "System Automated" erstellte Befehle werden automatisch vom System erstellt.

Mögliche Befehlszustände

Gerät geschoben	Eine Push-Anfrage wurde an den Push-Dienst (z.B. APNS) gesendet, um das Gerät anzuweisen, sich wieder mit dem EMM-Server zu verbinden.
Befehl erstellt	Der Befehl wurde im System erstellt.
Befehl gesendet	Der Befehl wurde an das Gerät gesendet, nachdem es sich mit dem Server verbunden hat.
Befehl Ausgeführt	Der Befehl wurde erfolgreich ausgeführt.
Befehl fehlgeschlagen	Der Befehl ist fehlgeschlagen. *
Befehl Teilweise fehlgeschlagen	Je nach Betriebssystem des Geräts können einige Befehle in Gruppen zusammengefasst werden. Dabei sind einige Teile dieser Befehlsgruppe fehlgeschlagen. *
Befehl ausgeführt, eventuell fehlgeschlagen	Der Befehl wurde ausgeführt, aber vielleicht auch nicht.
Kommando zurückgeschoben	Der Befehl wurde von einem Benutzer erneut gesendet.
Weggeworfen	Der Befehl wurde verworfen. Zum Beispiel, weil er durch einen anderen Befehl ersetzt wurde oder das Gerät neu registriert wurde und alte Befehle entfernt wurden

*Wenn sich hinter der Nachricht ein Ausrufezeichen befindet, erhalten Sie weitere Informationen, indem Sie mit dem Mauszeiger über das Symbol fahren.

Geräteeinstellungen

Client-Konfiguration

Hier können Sie die folgenden Konfigurationen auf Ihrem Android-Gerät vornehmen:

Warnmeldung nach Deaktivierung der Geräteverwaltung	Warnmeldung nach Deaktivierung der Geräteverwaltung erstellt
Zeit der Nichteinhaltung	Zeitlimit, nach dem die "Durchsetzungsmaßnahme nach Einhaltung" durchgeführt wird, wenn das Gerät nicht konform ist. Min. 1 Minute Max. 24 Stunden
Durchsetzungsmaßnahmen nach Ablauf der Einhaltungsfrist	Die Maßnahmen, die zu ergreifen sind, sobald ein Gerät nicht mehr konform ist. • nichts tun = keine Aktion • Gerät sperren = Gerät sperren • Gerät löschen = Das Gerät wird auf die Werkseinstellungen zurückgesetzt.
Häufigkeit der Datenerhebung	Häufigkeit, mit der Geräte-/GPS-Informationen gesammelt werden sollen
Herzschlagfrequenz des Geräts	Intervall, in dem das Gerät den AppTec360 Server kontaktieren soll Min. 1 Minute Max. 24 Stunden
Standortaktualisierungen aktivieren	Wenn aktiviert, sendet das Gerät Standortaktualisierungen an den AppTec360 Server
Standort Aktualisierungszeit	Legt fest, in welchen Zeitabständen das Gerät Standortaktualisierungen an AppTec sendet.
Verwenden Sie Google Location Accuracy für die Standortaktualisierung	Wenn aktiviert, wird die Google-Standortgenauigkeit (früher bekannt als Netzwerkstandort) für Standortaktualisierungen verwendet (wenn dies unter "Einschränkungen" deaktiviert wurde, hat diese Einstellung keine Auswirkungen).
GPS-Standort für Standortaktualisierung verwenden	Falls aktiviert, wird das GPS für Standortaktualisierungen verwendet.

Attraktive (gefälschte) Standorte zulassen	Ermöglicht das Fälschen von Standortinformationen über Apps von Drittanbietern
Aktion "Verlorene Verbindung	Ermöglicht es Ihnen, eine bestimmte Aktion festzulegen, die nach einer bestimmten Anzahl von fehlgeschlagenen Herzschlägen ausgeführt wird
Modus zur Durchsetzung von Richtlinien	Legt fest, wie aggressiv der AppTec360 Client den Benutzer auffordert, bestimmte Aktionen durchzuführen, die eine Benutzereingabe erfordern. Intervall (Standard) = in Intervallen fragen, so dass der Benutzer dies für eine Weile in den Hintergrund stellen kann. Kein Alarm = kein Popup für eine erforderliche Interaktion. Sie müssen den AppTec360 Client manuell öffnen, um zu prüfen, ob eine Aktion erforderlich ist Ständiger Alarm = Der Benutzer kann nur die gewünschte Aktion ausführen. Der AppTec360 Client drängt sich in den Vordergrund, wenn der Benutzer versucht, ihn zu vermeiden
AppTec360 Versionssperre	Hier können Sie eine Version des AppTec360 Clients festlegen, auf die sich der Client maximal aktualisiert.

Tapete

Hier können Sie ein benutzerdefiniertes Hintergrundbild festlegen.

Mit "Farbe angeben" können Sie eine Farbe im Hex-Format definieren (z.B. #000000). Es sind nur Hex-Werte erlaubt.

Mit "Bild als Hintergrundbild festlegen" können Sie ein Bild hochladen. Bitte beachten Sie, dass verschiedene Geräte mit unterschiedlichen Launchern und Betriebssystemversionen unterschiedlich funktionieren. Es gibt keinen allgemeinen Leitfaden für Größe und Verhältnis, da dies vom Gerät abhängt.

Verwenden Sie JPG (oder JPEG) oder PNG als Dateiformat.

Asset Management (nur auf Geräteebene)

Vermögensverwaltung

Geräte-Infos

Modell	**Bezeichnung des Gerätemodells**
Betriebssystem	OS
OS Version	OS-Version
AE-Unterstützung	Unterstützung für Android Enterprise (Container und vollständig verwaltet)
Seriennummer	Seriennummer
Gerät Name	Name des Geräts
Akku-Status	Status der Batterie
Freier / Gesamter Speicher	Freier / Gesamter Speicher
Samsung KNOX	Samsung KNOX API Level
SD-Karte verfügbar	SD-Karte verfügbar
Emulierte SD-Karte	SD-Karte emuliert
SD-Karte herausnehmbar	SD-Karte herausnehmbar
SD Freier / Gesamter Speicher	SD Freier / Gesamter SD-Kartenspeicher

Wi-Fi

IP-Adresse	IP-Adresse des Geräts
WiFi MAC	WiFi MAC-Adresse

Zellulär

Status	Status (SIM-Karte installiert)
Telefon Nummer	Telefon Nummer
Roaming (Sprache/Daten)	Roaming für Sprache/Daten
Roaming-Status	Aktueller Roaming-Status
IP-Adresse	IP-Adresse
Betreiber/Transporteur	Betreiber/Transporteur
Zellulare Technologie	Zellulare Technologie
IMEI	IMEI-Nummer
ICCID	Dies ist die ID für die SIM-Karte, oft auch eine Smartcard oder Integrated Circuit Card (ICC)
IMSI	Die International Mobile Subscriber Identity (IMSI) bietet in GSM- und UMTS-Mobilfunknetzen eine eindeutige Identifizierung der Netznutzer Die IMSI besteht aus maximal 15 Ziffern und wird auf folgende Weise konfiguriert: • Mobiler Ländercode (MCC), 3-stellig • Mobile Network Code (MNC), 2 oder 3 Ziffern • Mobile Subscriber Identification Number (MSIN), 1-10 Ziffern
Aktuelle MCC/MNC	Siehe "SIM MCC/MNC".
SIM MCC/MNC	Der Mobile Country Code ist eine etablierte Länderkennung, die von der ITU gemäß E.212 festgelegt wurde. Standard. Dieser funktioniert in Verbindung mit dem Mobile Network Code (MNC) zur Identifizierung des Mobilfunknetzes. Bedeutet den Länder-/Mobilfunknetzcode der SIM-Karte. Wenn Sie in ein anderes Mobilfunknetz roamen, sind die "Aktuelle MCC/MNC" und die "SIM MCC/MNC" logischerweise unterschiedlich.

Bluetooth

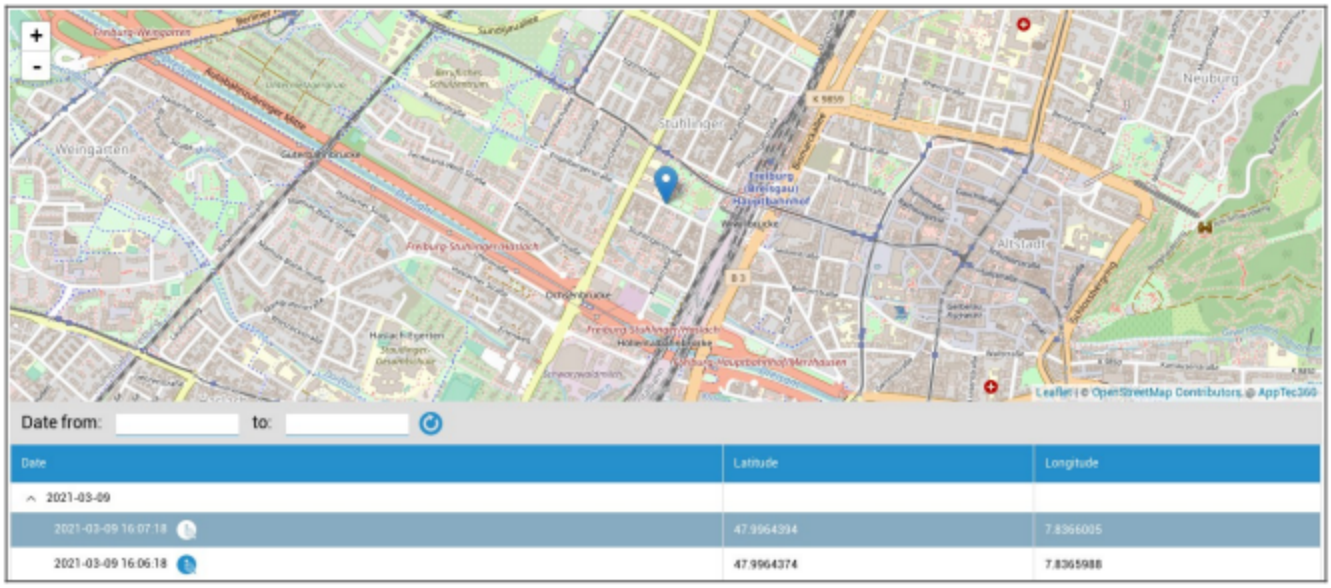
Bluetooth MAC	Bluetooth MAC-Adresse

Sicherheitsmanagement

Anti-Diebstahl (nur auf Geräteebene)

GPS-Informationen (nur auf Geräteebene)

Hier können Sie den aktuellen/letzten Standort des Geräts festlegen. Die Lokalisierung kann mit einem oder sogar zwei Passwörtern geschützt werden - Siehe: Allgemeine Einstellungen - Datenschutz - GPS-Zugang



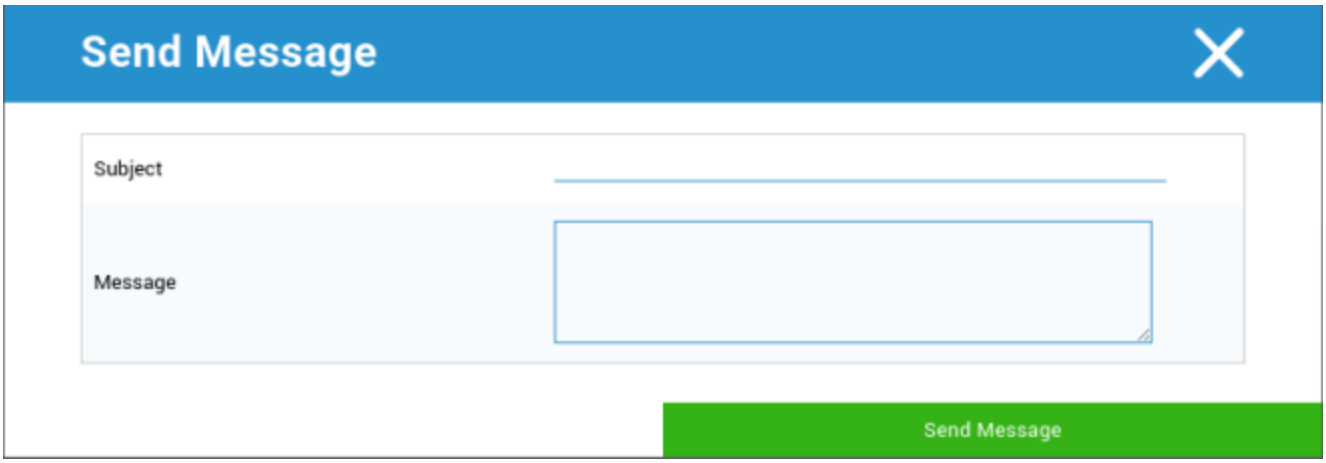
Wischen & Sperren (nur auf Geräteebene)

Unter "Wischen & Sperren" können Sie die folgenden drei Aktionen durchführen:

Vollständig abwischen	Das Gerät wird auf die Werkseinstellungen zurückgesetzt (Unternehmens- und persönliche Daten werden gelöscht)
Enterprise Wipe	Nur Unternehmensdaten werden vom Endbenutzergerät entfernt (alle Apps, Daten usw., die von AppTec360 bereitgestellt wurden)
Sperrbildschirm	Wenn die Bildschirmsperre aktiviert ist, reicht es aus, das Gerät mit dem Geräte-Passwort/PIN zu entsperren

Nachricht (nur auf Geräteebene)

Sie können den Betreff und eine Nachricht eingeben und diese an ein Endgerät senden. Diese Meldung wird im AppTec360 Client angezeigt.



Sicherheitskonfiguration

Passcode

Unter "Passcode" können Sie ein Gerätepasswort vergeben. Folgende Einstellungsmöglichkeiten stehen Ihnen zur Verfügung

Minimale Passwortlänge	Legt fest, wie viele Symbole ein Passwort mindestens enthalten muss
Passwort Qualität	Passwortstärke Nicht spezifiziert = nicht spezifiziert Jedes Passwort ist in Ordnung = jedes Passwort ist akzeptabel mindestens numerische Zeichen = muss mindestens numerische Zeichen enthalten mindestens komplexe Zeichen = muss mindestens Sonderzeichen enthalten mindestens alphanumerische Zeichen = muss mindestens alphanumerische Zeichen enthalten mindestens alphabetische Zeichen = muss mindestens alphabetische Zeichen enthalten
Sperre für maximale Inaktivitätszeit	Maximale Bildschirmzeitüberschreitung. Dies konfiguriert nur den maximalen Wert, der vom Benutzer ausgewählt werden kann
Mindestens Kleinbuchstaben im Passwort erforderlich	Mindestens Kleinbuchstaben im Passwort erforderlich
Mindestens Großbuchstaben im Passwort erforderlich	Mindestens Großbuchstaben im Passwort erforderlich
Mindestens erforderliche Nicht-Buchstaben-Zeichen im Passwort	Mindestens erforderliche Nicht-Buchstaben-Zeichen im Passwort
Mindestens erforderliche numerische Ziffern im Passwort	Mindestens erforderliche numerische Ziffern im Passwort
Mindestens erforderliche Symbole im Passwort	Mindestens erforderliche Symbole im Passwort
Zeitlimit für den Ablauf des Passworts	Legt fest, nach welchem Zeitintervall das Passwort abläuft und ein neues Passwort vergeben werden muss
Einschränkung des Passwortverlaufs	Anzahl der zuvor verwendeten Passwörter, die nicht erlaubt sind
Maximale Anzahl fehlgeschlagener Passwortversuche	Legt fest, wie oft ein Passwort falsch eingegeben werden kann, bevor ein komplettes Löschen des Geräts durchgeführt wird.

Verschlüsselung

Unter diesem Punkt können Sie sowohl den internen Gerätespeicher als auch den Speicher der SD-Karte verschlüsseln.

Verschlüsselung des Speichers verlangen	Wenn diese Einstellung aktiviert ist, wird der Gerätespeicher verschlüsselt, sofern das Gerät diese Funktion unterstützt. Sobald der Gerätespeicher zum ersten Mal verschlüsselt wurde, ist es nicht mehr möglich, ihn zu entschlüsseln. Ebenso wird die Passwortrichtlinie automatisch auf 6 alphanumerische Symbole umgestellt
Verschlüsselung der SD-Karte erforderlich	Diese Einstellung gilt nur für Samsung-Geräte! Wenn diese Einstellung aktiviert ist, kann die externe SD-Karte verschlüsselt werden und kann nur manuell auf dem Endgerät des Benutzers entschlüsselt werden. Ebenso wird die Passwortrichtlinie automatisch auf 6 alphanumerische Symbole umgestellt

AntiVirus

Wenn Sie AntiVirus aktivieren, wird Ikarus auf den Geräten installiert. Bitte beachten Sie, dass hierfür eine separate Lizenz erforderlich ist, die Sie unter Allgemeine Einstellungen → App-Verwaltung → Apps von Drittanbietern eingeben können.

Automatischer Scan	Legt fest, ob Ikarus automatisch scannt oder nicht und wie oft es diesen Scan durchführt Wenn Sie "Vollständiger automatischer Scan" aktivieren, wird ein vollständiger Scan durchgeführt. Andernfalls wird eine Schnellsuche durchgeführt
Automatische Updates	Aktiviert die automatische Aktualisierung der Virendatenbank und legt fest, wie oft dies geschieht
App-Schutz	Aktiviert den Scan von Apps zusätzlich zum regulären Scan, der nur Dateien scannt
SD-Karten Schutz	Aktiviert den SD-Kartenschutz. Ohne diese Option ist der Scan auf den lokalen Speicher beschränkt.
Nur Wi-Fi Update	Begrenzt Update auf Wi-Fi

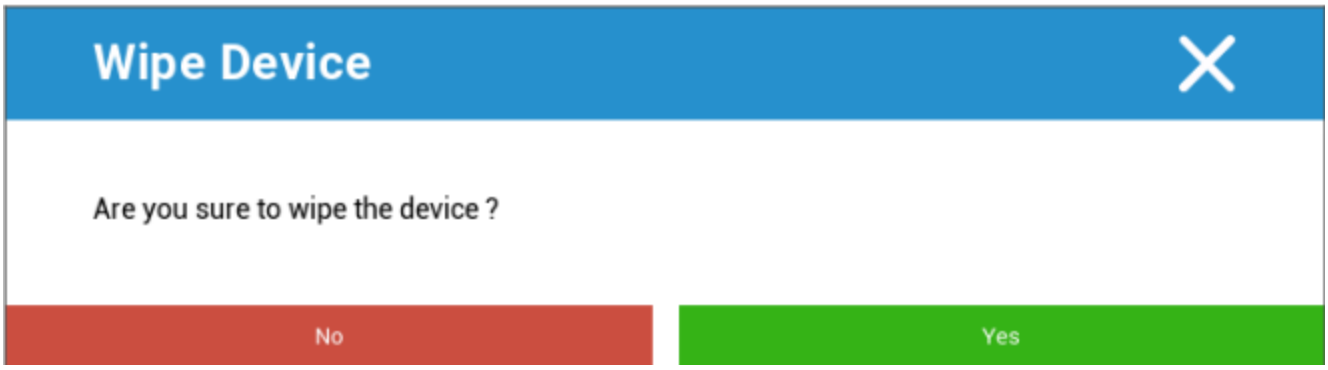
Ende der Lebensdauer (nur auf Geräteebene)

Wischen (nur auf Geräteebene)

Unter "Löschen" können Sie das Gerät auf seine Werkseinstellungen zurücksetzen. Hier werden sowohl die Unternehmensdaten als auch die privaten Daten auf dem Endgerät des Benutzers gelöscht.

Mit einem Klick auf das "Minus-Symbol" sollten Sie die folgende Meldung erhalten

SD-Karte auch löschen?	Der SD-Kartenspeicher wird ebenfalls gelöscht



Mit "Ja" können Sie die Löschung durchführen.

Unter "Wischbericht" können die folgenden Punkte angezeigt werden

Abgewischt von	Historie der Person, die den Wisch durchgeführt hat
Datum	Datum
Status	Status (z.B. ob der Löschvorgang erfolgreich durchgeführt wurde)

Einstellungen zur Einschränkung

Beschränkungen

Hier kann eine Vielzahl von Dingen eingeschränkt und blockiert werden.

Kamera einschalten	Verwendung der Kamera zulassen
Auto-Synchronisation erzwingen	Bezieht sich auf die Schnittstelle "Sync". Ein = die Synchronisierung ist permanent aktiviert Aus = die Synchronisierung ist dauerhaft deaktiviert Benutzerauswahl = vom Benutzer ausgewählt
Bluetooth erzwingen	Ein = Bluetooth ist permanent aktiviert Aus = Bluetooth ist dauerhaft deaktiviert Benutzerauswahl = vom Benutzer ausgewählt
GPS erzwingen	Ein = GPS ist permanent aktiviert Aus = GPS ist dauerhaft deaktiviert Benutzerauswahl = vom Benutzer ausgewählt
Erzwingen Sie die Google-Standortgenauigkeit	Ein = Permanente Internet-Lokalisierung Aus = Dauerhafte Deaktivierung der Internet-Lokalisierung Benutzerauswahl = vom Benutzer ausgewählt

Für Samsung-Geräte mit der Schnittstelle KNOX 1.0 oder höher stehen Ihnen die folgenden Einstellungsmöglichkeiten zur Verfügung.

SD-Karte zulassen	SD-Karte zulassen
Schreiben auf SD-Karte zulassen	Schreiben" auf der SD-Karte zulassen
Bildschirmaufzeichnung zulassen	Bildschirmaufnahme zulassen
Zwischenablage zulassen	Zwischenablage zulassen
Einstellungen und Anwendungsdaten in Google Cloud sichern	Aus = Google Backup deaktivieren Ein = Google Backup aktivieren Benutzerauswahl = vom Benutzer ausgewählt
USB-Debugging zulassen	USB-Debugging zulassen (wird z.B. für die Erstellung von Geräteprotokollen (ADB) verwendet)
Google Crash Report zulassen	Erlauben Sie das Versenden von Google Crash Report aus den Apps heraus
Werksreset zulassen	Ermöglicht es dem Benutzer, das Gerät auf seine Werkseinstellungen zurückzusetzen
OTA-Upgrade zulassen	Erlauben Sie "Over-The-Air"-Updates
USB-Host-Speicher zulassen	Wenn aktiviert, kann ein USB-Speicher in Form einer Festplatte oder eines SD-Kartenlesers angeschlossen werden.
USB Media Player zulassen (MTP,PTP)	USB Media Player zulassen (MTP,PTP)
Mikrofon zulassen	Ein = Mikrofon für 3rd Party Apps zulassen Aus = Mikrofon für 3rd Party Apps blockieren User Choice = Benutzer können wählen, ob die 3rd Party App Zugriff auf das Mikrofon hat
NFC (Nahfeldkommunikation) zulassen	NFC zulassen
Unbekannte Quellen zulassen (APK Sideloading)	Wenn diese Option aktiviert ist, ist das Nebenbei-Laden von Apps (APK-Dateien) erlaubt. Sobald diese Einstellung deaktiviert ist, muss der Benutzer sie manuell aktivieren, wenn Sie die Installation von APKs aus unbekannten Quellen wieder zulassen.
Benutzererstellung zulassen	Ermöglicht das Anlegen mehrerer Benutzer

AE Geräteeigentümer

(Das Gerät muss sich im Android Enterprise Device Owner Mode befinden) Es wird empfohlen, die Geräte als "Android Enterprise"-Gerät und nicht als "Android"-Gerät zu erstellen.

Sicherheit	
Freigabeort verbieten	Gibt an, ob ein Benutzer die Standortfreigabe nicht einschalten darf.
Abgesicherten Start nicht zulassen	Gibt an, ob der Benutzer das Gerät nicht in den abgesicherten Bootmodus neu starten darf.
Netzwerk-Reset nicht zulassen	Gibt an, ob ein Benutzer die Netzwerkeinstellungen nicht über die Einstellungen zurücksetzen darf.
Werksreset nicht zulassen	Gibt an, ob ein Benutzer das Gerät nicht zurücksetzen darf.
ADB aktivieren	Ermöglicht die Verbindung mit einem PC über ADB
Schlüsselschutz deaktivieren	Deaktiviert den Schlüsselschutz
Informationen zum Sperrbildschirm des Gerätebesitzers	Legt die Informationen zum Besitzer des Geräts fest, die auf dem Sperrbildschirm angezeigt werden sollen.
Durchsetzung der Compliance	Modus Benutzer auffordern - Der Benutzer wird aufgefordert, die notwendigen Aktionen durchzuführen. Mode Lock-Down Container - Blenden Sie alle Anwendungen aus, bis alle Anforderungen erfüllt sind

App Verwaltung	
Profilübergreifende App-Verknüpfung zulassen	Ermöglicht es Anwendungen im übergeordneten Profil, Weblinks aus dem verwalteten Profil zu verarbeiten.
App-Steuerung verbieten	Legt fest, ob ein Benutzer keine Anwendungen in den Einstellungen oder Launchern ändern darf.
App-Installation verbieten	Gibt an, ob einem Benutzer die Installation von Anwendungen untersagt ist.
Deinstallieren von Apps verbieten	Gibt an, ob ein Benutzer keine Anwendungen deinstallieren darf.
Richtlinie für Laufzeitberechtigungen	Legt fest, wie neue Berechtigungsanfragen von Anwendungen behandelt werden.
Unbekannte Quellen zulassen	Wenn diese Funktion aktiviert ist, können Benutzer Apps durch die Installation einer .apk-Datei sideloaden.

Konnektivität	
Mobile Netzwerkkonfiguration nicht zulassen	Gibt an, ob es einem Benutzer nicht erlaubt ist, mobile Netzwerke zu konfigurieren.
Tethering verbieten Konfig.	Gibt an, ob es einem Benutzer nicht erlaubt ist, Tethering und mobile Hotspots zu konfigurieren.
VPN-Konfiguration verbieten	Gibt an, ob einem Benutzer die Konfiguration eines VPN untersagt ist.
Wifi-Konfiguration verbieten	Gibt an, ob ein Benutzer die WiFi-Zugangspunkte nicht wechseln darf.
Ausgehenden NFC-Strahl verbieten	Legt fest, ob der Benutzer NFC nicht zum Beamen von Daten aus Apps verwenden darf.
WiFi-Konfiguration sperren	Diese Einstellung steuert, ob von einer App des Gerätebesitzers erstellte WiFi-Konfigurationen gesperrt werden sollen (d.h. nur von der App des Gerätebesitzers bearbeitet oder entfernt werden können, nicht einmal von der App Einstellungen).
Daten-Roaming aktivieren	Aktiviert Daten-Roaming

Bluetooth	
Bluetooth deaktivieren	Gibt an, ob Bluetooth auf dem Gerät nicht erlaubt ist. Benötigt Android 8.0
Bluetooth-Freigabe deaktivieren	Gibt an, ob die ausgehende Bluetooth-Freigabe auf dem Gerät nicht erlaubt ist. Benötigt Android 8.0
Bluetooth-Konfiguration nicht zulassen	Gibt an, ob einem Benutzer die Konfiguration von Bluetooth untersagt ist.

Kontoführung	
Hinzufügen eines verwalteten Profils nicht zulassen	Gibt an, ob einem Benutzer das Hinzufügen von verwalteten Profilen untersagt ist. Benötigt Android 8.0
Hinzufügen von Benutzern verbieten	Gibt an, ob einem Benutzer das Hinzufügen neuer Benutzer untersagt ist.
Nicht zulassen Verwaltetes Profil entfernen	Gibt an, ob verwaltete Profile dieses Benutzers entfernt werden können, außer von seinem Profileigentümer. Benötigt Android 8.0
Kontomodifikation verbieten	Gibt an, ob einem Benutzer das Hinzufügen und Entfernen von Konten untersagt ist, es sei denn, sie werden von Authenticator programmatisch hinzugefügt.

Telefonie	
Ausgehende Anrufe verbieten	Legt fest, dass der Benutzer keine ausgehenden Telefonanrufe tätigen darf.
SMS verbieten	Legt fest, dass der Benutzer keine SMS-Nachrichten senden oder empfangen darf.

System	
Fenstererstellung verbieten	Legt fest, dass neben den Anwendungsfenstern keine weiteren Fenster erstellt werden sollen.
Eingestelltes Benutzersymbol nicht zulassen	Gibt an, ob ein Benutzer sein Symbol nicht ändern darf.
Hintergrundbild einstellen verbieten	Benutzerbeschränkung, um das Einstellen eines Hintergrundbildes zu verbieten.
Statusleiste deaktivieren	Die Deaktivierung der Statusleiste blockiert Benachrichtigungen, Schnelleinstellungen und andere Bildschirmüberlagerungen, die das Verlassen eines Einweggeräts ermöglichen.
Auto Zeit aktivieren	Stellt die Uhrzeit automatisch ein.
Automatische Zeitzone aktivieren	Stellt die Zeitzone automatisch ein.
Bleibt eingeschaltet, wenn der Stecker eingesteckt ist	Das Gerät bleibt aktiv, solange es an eine Stromquelle angeschlossen ist.

Lagerung	
Deaktivieren Sie die App-Verifizierung	Gibt an, ob ein Benutzer die Anwendungsüberprüfung nicht deaktivieren darf.
Einhängen physischer Medien verbieten	Gibt an, ob es einem Benutzer nicht erlaubt ist, physische externe Medien einzuhängen.
Sicherungsdienst aktivieren	Der Backup-Dienst verwaltet alle Sicherungs- und Wiederherstellungsmechanismen auf dem Gerät. Wenn Sie diesen Wert auf false setzen, werden die Daten nicht gesichert oder wiederhergestellt. Der Backup-Dienst ist standardmäßig deaktiviert. Benötigt Android 8.0
Aktivieren Sie den USB-Massenspeicher	Ermöglicht die Verwendung des USB-Massenspeichers.

Tastatur	
Autofill deaktivieren	Gibt an, ob ein Benutzer die Autofill Services nicht verwenden darf. Benötigt Android 8.0
Kopieren und Einfügen zwischen Profilen verbieten	Gibt an, ob das, was in die Zwischenablage dieses Profils kopiert wird, in verwandte Profile eingefügt werden kann.

Ton	
Volumenanpassung nicht zulassen	Gibt an, ob ein Benutzer die Master-Lautstärke nicht verändern darf.
Mikrofon stummschalten nicht zulassen	Legt fest, ob ein Benutzer die Mikrofonlautstärke nicht verändern darf.
Gerät stummschalten	Gerät stummschalten.

System-Update-Richtlinie	
OS-Updates kontrollieren	Aktivieren Sie diese Option, um das Aktualisierungsverhalten auf automatisch, in einem Fenster oder zeitversetzt einzustellen.

BYOD Container

Android Unternehmen

Android Unternehmen

Android Enterprise aktivieren	Aktivieren Sie Android Enterprise (AE). AE wird ab Android 5.1 und höher unterstützt.
Durchsetzung der Compliance	Modus Benutzer auffordern - Der Benutzer wird aufgefordert, die notwendigen Aktionen durchzuführen. Mode Lock-Down Container - Blenden Sie alle Anwendungen aus, bis alle Anforderungen erfüllt sind
Richtlinie für Laufzeitberechtigungen	Aufforderung an den Benutzer für neue Berechtigungsanfragen Neue Genehmigungsanfragen immer gewähren Neue Genehmigungsanfragen immer ablehnen Warnung: Einige Apps haben Probleme, die Berechtigungen zu erkennen, wenn diese automatisch eingestellt sind. Wenn Sie immer Berechtigungen erteilen und Probleme mit Apps auftreten, die behaupten, dass Berechtigungen fehlen, setzen Sie dies auf "Benutzer auffordern" und installieren Sie die App neu.
Ausgehende Zwischenablage zulassen	Ermöglicht das Kopieren und Einfügen aus dem Inneren des Containers nach außen
Auflösung der Anrufer-ID zulassen	Zeigt den Namen für einen eingehenden Anruf basierend auf den Kontakten im Container an
Auflösung der Kontaktsuche zulassen	Ermöglicht die Suche nach Namen in den Containerkontakten bei Anrufen
Bluetooth-Kontaktfreigabe zulassen	Ermöglicht den Zugriff auf den Containerkontakt in einem Auto
Ausgehenden NFC-Strahl verbieten	Deaktiviert NFC für den Container
Unbekannte Quellen zulassen	Wenn diese Funktion aktiviert ist, können Benutzer Apps durch die Installation einer .apk-Datei sideloaden.
USB-Debugging zulassen	Wenn diese Option aktiviert ist, können Sie das USB-Debugging aktivieren.
Kontomodifikation verbieten	Verbietet die Erstellung, Löschung und Änderung von Konten im Container

	Beachten Sie, dass einige Anwendungen Konten erstellen oder ändern müssen, damit sie wie erwartet funktionieren.

Google Mail Austausch

Ermöglicht Ihnen die Konfiguration von Google Mail im Container. Bitte beachten Sie, dass die Aktivierung dieser Konfiguration nicht automatisch zur Installation der App führt. Sie müssen diese App noch als Pflichtanwendung hinzufügen.

E-Mail Adresse	E-Mail Adresse
Server-Hostname	Server-Hostname
Login-Name	Login-Name
Unterschrift	Unterschrift
Anzahl der zu synchronisierenden Vortage	Anzahl der zu synchronisierenden Vortage.
Geräte-Identifikator	EAS Identifier. Lassen Sie dies leer, wenn Ihre Umgebung dies nicht erfordert
Verwenden Sie Secure Sockets Layer (SSL)	Aktiviert die Verwendung von SSL. Die Deaktivierung dieser Funktion kann die Sicherheit verringern
Alle Zertifikate akzeptieren	Akzeptiert alle Zertifikate. Die Aktivierung dieser Funktion kann die Sicherheit verringern
Nicht verwaltete Konten zulassen	Ermöglicht es dem Benutzer, weitere Konten hinzuzufügen
Kundenzertifikat	Laden Sie das Client-Zertifikat hoch, wenn Ihr Exchange-Server dies erfordert

AE System Apps

Hier können Sie System-Apps für den Android Enterprise Container aktivieren. Bitte beachten Sie, dass sich die angegebene App im Speicher des Systems befinden muss, sonst passiert nichts.

Container Passcode

Nur für Android 7.0 oder höher

Ermöglicht es Ihnen, ein bestimmtes Passwort für den Container festzulegen.

Minimale Passwortlänge	Legt fest, wie viele Symbole ein Passwort mindestens enthalten muss
Passwort Qualität	Passwortstärke Nicht spezifiziert = nicht spezifiziert Jedes Passwort ist in Ordnung = jedes Passwort ist akzeptabel mindestens numerische Zeichen = muss mindestens numerische Zeichen enthalten mindestens komplexe Zeichen = muss mindestens Sonderzeichen enthalten mindestens alphanumerische Zeichen = muss mindestens alphanumerische Zeichen enthalten mindestens alphabetische Zeichen = muss mindestens alphabetische Zeichen enthalten
Sperre für maximale Inaktivitätszeit	Maximale Zeit, bis der Container gesperrt wird. Dies konfiguriert nur den maximalen Wert, der vom Benutzer ausgewählt werden kann
Mindestens Kleinbuchstaben im Passwort erforderlich	Mindestens Kleinbuchstaben im Passwort erforderlich
Mindestens Großbuchstaben im Passwort erforderlich	Mindestens Großbuchstaben im Passwort erforderlich
Mindestens erforderliche Nicht-Buchstaben-Zeichen im Passwort	Mindestens erforderliche Nicht-Buchstaben-Zeichen im Passwort
Mindestens erforderliche numerische Ziffern im Passwort	Mindestens erforderliche numerische Ziffern im Passwort
Mindestens erforderliche Symbole im Passwort	Mindestens erforderliche Symbole im Passwort
Zeitlimit für den Ablauf des Passworts	Legt fest, nach welchem Zeitintervall das Passwort abläuft und ein neues Passwort vergeben werden muss
Einschränkung des Passwortverlaufs	Anzahl der zuvor verwendeten Passwörter, die nicht erlaubt sind
Maximale Anzahl fehlgeschlagener Passwortversuche	Legt fest, wie oft ein Passwort falsch eingegeben werden kann, bevor der Container gelöscht wird

Samsung KNOX

Aktivierung

Hier können Sie den Samsung KNOX Container aktivieren. Bitte beachten Sie, dass dies von Samsung unter Android 10 oder höher nicht mehr unterstützt wird. Verwenden Sie den Android Enterprise Container unter Android 10 oder höher

Knox Passcode

Legen Sie die Richtlinien fest, die sich auf die Einstellungen des Gerätepassworts beziehen

Minimale Passwortlänge	Legt fest, wie viele Symbole das Passwort haben muss
Passwort Qualität	Passwortstärke Jedes Passwort ist in Ordnung = Jedes Passwort ist in Ordnung Mindestens numerische Zeichen = Mindestens numerische Zeichen müssen vorhanden sein Mindestens komplexe Zeichen = Mindestens Sonderzeichen müssen vorhanden sein Mindestens alphanumerische Zeichen = Mindestens alphanumerische Zeichen müssen vorhanden sein Mindestens alphabetische Zeichen = Mindestens alphabetische Zeichen müssen vorhanden sein
Mindestens komplexe Zeichen erforderlich	Es müssen mindestens komplexe Zeichen vorhanden sein
Maximale Zeitüberschreitung bei Inaktivität	Maximale Zeitspanne der Inaktivität des Benutzers, bevor die Tastatur gesperrt wird
Fingerabdruck-Authentifizierung zulassen	Fingerabdruck-Authentifizierung zulassen
Iris-Authentifizierung zulassen	Erlauben Sie die Authentifizierung per Iriserkennung
Maximales Passwort Alter	Legt fest, nach welcher Zeit das Passwort abläuft und ein neues Passwort vergeben werden muss
Gespeicherter Passwortverlauf	Anzahl ehemaliger Passwörter, die nicht erlaubt sind
Maximale Anzahl fehlgeschlagener Passwortversuche	Legt fest, wie oft das Passwort falsch eingegeben werden darf, bevor ein komplettes Löschen des Geräts durchgeführt wird.

Knox Sicherheit

Beschränken Sie bestimmte Gerätefunktionalitäten

Kamera einschalten	Erlauben Sie die Verwendung der Kamera

Samsung KNOX App Store zulassen	Erlauben Sie die Nutzung des Samsung KNOX App Store
Google Play Dienste zulassen	Google Play Dienste zulassen
Browser zulassen	Erlauben Sie die Verwendung des nativen Browsers
Screenshots zulassen	Erlauben Sie die Erstellung von Screenshots
Kontaktimport zulassen	Wenn aktiviert, ist der Zugriff auf Gerätekontakte aus dem KNOX Container erlaubt
Kontaktexport zulassen	Wenn aktiviert, ist der Zugriff auf die KNOX Kontakte vom Gerät aus erlaubt
Kalenderimport zulassen	Wenn aktiviert, ist der Zugriff auf den Gerätekalender aus dem KNOX Container erlaubt
Kalenderexport zulassen	Wenn aktiviert, ist der Zugriff auf den KNOX-Kalender vom Gerät aus erlaubt
Nicht sicheres Tastenfeld zulassen	Erlauben Sie die Verwendung eines nicht sicheren Keypads
Datei-Import aktivieren	Aktivieren Sie den Datei-Import in den KNOX Container
Aktivieren Sie den Dateiexport	Aktivieren Sie den Dateiexport aus dem KNOX Container

Knox Börse

Hier können Sie das Exchange-Profil für den KNOX Container konfigurieren

eMail-Adresse	Die angegebene E-Mail-Adresse des Benutzers Bitte beachten Sie die "Platzhalter", die Sie für die Arbeit mit Anmeldeinformationen verwenden können und die Sie nicht auf jedem Gerät manuell ändern müssen Mit einem Klick auf **Platzhalter anzeigen** können Sie sich diese anzeigen lassen
Server-Hostname	Serveradresse Ihres Exchange Servers
Login-Name	Der Login-Name für das jeweilige Endgerät, bitte beachten Sie hier auch die "Platzhalter".
Domain	Domänenadresse
Passwort (nur auf Geräteebene)	Optional kann ein einzelnes Gerät mit einem Passwort versehen werden. Sollte dieses leer bleiben, wird der Benutzer aufgefordert, sein Exchange-Passwort einzugeben.
Anzahl der zu synchronisierenden Vortage	Anzahl der Tage, die bestimmen, wann die E-Mails wieder synchronisiert werden
Unterschrift	Eine Signatur kann beigefügt werden
Standard-Konto	Legt fest, dass dieses E-Mail-Konto das Standardkonto ist
Verwenden Sie Secure Sockets Layer (SSL)	Verwenden Sie eine SSL-Verbindung
Verwenden Sie Transport Layer Security (TLS)	Verwenden Sie eine TLS-Verbindung
Alle Zertifikate akzeptieren	Alle Zertifikate werden akzeptiert. Bitte wählen Sie diese Option, wenn Ihr Exchange Server ein selbstsigniertes Zertifikat verwendet

Knox eMail

eMail-Adresse	Die angegebene E-Mail-Adresse des Benutzers Bitte beachten Sie die "Platzhalter", die Sie für die Arbeit mit Anmeldeinformationen verwenden können und die Sie nicht auf jedem Gerät manuell ändern müssen Mit einem Klick auf **Platzhalter anzeigen** können Sie sich diese anzeigen lassen
Protokoll des eingehenden Servers	Protokoll des eingehenden Servers IMAP oder POP
Adresse des eingehenden Servers	Adresse des eingehenden Servers
Port des eingehenden Servers	Port des eingehenden Servers
Login/Benutzername des Eingangsservers	Login/Benutzername des Eingangsservers
Passwort für den Posteingangsserver	Passwort für den Posteingangsserver
Eingehender Server verwendet SSL	Eingehender Server verwendet SSL
Eingehender Server verwendet TLS	Eingehender Server verwendet TLS
Eingehender Server akzeptiert alle Zertifikate	Eingehende Server akzeptieren alle Arten von Zertifikaten
Protokoll des ausgehenden Servers	Protokoll des ausgehenden Servers SMTP
Port des ausgehenden Servers	Port des ausgehenden Servers
Ausgehender Server verwendet zusätzliche Anmeldeinformationen	Zusätzliche Anmeldeinformationen für den ausgehenden Server. Wenn dies auf "off" gesetzt ist, werden die Einstellungen des Eingangsservers verwendet.
Anmeldung/Benutzername des Ausgangsservers	Anmeldung/Benutzername des Ausgangsservers
Passwort des Ausgangsservers	Passwort des Ausgangsservers
Ausgehender Server verwendet SSL	Ausgehender Server verwendet SSL
Ausgehender Server verwendet TLS	Ausgehender Server verwendet TLS
Ausgehender Server akzeptiert alle Zertifikate	Ausgehende Server akzeptieren alle Arten von Zertifikaten
Unterschrift	Hier kann eine Signatur angehängt werden

Benutzer bei Erhalt einer neuen eMail benachrichtigen	Benutzer bei Erhalt einer neuen eMail benachrichtigen

Knox Apps

Legen Sie hier die Anwendungen fest, die Sie an die Endbenutzergeräte verteilen möchten. Diese werden dann im KNOX-Container verfügbar sein. Um eine App hinzuzufügen, gehen Sie bitte wie im Menü Obligatorische Apps vor

Anwendung Name	Anwendung Name
Obligatorisch seit	Zeitpunkt, an dem die App hinzugefügt wurde
Quelle	Quelle der App (Play Store | In-House)

Durch Klicken auf das Symbol kann die jeweilige App wieder entfernt werden

Verbindungsmanagement

Wifi

Führen Sie für diese Einstellung die Vorkonfiguration der Endbenutzergeräte für den Zugriff auf interne Access Points durch

Services Set Identifier (SSID)	SSID für das Netzwerk, mit dem eine Verbindung hergestellt werden soll
Verborgenes Netzwerk	Aktivieren, für den Fall, dass der AP die SSID nicht sendet
Sicherheit Typ	Legen Sie den Sicherheitstyp des APs fest

Sicherheit Typ

WEP

Passwort	Passwort für den AP

WPA/WPA2

Passwort	Passwort für den AP

802.1x EAP

EAP-Methode	

PWD	Identität	Identität
	Passwort	Passwort

PEAP	Phase 2 Authentifizierungsprotokoll	keine	Kein zusätzliches Protokoll
		MSCHAPV2	MSCHAPV2-Protokoll
		GTC	GTC-Protokoll
	CA-Zertifikat	CA-Zertifikat	
	Identität	Identität	
	Anonyme Identität	Anonyme Identität	
	Passwort	Passwort	

EAP-Methode	

TTLS	Phase 2 Authentifizierungsprotokoll	keine	Kein zusätzliches Protokoll
		PAP	PAP-Protokoll
		MSCHAP	MSCHAP-Protokoll
		MSCHAPV2	MSCHAPV2-Protokoll
		GTC	GTC-Protokoll
	CA-Zertifikat	CA-Zertifikat	
	Identität	Identität	
	Anonyme Identität	Anonyme Identität	
	Passwort	Passwort	

TLS	CA-Zertifikat	CA-Zertifikat
	Identität	Identität
	Passwort	Passwort

VPN

Verbindungstyp	**VPN-Verbindungstyp einrichten**

Wenn Sie "Per-App VPN" als VPN-Typ auswählen, ändern sich die verfügbaren VPN-Clients. Per-App VPN beschränkt das VPN auf bestimmte Apps und startet die VPN-Verbindung automatisch, wenn eine bestimmte App gestartet wird.

AppTec360 VPN-Client	Verwendet den AppTec360 VPN Client in Kombination mit dem Universal Gateway
Name der Verbindung	Name der VPN-Verbindung
Gateway-Konfiguration	Wählen Sie die VPN-Konfiguration des Universal Gateway
Immer eingeschaltetes VPN	Erzwingt, dass das VPN immer aktiv ist, so dass der gesamte Datenverkehr über das VPN läuft.
Native Abriegelung aktivieren	Blockiert alle Netzwerke, wenn das Gerät nicht mit dem VPN verbunden ist. Verwenden Sie diese Option mit Bedacht, da sie bei falscher Konfiguration zu einem vollständigen Verbindungsabbruch führen kann. Nur für Android Enterprise unter Android 7 oder höher
AppTec360 Lockdown aktivieren	Sperrt die Nutzung aller Apps, bis die VPN-Verbindung gestartet ist

Cisco AnyConnect	
Name der Verbindung	Name der VPN-Verbindung
Server	Server Adresse
Zertifikat-Modus	Deaktiviert = Deaktiviert Automatisch = automatisch

L2TP (nur KNOX)	Nur auf Samsung-Geräten verfügbar
Name der Verbindung	Name der Verbindung
Server	Server Adresse
L2TP-Geheimnis aktivieren	
DNS-Suchdomänen	DNS-Suchdomänen

Verbindungstyp	**VPN-Verbindungstyp einrichten**

PPTP (nur KNOX)	Nur auf Samsung-Geräten verfügbar
Name der Verbindung	Name der VPN-Verbindung
Server	Server Adresse
Verschlüsselung einschalten	Aktivieren Sie die Verschlüsselung
DNS-Suchdomänen	DNS-Suchdomänen

L2TP / IPSec PSK (nur KNOX)	Nur auf Samsung-Geräten verfügbar
Name der Verbindung	Name der VPN-Verbindung
Server	Server Adresse
IPSec Pre-Shared Key	Pre-shared Key für die Authentifizierung
L2TP-Geheimnis aktivieren	
L2TP Geheimnis	
DNS-Suchdomänen	DNS-Suchdomänen

IPSec XAuth PSK (nur KNOX)	Nur auf Samsung-Geräten verfügbar
Name der Verbindung	Name der VPN-Verbindung
Server	Server Adresse
IPSec-Bezeichner	Nutzername für die Verbindung
IPSec Pre-Shared Key	Passwort für die Verbindung
DNS-Suchdomänen	DNS-Suchdomänen

OpenVPN	

Name der Verbindung	Name der Verbindung
OpenVPN-Profil	Hier wird der Inhalt der .ovpn-Datei kopiert
OpenVPN-App	Es gibt zwei verschiedene Apps für die Verwendung von OpenVPN Wir empfehlen die App "OpenVPN für Android". Alternativ kann auch die App "OpenVPN Connect" verwendet werden

Beschränkungen

Hier können Sie die Einschränkungen in Bezug auf die Verbindungsverwaltung festlegen.

Daten-Roaming zulassen	Mobile Daten beim Roaming zulassen
Daten-Roaming erzwingen	Falls aktiviert, ist das Roaming für mobile Daten dauerhaft aktiviert (nicht empfohlen!) Diese Einstellung überschreibt die Einstellung "Datenroaming zulassen"!
Die folgenden Einstellungen sind nur bei Samsung KNOX 2.0 oder höher verfügbar	
Nur Notrufe zulassen	Nur Notrufe zulassen
WiFi zulassen	WiFi zulassen
WiFi Netzwerk Mindest-Sicherheitsstufe	Minimale Sicherheitsstufe des WiFi-Netzwerks Offen = alle Arten von WiFi sind erlaubt
Verbieten Sie dem Benutzer, WiFi-Netzwerke hinzuzufügen	Der Benutzer kann nicht selbst ein WiFi-Netzwerk hinzufügen Diese Einstellung ist nur möglich, wenn unter "Verbindungsverwaltung" ein WiFi-Profil definiert wurde.
SMS & MMS zulassen	Alle = Der gesamte SMS- und MMS-Verkehr ist erlaubt Nur eingehende SMS = Nur eingehende SMS-Nachrichten sind erlaubt Nur ausgehende SMS = Nur ausgehende SMS-Nachrichten sind erlaubt Keine = Kein SMS / MMS-Verkehr ist erlaubt
Synchronisierung beim Roaming zulassen	Synchronisierung beim Roaming zulassen Ein = aktiviert Aus = Deaktiviert Wahl des Benutzers = Wahl des Benutzers
Sprachroaming zulassen	Sprachroaming zulassen Ein = aktiviert Aus = Deaktiviert User Choice = die Wahl des Benutzers
System http Proxy Server verwenden	Die Verwendung eines HTTP-Proxyservers, der von den Systemeinstellungen in den Einstellungen bereitgestellt wird, ist abhängig vom verbundenen Netzwerk (WiFi oder APN)

APN

Die folgenden Einstellungen sind nur auf Samsung SAFE 2.0 oder höher verfügbar!

APN-Anzeigename	APN-Anzeigename	
Name des Zugangspunkts	Name des APN	
Protokoll des ausgehenden Servers	Nicht festgelegt	
	Keine	
	PAP	PAP-Protokoll
	CHAP	CHAP-Protokoll
	PAP oder CHAP	Entweder das PAP- oder das CHAP-Protokoll
MCC - Mobiler Ländercode	Hier wird die MCC eingegeben. Lassen Sie dieses Feld leer, wenn die MCC der eingelegten SIM-Karte verwendet werden soll.	
MNC - Mobile Network Code	Hier wird der MNC eingegeben. Lassen Sie dieses Feld leer, wenn der MCC der eingelegten SIM-Karte verwendet werden soll.	
Server Adresse	Server Adresse	
Server-Portnummer	Server-Portnummer	
Server-Proxy-Adresse	Server-Proxy-Adresse	
MMS-Server-Adresse	MMS-Serveradresse, für Standard bitte leer lassen	
MMS-Anschlussnummer	MMS-Anschlussnummer	
MMS-Proxy-Adresse	MMS-Proxy-Adresse	
Name des Benutzers	Name des Benutzers	
Passwort	Passwort	
Zugangspunkt-Typ	Erlaubte Typen sind: "Standard", "mms", "supl" Wenn dieses Feld leer gelassen wird, wird "default,supl,mms" verwendet.	
Bevorzugter APN	APN wird bevorzugt	

Bluetooth

Hier können Sie eine Vielzahl von Bluetooth-Einstellungen vornehmen.

Die folgenden Einstellungen sind nur bei Samsung KNOX 1.0 oder höher verfügbar!

Geräteerkennung über Bluetooth zulassen	Geräteerkennung über Bluetooth zulassen
Bluetooth-Kopplung zulassen	Bluetooth-Kopplung zulassen
Bluetooth-Headset-Geräte zulassen	Bluetooth-Headset-Geräte zulassen
Bluetooth-Freisprecheinrichtungen zulassen	Bluetooth-Freisprecheinrichtungen zulassen
Bluetooth A2DP-Geräte zulassen	Erlauben Sie Bluetooth A2DP-Audiostreaming zwischen Geräten
Ausgehende Anrufe zulassen	Ausgehende Anrufe überBT zulassen
Datenübertragung über Bluetooth zulassen	Erlauben Sie die Datenübertragung über Bluetooth
Bluetooth-Tethering zulassen	Ermöglicht die Verwendung des Geräts als Modem (Bluetooth-Internetverbindung)
Verbindung zum Computer über Bluetooth zulassen	Verbindung zum Computer über Bluetooth zulassen

PIM-Verwaltung

Tauschen Sie

Nur verfügbar für Samsung KNOX 1.0 oder höher!

eMail-Adresse	Die angegebene E-Mail-Adresse des Benutzers Bitte beachten Sie die "Platzhalter", die Sie für die Arbeit mit Anmeldeinformationen verwenden können und die Sie nicht auf jedem Gerät manuell ändern müssen Mit einem Klick auf **Platzhalter anzeigen** können Sie sich diese anzeigen lassen
Server-Hostname	Serveradresse Ihres Exchange Servers
Login-Name	Der Login-Name für das jeweilige Endgerät, bitte beachten Sie auch die "Platzhalter hier
Domain	Domänenadresse
Passwort (nur auf Geräteebene)	Optional kann ein einzelnes Gerät mit einem Passwort versehen werden. Sollte dieses leer bleiben, wird der Benutzer aufgefordert, sein Exchange-Passwort einzugeben.
Anzahl der zu synchronisierenden Vortage	Anzahl der Tage, die bestimmen, wann die E-Mails wieder synchronisiert werden
Unterschrift	Eine Signatur kann angehängt werden (Hinweis: Einige Geräte erfordern eine HTML-Formatierung für die Signatur)
Standard-Konto	Legt fest, dass dieses Mailkonto das Standardkonto ist
Verwenden Sie Secure Sockets Layer (SSL)	Verwenden Sie eine SSL-Verbindung
Verwenden Sie Transport Layer Security (TLS)	Verwenden Sie eine TLS-Verbindung
Alle Zertifikate akzeptieren	Alle Zertifikate werden akzeptiert. Bitte wählen Sie diese Option, wenn Ihr Exchange Server ein selbstsigniertes Zertifikat verwendet

eMail

Hier können Sie IMAP- und POP-Konten auf die jeweiligen Endgeräte der Benutzer verteilen.

Die folgenden Einstellungen sind nur bei Samsung KNOX 1.0 oder höher verfügbar!		
eMail-Adresse	Die angegebene E-Mail-Adresse des Benutzers Bitte beachten Sie die "Platzhalter", die Sie für die Arbeit mit Anmeldeinformationen verwenden können und die Sie nicht auf jedem Gerät manuell ändern müssen Mit einem Klick auf **Platzhalter anzeigen** können Sie sich diese anzeigen lassen	
Protokoll des eingehenden Servers	Protokoll des eingehenden Servers	IMAP oder POP
Adresse des eingehenden Servers	Adresse des eingehenden Servers	
Port des eingehenden Servers	Port des eingehenden Servers	
Login/Benutzername des Eingangsservers	Login/Benutzername des Eingangsservers	
Passwort des Posteingangsservers (nur auf Geräteebene)	Passwort des Posteingangsservers (nur auf Geräteebene)	
Eingehender Server verwendet SSL	Eingehender Server verwendet SSL	
Eingehender Server verwendet TLS	Eingehender Server verwendet TLS	
Eingehender Server akzeptiert alle Zertifikate	Eingehende Server akzeptieren alle Arten von Zertifikaten	
Protokoll des ausgehenden Servers	Protokoll des ausgehenden Servers	SMTP
Port des ausgehenden Servers	Port des ausgehenden Servers	
Ausgehender Server verwendet zusätzliche Anmeldeinformationen	Zusätzliche Anmeldeinformationen für den Ausgangsserver. Wenn dies auf "off" gesetzt ist, werden die Einstellungen des Eingangsservers verwendet.	
Anmeldung/Benutzername des Ausgangsservers	Anmeldung/Benutzername des Ausgangsservers	
Passwort des Postausgangsservers (nur auf Geräteebene)	Passwort des Ausgangsservers	
Ausgehender Server verwendet SSL	Ausgehender Server verwendet SSL	
Ausgehender Server verwendet TLS	Ausgehender Server verwendet TLS	

Ausgehender Server akzeptiert alle Zertifikate	Der Ausgangsserver akzeptiert alle Arten von Zertifikaten
Unterschrift	Eine Signatur kann hier angehängt werden (Hinweis: Einige Geräte erfordern eine HTML-Formatierung für die Signatur)
Benutzer bei Erhalt einer neuen eMail benachrichtigen	Benachrichtigt den Benutzer bei Erhalt einer neuen E-Mail

AE Gmail Exchange

Info: Diese Konfiguration wird auf die Google Mail-App angewendet. Sie müssen also Gmail genehmigen und installieren.

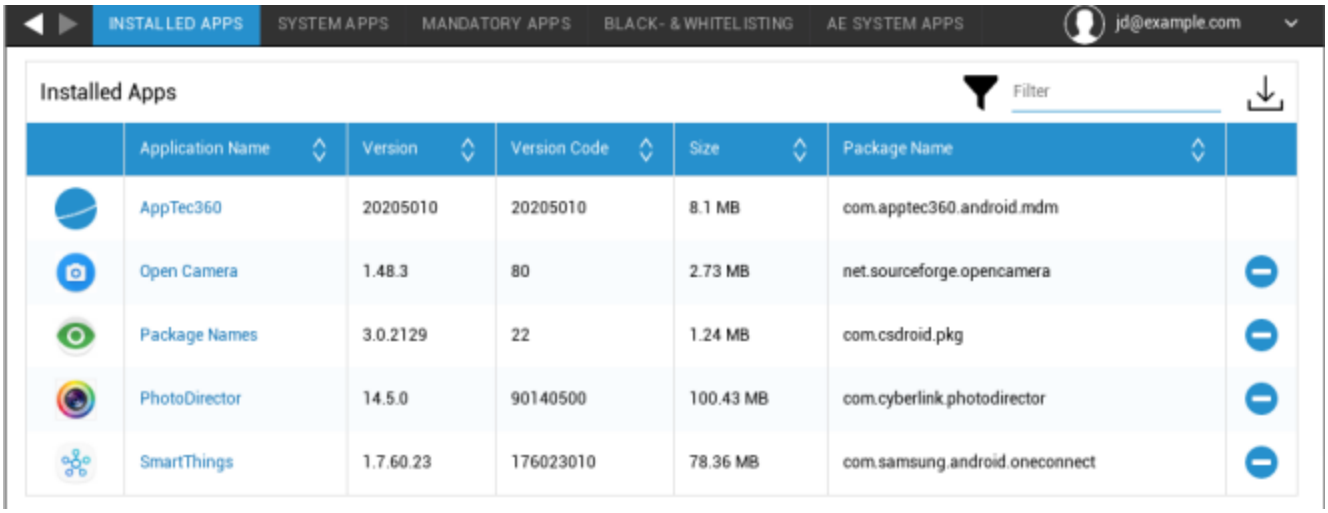
eMail-Adresse	Die angegebene E-Mail-Adresse des Benutzers Bitte beachten Sie die "Platzhalter", die Sie für die Arbeit mit Anmeldeinformationen verwenden können und die Sie nicht auf jedem Gerät manuell ändern müssen Mit einem Klick auf Platzhalter anzeigen können Sie sich diese anzeigen lassen
Server-Hostname	Serveradresse Ihres Exchange Servers
Login-Name	Der Login-Name für das jeweilige Endgerät, bitte beachten Sie auch die "Platzhalter hier
Unterschrift	Eine Signatur kann angehängt werden (Hinweis: Einige Geräte verlangen eine HTML-Formatierung für die Signatur)
Anzahl der zu synchronisierenden Vortage	Anzahl der Tage, die bestimmen, wann die E-Mails wieder synchronisiert werden
Geräte-Identifikator	EAS Identifier. Lassen Sie dies leer, wenn Ihre Umgebung dies nicht erfordert
Verwenden Sie Secure Sockets Layer (SSL)	Verwenden Sie eine SSL-Verbindung
Alle Zertifikate akzeptieren	Alle Zertifikate werden akzeptiert. Bitte wählen Sie diese Option, wenn Ihr Exchange Server ein selbstsigniertes Zertifikat verwendet
Nicht verwaltete Konten zulassen	Ermöglicht es dem Benutzer, weitere Konten hinzuzufügen
Kundenzertifikat	Laden Sie das Client-Zertifikat hoch, wenn Ihr Exchange-Server dies erfordert

App Verwaltung

Enterprise App Manager

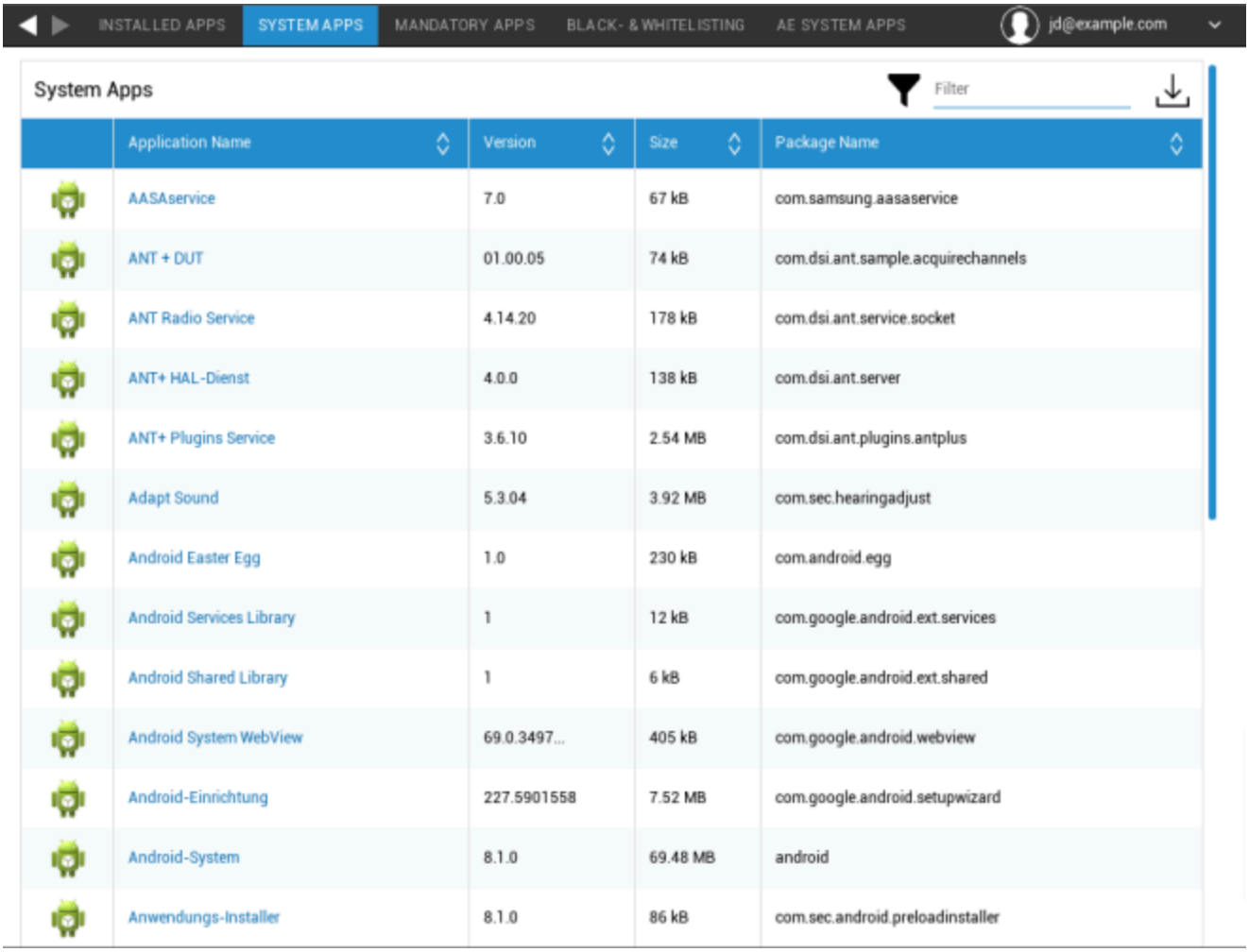
Installierte Apps (nur auf Geräteebene)

Hier werden Ihnen alle Apps angezeigt, die derzeit auf dem Endgerät des Benutzers installiert sind.


INSTALLED APPS
SYSTEM APPS
MANDATORY APPS
BLACK- & WHITELISTING
AE SYSTEM APPS
jd@example.com
Installed Apps
Filter
Application Name
Version
Version Code
Size
Package Name
AppTec360
20205010
20205010
8.1 MB
com.apptec360.android.mdm
Open Camera
1.48.3
80
2.73 MB
net.sourceforge.opencamera
Package Names
3.0.2129
22
1.24 MB
com.csdroid.pkg
PhotoDirector
14.5.0
90140500
100.43 MB
com.cyberlink.photodirector
SmartThings
1.7.60.23
176023010
78.36 MB
com.samsung.android.oneconnect

System-Apps (nur auf Geräteebene)

Unter "System-Apps" werden alle vorinstallierten Systeme mit ihrem Paketnamen und ihrer Version aufgelistet.



Obligatorische Apps

Unter Obligatorische Apps können Sie festlegen, welche Apps auf dem Gerät installiert sein müssen. Je nach Ihrer Konfiguration und Ihrem Gerät wird die App automatisch installiert oder der Benutzer wird aufgefordert, sie zu installieren.

Bitte beachten Sie, dass für eine einfache App-Verwaltung die Verwendung von Android Enterprise empfohlen wird.

Die Szenarien sind im Folgenden aufgeführt:

Normale Play Store Apps

Playstore App-Installationen erfordern immer eine Benutzerinteraktion. Außerdem muss auf dem Gerät ein Google-Konto eingerichtet werden.

InHouse App Installation

Auf Samsung-Geräten werden diese Apps unbemerkt installiert. Die einzige Ausnahme ist der Container, bei dem der Benutzer die Installation bestätigen muss.

In jedem anderen Szenario muss der Benutzer die Installation der App bestätigen.

Android Enterprise Play Store Apps

Diese Apps werden immer im Hintergrund installiert, ohne dass der Benutzer eingreifen muss.

Um eine obligatorische App hinzuzufügen, klicken Sie auf das "+" und wählen Sie die gewünschte App aus der Liste. Bitte beachten Sie, dass Sie keine Apps von der Registerkarte "Google Play Store" installieren können, wenn das Gerät mit Android Enterprise entweder als vollständig verwaltet oder als Container konfiguriert ist.

Wenn Sie Android Enterprise verwenden, wählen Sie die Apps aus dem Abschnitt "AE Play Store". Um Apps hier verfügbar zu machen, bestätigen Sie sie im Google Enterprise Play Store, indem Sie zu Allgemeine Einstellungen → AE Play Store → Play Store Apps gehen.

Wenn Sie eine obligatorische App entfernen, wird sie auch vom Gerät deinstalliert.

Sie können auf den Namen einer App in der Liste der obligatorischen Apps klicken und auf die Registerkarte "Konfiguration" gehen, um eine App zu konfigurieren. Dies erfordert die Verwendung von Android Enterprise und die App muss dies unterstützen. Daher hängen die verfügbaren Optionen von der ausgewählten App ab.

AE System Apps

Hier können Sie System-Apps für die Android Enterprise-Geräte aktivieren. Bitte beachten Sie, dass sich die angegebene App im Speicher des Systems befinden muss, sonst passiert nichts. 296

Beschränkungen & Einstellungen

Black- & Whitelisting

Hier können Sie eine Black- oder Whitelist definieren. Alle Apps auf der schwarzen Liste werden blockiert. Alle Apps, die nicht auf der Whitelist stehen, werden blockiert. Eine leere Blacklist blockiert nichts, während eine leere Whitelist alles blockiert*.

**Alle obligatorischen Apps und Apps aus dem Enterprise App Store werden automatisch auf die Whitelist gesetzt. Sie müssen sie nicht manuell hinzufügen*

Wenn Sie auf das "+" klicken, können Sie entweder nach einer App suchen, die Sie zu Ihrer Black- oder Whitelist hinzufügen möchten, oder einen Paketnamen manuell eingeben.

Sys App-Einschränkungen

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

Browser deaktivieren	Standard-Browser deaktivieren
Kalender deaktivieren	Nativen Kalender deaktivieren
Rechner deaktivieren	Taschenrechner deaktivieren
Chrome Browser deaktivieren	Chrome-Browser deaktivieren
Uhr deaktivieren	Uhr deaktivieren
Kontakte deaktivieren	Kontakte deaktivieren
Wählhilfe deaktivieren	Native Wählhilfe deaktivieren
eMail deaktivieren	E-Mail deaktivieren
Austausch deaktivieren	Exchange-Konten deaktivieren
Facebook deaktivieren	Facebook-App deaktivieren
Galerie deaktivieren	Deaktivieren Sie die native Galerie-App
Google Mail deaktivieren	Google Mail deaktivieren
Google Bücher deaktivieren	Google Bücher deaktivieren
Google Play Kiosk deaktivieren	Google Play Kiosk deaktivieren
Google Maps deaktivieren	Google Maps deaktivieren
Google Music deaktivieren	Google Music deaktivieren
Google Movies deaktivieren	Google Movies deaktivieren
Google Play Store deaktivieren	Deaktivieren Sie den Google Play Store (öffentlicher App Store)
Google Plus deaktivieren	Google Plus deaktivieren
Google Suche deaktivieren	Google Suche deaktivieren
Google Talk / Google Hangouts deaktivieren	Google Talk / Google Hangouts deaktivieren
Musik-Player deaktivieren	Deaktivieren Sie die native Musik-Player-App
Einstellungen deaktivieren	Geräteeinstellungen deaktivieren
Sim Toolkit deaktivieren	Sim Toolkit Dienste deaktivieren
SMS / MMS deaktivieren	SMS / MMS deaktivieren
Street View deaktivieren	Street View Dienste deaktivieren
Youtube deaktivieren	Youtube deaktivieren

Samsung Apps

Unter "Samsung Apps" können Sie zusätzliche Einstellungen und/oder Einschränkungen für Samsung-Geräte festlegen.

AllShare Play / Samsung Link deaktivieren	AllShare Play / Samsung Link deaktivieren
ChatON deaktivieren	ChatON deaktivieren
Game Hub deaktivieren	Game Hub deaktivieren
Gruppenspiel deaktivieren	Gruppenspiel deaktivieren
Hilfe deaktivieren	Samsung Hilfe deaktivieren
KNOX deaktivieren	Samsung KNOX-Behälter deaktivieren
Memo deaktivieren	Sprachnotiz deaktivieren
Meine Dateien deaktivieren	Meine Dateien deaktivieren
Optisches Lesegerät deaktivieren	Optisches Lesegerät deaktivieren
Polaris Office deaktivieren	Polaris Office deaktivieren
Readers Hub / Samsung Bücher deaktivieren	Readers Hub / Samsung Bücher deaktivieren
S Memo deaktivieren	Samsung Memo-App deaktivieren
S Translator deaktivieren	Samsung Translator App deaktivieren
S Voice deaktivieren	S Sprachassistent deaktivieren
Samsung Apps deaktivieren	Samsung App Store deaktivieren
Samsung Hub deaktivieren	Samsung Entertainment Stores deaktivieren
Video Player deaktivieren	Video Player deaktivieren
Sprachrekorder deaktivieren	Sprachrekorder deaktivieren
WatchON deaktivieren	WatchON deaktivieren (simuliert eine Fernbedienung)

Huawei Apps

Unter "Huawei Apps" können Sie zusätzliche Einstellungen und/oder Einschränkungen auf dem Huawei-Gerät festlegen.

DLNA deaktivieren	DLNA deaktivieren
App-Installer deaktivieren	App-Installer deaktivieren
Dateimanager deaktivieren	Dateimanager deaktivieren
Backup Manager deaktivieren	Backup Manager deaktivieren
System Updater deaktivieren	System Updater deaktivieren
Werkzeugkasten deaktivieren	Werkzeugkasten deaktivieren
Wetter deaktivieren	Wetter deaktivieren
FM-Radio deaktivieren	FM-Radio deaktivieren

App Management Einstellungen

Hier können Sie das Aktualisierungsverhalten von InHouse Apps festlegen.

Die Häufigkeit der Updateprüfung legt fest, wie oft die AppTec360 App nach Updates für InHouse Apps sucht. Sobald eine neue Version erkannt wurde, wird sie heruntergeladen und installiert.

Wi-Fi Threshold legt fest, ob der Download auf Wi-Fi-Verbindungen beschränkt werden soll, wenn die App größer ist als der von Ihnen konfigurierte Threshold. Wenn der Wert kleiner ist oder Sie keinen Schwellenwert festlegen, wird die App im Wi-Fi und in einem Mobilfunknetz heruntergeladen.

Enterprise App Store

Bitte beachten Sie, dass Apps, die hier (Enterprise App Store) hinzugefügt werden, NICHT automatisch auf dem/den Gerät(en) installiert werden. Der Benutzer muss den Enterprise App Store auf dem Gerät öffnen und die App manuell installieren.

Wenn Sie Apps automatisch auf dem Gerät installieren möchten, gehen Sie bitte zu "App Management" → "Enterprise App Manager" → "Obligatorische Apps" und fügen Sie dort die gewünschten Apps hinzu.

Unter diesem Punkt können Sie optionale Apps an Ihre Benutzer verteilen.

Playstore

Klicken Sie auf das "+", um eine Play Store-App zum Store hinzuzufügen. Wenn Sie Android Enterprise verwenden, gehen Sie bitte zu "App Management Enterprise Play Store". Beachten Sie auch, dass auf dem → Gerät ein Google-Konto eingerichtet sein muss, um die hier definierten Apps zu installieren.

Hausintern

Unter dem Punkt "In-House" können Sie intern entwickelte Apps hochladen und verbreiten.

Klicken Sie auf das "+", um eine InHouse App zum Enterprise App Store hinzuzufügen, die dann vom Benutzer installiert werden kann. In diesem Dialog können Sie auch eine neue InHouse-App hochladen.

Enterprise Play Store

Bitte beachten Sie, dass Apps, die hier (Enterprise Play Store) hinzugefügt werden, NICHT automatisch auf dem/den Gerät(en) installiert werden. Der Benutzer muss den Play Store auf dem Gerät öffnen und die App manuell installieren.

Wenn Sie Apps automatisch auf dem Gerät installieren möchten, gehen Sie bitte zu "App Management" → "Enterprise App Manager" → "Obligatorische Apps" und fügen Sie dort die gewünschten Apps hinzu.

Unter diesem Punkt können Sie optionale Apps an Ihre Benutzer verteilen.

Hier können Sie Apps zum Android Enterprise Playstore hinzufügen. Bitte beachten Sie, dass Sie Apps unter Allgemeine Einstellungen → AE Play Store → Play Store Apps genehmigen müssen. Diese Apps werden in den normalen Google Play Store aufgenommen.

Beachten Sie auch, dass Sie zunächst ein Layout mit Apps in Allgemeine Einstellungen → App-Verwaltung → AE Play Store → Store-Layout definieren müssen.

Apps müssen sich in einem Layout befinden, bevor Sie sie erfolgreich zum Store hinzufügen können.

Kiosk-Modus & Launcher

Kiosk-Modus

Der Kioskmodus ermöglicht es Ihnen, eine App oder eine URL vorzudefinieren. Dann wird es ausschließlich möglich sein, diese Anwendung und/oder URL auszuführen/aufzurufen.

Ebenso können verschiedene Hardware-Tasten im Kioskmodus deaktiviert werden.

Automatischer Start	Startet automatisch den Kioskmodus, sobald das Profil das Endgerät des Benutzers erreicht
Geplanter Kiosk-Modus?	Sie können eine Zeit für den Kioskmodus planen. Dieser startet und endet dann automatisch zu einer von Ihnen festgelegten Zeit.
Startzeit	Startzeit
Zeit in Minuten	Zeit in Minuten, nach der der Kioskmodus wieder beendet werden soll

Anwendungstyp

Einzelne App	Wenn Sie die App im Kioskmodus starten möchten, wählen Sie unter "Anwendungstyp" die Option "Paket".
Kiosk-Anwendung	Klicken Sie hier, um eine Anwendung auszuwählen, die im Kioskmodus gestartet werden soll Hier finden Sie die übliche Übersicht der App-Verwaltung Sie können zwischen einem "Google Play Store", "Android In-House Apps" und einem "Packagename" wählen.

Anwendungstyp	
URL	Wenn Sie eine URL im Kioskmodus starten möchten, wählen Sie unter "Anwendungstyp" die Option "URL". Definieren Sie dann die gewünschte URL-Adresse
Browser nach Inaktivität löschen	Hier können Sie ein Zeitintervall in Minuten festlegen, nach dem der Kioskmodus neu gestartet werden soll
Web-Cache und Cookies löschen	Wenn Sie diese Funktion aktivieren, wird nach einem Neustart des Kioskmodus der Web-Cache (Cookies und zwischengespeicherte Bilder) gelöscht.
Politik der gleichen Herkunft	Wenn diese Funktion aktiv ist, kann der Benutzer nur auf den Unterseiten einer bestimmten URL surfen Sie haben zum Beispiel die folgende URL definiert:www.mypage.com Dann kann der Benutzer weitersurfen: www.mypage.com/subpage
URLs auf der Whitelist	Hier können Sie eine Whitelist pflegen, alle diese URLs sind erlaubt Maximal 1 URL pro Zeile Eine URL muss mit http:/ oder https:// beginnen.
Auf der schwarzen Liste stehende URLs	Hier können Sie eine Blacklist pflegen, in der alle diese URLs nicht erlaubt sind Maximal 1 URL pro Zeile Eine URL muss mit http:/ oder https:// beginnen.
Bildschirmausrichtung	Diese Einstellung bezieht sich auf die Bildschirmeinstellungen Automatisch = automatisch Hochformat = vertikales Format Landscape = Querformat

Multi-App	Wenn Sie den Kioskmodus "Multi App" auswählen, wird die Verwendung des AppTec360 Launcher erzwungen.
Apps	Anwendung: Wählen Sie eine Playstore- oder eine hauseigene App als Kioskanwendung. Es ist auch möglich, einen Packungsnamen einzugeben. Die ausgewählte Kioskanwendung muss auf dem Gerät installiert sein. Denken Sie daran, die Kiosk-Anwendung als obligatorisch einzustellen. Verknüpfung auf dem Homescreen: Wenn Sie diese Option auf "Ein" setzen, wird eine Verknüpfung auf dem Homescreen erstellt. Wenn Sie die Option "Aus" wählen, wird die App trotzdem in der App-Liste angezeigt.

Exit-Passwort Aktiviert	Wenn Sie diese Funktion aktivieren, ist es dem Benutzer möglich, den Kioskmodus mit einem von Ihnen festgelegten Passwort zu beenden.
Exit-Passwort	Dies ist das Passwort, das Sie selbst festgelegt haben
Statusleiste automatisch einklappen	Wenn diese Option aktiviert ist, wird die Statusleiste automatisch kollabiert. Mit dieser Option können Benutzer die Informationen in der Statusleiste sehen, aber nicht auf ihre Funktionen zugreifen
Statusleiste deaktivieren	Die Statusleiste enthält Benachrichtigungen, Shortcuts und Informationen. Nur verfügbar für Samsung-Geräte mit KNOX 1.0 oder höher.
Lautstärketasten deaktivieren	Lautstärketasten deaktivieren (nur verfügbar auf Samsung-Geräten mit KNOX 1.0 oder höher)
Ein/Aus-Schalter deaktivieren	Ein/Aus-Schalter deaktivieren (nur bei Samsung-Geräten mit KNOX 1.0 oder höher verfügbar)
Home-Taste deaktivieren	Deaktivieren Sie die Home-Taste. Wenn diese Funktion aktiviert ist, kann der Kioskmodus nur in der AppTec360 Konsole beendet werden. (nur auf Samsung-Geräten mit KNOX 1.0 oder höher verfügbar)
Navigationsleiste deaktivieren	Damit können Sie die Navigationsleiste (Zurück / Menü) deaktivieren. Wenn diese Funktion aktiviert ist, kann der Kioskmodus nur in der AppTec360 Konsole beendet werden. (nur verfügbar auf Samsung-Geräten mit KNOX 1.0 oder höher)

App Update Einstellungen	
App-Updates zulassen	Die Benutzer werden aufgefordert, App-Updates durchzuführen, auch wenn der Kioskmodus aktiv ist. Auf Geräten mit Samsung KNOX werden Apps unbemerkt aktualisiert.
Fenster aktualisieren	Legen Sie ein Intervall fest, in dem die Benutzer aufgefordert werden, App-Updates zu installieren.

TeamViewer	
Unbeaufsichtigten Zugriff aktivieren	Wenn diese Funktion aktiviert ist, können Administratoren das Gerät ohne Benutzerinteraktion fernsteuern. Die App TeamViewer Host muss auf dem Gerät installiert sein.

AppTec360-Startprogramm

Aktivieren Sie AppTec360 Launcher	Ein: Aktiviert den AppTec360 Launcher. Der Benutzer muss ihn einmalig als Standard-Startprogramm festlegen. Hinweis: Wenn der Kioskmodus aktiviert ist und der Kioskmodus auf "Multi App" eingestellt ist, wird die Verwendung des AppTec360 Launcher erzwungen.
Große Icons	Ein: Zeigt eine größere Version der App-Symbole im Launcher an
AppTec360 App-Symbol ausblenden	Ein: Blendet die AppTec360 App vollständig aus
AppTec360 Store-Symbol ausblenden	Ein: Blendet den AppTec360 Enterprise AppStore vollständig aus.

AppTec360 Einstellungen

AppTec360 Einstellungen App aktivieren	Die AppTec360 Settings App ermöglicht die Kontrolle über WiFi- und Bluetooth-Verbindungen
Einstellungen in Multi-App aktivieren Kiosk-Modus	Wenn aktiviert, können Benutzer auf die AppTec360 Settings App zugreifen, während der Multi App Kiosk Modus aktiv ist.

Fernsteuerung

Splashtop

Zeigt den aktuellen Status der Splashtop-Einrichtung an. Hier sehen Sie die Schritte, die Sie für den Fernzugriff auf das Gerät über Splashtop ausführen müssen. Hier müssen Sie auch Ihren Einsatzcode eingeben, den Sie auf der Splashtop-Website erhalten. Der Bereitstellungscode ist erforderlich, um eine Verbindung mit dem Gerät herzustellen.

Teamviewer

Zeigt den aktuellen Status der Teamviewer-Einrichtung an. Hier sehen Sie die Schritte, die Sie für den Fernzugriff auf das Gerät über Teamviewer ausführen müssen.

Content Management

Inhaltsbox

Hier können Sie die Contentbox für dieses Gerät aktivieren. Nach der Aktivierung wird die Contentbox App auf dem Gerät installiert.

Sicherer Browser

Hier können Sie den sicheren Browser für dieses Gerät aktivieren. Nach der Aktivierung wird die Secure Browser App auf dem Gerät installiert. Dieser Browser kann so konfiguriert werden, dass er einen Webbrowser auf dem Gerät anbietet, der auf Ihre Bedürfnisse beschränkt ist.

Passwort anfordern	Verlangen Sie vom Benutzer die Einrichtung und Verwendung eines Passworts für den Zugriff auf den Browser.
Downloads einschränken / Öffnen in	Blockiert Downloads von Websites
Uploads einschränken	Schränkt Uploads auf bestimmte URLs ein. Geben Sie keine URL an, um den Upload vollständig zu blockieren
Kopieren zulassen	Erlauben Sie das Kopieren, Ausschneiden oder Teilen von Text innerhalb der Webseiten.
Bildschirmaufzeichnung zulassen	Erlauben Sie die Aufnahme von Bildschirmfotos.
Häufigkeit der Datenbereinigung	Wählen Sie, wie oft ALLE Benutzerdaten (Verlauf, Cache usw.) automatisch gelöscht werden sollen.
Lesezeichen für Unternehmen	Die Lesezeichen werden im Ordner "Firmenlesezeichen" in den Lesezeichen des Browsers angezeigt. Sie können vom Benutzer nicht bearbeitet werden.
Adressleiste ausblenden	Blendet die Adressleiste aus, damit der Benutzer die URL, die er besucht, nicht sehen kann
In-Browser Whitelisting (ohne Universal Gateway)	Aktiviert das URL-Whitelisting auf der Client-Seite. - Firmen-Lesezeichen sind immer auf der Whitelist - Nur für 100 URLs unterstützt - Bitte verwenden Sie den Universal Gateway für unbegrenztes Black- und Whitelisting
Gateway-basiertes Black- und Whitelisting	Das Blacklisting hat folgende Voraussetzungen: - Ein funktionierendes AppTec360 Universal Gateway ("Allgemeine Einstellungen" → "Universal Gateway") - Eine funktionierende VPN-Konfiguration mit einem angegebenen DNS-Server ("Allgemeine Einstellungen" → "Universal Gateway" → "VPN-Einstellungen") - Eine Blacklist-Konfiguration ("Allgemeine Einstellungen" → "Universal Gateway" → "Domain

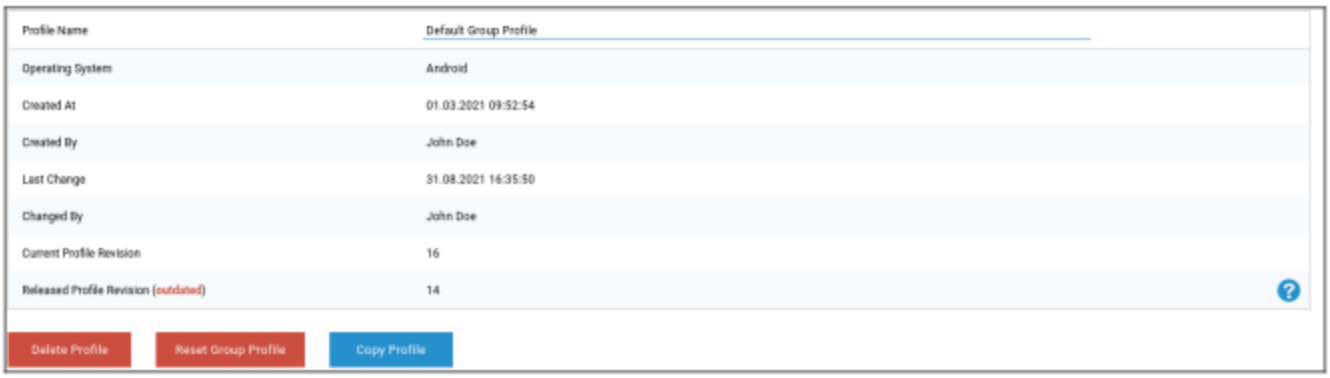
	Blacklist") - Eine gültige VPN-Verbindung im Profil ("Verbindungsverwaltung" → "VPN")

Konfiguration Windows 10 PC

Allgemein

Gruppenprofilübersicht (nur auf Gruppenebene)

Wenn Sie ein Gruppenprofil öffnen, erhalten Sie einen schnellen Überblick über das Profil.



Profil Name	Name des Profils (kann hier geändert werden)
Betriebssystem	Betriebssystem, für das das Profil bestimmt ist
Erstellt am	Zeitpunkt der Erstellung
Erstellt von	Der Ersteller des Profils
Letzte Änderung	Zeitpunkt der letzten Änderung des Profils
Geändert von	Konto, das die letzten Änderungen vorgenommen hat
Aktuelle Profilüberarbeitung	Revision des gespeicherten Profilstatus
Freigegebene Profil-Revision	Zugewiesene Profilrevision ("Jetzt zuweisen"). Wenn das Etikett hinter dem Text "(veraltet)" anzeigt, bedeutet dies, dass Sie das Profil zwar gespeichert, aber noch nicht zugewiesen haben, so dass die Geräte noch eine ältere Version erhalten.

Geräteübersicht (nur auf Geräteebene)

Die zusammengefasste Übersicht des Geräts, die Folgendes enthält:

PC Name	Name des PCs
Kunde	Die Geräte Windows-Typ
Letzter bekannter Standort	Den Breiten- und Längengrad des letzten bekannten Standorts des Geräts
Zugewiesene obligatorische Apps	Anzahl der dem Gerät zugewiesenen obligatorischen Apps
PC UID	UID des PCs
OS Ausgabe	Zeigt Ihre Windows Edition
OS Version	Aktuell installierte Windows-Version
OS Aufbau	Aktuelle Windows-Version
Betriebssystem	Derzeit installiertes Betriebssystem
Seriennummer	Seriennummer des Geräts
Geräteeigentum	Der konfigurierte Ownership-Typ
Gerätetyp	Der Typ des Geräts
Verwurzelt	Zeigt an, ob das Gerät gerootet ist
Konform	Zeigt an, ob das Gerät konform ist
Zuletzt gesehen	Datum und Uhrzeit, wann die Änderungen am Profil vorgenommen wurden
Benutzerzuordnung	Zeigt den Benutzer oder die Gruppe an, der dieses Gerät derzeit zugewiesen ist. Sie können das Gerät verschieben, indem Sie einen anderen Benutzer oder eine andere Gruppe aus der Dropdown-Liste auswählen.

Einstellungen

Automatische Aktualisierung zulassen	Automatische Betriebssystem-Updates zulassen oder verbieten.

Config Revision (nur auf Geräteebene)

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

Wenn Sie auf das Gruppenprofil klicken, haben Sie direkten Zugriff auf das Profil und können Einstellungen vornehmen.

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

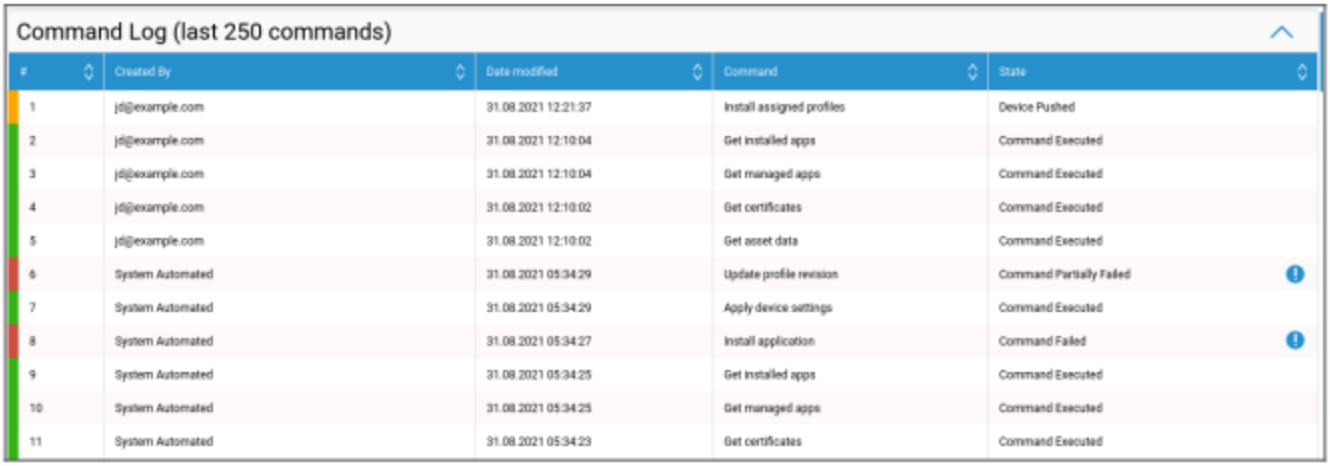
Mit dem Symbol können Sie das Geräteprofil so zurücksetzen, dass es keinerlei Einstellungen enthält.

"Neuere Revision verfügbar" bedeutet, dass das Gruppenprofil geändert und gespeichert, aber nicht zugewiesen wurde. Das Gruppenprofil muss mit "Jetzt zuweisen" auf Gruppenebene zugewiesen werden, um die Änderungen auf die Geräte anzuwenden.

Geräteprotokoll (nur auf Geräteebene)

Befehl Log

Hier können Sie sehen, welche Befehle für das Gerät erteilt wurden und welchen Status sie haben.



Mit "System Automated" erstellte Befehle werden automatisch vom System erstellt.

Mögliche Befehlszustände

Gerät geschoben	Eine Push-Anfrage wurde an den Push-Dienst (z.B. APNS) gesendet, um das Gerät anzuweisen, sich wieder mit dem EMM-Server zu verbinden.
Befehl erstellt	Der Befehl wurde im System erstellt.
Befehl gesendet	Der Befehl wurde an das Gerät gesendet, nachdem es sich mit dem Server verbunden hat.
Befehl Ausgeführt	Der Befehl wurde erfolgreich ausgeführt.
Befehl fehlgeschlagen	Der Befehl ist fehlgeschlagen. *
Befehl Teilweise fehlgeschlagen	Je nach Betriebssystem des Geräts können einige Befehle in Gruppen zusammengefasst werden. Dabei sind einige Teile dieser Befehlsgruppe fehlgeschlagen. *
Befehl ausgeführt, eventuell fehlgeschlagen	Der Befehl wurde ausgeführt, aber vielleicht auch nicht.
Kommando zurückgeschoben	Der Befehl wurde von einem Benutzer erneut gesendet.
Weggeworfen	Der Befehl wurde verworfen. Zum Beispiel, weil er durch einen anderen Befehl ersetzt wurde oder das Gerät neu registriert wurde und alte Befehle entfernt wurden

*Wenn sich hinter der Nachricht ein Ausrufezeichen befindet, erhalten Sie weitere Informationen, indem Sie mit dem Mauszeiger über das Symbol fahren.

Asset Management (nur auf Geräteebene)

Geräte-Infos

Hersteller	Hersteller des Geräts
Modell	Gerät Modell
Modellnummer	Modellnummer
Betriebssystem	Betriebssystem
OS Version	OS-Version
Seriennummer	Seriennummer
ExchangeID	ExchangeID
RAM gesamt	RAM gesamt
Display Auflösung	Display-Auflösung
Telefon Sprache	Sprache des Geräts
Firmware Version	Firmware Version
DM Client Version	Version von Device Management Client
Hardware Version	Hardware-Version des Geräts
CPU-Architektur	CPU-Architektur (Prozessortyp)

Zellulär

SIM-Betreiber Netzwerk	Trägernetzwerk
Telefon Nummer	Telefon Nummer
Roaming-Status	Roaming-Status
IMEI	IMEI
IMSI	IMSI
Modem-Firmware	Modem-Firmware

Informationen zur Synchronisierung

Sofortige DM-Verbindung	Das Gerät sollte sofort eine Verbindung zu AppTec herstellen
Erste Wiederholungsversuche	Erste Wiederholungszeit für diese erste Verbindung
Wiederholte Verbindungsversuche	Anzahl der erneuten Verbindungsversuche nach einem Abbruch der Verbindung durch den Verbindungsmanager oder einem Fehler auf WinInet-Ebene
Maximale Schlafdauer	Maximale Ruhezeit nach einem Fehler beim Paketversand
Erste Sync-Wiederholungen	Zeit für die erste Etappe nach der Immatrikulation
Intervall für den ersten Wiederholungsversuch	Zeit für die erste Etappe nach der Immatrikulation
Zweite Sync-Wiederholungen	Zeit für die zweite Etappe nach der Einschulung
Zweiter Wiederholungsversuch Intervall	Zeit für die zweite Etappe nach der Einschulung
Regelmäßige Wiederholungen der Synchronisation	Zeit für die weiteren Etappen nach der Immatrikulation
Regelmäßiges Wiederholungsintervall	Zeit für die weiteren Etappen nach der Immatrikulation

Sicherheitsmanagement

Anti-Diebstahl (nur auf Geräteebene)

GPS-Informationen (nur auf Geräteebene)

Hier können Sie den aktuellen/letzten Standort des Geräts festlegen. Die Lokalisierung kann mit einem oder sogar zwei Passwörtern geschützt werden - Siehe: "Allgemeine Einstellungen" > "Datenschutz" > "GPS-Zugang"

GPS-Einstellungen

GPS-Ortung aktivieren	Aktivieren Sie die regelmäßige Synchronisierung von GPS-Informationen.
Verfolgungsintervall	Legen Sie das Intervall für die Synchronisierung der GPS-Informationen fest.

Sicherheitskonfiguration

Passcode

Mindestlänge des Passworts	Minimale Passwortlänge	
Passwort Zusammensetzung	Legt die Anzahl der Zeichen fest, die das Passwort enthalten muss Diese bestehen aus Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen.	
Passwort Qualität	Hier können Sie die Passwortqualität festlegen	
	Alphanumerisch	Nur Zahlen und Buchstaben
	Numerisch	Nur Zahlen
	Numerisch oder Alphanumerisch	Zahlen oder Zahlen und Buchstaben
Maximale Inaktivitätszeit Sperre	Anzahl der Minuten der Inaktivität des Benutzers auf dem Gerät, nach denen das Gerät gesperrt wird. Der Benutzer muss das Gerät nach dieser Zeit entsperren, indem er sein Gerätepasswort eingibt.	
Passwort-Ablauf	Legen Sie die Zeit fest, bis ein neues Passwort festgelegt werden muss	
Einschränkung des Passwortverlaufs	Anzahl der zuvor verwendeten Kennwörter, die nicht erlaubt sind	
Maximale fehlgeschlagene Passwortversuche	Wie oft kann das Passwort falsch eingegeben werden, bevor das Gerät komplett gelöscht wird?	

Antivirus

Antivirus-Einstellungen - Konfiguration der Überprüfung festlegen	
Art des Scans	Wählt aus, ob ein schneller Scan oder ein vollständiger Scan durchgeführt werden soll.
Scan-Start einstellen	Wählt die Tageszeit aus, zu der Windows Defender den Scanvorgang startet
Scan-Frequenz	Wählt den Tag aus, an dem der Windows Defender-Scan ausgeführt werden soll
Häufigkeit der Signaturaktualisierung	Legt das Intervall in Stunden fest, in dem nach Signaturen gesucht wird.

Konfigurieren Sie den Typ der zu überprüfenden Dateien	
Scannen von Archivdateien zulassen	Erlauben oder verbieten Sie das Scannen von Archiven (z.B. .zip), wenn auf sie zugegriffen wird.
Scannen von Skripten zulassen	Erlaubt oder verbietet die Windows Defender Script Scanning-Funktion.
Scannen von E-Mails zulassen	Erlauben oder verbieten Sie das Scannen von E-Mails.
Scannen von Netzwerkdateien zulassen	Erlauben oder verbieten Sie das Scannen von Netzwerkdateien.
Vollständiges Scannen von zugeordneten Netzlaufwerken zulassen	Erlauben oder verbieten Sie das Scannen von zugeordneten Netzlaufwerken (nur aktiviert, wenn die vollständige Suche aktiviert ist).
Bidirektionales Scannen steuern	Steuert, welche Dateigruppen überwacht werden sollen.
Vollständiges Scannen von Wechsellaufwerken zulassen	Vollständiges Scannen von Wechsellaufwerken zulassen oder verbieten. Nur während des vollständigen Scans wird gestartet.

Typ der Dateien, die von der Überprüfung ausgeschlossen werden sollen	
Dateitypen beim Scannen ignorieren	Definieren Sie eine Reihe von Dateityp-Erweiterungen. Jede Dateierweiterung für jedes Feld.
Verzeichnispfade ignorieren	Definieren Sie eine Reihe von Verzeichnispfaden, um sie nicht zu scannen. Ein Pfad pro Feld. Beispiele: "C:\Beispiel", "C:\Windows" oder "C:\Benutzer".
Prozesse von der Überprüfung ausschließen	Schließen Sie Dateien, die von bestimmten Prozessen geöffnet wurden, von Microsoft Defender Antivirus-Scans aus. . Ein Pfad pro Feld. Beispiele: "C:\myFile.exe", "C:\Windows\myProcess.exe", "C:\myScript.bat

Extra Einstellungen	
Erlauben Sie die Überwachung in Echtzeit	Windows Defender-Echtzeitüberwachungsfunktion zulassen oder nicht zulassen
Verhaltensüberwachung zulassen	Erlauben oder verbieten Sie die Windows-Verhaltensüberwachung
Cloud-Schutz zulassen	Erlauben oder verbieten Sie, dass Windows Defender Informationen über jedes gefundene Problem an Microsoft sendet. Microsoft analysiert diese Informationen, erfährt mehr über das Problem, das das Gerät betrifft, und bietet verbesserte Lösungen an.
	Verhalten beim Versenden von Proben
Windows Defender IOAV-Schutz zulassen	Windows Defender IOAV-Schutz zulassen oder deaktivieren
Erlauben Sie den Zugriff auf Defenders "On Access protection" UI	
Durchschnittlicher CPU-Lastfaktor	Stellt den durchschnittlichen CPU-Lastfaktor für den Windows Defender-Scan dar (in Prozent).

Umgang mit Malware	
Geringer Schweregrad	Sie können für jeden Schweregrad festlegen, wie das Gerät mit Malware umgeht. Verfügbare Optionen sind: • Sauber • Quarantäne • Entfernen Sie • Erlauben Sie • Benutzerdefiniert • Block
Mäßiger Schweregrad	
Hoher Schweregrad	
Schwerer Schweregrad	
Tage, um gereinigte Malware aufzubewahren	Zeitraum in Tagen, in dem die Quarantänedateien/-objekte auf dem System gespeichert werden. Der Standardwert ist 0, wodurch Objekte in der Quarantäne verbleiben und nicht automatisch entfernt werden. Der maximale Wert ist 90.

Sicherheitszentrum

Windows Sicherheitscenter - Einstellungen für die Windows-Sicherheit	
Viren- und Bedrohungsschutz deaktivieren UI	
Ransomware Datenrettung ausblenden UI	
Kontoschutz UI deaktivieren	
Firewall und Netzwerkschutz deaktivieren UI	
App- und Browsersteuerung UI deaktivieren	
Änderungen am Exploit-Schutz nicht zulassen	Änderungen der Einstellungen für den Exploit-Schutz durch den Benutzer nicht zulassen
Gerätesicherheits-UI deaktivieren	
TPM-Fehlerbehebung ausblenden	TPM-Fehlerbehebungseinstellungen ausblenden
Schaltfläche TPM löschen deaktivieren	
UI für Geräteleistung und -zustand deaktivieren	
UI für Familienoptionen deaktivieren	

Toasts anpassen	
Benutzerdefinierte Support-Informationen aktivieren	Aktivieren Sie diese Option, um unten rechts in der Sicherheitscenter-App individuelle Kontaktinformationen für Ihr Unternehmen anzuzeigen.
E-Mail Adresse	E-Mail Adresse des Unternehmens festlegen
Name des Unternehmens	Name des Unternehmens festlegen
Telefon der Firma	Telefon der Firma einstellen
Hilfe-URL	Legen Sie die Hilfe-URL des Unternehmens fest

Extra Einstellungen	
Benachrichtigungen deaktivieren	Deaktivieren Sie die Anzeige von Benachrichtigungen des Windows Defender Sicherheitscenters.
Empfehlungen zur Aktualisierung der TPM-Firmware ausblenden	Blenden Sie die Empfehlung aus, die TPM-Firmware zu aktualisieren, wenn eine anfällige Firmware entdeckt wird.
Firmenname und Kontaktoptionen anzeigen	Zeigen Sie Ihren Firmennamen und Ihre Kontaktoptionen in einer Kontaktkarte an, die im Windows Defender Security Center eingeblendet wird.
Secure Boot ausblenden	Bereich Sicherheits-Boot ausblenden.
Steuerung des Sicherheitsbenachrichtigungsbereichs ausblenden	Das Steuerelement für den Benachrichtigungsbereich der Windows-Sicherheit ausblenden.

Firewall-Konfiguration

Firewall-Konfiguration - Globale Einstellungen	
Authentifizierungssatz ignorieren	Ignorieren Sie den gesamten Authentifizierungssatz, wenn sie nicht alle im Satz angegebenen Authentifizierungssuites unterstützen
Art der Paket-Warteschlangenbildung	Legt fest, wie die Skalierung für die Software auf der Empfangsseite sowohl für den verschlüsselten Empfang als auch für die Freigabe des Weiterleitungspfads für das IPsec-Tunnel-Gateway-Szenario aktiviert wird.
Deaktivieren Sie die Durchführung von Stateful-FTP-Filterung	Wenn diese Funktion deaktiviert ist, wird das Stateful File Transfer Protocol (FTP) nicht gefiltert, um sekundäre Verbindungen zuzulassen.
Leerlaufzeit der Sicherheitsvereinigung	Dieses Feld konfiguriert die Leerlaufzeit der Sicherheitsassoziation in Sekunden. Sicherheitsassoziationen werden gelöscht, nachdem für diesen Zeitraum kein Netzwerkverkehr stattgefunden hat.
Preshared Key Verschlüsselung	Legen Sie die Kodierung für den gemeinsamen Schlüssel fest
IPSec Ausnahmen	Konfigurieren Sie die Ausnahmen für das Internetprotokoll
Überprüfung der Zertifikatswiderrufsliste	

Firewall-Profile (Domänenprofil / Privates Profil / Öffentliches Profil)	
Aktivieren Sie die Firewall für dieses Profil	
Benachrichtigungen deaktivieren	Deaktivieren Sie die Anzeige einer Benachrichtigung für den Benutzer, wenn eine Anwendung für das Abhören eines Ports gesperrt ist.
Unicast-Antworten auf Multicast-Broadcasts blockieren	
Durchsetzung von Firewall-Regeln für autorisierte Anwendungen	Wenn sie nicht erzwungen wird, werden die Firewall-Regeln für autorisierte Anwendungen im lokalen Speicher ignoriert und nicht erzwungen.
Globale Port-Firewall-Regeln durchsetzen	Wenn sie nicht erzwungen wird, werden die globalen Port-Firewall-Regeln im lokalen Speicher ignoriert und nicht erzwungen. Die Einstellung hat nur dann eine Bedeutung, wenn sie im Gruppenrichtlinienspeicher gesetzt oder aufgezählt wird oder wenn sie aus dem GroupPolicyRSoPStore aufgezählt wird
Firewall-Regeln durchsetzen	Wenn sie nicht erzwungen wird, werden die Firewall-Regeln des lokalen Speichers ignoriert und nicht erzwungen.
Regeln für die Verbindungssicherheit durchsetzen	Wenn sie nicht erzwungen wird, werden die Sicherheitsregeln für Verbindungen aus dem lokalen Speicher ignoriert und nicht erzwungen.
Standard-Ausgangsaktion	Die Aktion, die die Firewall standardmäßig bei ausgehenden Verbindungen durchführt
Standard-Eingangsaktion	Die Aktion, die die Firewall standardmäßig bei eingehenden Verbindungen durchführt
Stealth-Modus deaktivieren	Der Stealth-Modus ist ein Mechanismus in der Windows-Firewall, der verhindert, dass böswillige Benutzer Informationen über Netzwerkcomputer und die von ihnen ausgeführten Dienste herausfinden können.
Deaktivieren Sie das Reagieren auf unerwünschten Datenverkehr	Wenn diese Option deaktiviert ist, dürfen die Stealth-Modus-Regeln der Firewall den Host-Computer nicht daran hindern, auf unaufgeforderten Netzwerkverkehr zu reagieren, wenn dieser Verkehr durch IPsec gesichert ist.

Firewall-Regeln

Firewall-Regeln	
Name	Name der Regel
Beschreibung	Beschreibung der Regel
Aktion	Geben Sie an, ob diese Regel den Datenverkehr blockieren oder zulassen soll. Bitte beachten Sie, dass die Option Blockieren auch den Datenverkehr (abhängig von der restlichen Konfiguration) zwischen dem MDM-Server und dem Gerät blockieren kann.
Richtung	
Edge-Traversal aktivieren (nur verfügbar, wenn **Richtung** auf **eingehenden Verkehr** eingestellt ist)	Zeigt an, dass bestimmter eingehender Datenverkehr mit Hilfe der Teredo-Tunneling-Technologie durch NATs und andere Edge-Geräte getunnelt werden darf.

Programme & Dienstleistungen	
Definieren Sie Anwendungen, alle anderen	Wenn nicht aktiviert, werden alle Anträge berücksichtigt.
Paket Familienname	Der Name der Paketfamilie, für die die Regel gelten soll.
Dateipfad der Anwendung	Die vollständige Anwendung wie z.B. C:\Windows\System\Notepad.exe, auf die die Regel angewendet werden soll
Vollständig qualifizierter binärer Name	Der vollständig qualifizierte binäre Name, auf den die Regel angewendet werden soll. Ein FQBN ist eine Zeichenfolge in der folgenden Form: {Herausgeber, Produkt, Dateiname, Version}
Dienst Name	Geben Sie den Namen eines Dienstes ein (z.B. "EventLog"). Sie können eine Liste der Dienstnamen über Powershell abrufen, indem Sie den Befehl "Get-Service" ausführen.

Protokolle & Ports				
Protokoll	Das von der Regel verwendete Protokoll.			
	Verfügbare Werte: - Jede - Benutzerdefiniert - HOPORT - ICMPv4 - IGMP - TCP - UDP - IPv6 - IPv6-Route - IPv6-Frag - GRE - ICMPv6 - IPv6-NoNxt - IPv6-Optionen - VRRP - PGM - L2TP	Bei Einstellung auf Benutzerdefiniert	Geben Sie eine Protokollnummer zwischen 0 und 255 ein.	Die Protokollnummer
		Bei Einstellung auf TCP oder UDP	Geben Sie lokale Ports an, ansonsten werden alle verwendet	Lokale Ports, die von der Regel verwendet werden, Bereichsports sind ebenfalls erlaubt
			Lokaler Hafen	Einzelner Port oder eine Reihe von Ports. Z.B. 100-120,200,300-320.
			Geben Sie entfernte Ports an, ansonsten werden alle verwendet	Entfernte Ports, die die Regel verwenden wird, Bereichsports sind ebenfalls erlaubt
			Entfernter Anschluss	Einzelner Port oder eine Reihe von Ports. Z.B. 100-120,200,300-320.

Umfang	
Geben Sie lokale IPs an, andernfalls eine beliebige IP	Menge lokaler IPs, es kann auch ein Bereich von IPs sein, der durch -
Lokale IP-Adresse	Eine Reihe von einzelnen IPs oder ein Bereich von IPs, getrennt durch -
Geben Sie entfernte IPs an, andernfalls jede entfernte IP	Geben Sie eine Gruppe von Remote-IPs an, es kann auch ein durch "-" getrennter Bereich von IPs sein.
Entfernte IP-Adresse	Geben Sie einzelne IPs oder eine Reihe von IPs an
Wertmarken	Token, die zusammen mit Remote-Adressen festgelegt werden können. Tokens Intranet, RmtIntranet und Ply2Renders werden in Windows 10, Version 1809 und höher, unterstützt.

Erweiterte Einstellungen

Geben Sie Profile an, sonst werden alle verwendet	Wenn deaktiviert, werden alle Profile verwendet.
Domain	Domänenprofil
Privat	Privates Profil
Öffentlich	Öffentliches Profil
Geben Sie Schnittstellen an, sonst werden alle verwendet	Wenn deaktiviert, werden alle Schnittstellen verwendet.
Lokales Netzwerk	Local Area Network-Schnittstelle
Fernzugriff	Schnittstelle für Fernzugriff
Drahtlos	Drahtlose Schnittstelle

Lokale Schulleiter	
Autorisierte lokale Benutzer hinzufügen	Erlauben Sie das Hinzufügen einer Liste von lokalen Benutzern, die diese Regel verwenden sollen
Autorisierte Benutzer	Liste der autorisierten lokalen Benutzer für diese Regel. Der Benutzer muss im SDDL-Format (Security Description Definition Language) vorliegen, z.B. PC_NAME\USERNAME. Dieses Feld darf nicht ausgefüllt werden, wenn ein Dienstname für die Verwendung dieser Regel festgelegt wurde.

Einstellungen zur Einschränkung

Gerätefunktionalität

SD-Karte zulassen	Erlauben Sie die Verwendung einer SD-Karte
Kamera zulassen	Erlauben Sie die Verwendung der Kamera
Standortdienst zulassen	Gerätestandortdienst zulassen
Sideloading von Apps zulassen	Installation von Apps aus unbekannten Quellen zulassen
Entwicklermodus zulassen	Erlaubt den Entwicklermodus
Mobiles Datenroaming zulassen	Erlauben Sie mobiles Datenroaming
Cortana zulassen	Sprachassistentin Cortana zulassen
Erlauben, dass die Suche den Standort verwendet	Erlauben Sie die Suche nach dem Standort
Hinzufügen von Nicht-Microsoft-E-Mail-Konten zulassen	Legen Sie fest, ob der Benutzer Nicht-MSA-E-Mail-Konten hinzufügen darf.
Microsoft-Kontoverbindung zulassen	Legen Sie fest, ob Sie die Verwendung des MSA-Kontos für nicht E-Mail-bezogene Verbindungsauthentifizierung und -dienste zulassen möchten.
Synchronisieren meiner Einstellungen zulassen	Ermöglicht die Synchronisierung von Einstellungen auf dem gesamten Gerät
Geschützte Domänennamen für Unternehmen	Gibt die durch ";" getrennten Unternehmensdomänennamen an.
Dem Benutzer erlauben, die Systemwiederherstellung zu deaktivieren	Ermöglicht es dem Benutzer, die Systemwiederherstellung zu deaktivieren. **WARNUNG!** Diese Funktion sollte nur auf Geräten verwendet werden, die dem Unternehmen oder der Organisation gehören oder von ihr zur Verfügung gestellt werden, oder auf einem benutzereigenen Gerät, bei dem der Benutzer zustimmt, dass das Gerät vollständig vom Unternehmen verwaltet wird. Wenn Sie diese Richtlinieneinstellung deaktivieren, wird die Systemwiederherstellung ausgeschaltet und der Assistent für die Systemwiederherstellung kann nicht aufgerufen

	werden. Die Option, die Systemwiederherstellung zu konfigurieren oder einen Wiederherstellungspunkt über den Systemschutz zu erstellen, ist ebenfalls deaktiviert.
Benutzerentlassung zulassen	Ermöglicht es dem Benutzer, den Unternehmensteil vom Gerät zu entfernen und damit die Verbindung zu den AppTec360 Servern zu trennen. Sollte dies der Fall sein, ist es nicht mehr möglich, das Gerät zu verwalten. **WARNUNG!** Diese Funktion sollte nur auf Geräten verwendet werden, die dem Unternehmen oder der Organisation gehören oder von ihr zur Verfügung gestellt werden, oder auf einem benutzereigenen Gerät, bei dem der Benutzer zustimmt, dass das Gerät vollständig vom Unternehmen verwaltet wird. Wenn Sie diese Richtlinieneinstellung deaktivieren, können Benutzer keine MDM-Registrierungen entfernen. Geben Sie an, ob der Benutzer das Arbeitsplatzkonto über das Arbeitsplatz-Kontrollzentrum löschen darf. Der MDM-Server konnte das Konto immer aus der Ferne löschen.

BitLocker

BitLocker-Konfiguration

Allgemeine Einstellungen	
Verschlüsselung der Geräte verlangen	Abhängig von der Windows-Edition und der Systemkonfiguration werden die Benutzer möglicherweise aufgefordert, die Geräteverschlüsselung zu aktivieren: - Zur Bestätigung, dass die Verschlüsselung eines anderen Anbieters nicht aktiviert ist. - So deaktivieren Sie BitLocker Drive Encryption und schalten BitLocker wieder ein.
Verschlüsselungsmethoden	
Verschlüsselungsmethode für Betriebssystemlaufwerke	
Verschlüsselungsmethode für feste Datenlaufwerke	
Verschlüsselungsmethode für Wechseldatenträger	
Warnung über Festplattenverschlüsselung von Drittanbietern deaktivieren	Deaktivieren Sie die Warnmeldung über die Verwendung eines Festplattenverschlüsselungsdienstes eines Drittanbieters auf dem Gerät. Ab Windows 10, Version 1803, wird diese Einstellung nur für Geräte unterstützt, die mit Azure Active Directory verbunden sind.
Verschlüsselung zulassen, während ein Nicht-Administrator-Benutzer eingeloggt ist	Nur unterstützt für Geräte, die mit Azure Active Directory verbunden sind

AppTec360 Erweiterungen	
Stille Verschlüsselung	Wenn Sie diese Option zusammen mit "Geräteverschlüsselung anfordern" auswählen, führt der AppTec360 Management Service eine automatische, stille Verschlüsselung der Gerätelaufwerke durch.
Automatisch Benutzeranmeldeinformationen generieren	Das verschlüsselte OS-Laufwerk wird mit automatisch generierten Benutzeranmeldeinformationen geschützt. Entweder eine TPM-PIN, wenn ein TPM verfügbar ist, oder ein 6-stelliges Textpasswort. Die generierten Anmeldedaten werden an die für das Gerät registrierte E-Mail-Adresse gesendet. Wenn diese Option deaktiviert ist, ist der einzig mögliche Schutz für die stille Verschlüsselung die Verwendung des TPM. In diesem Fall schlägt die stille Verschlüsselung bei Geräten ohne TPM fehl.
Feste Laufwerke verschlüsseln	Alle verfügbaren festen Datenlaufwerke werden ebenfalls verschlüsselt und mit einem auf dem Betriebssystemlaufwerk gespeicherten Schlüssel durch "Automatische Entsperrung" geschützt.

OS Laufwerkseinstellungen

Beim Start eine zusätzliche Authentifizierung verlangen	Mit dieser Einstellung können Sie festlegen, ob BitLocker bei jedem Start des Computers eine Authentifizierung verlangt. Diese Einstellung wird während der Einrichtung von BitLocker vorgenommen. Wenn Sie diese Einstellung aktivieren, können Benutzer erweiterte Startoptionen im BitLocker-Einrichtungsassistenten konfigurieren.
BitLocker ohne kompatibles TPM blockieren	
Nur TPM	
TPM und PIN	
TPM und Schlüssel	
TPM, Schlüssel und PIN	Wenn Sie die Verwendung einer PIN und eines USB-Flash-Laufwerks (Schlüssel) vorschreiben möchten, muss der Benutzer BitLocker mit dem

		Befehlszeilentool "manage-bde" anstelle des Assistenten zur Einrichtung der BitLocker-Laufwerksverschlüsselung einrichten.

Mindestlänge der PIN verlangen	
	Minimum Zeichen

Konfigurieren Sie die Pre-Boot-Wiederherstellungsmeldung und die URL	Konfigurieren Sie die gesamte Wiederherstellungsmeldung oder ersetzen Sie die vorhandene URL, die auf dem Bildschirm für die Wiederherstellung vor dem Start angezeigt wird, wenn das Betriebssystemlaufwerk gesperrt ist. Hinweis: Nicht alle Zeichen und Sprachen werden im Pre-Boot unterstützt. Es wird dringend empfohlen, zu testen, ob die von Ihnen verwendeten Zeichen auf dem Pre-Boot-Recovery-Bildschirm korrekt angezeigt werden.
	Option für die Wiederherstellungsmeldung vor dem Start
	Benutzerdefinierte Wiederherstellungsnachricht
	Benutzerdefinierte Wiederherstellungs-URL

Optionen zur Wiederherstellung von OS-Laufwerken	Mit dieser Einstellung können Sie steuern, wie BitLocker-geschützte Betriebssystemlaufwerke wiederhergestellt werden, wenn die erforderlichen Anmeldeinformationen nicht vorhanden sind. Diese Einstellung wird während der Einrichtung von BitLocker vorgenommen. Standardmäßig ist ein zertifikatsbasierter Datenwiederherstellungsagent erlaubt, die Wiederherstellungsoptionen können vom Benutzer festgelegt werden, einschließlich des Wiederherstellungskennworts und des Wiederherstellungsschlüssels, und die Wiederherstellungsinformationen werden nicht in AD DS gesichert.
Blockzertifikat-basierter Datenrettungsagent	Geben Sie an, ob ein Datenwiederherstellungs-Agent mit BitLocker-geschützten Betriebssystemlaufwerken verwendet werden kann. Bevor ein Datenwiederherstellungs-Agent verwendet werden kann, muss er über das Element Public Key Policies entweder in der Verwaltungskonsole für Gruppenrichtlinien oder im Editor für lokale Gruppenrichtlinien hinzugefügt werden. Weitere Informationen zum Hinzufügen von Datenwiederherstellungsagenten finden Sie im BitLocker Drive Encryption Deployment Guide auf Microsoft TechNet.
Einstellungen für das BitLocker-Wiederherstellungskennwort	
Einstellungen für den BitLocker-Wiederherstellungsschlüssel	
BitLocker-Wiederherstellungsinformationen in Active Directory Domain Services speichern	
AD DS BitLocker-Wiederherstellungsspeicher-Konfiguration	Die Speicherung des Schlüsselpakets unterstützt die Wiederherstellung von Daten von einem physisch beschädigten Laufwerk.
Speicherung von Wiederherstellungsdaten in AD DS erforderlich machen	Verhindern Sie, dass Benutzer BitLocker aktivieren, wenn der Computer nicht mit der Domäne verbunden ist und

Feste Laufwerkseinstellungen	
Optionen zur Wiederherstellung von Festplatten	Mit dieser Einstellung können Sie steuern, wie BitLocker-geschützte feste Laufwerke wiederhergestellt werden, wenn die erforderlichen Anmeldeinformationen nicht vorhanden sind. Diese Einstellung wird während der Einrichtung von BitLocker vorgenommen. Standardmäßig ist ein zertifikatsbasierter Datenwiederherstellungsagent erlaubt, die Wiederherstellungsoptionen können vom Benutzer festgelegt werden, einschließlich des Wiederherstellungskennworts und des Wiederherstellungsschlüssels, und die Wiederherstellungsinformationen werden nicht in AD DS gesichert.
Blockzertifikat-basierter Datenrettungsagent	
Einstellungen für das BitLocker-Wiederherstellungskennwort	
Einstellungen für den BitLocker-Wiederherstellungsschlüssel	
BitLocker-Wiederherstellungsinformationen in Active Directory Domain Services speichern	
AD DS BitLocker-Wiederherstellungsspeicher-Konfiguration	Die Speicherung des Schlüsselpakets unterstützt die Wiederherstellung von Daten von einem physisch beschädigten Laufwerk.
Speicherung von Wiederherstellungsdaten in AD DS erforderlich machen	Verhindern Sie, dass Benutzer BitLocker aktivieren, es sei denn, der Computer ist mit der Domäne verbunden und die Sicherung der BitLocker-Wiederherstellungsinformationen in AD DS ist erfolgreich. Hinweis: Das Wiederherstellungspasswort wird automatisch generiert.
Schreibzugriff auf ungeschützte Festplatten verweigern	

Einstellungen für Wechsellaufwerke	
Schreibzugriff auf ungeschützte Wechsellaufwerke verweigern	Verweigern Sie den Schreibzugriff auf Wechseldatenträger, die nicht durch Bitlocker geschützt sind. Hinweis: Wenn "Wechseldatenträger: Schreibzugriff verweigern" in der Gruppenrichtlinie aktiviert ist, wird diese Richtlinieneinstellung ignoriert.
Schreibzugriff auf Geräte verweigern, die in einer	Nur Laufwerke mit Identifikationsfeldern, die mit den Identifikationsfeldern des Computers übereinstimmen, erhalten Schreibzugriff. Diese Felder werden durch die

anderen Organisation konfiguriert wurden	Gruppenrichtlinieneinstellung "Stellen Sie die eindeutigen Identifikatoren für Ihre Organisation bereit" definiert.

BitLocker-Status

Hier sehen Sie den aktuellen Status der mit BitLocker verschlüsselten Laufwerke

C [OS Drive]
Status der Verschlüsselung
Verschlüsselt (%)
Schutzstatus
Verschlüsselungsmethode
Schlüssel-Schutzvorrichtungen
Passwort wiederherstellen

Mit einem Klick auf die Schaltfläche "Wiederherstellungskennwort rotieren" können Sie das BitLocker-Wiederherstellungskennwort rotieren.

Zertifikat Management

Zertifikat Liste

Hier finden Sie eine Liste der Zertifikate, die auf dem angezeigten Gerät installiert sind.

Zertifikat Konfiguration

Hier können Sie Zertifikate konfigurieren und festlegen, wie sie auf dem Gerät installiert werden sollen.

Vertrauenswürdiges Zertifikat	
Beschreibung	Beschreibung des Zertifikats
Umfang	Umfang der Zertifikatsverteilung: Aktueller Benutzer vs. Gerät
Zertifikatsspeicher	"Nicht vertrauenswürdige Zertifikate" ist erst ab Windows 10, Version 1803 verfügbar
Zertifikatsdatei	Hochladen einer PKCS#1-Datei

Identitätsnachweis			
Beschreibung	Beschreibung des Zertifikats		
Umfang	Umfang der Zertifikatsverteilung: Aktueller Benutzer vs. Gerät		
Wichtige Lage	Der Schlüsselspeicheranbieter, auf dem der private Schlüssel installiert werden soll.		
		TPM. Fehlgeschlagen, wenn kein TPM vorhanden	
	TPM. Wenn kein TPM vorhanden ist, wird auf Software-KSP zurückgegriffen.		
	Software-Schlüsselspeicheranbieter		Privaten Schlüssel als exportierbar markieren
	Windows Hello für Unternehmen	Name des Containers	Gibt den Containernamen für Windows Hello for Business (früher bekannt als Microsoft Passport for Work) an.
		PIN-Abfragetext	Gibt den benutzerdefinierten Text an, der bei der Zertifikatsregistrierung auf der Windows Hello for Business PIN-Eingabeaufforderung angezeigt werden soll.

Berechtigungsnachweis	Hochladen einer PKCS#12-Datei

SCEP

Beschreibung	SCEP Server Beschreibung		
Umfang des Einsatzes	Umfang der Zertifikatsverteilung: Aktuelles Gerät vs. Benutzer		
SCEP-Server-URLs	Ein oder mehrere Server, die Zertifikate über SCEP ausstellen		
Thema	Darstellung eines X.500-Namens. Z.B. "C=US, O=Microsoft Corporation, CN=foo, 1.2.5.3=bar"		
Betreff alternative Namen	Typ	E-Mail Adresse	
		DNS	
		URI	
		Benutzerprinzipalname (UPN)	
CA Fingerabdruck	Der SHA1-Fingerabdruck des Zertifikats der Zertifizierungsstelle. E.g. 31:8F:1E:78:5C:D5:12:9F:7E:3B:AD:F3:1C:C0:19:03:96:43:A9:E5		
Gültigkeitsdauer Einheiten	Tage, Monate oder Jahre		
Gültigkeitsdauer			
Herausforderung	Wird als Pre-Shared Secret für die automatische Anmeldung verwendet		
Wiederholungen	Die Anzahl der Versuche, die das Gerät wiederholen soll, wenn der Server eine PENDING-Antwort sendet. Der Standardwert ist 5. Der maximale Wert ist 30.		
Wiederholungsverzögerung	Anzahl der Minuten, die vor einem erneuten Versuch gewartet werden soll. Der Standardwert ist 5. Der Mindestwert ist 1.		
Schlüsselgröße	Schlüsselgröße in Bits		
Hash-Algorithmus	Familie der Hash-Algorithmen		
Wichtige Verwendung	Die Schlüsselverwendungserweiterung definiert den Zweck (z. B. Verschlüsselung, Signatur) des im Zertifikat enthaltenen Schlüssels. Mindestens eine der Optionen "Digitale Signatur" oder "Schlüsselverschlüsselung" muss ausgewählt werden.		
Erweiterte Schlüsselverwendung	Legt erweiterte Schlüsselverwendung fest, abhängig von der SCEP-Serverkonfiguration. Geben Sie die Liste der entsprechenden OIDs an, z. B. 1.3.6.1.5.5.7.3.2 (Client-Authentifizierung)		
Wichtige Lage	Der Schlüsselspeicheranbieter, auf dem der private Schlüssel installiert werden soll.		
		TPM. Fehlgeschlagen, wenn kein TPM vorhanden	

	TPM. Wenn kein TPM vorhanden ist, wird auf Software-KSP zurückgegriffen.			
	Software-Schlüsselspeicheranbieter			
	Windows Hello für Unternehmen	Name des Containers	Gibt den Containernamen für Windows Hello for Business (früher bekannt als Microsoft Passport for Work) an.	
		PIN-Abfragetext	Gibt den benutzerdefinierten Text an, der bei der Zertifikatsregistrierung auf der Windows Hello for Business PIN-Eingabeaufforderung angezeigt werden soll.	

Verbindungsmanagement

Wifi

Bei dieser Einstellung führen Sie die Vorkonfiguration der Endbenutzergeräte für den Zugriff auf interne Access Points durch

Service Set Identifier (SSID)	SSID des Netzwerks, zu dem die Verbindung hergestellt werden soll
Auto Join	Aktivieren Sie die automatische Verbindung zum Netzwerk
Verborgenes Netzwerk	Aktivieren, für den Fall, dass der AP die SSID nicht sendet

Sicherheit Typ

AP-Sicherheitstyp einrichten

WEP Offenes System	
Passwort	Passwort für den AP

WPA PSK	
Passwort	Passwort für den AP

WPA EAP	
Art der Authentifizierung	Authentifizierungstyp, nur möglich mit "PEAP-MSCAHPv2".
Schnelles Wiederverbinden	Geräte können zwischen Access Points wechseln, ohne sich erneut authentifizieren zu müssen
Gastzugang	Der Benutzer hat kein Konto und sollte sich daher als Gast registrieren
Quarantäne-Kontrollen	Der Client muss NAP-Checks (Network Access Protection) durchführen und die Ergebnisse an das System weitergeben, das dann entscheidet, ob der Client eine Verbindung herstellen kann.
Krypto-Bindung erforderlich machen	Authentifizierung ist nur über Crypto Binding möglich
Server-Validierung	Der Client überprüft, ob das Serverzertifikat gültig ist. Wenn dies der Fall ist, wird eine Verbindung hergestellt
Aufforderung zur Vorlage von Zertifikaten	Ermöglicht es dem Benutzer, nicht vertrauenswürdige Zertifikate zu akzeptieren
Server-Namen	Bietet die Möglichkeit, den Namen des RADIUS-Servers anzuzeigen, der die Netzwerkauthentifizierung und -autorisierung anbietet

WPA2-PSK	
Passwort	AP-Kennwort

WPA2 EAP	
Art der Authentifizierung	Authentifizierungstyp, nur möglich mit "PEAP-MSCAHPv2".
Schnelles Wiederverbinden	
Gastzugang	
Quarantäne-Kontrollen	Aktiviert den Netzwerkzugriffsschutz NAP
Krypto-Bindung erforderlich machen	Authentifizierung ist nur über Crypto Binding möglich
Server-Validierung	
Aufforderung zur Vorlage von Zertifikaten	Fragt nach einem validierten Serverzertifikat, Namen oder einer Root-Zertifikat-Authentifizierung (CA)
Server-Namen	Auflistung der Server, die von den Geräten als vertrauenswürdig eingestuft werden sollen
Keine	Keine etablierte Sicherheit
Proxy-Server verwenden	Verwendung eines Proxyservers
Server Adresse	Adresse des Proxy-Servers
Server-Anschluss	Server-Port des Proxy-Servers

Proxy-Server verwenden

Aktivieren Sie die Verwendung des Proxyservers.

Server Adresse	Von diesem Netzwerk verwendete Proxy-Server-Adresse.
Server-Anschluss	Proxy-Server-Port, der von diesem Netzwerk verwendet wird.

Wifi-Einschränkungen

Hier können Sie verschiedene Wifi-Einschränkungen festlegen.

WiFi zulassen	WiFi zulassen/verweigern
Internetfreigabe zulassen	Verwendung eines Hotspots zulassen
Automatische Verbindung zu WiFi Sense Hot Spots zulassen	Automatische Verbindung zu WiFi Sense Hot Spots zulassen
Manuelle WiFi-Konfiguration zulassen	Dem Benutzer erlauben, sich mit WiFi-Netzwerken zu verbinden, die nicht von AppTec definiert wurden
WLAN-Suchlauffrequenz	Legt das WLAN-Scan-Intervall fest. Hier erhöht ein höherer Wert die Fähigkeit, WIFI-Netzwerke zu erkennen.

VPN

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

Name der Verbindung	Angezeigter Verbindungsname		
VPN-Typ	Eine Pro-App-VPN-Verbindung wird verwendet, um den Datenverkehr bestimmter Apps zu sichern.		
	VPN	Immer eingeschaltet	Dadurch wird das VPN bei der Anmeldung automatisch verbunden und bleibt verbunden, bis der Benutzer die Verbindung manuell trennt.
	Pro-App VPN	VPN-Apps	Definieren Sie Apps, die diese VPN-Verbindung verwenden
		Sperrung pro App	Per-App Lockdown können die ausgewählten Apps nur über diese VPN-Verbindung eine Verbindung herstellen. Diese Funktion hängt von der Windows Defender Firewall ab.
	WIP-Profil	WIP-Domäne für diese Verbindung	Unternehmens-ID, die für die Verbindung dieses VPN-Profils mit einer Windows Information Protection (WIP)-Richtlinie erforderlich ist

Verbindungstyp

AppTec360 VPN	
Für "AppTec360 VPN" ist es erforderlich, dass App-Sideloading erlaubt ist. Bitte aktivieren Sie "Sideloading von Apps zulassen" unter "Sicherheitsmanagement" → "Einstellungen für Einschränkungen" → "Gerätefunktionen".	
Gateway-Konfiguration	Um eine VPN-Verbindung mit Blacklisting zu konfigurieren, wählen Sie bitte eine VPN-Konfiguration mit einem bestimmten DNS-Server. Sie können eine VPN-Konfiguration unter "Allgemeine Einstellungen" → "Universal Gateway" → "VPN-Einstellungen" einrichten.

IKEv2		
Server	Liste der VPN-Server	
Gerätetunnel	Aktivieren Sie die Verbindung vor der Benutzeranmeldung.	
Methode zur Authentifizierung	EAP	EAP XML
	Maschinen-Zertifikate	
Verschlüsselungsalgorithmus		
Algorithmus zur Integritätsprüfung		
Diffie-Hellman-Gruppe		
Algorithmus zur Chiffriertransformation		
Algorithmus zur Authentifizierungstransformation		
Perfektes Vorwärtsgeheimnis (PFS) Gruppe		

PPTP		
Server	Liste der VPN-Server	
Methode zur Authentifizierung	EAP	EAP XML

L2TP		
Server	Liste der VPN-Server	
Methode zur Authentifizierung	EAP	EAP XML
Verschlüsselungsalgorithmus		
Algorithmus zur Integritätsprüfung		
Diffie-Hellman-Gruppe		
Algorithmus zur Chiffriertransformation		
Algorithmus zur Authentifizierungstransformation		
Perfektes Vorwärtsgeheimnis (PFS) Gruppe		

Automatisch		
Server	Liste der VPN-Server	
Methode zur Authentifizierung	EAP	EAP XML

Allgemeine VPN-Konfigurationen

Anmeldedaten bei jeder Anmeldung speichern	
IP-Adressen bei internem DNS registrieren	
Regeln zur Filterung des Netzwerkverkehrs	Beschränken Sie die VPN-Verbindung auf die definierten Regeln.
DNS-Suffix-Suchliste	DNS-Suffixe, die der DNS-Suchliste für das Routing von Kurznamen hinzugefügt werden sollen.
Regeln für die Tabelle der Namensauflösungsrichtlinien (NRPT)	Die NRPT-Regeln (Name Resolution Policy table) legen fest, wie der DNS Namen auflöst, wenn eine Verbindung zum VPN besteht.
Erkennung vertrauenswürdiger Netzwerke	Liste der DNS-Suffixe zur Identifizierung des vertrauenswürdigen Netzwerks.
Geteilter Tunnelbau	Split-Tunneling bedeutet, dass der Datenverkehr über eine beliebige, vom Netzwerk-Stack festgelegte Schnittstelle laufen kann.
Split-Tunneling-Routen	Liste der Routen, die der Routing-Tabelle für die VPN-Schnittstelle hinzugefügt werden sollen.
Proxy-Einrichtung	Konfiguriert den für dieses Netzwerk verwendeten Proxy
Proxy Adresse	Die Adresse des Proxy-Servers als vollständig qualifizierter Hostname oder als IP-Adresse.
Hafen	Port des Proxy-Servers.
Proxy Auto-Konfigurations-URL	URL, um die Proxy-Einstellungen automatisch abzurufen.

VPN-Einschränkungen

Hier können Sie verschiedene VPN-Einschränkungen festlegen.

VPN-Einstellungen zulassen	Diese Richtlinie erlaubt/verwehrt es dem Benutzer, die VPN-Einstellungen zu deaktivieren und zu ändern
VPN über das Mobilfunknetz zulassen	Erlaubt/verbietet dem Gerät, eine VPN-Verbindung aufzubauen, wenn das Gerät mobile Daten verwendet
VPN-Roaming über Mobilfunk zulassen	Erlaubt/verbietet dem Gerät, eine VPN-Verbindung aufzubauen, wenn das Gerät roamt

Bluetooth

Hier können Sie festlegen, ob Bluetooth erlaubt/verboten sein soll.

Bluetooth zulassen	Aktivieren/Deaktivieren von Bluetooth

PIM-Verwaltung

Exchange Active Sync

Einrichten des ActiveSync-Kontos auf dem Endgerät

Konto Name	Name des E-Mail-Kontos
Server-Hostname	Server-Adresse/FQDN
Domain-Name	Server-Domäne
E-Mail Adresse	E-Mail Adresse
Benutzer Name	Name des Benutzers
Benutzer-Passwort	Optional können Sie dem Benutzer hier bereits ein Passwort zuweisen
SSL verwenden	SSL-Verbindung verwenden
Sync-Intervall	Hier kann das Synchronisationsintervall festgelegt werden Manuelle Synchronisierung = Der Benutzer muss seine E-Mails herunterladen und eine manuelle Synchronisierung durchführen.
Mail-Altersfilter	Zeitspanne, bis die Emails synchronisiert werden sollen Kein Filter = unbegrenzt
Log Level	Festlegung der Protokollierungsstufen für den ActiveSync-Datenverkehr
E-Mail synchronisieren	Aktiviert = E-Mails werden synchronisiert
Kontakte synchronisieren	Aktiviert = Kontakte werden synchronisiert
Kalender synchronisieren	Aktiviert = Kalender wird synchronisiert
Aufgaben synchronisieren	Aktiviert = Aufgaben werden synchronisiert

eMail

Einrichtung von POP3/IMAP4-Konten auf dem Endbenutzergerät.

Konto Beschreibung	Name des E-Mail-Kontos
Absender Name	Angezeigter Absendername
Domain-Name	Domänenname für das E-Mail-Konto
E-Mail Adresse	Benutzer-E-Mail-Adresse
Benutzer Name	Name des Benutzers
Benutzer-Passwort	Optional können Sie dem Benutzer hier bereits ein Passwort zuweisen
Alternative Anmeldeinformationen für ausgehende Server	Hier kann festgelegt werden, ob für den Ausgangsserver weitere Anmeldeinformationen erforderlich sind
Ausgehender Domainname	Ausgehender Domainname
Ausgehender Server-Benutzername	Benutzername des ausgehenden Servers
Passwort für den Ausgangsserver	Passwort des Ausgangsservers
E-Mail-Protokoll	POP3 oder IMAP4, kann als Protokoll verwendet werden
Hostname des Posteingangsservers	Hostname des Posteingangsservers
Verwenden Sie SSL für eingehende Mails	Verwenden Sie SSL für eingehende Emails
Hostname des Postausgangsservers	Hostname des Postausgangsservers
Verwenden Sie SSL für ausgehende Mails	Verwenden Sie SSL für ausgehende E-Mails
Authentifizierung ausgehender Server	Eine Authentifizierung des ausgehenden Servers ist erforderlich
Sync-Intervall	Hier kann das Synchronisationsintervall festgelegt werden Manuelle Synchronisierung = Der Benutzer muss seine E-Mails herunterladen und eine manuelle Synchronisierung durchführen.
Mail-Altersfilter	Zeitspanne, bis die Emails synchronisiert werden sollen Kein Filter = unbegrenzt

App Verwaltung

Enterprise App Manager

Installierte Apps

Hier finden Sie eine Liste der Apps, die derzeit auf dem angezeigten Gerät installiert sind.

Obligatorische Apps

Hier können Sie eine Liste von Apps konfigurieren, die auf dem Gerät obligatorisch sind.

Diese Liste wird jedes Mal überprüft, wenn das Gerät eine Verbindung zum MDM herstellt, und installiert alle Apps auf dieser Liste, die nicht auf dem Gerät installiert sind, unabhängig davon, ob die App deinstalliert wurde oder noch nie installiert war.

Sie können Windows 10 In-House Apps hochladen und sie dann zu dieser Liste hinzufügen oder Sie können Microsoft Office-Konfigurationen hinzufügen, die zuvor unter "Allgemeine Einstellungen" > "App-Verwaltung" > "Microsoft Office" konfiguriert werden müssen.

Sys App-Einschränkungen

Posteingang Apps
Alarme und Uhr zulassen
Taschenrechner zulassen
Kamera zulassen
Erlauben Sie Kontakt-Support
Cortana zulassen
Datei-Explorer zulassen
Erlauben Sie Get Started
Groove Musik zulassen
Karten zulassen
Messaging zulassen
Microsoft Edge zulassen
Erlauben Sie Filme und Fernsehen
Geld zulassen
Nachrichten zulassen
OneDrive zulassen
OneNote zulassen
Outlook Kalender und Mail zulassen
Menschen zulassen
Telefon zulassen
Fotos zulassen
Powerpoint zulassen
Einstellungen zulassen
Skype zulassen
Erlauben Sie Sport
Laden zulassen
Sprachrekorder zulassen
Brieftasche zulassen
Wetter zulassen

Windows Feedback Hub zulassen
Wort zulassen
Xbox zulassen

Seiten einstellen
Konten zulassen Arbeitsplatz
Erweiterte Informationen zulassen
Apps zulassen Ecke
Blockieren und Filtern zulassen
Farbprofil zulassen
Fahrmodus zulassen
E-Mail und Konten zulassen
Equalizer zulassen
Tastatur zulassen
Navigationsleiste zulassen
Netzwerk-Flugzeugmodus zulassen
Netzwerk-Internetfreigabe zulassen
Netzwerkdienste zulassen
Netzwerk Wi-Fi zulassen
PC-System-Bluetooth zulassen
Lassen Sie Ihr Gerät bewerten
Update wiederherstellen zulassen
Freigabe erlauben
Start zulassen
Zeit zulassen Sprache
Zeit zulassen Region
Windows-Standardsperrbildschirm zulassen
Konto für Arbeit oder Schule zulassen

Black- & Whitelisting

Unter "Black- & Whitelisting" können Sie zwischen dem Modus "Whitelist" und dem Modus "Blacklist" wählen.

Whitelist	Nur Apps und Dienste, die der Liste hinzugefügt werden, können auf dem Endgerät des Benutzers installiert werden. Wenn diese bereits auf dem Endbenutzergerät vorinstalliert sind, werden sie aktiviert und so eingestellt, dass der Benutzer sie ausführen kann.
	Alle anderen Apps, die nicht zur Liste hinzugefügt werden, können nicht auf dem Endgerät des Benutzers installiert werden. Wenn diese bereits auf dem Endbenutzergerät vorinstalliert sind, werden sie deaktiviert und so eingestellt, dass der Benutzer sie nicht ausführen kann.
Schwarze Liste	Apps und Dienste, die der Liste hinzugefügt werden, können nicht auf dem Endgerät des Benutzers installiert werden. Wenn diese bereits auf dem Endbenutzergerät vorinstalliert sind, werden sie deaktiviert und so eingestellt, dass der Benutzer sie nicht ausführen kann.
	Alle anderen Apps, die nicht zur Liste hinzugefügt werden, können auf dem Endgerät des Benutzers installiert werden. Wenn diese bereits auf dem Endbenutzergerät vorinstalliert sind, werden sie aktiviert und so eingestellt, dass der Benutzer sie ausführen kann.

Über die Taste , fügen Sie der aktuell verwendeten Liste weitere Apps oder Dienste hinzu.

Über die Taste , fügen Sie der derzeit inaktiven Liste weitere Apps oder Dienste hinzu.

Sie können entweder eine App aus dem "Windows App Store" hinzufügen oder direkt eine "App-Kennung" eingeben, um sie der Black- oder Whitelist hinzuzufügen.

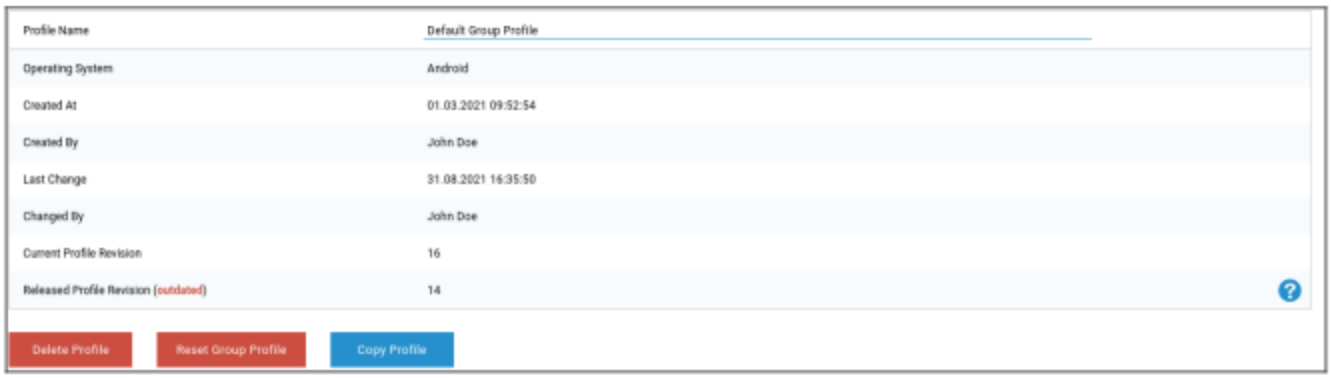
MacOS Konfiguration

Je nachdem, ob Sie ein Profil oder ein Gerät ausgewählt haben, sind die Anzeige und ihre Unterpunkte unterschiedlich - bitte beachten Sie dies genau!

Allgemein

Gruppenprofilübersicht (nur auf Gruppenebene)

Wenn Sie ein Gruppenprofil öffnen, erhalten Sie einen schnellen Überblick über das Profil.



Profil Name	Name des Profils (kann hier geändert werden)
Betriebssystem	Betriebssystem, für das das Profil bestimmt ist
Erstellt am	Zeitpunkt der Erstellung
Erstellt von	Der Ersteller des Profils
Letzte Änderung	Zeitpunkt der letzten Änderung des Profils
Geändert von	Konto, das die letzten Änderungen vorgenommen hat
Aktuelle Profilüberarbeitung	Revision des gespeicherten Profilstatus
Freigegebene Profil-Revision	Zugewiesene Profilrevision ("Jetzt zuweisen"). Wenn das Etikett hinter dem Text "(veraltet)" anzeigt, bedeutet dies, dass Sie das Profil zwar gespeichert, aber noch nicht zugewiesen haben, so dass die Geräte noch eine ältere Version erhalten.

Geräteübersicht (nur auf Geräteebene)

Die zusammengefasste Übersicht des Geräts.

Gerät Name	Name des Geräts
Modell	Modell
Betriebssystem	Betriebssystem
Seriennummer	Seriennummer des Geräts
Geräteeigentum	Der konfigurierte Ownership-Typ
Gerätetyp	Der Typ des Geräts
Konform	Zeigt an, ob das Gerät konform ist
IP-Adresse	Die IP-Adresse, über die das Gerät mit dem Server verbunden ist
Zuletzt gesehen	Zeitpunkt der letzten Verbindung vom Gerät
Letzter Schub	Zeitpunkt des letzten an das Gerät gesendeten Push
Zuweisung	Hier können Sie das Gerät einem anderen Benutzer oder einer Gruppe zuweisen

Config Revision (nur auf Geräteebene)

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

Wenn Sie auf das Gruppenprofil klicken, haben Sie direkten Zugriff auf das Profil und können Einstellungen vornehmen.

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

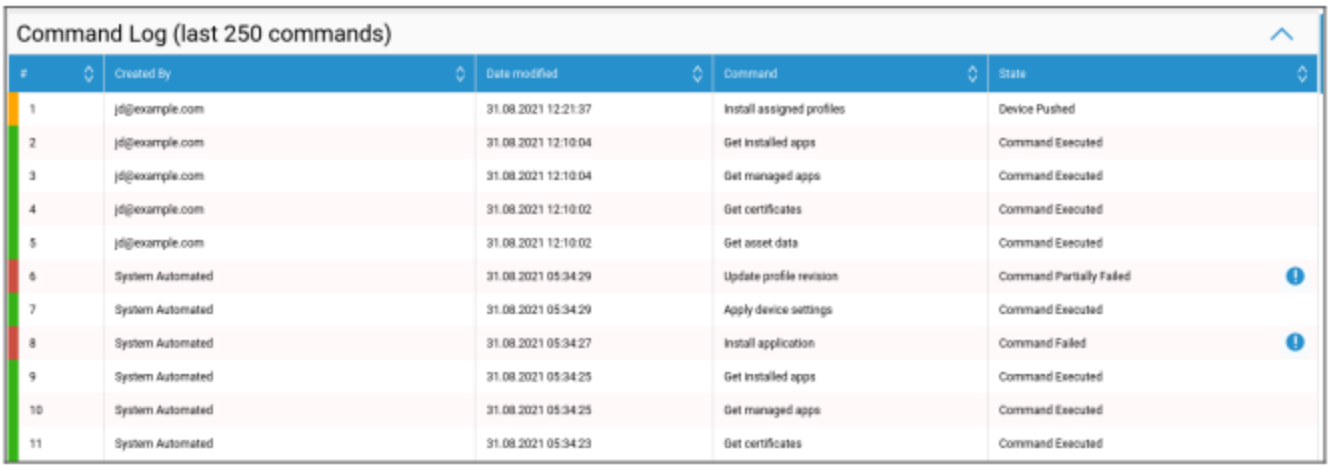
Mit dem Symbol können Sie das Geräteprofil so zurücksetzen, dass es keinerlei Einstellungen enthält.

"Neuere Revision verfügbar" bedeutet, dass das Gruppenprofil geändert und gespeichert, aber nicht zugewiesen wurde. Das Gruppenprofil muss mit "Jetzt zuweisen" auf Gruppenebene zugewiesen werden, um die Änderungen auf die Geräte anzuwenden.

Geräteprotokoll (nur auf Geräteebene)

Befehl Log

Hier können Sie sehen, welche Befehle für das Gerät erteilt wurden und welchen Status sie haben.



Mit "System Automated" erstellte Befehle werden automatisch vom System erstellt.

Mögliche Befehlszustände

Gerät geschoben	Eine Push-Anfrage wurde an den Push-Dienst (z.B. APNS) gesendet, um das Gerät anzuweisen, sich wieder mit dem EMM-Server zu verbinden.
Befehl erstellt	Der Befehl wurde im System erstellt.
Befehl gesendet	Der Befehl wurde an das Gerät gesendet, nachdem es sich mit dem Server verbunden hat.
Befehl Ausgeführt	Der Befehl wurde erfolgreich ausgeführt.
Befehl fehlgeschlagen	Der Befehl ist fehlgeschlagen. *
Befehl Teilweise fehlgeschlagen	Je nach Betriebssystem des Geräts können einige Befehle in Gruppen zusammengefasst werden. Dabei sind einige Teile dieser Befehlsgruppe fehlgeschlagen. *
Befehl ausgeführt, eventuell fehlgeschlagen	Der Befehl wurde ausgeführt, aber vielleicht auch nicht.
Kommando zurückgeschoben	Der Befehl wurde von einem Benutzer erneut gesendet.
Weggeworfen	Der Befehl wurde verworfen. Zum Beispiel, weil er durch einen anderen Befehl ersetzt wurde oder das Gerät neu registriert wurde und alte Befehle entfernt wurden

*Wenn sich hinter der Nachricht ein Ausrufezeichen befindet, erhalten Sie weitere Informationen, indem Sie mit dem Mauszeiger über das Symbol fahren.

Asset Management (nur auf Geräteebene)

Geräte-Infos

Modellnummer	Modellnummer
Hostname	Hostname
Lokaler Hostname	Lokaler Hostname
Betriebssystem	Betriebssystem
OS Version	OS-Version
UDID	UDID
Freier / Gesamter Speicher	Freier / Gesamter Speicher

WiFi

IP-Adresse	IP-Adresse
WiFi MAC	WiFi MAC

Zellulär

Telefon Nummer	Telefon Nummer
Roaming-Status	Roaming-Status
Roaming (Sprache/Daten)	Roaming (Sprache/Daten)
IP-Adresse	IP-Adresse
Betreiber/Transporteur	Betreiber/Transporteur
SIM-Betreiber Netzwerk	Trägernetzwerk
Carrier Version	Carrier Version
ICCID	ICCID
Aktuelle MCC/MNC	Aktuelle MCC/MNC
SIM MCC/MNC	SIM MCC/MNC

Bluetooth

Bluetooth MAC	Bluetooth MAC

Update Management (nur auf Geräteebene)

Infos aktualisieren

Diese Registerkarte enthält Informationen zu den Einstellungen für die Systemaktualisierung auf dem Gerät.

Autocheck aktiviert	Wenn das System automatisch nach Updates sucht.
Automatische App-Aktualisierung aktiviert	Wenn das System App-Updates automatisch installieren soll.
Automatische OS-Updates aktiviert	Wenn das System Betriebssystem-Updates automatisch installieren soll.
Automatische Sicherheitsupdates aktiviert	Wenn das System Sicherheitsupdates automatisch installiert.
App Update Hintergrund-Download aktiviert	Wenn das System App-Updates im Hintergrund herunterladen soll.
Katalog-URL	Die URL zum Software-Update-Katalog, den der Client verwendet.
Ist Standardkatalog	Wenn "ja", ist Katalog der Standardkatalog.
Regelmäßige Überprüfung durchführen	Wenn "ja", starten Sie einen neuen Suchlauf.
Vorheriges Scan-Datum	Das Datum des letzten Software-Update-Scans.
Vorheriges Scan-Ergebnis	Der Ergebniscode des letzten Software-Update-Scans.

Sicherheitsmanagement

Anti-Diebstahl

Wischen & Sperren

Vollständig abwischen	Senden Sie einen Befehl zum Zurücksetzen des Geräts auf die Werkseinstellungen
Enterprise Wipe	Entfernen Sie das MDM vom Gerät und entfernen Sie alle MDM-Daten (z.B. Konten, Apps)
Sperrbildschirm	Das Gerät wieder auf den Sperrbildschirm bringen

Sicherheitskonfiguration

Passcode

Code-Deaktivierung erlaubt	Legt fest, ob der Benutzer gezwungen wird, eine PIN festzulegen. Die einfache Einstellung dieses Wertes (und nicht anderer) zwingt den Benutzer zur Eingabe eines Passcodes, ohne eine Länge oder Qualität vorzuschreiben.
Einfachen Wert zulassen	Erlauben Sie dem Benutzer, die gleichen, eskalierenden und reduzierenden Nummernfolgen zu verwenden (z.B. 1234, 1111)
Alphanumerischer Wert erforderlich	Passwörter müssen mindestens einen Buchstaben enthalten
Mindestlänge des Passcodes	Minimale Passwortlänge
Mindestanzahl von komplexen Zeichen	Minimale Anzahl von alphanumerischen Symbolen im Passwort
Maximales Alter des Passcodes	Anzahl der Tage, nach denen das Passwort geändert werden muss
Maximum Auto-Lock	Maximale Zeit, nach der das Gerät gesperrt wird
Maximale Karenzzeit für die Gerätesperre	Zeitspanne, in der das Gerät gesperrt werden kann, ohne dass bei der Entsperrung ein Passcode abgefragt wird
Maximales Alter des Passcodes (1-730 Tage, oder keine)	Tage, nach denen der Passcode geändert werden muss
Passcode-Historie (1-50 Passcodes, oder keine)	Anzahl der eindeutigen Passcodes vor der Wiederverwendung

Zertifikat

PKCS#1	
Beschreibung	Geben Sie eine Beschreibung für das Zertifikat ein
Berechtigungsnachweis	Eine pkcs1 Datei hochladen

PKCS#12	
Beschreibung	Geben Sie eine Beschreibung für das Zertifikat ein
Berechtigungsnachweis	Eine pkcs12 Datei hochladen

Einstellungen zur Einschränkung

Gerätefunktionalität

Kamera zulassen	Erlauben Sie die Verwendung der Kamera
Game Center zulassen	Wenn die Einstellung falsch ist, wird Game Center deaktiviert und sein Symbol wird vom Startbildschirm entfernt.
Erlauben Sie Multiplayer-Spiele	Wenn falsch, wird das Spielen im Mehrspielermodus verboten.
Hinzufügen von Game Center Freunden zulassen	Wenn falsch, wird das Hinzufügen von Freunden zu Game Center verboten.
iCloud-Fotomediathek zulassen	Wenn diese Option auf false gesetzt ist, wird die iCloud Photo Library deaktiviert. Alle Fotos, die nicht vollständig aus der iCloud-Fotomediathek auf das Gerät geladen wurden, werden aus dem lokalen Speicher entfernt.
Touch ID zulassen	Wenn falsch, wird verhindert, dass Touch ID ein Gerät entsperrt.

iCloud

Blockieren bestimmter Funktionen während der iCloud-Kopplung

Synchronisierung von Dokumenten zulassen	Synchronisierung von Dokumenten zulassen
iCloud Schlüsselbund-Synchronisierung zulassen	iCloud Schlüsselbund-Synchronisierung zulassen
iCloud-Notizen zulassen	Wenn falsch, werden die MacOS iCloud Notes-Dienste deaktiviert.
iCloud BTMM zulassen	Wenn falsch, wird der MacOS Back to My Mac iCloud-Dienst deaktiviert.
iCloud FMM zulassen	Wenn falsch, wird der MacOS Find My Mac iCloud-Dienst deaktiviert.
iCloud-Lesezeichen zulassen	Wenn falsch, wird die MacOS iCloud Lesezeichen-Synchronisierung deaktiviert.
iCloud Mail zulassen	Wenn falsch, werden die iCloud-Dienste von MacOS Mail deaktiviert.

iCloud-Kalender zulassen	Wenn falsch, werden die iCloud-Dienste von MacOS Cloud deaktiviert.
iCloud-Erinnerungen zulassen	Wenn falsch, werden die iCloud-Erinnerungsdienste deaktiviert.
iCloud-Adressbuch zulassen	Wenn falsch, werden die MacOS iCloud-Adressbuchdienste deaktiviert.

Medienmanagement

Auswerfen bei Abmeldung	Alle Wechselmedien beim Abmelden auswerfen
Netzwerk zulassen	Zugriff für Netzwerkmedien zulassen
Interne Festplatte zulassen	Erlauben Sie den Zugriff auf die interne Festplatte.
Authentifizierung verlangen	Authentifizierung für die Verwendung dieses Mediums erforderlich machen
Nur lesen	Der Benutzer kann nur Daten von den Medien lesen
Externe Festplatte zulassen	Zugriff für externe Festplatte zulassen.
Authentifizierung verlangen	Authentifizierung für die Verwendung dieses Mediums erforderlich machen
Nur lesen	Der Benutzer kann nur Daten von den Medien lesen
Verwendung von Disk Images zulassen	Zugriff für Bilder zulassen.
Authentifizierung verlangen	Authentifizierung für die Verwendung dieses Mediums erforderlich machen
Nur lesen	Der Benutzer kann nur Daten von den Medien lesen
Verwendung von DVD-RAMs zulassen	Zugriff für DVD-RAM-Datenträger zulassen.
Authentifizierung verlangen	Authentifizierung für die Verwendung dieses Mediums erforderlich machen
Nur lesen	Der Benutzer kann nur Daten von den Medien lesen
Erlauben Sie die Verwendung von DVDs	Zugriff für DVD-Diskette zulassen.
Authentifizierung verlangen	Authentifizierung für die Verwendung dieses Mediums erforderlich machen
Erlauben Sie die Verwendung von CDs	Zugriff für CD-Diskette zulassen.
Authentifizierung verlangen	Authentifizierung für die Verwendung dieses Mediums erforderlich machen

Verbindungsmanagement

Wi-Fi

Hier können Sie Wi-Fi-Verbindungen hinzufügen und konfigurieren

Service Set Identifier (SSID)	SSID des Netzwerks, zu dem die Verbindung hergestellt werden soll
Auto Join	Aktivieren Sie den automatischen Beitritt für das Netzwerk
Verborgenes Netzwerk	Aktivieren, für den Fall, dass der AP die SSID nicht sendet
Proxy-Einrichtung	Konfigurieren eines Proxys für jeden Access Point
Keine	Verwenden Sie keinen Proxy-Server
Handbuch	Einen manuellen Proxy einrichten
Proxy-Server-URL	Adresse für den Zugriff auf die Proxy-Einstellungen
Hafen	Legen Sie den Port für den Proxy fest
Authentifizierung	Benutzernamen für die Authentifizierung auf dem Proxy
Passwort	Passwort für die Authentifizierung auf dem Proxy
Automatisch	Automatisch einen Proxy einrichten
Proxy-Server-URL	URL für die Proxy-Einstellungsdatei
Sicherheit Typ	Sicherheitstyp für den AP einrichten
WEP	
Passwort	Passwort für den AP
WPA/WPA2	
Passwort	Passwort für den AP
WEP Unternehmen - WPA / WPA2 Unternehmen / Jedes Unternehmen	Siehe Tabelle Fehler: Verweisquelle unten nicht gefunden
Keine	Keine Sicherheit einrichten
MAC-Adress-Randomisierung deaktivieren	Deaktiviert die Zufallsgenerierung der MAC-Adresse für dieses Wi-Fi-Netzwerk, während es mit dem Netzwerk verbunden ist. Außerdem wird in den Einstellungen eine Datenschutzwarnung angezeigt, die darauf hinweist, dass das Netzwerk den Schutz der Privatsphäre reduziert hat.

Wi-Fi-Konfiguration für Unternehmen

Hinweis: Nur verfügbar, wenn "Sicherheitstyp" auf einen Unternehmenstyp eingestellt ist.

Protokolle	Im Zielnetzwerk unterstütztes Authentifizierungsprotokoll
TLS	Aktivieren / Deaktivieren Verwendung
TTLS	Aktivieren / Deaktivieren Verwendung
Innere Authentifizierungen	Authentifizierungsprotokoll, das verwendet werden soll: PAP, CHAP, MSCHAP, MSCHAPv2
LEAP	Aktivieren / Deaktivieren Verwendung
PEAP	Aktivieren / Deaktivieren Verwendung
EAP-FAST	Aktivieren / Deaktivieren Verwendung
EAP-SIM	Aktivieren / Deaktivieren Verwendung
PAC verwenden	Verwendung von PAC (Protected Access Control)
Rückstellung PAC	Konfiguration der Provision PAC
Anonyme Bereitstellung von PAC	Anonyme Bereitstellung von PAC
Authentifizierung	
Benutzername	Benutzername für die Authentifizierung
Verwenden Sie nicht Pro Verbindung Passwort	Verwenden Sie kein Passwort pro Verbindung
Passwort	Das zu verwendende Passwort
Identitätszertifikat	Authentifizierungszertifikat hochladen/auswählen
Äußere Identität	Identität, die von außen sichtbar ist
Vertrauen Sie	
Vertrauenswürdiges Zertifikat 1	Erstes vertrauenswürdiges Zertifikat hochladen
Vertrauenswürdiges Zertifikat 2	Zweites vertrauenswürdiges Zertifikat hochladen
Vertrauenswürdiges Zertifikat 3	Drittes vertrauenswürdiges Zertifikat hochladen
Vertrauenswürdiger Server	Die Namen der erwarteten Serverzertifikate

Zertifikat-Namen	(in einer durch Komma getrennten Liste)

VPN

Je nach ausgewähltem Verbindungstyp können unterschiedliche Felder sichtbar sein.

Name der Verbindung	Name des VPN-Profils
VPN-Typ	
VPN	Der gesamte Netzwerkverkehr des Geräts wird über eine VPN-Verbindung geleitet.
Verbindungstyp	VPN-Verbindungstyp einrichten
IPsec (cisco)	IPsec-Protokoll von cisco
L2TP	L2TP-Protokoll
Benutzerdefiniertes SSL	Verbindung über Custom SSL
IKEv2	IKEv2-Protokoll
Proxy-Einrichtung	Konfigurieren eines Proxys für die VPN-Verbindung
Keine	Keine Vollmacht einrichten
Handbuch	Manuelles Einrichten eines Proxys
Proxy-Server-URL	Adresse für den Zugang zu den Proxy-Einstellungen
Hafen	Legen Sie den Port für den Proxy fest
Authentifizierung	Benutzername für die Authentifizierung beim Proxy
Passwort	Passwort für die Authentifizierung beim Proxy
Automatisch	Automatisch einen Proxy einrichten
Proxy-Server-URL	URL für den Zugriff auf die Proxy-Einstellungen

HTTP-Proxy

Proxy Typ	
Handbuch	Einen Proxy manuell einrichten
Proxy-Server-URL	Adresse für den Zugriff auf die Proxy-Einstellungen
Hafen	Proxy-Port einrichten
Authentifizierung	Benutzername für die Authentifizierung beim Proxy
Passwort	Passwort für die Authentifizierung beim Proxy
Automatisch	Automatisch einen Proxy einrichten
Proxy PAC URL	Proxy PAC URL
Direkte Verbindung zulassen, wenn PAC nicht erreichbar ist	Direkte Verbindung (ohne VPN) zulassen, wenn PAC nicht erreichbar ist
Erlaubt die Umgehung des Proxys für den Zugriff auf firmeneigene Netzwerke	Erlauben Sie die Umgehung des Proxys für den Zugriff auf firmeninterne Netzwerke

AirPrint

IP-Adresse	IP-Adresse des Druckers
Ressource Pfad	Eindeutiger Pfad zum AirPrint-Gerät

AirPlay

Gerät Name	Name des Geräts
Passwort	Passwort für die Kopplung
Whitelist	Definieren Sie eine Liste von Geräten, mit denen sich das Gerät exklusiv koppeln kann

PIM-Verwaltung

Exchange Active Sync

Konto Name	Name des Kontos.
eMail-Adresse	Die Adresse des Kontos (z.B. max@company.com)
Server-Hostname	Interner Hostname
Login-Name	Die Felder "Domäne" und "Anmeldename" müssen leer sein, damit das Gerät nach dem Benutzer fragt.
Domain	Die Felder "Domäne" und "Anmeldename" müssen leer sein, damit das Gerät nach dem Benutzer fragt. Wenn eine ACL-Gateway-Konfiguration aktiviert ist und das Feld Domain nicht leer ist, authentifiziert das AppTec360 Universal Gateway das Gerät mit folgendem Namen "Domain\Login Name"
Passwort	Das Passwort für das Konto (z.B. secretUserPassword)
Vergangene Tage von Mail to Sync	Die Anzahl der zu synchronisierenden Mails der letzten Tage
SSL verwenden	Verwenden Sie SSL für den internen Exchange-Host
Erweiterte Option	Erweiterte Optionen anzeigen
Server-Anschluss	Interner Anschluss
Server Pfad	Interner Pfad
Externer Hostname	Externer Host
Externer Anschluss	Externer Anschluss
Externer Pfad	Externer Pfad
Verwenden Sie SSL für Externe Host austauschen	SSL für externen Exchange-Host verwenden

eMail

Einrichtung von POP3 / IMAP-Konten auf dem Endgerät des Benutzers

Konto Beschreibung	Name des E-Mail-Kontos
Konto Typ	
IMAP	
Pfad-Präfix	Das Pfadpräfix für spezielle Ordner
POP	
Benutzer Display Name	Anzeigename des Benutzers
E-Mail Adresse	Benutzer-E-Mail-Adresse

Eingehende Post	Einstellungen für eingehende Server
Mail Server Adresse	Mail Server Adresse
Mail Server Port	Mail-Server-Port
Benutzer Name	Entsprechender Nutzername
Art der Authentifizierung	Art der Authentifizierung
Keine	Kein Authentifizierungstyp
Passwort (nur auf Geräteebene)	Passwortabfrage
MDM-Herausforderung-Antwort	
NTLM	NTLM-Authentifizierung
HTTP MD5-Digest	
SSL verwenden	Verwenden Sie SSL, falls erforderlich

Ausgehende Post	Einstellungen für den Ausgangsserver
Mail Server Adresse	Mail Server Adresse
Mail Server Port	Mail Server Port
Benutzer Name	Entsprechender Benutzername
Art der Authentifizierung	
Keine	Keine Authentifizierungsmethode
Passwort (nur auf Geräteebene)	Passwortabfrage
MDM-Herausforderung-Antwort	
NTLM	NTLM-Authentifizierung
HTTP MD5-Digest	
SSL verwenden	Verwenden Sie SSL, falls erforderlich
Ausgehendes Passwort gleich wie eingehendes	Ausgehendes Passwort gleich wie eingehendes
Nur in der Post verwenden	Aktivieren Sie diese Option, wenn alle ausgehenden E-Mails über die Mail-App versendet werden sollen.

CalDav

Konfigurieren Sie die Einrichtung und Verteilung eines CalDav-Kontos

Konto Beschreibung	Anzeigename des Kontos
Hostname	Hostname und/oder IP-Adresse
Hafen	Port des CalDav-Kontos
Haupt-URL	Haupt-URL des Kontos
Benutzername	Entsprechender CalDav-Benutzername
Passwort (nur auf Geräteebene)	Entsprechendes CalDav-Passwort
SSL verwenden	Verwenden Sie SSL, falls erforderlich

CardDav

Konfigurieren Sie die Einrichtung und Verteilung eines CardDav-Kontos

Konto Beschreibung	Anzeigename des Kontos
Hostname	Hostname und/oder IP-Adresse
Hafen	Port des CardDav-Kontos
Haupt-URL	Haupt-URL des Kontos
Benutzername	Entsprechender CardDav-Benutzername
Passwort (nur auf Geräteebene)	Entsprechendes CardDav-Passwort
SSL verwenden	Verwenden Sie SSL, falls erforderlich

LDAP

Richten Sie in diesem Bereich eine LDAP-Verbindung ein, um einen dynamischen Zertifikatsaustausch zwischen dem Endbenutzergerät und dem Active Directory zu ermöglichen.

Bitte beachten Sie, dass der ausgewählte Benutzer die entsprechende Leseberechtigung benötigt.

Konto Beschreibung	Konto Beschreibung
Konto-Benutzername	Benutzer für LDAP-Zugang
Konto-Passwort	Passwort für LDAP-Zugang
Konto Hostname	LDAP Server Hostname/IP-Adresse
SSL verwenden	Verwenden Sie SSL, falls erforderlich

Im zweiten Teil können Sie individuelle Filter für die Suche in der LDAP-Registrierung definieren.

Beschreibung	Umfang	Basis durchsuchen
Filter Beschreibung	Suchebene in der LDAP-Registrierung	Definieren Sie den individuellen Filter

Dashboard & Berichterstattung

Dashboard Einstellungen

Hier können Sie sehen, welche Dashboards existieren, sie bearbeiten oder neue erstellen. Jedes Dashboard verfügt über einen eigenen Satz von Daten, die angezeigt und grafisch konfiguriert werden können.

Steuerung der Dashboard-Einstellungen

Öffentlich	Stellt das Dashboard öffentlich ein, so dass andere Benutzer das Dashboard sehen können. Die Benutzer müssen natürlich in der Lage sein, sich anzumelden und Dashboards einzusehen. Wenn "Öffentlich" nicht aktiviert ist, kann nur der Ersteller sie sehen.
Standard	Legt das Dashboard als Standard fest, so dass es automatisch geöffnet wird, wenn Sie das nächste Mal die Dashboard-Ansicht aufrufen.
	Zeigen Sie das Dashboard und seine Diagramme an
	Löschen Sie das Dashboard
	Bearbeiten Sie den Namen und die Einstellungen des Dashboards
	Erstellen Sie eine Kopie des Dashboards
	Ein komplett neues Dashboard hinzufügen

Dashboard Ansicht

Hier werden die Daten und Diagramme des ausgewählten Dashboards angezeigt und Sie können diese auch ändern.

Dashboard Steuerung

	Hier können Sie festlegen, welche Daten im Dashboard angezeigt werden, wie viele Daten angezeigt werden sollen und in welcher Größe diese Daten angezeigt werden sollen.
	Bringt Sie zurück zur Übersicht des Dashboards
	Setzt das aktuell geöffnete Dashboard auf seine Standardeinstellungen zurück
	Speichert alle Änderungen, die Sie an dem aktuell geöffneten Dashboard vorgenommen haben (z.B. welche Daten angezeigt werden sollen)
	Diagrammtyp in Säulendiagramm ändern
	Diagrammtyp in Kreisdiagramm ändern
	Diagrammtyp in Doughnut-Diagramm ändern
	Ändern Sie den Chart-Typ in ein Polardiagramm
	Sortierreihenfolge ändern

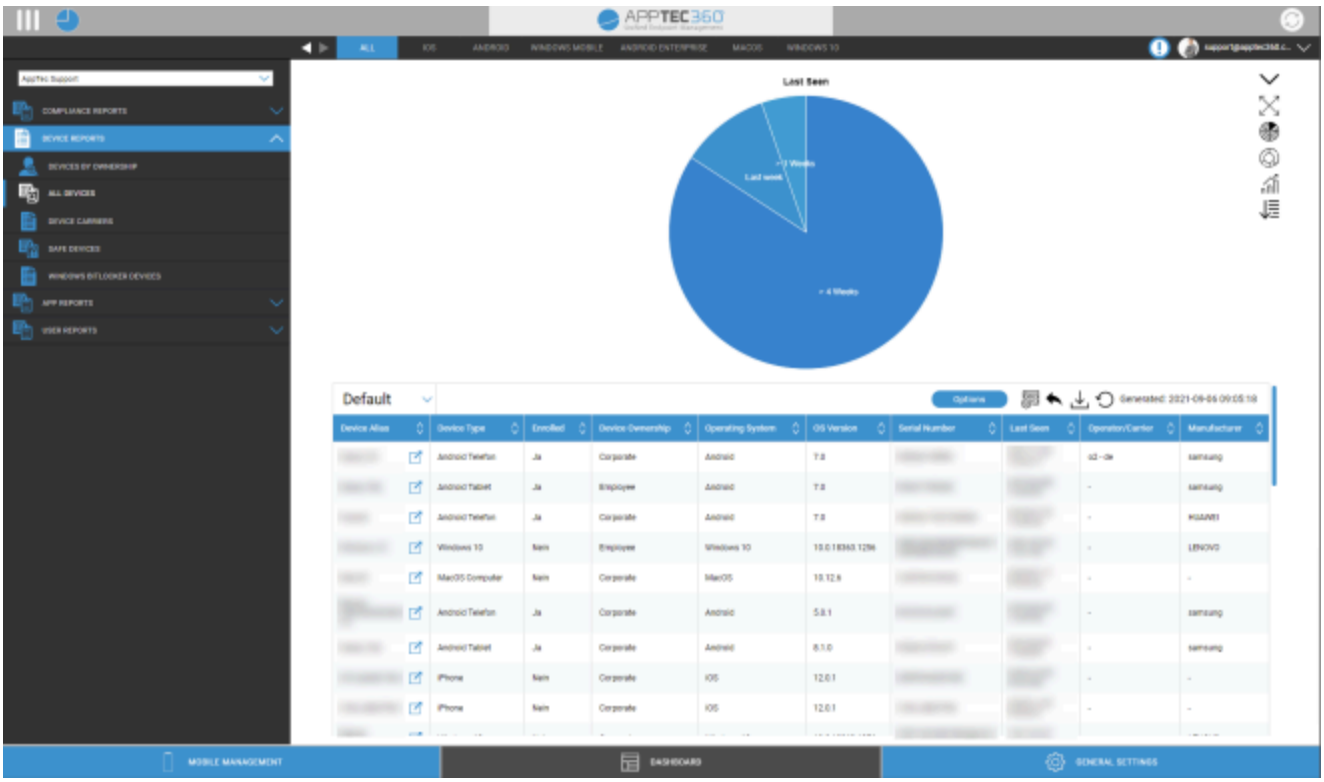
Erweiterte Berichterstattung

Die "Erweiterte Berichterstattung" bietet detaillierte Übersichten und Diagramme über Geräte- und Benutzerinformationen.

Es gibt ein paar Standardberichte, aber alle können manuell geändert werden, um Daten hinzuzufügen oder zu entfernen.

Bitte beachten Sie, dass Sie nur manuell ändern können, welche Daten angezeigt werden. Die gewählte Berichtskategorie definiert die Daten, auf denen dies basiert. So können Sie z.B. niemals Android-Geräte im iOS-Bericht in Geräteberichte Alle Geräte iOS sehen.

Oben links können Sie die Daten der Berichterstattung auf eine bestimmte Gruppe (und alle ihre Untergruppen) beschränken. Standardmäßig ist dies auf Ihren Stammknoten eingestellt, so dass ALLE Geräte und Benutzer berücksichtigt werden.



Erweiterte Berichtskontrolle

In jeder Übersicht können Sie die folgenden Funktionen verwenden, um den Bericht nach Ihren Wünschen zu verändern:

	Diagramm ausblenden (wenn das Diagramm angezeigt wird)
	Diagramm anzeigen (wenn das Diagramm ausgeblendet ist)
	Diagramm erweitern (wenn das Diagramm zugeklappt ist)
	Diagramm einklappen (wenn das Diagramm erweitert ist)
	Diagrammtyp in Säulendiagramm ändern
	Diagrammtyp in Kreisdiagramm ändern
	Diagrammtyp in Doughnut-Diagramm ändern
	Ändern Sie den Chart-Typ in ein Polardiagramm
	Sortierreihenfolge ändern
	Ändern Sie die folgenden Teile der angezeigten Übersicht: • Spalten hinzufügen/entfernen • Legen Sie die Reihenfolge fest, in der die Spalten angezeigt werden • Das Diagramm über der Tabelle ein-/ausblenden • Wählen Sie die Spalte, die für das Diagramm verwendet werden soll • Filtern Sie die Daten Ihrer Tabelle
	Öffnen Sie den Setup-Manager, um verschiedene Berichte zu speichern und zu laden
	Setzt den aktuell geöffneten Bericht auf die Standardeinstellungen zurück
	Exportieren Sie den aktuellen Bericht als .csv-Datei
	Daten neu generieren und den aktuellen Bericht neu laden

Eine Liste aller Standardberichte finden Sie auf den nächsten Seiten.

Compliance-Berichte

Verwurzelte Geräte

Übersicht über die Geräte, die gerootet/jailbroken wurden.

Standardspalten für diesen Bericht:

Geräte-Alias
Besitzer des Geräts
E-Mail
Betriebssystem
Telefon Nummer
Zuletzt gesehen
Hersteller

Roaming-Geräte

Übersicht über alle Geräte, die sich im Roaming befinden

Standardspalten für diesen Bericht:

Geräte-Alias
Besitzer des Geräts
E-Mail
Gerätetyp
Betriebssystem
Telefon Nummer
Zuletzt gesehen

Roaming-fähige Geräte

Übersicht über alle Geräte, die Roaming aktiviert haben, aber nicht unbedingt gerade roamen.

Standardspalten für diesen Bericht:

Geräte-Alias
Besitzer des Geräts
E-Mail
Gerätetyp
Betriebssystem
Telefon Nummer
Zuletzt gesehen

Überwachte Geräte

Übersicht über alle Geräte, die im überwachten Modus überwacht werden (nur iOS)

Standardspalten für diesen Bericht:

Geräte-Alias
Besitzer des Geräts
E-Mail
Gerätetyp
Zuletzt gesehen

Inaktive Geräte

Übersicht über alle Geräte, die sich in den letzten 7 Tagen nicht mit dem Server verbunden haben

Standardspalten für diesen Bericht:

Geräte-Alias
Besitzer des Geräts
E-Mail
Gerätetyp
Betriebssystem
Zuletzt gesehen

Geräteberichte

Geräte nach Eigentümerschaft

Hier können Sie sehen, wie viele Geräte derzeit als Unternehmensgeräte (Firmengeräte) und als Mitarbeitergeräte (private Geräte) bereitgestellt wurden.

Standardspalten für diesen Bericht:

Geräte-Alias
Besitzer des Geräts
Gerätetyp
Geräteeigentum
Betriebssystem

Alle Geräte

Hier sehen Sie eine Übersicht über alle Geräte mit den wichtigsten Informationen.

Standardspalten für diesen Bericht:

Geräte-Alias
Gerätetyp
Eingeschrieben
Geräteeigentum
Betriebssystem
OS Version
Seriennummer
Zuletzt gesehen
Betreiber/Transporteur
Hersteller

Geräteträger

Hier sehen Sie eine Übersicht über den Netzbetreiber (Mobilfunkanbieter).

Standardspalten für diesen Bericht:

Geräte-Alias
Besitzer des Geräts
E-Mail
Betriebssystem
OS Version
Betreiber/Transporteur

SAFE Geräte

Hier sehen Sie eine Übersicht darüber, welche Geräte SAFE Version verwenden.

Da die Übersicht und/oder SAFE nur für Samsung-Geräte verfügbar ist, sehen Sie unter diesem Punkt nicht die üblichen Registerkarten.

Standardspalten für diesen Bericht:

Geräte-Alias
Besitzer des Geräts
E-Mail
Gerätetyp
Zuletzt gesehen
SAFE Version

Windows BitLocker-Geräte

Hier sehen Sie eine Übersicht über die Windows-Geräte, die BitLocker verwenden.

Standardspalten für diesen Bericht:

Geräte-Alias
Besitzer des Geräts
E-Mail

BitLocker-Status

App Berichte

Hier erhalten Sie eine Vielzahl von Übersichten über Apps. In all diesen Berichten können Sie auf einen Eintrag klicken, um zu sehen, welche Versionen auf den Geräten installiert sind und wie oft. In dieser Ansicht können Sie erneut auf eine bestimmte Version klicken, um zu sehen, auf welchen Geräten diese spezielle Version installiert ist.

Hinweis: Es kann einige Zeit dauern, bis das System die aktuellen Informationen vom Gerät erhält. Außerdem werden die Berichte nicht jede Minute aktualisiert. Wenn Sie gerade eine neue App oder Version zugewiesen haben, müssen Sie möglicherweise etwas Geduld haben, um den aktuellen Status zu sehen. Wenn Sie den Bericht manuell neu laden, zeigt er die aktuellsten verfügbaren Daten an.

Installierte Apps

Hier erhalten Sie einen Überblick über alle installierten Apps.

Standardspalten für diesen Bericht:

Name	Name der jeweiligen App und/oder des Dienstes
Kennung	Eindeutige App/Dienst-ID
Gesamtanzahl	Wie oft diese App / dieser Dienst auf den Geräten der Endbenutzer installiert wurde

Meist installierte Apps

Hier erhalten Sie einen Überblick über die Apps, die am häufigsten installiert wurden.

Standardspalten für diesen Bericht:

Name	Name der jeweiligen App und/oder des Dienstes
Kennung	Eindeutige App/Dienst-ID
Gesamtanzahl	Wie oft diese App / dieser Dienst auf den Geräten der Endbenutzer installiert wurde

Obligatorische Apps

Hier erhalten Sie einen Überblick über die obligatorischen (zwingend erforderlichen) Anwendungen.

Standardspalten für diesen Bericht:

Name	Name der jeweiligen App und/oder des Dienstes
Kennung	Eindeutige App/Dienst-ID
App Quelle	Um welchen AppStore es sich handelt: • Google PlayStore (Android) • iTunes AppStore (iOS)
OS	Betriebssystem

Auf der schwarzen Liste stehende Apps

Hier erhalten Sie einen Überblick über alle definierten Apps auf der schwarzen Liste.

Standardspalten für diesen Bericht:

Name	Name der jeweiligen App und/oder des Dienstes
Kennung	Eindeutige App/Dienst-ID
App Quelle	Um welchen AppStore es sich handelt: • Google PlayStore (Android) • iTunes AppStore (iOS)
OS	Betriebssystem

Benutzerberichte

Tarif

Hier erhalten Sie einen Überblick über die Telefontarife und SIM-Karten Ihrer Benutzer.

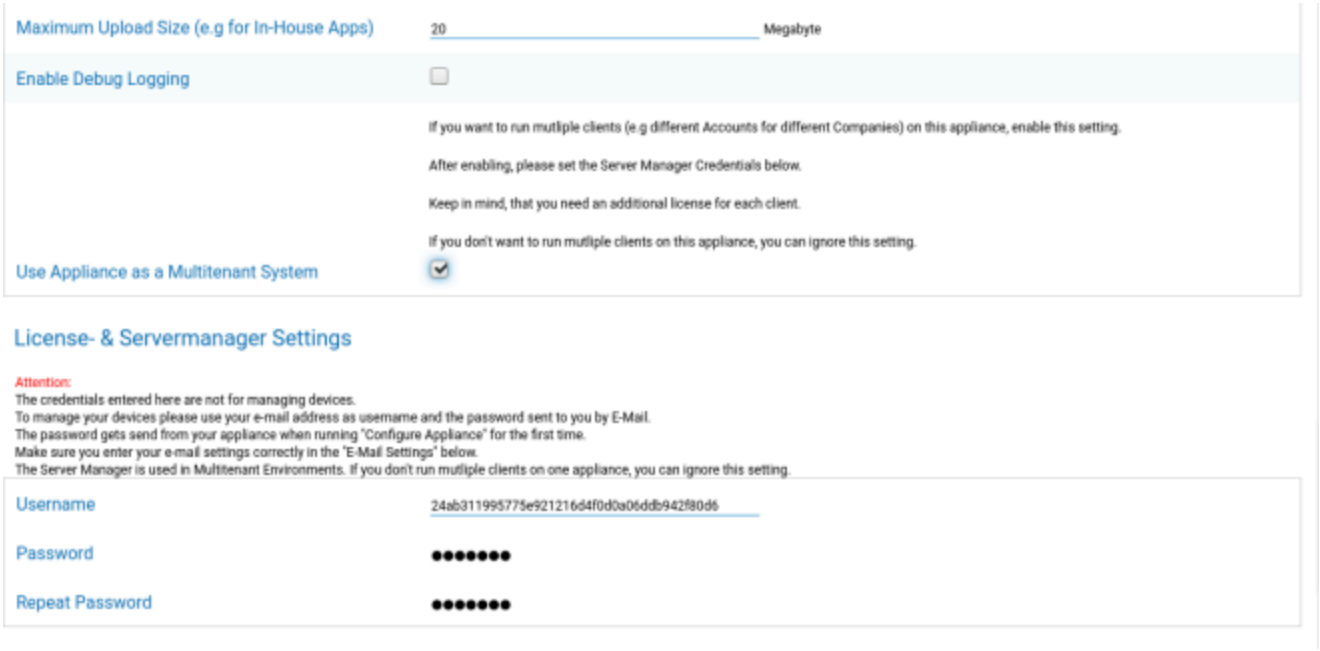
Standardspalten für diesen Bericht:

E-Mail
Name
TelefonNummer
Träger
Tarif
Option
Preis
contractCancelled
VertragStart
währendZeit
mobileAndData
dataVolume
multiSIM
Typ
simCardSerial1
simCardSerial2
simCardSerial3
Pin1
Pin2
puk1
puk2
Notiz

Multi-Mandanten-Verwaltung

AppTec360 EMM ist in der Lage, mehrere separate Mandanten zu hosten, jeder mit eigenen Benutzern und Gruppen, Berechtigungen und globalen Einstellungen.

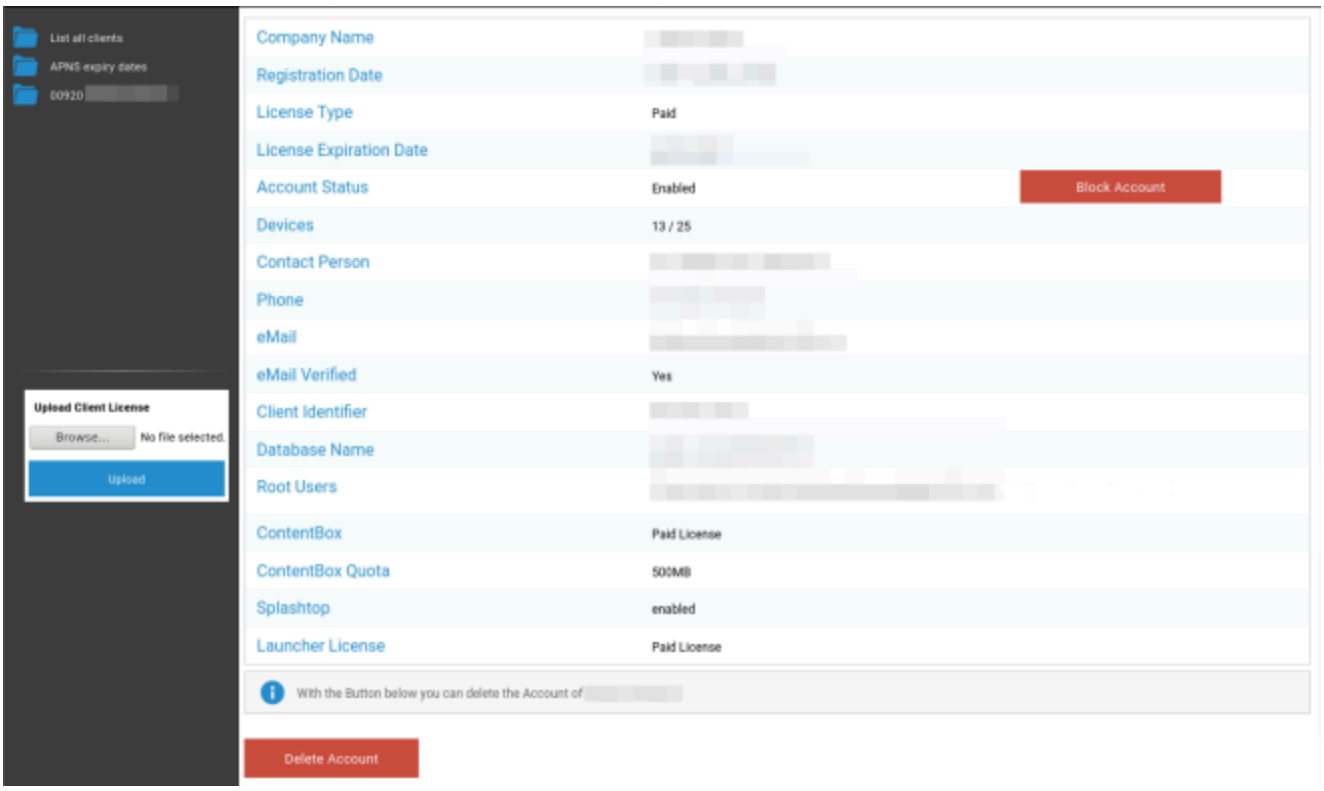
Um die Multitenant-Funktionen zu aktivieren, müssen Sie sie in der Konfigurationsoberfläche der Appliance unter "Schritt drei - Servereinstellungen" aktivieren.



Legen Sie in dem neuen Menü einen Benutzernamen und ein Passwort für den Servermanager fest. Speichern Sie die Einstellungen und führen Sie "Appliance konfigurieren" in "Schritt Fünf - Lizenzvereinbarung" aus, um die Einstellung zu übernehmen.

Wenn die Konfiguration abgeschlossen ist, können Sie sich nun mit den festgelegten Anmeldedaten über die normale Mobile Management-Oberfläche anmelden.

Nach der Anmeldung sehen Sie die folgende Ansicht.



Auf der linken Seite sehen Sie alle Mieter (in diesem Fall nur einen mit der ID 920) und auf der rechten Seite die Informationen zu diesem Kunden. Sie haben auch die Möglichkeit, den Zugriff auf das Konto zu sperren und den Client zu löschen (ACHTUNG: Dadurch werden alle Daten zu diesem Client gelöscht).

Auf der linken Seite können Sie eine neue Client-Lizenz hochladen. Dabei kann es sich entweder um eine Lizenzaktualisierung für einen bestehenden Client handeln oder um eine neue Lizenz, mit der automatisch ein neuer Client erstellt wird. Wenn ein neuer Client erstellt wird, wird automatisch eine E-Mail mit dem Anmeldepasswort an die E-Mail-Adresse gesendet, für die die Lizenz ausgestellt wurde.

Um eine neue oder aktualisierte Client-Lizenz zu erhalten (z.B. wenn Sie mehr Gerätelizenzen benötigen), wenden Sie sich an Ihren Vertriebsmitarbeiter.

Zusätzliche Ansichten

Alle Kunden auflisten

Zeigt eine Übersicht über alle Clients im System.

Kunden-ID	Kunden-ID
Kennung	Kennung des Kunden
Datenbank	Datenbank
Name des Unternehmens	Name des Unternehmens
eMail	Kontaktperson eMail
Geprüft	Ob die E-Mail der Kontaktperson verifiziert ist oder nicht
Land	Land
Geräte	Anzahl der registrierten Geräte
Datum der Registrierung	Zeitpunkt der Lizenzvergabe
Letzte Anmeldung	Letzte Anmeldung des Administratorkontos
Lizenz	Anzeige des Lizenztyps (Kostenlos|Bezahlt)
CB-Lizenz	ContentBox Lizenztyp (Kostenlos|Bezahlt)
Status	Aktueller Status des AppTec-Clients
Abgelaufen	Zeigt an, ob die Lizenz abgelaufen ist
iOS	Anzahl von iOS-Geräten
Android	Anzahl der Android-Geräte
Windows Mobile	Anzahl der Windows Mobile-Geräte
MacOS	Anzahl von MacOS-Geräten
Windows 10	Anzahl von Windows 10 Geräten
Android Unternehmen	Anzahl der Android Enterprise-Geräte
IOS BYOD (Benutzerregistrierung)	Anzahl der IOS BYOD-Geräte (Benutzerregistrierung)
IoT	Anzahl der IoT-Geräte

APNS Verfallsdaten

Zeigt eine Übersicht über die Ablaufdaten aller APNS-Zertifikate aller Clients.

Kunden-ID	Kunden-ID
Name des Unternehmens	Name des Unternehmens
Verfallsdatum	Ablaufdatum für das Apple APNS-Zertifikat
Infos	Informationen zum Ablauf der Frist

Kontakt

Weitere Fragen? Kontaktieren Sie uns einfach unter:

Für allgemeine technische Fragen

support@apptec360.com

+41 61 511 3210

Für Fragen im Zusammenhang mit der Installation einer virtuellen Appliance

consulting@apptec360.com

+41 61 511 3214

Haftungsausschluss