AppTec360 Enterprise Mobile Manager & ContentBox

Ръководство за администриране | Версия 5.0 (202110)

Съдържание

Общ преглед

- Въведение в AppTec360
- Поддържани операционни системи на устройствата
- Поддържани директории LDAP
- Обяснение на режима „Под наблюдение“ при устройствата на Apple
  - Налично в режим на наблюдение
  - Активиране на режима на наблюдение
  - Добавяне на устройство в DEP
- Обяснение на Android Enterprise
  - Какво е Android Enterprise?
  - Какви са изискванията за използване на Android Enterprise?.
  - Какви са наличните режими с Android Enterprise?
  - Как мога да задам приложения на устройства с Android Enterprise?
- Качване на собствени приложения в Google Play Store

Изисквания и инсталиране

- Изисквания
  - Системни изисквания
  - Ключ за лиценз
  - Разпознаване на IP адреси и DNS
  - SSL-сертификат
  - SMTP сървър
  - Правила на защитната стена
- Актуализации на сигурността
  - Пароли по подразбиране на виртуалното устройство
- Конфигуриране на виртуалното устройство
  - Подготовка
    - Конфигуриране от външен хост
  - Първа стъпка – Лиценз за уреда
  - Втора стъпка – SSL сертификат
    - Автоматичен

- Потребителски
- Трета стъпка – Настройки на сървъра
- Четвърта стъпка – Настройка на MySQL
- Пета стъпка – Лицензионно споразумение
- Отстраняване на неизправности
- Препоръки за сигурност

Общи настройки

Преглед на профила

- Информация за профила
  - Преглед
  - Доклад за грешка
  - Заявка за функция

Глобално конфигуриране

- Настройки на електронната поща
- Шаблони за електронна поща
- Записване в SMS

Поверителност

- Достъп до GPS

Достъп, базиран на роли

- Управление на роли
- Присвояване на роли
  - Присвояване на роля
- Достъп до API
  - Достъп до AppTec360 REST API
  - Общи правила
  - Пример за заявка
  - Запитвания
  - Примерен код в Python3

Конфигурация на Apple

- APNS сертификат
  - Стъпка 1
  - Стъпка 2
  - Стъпка 3
- Управляван достъп

- Записване на потребители
- Споделен iPad
- DEP
- Конфигуратор и URL
  - URL адреси за записване в басейна
  - MDM профил – Конфигуратор на Apple

Конфигурация на Android

- Конфигурация на Android
- Автоматично записване
- Android Enterprise
  - Първи метод: Акаунт за Android Enterprise (Google акаунт)
  - Втори метод: Акаунт в G-Suite
  - Защита от нулиране на фабриката
- Записване в AE
  - Метод 1: Записване с QR код
  - Метод 2: Записване в NFC
  - Метод 3: Акаунт в Google
- KNOX Записване
- Zero-Touch

Конфигурация на Windows

- Конфигурация на Windows

ContentBox

- Конфигурация

Конфигурация на LDAP

- Преглед на LDAP

Управление на приложения

- Вътрешнофирмени приложения DB
  - Android
  - iOS
  - MacOS
  - Windows 10
- Настройки на приложението
  - Настройки на приложението за iOS
  - Настройки на приложението за Android

- Приложения на трети страни
  - Android
  - iOS
- VPP / KNOX Premium
  - Лицензи за VPP
  - Токен на VPP
  - KNOX Premium Key
- Настройки на App Store
  - Регион и език
- Магазин за игри AE
  - Одобрени приложения
  - Приложения за Play Store
  - Частни приложения
  - Уеб приложения
  - Разположение на магазина
- Пакет от приложения

Дистанционно управление

- TeamViewer
  - TeamViewer Connector
  - Инсталиране на TeamViewer QuickSupport
  - Дистанционно управление на вашето устройство
  - Достъп без надзор
- Splashtop

Управление на SIM карти

- CSV групов внос
- Превозвач и тарифа

Управление на абонаменти

- Управление на абонаменти

Общ одитен дневник

- Одитен дневник
- Настройки на дневника за одит

Управление на сертификати

Управление на мобилни устройства

Екран за управление на мобилни устройства

- Филтър на устройството
- Прозорец за търсене
- Задвижване на опциите
- Стрелки за навигация

Настройки на акаунта в администрацията

- Информация за потребителя
- Настройки на конзолата
- Вход

Корпоративна администрация (Root-Node) в мобилното управление

- Създаване на подгрупа
- Преименуване на коренния възел
- Масово записване
- Присвояване на маса
- Бързо администриране на приложения
- Импортиране на потребители в CSV

Управление на групи в мобилното управление

- Създаване на подгрупа
- Редактиране на избрана група
- Изтриване на избрана група
- Създаване на потребител
  - Създаване на нов администраторски потребител

Управление на потребителите в мобилното управление

- Добавяне и записване на устройство

Управление на профили в мобилното управление

- Създаване на профил
- Редактиране на профила
- Копиране на профил
- Изтриване на профил
- Наследяване на профили

Управление на устройствата в мобилното управление

- IOS
  - Редактиране на устройство
  - Изчистване на паролата
  - Устройство за заключване

- Устройство за изключване
- Рестартиране на устройството
- Аларма и режим на изгубване | Деактивиране на режима на изгубване
- Изтриване на устройство
- Изтриване на устройството
- Изтриване на данни в предприятието | Премахване на MDM
- Изпрати съобщение
- Дистанционно управление на TeamViewer
- Изпращане на заявка за записване

Android

- Редактиране на устройство
- Изчистване на паролата
- Устройство за заключване
- Изтриване на устройство
- Изтриване на устройството
- Премахване на MDM
- Изпрати съобщение
- Трансформиране в режим COPE
- Изпращане на заявка за записване
- Мигриране на наследеното устройство

Windows

- Редактиране на устройство
- Изтриване на устройство
- Изтриване на данни в предприятието | Премахване на MDM
- Дистанционно управление на TeamViewer
- Изпращане на заявка за записване

Управление на съдържанието

- Групови файлове
- Изследовател на файлове
- Одитна следа
- Отпадъци
- Външно съхранение

Одитен дневник

Конфигурация на iOS

- Обща информация
  - Преглед на профила на групата (само на ниво група)
  - Обща информация
  - Настройки
  - Ревизия на конфигурацията
  - Дневник на устройството (само на ниво устройство)
    - Дневник на командите
    - Възможни състояния на командата
- Управление на активи (само на ниво устройство)
  - Управление на активи (само на ниво устройство)
    - Информация за устройството
    - Wi-Fi
    - Клетъчен
    - Bluetooth
- Управление на сигурността
  - Защита от кражба (само на ниво устройство)
    - GPS информация (само на ниво устройство)
    - Изтриване и заключване (само на ниво устройство)
    - Съобщение (само на ниво устройство)
  - Конфигурация на сигурността
    - Парола
    - Сертификат (само на ниво устройство)
    - Криптиране
    - Еднократно влизане в системата
  - Край на живота (само на ниво устройство)
    - Избърсване (само на ниво устройство)
  - Настройки на ограниченията
    - Функционалност на устройството
    - iCloud
    - Сигурност и поверителност
- BYOD
  - Вградена защита на iOS (контейнер)
    - Активиране
    - SecurePIM Парола

- SecurePIM Сигурност
- Браузър SecurePIM
- Обмен

Управление на връзките

- Wi-Fi
  - Настройка на прокси сървъра
  - Вид сигурност
- VPN
  - Тип VPN
    - VPN
    - VPN за всяко приложение
  - Настройка на прокси сървъра
- APN
- Клетъчен
- HTTP прокси
- AirPrint
- AirPlay

Управление на PIM

- Exchange Active Sync
- Електронна поща
  - Входяща поща
  - Изходяща поща
- CalDav
- Абонирани календари
- LDAP

Уеб управление

- Уебклипове
- Филтър за уеб съдържание

Управление на приложения

- Мениджър на корпоративни приложения
  - Инсталирани приложения (само на ниво устройство)
  - Задължителни приложения
    - Опции за инсталиране
  - Уеб приложения

- Ограничения и настройки
  - Приложения в черния списък / в белия списък
  - Ограничения на SysApp
  - App-VPN
  - Настройки на приложението
- Магазин за корпоративни приложения
  - Приложения на iTunes
  - Вътрешен
- Режим на киоск
  - Тип приложение
    - Пакет
    - URL
  - Настройки на режима Kiosk

Android Enterprise – Напълно управлявано конфигуриране на устройства

Обща информация

- Преглед на профила на групата (само на ниво група)
- Преглед на устройството (само на ниво устройство)
- Ревизия на конфигурацията (само на ниво устройство)
- Дневник на устройството (само на ниво устройство)
  - Дневник на командите
  - Възможни състояния на командата
- Настройки на устройството
  - Конфигурация на клиента
  - Тапети

Управление на активи (само на ниво устройство)

- Информация за устройството
  - Wi-Fi
- Клетъчен
- Bluetooth

Управление на сигурността

- Защита от кражба (само на ниво устройство)
  - GPS информация (само на ниво устройство)
  - Изтриване и заключване (само на ниво устройство)

- Съобщение (само на ниво устройство)
- Конфигурация на сигурността
  - Парола на устройството
  - Антивирус
- Край на живота (само на ниво устройство)
  - Избърсване (само на ниво устройство)
- Настройки на ограниченията
  - Ограничения
- Управление на сертификати

Управление на връзките

- Wifi
  - Вид сигурност
    - WEP
    - WPA/WPA2
    - 802.1x EAP
- VPN
  - Тип VPN
    - VPN
    - VPN за всяко приложение
- Ограничения

Управление на PIM

- Gmail Exchange

Управление на приложения

- Мениджър на корпоративни приложения
  - Инсталирани приложения (само на ниво устройство)
  - Системни приложения (само на ниво устройство)
  - Задължителни приложения
  - Черни и бели списъци
  - Приложения на системата AE
- Ограничения и настройки
  - Настройки за управление на приложения
- Магазин за корпоративни приложения
  - Вътрешен
- Магазин Play за предприятия
  - Магазин за игри AE

- Режим на киоск и стартиране
  - Режим на киоск
  - AppTec360 Launcher
  - Настройки на AppTec360
- Дистанционно управление
  - Splashtop
  - TeamViewer
- Управление на съдържанието
  - ContentBox
  - Сигурен браузър
- Допълнителен API
  - Samsung KNOX
    - Ограничения
    - Имейл
    - Обмен
    - APN
    - Bluetooth
    - Връзка
- Android Enterprise – Напълно управлявано устройство с работен профил (COPE)
  - Общо обяснение на COPE
  - Конфигуриране на профили за устройства COPE
  - Връщане към AE напълно управлявано устройство
- Android Enterprise – Конфигуриране на контейнери
  - Обща информация
    - Преглед на профила (само на ниво профил)
    - Преглед на профила на групата (само на ниво група)
    - Преглед на устройството (само на ниво устройство)
    - Ревизия на конфигурацията
    - Дневник на устройството (само на ниво устройство)
      - Дневник на командите
      - Възможни състояния на командата
  - Настройки на устройството

- Конфигурация на клиента
- Тапети

Управление на активи (само на ниво устройство)

- Информация за устройството
  - Wi-Fi
- Клетъчен
- Bluetooth

Управление на сигурността

- Защита от кражба (само на ниво устройство)
  - GPS информация (само на ниво устройство)
  - Изтриване и заключване (само на ниво устройство)
  - Съобщение (само на ниво устройство)
- Конфигурация на сигурността
  - Парола на устройството
  - Парола на контейнера
  - Антивирус
- Край на живота (само на ниво устройство)
  - Избърсване (само на ниво устройство)
- Настройки на ограниченията
  - Ограничения
- Управление на сертификати

Управление на връзките

- Wifi
  - Вид сигурност
    - WEP
    - WPA/WPA2
    - 802.1x EAP
- VPN
  - Тип VPN
    - VPN
    - VPN за всяко приложение
- Ограничения

Управление на PIM

- Gmail Exchange

Управление на приложения

- Мениджър на корпоративни приложения
  - Инсталирани приложения (само на ниво устройство)
  - Системни приложения (само на ниво устройство)
  - Задължителни приложения
  - Приложения на системата AE
- Ограничения и настройки
  - Настройки за управление на приложения
- Магазин за корпоративни приложения
  - Вътрешен
- Магазин Play за предприятия
  - Магазин за игри AE

Управление на съдържанието

- ContentBox
- Сигурен браузър

Конфигурация на Android

Обща информация

- Преглед на профила на групата (само на ниво група)
  - Преглед на устройството (само на ниво устройство)
- Ревизия на конфигурацията (само на ниво устройство)
- Дневник на устройството (само на ниво устройство)
  - Дневник на командите
  - Възможни състояния на командата
- Настройки на устройството
  - Конфигурация на клиента
  - Тапети

Управление на активи (само на ниво устройство)

- Управление на активи
  - Информация за устройството
  - Wi-Fi
  - Клетъчен
  - Bluetooth

Управление на сигурността

- Защита от кражба (само на ниво устройство)
  - GPS информация (само на ниво устройство)

- Изтриване и заключване (само на ниво устройство)
- Съобщение (само на ниво устройство)
- Конфигурация на сигурността
  - Парола
  - Криптиране
  - Антивирус
- Край на живота (само на ниво устройство)
  - Избърсване (само на ниво устройство)
- Настройки на ограниченията
  - Ограничения
  - Собственик на устройството AE

Контейнер BYOD

- Android Enterprise
  - Android Enterprise
  - Gmail Exchange
  - Приложения на системата AE
  - Парола на контейнера
- Samsung KNOX
  - Активиране
  - Код за достъп на Knox
  - Knox Security
  - Knox Exchange
  - Електронна поща на Нокс
  - Приложения Knox

Управление на връзките

- Wifi
  - Вид сигурност
    - WEP
    - WPA/WPA2
    - 802.1x EAP
- VPN
- Ограничения
- APN
- Bluetooth

Управление на PIM

- Обмен
- Електронна поща
- AE Gmail Exchange

Управление на приложения

- Мениджър на корпоративни приложения
  - Инсталирани приложения (само на ниво устройство)
  - Системни приложения (само на ниво устройство)
  - Задължителни приложения
  - Приложения на системата AE
- Ограничения и настройки
  - Черни и бели списъци
  - Ограничения на системните приложения
    - Приложения на Samsung
    - Приложения на Huawei
  - Настройки за управление на приложения
- Магазин за корпоративни приложения
  - Playstore
  - Вътрешен
- Магазин Play за предприятия
- Режим на киоск и стартиране
  - Режим на киоск
  - AppTec360 Launcher
  - Настройки на AppTec360

Дистанционно управление

- Splashtop
- Teamviewer

Управление на съдържанието

- Поле за съдържание
- Сигурен браузър

Конфигуриране на компютър с Windows 10

Обща информация

- Преглед на профила на групата (само на ниво група)
- Преглед на устройството (само на ниво устройство)
- Настройки

- Ревизия на конфигурацията (само на ниво устройство)
- Дневник на устройството (само на ниво устройство)
  - Дневник на командите
  - Възможни състояния на командата
- Управление на активи (само на ниво устройство)
  - Информация за устройството
  - Клетъчен
  - Информация за синхронизиране
- Управление на сигурността
  - Защита от кражба (само на ниво устройство)
    - GPS информация (само на ниво устройство)
    - Настройки на GPS
  - Конфигурация на сигурността
    - Парола
    - Антивирусна програма
    - Център за сигурност
    - Конфигуриране на защитната стена
    - Правила на защитната стена
  - Настройки на ограниченията
    - Функционалност на устройството
  - BitLocker
    - Конфигурация на BitLocker
    - Състояние на BitLocker
  - Управление на сертификати
    - Списък на сертификатите
    - Конфигурация на сертификата
    - SCEP
- Управление на връзките
  - Wifi
    - Вид сигурност
    - Използване на прокси сървър
  - Ограничения за Wi-Fi
  - VPN
    - Вид на връзката
    - Общи конфигурации на VPN
  - Ограничения за VPN
  - Bluetooth

- Управление на PIM
  - Exchange Active Sync
  - Електронна поща
- Управление на приложения
  - Мениджър на корпоративни приложения
    - Инсталирани приложения
    - Задължителни приложения
    - Ограничения на системните приложения
    - Черни и бели списъци

Конфигурация на MacOS

Обща информация

- Преглед на профила на групата (само на ниво група)
- Преглед на устройството (само на ниво устройство)
- Ревизия на конфигурацията (само на ниво устройство)
- Дневник на устройството (само на ниво устройство)
  - Дневник на командите
  - Възможни състояния на командата

Управление на активи (само на ниво устройство)

- Информация за устройството
- WiFi
- Клетъчен
- Bluetooth

Управление на актуализациите (само на ниво устройство)

- Актуализиране на информацията

Управление на сигурността

- Защита от кражби
  - Избърсване и заключване
- Конфигурация на сигурността
  - Парола
  - Сертификат
- Настройки на ограниченията
  - Функционалност на устройството
  - iCloud
  - Управление на медиите

- Управление на връзките
  - Wi-Fi
    - Конфигуриране на Wi-Fi в предприятието
  - VPN
  - HTTP прокси
  - AirPrint
  - AirPlay
- Управление на PIM
  - Exchange Active Sync
  - Електронна поща
  - CalDav
  - CardDav
  - LDAP

Информационно табло и отчитане

- Настройки на таблото за управление
- Изглед на таблото за управление
- Разширено отчитане
  - Доклади за съответствие
    - Вкоренени устройства
    - Устройства в роуминг
    - Устройства с разрешен роуминг
    - Контролирани устройства
    - Неактивни устройства
  - Доклади за устройства
    - Устройства по собственост
    - Всички устройства
    - Носители на устройства
    - Устройства SAFE
    - Устройства с Windows BitLocker
  - Доклади за приложения
    - Инсталирани приложения
    - Най-инсталирани приложения
    - Задължителни приложения
    - Приложения в черния списък

- Доклади на потребителите
  - Тарифа
- Управление на множество наематели
- Допълнителни изгледи
  - Списък на всички клиенти
  - Дати на изтичане на валидността на APNS
- Свържете се с
- За общи технически въпроси
- За въпроси, свързани с инсталирането на виртуален уред
- Отказ от отговорност

Общ преглед

Въведение в AppTec360

Решението за управление на мобилни устройства на AppTec предлага възможност за управление и конфигуриране на всички мобилни устройства с интуитивната си конзола за управление. При този сценарий сървърът на EMM може да работи в собствената ви среда или да използвате нашето решение, базирано на облак.

Дори и по темата за централизирано инсталиране на корпоративни приложения на смартфони, сте попаднали на правилното място. С помощта на Enterprise Mobile Manager можете да разпространявате корпоративни приложения и документи на устройствата за секунди или да блокирате нежеланите приложения с помощта на бял/черен списък.

Използването на частни устройства в компаниите поставя ново предизвикателство пред защитата на смартфони и таблети. Поради факта, че служителите искат да използват смартфоните си все повече и повече, ИТ администраторите трябва да защитават голям брой различни видове устройства. Ще ви помогнем да защитите всички устройства и чувствителните данни, които се съхраняват на тях, и да ги управлявате от интуитивна конзола.

Поддържани операционни системи на устройствата

AppTec360 предлага поддръжка за устройства с iOS, Android и Windows. Имайте предвид, че капацитетът на функциите на споменатите платформи може да се различава при различните операционни системи.

- Apple iOS 11.0 или по-нова версия*
- Apple macOS 10.11 или по-нова версия
- Google Android 4.4 или по-нова версия** на версията в облака
- Google Android 4.1 или по-висока версия** за версията OnPrem
- MS Windows 10 или по-нова версия*** (настолен компютър, преносим компютър и таблет)

**Моля, имайте предвид, че устройства с iOS 10 или по-ранни версии не могат да бъдат записани поради драстични промени, направени от Apple в процеса на записване.*

***Устройствата могат да бъдат свързвани и конфигурирани, дори ако използват версия, която вече не се поддържа от производителя. Моля, обърнете внимание, че е възможно да има функции, които изискват определена версия на Android. В случаите на поддръжка следваме официалната поддръжка на производителя. В случай на проблеми или грешки, причинени от остаряла версия, която вече не се поддържа от производителя, си запазваме правото да предложим само ограничена поддръжка.*

****Най-домашната версия на Windows не се поддържа поради ограниченията на операционната система. Препоръчваме ви да използвате версия на операционната система, която все още се поддържа от производителя. Не само от съображения за съвместимост, но и от съображения за сигурност. Затова препоръчваме iOS 12 или по-нова версия и Android 9 или по-нова версия.*

Поддържани директории LDAP

- Microsoft Active Directory
- Отваряне на LDAP

Актуална информация за "Поддържани операционни системи на устройства" и "Поддържани директории LDAP" можете да намерите тук:

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

Обяснение на режима „Под наблюдение“ при устройствата на Apple

Режимът "Под наблюдение" представлява разширен интерфейс за устройствата с iOS.

Към съответно конфигурираното устройство могат да бъдат приложени допълнителни ограничения, свързани с функционалността на крайното потребителско устройство. Те се съдържат и в наръчника на администрацията и са обозначени с банер.

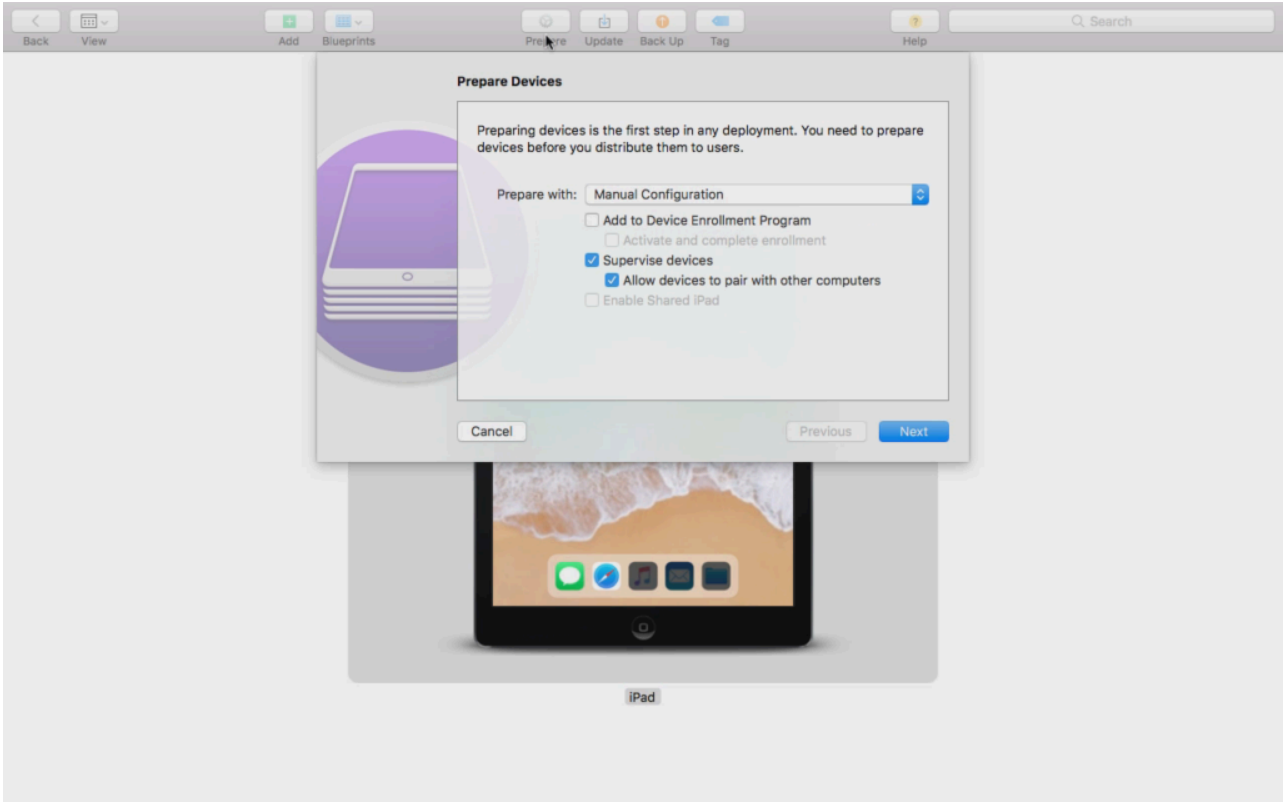
Налично в режим на наблюдение

Режимът "Supervised-Mode" може да се активира с програмата "Apple Configurator". Конфигураторът на Apple може да задава настройките по подразбиране на новите iOS устройства като инструмент за конфигуриране (чрез USB интерфейс).

Инструментът може да инсталира не само конфигурационни профили, но и приложения. Тя е безплатна, но изисква компютър Mac.

Активиране на режима на наблюдение

1. Отворете Конфигуратора на Apple



2. Кликнете върху устройството и изберете "Prepare".
3. Изберете "Ръчно конфигуриране" и "Надзор на устройствата".
4. Кликнете върху "Напред".
5. (по избор) Сега можете да добавите MDM сървър, в който ще бъде записано устройството. Връзката за това се намира в "Общи настройки - Конфигурация на iOS - Конфигуратор и URL" Изберете организацията си или създайте нова.
6. Изберете своята организация или създайте нова.
7. Изберете кои стъпки трябва да бъдат пропуснати при първоначалната настройка и щракнете върху "Напред" (ВНИМАНИЕ: Продължаването ще доведе до изтриване на устройството ви!)

Сега устройството ви ще бъде поставено в режим на наблюдение. Това може да отнеме няколко минути. След като това стане, устройството ще се рестартира.

Сега устройството ви е под надзор!

Добавяне на устройство в DEP

Можете също така да добавяте устройства към DEP (Device Enrollment Programm) с помощта на Apple Configurator, ако устройствата ви са с iOS 11 или по-нова версия.

Повече информация за DEP: https: //www.apple.com/business/dep/

Изпълнете същите стъпки, както при надзора на устройство, и допълнително поставете отметка на "Add to Device Enrollment Programm" (Добавяне към програмата за записване на устройства). Ще бъдете помолени да предоставите данните си за вход в DEP, ако досега не сте влизали в DEP с помощта на Apple Configurator.

След приключване на процеса устройството може да бъде намерено в сървъра DEP "Devices Added by Apple Configurator 2". Сега можете да използвате този сървър и да го свържете към конзолата за управление или да прехвърлите устройството към вече съществуващ сървър.

Вече успешно сте добавили устройство в DEP!

Обяснение на Android Enterprise

Какво е Android Enterprise?

Android Enterprise предлага по-добър контрол на работните устройства, които се управляват с MDM. Това позволява на администраторите или да имат пълен контрол над своите устройства с Android, или да разделят данните на компанията от личните данни на контейнерните устройства. Освен това Android Enterprise позволява по-лесно записване на устройствата и лесно разпространение на приложения.

Какви са изискванията за използване на Android Enterprise?.

Android Enterprise може да се използва безплатно от всички. Необходимо е само да свържете акаунт в Google към MDM, за да активирате всички функции на Android Enterprise. Повече за това можете да намерите в раздела Android Enterprise.

Android Enterprise може да се използва на устройства с Android 5.1 или по-нова версия, с изключение на Enhanced Work Profile (вж. по-долу). Препоръчваме поне Android 7 или по-висока версия за по-лесно записване или Android 11, за да се използват всички налични функции.

Какви са наличните режими с Android Enterprise?

Има 3 различни режима за използване при работа с Android Enterprise.

AE Напълно управлявано устройство (Управлявана работа): Напълно управлявано устройство, което се използва само за работа. Това позволява на администратора пълен контрол върху устройството. Това не позволява частно използване на устройството. За да се регистрират устройства в този режим, устройствата трябва да се нулират и да се регистрират с QR код (вж. AE Enrollment) или да се регистрират чрез Knox Enrollment или Zero Touch.

AE BYOD Container: Контейнерът BYOD (bring your own device) позволява на потребителите да имат достъп до фирмени данни на личния си телефон в отделен контейнер. В този режим частните приложения не могат да виждат фирмени данни и приложения и обратно. За да се регистрират устройствата в този режим, трябва да се изтегли приложението AppTec и да се сканира QR код. Създайте устройство в конзолата и изберете "AE Container (BYOD & Enahnced Work Profile)" (Контейнер AE (BYOD и активиран работен профил)) като тип устройство. Щракнете върху QR кода на новосъздаденото устройство, за да получите QR кода и да зададете първия превключвател на "Legacy & BYOD".

AE Enhanced Work Profile: (изисква Android 11 или по-нов) Докато гореспоменатият BYOD Container пренася данните на компанията на частно устройство, Enhanced Work Profile прави същото, но за устройство, собственост на компанията. Той създава същия контейнер, но дава

на администратора малко по-голям контрол върху устройството, така че потребителят не може просто да премахне MDM от устройството. Създайте устройство в конзолата и изберете "AE Container (BYOD & Enahnced Work Profile)" (Контейнер AE (BYOD и разширен работен профил)) като тип устройство. Щракнете върху QR кода на новосъздаденото устройство, за да получите QR кода и да зададете първия превключвател на "Enhanced Work Profile". Този QR код може да бъде сканиран, след като нулирате устройството и докоснете 6 пъти екрана, както е обяснено в Метод 1 в AE Enrollment (Записване на AE).

Как мога да задам приложения на устройства с Android Enterprise?

Първо трябва да одобрите приложенията, които искате да използвате, в Общи настройки → Управление на приложения → AE Play Store → Play Store Apps. След като одобрите дадено приложение, можете да го назначите в списъка със задължителни приложения → на профила си, като кликнете върху "+" и изберете приложението от раздела "AE Play Store". Това ще доведе до автоматично изтегляне и инсталиране на приложението. Не е необходим акаунт в Google на устройството и потребителят не трябва да потвърждава или разрешава това.

Качване на собствени приложения в Google Play Store

Възможно е да качите вътрешните си приложения в Google Play Store. По този начин можете да се възползвате от различни предимства, като например механизма за актуализиране на Play Store.

За целта ви е необходим акаунт за разработчици в Google. Влезте в Google Play Console(https://play.google.com/apps/publish).

Кликнете върху "Създаване на приложение". Изберете езика по подразбиране и заглавието на приложението.

Create application

Default language *

English (United Kingdom) – en-GB ▾

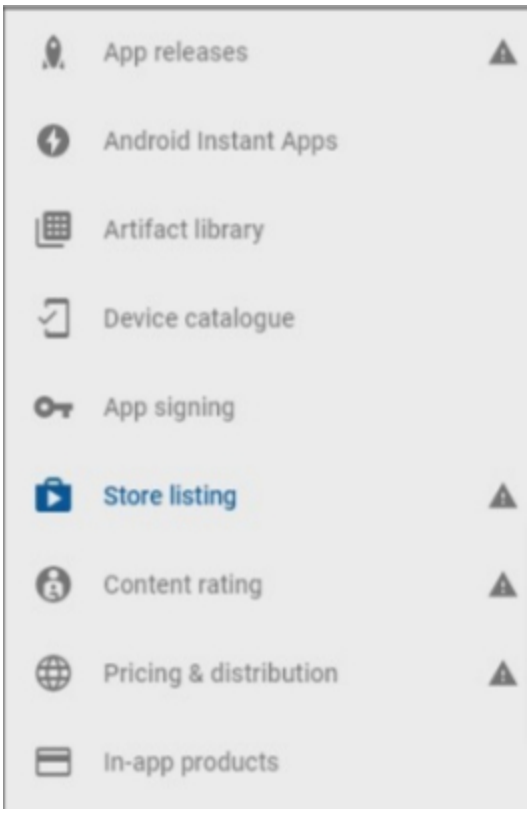
Title *

AppTec Demo App

15/50

CANCEL CREATE

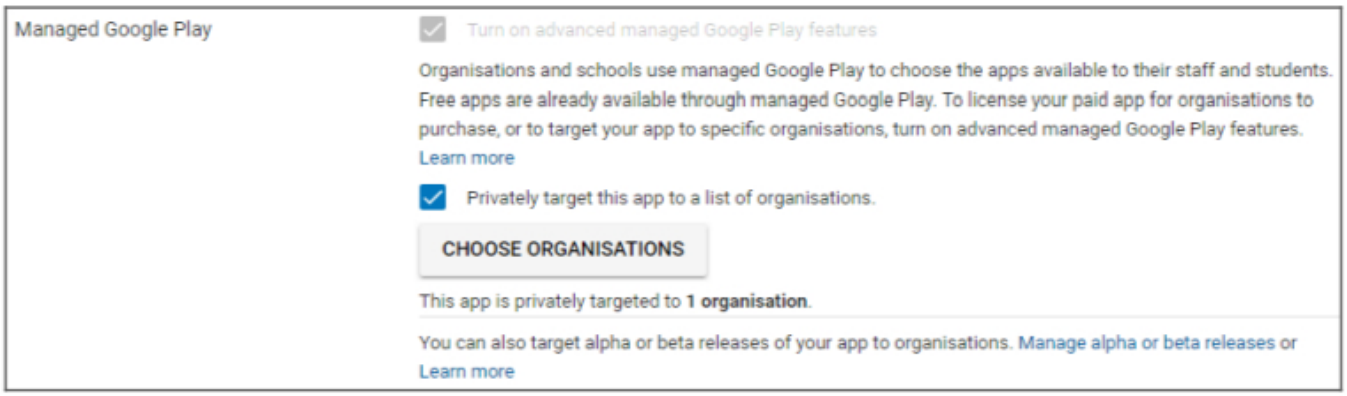
На следващата страница ще бъдете помолени да въведете различни данни за вашето приложение.



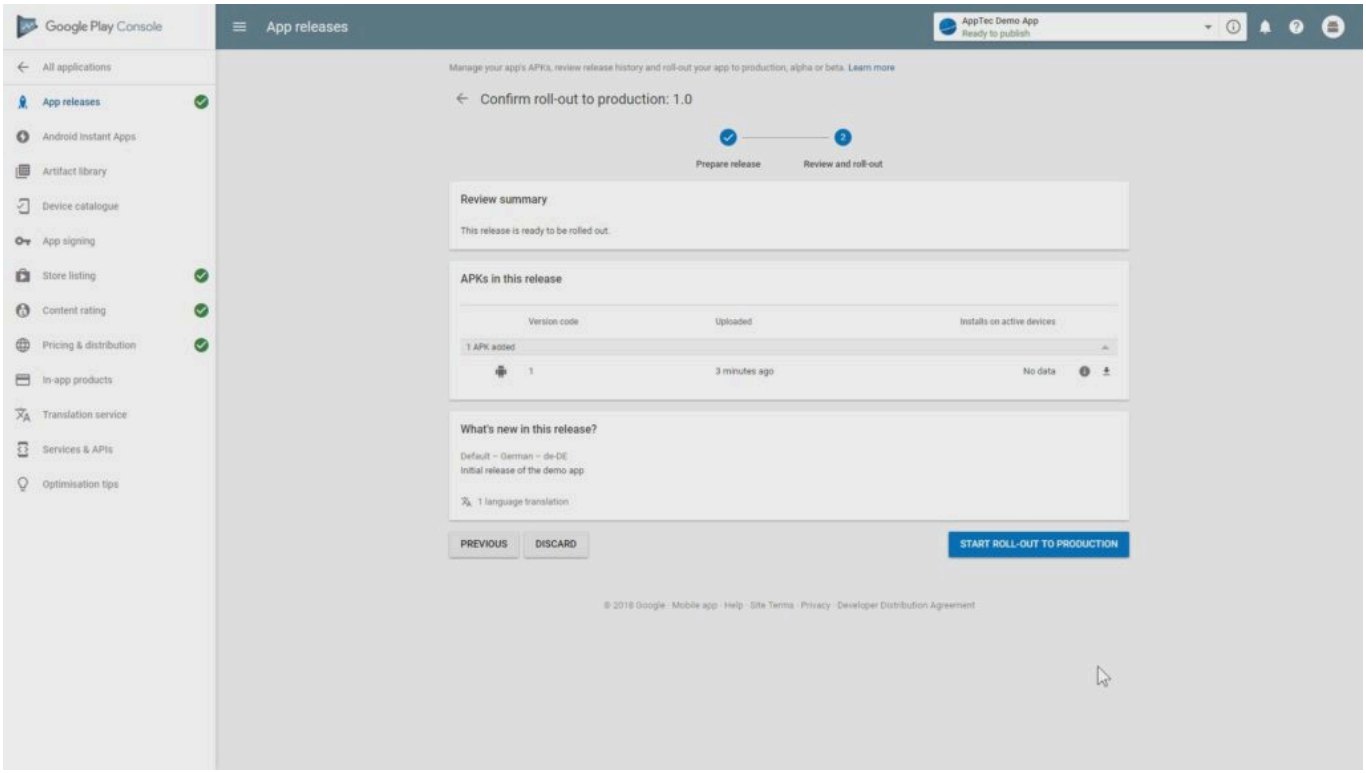
След като въведете всички данни, в лявата част ще видите различни символи за подсказване.

Поставете курсора върху тях, за да видите кои стъпки остават, и ги следвайте в произволен ред.

Бележка: Не забравяйте да поставите отметка в двете квадратчета на "Managed Google Play" в "Pricing & Distribution". В противен случай приложението ще бъде публично и ще може да бъде достъпно за всички. Също така се уверете, че сте избрали страната за разпространение.



След като сте изпълнили всички стъпки, можете да отидете в "App releases". Кликнете върху "Review" и "Start Roll-Out to Production", за да финализирате проекта си и да публикувате приложението.



Трябва да мине известно време, докато приложението бъде налично в Play Store. След като процесът приключи, можете да потърсите приложението си в магазина Play for Work и да го одобрите. След това можете просто да назначите приложението на устройствата, като използвате конзолата EMM, точно както го правите с други приложения.

Изисквания и инсталиране

Изисквания

Системни изисквания

Виртуалното устройство се предлага в отворен формат за виртуализация (VMWare, VirtualBox, Citrix Xen Server) и като компресиран .vhdx (Hyper-V) файл*.

*Забележка: Машината трябва да бъде създадена с Generation 1, когато използвате Hyper-V.

Целевият размер на виртуалния диск е 20 GB, а машината се нуждае от 4 GB RAM.

Устройството е базирано на Debian 9 64bit

Актуализирайте импортираната машина до най-новата съвместимост (напр. във VMWare) и се уверете, че типът на операционната система на машината е зададен правилно във вашия хипервайзор.

Ключ за лиценз

За успешното активиране и инсталиране на сървъра се нуждаете от валиден лицензионен файл. Можете да го получите директно от AppTec360 и/или от съответния дистрибутор.

Разпознаване на IP адреси и DNS

Устройството AppTec360 може да бъде достигнато от устройството, използващо името на хоста, за който е издаден лицензът.

За да запишете устройства с Windows 10, трябва да настроите и допълнителен поддомейн под формата на "enterpriseenrollment.", който да сочи към уреда.

SSL-сертификат

Тъй като всички връзки към и от устройствата трябва да бъдат защитени с помощта на SSL, е необходим валиден сертификат за името на хоста, издаден от удостоверяващ орган, на който устройството има доверие. Частният ключ за сертификата трябва да бъде качен без защита с парола. В повечето случаи се изисква междинен сертификат за Удостоверяващия орган, за да могат устройствата да разпознаят сертификата на сървъра.

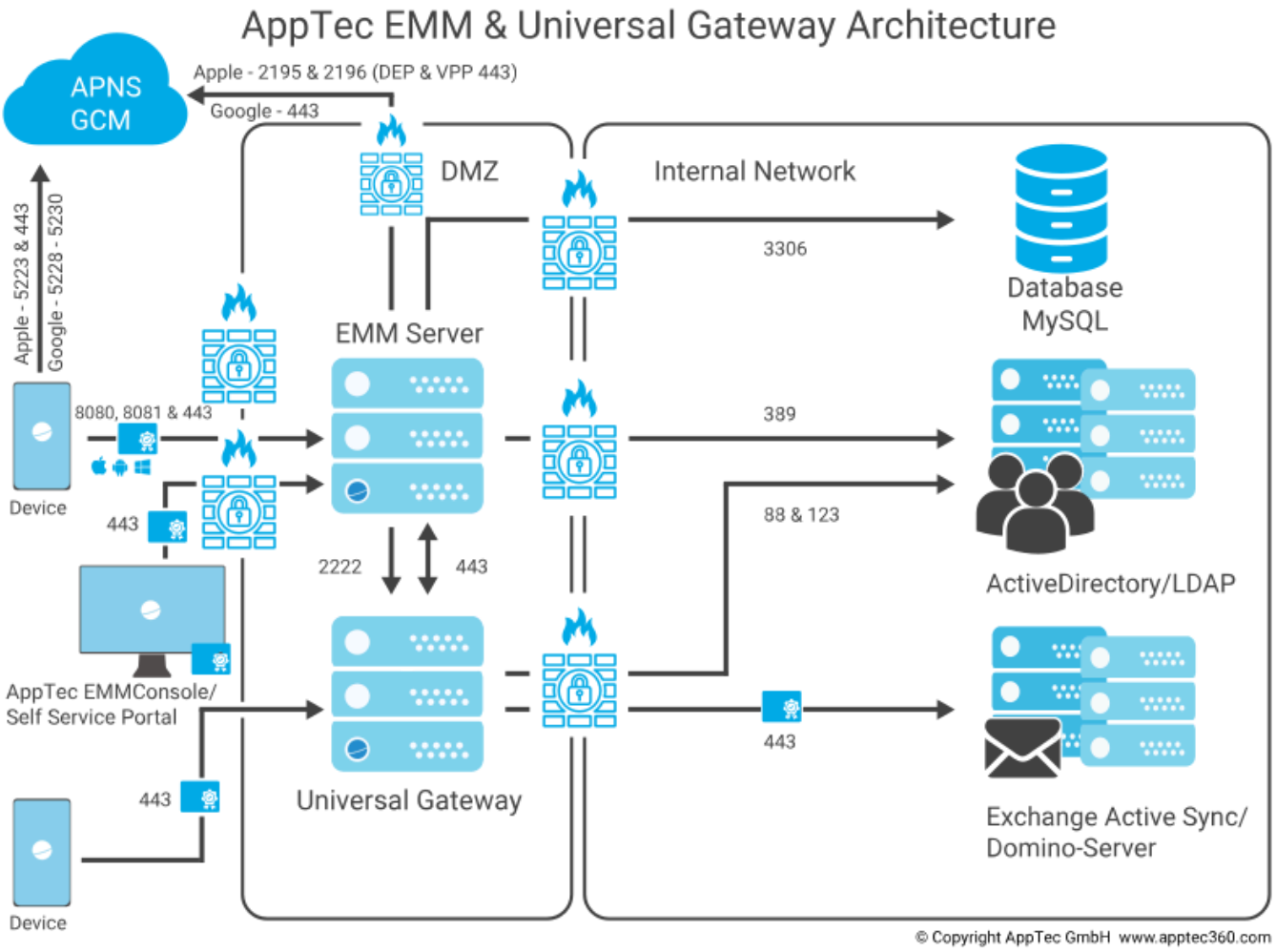
Устройствата с Windows 10 се нуждаят от специфичен сертификат за поддомейна за записване в предприятието.

От версия 202104 на уреда можете да използвате и сертификати Let's Encrypt, които се генерират автоматично (описано в Стъпка 2 - SSL сертификат).

SMTP сървър

Необходим е сървър за електронна поща и/или имейл релей, за да може AppTec360 EMM да изпраща имейли (напр. за регистрация на устройства и потвърждаване на акаунти).

Правила на защитната стена



Тази диаграма показва коя връзка е необходима в зависимост от услугите, които искате да използвате.

За по-подробно описание вижте таблицата на следващата страница.

Всички (външни/ устройства)	→	**AppTec360 Appliance / emmconsole.com**
Портове	443	Управление, Enterprise AppStore и комуникация с Windows Phone
	8080	Комуникация с Android и iOS
	80	Първа настройка на Let´s Encrypt. След това се използва 443.
Всички (устройства)	→	**Всеки (външен)**
Портове	5223, 443	Услугата Apple Push Service, трябва да е достъпна без прокси, 443 като резервен вариант, вижте https://support.apple.com/en-us/HT203609
	5228-5230	Услугата Android Push Service (FCM), трябва да е достъпна без прокси
AppTec360 Appliance	→	**Контролер на домейна**
Портове	389, (LDAPS 636)	Синхронизиране на потребители с LDAP
AppTec360 Appliance	→	**Всички**
Пристанище	443	Използва се за услугата Android Push Service (GCM) Търсене в AppStore / Play Store
AppTec360 Appliance	→	**emmconsole.com**
Портове	443	AppTec360 Appliance Updates, APNS сертификат поколение
AppTec360 Appliance	→	**Мрежа на Apple (17.0.0.0/8)**
Портове	2195, 2196	Услуга Apple Push и услуга за обратна връзка
	443	DEP И VPP

Актуализации на сигурността

Операционната система Дебиан трябва да се актуализира редовно, за да се получат най-новите поправки на сигурността. Въпреки това не преминавайте към по-нова основна версия на Дебиан ръчно. Когато AppTec360 EMM е съвместим с по-нова основна версия, ще добавим начин за обновяване в актуализация на устройството.

Пароли по подразбиране на виртуалното устройство

Потребител за вход (Входът в Root е забранен. Използвайте "sudo" за административни задачи)

apptec

Парола за вход

apptec

Потребител на MySQL Root

корен

Коренна парола на MySQL

apptec

Потребител по подразбиране на MySQL

AppTec

Потребителска парола по подразбиране на MySQL

AppTec

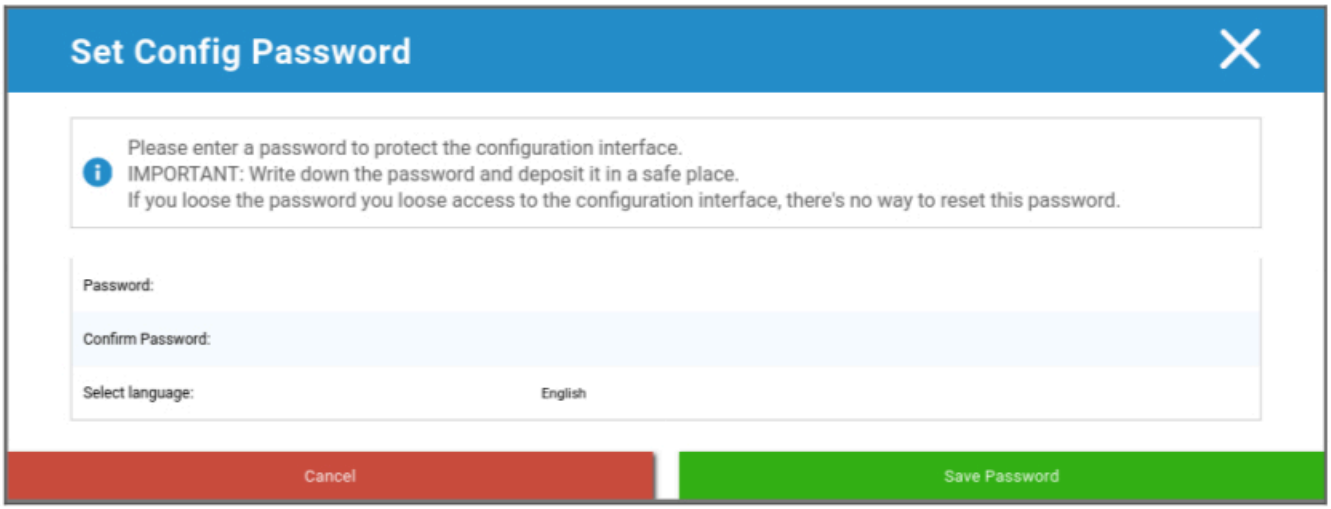
Конфигуриране на виртуалното устройство

Важно: Преди да започнете с конфигурирането на виртуалното устройство, разделителната способност на дисплея трябва да бъде настроена на поне 1280 x 800 пиксела.

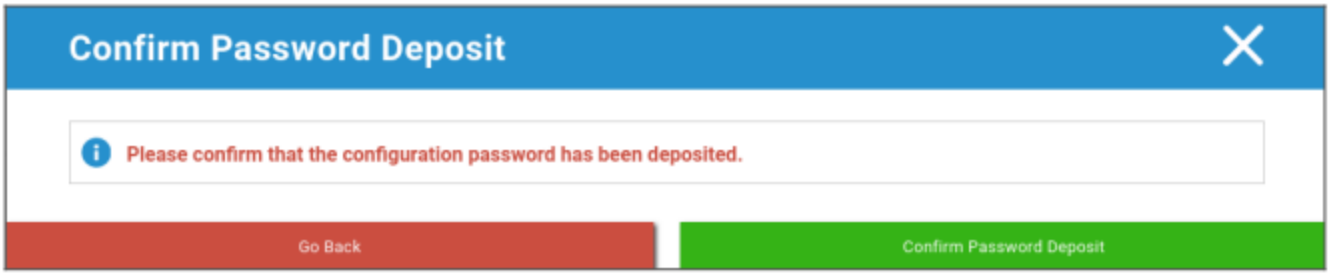
След като влезете в устройството, Firefox трябва автоматично да се стартира и да покаже интерфейса за конфигуриране.

Подготовка

Първо трябва да въведете парола за интерфейса за конфигуриране. Тази парола се използва за криптиране на цялата информация и файлове, въведени в конфигурационния интерфейс. Тук можете също така да зададете езика, на който да се показва интерфейсът (може да бъде променен по-късно).

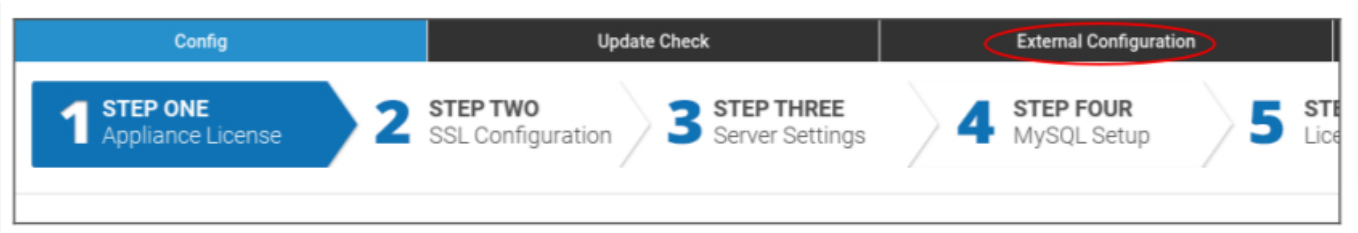


Паролата може да бъде възстановена само от поддръжката на AppTec360, затова се уверете, че сте я сложили на сигурно място и потвърдете предстоящия изскачащ прозорец.



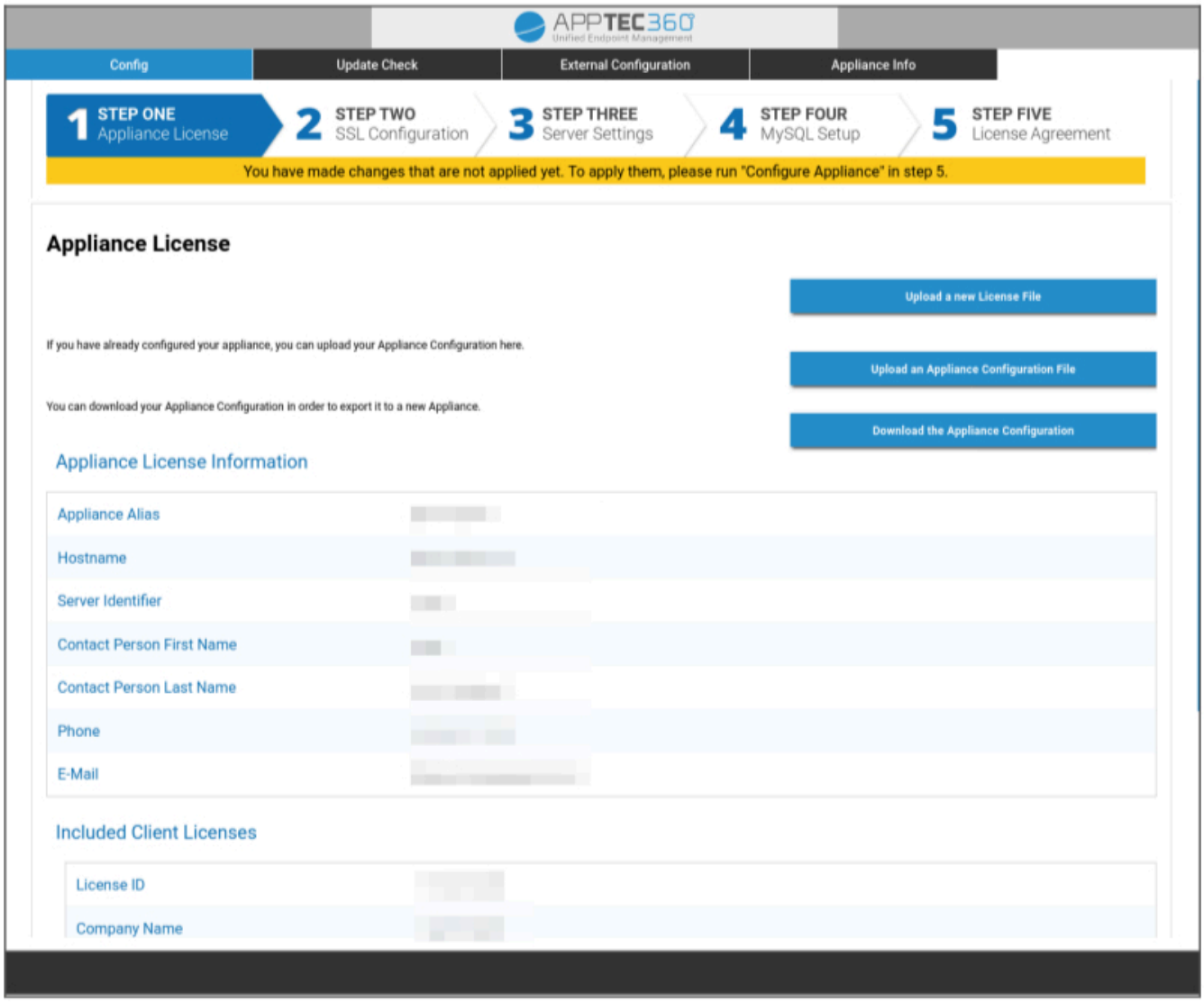
Конфигуриране от външен хост

За да улесните процеса на конфигуриране, можете да направите страницата за конфигуриране достъпна от дистанционно управление. За да направите това, следвайте стъпките в "Конфигуриране от външен хост".



Първа стъпка – Лиценз за уреда

1. Моля, качете лицензионния файл, който сте получили от AppTec.
2. Ако файлът с лицензия е бил качен успешно, можете да видите информацията за лицензия на уреда, както е показано на снимката по-долу.



Втора стъпка – SSL сертификат

Можете да използвате автоматичната настройка на сертификати с помощта на Let's Encrypt или да предоставите сертификатите сами (за повече информация вижте SSL-Certificate).

Автоматичен

Сертификатът ще бъде генериран автоматично с помощта на услугата Let's Encrypt.

AppTec360 EMM използва предизвикателството HTTP-01 за валидиране на домейна, което означава, че HTTP портът трябва да бъде отворен от интернет за първото искане на сертификат. Следващите заявки за подновяване могат да бъдат валидирани чрез HTTPS.

Превключете радио бутоните на "Automatic (Let's Encrypt)" и натиснете "SAVE VALUES". Сертификатът ще бъде поискан автоматично при прилагане на конфигурацията в стъпка пет - Лицензионно споразумение. Сертификатът ще бъде автоматично подновен, ако е необходимо, и ще получите имейл, ако срокът на сертификата изтича (което означава, че подновяването може да е неуспешно).

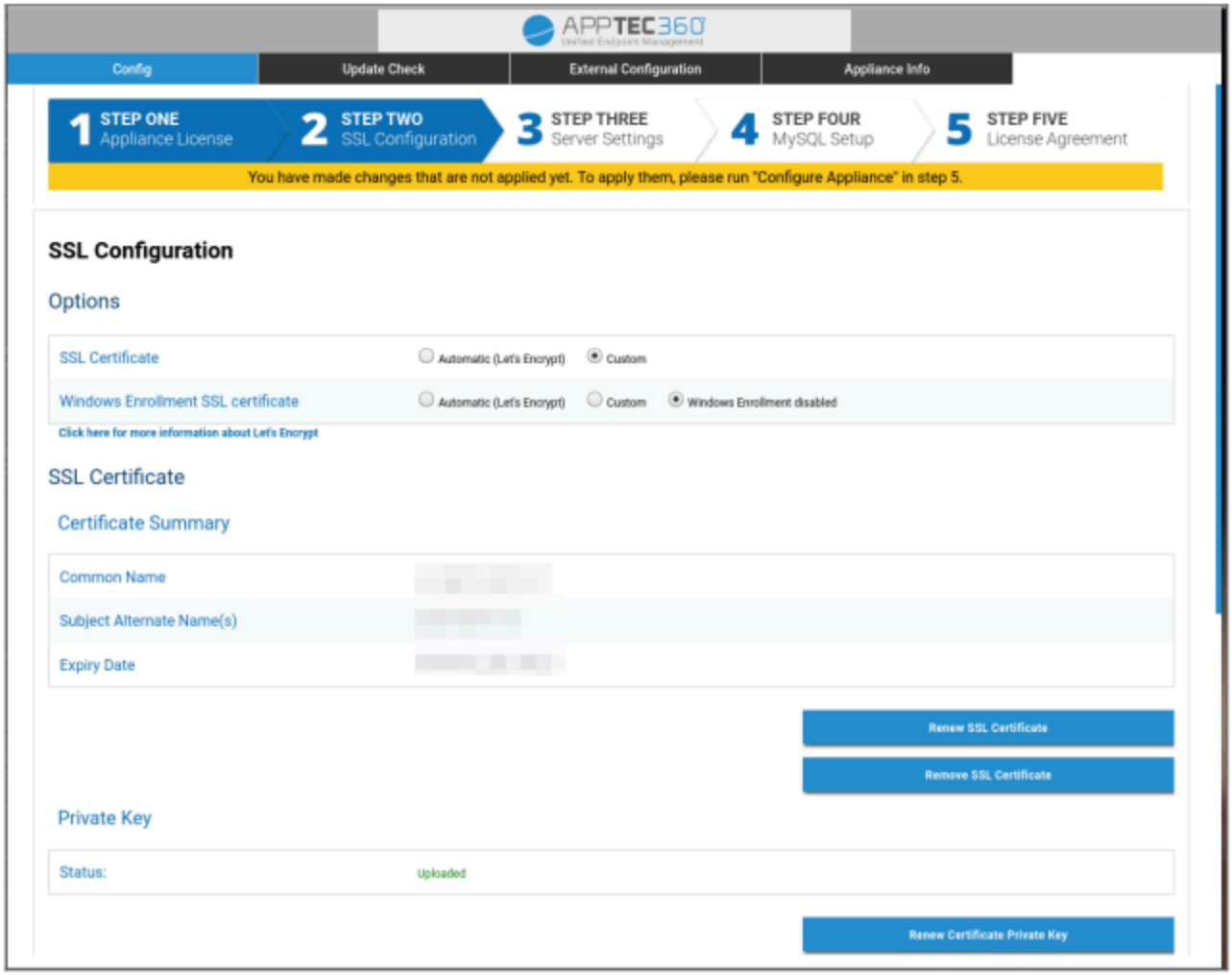
Потребителски

1. Качете SSL-сертификата за вашето лицензирано име на хост. Можете да видите името на хоста в Стъпка първа - Лиценз на уреда.

2. Моля, качете и частния ключ за сертификата и, ако е необходимо, междинния сертификат.

Важно: Ключът не трябва да е защитен с парола. Ако е защитен, премахнете паролата, преди да го качите.

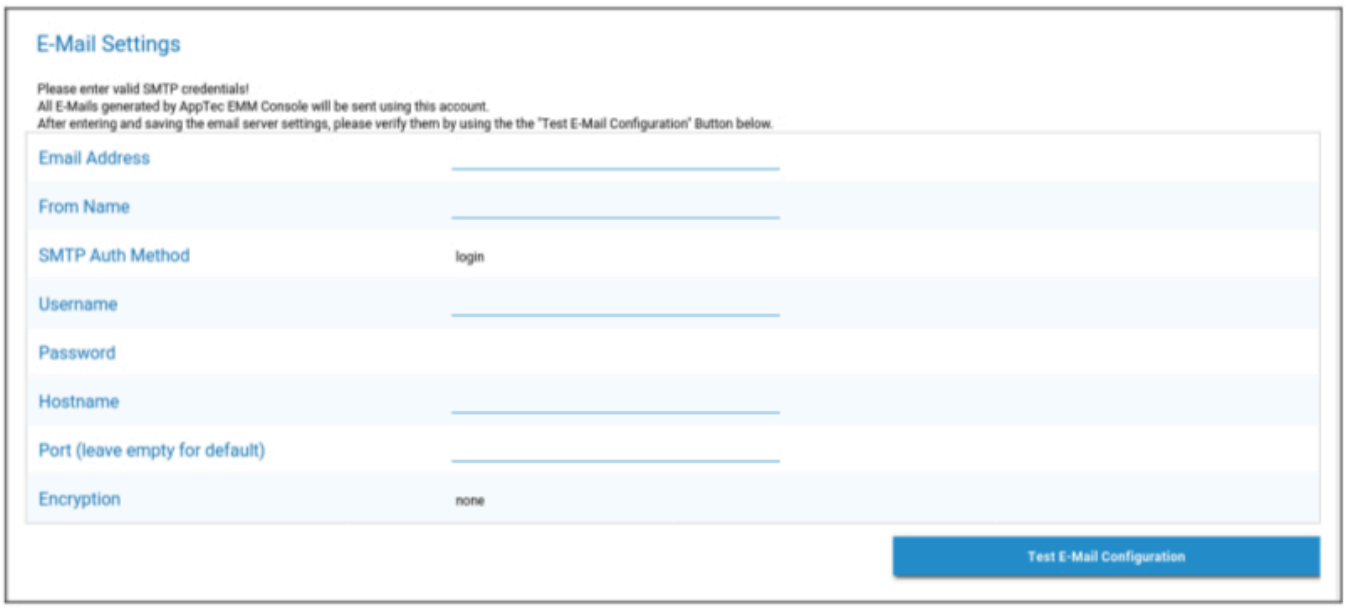
Съвет: Ако искате да използвате и устройства с Windows 10, трябва да разрешите "Windows Enrollment SSL certificate" и да качите сертификата, частния ключ и междинния сертификат за вашия поддомейн (описано в раздел IP-адрес и DNS резолюция) в долната част на страницата.



Трета стъпка – Настройки на сървъра

1. Моля, въведете глобален имейл адрес за поддръжка. Този адрес ще се използва в имейлите до вашите потребители, за да знаят към кого да се обърнат в случай на проблеми с тяхното устройство.

2. Доставка на настройки за електронна поща, които да се използват от системата за изпращане на електронни съобщения. Настройките ще се използват за изпращане на имейли до потребителя, както и за изпращане на съобщения за грешки и заявки за функции на"support@apptec360.com". След като запазите настройките за електронна поща, трябва да ги проверите, като щракнете върху "Test E-Mail Configuration" и следвате инструкциите.



Четвърта стъпка – Настройка на MySQL

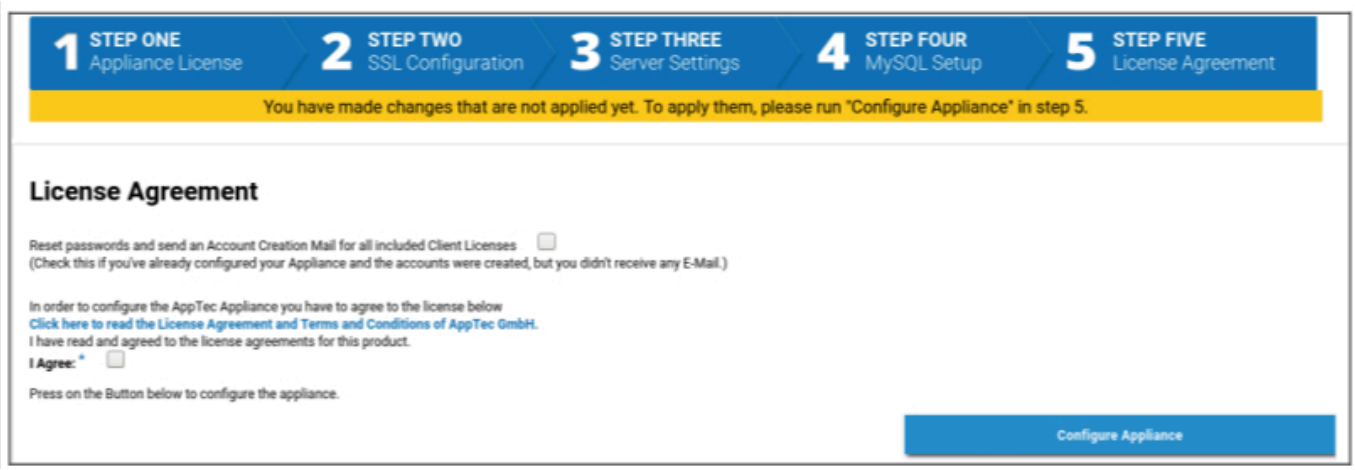
1. Ако искате да използвате вътрешната база данни, можете да пропуснете тази стъпка. В противен случай можете да въведете информацията за връзката с външния сървър за бази данни.


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)

Пета стъпка – Лицензионно споразумение

1. Моля, прочетете лицензионното споразумение.
2. Отбележете "I Agree" (Съгласен съм) и натиснете бутона "Configure Appliance" (Конфигуриране на уред), за да приложите настройките.

Съвет: За да приложите настройките, ще трябва да стартирате "Configure Appliance" всеки път, когато променяте настройките в 5-те стъпки.



Поздравления!

Завършихте конфигурирането на виртуалния уред.

На адреса, който сте предоставили за лицензa (видим в "Включени клиентски лицензи" в Стъпка 1 - Лиценз за уреда), е изпратен имейл, включващ паролата ви.

Сега можете да влезете в конзолата, като използвате тази парола и имейл адреса, на който сте я получили.

За да влезете в конзолата, въведете името на хоста на конзолата в адресната лента на браузъра си.

Можете да намерите името на хоста на вашия уред в Стъпка 1 - Лиценз на уреда.

Отстраняване на неизправности

1. Не сте получили имейл при конфигурирането на уреда в стъпка пет - Лицензионно споразумение:

Уверете се, че настройките на електронната поща в Стъпка 3 - Настройки на сървъра са правилни. За да изпратите отново паролата, проверете "Reset passwords and send an Account Creation Mail for all included Client Licenses" (Нулиране на пароли и изпращане на поща за създаване на акаунт за всички включени клиентски лицензи) в Стъпка пет - Лицензионно споразумение, преди да стартирате отново "Configure Appliance" (Конфигуриране на уреда).

2. Получили сте грешка по отношение на Let's Encrypt по време на конфигурирането в стъпка 5 - Лицензионно споразумение:

Уверете се, че уредът е достъпен чрез името на домейна си на порт 80. Let's encrypt също така записва дневник в "/var/log/letsencrypt", който може да помогне при по-нататъшното отстраняване на неизправности.

Препоръки за сигурност

Препоръчително е да извършите следните стъпки, за да защитите устройството AppTec360.

Това не е пълен набор от инструкции, а само препоръка за основна конфигурация.

- Промяна на паролата за потребителя на AppTec360
- Променете паролата на потребителите на MySQL "root" и "AppTec" и актуализирайте съответно стъпка 4 - Настройка на MySQL
- Промяна на порта по подразбиране на SSH сървъра
- Блокирайте порт 80 в конзолата си и забранете входящия HTTP трафик, използвайте само HTTPS. Веднъж конфигурирана, е възможна и външна конфигурация през HTTPS.
- Ограничаване на достъпа до интерфейса за управление само за определени потребители в долната част на трета стъпка - Настройки на сървъра
- Конфигуриране на защитната стена

Общи настройки

Преглед на профила

Информация за профила

Преглед

Тук можете да видите общ преглед на вашия акаунт в AppTec360.

Име на компанията	Името на вашата компания
Дата на създаване	Дата на създаване на вашата сметка
Вид лиценз	Paid = платен лиценз Свободен = неплатен лиценз Бележка: По технически причини сметките на локално устройство винаги се показват като платени.
Идентификатор на клиента	Идентификатор на вашата сметка (това НЕ е вашият клиентски номер)
Дата на изтичане на лиценза	Дата на изтичане на лиценза ви за AppTec360
Лиценз за ContentBox	Безплатно = безплатен лиценз за 25 устройства Платен = платен лиценз за x устройства
Стартиране	Показва дали можете да използвате персонализирания стартъп за Android
Устройства	Брой на използваните в момента лицензи / общ брой лицензи
Лице за контакт	Осигурено лице за контакт
Телефон	Предоставен телефонен номер
Електронна поща*	Предоставен имейл адрес
Потребител на корена	Потребители на Root, които могат да влизат в системата
Версия на софтуера	Текуща версия на софтуера

**Забележка: Посоченият тук имейл адрес е този, който сте въвели при регистрацията на акаунта. Въз основа на него в дървото на потребителите/устройствата ще бъде създаден потребител, който може да бъде променян. Редактирането на този потребител ще*

промени имейл адреса, който трябва да използвате за влизане, но не и информацията в прегледа на профила .

Доклад за грешка

Доклад за грешка може да бъде изпратен директно до поддръжката, за да съобщите за проблеми или грешки, и включва информация и записи за вашия акаунт и настройки.

Тема	Предметът на доклада за грешка. Включете номер на билета, ако искате да го добавите към съществуващ билет за поддръжка.
Очаквано поведение	Опишете подробно какво сте направили и какво сте очаквали да се случи
Действително поведение	Опишете подробно какво точно се е случило. Моля, цитирайте точно съобщенията за грешки. Също така ще ви помогне, ако добавите скрийншоти към прикачения файл.
По кое време се появи проблемът?	Моля, посочете точен момент, в който сте получили конкретно съобщение за грешка/проблем. В най-добрия случай включете и секундите, например 18:55:27
Може ли проблемът да се повтори? Ако да, как (подробно)?	Опишете подробно как можете да възпроизведете проблема.
Работила ли е тази функция преди това според очакванията ви? Ако да, до кога?	Оставете празно, ако не знаете.
Имаше ли някакви конкретни промени в системата, направени преди появата на този проблем? Ако да, какви промени (подробно)?	Винаги споменавайте каква е била последната ви промяна или действие преди появата на проблема, дори и да смятате, че това е без значение.
Ако е приложимо: Кои модели устройства и версии на операционната система са засегнати?	Винаги посочвайте точната версия на операционната система (напр. iOS 14.7.1 или Android 11)
Ако е приложимо: Какъв е публичният IP адрес или/и серийният номер на устройството?	Посочете поне едно, дори ако са засегнати всички устройства.
Включване на регистрационни файлове	Поставете тази отметка, за да изпратите регистрационния файл с доклада за грешка. Това е препоръчително да се направи.
Извличане на текущото състояние на VPP от Apple и включване в доклада за грешка	Включва информация за присвояването на лицензи за VPP. Активирайте го само ако ви помолят за това

	от поддръжката или ако проблемът ви е свързан с VPP.
Приложение	Приложете всеки файл, който може да бъде полезен (напр. Снимки на екрана на съобщение за грешка)

Заявка за функция

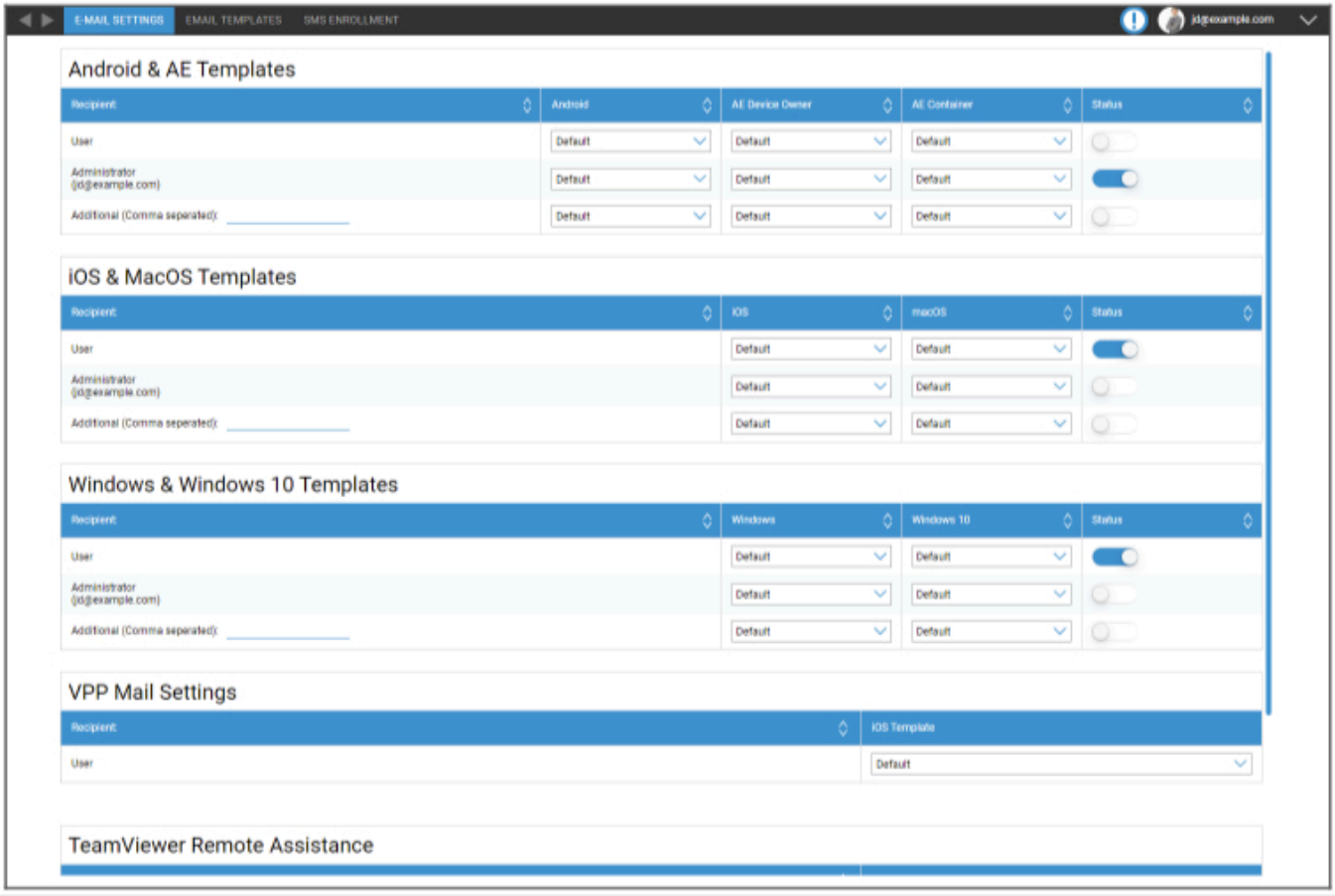
Заявка за функция може да бъде изпратена директно до поддръжката. Тя може да съдържа искане за конкретна функция или подобрение за

Резюме	Кратко резюме на проблема ви
Описание	Подробно описание на вашия проблем, моля, бъдете възможно най-конкретни.
Приложение	Прилагане на файлове към доклада за грешка

Глобално конфигуриране

Настройки на електронната поща

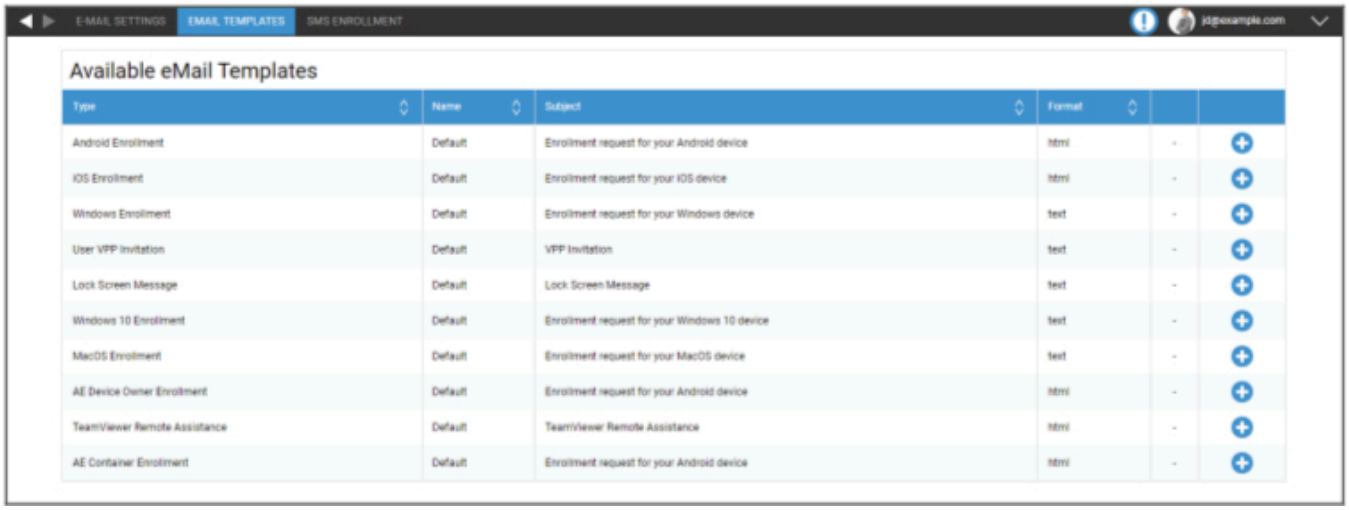
Тук можете да определите кой да получи писмо, когато се генерира заявка за записване, и кой шаблон за текст ще се използва за това писмо.



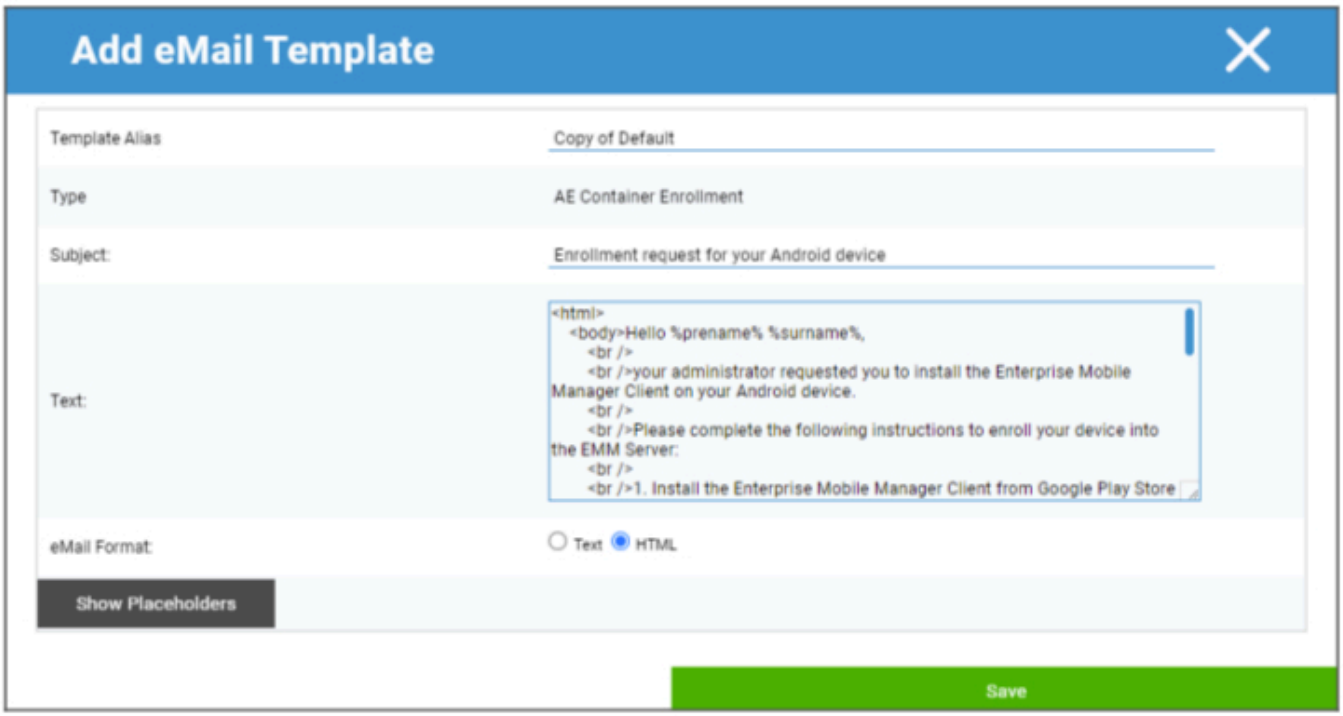
Шаблони за електронна поща

Тук можете да генерирате и редактирате своите шаблони за различни сценарии. Те могат да бъдат в нормална текстова форма или в HTML. При HTML можете да контролирате по-добре форматирането на текста.

Шаблоните по подразбиране не могат да се редактират или изтриват.



Можете също така да използвате заместващи символи като променлива, която ще бъде заменена автоматично. Щракнете върху "Show Placeholders" (Показване на заместващи символи) по време на редактиране, за да видите наличните заместващи символи. Различните категории имат различни Placeholder.



Записване в SMS

Тук можете да въведете/активирате процеса на SMS записване.

(По подразбиране: деактивиран)

Ще видите и дисплей, който показва колко SMS кредита са все още налични.

SMS кредитите трябва да бъдат закупени отделно.

Поверителност

Достъп до GPS

Тук можете да защитите GPS изгледа за всяко устройство с 1 или 2 пароли (принцип на четирите очи). Ще бъдете подканени да въведете паролата(ите) всеки път, когато се опитате да получите достъп до местоположението на дадено устройство.

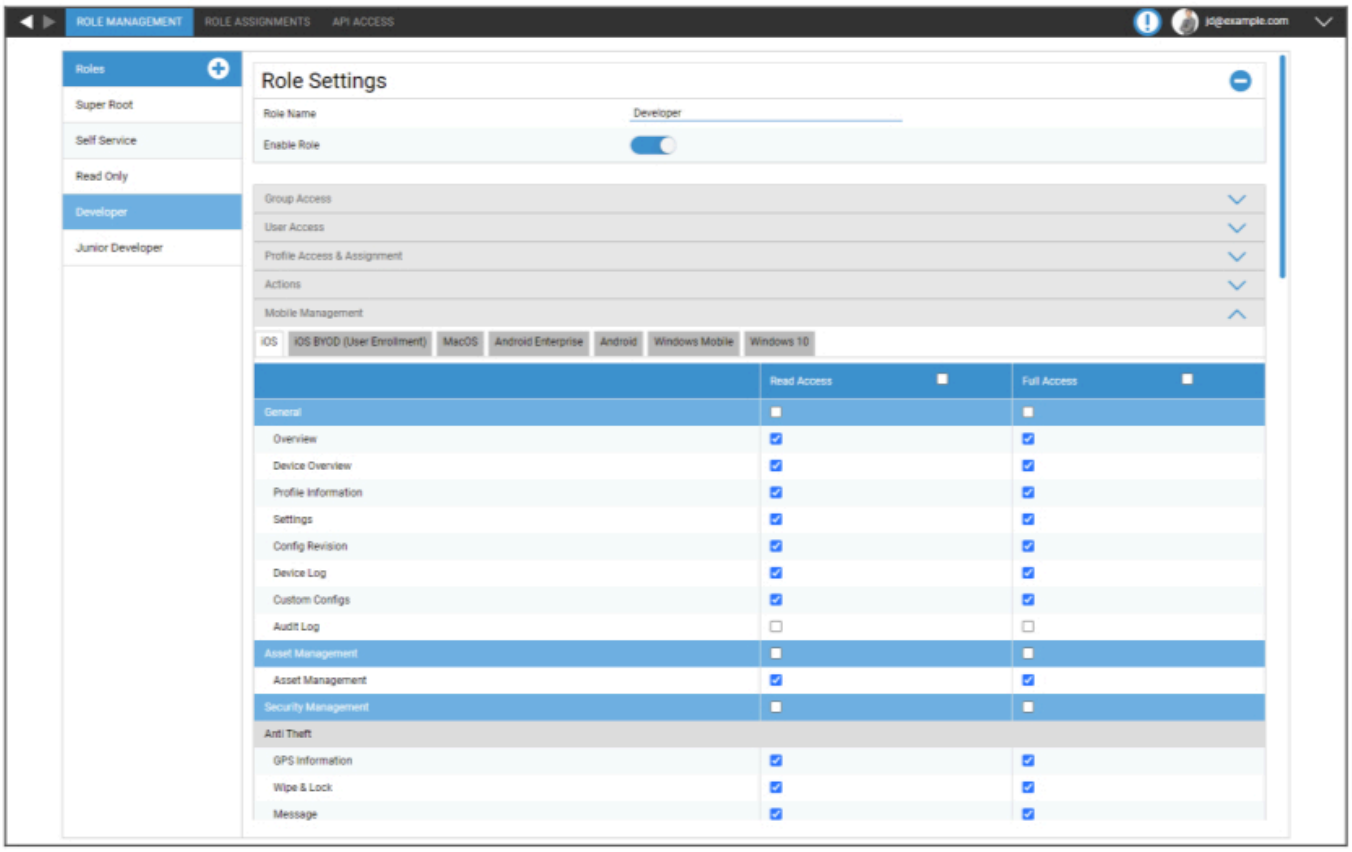
Ограничаване на достъпа до настройките на GPS	Изключено = функцията е изключена и не се изисква парола за локализиране.
	Включено = функцията е включена и се изисква парола за локализиране.
Метод на защита	Използване на една парола = използване на една парола за локализиране
	Използване на две пароли = използване на две пароли за локализиране
Въвеждане на парола (1)	Въведете избраната парола
Повтаряне на паролата (1)	Повторно въвеждане на избраната парола
по избор: Въведете парола 2	Въведете втората избрана парола
по избор: Повтаряне на парола 2	Повторно въвеждане на втората избрана парола

Забележка: След като зададете паролата си, трябва да я въведете още веднъж, преди да бъде напълно активирана.

Достъп, базиран на роли

Управление на роли

Ролите определят какво може да вижда и прави даден потребител, когато влезе в конзолата за управление. Това ви позволява да създавате потребители, които могат да влизат в системата, но имат ограничена функционалност.



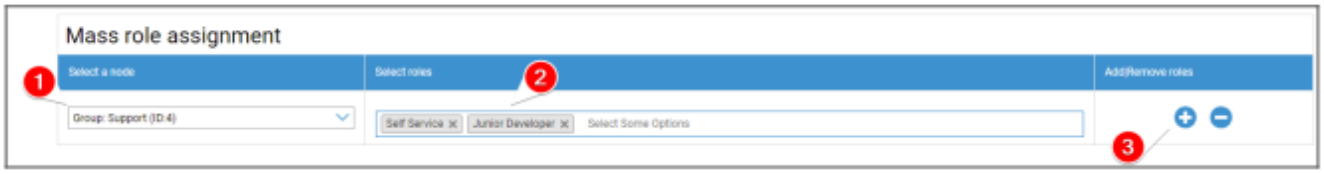
Ролята Super Root е роля по подразбиране, която винаги може да вижда и променя всичко. Тя не може да бъде променяна или изтривана. Ролята за самообслужване може да вижда само собствените си потребители и устройства. Можете да комбинирате Self Service (Самообслужване) и потребителска роля, за да позволите например на потребителите да влизат и да регистрират устройства самостоятелно и само за своя потребител.

Потребителските роли могат да се активират или деактивират ръчно. Новите роли са деактивирани по подразбиране. Потребителите с деактивирана роля работят така, сякаш не притежават тази роля. Това ви позволява напр. временно да ограничите действията на дадена роля.

Всички разрешения са разделени на "Достъп за четене" и "Пълен достъп". Предоставянето на достъп за четене на дадена роля ѝ позволява да вижда конкретната част от конзолата. Предоставянето на Пълен достъп позволява на Ролята да вижда и променя конкретната част от конзолата.

Присвояване на роли

Тук можете да прегледате всички потребители, които имат роля, и да видите коя от тях имат. Тук можете също така да присвоите роля на потребители или на цели групи:

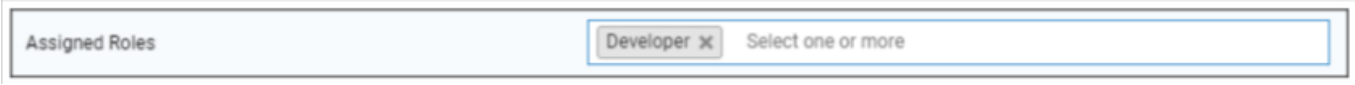


1. Изберете за коя група или потребител искате да добавите или премахнете роли. Можете да изберете отделен потребител или група. Когато изберете група, промяната ви ще засегне всички потребители в тази група и всички потребители на подгрупи в рамките на избраната група.
2. Изберете ролята, която искате да добавите или премахнете. Можете да изберете една или няколко роли.
3. . Select what operation you want to perform. Clicking the “+” adds the selected roles if the user(s) did not have them already. Clicking the “-” removes the selected roles from the user(s). If you add roles to a user which did not yet have any role, it will automatically enable “Can Login” for the user.
4. Запишете, за да завършите процеса. Потребителите, които преди това не са имали роля и "Може да влезе" е било забранено, автоматично ще получат имейл с връзка за задаване на парола.

Под присвояването на масовата роля можете да намерите преглед на присвоените роли. Там можете също така ръчно да променяте ролите за конкретни потребители.

Присвояване на роля

За да присвоите роля на потребител, трябва да отидете в Mobile Management, където се намира дървото на вашите групи, потребители и устройства. Редактирайте потребителя, за да му присвоите роля. Като алтернатива можете да използвате гореспоменатия метод и само за отделни потребители.



Достъп до API

Достъп до AppTec360 REST API

AppTec360 REST API изисква удостоверителен токен (API ключ) и частен ключ, които трябва да бъдат генерирани в конзолата за управление.

За да направите това, влезте в AppTec360 EMM и отидете на

Общи настройки → Достъп на база роли → Достъп до API и добавете нов ключ.

Трябва да изберете потребител, чиито разрешения ще се прилагат към API ключа.

Частният ключ може да бъде изтеглен само веднъж. След като изтеглянето започне, ключът ще бъде изтрит, а бутонът "Изтегляне" ще изчезне.

Ако загубите частния си ключ, трябва да генерирате нов API ключ.

Общи правила

- REST API е достъпен под базовия URL адрес:

/public/external/api

- Всички заявки трябва да се изпращат чрез POST.
- REST API поддържа само заявки през HTTPS.
- Заявките трябва да съдържат следните заглавия:

Име на заглавието	Стойност на заглавието	Описание
Тип съдържание	application/json	фиксиран
авт.	123...xyz	API ключ от раздела "Достъп до API"
подпис	Подпис, кодиран в Base64	Подпис на полезния товар, генериран с частен ключ от раздела "Достъп до API"

- Тялото на заявката трябва да бъде кодиран в json обект, който трябва да съдържа следните стойности:

Поле	Пример за поле Стойност	Описание
api	v2/device/listdevices	Име на API
време	1529662725	Unix Timestamp (UTC) на клиентската машина. Максимално допустимата разлика във времето между клиента и сървъра е 30 минути.

- При успех API връща заявените данни (вж. Запитвания по-долу) и HTTP код на състоянието 200.
- Ако възникне грешка, кодът на състоянието на HTTP ще бъде между 4xx и 5xx в зависимост от грешката, а обектът на отговора ще съдържа масив с ключ "errors", който съдържа списък със съобщения за грешки, които могат да бъдат разчетени от човека.
- Ако за дадено устройство няма подходящи данни, ще бъде върнат празен масив.
- Ако Id на устройството не съществува, върнатите данни ще бъдат нулеви.

Пример за заявка

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]}}

Запитвания

Списък на всички устройства

Функционалност: Връща списък на всички устройства, съдържащ идентификатора на устройството, IMEI и серийния
API URI: v2/device/listdevices
Задължителни параметри: няма
Незадължителни параметри: няма

Пример за тяло на заявка


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


Пример за тяло на отговор


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

Получаване на списък с (GPS) позиции

Функционалност: Връща списък на всички съхранени записи в дневника на позициите за идентификатори на устройства
API URI: v2/device/listposition
Задължителни параметри: "ids" - масив от идентификатори на устройства
Незадължителни параметри: none

Пример за тяло на заявка


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


Пример за тяло на отговор


```
{
"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":[],
]
}
```

Получаване на карта на активите

Функционалност:
Връща списък на всички съхранени възможни активи, които да бъдат поискани с помощта на Get any asset data (Получаване на данни за всеки актив).
Можете да използвате формата за четене от човека или етикета на актива, за да поискате данните.
API URI: v2/device/getassetmap
Задължителни параметри: няма
Незадължителни параметри: няма

Пример за тяло на заявка

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

Пример за тяло на отговор

Този отговор е съкратен с цел по-добра четимост.

```
{
"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": []
}
```

Получаване на данни за всеки актив

Функционалност: Връща списък със заявените данни за активи за идентификатори на устройства
API URI: v2/device/getassetdata
Задължителни параметри: "ids" - Масив от идентификатори на устройства
Незадължителни параметри:
"assetkeys" - Ключове за връщане на данни за активи. Ако не са посочени, ще бъдат върнати всички налични данни за активи
. Можете да получите списък на ключовете на активите, като използвате Get asset map (Получаване на карта на активите).

Пример за тяло на заявка


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


Пример за тяло на отговор


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

Примерен код в 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)
```

Конфигурация на Apple

APNS сертификат

Тук можете да качите сертификат APNS. То е необходимо за управление на устройства с iOS и MacOS.

Забележка: Сертификатът APNS е валиден само за една година. То трябва да бъде подновено преди изтичането му. Процесът на подновяване е идентичен със създаването (вж. по-долу) и отнема само няколко кратки минути.

Ако забравите да го подновите навреме, не можете да правите промени във вече регистрираните си устройства. **и трябва да регистрирате всички устройства отново.**.

Стъпка 1

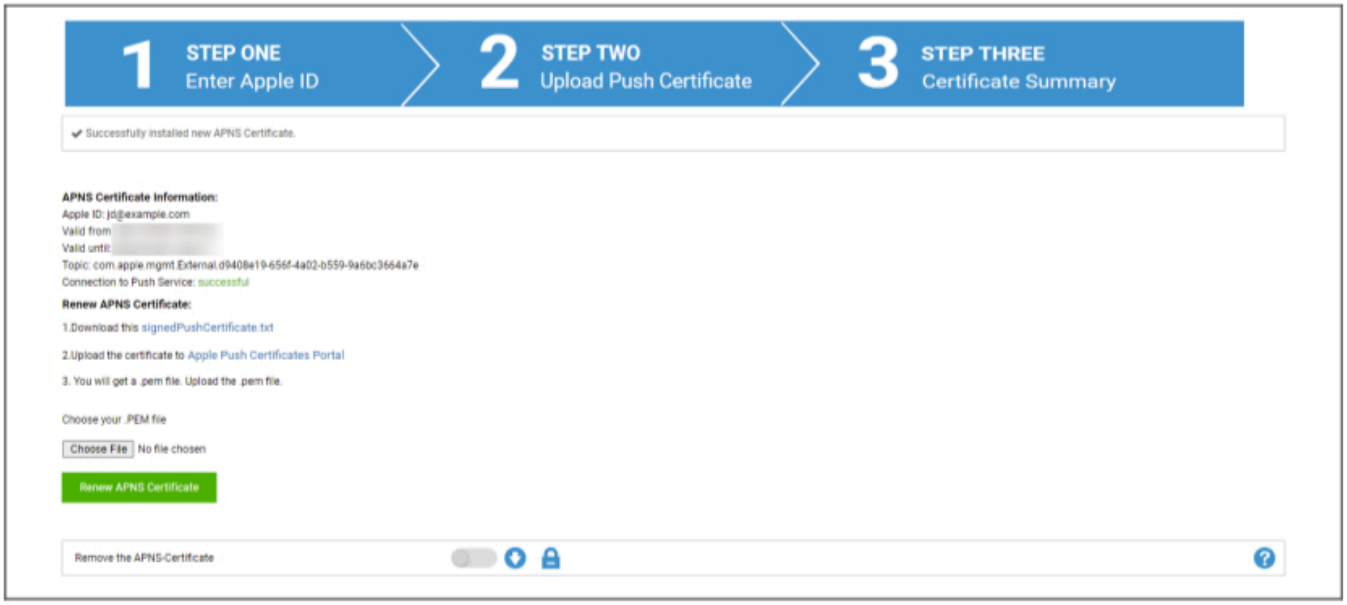
- Първо въведете своя Apple ID, който искате да използвате за създаване на APNS сертификат.

Забележка: Този идентификатор на Apple се използва само за създаването на сертификат APNS. Този идентификатор на Apple няма нищо общо с устройствата и устройствата няма да знаят за този идентификатор на Apple. Освен това ви е необходим достъп до този Apple ID, за да подновите сертификата APNS. Затова се препоръчва да използвате някакъв общ Apple ID и да документирате данните за вход. Преди изтичането на валидността на сертификата APNS се изпраща напомняне на използвания пощенски адрес на Apple ID.

- Щракнете върху "Следваща стъпка", за да продължите.
- (по избор) Можете също така да възстановите изтрития преди това сертификат APNS, ако сте го изтрили по погрешка

Стъпка 2

- Изтегляне на подписанияPushCertificate.txt
- Отидете на https://identity.apple.com/pushcert/ и влезте с Apple ID от стъпка 1
- Кликнете върху "Създаване на сертификат".
- (по избор) въведете бележка. Това може да е полезно, ако управлявате няколко наематели, за да ги идентифицирате лесно.
- Кликнете върху "Choose File", за да изберете изтегления по-рано signedPushCertificate.txt
- Кликнете върху "Качване".
- Сега ще видите потвърждението, че сте създали сертификат APNS.
- Кликнете върху "Изтегляне" и го запазете.
- Върнете се в конзолата за управление.
- Кликнете върху "Изберете файл" и изберете сертификата APNS, който искате да качите.
- Кликнете върху "Качване"



Стъпка 3

Вече успешно сте настроили сертификата APNS и можете да управлявате устройства с iOS и MacOS.

В стъпка 3 ще видите преглед на използвания в момента сертификат APNS.

Също така имате възможност да подновите сертификата APNS, като следвате стъпките, показани на екрана. Имайте предвид, че трябва да го подновите, преди да е изтекъл срокът му.

Когато подновявате сертификата APNS, не забравяйте да влезете с Apple ID, показано в Стъпка 3, както и да подновите използвания преди това сертификат, а НЕ да създавате нов. Ще видите "темата" на сертификата APNS в Стъпка 3 и когато щракнете върху "i" в портала за сертификати Apple Push. Това е уникалният идентификатор, който идентифицира сертификата. Това ще ви помогне да идентифицирате правилния и да подновите правилния.

Когато получите съобщение "Error: При подновяването на сертификата Push има различна тема!", това означава, че сте подновили друг сертификат или сте създали нов.

Ако искате да качите нов сертификат, например ако вече нямате достъп до използвания преди това Apple ID, първо трябва да изтриете текущо качения сертификат.

Така или иначе, изтриването на сертификата APNS означава, че вече не можете да правите промени за записаните в момента устройства, докато не ги запишете отново. Затова се уверете, че сте подготвени за това и премахвайте сертификата само ако няма друг начин.

Управляван достъп

Тук можете да активирате User-Enrollment for iOS Devices и Shared iPad for iOS Devices.

Записване на потребители

"Записване на потребител" активира специален режим за BYOD устройства.

За всеки потребител трябва да се създаде управляван Apple-ID в Apple Business Portal.

По време на процеса на записване потребителите ще бъдат помолени да предоставят своите идентификационни данни за Apple-ID.

"Вписване на потребител" гарантира максимална безопасност за потребителя, тъй като позволява само ограничен набор от настройки и ограничения, които могат да бъдат конфигурирани от MDM.

Управляван домейн:

Домейнът, използван за съпоставяне на имейл адреса на потребителя с управлявания от него Apple-ID (трябва да бъде във формат: "@appleid.company.com").Например john.doe@example.com ще бъде съпоставен с john.doe@appleid.company.com.

Проверете в Бизнес мениджъра на Apple, за да видите своя управляван домейн

Споделен iPad

Споделеният iPad е DEP устройство, конфигурирано със специален DEP профил.

Това позволява на няколко потребители да влизат в устройството, като използват управляваната от тях Apple-ID.

Управляваният Apple-ID трябва да бъде създаден в бизнес портала на Apple или в Apple School Manager.

От потребителите, които влизат в споделен iPad, се изисква да предоставят своите управлявани идентификационни данни Apple-ID.

Управляван домейн:

Домейнът, използван за съпоставяне на имейл адреса на потребителя с управлявания от него Apple-ID (трябва да бъде във формат: "@appleid.company.com").Например john.doe@example.com ще бъде съпоставен с john.doe@appleid.company.com.

Проверете в Бизнес мениджъра на Apple, за да видите своя управляван домейн

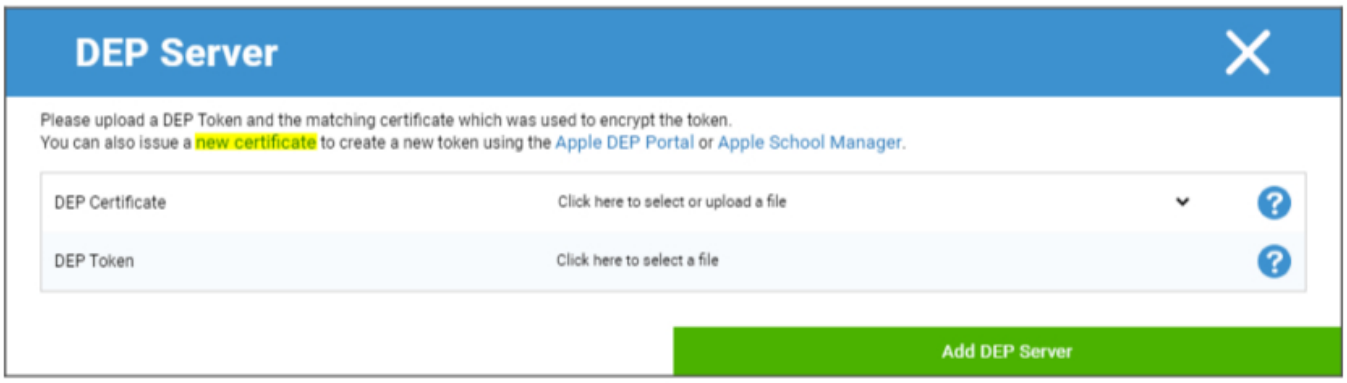
DEP

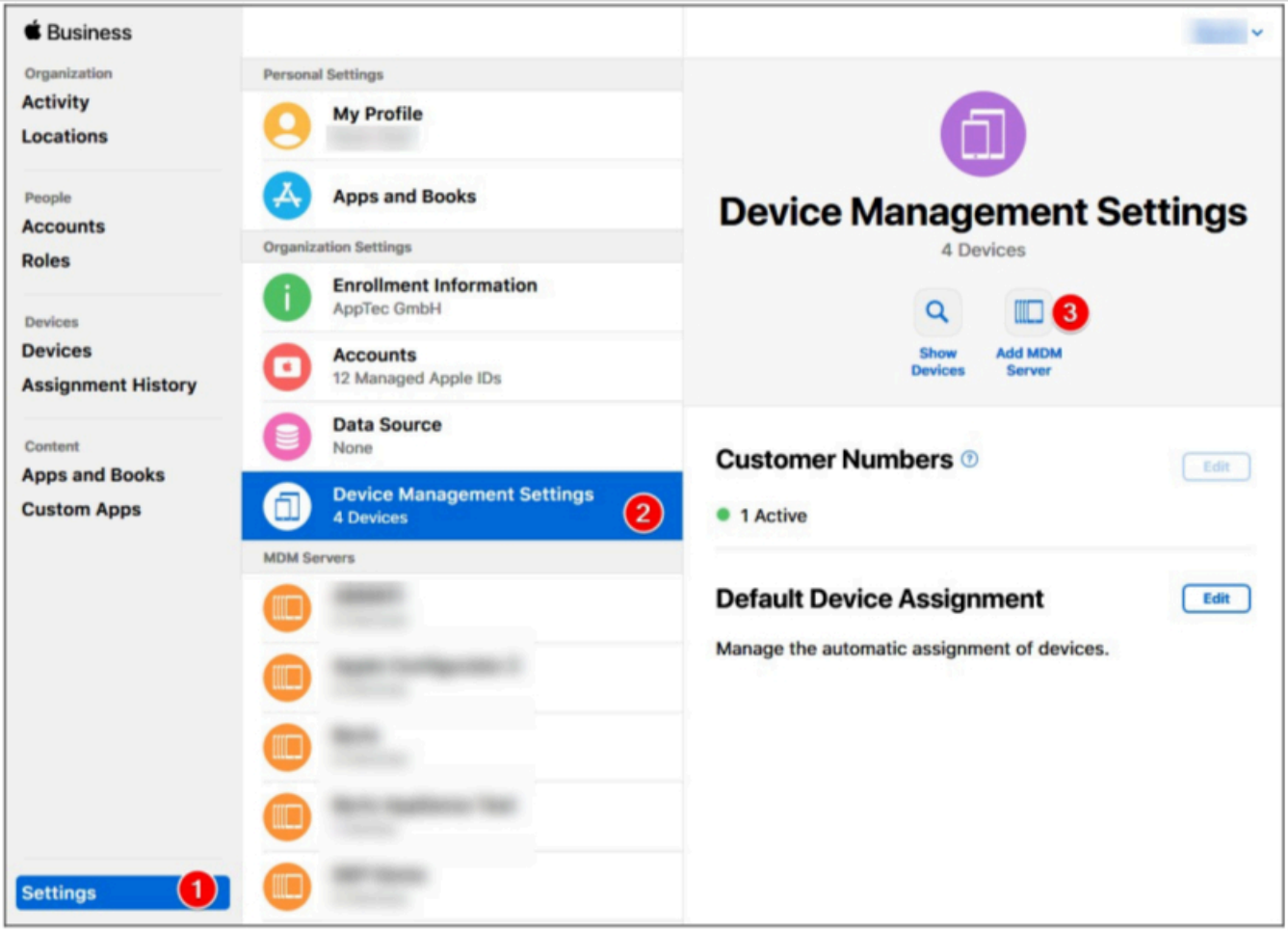
DEP (Device Enrollment Program - Програма за записване на устройства) ви позволява лесно да записвате устройства в MDM. Когато използвате DEP, устройствата ще бъдат автоматично свързани към MDM при настройката на устройството. Можете също така да прескочите почти всички стъпки за настройка, които обикновено са задължителни в iOS.

Имайте предвид, че трябва да закупите устройствата от дистрибутор, който поддържа DEP. За повече информация се свържете с вашия дистрибутор или с Apple.

Повече информация за DEP: https: //www.apple.com/business/dep/

Щракнете върху "+", за да добавите DEP токен. В изскачащия прозорец щракнете върху "new certificate" (нов сертификат) в текста (отбелязан в жълто на изображението по-долу). Това ще генерира и изтегли DEP сертификат. След това отидете в Apple Business Manager(https://business.apple.com/) или Apple School Manager(https://school.apple.com/).

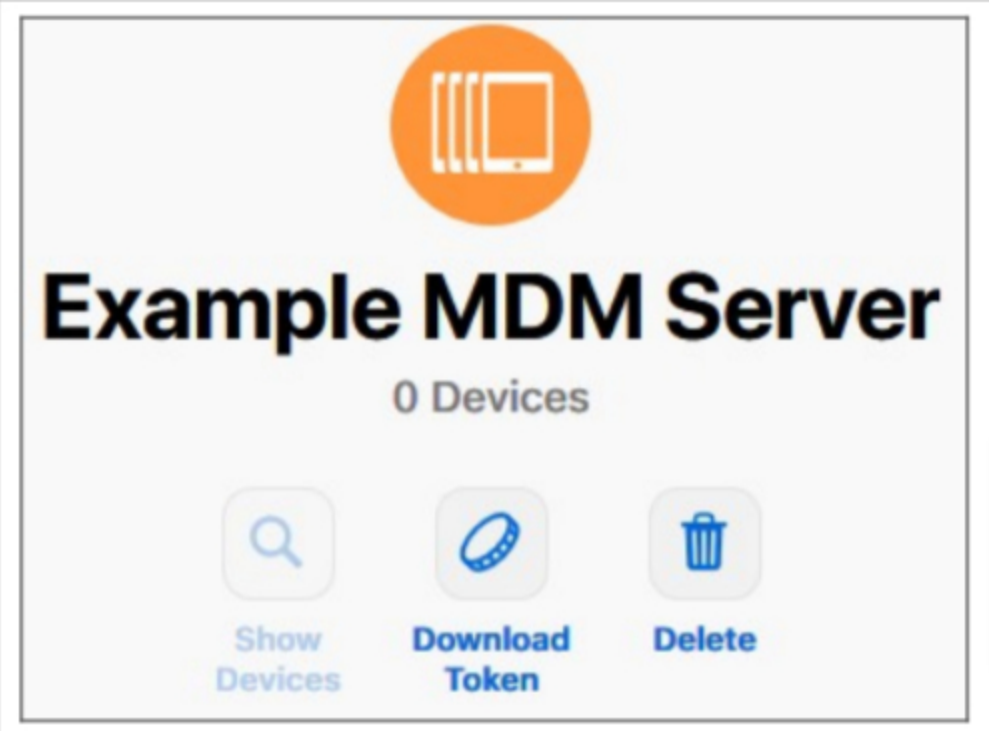




В Apple Business Manager следвайте стъпките, показани на изображението по-горе. Настройки → Настройки за управление на устройствата → Добавяне на MDM сървър.

Дайте желаното име на сървъра и качете предварително изтегления DEP сертификат в менюто MDM Server Settings → Upload Public Key и кликнете върху "Save".

Сега ще имате възможност "Изтегляне на токена". Кликнете върху нея и я запазете. Токенът е валиден само за 1 година. Но само като кликнете отново върху "Изтегляне на токена", ще получите нов, което прави подновяването на токена много лесно.



Сега можете да се върнете в MDM, откъдето преди това сте изтеглили сертификата DEP. Ако не сте затворили раздела, изскачащият прозорец за добавяне на DEP сървър трябва да е отворен и DEP сертификатът вече да е избран. Сега можете да качите своя токен в полето "DEP Token" и да щракнете върху DEP Server.

В колоната "**Devices" (Устройства**) ще видите броя на устройствата, които са присвоени към този DEP Server. Устройствата, добавени към този DEP сървър, ще бъдат автоматично създадени в DEP пула в Mobile Management.

Можете да щракнете върху този номер, за да получите преглед на всички DEP устройства и тяхното състояние.

Забележка: В зависимост от работния процес или конфигурацията в Business Manager е възможно да се наложи ръчно задаване на тези устройства към DEP Server. Можете също така да зададете DEP сървър по подразбиране в Apple Business Manager за нови устройства.

В колоната "**Профили**" ще видите броя на профилите DEP, с които разполагате. Можете също така да щракнете върху това число, за да видите подробна информация за вашите DEP профили и да изтриете стари/неизползвани профили. Понастоящем не е възможно да ги променяте. Ако искате да направите промяна, трябва да създадете нов такъв.

В колоната "**Последна синхронизация**" можете ръчно да синхронизирате сървъра DEP (например ако току-що сте добавили ново устройство към DEP) и да видите датата на последната успешна синхронизация.

В колоната "**Автоматичен профил**" можете да зададете профил DEP като автоматичен по подразбиране. Този профил ще бъде присвоен автоматично на нови устройства. Ако не зададете автоматичен профил, ще трябва всеки път ръчно да задавате профил на новите устройства.

В колоната "**Добавяне на профил**" можете да добавите нов профил DEP. Устройството ще го получи в началото на настройката на устройството. Профилът DEP определя как се настройва устройството и кои стъпки за настройка ще бъдат прескочени.

Забележка: след като устройството е регистрирано, тези настройки могат да бъдат променени само чрез възстановяване на фабричните настройки и регистриране на устройството с нов профил. Това е особено важно за "**Removable" (Премахване)**и "**Allow pairing**" (**Разрешаване на сдвояване**). В случай на "**Allow pairing**" (**Позволи сдвояване**) е препоръчително да се включи, тъй като това може да бъде забранено чрез MDM ограничения, но не може да бъде включено отново, ако е забранено в DEP профила.

В колоната "**Редактиране**" можете да качите нов токен, например при подновяване на токен.

Конфигуратор и URL

URL адреси за записване в басейна

Тук можете да създадете URL адрес за записване и QR код за записване, който е валиден за определен период на записване и до определена дата. Това ви позволява да записвате множество устройства, които използват само една връзка или QR код.

Устройствата, записани с този URL адрес или QR код, ще бъдат в пула в управлението на мобилни устройства и след това трябва ръчно да ги присвоите на група или потребител.

Бележка: това се отнася само за ръчно записване. Не използвайте този URL адрес, ако записвате устройствата чрез Apple Configurator.

MDM профил – Конфигуратор на Apple

Тук можете да получите URL адреса, който ви е необходим при записването на устройства чрез Apple Configurator. Докато подготвяте устройствата с Apple Configurator, можете да добавите устройствата към MDM в същия процес. За тази цел Apple Configurator изисква този URL адрес.

Устройствата, добавени чрез Apple Configurator, ще бъдат в пула в Mobile Management и след това ще трябва ръчно да ги присвоите на група или потребител.

Тук ще намерите и файл .mobileconfig, който може да се използва за регистриране на устройствата чрез Apple Configurator. Във всеки случай се препоръчва използването на URL адреса.

Конфигурация на Android

Конфигурация на Android

Деинсталиране на защита	Ако тази функция е активирана, потребителят не може да деактивира администратора на устройството, без да въведе паролата, зададена от администратора на MDM. Паролата се задава по време на регистрацията, така че устройствата трябва да бъдат регистрирани отново, за да се актуализира паролата. Има два варианта за премахване на администраторите на устройства: 1. Ръчно в устройството ◦ Отворете приложението EMM на устройството ◦ Преминете към раздела Статус ◦ Докоснете "Деинсталиране на защита" ◦ Въведете паролата Можете да използвате Ревизия, за да получите правилната парола от "История на паролите" в конзолата. ◦ Превъртете надолу и докоснете новодобавената точка, "Докоснете, за да деинсталирате AppTec360 MDM App" (имате 20 секунди, за да изпълните тази задача) ◦ Потвърдете диалога "Деинсталиране на AppTec360 MDM App" с "ok". Това ще дезактивира устройството от конзолата. ◦ За да премахнете приложението от устройството, потвърдете диалога "AppTec360 MDM ще бъде деинсталиран" с "UNINSTALL". 2. автоматичната (конзола) ◦ Изберете устройството в конзолата ◦ Кликнете върху синята икона на зъбно колело и изберете "Enterprise Wipe".

	Забележка: Предлага се само с Android 4.x и по-ниски версии или на устройства с KNOX API (устройства на Samsung).
Парола за деинсталиране (ревизия x)	Установената парола, с която потребителят може да отстрани администратора на устройството Ревизия x = брояч, колко често паролата вече е била променяна Важно е коя парола е необходима на потребителя, защото е възможно устройството да не се е свързало със сървъра AppTec360 и поради това най-новата парола все още да не е предадена.
История на паролите	Когато щракнете върху синия бутон ("Покажи историята"), можете да видите предварително установените пароли.
Разширена защита при деинсталиране	Тази опция предлага защита срещу устройства, които не са от типа SAFE. Докато тази настройка е активирана, не е възможно лесно да деактивирате администратора на устройството.
Да подканите потребителя да деинсталира блокираните приложения?	Ако е възможно, блокираните Приложения не само ще бъдат блокирани, но и деинсталирани автоматично. Потребителят ще бъде подканен да деинсталира блокираните Приложения, ако не е възможно автоматично деинсталиране.
Интелигентна система Блокиране на приложения	Ако е активиран белият списък, Android MDM клиентът блокира всички инсталирани от потребителя приложения. Разрешете тази настройка, за да блокирате всички стартирани системни приложения в режим на бял списък.

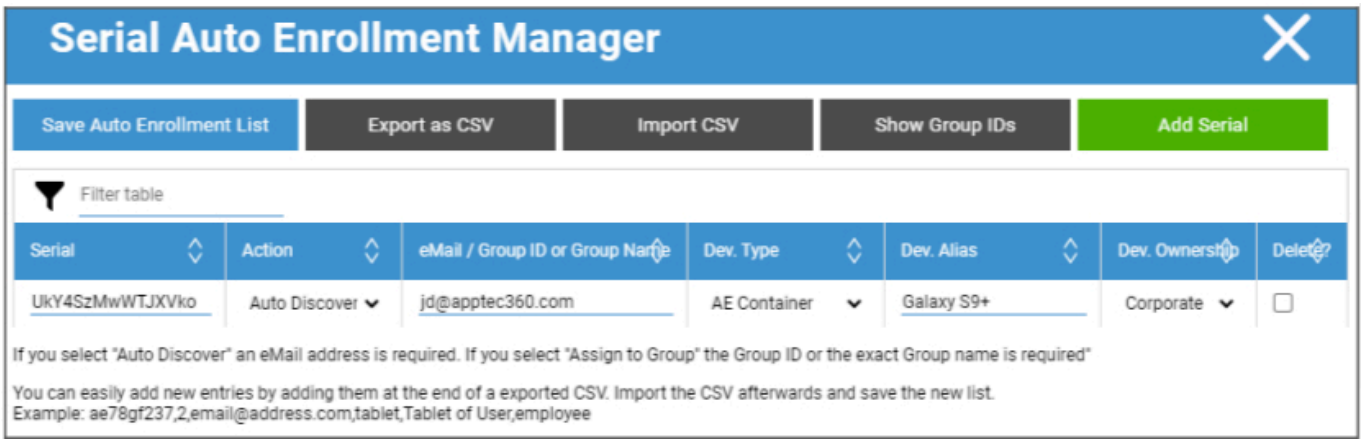
Автоматично записване

Тук можете да активирате функцията Auto Enrollment (Автоматично записване), за да записвате устройствата си автоматично, когато AppTec360 MDM Client се отвори на устройството.

Важно: Този метод за записване е остарял и вече не работи при Android 10 или по-нови версии. Така или иначе, когато използвате Android 7 или по-нова версия, трябва да запишете устройствата като напълно управлявани от Android Enterprise. Ако искате да използвате контейнера Android Enterprise BYOD и сте с Android 10 или по-нова версия, трябва ръчно да запишете устройството чрез идентификационни данни, QR код или SMS. Както и да е, списъкът за автоматично записване все още се използва за автоматизиране на процеса на записване например за AE Enrollment, Knox Enrollment и др.

Така или иначе, списъкът за автоматично записване все още се използва за автоматизиране на процеса на записване, например за записване в AE, записване в Knox и др.

Като кликнете върху "Serial Manager" или "IMEI Manager", можете да добавите съответно серийния или IMEI номера на устройствата си. Не е необходимо да правите и двете за вашите устройства, достатъчно е само едно.



Действието определя дали устройствата ще бъдат записани в пул, потребител или група.

Можете също така да експортирате и импортирате .csv файл и да филтрирате записите си по ключови думи.

Android Enterprise

Тук можете да настроите Android Enterprise. Това е необходимо, за да използвате всички функции на Android Enterprise.

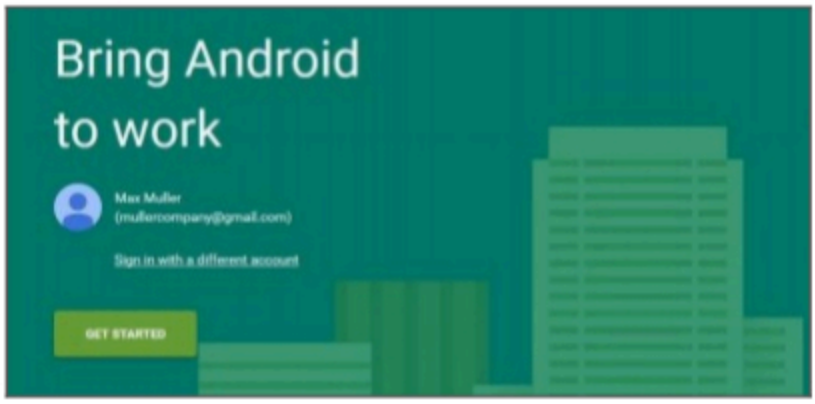
Първи метод: Акаунт за Android Enterprise (Google акаунт)

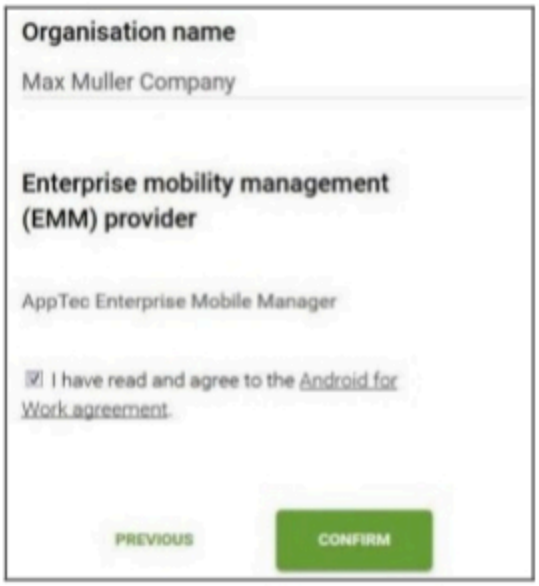
Първо натиснете "Prepare Setup" (Подготовка на настройката), а след малко трябва да се появи бутонът "Start Setup" (Стартиране на настройката).

Това ще ви отведе до страницата за настройка на Android Enterprise на Google.

Влезте в профила в Google, който искате да използвате, ако още не сте влезли, и натиснете "Започни".

Сега можете да въведете името на вашата компания. След като го направите, поставете отметка в квадратчето и натиснете "Потвърди".





В последната стъпка можете да завършите регистрацията си и да се върнете в конзолата. Ако всичко е работило, тя трябва да изглежда така:

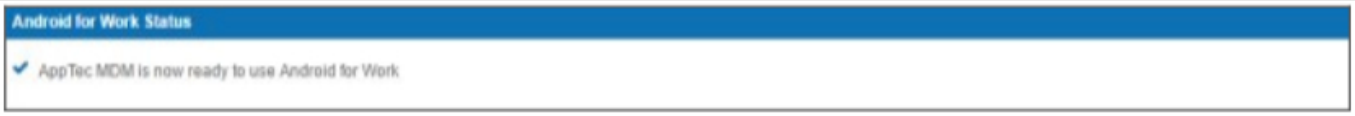
Сега можете да започнете да конфигурирате своя контейнер за Android Enterprise.

Втори метод: Акаунт в G-Suite

Натиснете бутона "Use G-Suite" и влезте в акаунта си на администратор в Google. Там отидете в "Security" (Сигурност) -> "Show more" (Покажи повече) -> "Manage EMM provider for Android" (Управление на доставчика на EMM за Android) и генерирайте токен. Забележка: Ако не виждате Android Enterprise Settings в профила си в G-Suite, трябва да отидете в "Get more apps and services" (Получаване на повече приложения и услуги) и да добавите управлението на устройства за Android. Сега въведете Token и основния си домейн в нашата конзола и кликнете върху "Save Changes" (Запазване на промените). Когато приключите, щракнете върху "Use Android Enterprise Account" (Използване на акаунта на Android Enterprise).

Сега трябва да видите бутона "Създаване на акаунт за услуги". Щракнете върху него. Този процес може да отнеме няколко минути.

Ако всичко е било наред, тя трябва да изглежда така:



Сега можете да започнете да конфигурирате своя контейнер за Android Enterprise.

Защита от нулиране на фабриката

Със защитата за нулиране на фабричните настройки можете да свържете устройството си с избран от вас акаунт в Google, който отменя и всяко съществуващо свързване с акаунт в Google. За да използвате Защитата от фабрично нулиране, трябва първо да я настроите тук и след това да я активирате в профилите си.

За да настроите защитата от фабрично нулиране, щракнете върху "FRP Setup" и следвайте инструкциите на екрана.

ЗАБЕЛЕЖКА: Прочетете внимателно и изпълнете стъпките. Препоръчваме ви да направите това в нов прозорец на браузъра в режим инкогнито, за да избегнете автоматично влизане в грешния акаунт в Google. Можете напълно да се блокирате от устройството, ако въведете грешен идентификатор или загубите достъп до използвания акаунт в Google!

Записване в AE

Тук можете да активирате Android Enterprise Ernollment. Използването на този метод ще включи устройствата ви в режима на собственик на устройства Android Enterprise. В този режим ще имате пълен контрол върху устройството.

Активиране на записването на AE	Активира предупреждението за записване на AE: Ако деактивирате AE Enrollment, съществуващите QR кодове и вече конфигурираните NFC програмиращи устройства ще спрат да работят. Ако активирате AE Enrollment отново, ще трябва да изпратите отново конфигурациите на NFC push устройствата / да генерирате нови QR кодове.
Активиране на автоматичното откриване	Когато дадено устройство се регистрира чрез "AE Enrollment", системата ще се опита да го присвои на потребител въз основа на информацията, зададена в белия списък на серийните номера / IMEI ("General Settings" (Общи настройки) > "Android Configuration" (Конфигурация на Android) > "Auto Enrollment" (Автоматично регистриране)).
Блокиране на неизвестни устройства	Само устройства, които са включени в белия списък на серийните устройства / IMEI ("Общи настройки" > "Конфигурация на Android" > "Автоматично записване"), могат да се запишат.

Забележка за метод 1 и 2: "Добре дошъл екран" се отнася за първия екран, който виждате след нулиране на фабричните настройки. Той може да изглежда различно в зависимост от версията на Android и/или модела на устройството, което използвате.

Метод 1: Записване с QR код

(изисква Android 7.0 или по-нова версия) Препоръчваме ви винаги да използвате този метод, ако използвате Android 7 или по-нова версия.

1. Възстановяване на фабричните настройки на устройството
2. Генерирайте QR кода за записването, като използвате един от следните два метода:
   - Кликнете в "Общи настройки -> Конфигурация на Android -> Записване на AE" върху "Генериране на QR код". Изберете дали искате да пропуснете криптирането на паметта и/или всички системни приложения да бъдат премахнати.
   - (алтернативно) Изберете съществуващо устройство. В "Преглед на устройствата" щракнете върху показания там QR код. Изберете дали искате да пропуснете криптирането на паметта и/или всички системни приложения да бъдат премахнати.
3. Сега докоснете 6 пъти екрана за посрещане на вашето устройство. Това трябва да стартира режима за записване на QR.
4. Свържете се с безжична мрежа и изчакайте известно време, докато се инсталира четецът на QR кодове.

5. Сега сканирайте QR кода
6. Това е всичко. Устройството ви вече е записано в режим на Android Enterprise Device Mode.
    - a. Ако сте използвали QR кода в "Общи настройки", можете да намерите устройството си в "Пул -> Устройства на собственика на AE устройства". (Съвет: Възможно е да се наложи да презаредите сайта, за да видите устройствата). Ако сте поставили отметка на "Enable Auto Discover" (Включване на автоматичното откриване), ще го намерите в рамките на потребителя си за автоматично откриване.
    - Ако сте използвали QR кода на съществуващ профил на устройство, устройството ще бъде записано в този профил.

Метод 2: Записване в NFC

(изисква NFC и Android 6.0 или по-нова версия)

Приготвяне: Въведете информацията за Wi-Fi в "Общи настройки -> Конфигурация на Android -> Записване на AE -> Данни за NFC провизиране". Сега използвайте "NFC Device", за да потърсите устройството, което ще стане програматор. Това устройство ще бъде използвано за изпращане на информацията за записване до другите устройства чрез NFC.

1. Нулиране на фабричните настройки на устройството
2. Отворете приложението за NFC сдвояване от AppTec360 на вашия програматор
3. Изберете дали искате да пропуснете криптирането на паметта и/или дали да бъдат премахнати всички системни приложения.
4. Дръжте двете устройства едно до друго
5. Сега записването в Android Enterprise трябва да е силно
6. Сега можете да намерите устройството си в конзолата
    - a. Ако не сте конфигурирали функцията за автоматично откриване, в пула
    - b. В рамките на потребителя, който сте конфигурирали за функцията Auto Discover
    - c. Съвет: Възможно е да се наложи да презаредите сайта, за да видите устройствата.

Метод 3: Акаунт в Google

(изисква Android 5.1 или по-нова версия)

(Забележка: Ако използвате този метод, устройството няма да бъде записано автоматично. Вместо това трябва да го запишете ръчно или да автоматизирате процеса, като използвате функцията за автоматично записване.)

1. Нулиране на фабричните настройки на устройството
2. Преминете през стъпките за настройка, докато можете да влезете с акаунт в Google
3. Въведете "afw#apptec" като потребителско име/поща
4. Докоснете "Next".

5. Вашето устройство вече е устройство с Android Enterprise

KNOX Записване

Тук можете да активирате KNOX Enrollment и да намерите информацията, която ви е необходима за създаване на профил за KNOX Enrollment в портала за внедряване на KNOX. Необходим ви е акаунт в Портала за внедряване на KNOX, за да конфигурирате и използвате това.

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

Активиране на записването на KNOX	Активира KNOX Записване. Внимание: Ако деактивирате KNOX Enrollment, съществуващите MDM профили ще спрат да работят. Ако активирате KNOX Enrollment отново, ще трябва да актуализирате полето "Custom JSON Data" на вашия MDM профил.
Активиране на автоматичното откриване	Когато дадено устройство се регистрира чрез "KNOX Enrollment", системата ще се опита да го присвои на потребител въз основа на информацията, зададена в белия списък със серийни номера / IMEI ("General Settings" (Общи настройки) > "Android Configuration" (Конфигурация на Android) > "Auto Enrollment" (Автоматично регистриране)).

1. Влезте в портала за мобилно записване на Samsung KNOX https://eukme.samsungknox.com/itadmin
2. Отидете на "Профили на MDM"
3. Кликнете върху "Добавяне"
4. Изберете "Server URI not required for my MDM" и щракнете върху "Next".
5. Сега създайте профил с информацията, показана в конзолата за управление

Сега този профил за записване на KNOX може да бъде инсталиран директно на устройството от Samsung, ако придобиете устройствата директно от Samsung.

Можете също така да изтеглите приложението за внедряване на KNOX, да влезете в профила си за внедряване на KNOX и да изпратите профила за записване на KNOX чрез NFC на други устройства.

Ако устройството има инсталиран профил за записване KNOX, то ще изтегли нашето приложение и ще запише устройството, ако има работеща интернет връзка.

Регистрирането на устройства чрез KNOX Enrollment може да се намери в "Pool -> KNOX Enrollment" или в рамките на потребителя, който сте посочили в Auto Discover.

Zero-Touch

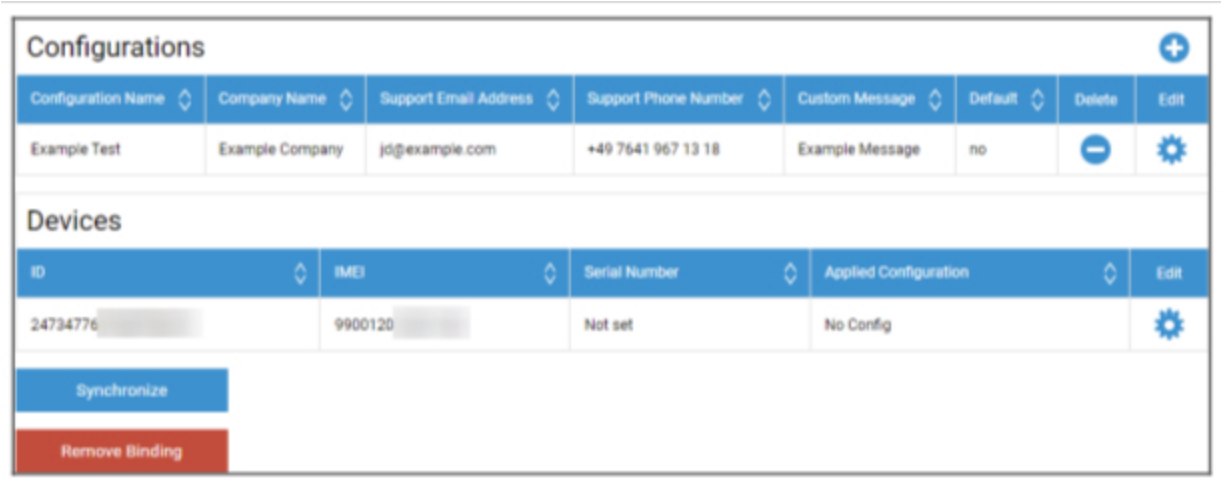
С функцията Zero-Touch можете лесно да регистрирате устройствата си, без да е необходимо да ги докосвате или да конфигурирате каквото и да било на самото устройство. Трябва само да го включите, да преминете през обичайното конфигуриране и устройството ще получи цялата информация за това как да се настрои и свърже с MDM напълно автоматично.

За да използвате Zero-Touch, трябва да закупите устройствата си от дистрибутор, който поддържа Zero-Touch. Същият този дистрибутор създава за вас и акаунт в портала Zero-Touch. Свържете се с вашия дистрибутор, за да получите повече информация за процедурата или ако имате проблеми при достъпа до портала Zero-Touch.

Щракнете върху "Start Setup" (Стартиране на настройката), за да стартирате настройката. Ще бъдете пренасочени към страница за вход, където трябва да изберете своя акаунт в Google, който има достъп до портала Zero-Touch.

ЗАБЕЛЕЖКА: Възможно е да изберете ВСЯКА сметка. Затова не забравяйте да изберете правилния акаунт в тази стъпка. Ако не виждате устройствата/конфигурациите си, най-вероятно сте използвали грешен акаунт.

След като завършите влизането в системата, тя ще изглежда по следния начин:



Щракнете върху "+", за да добавите конфигурация, и попълнете полетата, както е показано на екрана. Ако разрешите Конфигурацията като Конфигурация по подразбиране, тя ще бъде присвоена на новите устройства автоматично. Създаването или задаването на конфигурация по подразбиране не я присвоява на вече съществуващи устройства.

Ако за дадено устройство не е зададена конфигурация, то ще се настрои като обикновено устройство и няма да се свърже с MDM. Затова се уверете, че на устройствата ви е зададена Конфигурация.

След като сте свързали акаунта си, устройствата ви са видими и към тях е зададена конфигурация, можете да започнете да настройвате устройствата.

Можете да добавите устройствата в списъка за автоматично записване, така че те да бъдат автоматично записани в определена група или потребител. Ако не сте конфигурирали нищо в списъка за автоматично записване, устройствата ще бъдат записани в пула.

Конфигурация на Windows

Конфигурация на Windows

Тук имате възможност да разрешите следните конфигурации на вашия компютър с Windows 10:

Незабавна връзка с DM	
Първоначално време за повторение	Установява първия опит за връзка с устройството, тази стойност се увеличава експоненциално
Повторения на връзката	Посочва колко опита за свързване трябва да извърши DM-клиентът при грешка във връзката.
Максимално време за сън	Посочва максималното време за заспиване след грешка при свързване
Първи повторения на синхронизацията	Интервали, през които устройството трябва да комуникира със сървъра след първото свързване
Интервал за първо повторение	Отнася се за "Първи повторения на синхронизацията" Тук времената са посочени в минути Например под "First Sync Retries" (Първи повторения на синхронизацията) е посочена стойността "2", а под "First Retry Interval" (Първи интервал на повторенията) е посочена стойността "4 Minutes" (4 минути), като по този начин устройството комуникира 2 пъти на всеки 4 минути след първата връзка.
Втори повторения на синхронизацията	Интервали, през които устройството трябва да се свърже със сървъра, след като завърши "Първи повторения на синхронизацията".
Интервал на повторение на секундата	Същият принцип като за "Първи интервал на повторение" - само че тук той се прилага за "Втори повторения на синхронизацията".
Редовни повторения на синхронизацията	Интервали за това колко често устройството трябва да комуникира със сървъра в бъдеще По подразбиране: "Infinite" Препоръчваме да не променяте тази стойност, защото ако въведете "10", устройството ще комуникира със сървъра 10 пъти и след това ще спре Следователно комуникацията със сървъра AppTec360 е прекъсната!
Редовен интервал на повторение	Същият принцип като при "Първи/втори интервал на повторение" - само че тук настройките се прилагат за в бъдеще.

Редовен интервал на повторение	Същият принцип като при "Първи/втори интервал на повторение" - само че тук настройките се прилагат за в бъдеще.

ContentBox

Конфигурация

Тук можете да конфигурирате ContentBox. Можете да поставите файлове за групи в ContentBox, които могат да бъдат достъпни с приложението ContentBox на устройството.

Разрешаване на ContentBox	Активиране на ContentBox. Деактивирането на тази опция, ако не използвате ContentBox, може да спести ресурси на локалните машини.
Използване на външна инсталация на ContentBox	ContentBox може да се използва и с вашия собствен Nextcloud.
URL	Пълен URL адрес на структурата Nextcloud
Потребител на корена	Потребител с корен на акаунта в Nextcloud
Парола за корен	Коренна парола на акаунта в Nextcloud
Разрешения за групови папки по подразбиране	Разрешения за групови папки по подразбиране, които могат да се променят индивидуално от групата (в Mobile Management)
Споделяне на групова папка с подгрупи	Ако е активна, всяка подгрупа може да чете всички папки на основната група, може да бъде конфигурирана индивидуално за всяка група (Управление на мобилни устройства).
Разрешения за подгрупи	Разрешения за подгрупи може да се конфигурира индивидуално за всяка група (Управление на мобилни устройства).
Разрешаване на споделянето	Позволява на потребителя да споделя съдържанието чрез връзки, може да бъде конфигурирано индивидуално за всяка група.
Максимален размер за качване на файл в MB	Максимален размер на файла Стандартно: 512 MB Максимална конфигурация: 2048
Удостоверения за WebDAV	
URL адрес на WebDAV	Можете също така да отворите ContentBox с помощта на WebDAV. Моля, не изтривайте следните папки при никакви обстоятелства: /apptecgroups /apptecgroups/AppTecGroup-X
Потребител на корена	Име на коренните потребители

Парола	Парола на кореновите потребители

Синхронизирането със ContentBox се извършва автоматично. Можете обаче да извършите ръчна синхронизация с "Синхронизиране на ContentBox".

Освен това тук можете да активирате/деактивирате ContentBox за всяко отделно устройство.

Това е от значение само ако не сте лицензирали допълнително ContentBox, тогава все още имате достъп до 25 устройства, с които можете да тествате ContentBox - тук можете да активирате това за съответните устройства.

Конфигурация на LDAP

Преглед на LDAP

Тук можете да установите връзка с вашата Active Directory чрез LDAP, за да импортирате масово потребители и групи. Синхронизирането трябва да се извърши ръчно. Можете да конфигурирате няколко LDAP връзки към различни системи или с различни конфигурации/филтри.

Име на сървъра	Показваното име на сървъра
Тип	Понастоящем се поддържат само активни директории, които поддържат LDAP
Домейн на LDAP	Основният домейн на LDAP (напр. example.com)
Хост на LDAP	Необходимо е само ако LDAP хостът не е достъпен под дадения LDAP домейн.
Пристанище	Оставете празно, за да използвате стандартен порт (389 или 636 за SSL)
Потребителско име	Напр. CN=John,OU=Users,DC=EXAMPLE,DC=COM Забележка: Повечето системи изискват потребителско име в този формат и не приемат "John" като потребителско име.
Парола	
Потвърждаване на паролата	
Сигурност на връзката	Забележка: когато използвате SSL или TLS, ще бъде проверен сертификатът на Active Directory. Ако той е самоподписан, трябва да добавите главния удостоверяващ орган в хранилището за доверие на локалната машина. Ако сте в облака, Active Directory трябва да предостави доверен сертификат, в противен случай връзката ще работи само без криптиране
Автоматична синхронизация.	Активира автоматичното синхронизиране на директорията LDAP през интервала от време, посочен в общите настройки на LDAP.
Базов DN	Ако не искате да синхронизирате цялата директория, можете да посочите OU тук.Например OU=AndroidUsers,OU=Users,DC=EXAMPLE,DC=COM
Член на	Всички импортирани потребители ще бъдат добавени към избраната група.
Само активирани потребители?	Когато е разрешено, атрибутът userAccountControl ще бъде взет предвид, а потребителите без този атрибут няма да бъдат импортирани.

Филтър LDAP	Можете да използвате LDAP филтър, за да филтрирате кои потребители се импортират
Регестов филтър	Можете да използвате филтър Regex, за да филтрирате кои потребители да бъдат импортирани
Тестова връзка	Тестване на връзката при запазване на конфигурацията
Нулиране на структурата на директорията при синхронизиране?	Ако е вярно, всички записи в LDAP ще бъдат преместени обратно на първоначалното им място в дървото на LDAP. Препоръчва се да бъде разрешено.
Повторно импортиране на изтрити потребители и групи?	Когато е разрешено, потребителите и групите, които са били изтрити, ще бъдат създадени отново. Препоръчително е да се активира.
Синхронизиране на изтривания?	Когато е разрешено, групите и потребителите ще бъдат изтрити, когато бъдат изтрити от LDAP сървъра. Ще бъдат изтрити и устройствата на изтритите потребители.

Под списъка с конфигурациите на LDAP можете да определите периода, през който системата да се синхронизира автоматично. Използват се само конфигурациите LDAP за автоматично синхронизиране, за които е активирана съответната опция.

Управление на приложения

Вътрешнофирмени приложения DB

Android

Тук можете да качвате приложенията за Android, които вашата компания е разработила, и да ги разпространявате по-късно в Mobile Management в профили на устройства или групи.

Моля, имайте предвид, че препоръчваме да разпространявате по този начин само приложения, които не са налични в Google Play Store.

Кликнете върху "+", за да качите APK файла на приложението, което искате да качите. В момента се поддържа само формат APK.

Ограничението за качване на локални устройства може да бъде увеличено в Стъпка 3 от Конфигурацията на устройството. Ако желаете да увеличите лимита за качване в облака, моля, свържете се с отдела за поддръжка за повече информация.

Имайте предвид, че обикновено APK файловете са малко по-малки от съдържанието им. Възможно е качването да се провали поради тази причина, тъй като APK се разопакова в процеса. Например възможно е 95MB APK да се провали при ограничение за качване от 100MB. В този случай увеличете лимита за качване, както е посочено по-горе.

Съветваме също така първо ръчно да преместите APK файла на едно тестово устройство (например чрез USB) и да се опитате да го инсталирате ръчно с приложението Files на устройството. Ако това не се получи по някаква причина, то няма да успее и чрез MDM.

Актуализиране на целта

С функцията "Цел на актуализация" можете да изберете коя версия на дадено приложение да бъде инсталирана или до коя версия да бъде актуализирано дадено приложение, ако сте активирали "Поддържане на актуална версия" за дадено приложение.

Ако не сте избрали цел за актуализация, ще бъде използвана най-високата версия.

Имайте предвид, че Android не може да понижава нивото на приложенията. Също така имайте предвид, че "кодът на версията" определя дали дадена версия е по-висока, по-ниска или същата. Затова се уверете, че правилно сте увеличили тази версия в приложението си, когато изграждате актуализация.

iOS

Тук можете да качвате разработените iOS приложения и да ги разпространявате по-късно в Mobile Management в профила на вашето устройство или група.

Щракнете върху "+", за да качите IPA на приложението, което искате да качите. Засега се поддържа само формат IPA.

Ограничението за качване на локални устройства може да бъде увеличено в Стъпка 3 от Конфигурацията на устройството. Ако желаете да увеличите лимита за качване в облака, моля, свържете се с отдела за поддръжка за повече информация.

Актуализиране на целта

С функцията "Цел на актуализация" можете да изберете коя версия на дадено приложение да бъде инсталирана или до коя версия да бъде актуализирано дадено приложение, ако сте активирали "Поддържане на актуална версия" за дадено приложение.

Ако не сте избрали цел за актуализация, ще бъде използвана най-високата версия.

MacOS

Тук можете да качвате разработените от вас приложения за MacOS и да ги разпространявате по-късно в Mobile Management в профила на вашето устройство или група.

Щракнете върху "+", за да качите PKG на приложението, което искате да качите. Засега се поддържа само PKG формат.

Ограничението за качване на локални устройства може да бъде увеличено в Стъпка 3 от Конфигурацията на устройството. Ако желаете да увеличите лимита за качване в облака, моля, свържете се с отдела за поддръжка за повече информация.

Актуализиране на целта

С функцията "Update Target" можете да изберете коя версия на дадено приложение да бъде инсталирана или до коя версия да бъде актуализирано дадено приложение, ако сте активирали "Keep up to date" за дадено приложение.

Ако не сте избрали цел за актуализация, ще бъде използвана най-високата версия.

Windows 10

Тук можете да качвате приложенията на Windows 10 и да ги разпространявате по-късно в Mobile Management в профила на устройството или групата.

Щракнете върху "+", за да качите APPX, APPXBUNDLE или MSI на приложението, което искате да качите. Засега се поддържа само форматът APPX, APPXBUNDLE или MSI.

Можете също така да качвате и определяте зависимости за дадено приложение, които ще бъдат автоматично разпределени и инсталирани преди инсталирането на желаното приложение.

Ограничението за качване на локални устройства може да бъде увеличено в Стъпка 3 от Конфигурацията на устройството. Ако желаете да увеличите лимита за качване в облака, моля, свържете се с отдела за поддръжка за повече информация.

Актуализиране на целта

С функцията "Update Target" можете да изберете коя версия на дадено приложение да бъде инсталирана или до коя версия да бъде актуализирано дадено приложение, ако сте активирали "Keep up to date" за дадено приложение.

Ако не сте избрали цел за актуализация, ще бъде използвана най-високата версия.

Пакет Win32 (.exe)

Можете също така да разпространявате .exe файлове/инсталатори на своите устройства.

Име на пакета	Името, което ще се показва в MDM
Описание	Описание, показано в MDM
Пакетен файл	Разрешени са само .zip файлове. Поставете файловете, които искате да разположите, в този zip файл.
Контекст на внедряване	**Система**: Командата за инсталиране се изпълнява със системни привилегии, които са по-високи от "Потребител". Също така при използване на "System" процесът няма потребителски интерфейс, така че ще бъде безшумен и потребителският профил, например променливите на средата като %AppDat%, не е достъпен. **User (Потребител)**: Командата за инсталиране има достъп до потребителския профил и може да покаже потребителски интерфейс, ако е необходимо. Забележка: Някои процеси могат да работят само в един контекст. Напр. ако даден софтуер се инсталира в AppData, той ще работи само при избор на "Потребител"
Команда за инсталиране	Командата, използвана за инсталиране на програмата. Например командата за инсталиране на zip файл, съдържащ в корена си "setup.exe", който поддържа параметъра "/s" за безшумна инсталация, ще бъде "setup.exe /s". Имайте предвид, че различните софтуери могат да имат различни параметри.
Команда за деинсталиране	Командата, която трябва да се изпълни, за да се деинсталира софтуерът чрез MDM. Обикновено тя сочи към програмата за деинсталиране. Например "C:\Program Files\ExampleSoftware\uninstall.exe".
Изисквания	
Забележка: За да се инсталира софтуерът, трябва да са изпълнени всички зададени изисквания. В противен случай той няма да бъде инсталиран. Някои полета може да са задължителни. Ако за дадено изискване не е зададена стойност, то ще бъде игнорирано.	
Архитектура на операционната система	Архитектура на операционната система
Версия на Min OS	Версия на Min OS

Минимално свободно дисково пространство (MB)	Минимално свободно дисково пространство (MB)
Минимална физическа памет (MB)	Минимална физическа памет (MB)
Минимален брой логически процесори	Минимален брой логически процесори
Минимална скорост на процесора (MHz)	Минимална скорост на процесора (MHz)
Допълнителни изисквания	Ако желаете, можете също така ръчно да дефинирате правила или да качите скрипт, за да извършите допълнителни проверки на изискванията.
Правила за откриване	
Метод на откриване	Тук можете да определите как да се определи дали приложението е инсталирано на устройството. Командите за инсталиране ще се изпълняват само когато тези правила установят, че приложението НЕ е инсталирано. Командите за деинсталиране се изпълняват само когато тези правила установят, че приложението не е инсталирано. **Ръчно дефиниране на правила**: Позволява ви ръчно да дефинирате едно или повече правила, за да проверите например дали е налице определен файл, папка, MSI или ключ от регистъра. Ако всички дадени правила за откриване са верни, приложението ще се счита за налично. **Използване на скрипт:** Качете свой собствен скрипт със собствени проверки. Ако скриптът върне "$TRUE", приложението ще се счита за налично.
Правила за откриване	

Настройки на приложението

Настройки на приложението за iOS

Тук можете да определите настройките по подразбиране за добавяне на приложение в задължителния магазин за приложения или в магазина за корпоративни приложения.

Забележка: Това задава само това, което е избрано по подразбиране при добавяне на приложения. Това НЕ променя съществуващите настройки за приложения, които вече са добавени в задължителния магазин за приложения или в магазина за корпоративни приложения.

Бъдете в крак с новостите	Автоматично поддържа приложението в актуално състояние. Моля, имайте предвид, че след пускането на актуализация може да минат до 7 дни, докато приложението бъде актуализирано.
Изпреварване, когато не се управлява	Ако дадено приложение вече е инсталирано като неуправлявано (от потребителя), то ще бъде изпреварено и управлявано от MDM.
Премахване на приложението при премахване на MDM профила	Деинсталира приложението, когато MDM бъде премахнат.
Предотвратяване на архивирането на данните на приложението	Предотвратява архивирането на данните на приложението.

Настройки на приложението за Android

Тук можете да определите настройките по подразбиране за добавяне на приложение в задължителния магазин за приложения или в магазина за корпоративни приложения.

Забележка: Това задава само това, което е избрано по подразбиране при добавяне. Това НЕ променя настройките за приложения, които вече са добавени в задължителния магазин за приложения или в магазина за корпоративни приложения.

Бъдете в крак с новостите	Автоматично поддържа приложението в актуално състояние. Налично само за InHouse Apps.
Контролирана актуализация на клиента на AppTec360 EMM	Ако е разрешено, администраторите могат да определят целта на актуализация за AppTec360 EMM Client. Списъкът с всички налични версии на AppTec360 EMM Client ще бъде показан в "Общи настройки" → "Управление на приложения" → "Вътрешна база данни на приложенията" → "Android".

Приложения на трети страни

Android

Тук можете да зададете своя код за активиране за Ikarus.

Настройте тази опция на "Use Activation Code" (Използвай код за активиране) и въведете кода си за активиране тук.

Забележка: След въвеждане на кода и запазване, кодът все още не е добавен към профила, който се изпраща на устройството. Трябва да извършите някаква промяна в профила си, за да се добави кодът към профила. Напр. променете който и да е превключвател в профила от изключен → включен → изключен - Запазване → Присвояване сега.

iOS

Тук можете да въведете своя SecurePIM лиценз. След като въведете лиценза, натиснете "Save Changes" и можете да използвате опциите на SecurePIM.

VPP / KNOX Premium

Програмата за закупуване на обеми (VPP) на Apple ви позволява лесно да разпространявате платени и безплатни приложения на вашите устройства. Това е силно препоръчително, тъй като не се нуждаете от Apple ID на устройствата, потребителите не трябва да потвърждават инсталацията (под надзор), няма да се налага да въвеждат паролата на Apple ID и можете лесно да разпространявате платени Apps, без да ги купувате отново на всяко устройство.

За да използвате VPP, трябва да се регистрирате в Apple Business Manager.

Лицензи за VPP

Тук можете да получите обща информация за вашите VPP приложения, колко лицензa са използвани и колко са налични.

Щракването върху колелото ще ви позволи да видите кои устройства имат присвоен лиценз и какво е състоянието на това присвояване.

Щракването върху опреснява кеша на VPP, който сравнява лицензите, присвоени в MDM, с лицензите, присвоени от страна на Apples. В някои случаи това може да разреши проблеми с лицензите.

Токен на VPP

Тук можете да качите своя VPP токен, който можете да намерите в Бизнес мениджъра на Apple в Настройки → Приложения и книги. Можете да качвате няколко VPP токена.

Можете да подновите токена, като просто изтеглите нов в Apple Business Manager, щракнете върху колелото "Редактиране" и качите новия токен.

Режимът "VPP" определя как се обработва присвояването на лицензa. В зависимост от вашия сценарий трябва да използвате различни режими:

"Device based" (базирано на устройство) трябва да се използва при регистриране на устройствата чрез QR Code, Link, Apple Configurator или DEP.

"Базирано на потребител" се изисква, ако устройствата са записани с потребителско записване или като споделен iPad.

Ако активирате "Автоматично управление на лицензи", на потребителите, които са преместени от една група в друга, автоматично ще бъдат присвоени лицензи Apple VPP въз основа на профила на групата, в която са преместени.

Съществуващите лицензи за Apple VPP от групата, от която са преместени, няма да бъдат отнети.

На новите потребители, добавени към дадена група, автоматично ще бъдат присвоени лицензи за Apple VPP въз основа на съответния профил на групата.

KNOX Premium Key

Тук можете да въведете своя KNOX Premium Key, за да използвате контейнера Samsung KNOX.

Имайте предвид, че от Android 10 насам тази функция вече не се поддържа. Вместо това използвайте Android Enterprise Container.

Настройки на App Store

Регион и език

Тук можете да зададете езика и региона по подразбиране за търсенето на приложения в App Management.

Имайте предвид, че настройката за iTunes определя и начина, по който системата получава информация за определени приложения. Ако в списъците си срещнете приложения, които се показват по странен начин (напр. липсваща икона), може би сте задали регион, в който конкретното приложение не е достъпно.

Магазин за игри AE

Тук можете да намерите всички опции за Play Store за корпоративни устройства с Android, за да одобрявате приложения, да качвате собствени приложения в Play Store или да създавате собствени уеб приложения.

Одобрени приложения

Тук можете да получите преглед на всички одобрени от вас приложения.

Приложения за Play Store

Това ще зареди iFrame, показващ магазина за игри. Потърсете желаното приложение, щракнете върху него и го одобрете. Докато одобрявате приложението, можете също така да определите, че одобрението се отменя, ако изискваните разрешения се променят. Препоръчваме да оставите тези настройки по подразбиране при одобряване на Приложения.

След като дадено приложение бъде одобрено, можете да го добавите към профилите си.

Бутонът "Одобряване" ще се промени на "Отмяна на одобрението", след като го одобрите, така че винаги можете да премахнете приложенията, ако вече нямате нужда от тях.

Частни приложения

Тук можете да качите собствено приложение като частно приложение в Google Play Store. Това ви позволява да разпространявате приложението чрез услугите на Google и да го актуализирате чрез тях. Предимство на това е и фактът, че вашите собствени приложения могат да бъдат инсталирани без потвърждение от потребителя, което обикновено е необходимо.

Уеб приложения

Тук можете да създавате уеб приложения, които представляват връзки към определени уеб страници, които могат да бъдат задавани като приложения.

Можете също така да дадете на този елемент персонализирана икона и да определите допълнително как точно да се показва.

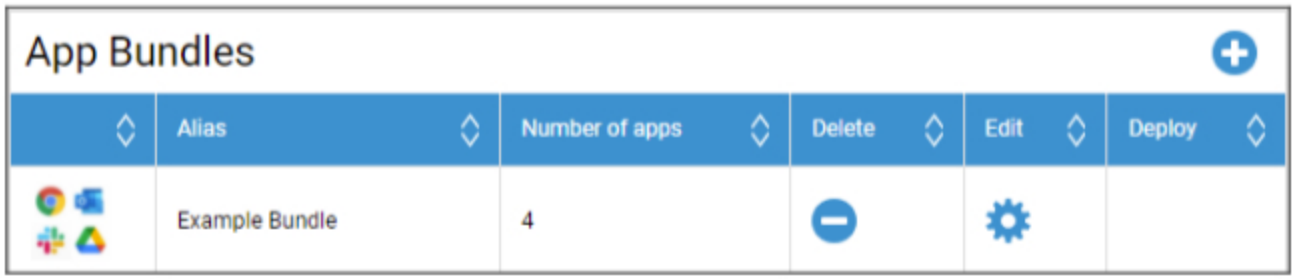
Разположение на магазина

Разположението на магазина определя начина, по който приложенията се показват в Play Store, или дали изобщо се показват.

Имайте предвид, че ако искате да покажете приложения в Play Store, които потребителят да инсталира ръчно, те трябва да бъдат добавени тук в оформлението. **И** в профила към Enterprise Play Store. Ако добавите приложение само в едно от тях, то няма да бъде показано.

Пакет от приложения

С помощта на пакетите с приложения можете да дефинирате групи от приложения, които могат да бъдат присвоени на профили на устройства или групи с едно кликване.



Щракнете върху "+", за да създадете нов пакет от приложения. След като създадете пакет от приложения, можете да щракнете върху "Редактиране", за да добавите приложения от различни източници към пакета.

Пакетът може да бъде добавен към профилите, както всички останали приложения. Когато добавяте приложения, ще имате допълнителен раздел, наречен "Пакети с приложения", в който ще имате своите пакети.

Ако направите някаква промяна в пакета с приложения, ще се появи бутон в колоната "Deploy". Това ще ви позволи да изпратите тези промени към всички профили, съдържащи този пакет. Така че имайте предвид, че трябва да направите това ръчно след добавяне или премахване на приложения в даден пакет.

Дистанционно управление

TeamViewer

TeamViewer Connector

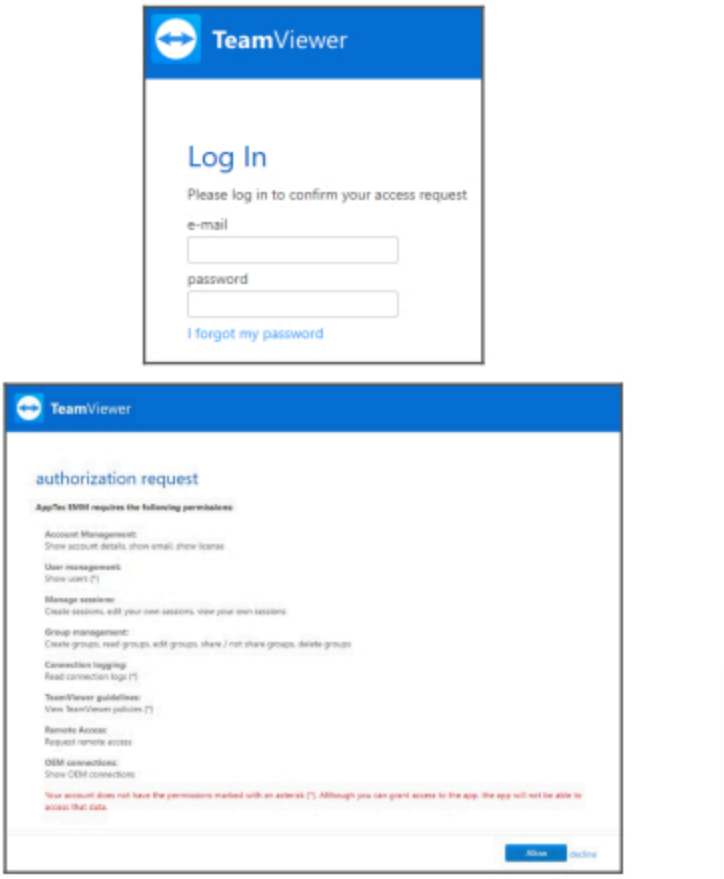
Забележка: В безплатната пробна версия на нашата облачна версия не можете да свържете своя TeamViewer акаунт. Вместо това автоматично ще бъде свързан безплатен демо акаунт.

Отидете в Общи настройки -> Дистанционно управление -> TeamViewer. Тук можете да свържете акаунта си в TeamViewer с конзолата или да видите информация за текущо свързания акаунт. Също така можете да видите всички активни в момента сесии, ако отидете на "Активни сесии".

За да свържете акаунта си, кликнете върху "Start Setup".

Това ще ви препрати към нова страница, в която трябва да влезете с профила си в TeamViewer.

След като влезете в системата, трябва да разрешите на AppTec360 MDM да използва този акаунт. След като потвърдите това, трябва да изчакате няколко секунди и акаунтът е свързан.


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

Инсталиране на TeamViewer QuickSupport

Добавете приложението "TeamViewer QuickSupport" към задължителните приложения в профила на устройството или груповия профил и кликнете върху "Assign Now". Изчакайте, докато приложението се инсталира на устройството.

Ако се опитате да осъществите достъп до устройство, на което приложението не е инсталирано, то ще бъде инсталирано или ще бъде поискано да бъде инсталирано, в зависимост от конфигурацията на устройството.

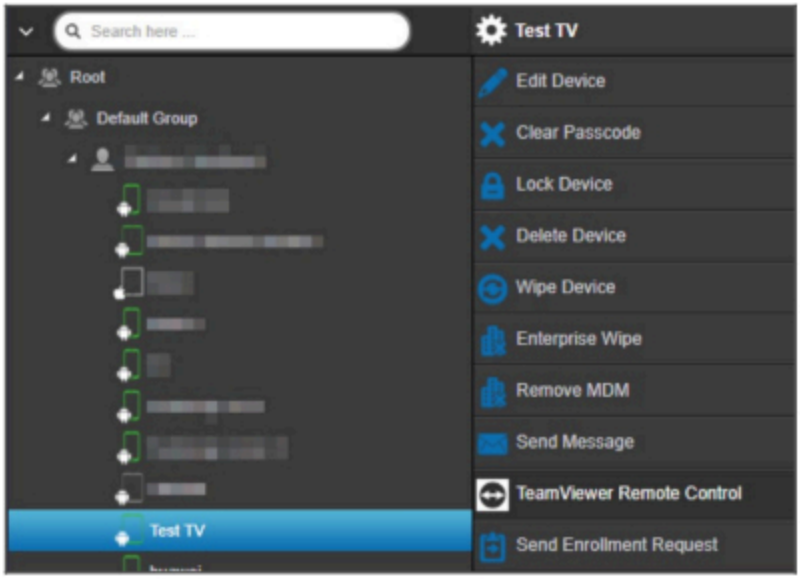
Дистанционно управление на вашето устройство

За да управлявате дистанционно устройството си, изберете устройството, щракнете върху колелото и изберете "TeamViewer Remote Control".

Ако вече има активна сесия, можете да използвате старата сесия или да създадете нова.

Потвърдете, че искате да създадете нова сесия на TeamViewer.

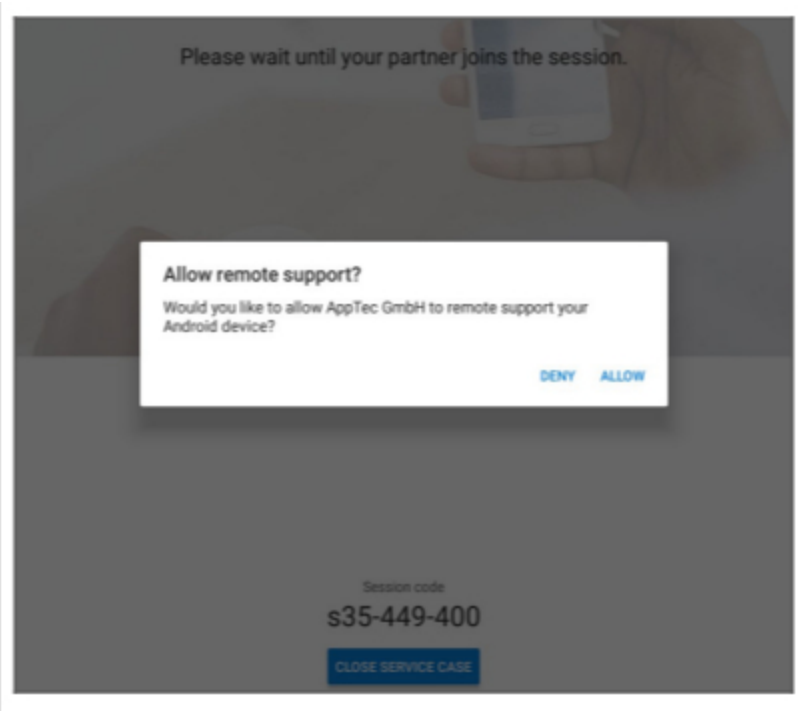
След няколко секунди ще получите връзка за вашата TeamViewer сесия. Можете да щракнете върху "Start", за да отворите тази връзка в нов прозорец.


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

Тази връзка ще отвори инсталирания TeamViewer и ще ви свърже с устройството.

Сега трябва да потвърдите връзката в самото устройство, за да го управлявате дистанционно.

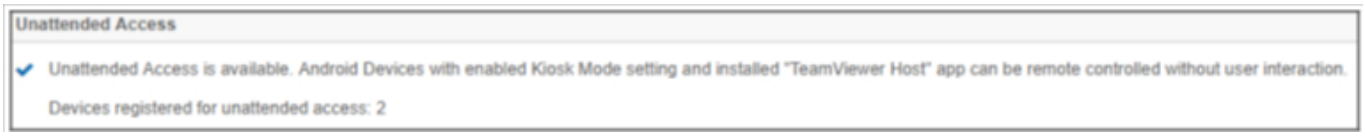


Ако използвате iOS, ще получите съобщение в AppTec360 MDM Client. С тази връзка устройството ще се присъедини към отдалечената сесия. В зависимост от настройките за уведомяване на устройството е възможно да не получите известие и да се наложи да отворите AppTec360 MDM Client ръчно.

На някои устройства с Android (напр. Samsung) е необходимо да инсталирате допълнително приложение като добавка. Приложението TeamViewer на устройството ще ви информира за това, ако това е необходимо на вашето устройство.

Достъп без надзор

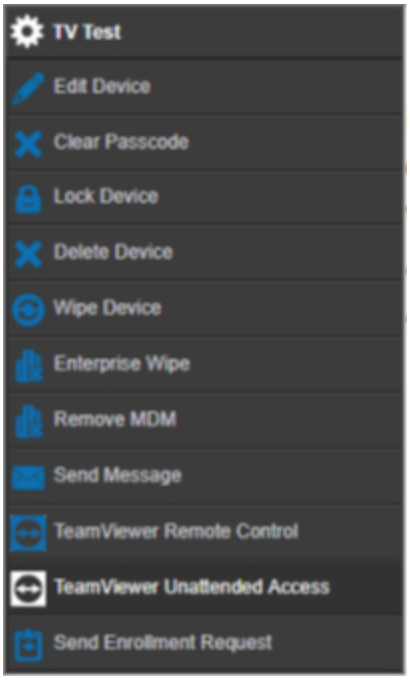
Забележка: Необслужваният достъп е възможен само на устройства с Android.



Можете да се свързвате с устройствата си, без да приемате връзката на устройството, само ако профилът ви в TeamViewer използва лиценз "Tensor" или "Corporate".

Можете да проверите това, след като свържете профила си, в "Общи настройки".

За да използвате необслужваемия достъп, трябва да инсталирате приложението "TeamViewer Host" и да активирате "Enable Unattended Access" (Активиране на необслужваемия достъп) под "Kiosk Mode & Launcher" (Режим на киоск и стартиране) в профила си. Моля, имайте предвид, че това е възможно само ако използвате режим Kiosk Mode.



Сега можете да изберете необслужван достъп, ако изберете устройството си и щракнете върху колелото. Това ще ви свърже с устройството, без да е необходимо потвърждение на самото устройство. Моля, имайте предвид, че може да отнеме няколко минути, докато получите връзката за достъп до вашето устройство.

Splashtop

Ако разрешите опцията Splashtop, ще видите опциите за конфигуриране на Splashtop в профилите си.

За да използвате Splashtop, трябва да зададете Splashtop Streamer (com.splashtop.streamer.csrs) като задължително приложение в профила си. След това можете да активирате конфигурацията на Splashtop в профила си в "Дистанционно управление". Включването на тази опция ще конфигурира приложението Splashtop Streamer. Ако използвате Splashtop Streamer, но не в комбинация с MDM, трябва да оставите това изключено.

В профила си под "Дистанционно управление" трябва да зададете и код за разгръщане. Отидете на https://my.splashtop.com и влезте в профила си в Splashtop. Щракнете върху "Add Computer" (Добавяне на компютър) и копирайте 12-цифрения код за разполагане от получената страница.

Без кода за внедряване дистанционното управление НЕ е възможно.

След като го направите, можете да щракнете с десния бутон на мишката върху устройството си и да стартирате отдалечена сесия, като щракнете върху "Splashtop Remote Control".

Управление на SIM карти

CSV групов внос

Това показва преглед на назначените SIM карти и цялата информация за тях. Това ви помага да разполагате с цялата информация не само за вашите устройства, но и за вашите SIM карти в една система.

ЗАБЕЛЕЖКА: Това е ръчно управление/документация. Не е възможно тези данни да се получават автоматично от устройствата поради механизмите за поверителност/сигурност на операционните системи.

Можете също така да импортирате този списък като CSV.

Превозвач и тарифа

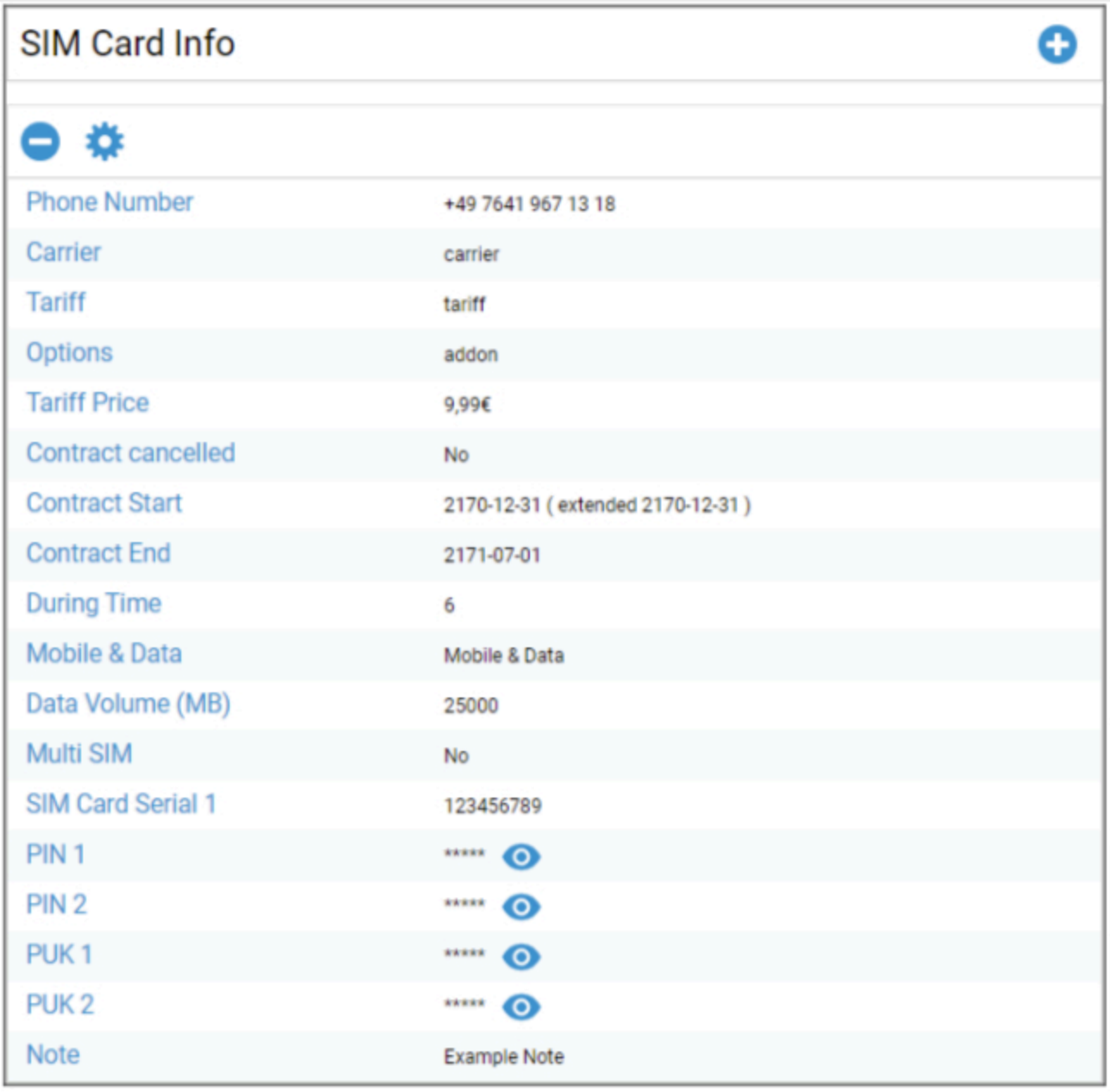
За да добавите SIM карта, първо щракнете върху бутона за добавяне на един или няколко оператора.

След това кликнете върху "+" в "Информация за тарифата", за да добавите тарифа към превозвач.

По желание можете да добавите допълнителни опции по-долу, ако имате нещо подобно.

Това е всичко необходимо за добавяне на действителна SIM карта. В момента SIM картите се присвояват на потребител. Затова отидете в Управление на мобилни устройства, изберете Потребител и отидете на "Преглед на сим картите.

Тук можете да видите SIM картите на тези потребители. Ако има такава, можете да я редактирате или премахнете. Потребителите могат да имат няколко SIM карти.

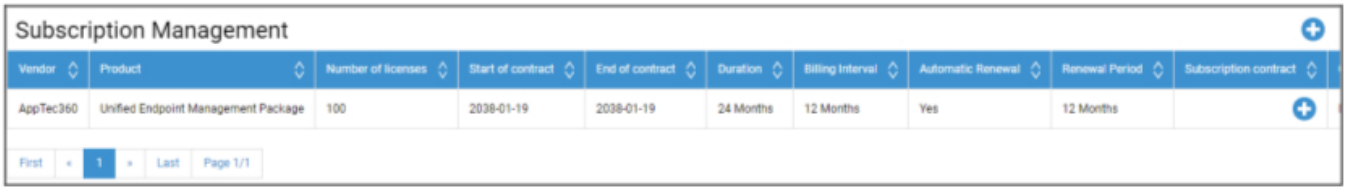


Щракнете върху "+", за да добавите SIM карта и да добавите цялата необходима информация. Тези SIM карти ще бъдат изброени и в списъка с всички ваши SIM карти в Общи настройки → Управление на SIM карти.

Управление на абонаменти

Управление на абонаменти

Тук можете да документирате текущите абонаменти, техните данни и да съхранявате различни файлове, например подписан договор, писмо за прекратяване и др. Можете също така да настроите напомняния, които да ви напомнят по пощата преди края на абонамента и може би да се удължат автоматично.



Кликнете върху "+" в горната част, за да добавите абонамент. Можете да добавите толкова абонаменти, колкото искате.

Щракнете върху "+" в различните полета, за да качите файлове, свързани с този абонамент. Технически можете да качите всеки тип файл, но имайте предвид, че не всеки тип файл може да бъде прегледан в браузъра.

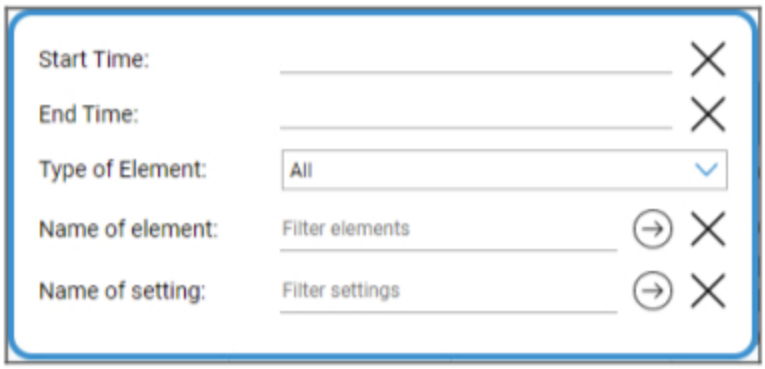
Общ одитен дневник

Одитен дневник

Тук имате общ одитен дневник, който показва всички направени промени. Докато дневникът за одит при даден потребител или група показва само промените, свързани с този потребител или група, този показва ВСЯКА промяна, направена навсякъде в конзолата.

Можете да видите какво е променено, от кого, кога и къде. В някои случаи можете също така да разширите записа, за да видите допълнителни подробности.

Възможно е да щракнете върху потребителя или върху записа в "Path / Type" (Път/Тип), за да стигнете до мястото, където е направена промяната.



В горния десен ъгъл можете също така да дефинирате филтър, който може да ви помогне да откриете определени промени в среда, в която се случват много промени.

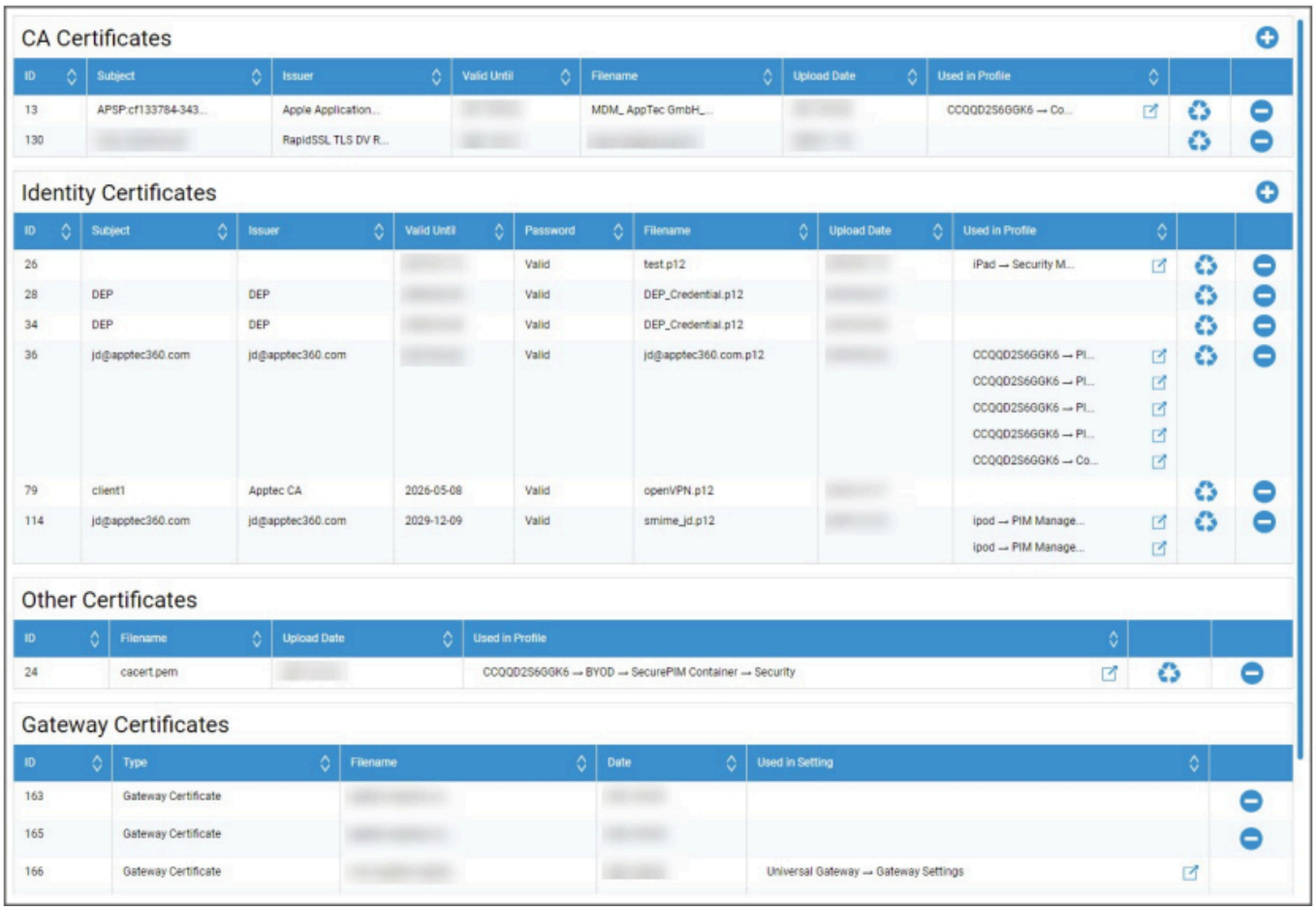
Настройки на дневника за одит

"Период на съхранение на одитните журнали" определя колко дълго трябва да се съхраняват одитните журнали, преди да бъдат изтрити.

Управление на сертификати

Тук ще получите преглед на всички сертификати, качени и използвани в конзолата. Това е само преглед. Действителната конфигурация, например за Wi-Fi сертификати, все още се извършва в профила на съответното място.

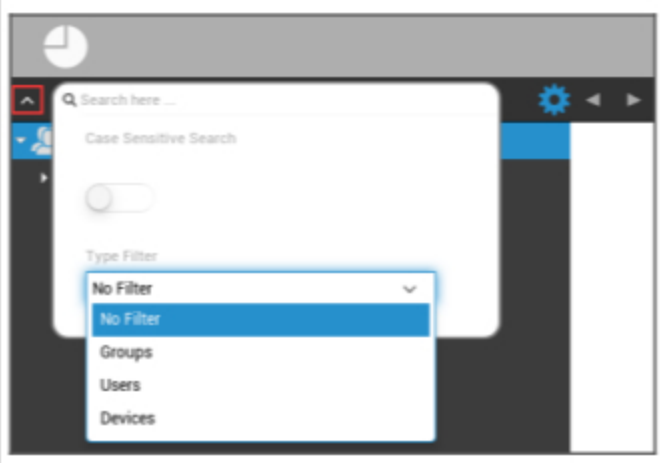
Тук можете също така да премахвате или актуализирате сертификати, което автоматично ще се отрази в засегнатите профили. Щракнете върху информацията в "Used in Profile" (Използвано в профила), за да видите къде точно все още е присвоен даден сертификат.



Управление на мобилни устройства

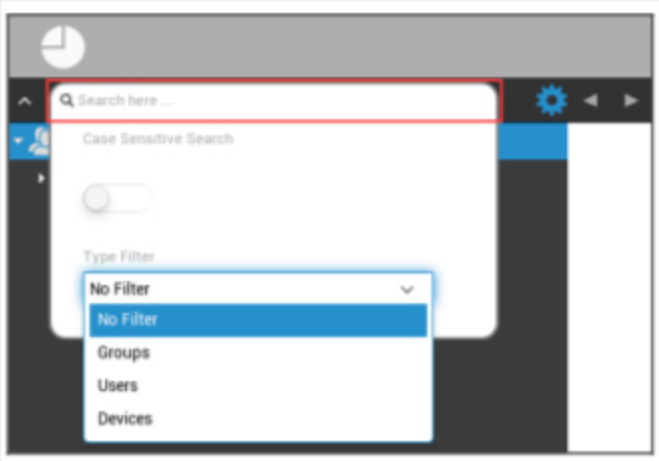
Екран за управление на мобилни устройства

Филтър на устройството



С едно кликване в горния ляв ъгъл на екрана можете да намерите различни филтри за показване на устройствата.

Прозорец за търсене



Прозорецът за търсене ви позволява да търсите всички устройства и/или потребители с определена ключова дума.

Задвижване на опциите

След като щракнете върху съответния символ, ще се покаже списък с наличните опции.

Те се променят с всеки текущ прозорец и са обяснени в съответните глави.

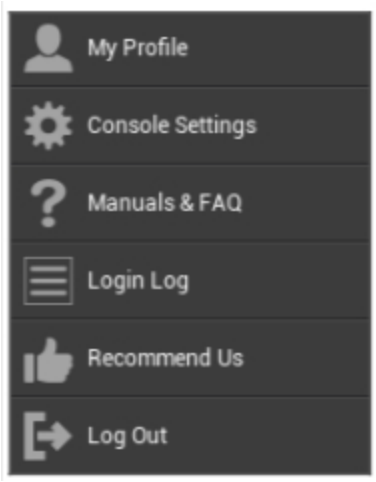
Стрелки за навигация

С натискане на стрелката наляво ще бъдете прехвърлени на предишната страница.

След това с едно кликване върху стрелката надясно ще бъдете прехвърлени на страницата, която току-що сте напуснали.

Настройки на акаунта в администрацията

Щракването върху имейл адреса, както е показано по-горе, показва следното меню:



Моят профил	Редактиране на данните за профила на администраторите
Настройки на конзолата	Конфигуриране на настройките на конзолата за акаунта Admins
Ръководства и често задавани въпроси	Преглед на страницата "Ръководства и често задавани въпроси" в "Общи настройки"
Вход	Достъп до "Вход"
Препоръчайте ни	Преглед на страницата "Препоръчай ни" в "Общи настройки"
Излизане от системата	Излизане от конзолата MDM

Информация за потребителя

Тук можете да редактирате данните за профила на влезлия в момента администратор.

Потребителско име	Потребителско име и/или имейл адрес на акаунта
Име	Първото име на администраторите
Фамилия	Фамилно име на администраторите
Име за вход	Име за вход на администраторите
Електронен адрес	Имейл адрес на администраторите
Алтернативен електронен адрес	Алтернативен имейл адрес на администраторите
Снимка	Профилна снимка
Телефонен номер	Телефонен номер на администраторите
Мобилен номер	Мобилен номер на администраторите
Удължаване на телефона	Удължаване на телефона
Местоположение	Местоположение
Позиция	Позиция в компанията
Потребителска група	Изберете към коя потребителска група искате да присвоите акаунта на администратора
Коментар:	Въведете коментар
Въведете нова парола	Въведете паролата за промяна на паролата
Повтаряне на новата парола	Повторете новата парола, за да я потвърдите

Имайте предвид, че достъпът до администрацията може да бъде подаден и като локален потребителски акаунт в структурата на йерархията. Без да е създаден допълнителен администратор, този не трябва да се изтрива!

Настройки на конзолата

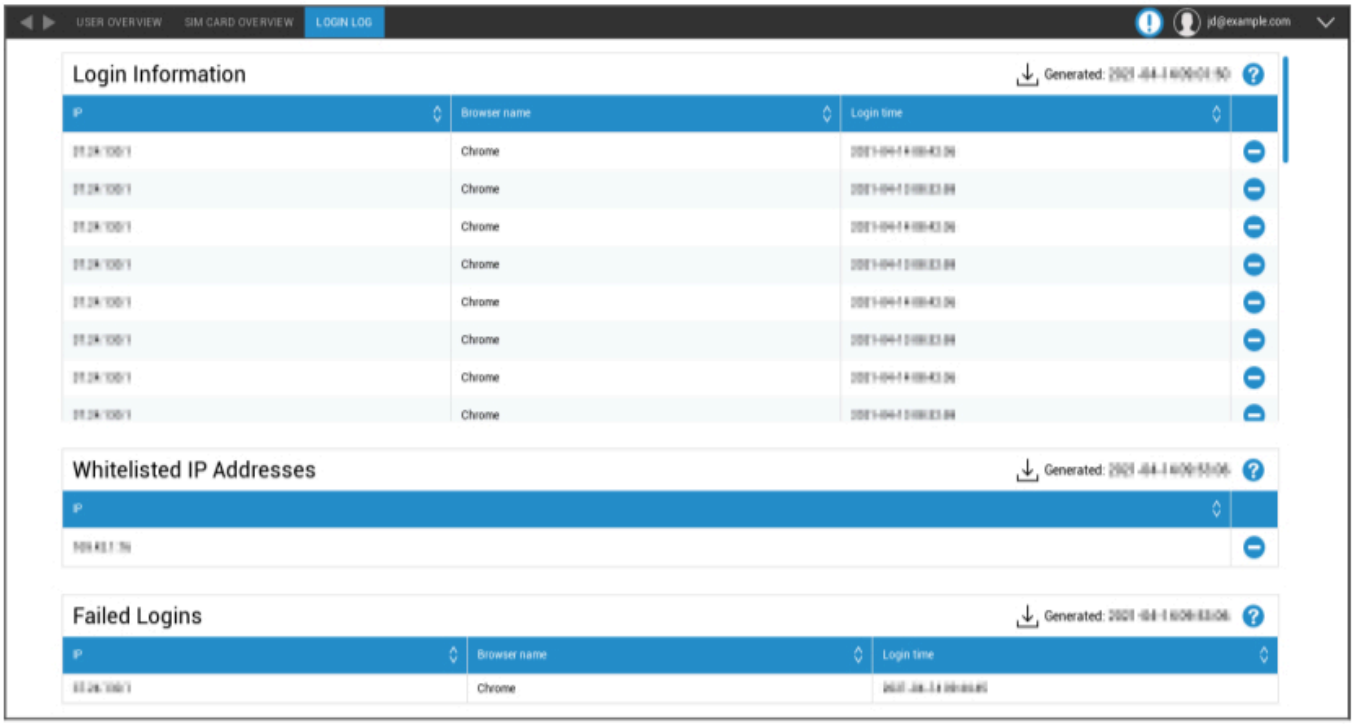
Тук можете да конфигурирате следните настройки на конзолата за акаунта Admins:

Опции за показване на потребителя на директорията	Определяне на начина, по който потребителите трябва да бъдат маркирани в дървото
Опции за показване на устройството за директория	Определяне на начина на етикетиране на устройствата в дървото
Време на сесията	Ако потребителят не направи нищо в рамките на посоченото време, той ще бъде изведен от системата. Стойността по подразбиране е 60 минути. Моля, излезте и влезте отново, след като промените тази настройка.
Часови пояс	Изберете използваната часова зона
Формат на времето	Изберете как да се показват времевите маркери
Език на конзолата	Изберете езика, на който да се показва конзолата. Предлагат се английски и немски език.
Основен цвят	Можете да зададете цвят, който ще се използва като основен за цветовата схема на конзолата. Можете да използвате инструмента за избор на цвят или да въведете цвят в HTML HEX. RGB форматите като "розово", "жълто" също работят.
Команда за запазване	Комбинацията от клавиши за задействане на запаметяване, без да натискате бутона "Запаметяване".
Използване на двуфакторно удостоверяване	Активирайте използването на двуфакторно удостоверяване при влизане в системата. При влизане в системата ще получите имейл с код, който трябва да въведете, за да влезете в системата.
Време за двуфакторно удостоверяване	Задайте период от време, през който няма да ви бъде поискано двуфакторно удостоверяване след вече успешно удостоверяване.
Изпратете кода за проверка чрез	Кодът за проверка ще бъде изпратен на избраните опции. Съобщението за устройството ще бъде показано в приложението AppTec360 MDM на всички устройства с Android и iOS, които ви принадлежат.

Изпращане на съобщение за вход след влизане	Ако е разрешено, ще бъде изпратен имейл за всяко влизане от IP адрес, който не е включен в белия списък. Имейлът съдържа информация за влизането (напр. IP, браузър).

Вход

Тук можете да видите информация за влизанията в акаунта на администратора, който е влязъл в момента.



Информация за вход	Списък, съдържащ влизанията в текущия администраторски акаунт, които са записани от конзолата. Този списък показва всички успешни влизания през последните 30 дни.
IP адреси в белия списък	Това е списъкът с всички IP адреси, включени в белия списък. Ако влезете от IP адрес, който е посочен тук, няма да получите съобщението за вход. Можете да добавите IP адрес към този списък, като щракнете върху бутона до записа в списъка "Информация за вход" по-горе. Можете да премахнете даден IP адрес от този списък, като щракнете върху бутона до записа в този списък или в списъка "Информация за вход" по-горе.
Неуспешни влизания	Това е списък на всички неуспешни опити за влизане през последните 30 дни. Ако не сте успели да въведете правилната парола поне 3 пъти в рамките на 20 минути, в този списък ще се появи запис. За неуспешните опити за влизане в системата ще бъдете информирани и по имейл.

Корпоративна администрация (Root-Node) в мобилното управление

Когато достигнете до Root-Node (първата група), можете да извършите различни настройки за вашата компания по отношение на Mobile Management.

Създаване на подгрупа	Създаване на подгрупа
Преименуване на коренния възел	Преименуване на кореновия възел (например името на вашата компания)
Масово записване	Записване на няколко устройства/потребители по едно и също време
Присвояване на маса	Присвояване на профил за съответните групи с един поглед
Бързо администриране на приложения	Изпращане на заявки за (не)инсталиране на приложение до устройствата от съответните групи
Импортиране на потребители в CSV	Импортиране на потребители от CSV в съответната група

Създаване на подгрупа

Чрез "Създаване на подгрупа" можете да създадете допълнителна подгрупа.

Можете да определите към коя група да бъде причислена подгрупата.

(По подразбиране се създава нова група, която е назначена като подгрупа в основния възел)

Преименуване на коренния възел

Тук можете да преименувате главното си име. Обикновено в този случай се използва името на компанията.

Масово записване

С функцията "Масово записване" можете да запишете множество устройства и потребители.

Можете да изберете директно по какъв начин потребителят да получи записването (електронна поща; алтернативна електронна поща; SMS).

В зависимост от това кое устройство ще получи потребителят (iOS, Android, Windows Phone), можете директно да отбележите това тук.

Тук може да се конфигурира и разграничението дали става въпрос за смартфон или таблет, което трябва да изберете правилно с отметка.

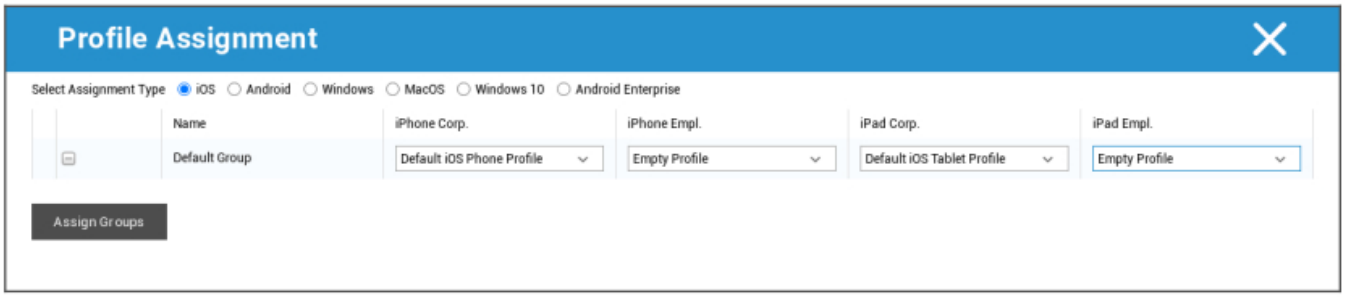
Като последна стъпка можете да установите дали съответното устройство е фирмено или частно (BYOD).

С "Експортиране като CSV" можете да експортирате информацията като CSV файл с данни. В замяна на това можете също да импортирате CSV файла с данни с "Import CSV", като файлът трябва да изглежда като примера по-долу:

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

Присвояване на маса

В раздел Масово задаване можете да зададете профил на всички групи, като той е разделен на iOS - Android - Windows - MacOS - Windows 10 - Android Enterprise.

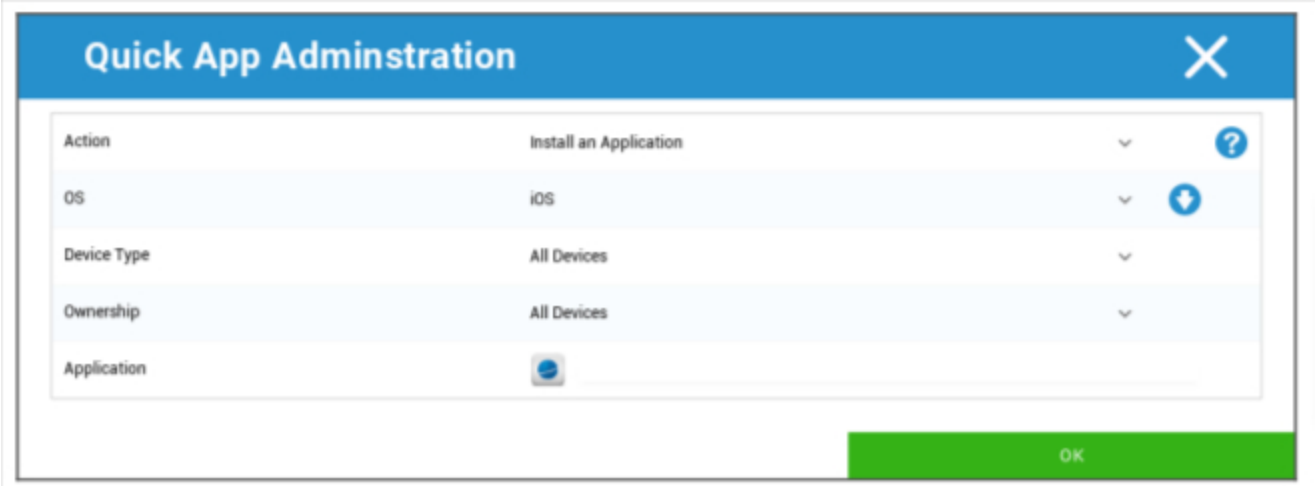


Windows - MacOS - Windows 10 - Android Enterprise

Бързо администриране на приложения

В раздела Бързо администриране на приложения можете да изпращате заявки за инсталиране или деинсталиране на определено приложение до избрана от вас операционна система.

Можете също така да определите дали заявката да бъде изпратена до всички типове устройства на избраната операционна система или само до определен тип устройство.



Импортиране на потребители в CSV

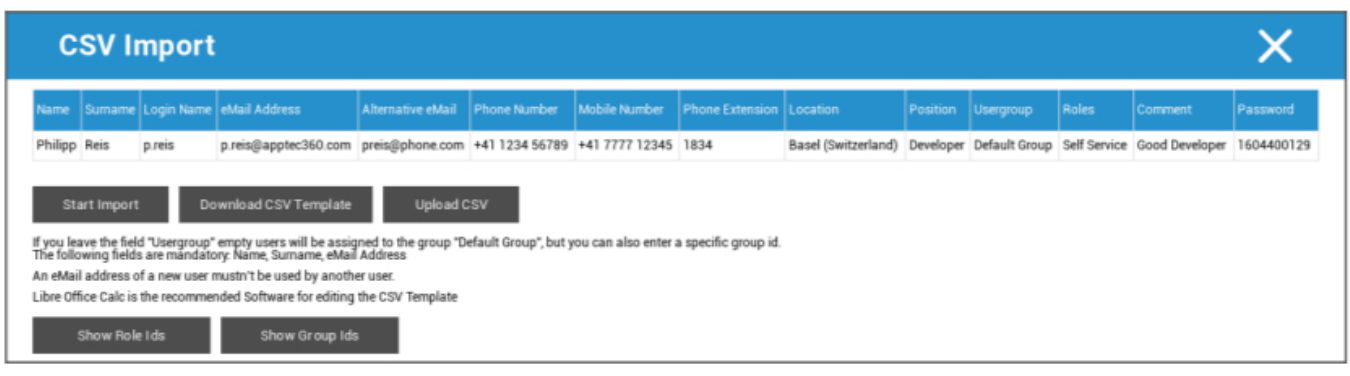
Импортиране на потребители от CSV в съответната група.

С "Изтегляне на шаблон CSV" можете да експортирате файл с шаблон CSV, който може да се попълни (или да се използва като справка).

Можете също така да използвате опциите "Show Role Ids" и "Show Group Ids" като референция за създаване на собствен CSV файл.

CSV файлът може да бъде качен в MDM с "Upload CSV".

Като последна стъпка можете да стартирате импорта, като кликнете върху "Start Import".



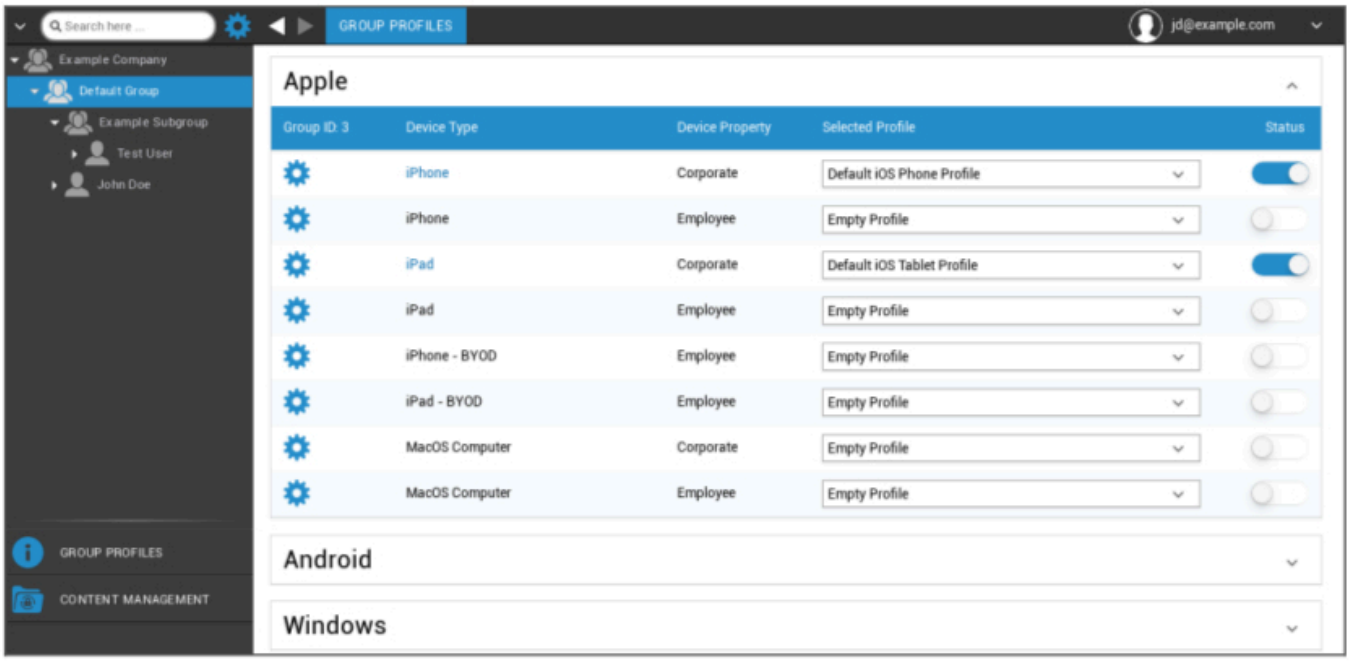
Управление на групи в мобилното управление

С едно кликване върху прегледа се показват различните профили на конфигурация за съответните платформи.

Един профил съдържа всички опции за настройки, които могат да бъдат предварително установени с AppTec360 на устройството на крайния потребител. На всяка платформа можете да създавате профили за корпоративни устройства (Corporate) или за устройства, които се ползват от служителите (Bring-Your-Own-Device).

За да се диференцират конфигурациите на групите устройства, например въз основа на местоположение или функция, се препоръчва да се създадат няколко подгрупи.

Обърнете внимание на управлението на профили в Mobile Management

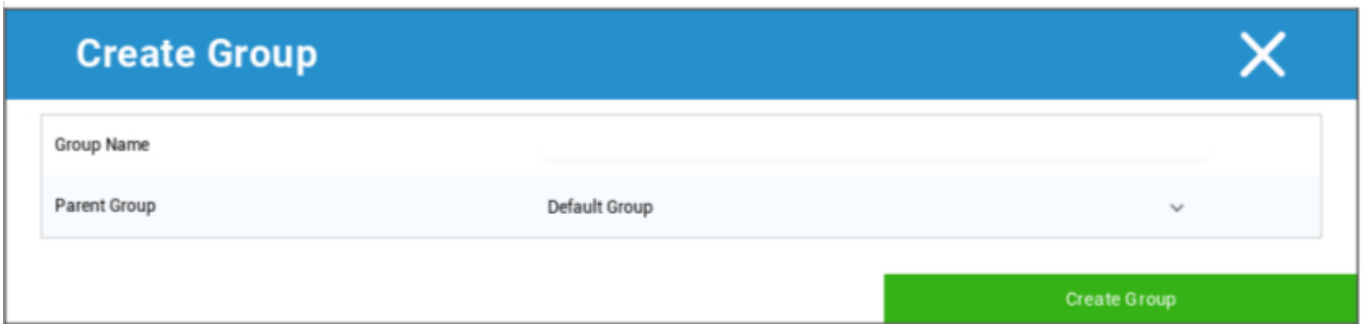


В менюто на предавките се задават различни настройки за съответната (под)група.

Създаване на подгрупа	Създаване на подгрупа за съответната (под)група
Редактиране на избрана група	Редактиране на избрана група
Изтриване на избрана група	Изтриване на избрана група
Масово записване	Записване на много устройства/потребители наведнъж за избрания профил

Присвояване на маса	Присвояване на профили на групата, която е избрана в момента
Създаване на подгрупа	Създаване на подгрупа за съответната (под)група
Създаване на потребител	Създаване на потребител за съответната (под)група

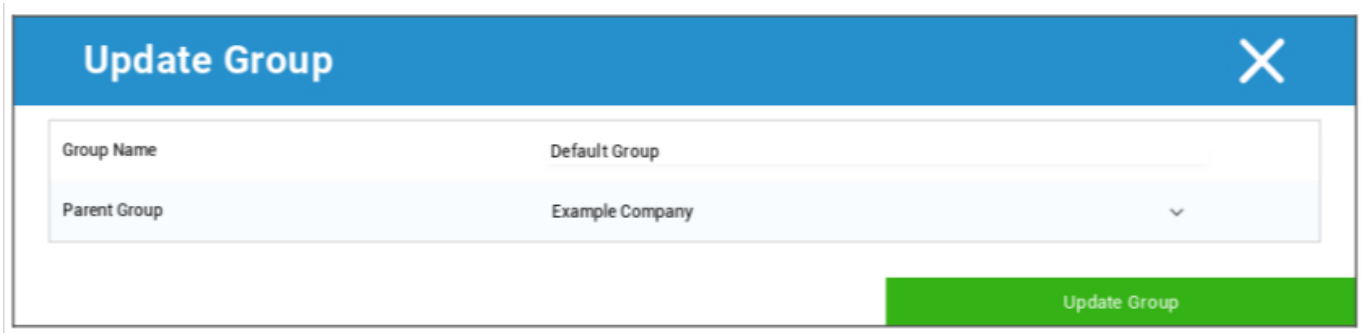
Създаване на подгрупа



Чрез "Създаване на подгрупа" можете да създадете допълнителна подгрупа.

Можете да определите към коя група да бъде причислена подгрупата (по подразбиране подгрупата се причислява към групата, която е избрана в момента).

Редактиране на избрана група



Тук можете да редактирате профила - тук са възможни следните настройки:

- Името на групата може да бъде променено
- Групата на родителите може да бъде променена

Изтриване на избрана група

Под "Изтриване на избрана група" се показват всички потребители и устройства, които са в съответната група. Тук имате възможност да ги изтриете.

За един потребител можете да изпълнявате следните команди за изтриване:

Изтриване на потребител	Потребителят е изтрит
Преместване на потребител в група:	Можете да преместите потребителя в друга група (следващата колона, например "Администратори").

За едно устройство можете да изпълнявате следните команди за изтриване:

Изтриване и изтриване	Изтриване и изтриване на устройство
Изтриване от системата	Премахване на устройството само от AppTec

Справка: Масово записване

Справка: Присвояване на маса

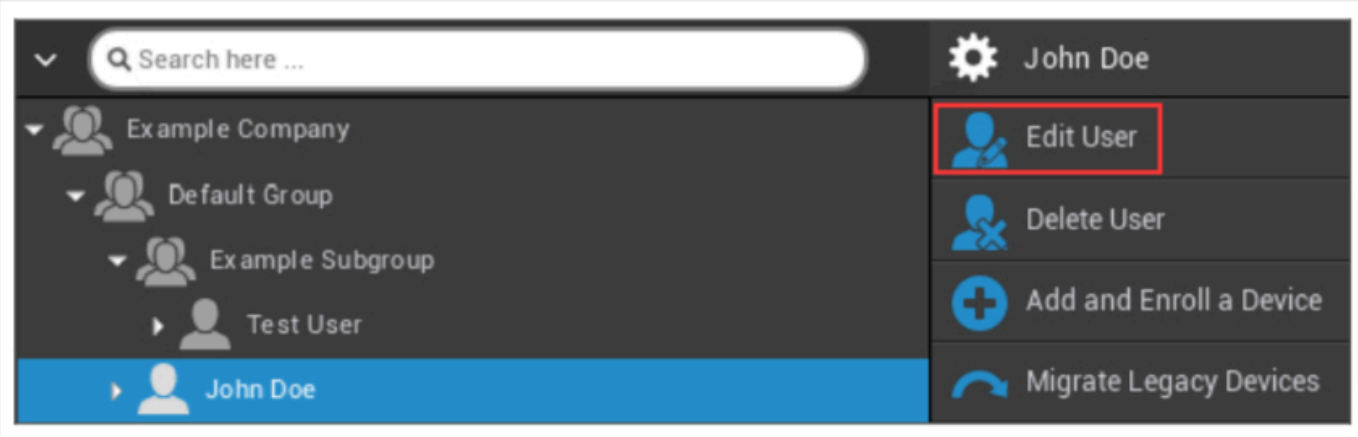
Създаване на потребител

Чрез "Създаване на потребител" можете да добавите нов потребител.

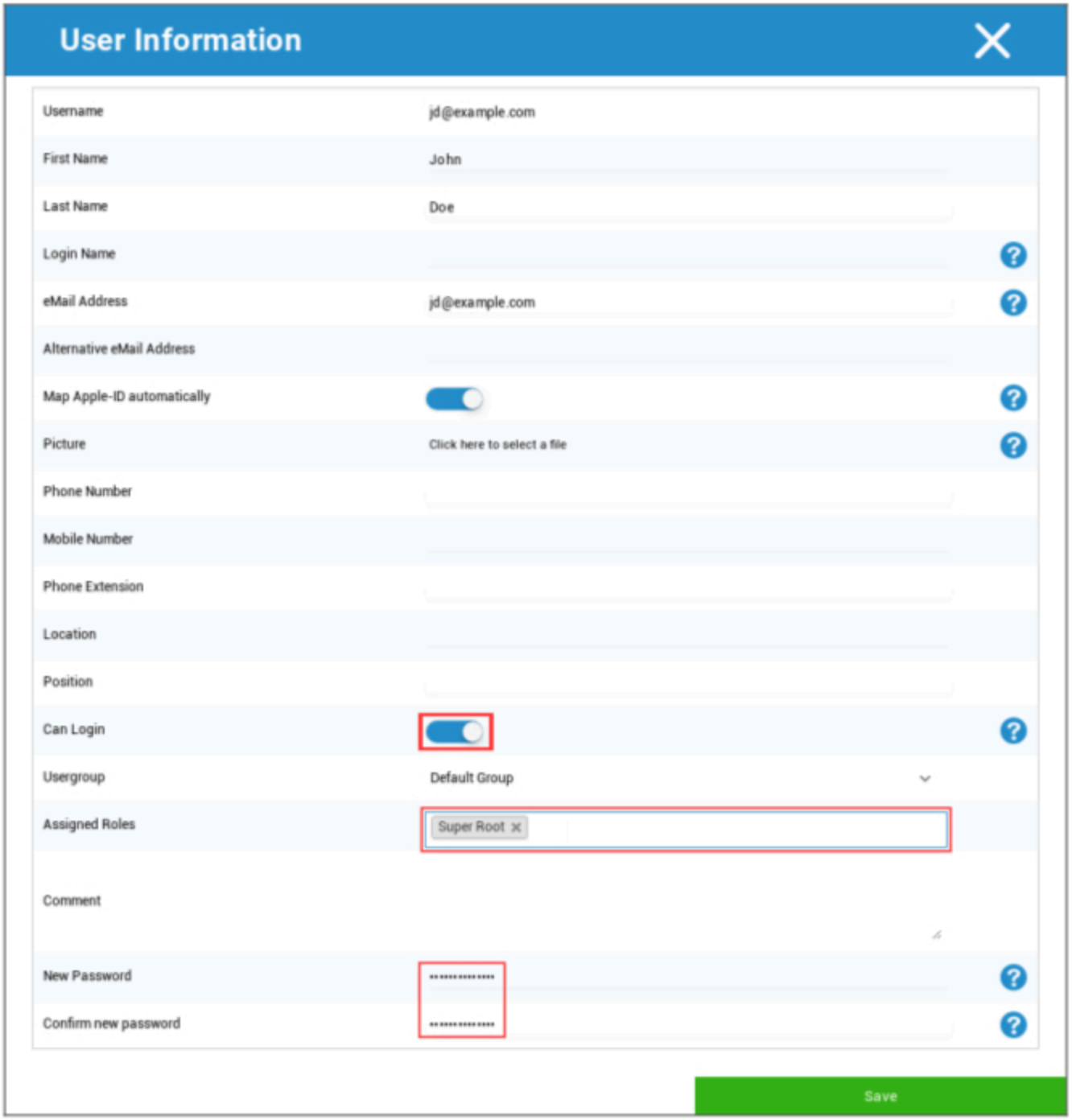
Създаване на нов администраторски потребител

Можете да зададете потребител като Admin-User. Това ще му даде права да влиза в конзолата, както и да променя потребители/групи/устройства.

Създайте нормален потребител или използвайте съществуващ потребител. Изберете Потребителя, на когото искате да дадете администраторски права, щракнете върху колелото и изберете "Редактиране на потребител":



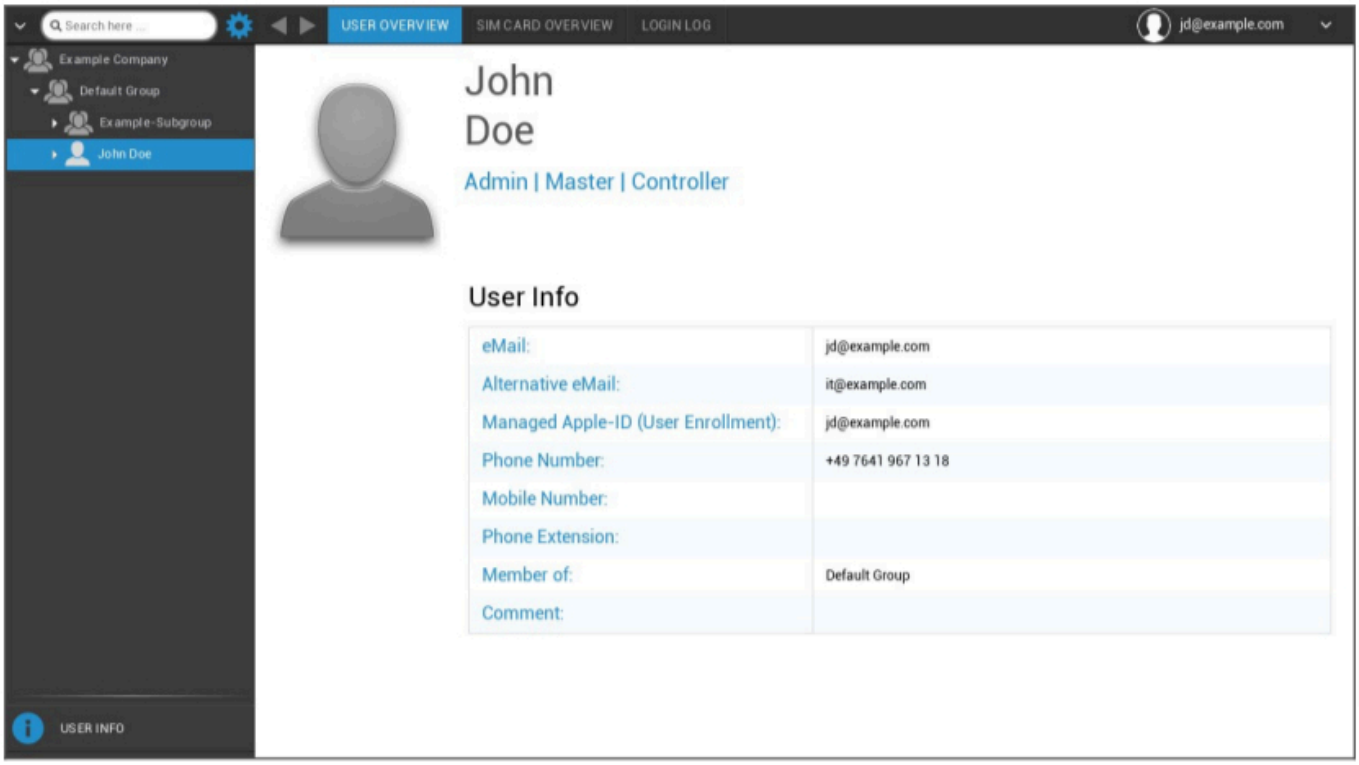
Активирайте превключвателя за "Can Login" (Може да влиза), задайте на потребителя ролята "Super-Root" и задайте парола.



Запазете това и потребителят вече може да влезе с потребителското име и паролата.

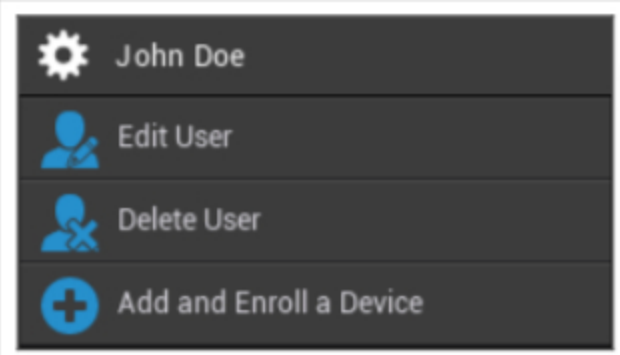
Управление на потребителите в мобилното управление

Когато изберете определен потребител, ще видите следния преглед:



Ще получите преглед на цялата информация, която сте въвели по-рано в "Създаване на потребител".

С монтираното в горната част съоръжение можете да извършите следните конфигурации:



Потребителско име	Потребителско име на избрания потребител
Редактиране на потребител	Редактиране на информация за потребителя

Изтриване на потребител	Изтриване на потребител • Изтриване от системата = устройството ще бъде премахнато от AppTec • Изтриване и изтриване = Устройството ще бъде възстановено до фабричните настройки и премахнато от AppTec
Добавяне и записване на устройство	Записване на устройство за избрания потребител

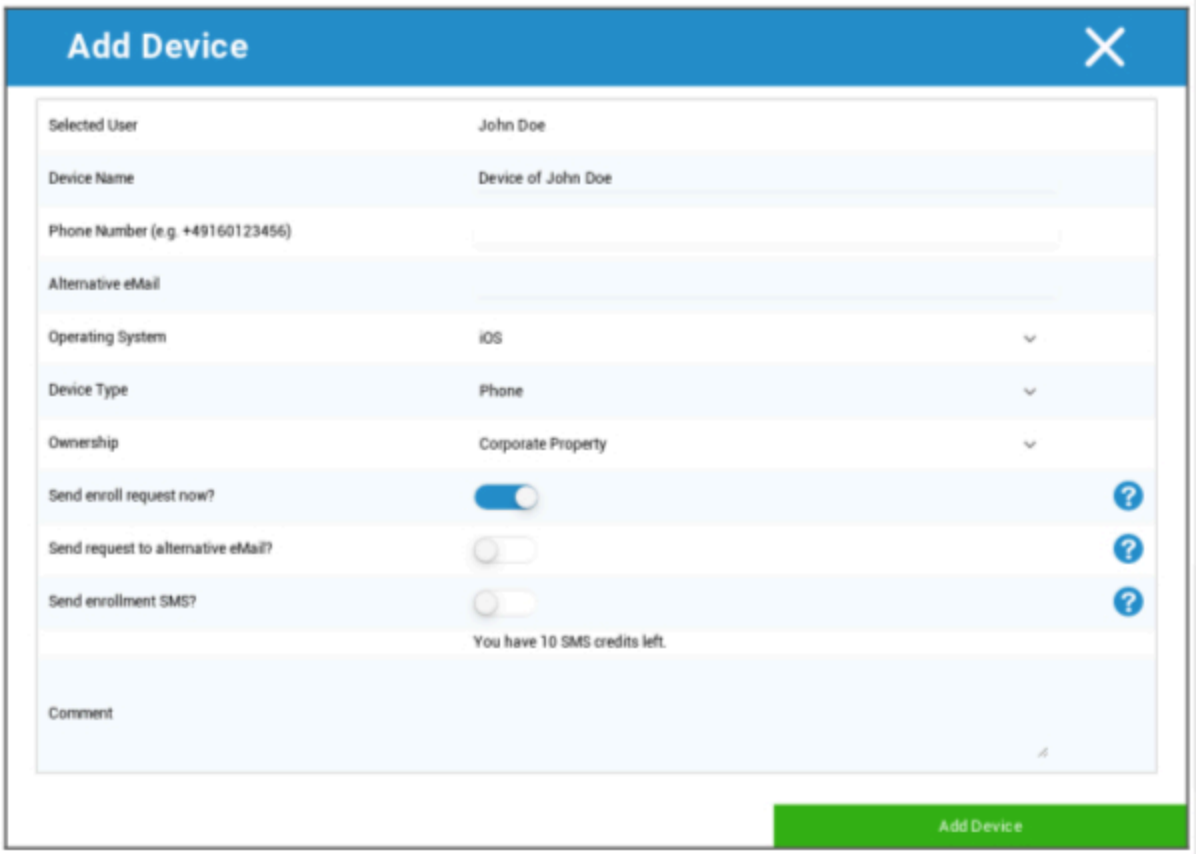
Имайте предвид, че достъпът до администрацията може да бъде подаден и като локален потребителски акаунт в структурата на йерархията. Без да е създаден допълнителен администратор, този не трябва да се изтрива!

Добавяне и записване на устройство

Тук можете да изберете устройство за избраната употреба.

Можете също така да запишете устройства в група директно. За целта щракнете върху групата, щракнете върху колелото и изберете "Добавяне и записване на устройство".

Трябва да видите следния преглед:



В зависимост от вида на устройството, което искате да запишете, трябва да извършите следните конфигурации:

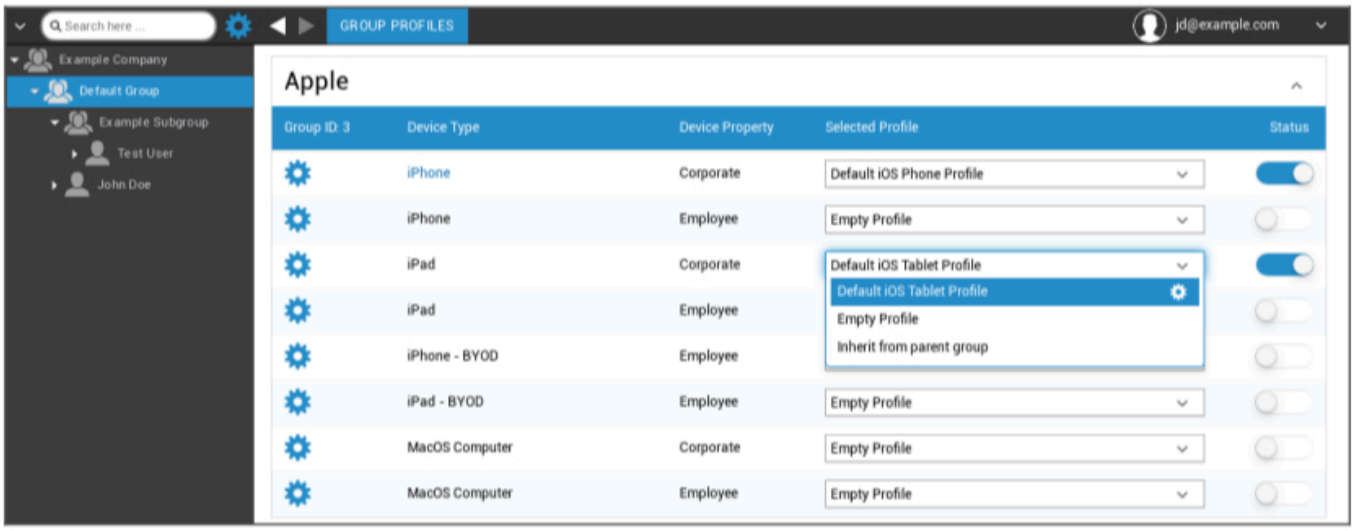
Избран потребител	Избран потребител (попълва се автоматично)
Име на устройството	Попълва се автоматично (устройство за "име на потребителя") - може обаче да се промени
Телефонен номер	Телефонният номер ще бъде попълнен автоматично (стига да е бил предоставен от потребителя) - тук обаче може да бъде добавен или променен.
Алтернативна електронна поща	Алтернативен имейл, ще бъде попълнен автоматично (стига да е бил предоставен от потребителя) - тук обаче може да бъде добавен или променен.
Собственик на устройството	Корпоративна собственост = корпоративно устройство Собственост на служителя = устройство BYOD
Изберете операция Система	Тук можете да избирате между следните операционни системи: • iOS • iOS BYOD (записване на потребители) • MacOS • Android Enterprise • Android • Windows Mobile • Windows 10
Изпращане на заявка за записване?	Имейлът се изпраща незабавно на основния имейл адрес и потребителят се подканва да свърже устройството си.
Изпращане на заявка за алтернативна електронна поща?	Изпратете имейла допълнително или изключително (в случай че "Изпращане на заявка за записване?" е деактивирана) на алтернативния имейл адрес (имейлът е различен от "нормалния" имейл за заявка за записване)
Изпращане на SMS за записване?	Изпращане на заявка за записване чрез SMS (трябва да се въведе "телефонен номер")

След като бъде изпратена заявката за записване, устройството веднага ще бъде показано (маркирано в червено).

Щом устройството бъде успешно свързано, скоро след това то ще бъде маркирано в зелено и по този начин ще бъде готово да получава ограничения, приложения и т.н.

Управление на профили в мобилното управление

След като щракнете върху група, ще получите преглед на всички платформи на устройства, които трябва да бъдат конфигурирани, и съответно назначените профили.



	Извършване на конфигурацията за избрания профил
Тип устройство	Тип и/или модел на устройството
Собственост на устройството	Собственик на устройството (корпоративен = корпоративна собственост, служител = частно устройство на служител)
Избран профил	Избран профил (зъбното колело отваря диалога за конфигуриране на профила)
Статус	Вкл./Изкл. (профилът е активиран/деактивиран)

Когато изберете предавката, ще получите следните опции:

Създаване на профил

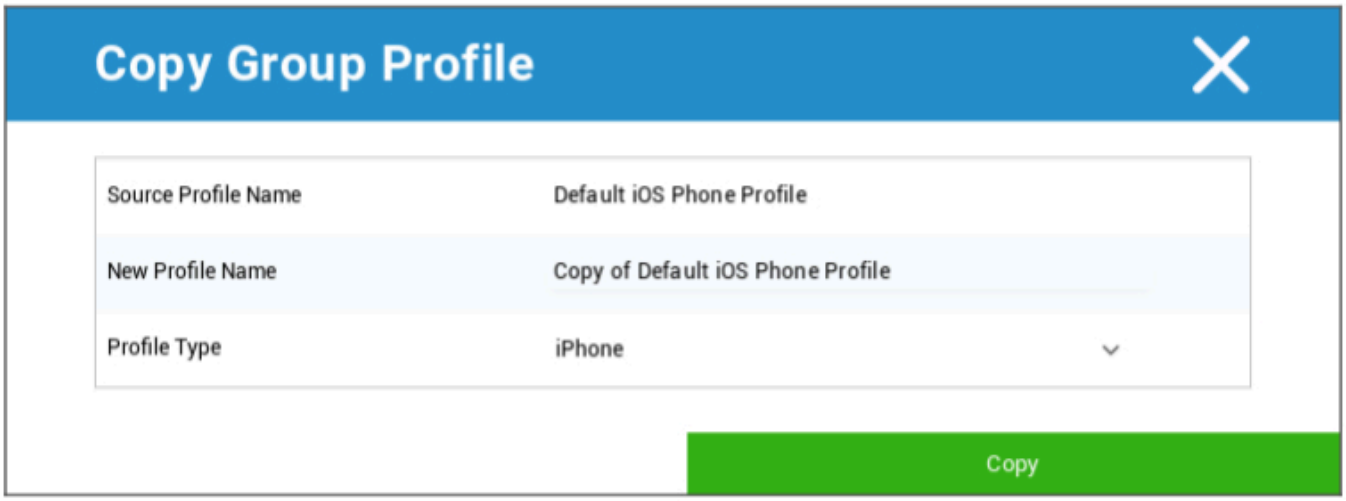
Можете да създавате и конфигурирате нов профил за всеки запис и/или платформа. След като щракнете върху тази подточка, профилът ще бъде създаден незабавно и можете да започнете с конфигурирането на iOS, Android und Windows Phone веднага.

Редактиране на профила

След като щракнете върху "Edit Profile" (Редактиране на профил), ще се покаже конфигурацията на съответния профил, където можете да зададете конфигурациите.

Копиране на профил

С помощта на функцията "Копиране на профил" можете да копирате настройките/ конфигурациите от вече съществуващ профил и да ги добавите към нов профил.

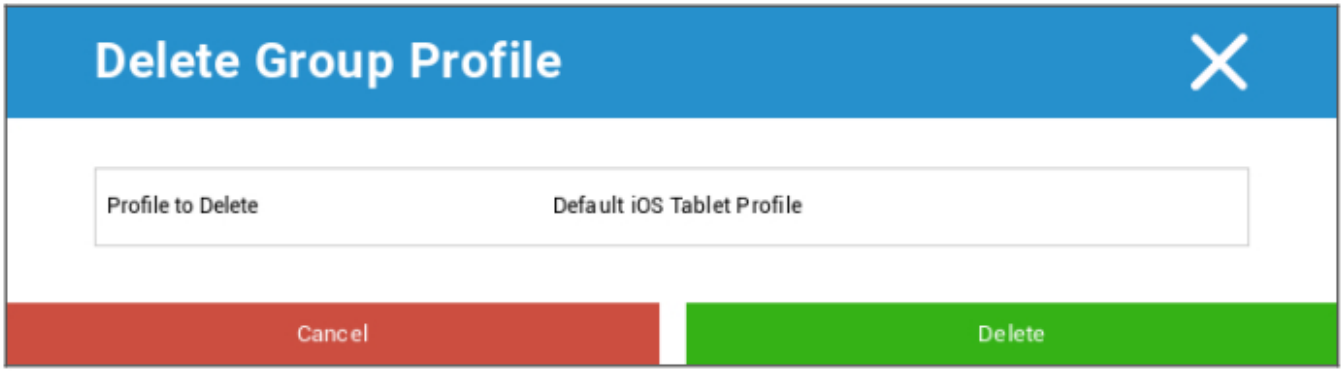


Име на профила на източника	Име на профила, който трябва да се копира
Ново име на профила	Име на новия профил
Тип на профила	Тип на профила (Телефон/таблет)

След като щракнете върху "Копиране", профилът ще бъде създаден и вече може да бъде присвоен на групата.

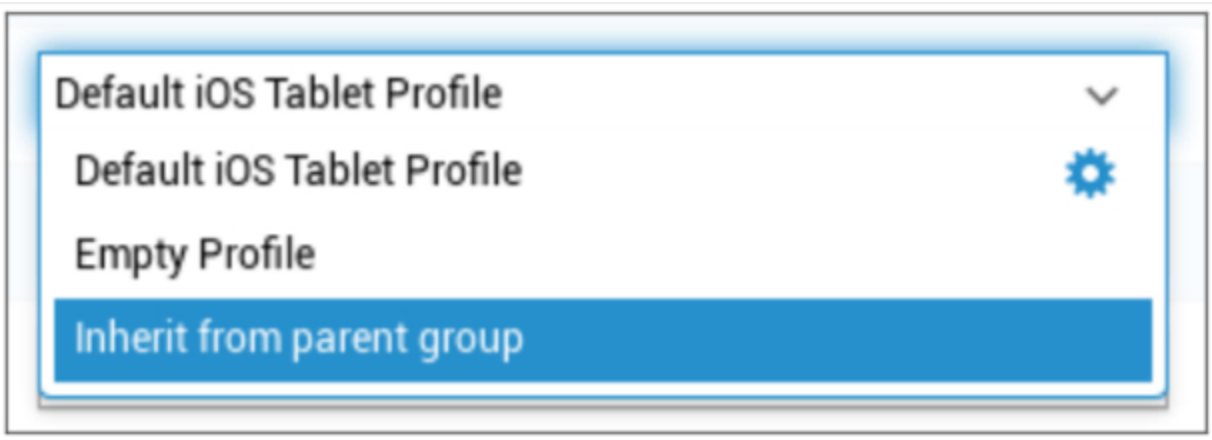
Изтриване на профил

Тук можете да изтриете за постоянно даден профил. Моля, имайте предвид, че по време на процеса на изтриване и на последващия процес "Assign Now" за профила конфигурацията ще изчезне на съответните устройства от засегнатата група и няма да може да бъде възстановена!


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

Наследяване на профили

По време на избора на профилите е налична опцията "Наследи от родителската група".



Когато профилът е активиран, профилът на родителската група ще се използва за съответно избраното устройство (и съответния тип устройство). Моля, имайте предвид също, че промените в този профил могат да засегнат множество групи.

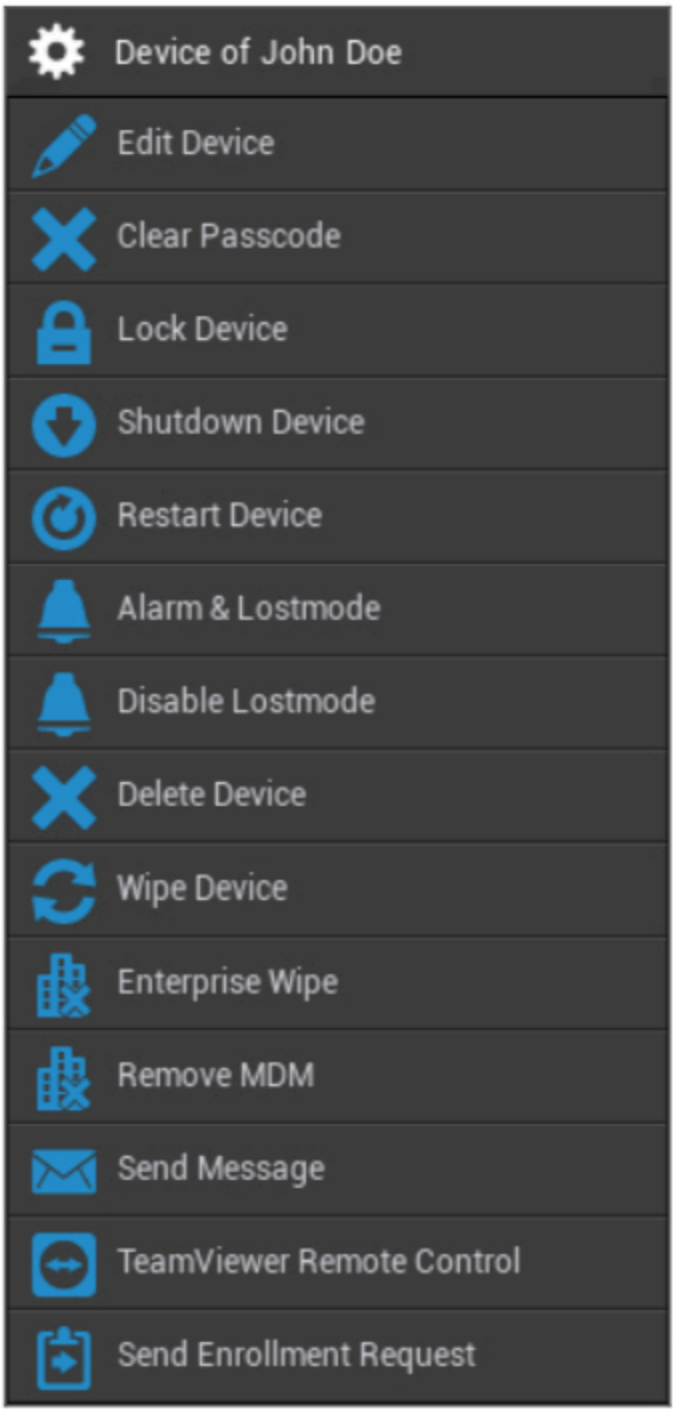
Тази конфигурация се задава като стойност по подразбиране, когато се създава нова подгрупа.

Налична е и конфигурацията "Празен профил", която съответства на празен профил, което означава, че в крайна сметка няма да се извършват нови конфигурации на крайното потребителско устройство.

Управление на устройствата в мобилното управление

Когато изберете устройство, можете да изпълнявате различни задачи чрез "зъбното колело". Те са различни, в зависимост от платформите на операционната система (iOS, Android Enterprise, Android, Windows Mobile, Windows 10).

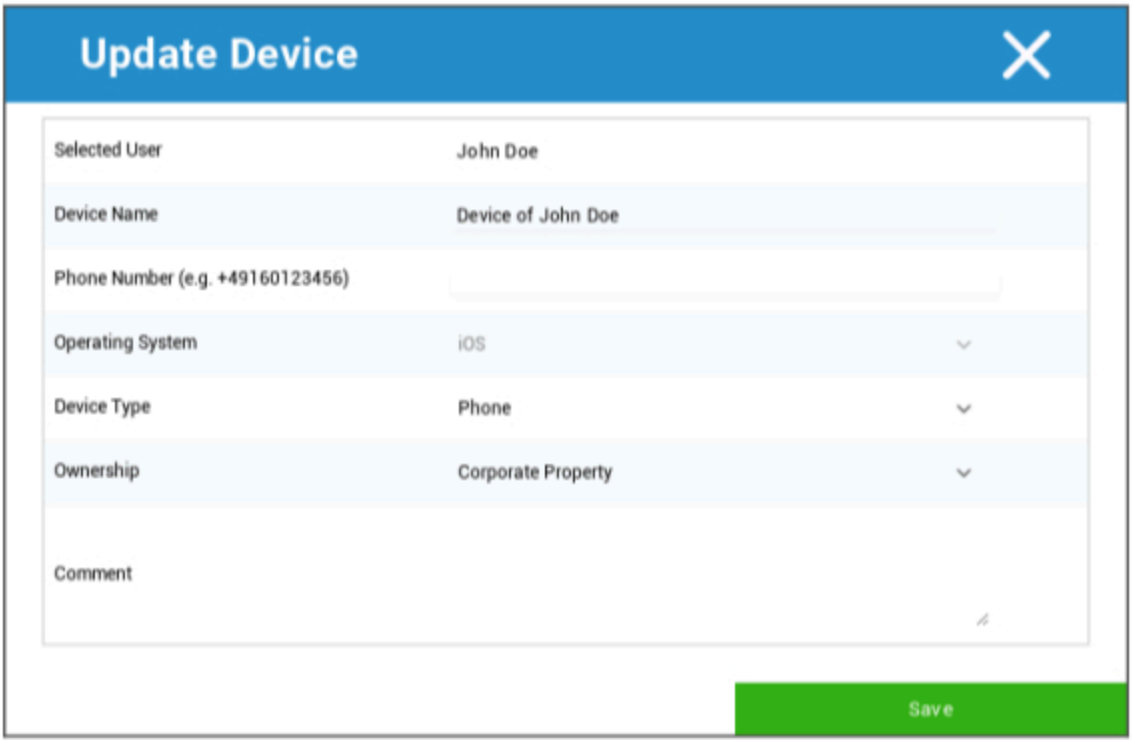
IOS



Редактиране на устройство	Редактиране на устройство
Изчистване на паролата	Кодът за достъп на устройството е изтрит
Устройство за заключване	Заключване на устройството (заключен екран)

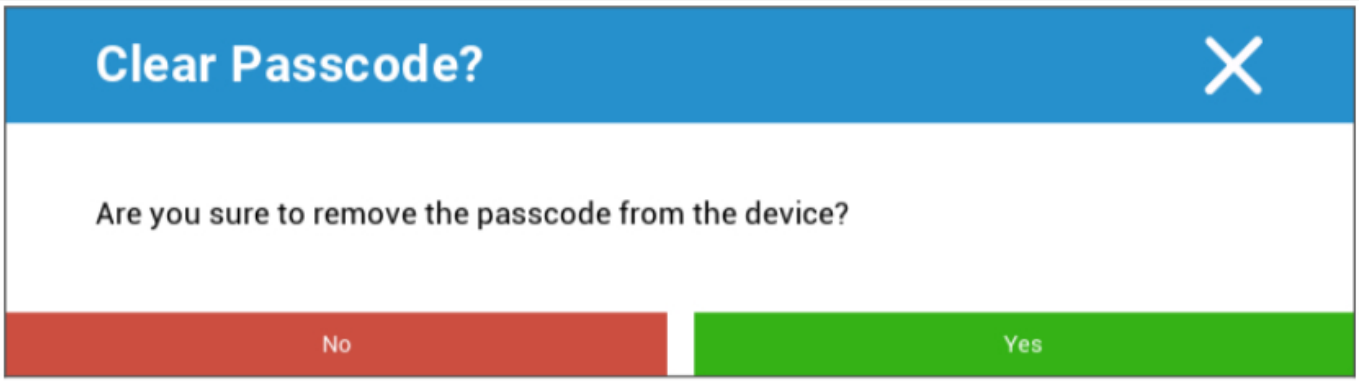
Устройство за изключване	Устройство за изключване
Рестартиране на устройството	Рестартиране на устройството
Аларма и режим Lostmode	Стартиране на алармата и Lostmode
Деактивиране на Lostmode	Деактивиране на Lostmode
Изтриване на устройство	Премахване на устройството от AppTec
Изтриване на устройството	Възстановяване на фабричните настройки на устройството
Изтриване на предприятието	Информацията, приложенията и профилите, предоставени от AppTec360, се изтриват (устройството се отделя от MDM).
Премахване на MDM	
Изпрати съобщение	Изпращане на известия Push до устройството Съобщението ще бъде показано в приложението AppTec360 (таб Съобщение)
Дистанционно управление на TeamViewer	Стартиране на сесия за дистанционно управление с помощта на TeamViewer
Изпращане на заявка за записване	Изпращане (повторно) на заявка за записване

Редактиране на устройство



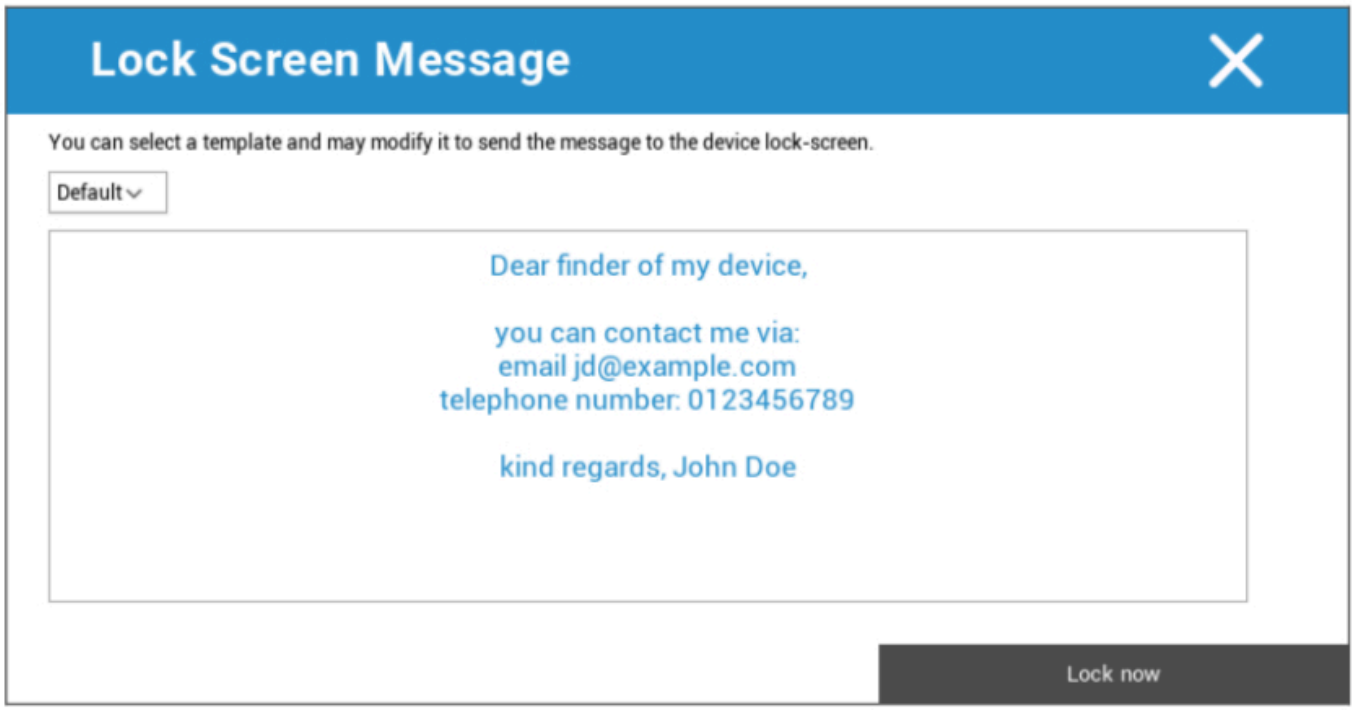
Тук можете да актуализирате разнообразна информация за устройството.

Изчистване на паролата



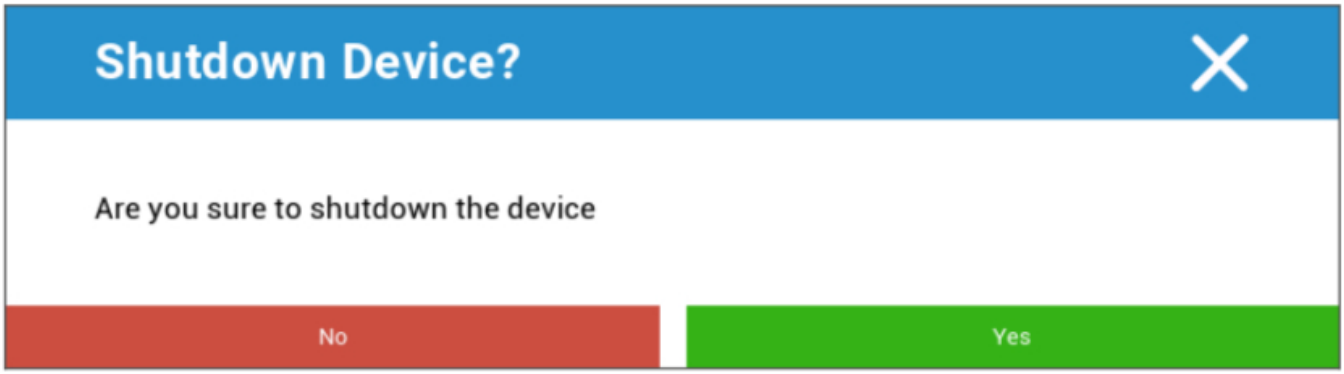
Под "Изчистване на паролата" можете да премахнете паролата от устройството от разстояние. Впоследствие потребителят ще бъде подканен да издаде нова парола (в зависимост от указанията за паролата).

Устройство за заключване



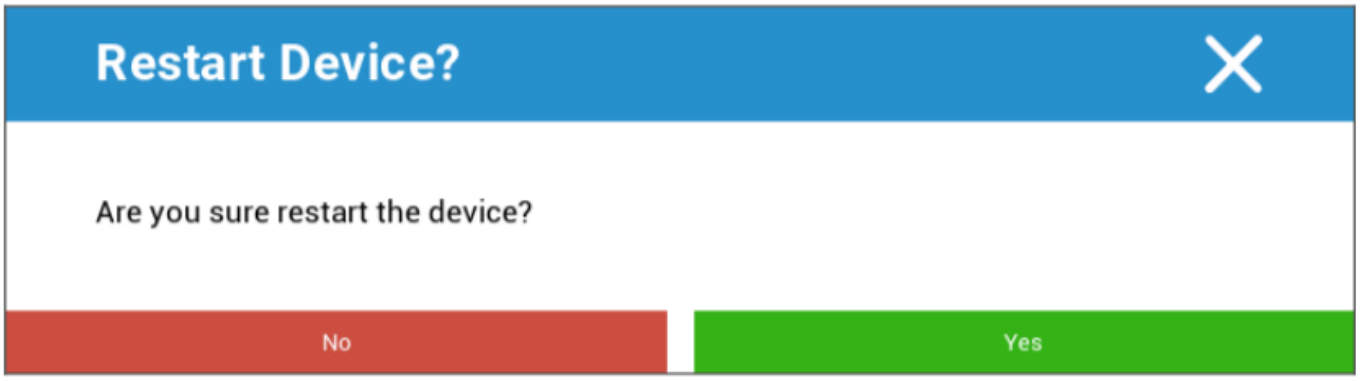
Тук се изпраща команда за заключване на крайното потребителско устройство (екран за заключване).

Устройство за изключване



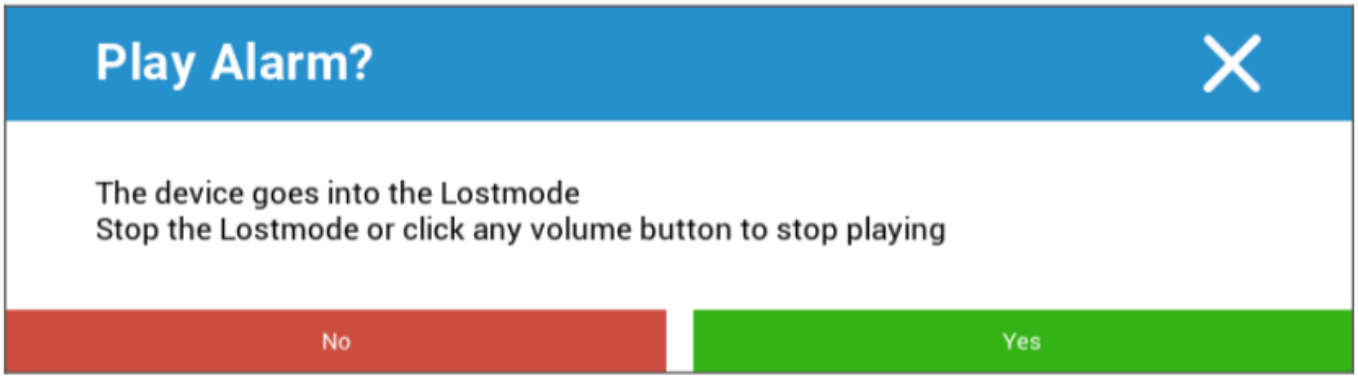
Тук се изпраща команда за изключване на крайното потребителско устройство.

Рестартиране на устройството

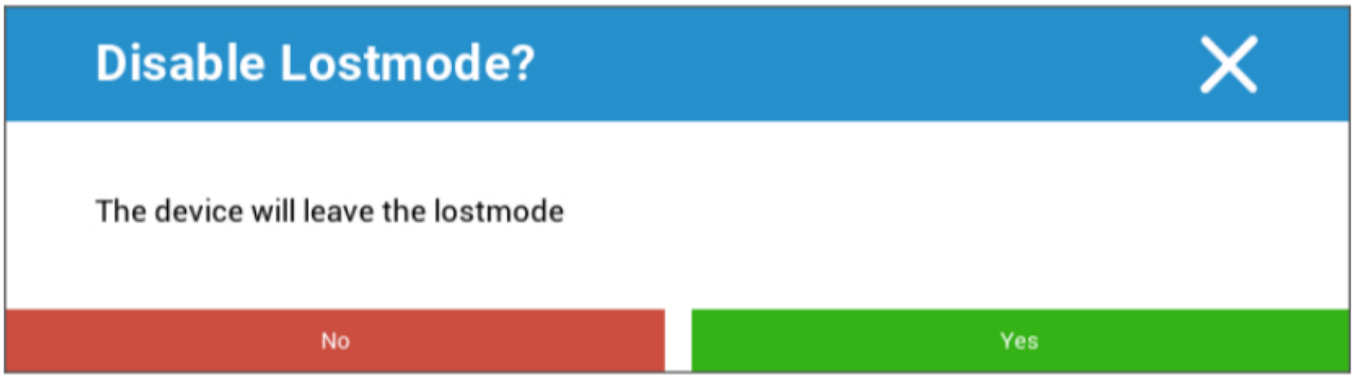


Тук се изпраща команда за рестартиране на крайното потребителско устройство.

Аларма и режим на изгубване | Деактивиране на режима на изгубване



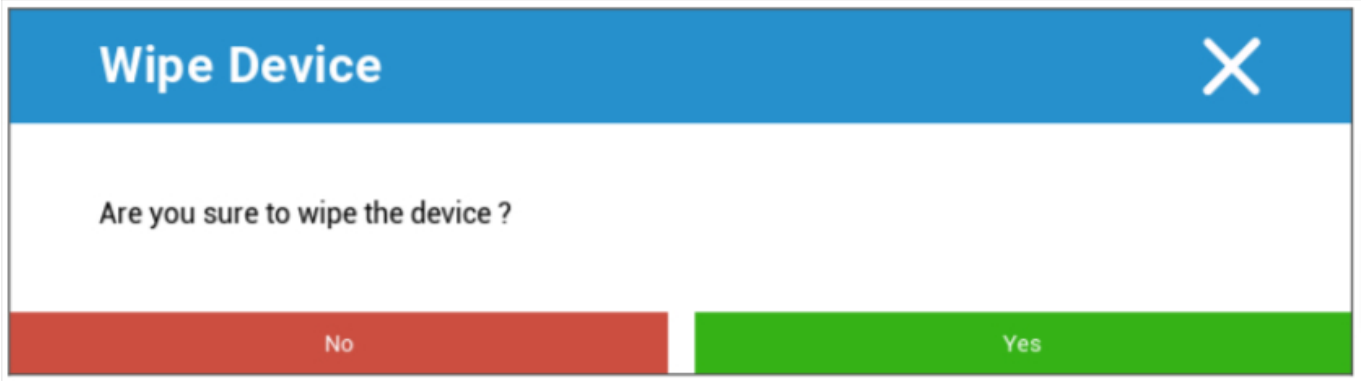
Тук устройството може да бъде настроено в режим Lostmode, който настройва устройството да възпроизвежда постоянно алармен звук. Режимът Lostmode може да бъде спрян чрез натискане на който и да е бутон за сила на звука на устройството или дистанционно чрез щракване върху "Disable Lostmode" (Изключване на режима Lostmode):



Изтриване на устройство

Тук може да се изпълни командата за изтриване. Отново можете да решите дали устройството да бъде премахнато само от AppTec360 ("Изтриване от системата") или дали устройството да бъде премахнато от AppTec360 и да бъде възстановено до фабричните му настройки ("Изтриване и изтриване").

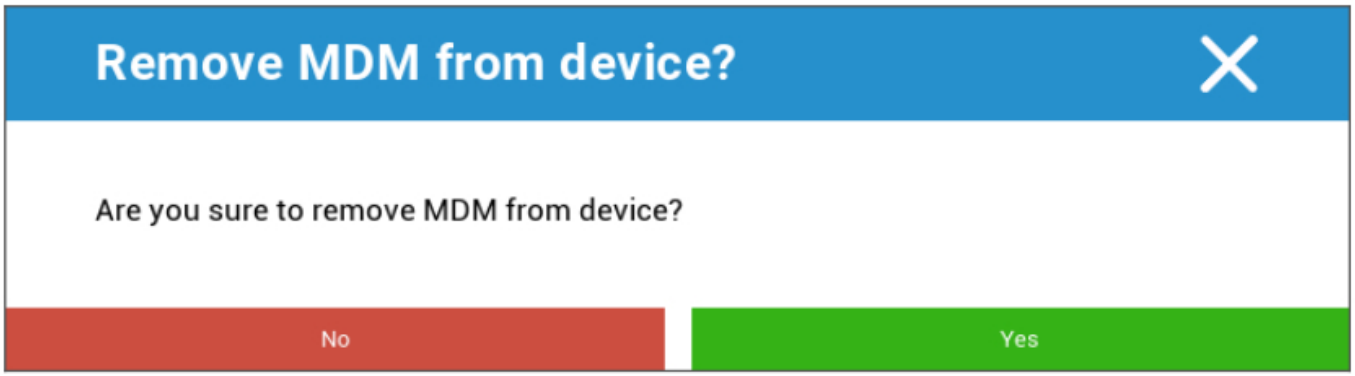
Изтриване на устройството



Под "Изтриване на устройството" можете да извършите пълно изтриване на устройството. Устройството ще бъде възстановено до фабричните си настройки.

Изтриване на данни в предприятието | Премахване на MDM

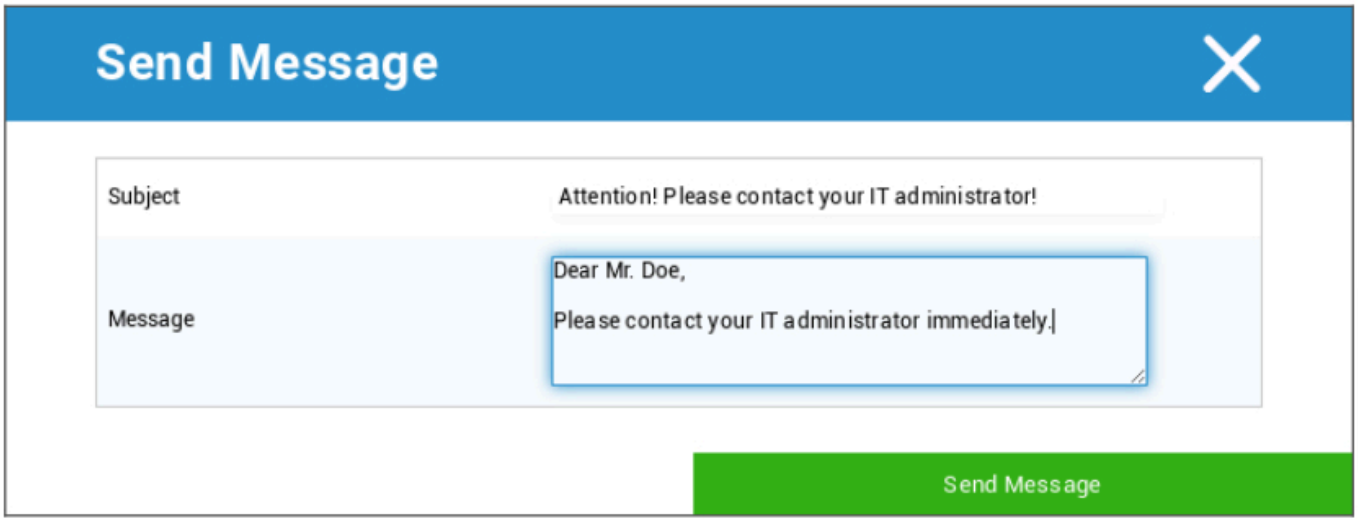
Изтриват се само информацията, приложенията и профилите, предоставени от AppTec360. По този начин корпоративните данни вече няма да са достъпни на устройството на крайния потребител. Личната зона не е засегната и продължава да бъде на устройството на крайния потребител.



С "Remove MDM" можете да премахнете MDM профила на крайното потребителско устройство и всички други елементи, предоставени от AppTec.

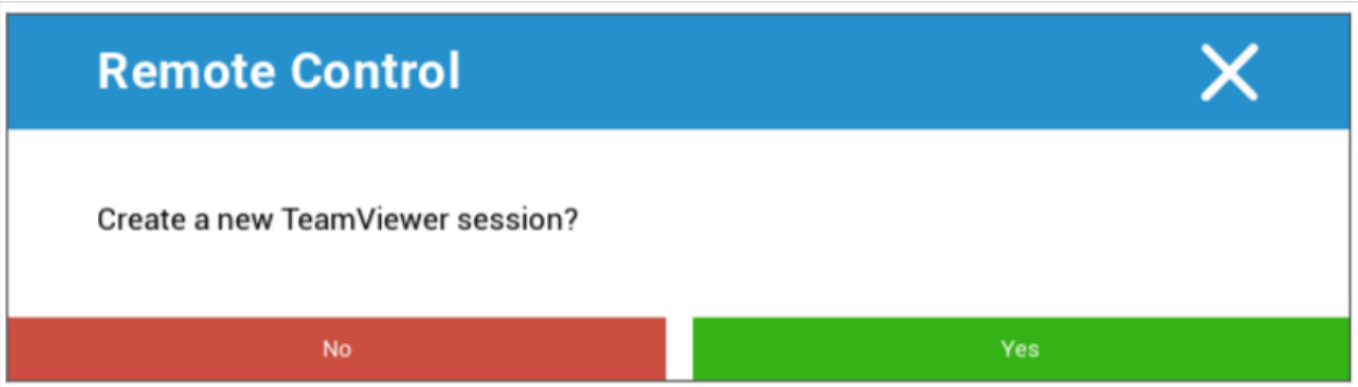
Тази команда изпълнява същото действие като "Enterprise Wipe".

Изпрати съобщение



Тук можете да изпратите Push известие до съответното устройство.

Дистанционно управление на TeamViewer



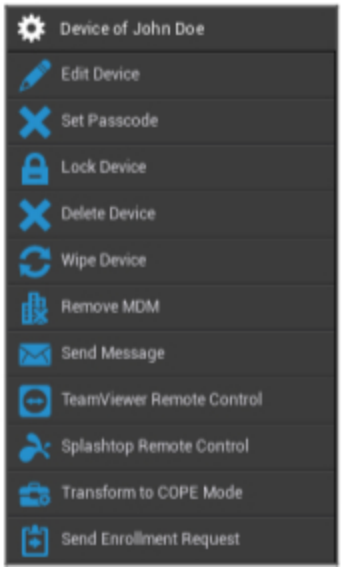
Тук може да се стартира сесия за дистанционно управление Teamviewer.

Изпращане на заявка за записване

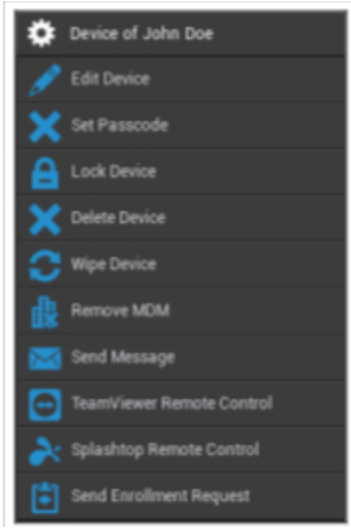
С "Изпращане на заявка за записване" можете да изпратите заявка за записване (отново) до съответния потребител.

Android

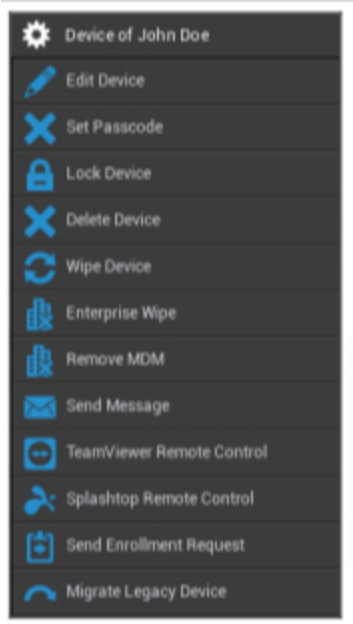
AE Напълно управлявано устройство (Управлявана работа)



Работен профил на AE (контейнер)



Телефон с Android | Таблет

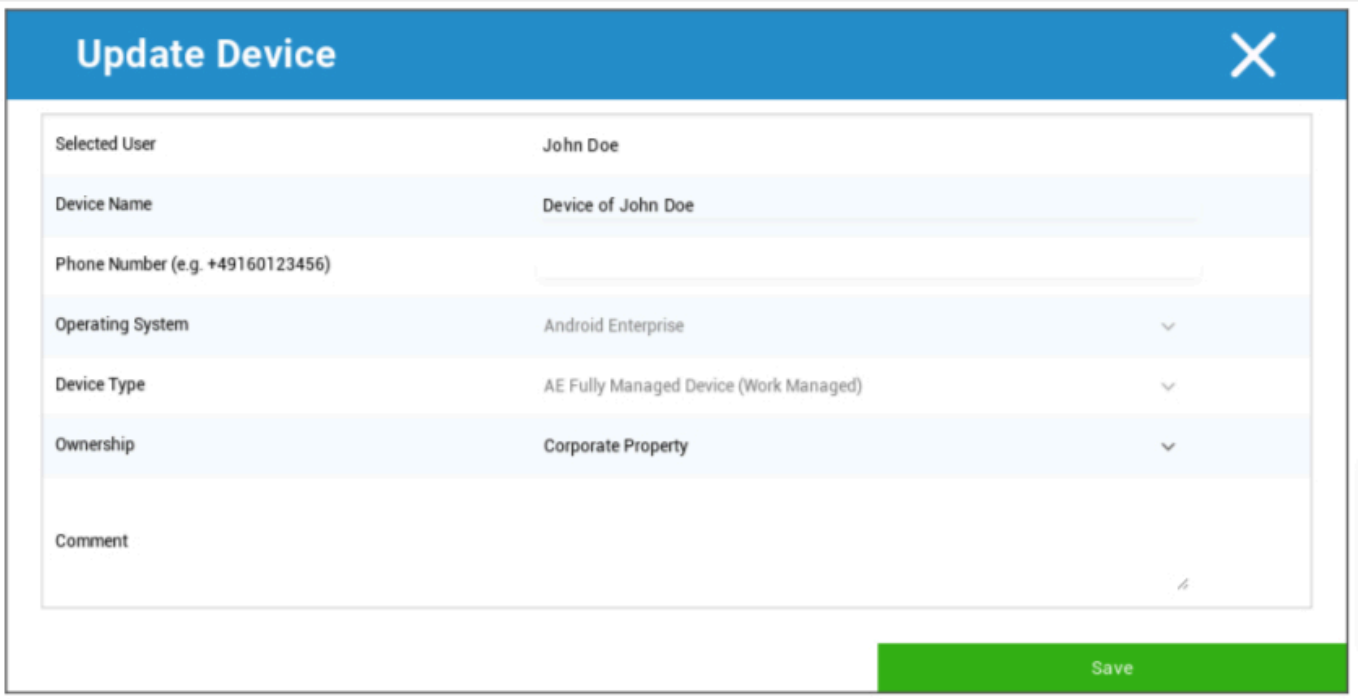


Редактиране на устройство	Редактиране на информация за устройството
Задаване на код за достъп	Задаване на код за достъп на устройството
Устройство за заключване	Заключване на устройството (заключен екран)
Изтриване на устройство	Изтриване на устройството от AppTec
Изтриване на устройството	Възстановяване на фабричните настройки на устройството
Изтриване на предприятието	Информацията, приложенията, профилите, които са предоставени от AppTec360, се изтриват (устройството ще бъде отделено от MDM)
Премахване на MDM	
Изпрати съобщение	Изпращане на известия Push до устройството Съобщението ще бъде показано в приложението AppTec360 (таб Съобщение)
Дистанционно управление на TeamViewer	Стартиране на сесия за дистанционно управление на това устройство с помощта на TeamViewer
Дистанционно управление Splashtop	Стартиране на сесия за дистанционно управление на това устройство с помощта на Splashtop

Трансформиране в режим COPE (само при напълно управлявано устройство AE (Work Managed))	Създаване на работен профил на това устройство с пълно управление на AE (управление на работата)
Изпращане на заявка за записване	Изпращане на (повторна) заявка за записване
Мигриране на наследено устройство (само за телефон/таблет с Android, когато е регистриран с помощта на Device Owner Mode Provisioning)	Мигриране на профил на телефон/таблет с Android към профил на напълно управлявано устройство (управлявано от работата) на AE

Редактиране на устройство

Тук можете да актуализирате разнообразна информация за устройството.



Избран потребител	Потребител на устройството
Име на устройството	Име на устройството
Телефонен номер	Телефонен номер на устройството
Операционна система	Android Enterprise Android
Тип устройство	Android Enterprise: • AE Напълно управлявано устройство (Управлявана работа) • Режим на работния профил AE (само за контейнери) • AE Напълно управлявано устройство с работен профил (COPE) Android: • Телефон • Таблет
Собственост	Corporate = корпоративна собственост

	Employee = свойство на служителя
Коментар:	Допълнителни описания на устройството

Изчистване на паролата

Тук можете да премахнете паролата на избраното устройство. По подразбиране при Android кодът за достъп е зададен на "123456" - това може и трябва да бъде променено от потребителя впоследствие.

Устройство за заключване

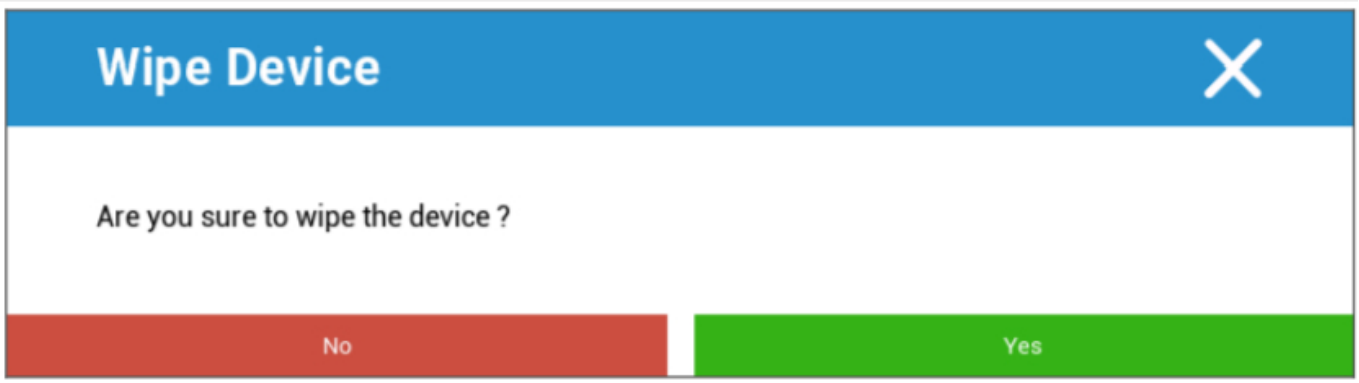
Тук към устройството ще бъде изпратена команда за заключване на устройството (заключване на екрана).

Изтриване на устройство

Тук може да се изпълни команда за изтриване. Отново можете да решите дали устройството да бъде премахнато само от AppTec360 ("Изтриване от системата") или дали устройството да бъде премахнато от AppTec360 и допълнително да бъдат възстановени фабричните му настройки ("Изтриване и изтриване").

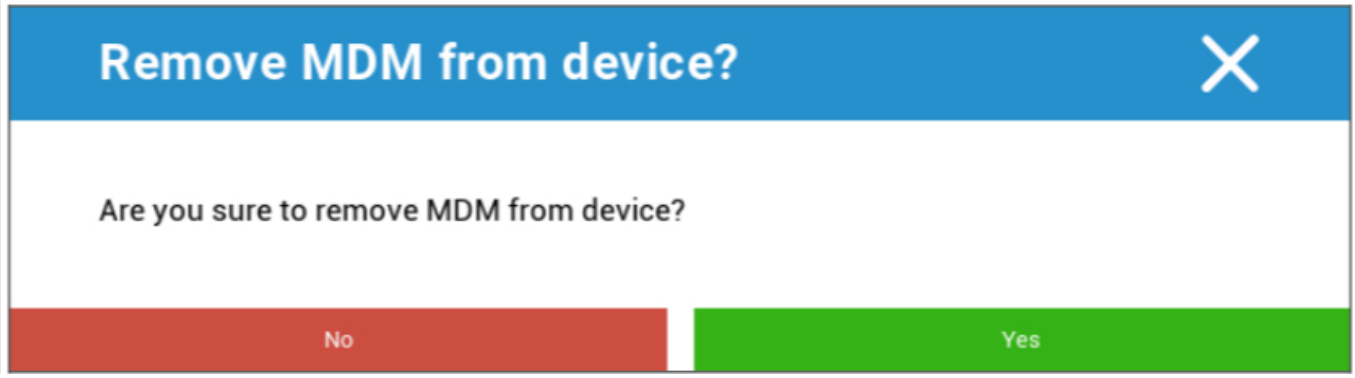
Изтриване на устройството

Под "Изтриване на устройството" можете да извършите пълно изтриване на устройството. След това устройството ще бъде възстановено до фабричните си настройки.



Освен това, ако устройството съдържа SD карта, можете да изтриете SD картата. Можете да постигнете това, като зададете "Wipe SD Card too? " на "Вкл.".

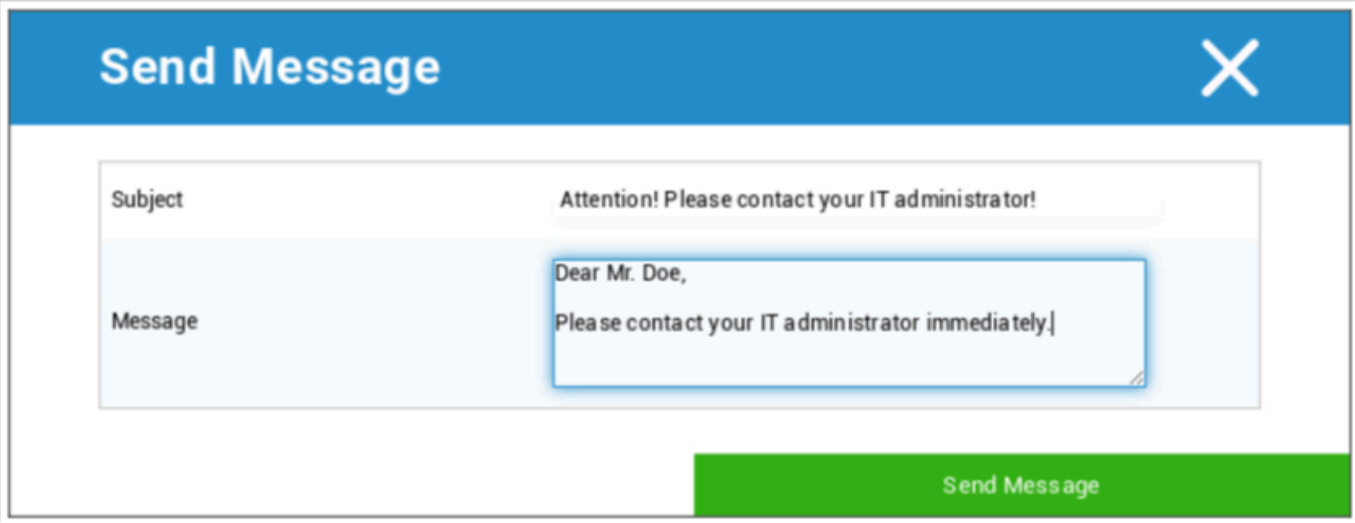
Премахване на MDM



Това е препоръчителният метод за създаване на отделяне от MDM.

Изтриват се само информацията, приложенията и профилите, предоставени от AppTec360, което означава, че всички корпоративни данни вече няма да са налични на устройството на крайния потребител. Частната сфера обаче не е засегната и продължава да бъде на устройството на крайния потребител.

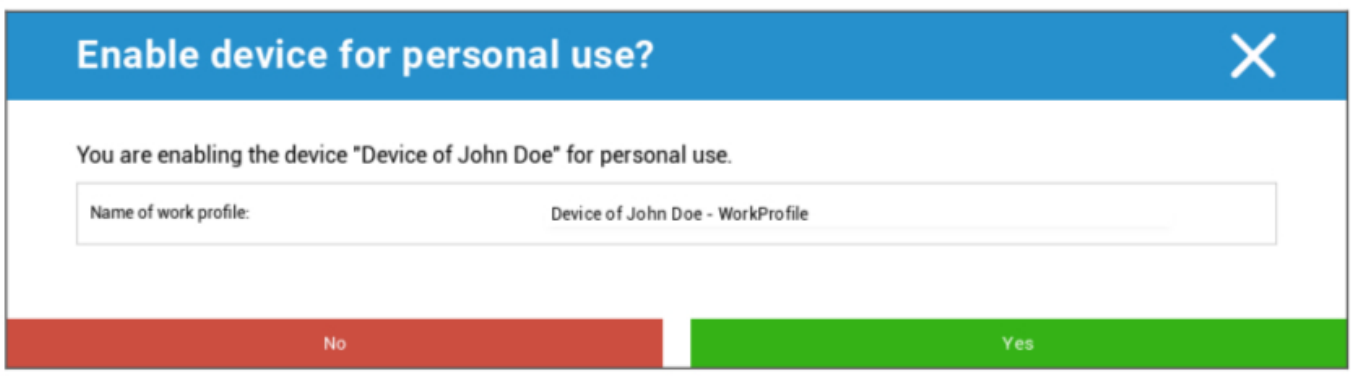
Изпрати съобщение



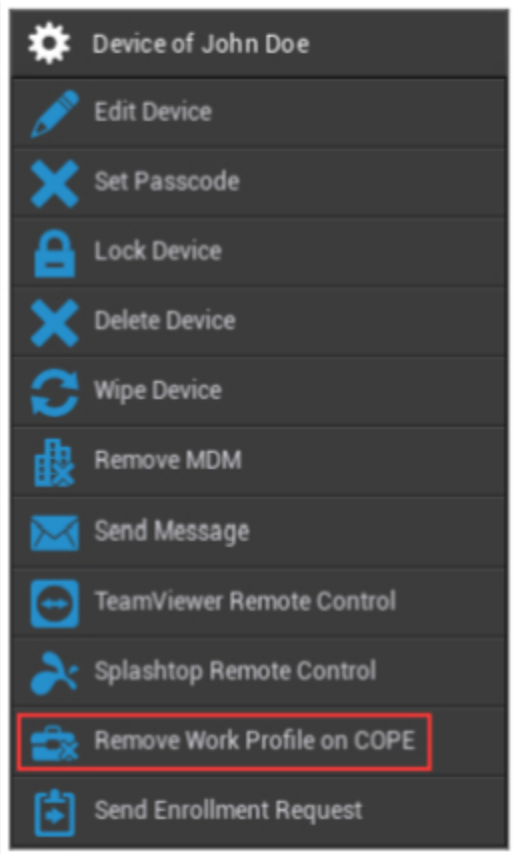
Тук можете да изпратите Push известие до съответното устройство на крайния потребител.

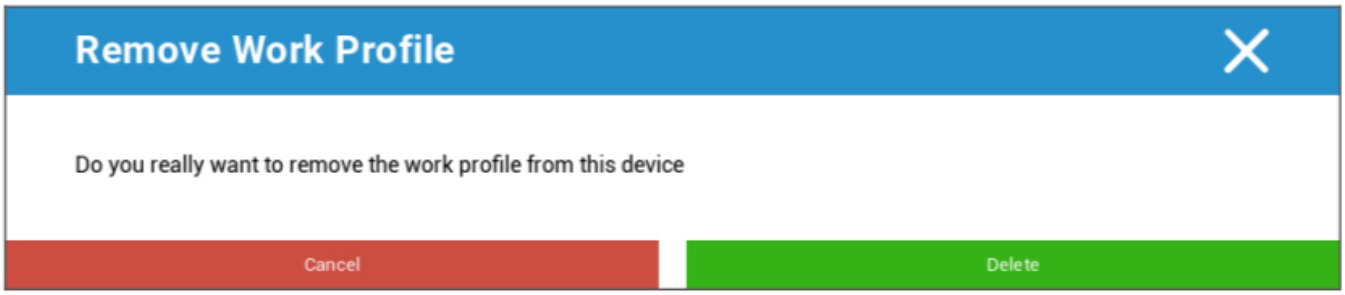
Трансформиране в режим COPE

Създаване на работен профил на това устройство с пълно управление на AE (управление на работата)



След като трансформирате устройството в режим COPE, можете да премахнете работния профил, като щракнете върху опцията **Премахване на работния профил в COPE**:




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

Изпращане на заявка за записване

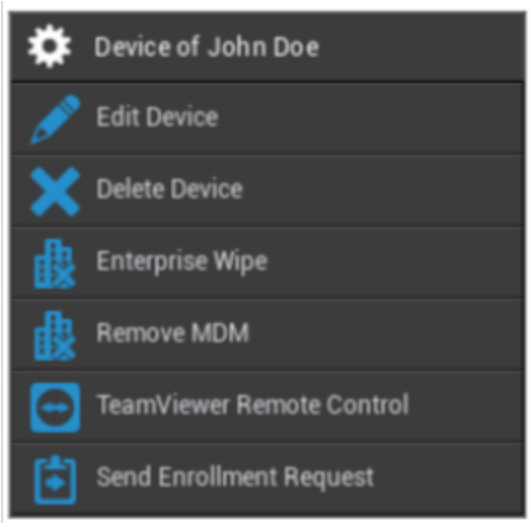
С "Изпращане на заявка за записване" можете да изпратите заявка за записване (отново) до съответния потребител.

Моля, обърнете внимание, че само най-новата заявка за записване е валидна.

Мигриране на наследеното устройство

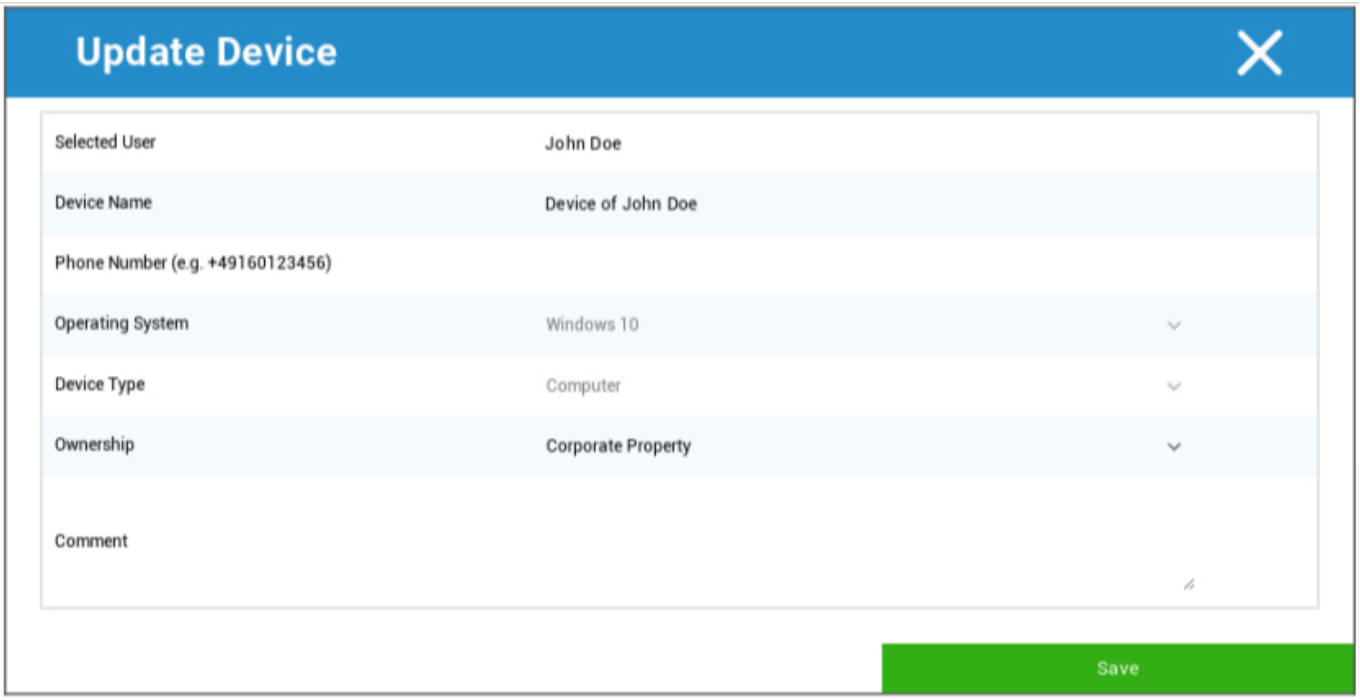
Мигриране на профил на телефон/таблет с Android към профил на напълно управлявано устройство (управлявано от работата) на AE

Windows



Име на устройството	Име на избраното устройство
Редактиране на устройство	Редактиране на устройство
Изтриване на устройство	Премахване на устройството от AppTec
Изтриване на предприятието	Информацията, приложенията и профилът, предоставени от AppTec360, се изтриват
Премахване на MDM	
Дистанционно управление на TeamViewer	Дистанционно управление на устройството с TeamViewer
Изпращане на заявка за записване	Изпращане на заявка за записване (отново)

Редактиране на устройство

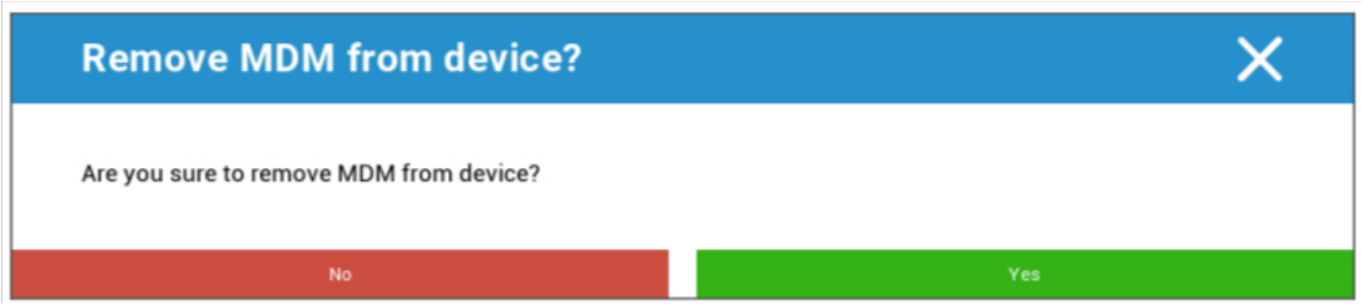


Тук можете да актуализирате разнообразна информация за устройството.

Изтриване на устройство

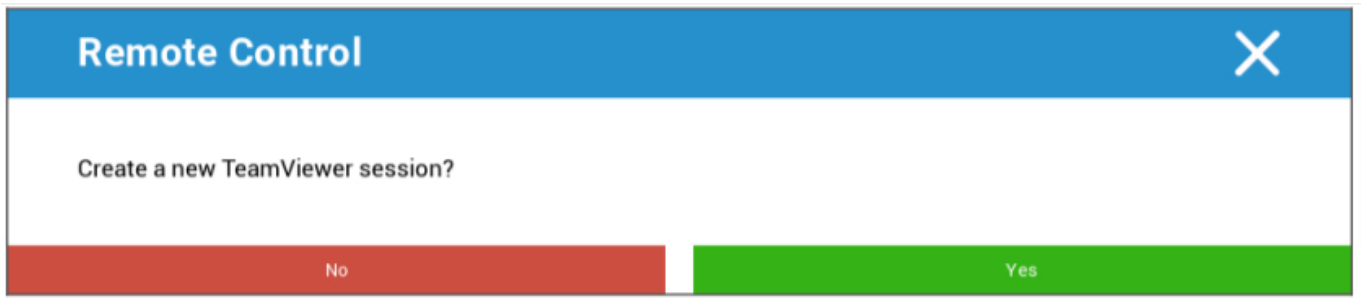
Тук може да се изпълни командата за изтриване, която само премахва устройството от AppTec360.

Изтриване на данни в предприятието | Премахване на MDM



Изтриват се само информацията, приложенията и профилите, предоставени от AppTec360. По този начин корпоративните данни вече няма да са достъпни на устройството на крайния потребител. Личната зона не е засегната и продължава да бъде на устройството на крайния потребител.

Дистанционно управление на TeamViewer



Тук можете да стартирате сесия за дистанционно управление TeamViewer за това устройство.

Изпращане на заявка за записване

С "Изпращане на заявка за записване" можете да изпратите заявка за записване (отново) до съответния потребител.

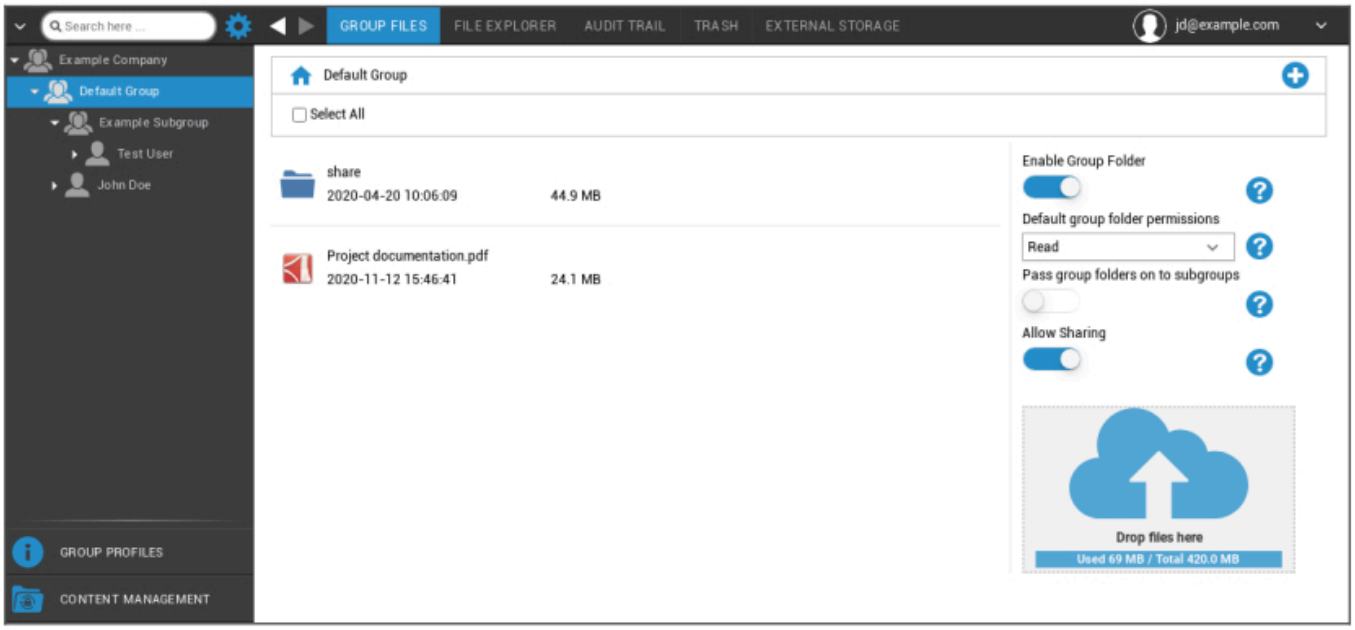
Управление на съдържанието

Когато сте в група, можете да управлявате ContentBox на AppTec с "Управление на съдържанието".

С помощта на Content Box можете безопасно да разпространявате документи и други корпоративни данни на устройствата на крайните потребители.

Групови файлове

"Групови файлове" представлява основна част от ContentBox. Тук можете да определяте настройки, да качвате документи, да създавате нови папки и т.н.



Със символа в горния десен ъгъл можете да създавате нови папки, които са определени за съответната група с "Добавяне на папка".

Със символа в горния десен ъгъл можете да създадете нова папка чрез "Добавяне на папка", която трябва да бъде присвоена към съответната група.

Можете да наречете папката по свой избор.

Чрез "Качване на файлове" можете да качвате данни. Тук ще се отвори вашият Standard-Explorer. Разбира се, можете да извършвате тези две действия във всяка (под)папка.

Със символа в горния ляв ъгъл можете да се върнете в главното меню.

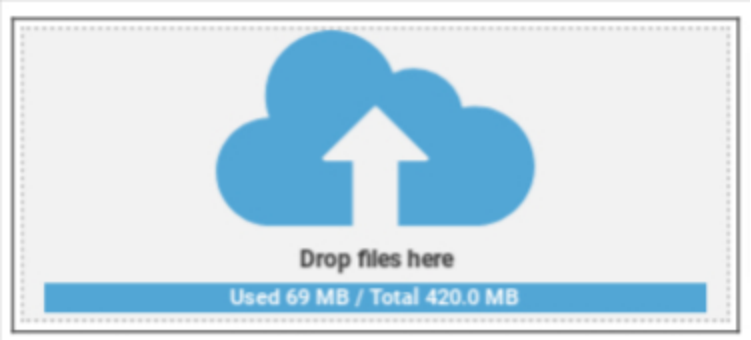
Можете да изберете няколко папки и файлове и да ги изтеглите с бутона "Изтегляне" или да ги изтриете, като щракнете върху "Изтриване".

Можете също така да изберете всички файлове и папки с и да изпълните командите "Изтегляне" и "Изтриване".

Когато преместите мишката върху папка или файл, ще видите следния преглед:

- С "Преименуване" можете да преименувате папката/файла.
- С "Изтегляне" можете да изтеглите папката/файла.
- С "Изтриване" можете да изтриете папката/файла.

Активиране на групова папка	Ако е активирано, всички членове на групата имат достъп до съответната папка.
Разрешения за групови папки по подразбиране	Разрешения на потребителите в избраната група: Read = разрешение само за четене Актуализация = разрешение за актуализация Създаване = разрешение за създаване Изтриване = разрешение за изтриване
Предаване на групови папки на подгрупи	Ако е активирано, съответните подгрупи могат да имат достъп до родителските файлове с данни.
Разрешения за подгрупи	Разрешения на потребителите в избраната подгрупа: Read = разрешение само за четене Актуализация = разрешение за актуализация Създаване = разрешение за създаване Изтриване = разрешение за изтриване
Разрешаване на споделянето	Ако е активирано, потребителят може да споделя файлове чрез връзка.



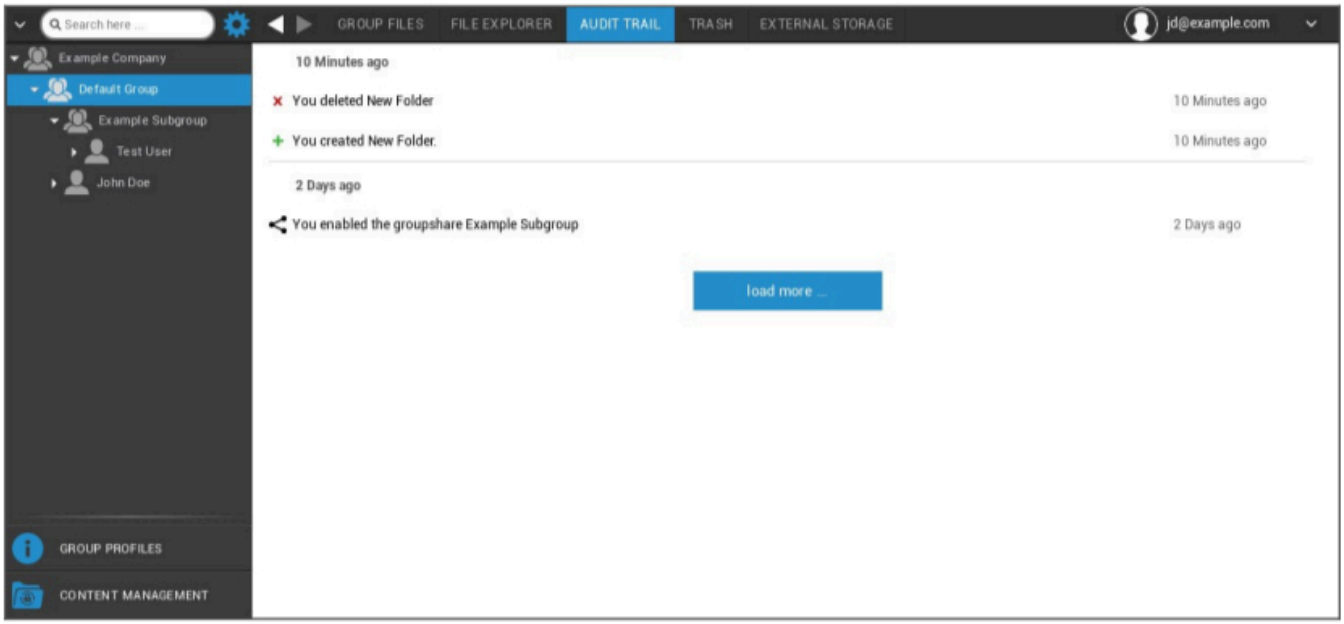
За да качвате файлове, можете да използвате това поле, като изтеглите файл чрез плъзгане и пускане в този прозорец. Можете също така да щракнете върху това поле, за да изберете и качите файл с помощта на Internet Explorer.

Изследовател на файлове

С "File Explorer" можете да управлявате всички папки и файлове, независимо от групата, в която са подадени.

Ще намерите също така настройките и бутоните, за които научихте в "Групови файлове".

Одитна следа



В "Audit Trail" можете да видите в историята кой потребител какво е създал, изтрил или споделил. По този начин можете да установите по всяко време какво е било направено с корпоративните данни.

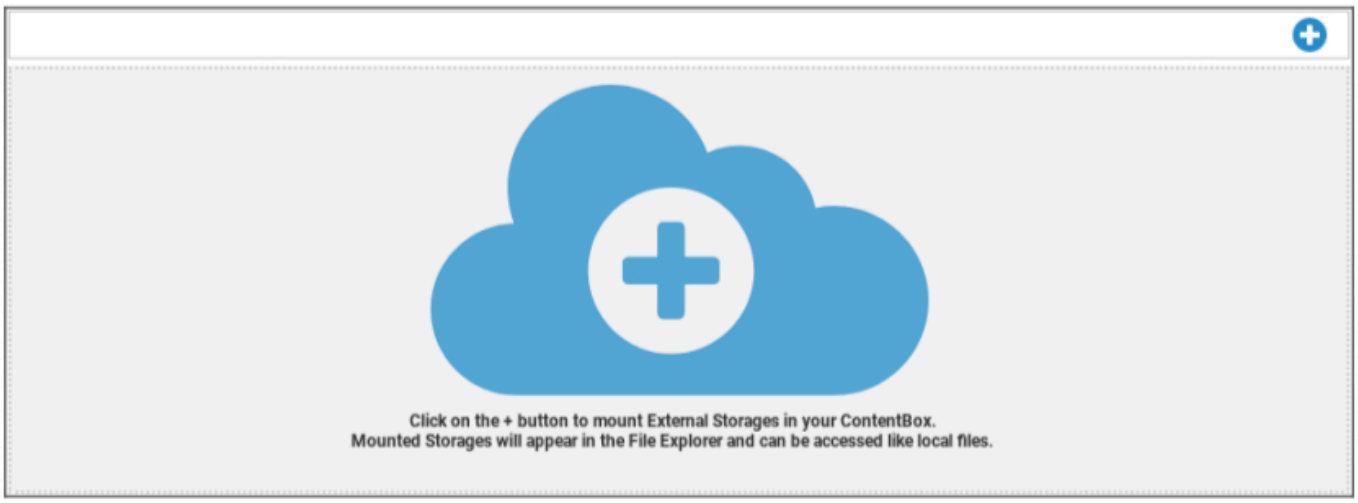
Отпадъци

Ако сте изтрили нещо (по невнимание), можете да видите папките и файловете в "Кошче" и да ги възстановите според желанието си.

- С "Undelete" можете да възстановите данните/папката.
- С "Изтриване" можете да изтриете окончателно данните/папката - трябва да потвърдите командата за изтриване още веднъж.

Моля, обърнете внимание, че капацитетът за съхранение, който се използва в кошчето, намалява наличното "Общо пространство" - това е изискване на ownCloud.

Външно съхранение



Под заглавието "Външно хранилище" можете да свържете външно хранилище.

Със символа може да се добави (допълнително) място за съхранение.

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

Amazon S3	
Име на дисплея	Показвайте името
Ключ за достъп	Ключ за достъп
Секретен ключ	Ключ за сигурност
Кофа	Определяне на идентичността на подпапката, която ви е била присвоена
Име на хост (по избор)	Име на хост (по избор)
Порт (по избор)	Порт (по избор)
Регион	Регион (по избор)
Активиране на SSL	Активиране на SSL
Разрешаване на стила на пътя	Изчистване на адреса на пътя, който ви е бил присвоен

FTP	
Име на дисплея	Показвайте името
Домакин	Адрес на хоста
Потребителско име	Потребителско име
Парола	Парола
Корен	Главно меню
Secure ftps://	

SFTP	
Име на дисплея	Показвайте името
Домакин	Адрес на хоста
Потребителско име	Потребителско име
Парола	Парола
Корен	Главно меню

ownCloud	
Име на дисплея	Показвайте името
URL	URL адрес на ownCloud
Потребителско име	Потребителско име
Парола	Парола
Отдалечен подпапка	Стандартна папка
Сигурно https://	

WebDAV	
Име на дисплея	Показвайте името
URL	URL адрес на WebDAV
Потребителско име	Потребителско име
Парола	Парола
Корен	Главно меню
Сигурно https://	
Споделяне на Windows	Поддръжката на Windows Share ще бъде налична скоро
SharePoint	Поддръжката на Microsoft SharePoint ще бъде налична скоро

Одитен дневник

Тук можете да намерите дневник, в който се записва информация за действията, извършени в конзолата MDM.

С помощта на иконата за филтър можете да прилагате филтри към показания списък.

С падащото меню **Items per page (Елементи на страница)**: можете да изберете броя на елементите, които да се показват на една страница на списъка.

Предприети действия / променени настройки	Предприетото действие / Променената настройка
Стойност	Стойността на предприетото действие/променената настройка
Потребител	Името на потребителя, който е предприел действието/ променил настройката
Дата	Времевата марка на предприемането на това действие/ промяната на тази настройка
Път / Тип	Пътят до мястото, където е извършено това действие / е променена тази настройка

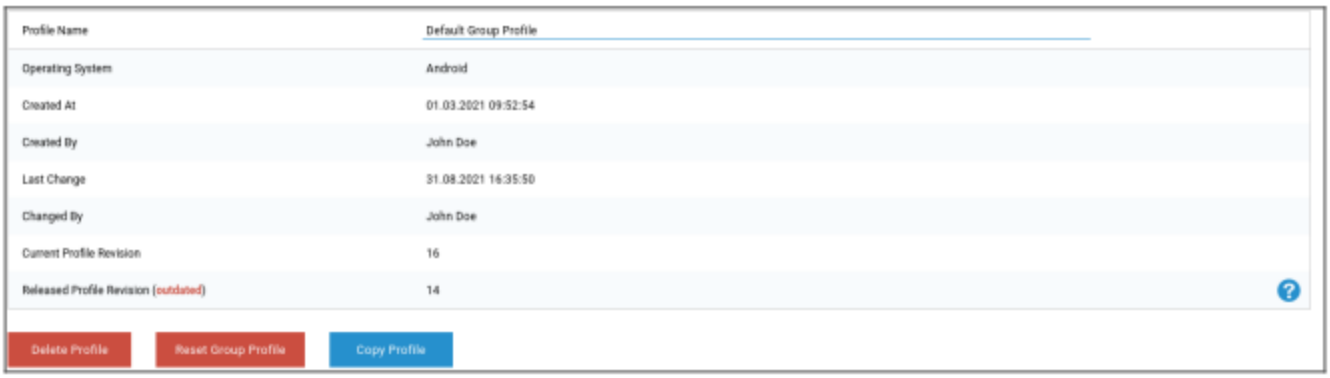
Конфигурация на iOS

Обща информация

В зависимост от това дали в момента сте избрали група или устройство, дисплеят и неговите подточки са различни - моля, обърнете внимание на това!

Преглед на профила на групата (само на ниво група)

При отваряне на групов профил ще получите бърз преглед на профила.



Име на профила	Име на профила (може да бъде променено тук)
Операционна система	Операционна система, за която е предназначен профилът
Създаден в	Време на създаване
Създаден от	Създател на профила
Последна промяна	Време на последната промяна в профила
Променено от	Акаунт, в който са направени последните промени
Текуща ревизия на профила	Преразглеждане на запазеното състояние на профила
Освободена ревизия на профила	Присвоена ревизия на профила ("Присвои сега"). Ако етикетът показва " (остарял)" зад текста, това означава, че сте запазили профила, но все още не сте го назначили, така че устройствата все още ще получават по-стара версия.

Обща информация

Ако се намирате директно в устройството, ще получите кратък преглед на избраното от вас устройство.

Име на устройството	Име на устройството
Телефонен номер	Телефонен номер на устройството
Модел	Номер на модела
Операционна система	OS
Сериен номер	Сериен номер на устройството
Притежание на устройство	Корпоративно или частно устройство Корпоративен = корпоративно устройство Служител = частно устройство
Тип устройство	Тип устройство (таблет или телефон)
Jailbroken	Ако на устройството има Jailbreak
Наблюдавана	Показва дали това е контролирано устройство.
Съответстващ	Ако са били нарушени някакви насоки
Последно видян	Състояние на последната комуникация на устройството със сървъра AppTec360

Настройки

Тези настройки съдържат името на устройството и предварително определен фон.

Име на устройството към името на системата	Името, което ще бъде издадено в конзолата AppTec360 (в лявата йерархична структура), ще бъде същото като на съответното устройство на крайния потребител (може да се види в настройките на устройството).
Използване на персонализиран тапет (само за контролирани устройства)	Тук можете предварително да дефинирате фона, който трябва да се показва на устройството на крайния потребител (например за корпоративно брандиране на устройството). Наличен е само в режим "Под наблюдение"!
Автоматични актуализации на операционната система	Налага актуализации на операционната система, ако са налични. Само за DEP устройства в контролиран режим.
Потребителски шрифтове	Тук можете да добавите персонализирани шрифтове.
Име	По избор. Името на шрифта, видимо за потребителя. Това поле се заменя с действителното име на шрифта след инсталирането му.
Шрифт	Качете файла с шрифта (.otf или .ttf).

Ревизия на конфигурацията

Тук ще получите преглед на това кой групов профил е определен за устройството.

Ако щракнете върху профила на групата, ще получите директен достъп до профила и ще можете да извършвате настройки.

Със символа можете да върнете зададените приложения към настройките на груповия профил.

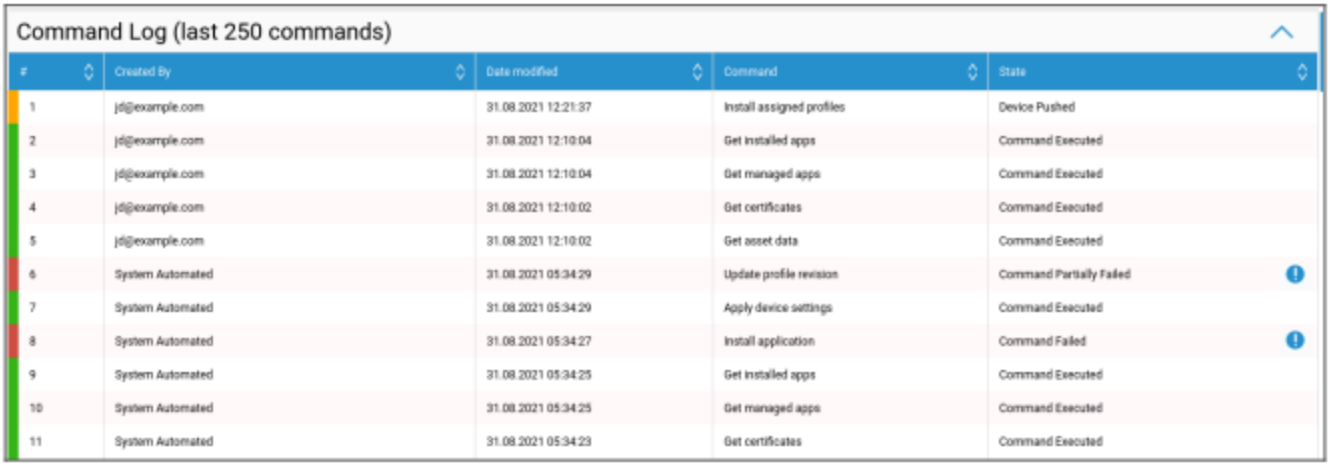
Със символа можете да нулирате профила на устройството, така че да няма никакви настройки.

"Налична е по-нова ревизия" показва, че профилът на групата е променен и запазен, но не е присвоен. Груповият профил трябва да бъде присвоен с "Assign now" (Присвояване сега) на ниво група, за да се приложат промените към устройствата.

Дневник на устройството (само на ниво устройство)

Дневник на командите

Тук можете да видите кои команди са издадени за устройството и какво е тяхното състояние.



Командите, създадени от "System Automated", се създават автоматично от системата.

Възможни състояния на командата

Натиснато устройство	Изпратена е заявка за натискане до услугата за натискане (напр. APNS), за да се каже на устройството да се свърже отново със сървъра на EMM.
Създадена команда	Командата е създадена в системата.
Изпратена команда	Командата е изпратена на устройството, след като то се е свързало със сървъра.
Изпълнена команда	Командата е изпълнена успешно.
Командата е неуспешна	Командата не е изпълнена. *
Командата е частично неуспешна	В зависимост от операционната система на устройството някои команди могат да бъдат групирани заедно. При това някои части от тази група команди не успяха. *
Командата е изпълнена, но в крайна сметка е неуспешна	Командата е изпълнена, но може би не е.
Пренасочване на командата	Командата е била изпратена отново от потребител.
Изхвърлени	Командата беше отхвърлена. Например защото е била заменена от друга команда или устройството е било презаписано и старите команди са били премахнати.

Ако зад съобщението има възклицателен знак, можете да получите повече информация, като задържите курсора върху иконата.

Управление на активи (само на ниво устройство)

Управление на активи (само на ниво устройство)

Информация за устройството

Модел	Номер на модела на устройството
Операционна система	OS
Версия на операционната система	Версия на операционната система
Сериен номер	Сериен номер
UDID	UDID на устройството
Име на устройството	Име на устройството
Наблюдавана	Показва дали устройството е под наблюдение
Състояние на батерията	Състояние на батерията

Wi-Fi

IP адрес	IP адрес на устройството
WiFi MAC	WiFi MAC адрес

Клетъчен

Статус	Състояние (наличие на SIM карта)
Телефонен номер	Телефонен номер
Състояние на роуминга	Текущо състояние на роуминга
Роуминг (глас/данни)	Статус на роуминг за глас/данни
IP адрес	IP адрес
IMEI	IMEI-номер
Оператор/превозвач	Доставчик на клетъчни услуги
Мрежа на оператора на SIM	Мрежа на оператора на SIM
Версия на носителя	Версия на носителя
Фърмуер на модема	Вграден софтуер на модема
Текущи MCC/MNC	Вижте "SIM MCC/MNC".
SIM MCC/MNC	Кодът на мобилната мрежа е установена от ITU идентификация на страната съгласно стандарт E.212, която в комбинация с кода на мобилната мрежа (MNC) се използва за идентифициране на клетъчна мрежа (=код на страната). Когато влезете в друга клетъчна мрежа, "Current MCC/MNC" и "SIM MCC/MNC" са различни.

Bluetooth

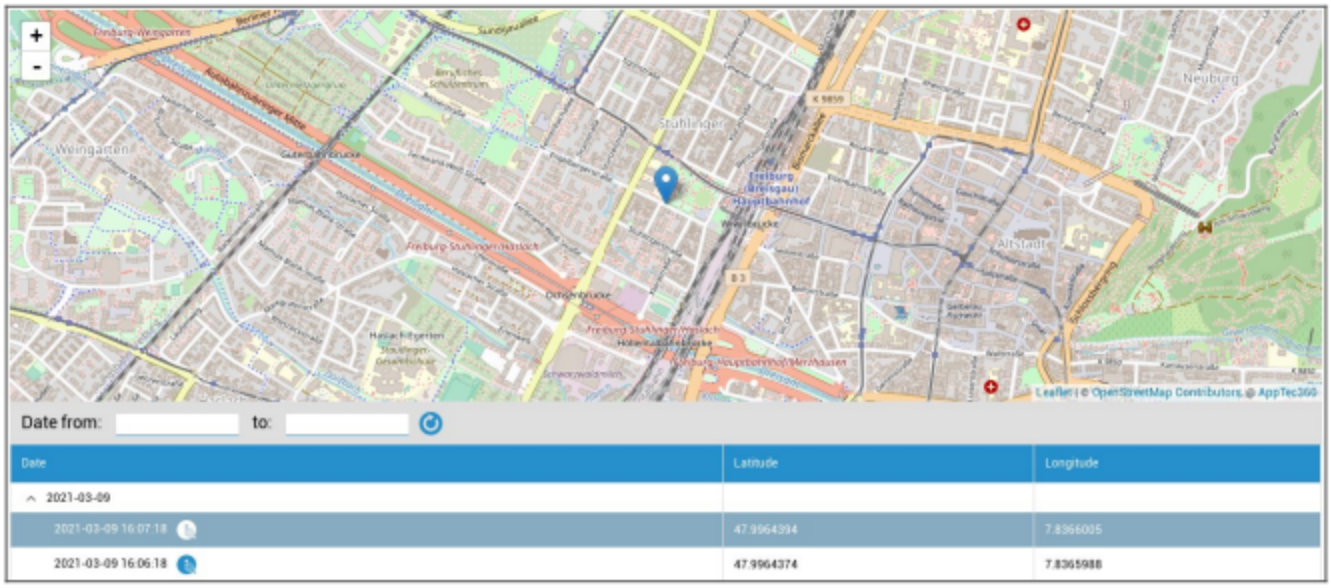
Bluetooth MAC	Bluetooth MAC адрес

Управление на сигурността

Защита от кражба (само на ниво устройство)

GPS информация (само на ниво устройство)

Тук можете да определите текущото/последното местоположение на устройството. Локализирането може да бъде защитено с една или дори с две пароли - вж: Общи настройки - Поверителност - Достъп до GPS



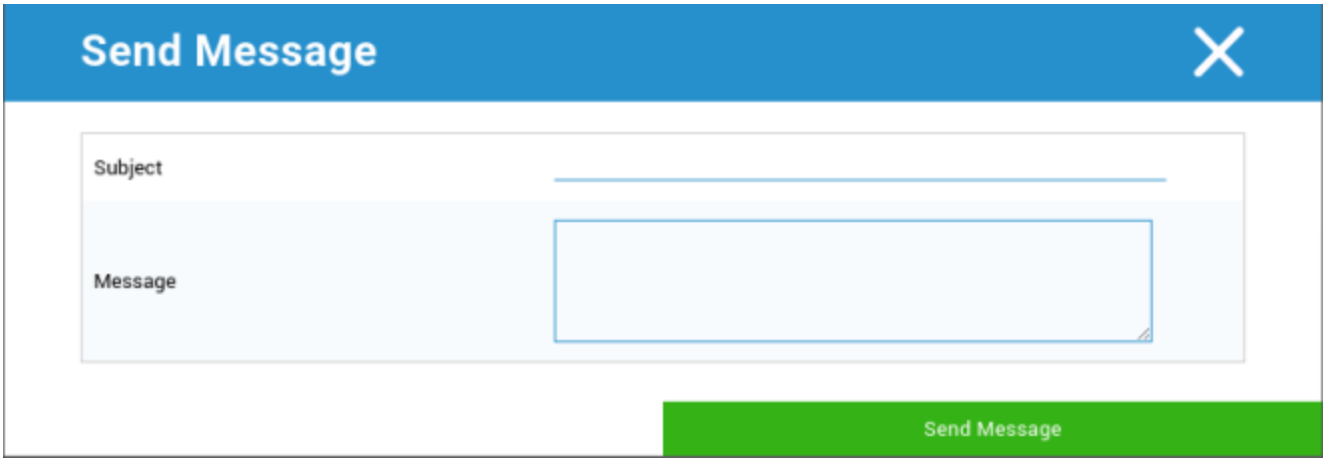
Изтриване и заключване (само на ниво устройство)

В "Изтриване и заключване" можете да извършите следните три действия:

Пълно избърсване	Устройството се възстановява до фабричните си настройки (корпоративните и личните данни се изтриват).
Изтриване на предприятието	От устройството на крайния потребител се премахват само корпоративните данни (всички приложения, данни и т.н., които са били предоставени от AppTec)
Екран за заключване	Активирано е заключване на екрана, достатъчно е да отключите устройството с паролата на устройството/ ПИН кода.
Съдебно блокиране (само за контролирани устройства)	Ако тази функция бъде активирана със символа  , устройството ще бъде заключено, като се покаже съобщение, което не може да бъде затворено. Служителят също така не може да отключи устройството. Само администраторът може да отключи устройството в конзолата със символа за отключване  .
Разрешаване на заключването за активиране (само за контролирани устройства)	Ако тази функция бъде активирана , устройството ще бъде заключено, веднага щом "Find my iPhone" бъде активирана в настройките на iCloud.

Съобщение (само на ниво устройство)

В следващия прозорец можете да попълните темата и съобщението и да го изпратите на крайно потребителско устройство:



Конфигурация на сигурността

Парола

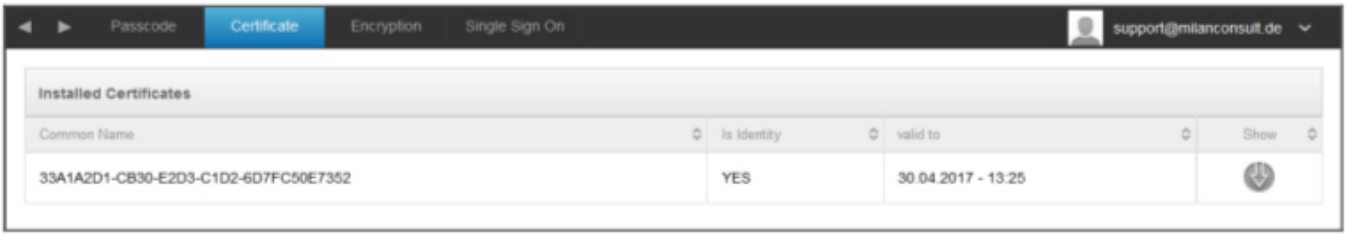
Тук се определят настройките за паролата на устройството

Разрешено е деактивиране на кода	Когато тази настройка е активирана, няма подкана за въвеждане на парола. Веднага щом паролата е установена, тя не може да бъде деактивирана.
Позволете проста стойност	Позволете на потребителя да използва еднакви, ескалиращи и редуциращи се поредици от номера (например 1234, 1111)
Изискване за буквено-цифрова стойност	Паролите трябва да съдържат поне една буква.
Минимална дължина на кода за достъп	Минимална дължина на паролата
Минимален брой сложни символи	Минимален брой буквено-цифрови символи в паролата
Максимална възраст на кода за достъп	Брой дни, след които паролата трябва да бъде променена
Максимално автоматично заключване	Максимално време, след което устройството се заключва
Максимален гратисен период за заключване на устройството	време, след което устройството преминава в заключен режим Stand-By
Максимален брой неуспешни опити	Установява колко често паролата може да бъде въведена неправилно, преди да се извърши пълно изтриване на устройството.
Максимална възраст на кода за достъп (1-730 дни)	Максимална възраст на паролата
История на паролите (1-50 пароли)	Използването на стара парола е разрешено след този номер.

Щракване върху кошчето отваря диалоговия прозорец за възстановяване на паролата, с който може да се изтрие забравена парола на устройството.

Сертификат (само на ниво устройство)

Показва сертификатите, които са налични в устройството



Криптиране

Изискване за криптиране на съхранението	Активиране на функцията за криптиране на инсталираното устройство

Еднократно влизане в системата

В точката "Single Sign-On" можете да конфигурирате удостоверяването с Kerberos.

Тук установявате данните за достъп и съответните URL адреси/приложения, на които е разрешено да използват токените Kerberos.

Наличен в режим на наблюдение	
Име на сметката	Име на сметката
Основно име	Уникална идентичност, към която могат да се разпространяват билети Kerberos
Realm	Вашият Kerberos Realm, който трябва да се използва (например вашият домейн)

Със символа можете да създадете допълнителни URL адреси.

Модел на URL, използван за ограничаване на този акаунт	Да се определят URL адресите, до които могат да се разпространяват билети Kerberos

Със символа можете да създадете допълнителни приложения.

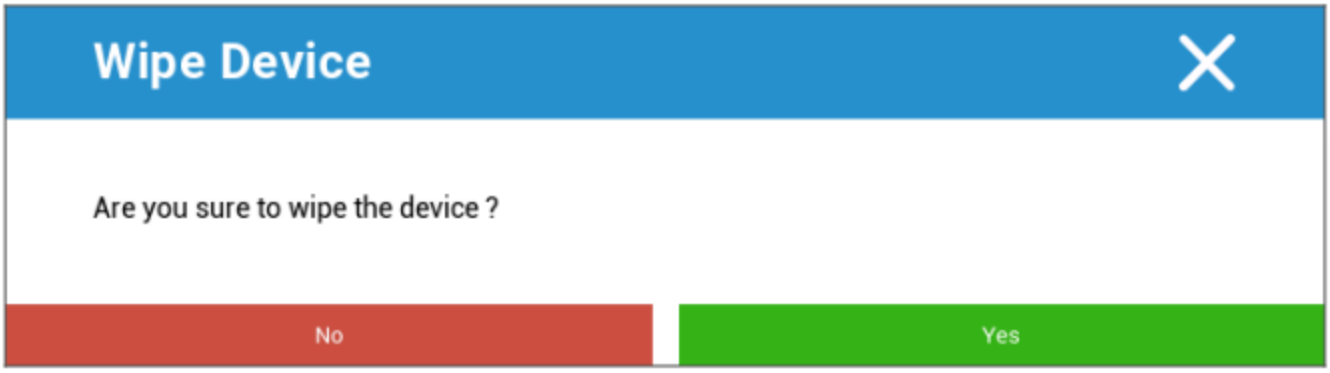
Приложения за ограничаване на този акаунт	Предстои да се определи Приложения, към които могат да се разпространяват билети Kerberos

Край на живота (само на ниво устройство)

Избърсване (само на ниво устройство)

Под "Изтриване" можете да възстановите фабричните настройки на устройството. Тук корпоративните, както и личните данни ще бъдат изтрити от устройството на крайния потребител.

След като кликнете върху символа "минус", трябва да получите следното съобщение



С "Да" можете да извършите изтриването.

Под "Отчет за изтриване" могат да бъдат показани следните елементи

Изтрити от	История на лицето, извършило изтриването
Дата	Дата
Статус	Статус (например дали изтриването е извършено успешно)

Настройки на ограниченията

Функционалност на устройството

Тук можете да блокирате отделни функционалности на устройствата на крайните потребители.

Разрешаване на инсталирането на приложения	Разрешаване на инсталирането на приложения
Разрешаване на камерата	Разрешаване на използването на камерата
Разрешаване на FaceTime	Разрешаване на FaceTime
Позволете заснемане на екрана	Позволете заснемане на екрана
Разрешаване на автоматична синхронизация при роуминг	Разрешаване на автоматична синхронизация при роуминг
Разрешаване на Siri	Разрешаване на Siri
Разрешаване на гласово набиране	Разрешаване на гласово набиране
Разрешаване на покупка в приложението	Разрешаване на покупка в приложението
Изискване на парола за iTunes Store за всички покупки	Изискване на парола за iTunes Store за всички покупки
Разрешаване на мултиплейър игри	Разрешаване на мултиплейър игри
Разрешаване на добавянето на приятели в Game Center	Разрешаване на добавянето на приятели в Game Center
Разрешаване на отваряне от управлявано към неуправлявано	Разрешаване на отварянето на съдържание от управлявани приложения в неуправлявани приложения
Разрешаване на отваряне от неуправляван към управляван	Разрешаване на отварянето на съдържание от неуправлявани приложения в управлявани приложения
Разрешаване на изгледа днес в заключения екран	Когато тази настройка е активна, изгледът "Днес" ще се показва в Центъра за известия на заключения екран.
Разрешаване на контролния център в заключения екран	Разрешаване на Центъра за управление на заключения екран
Разрешаване на TouchID	Разрешаване на TouchID
Разрешаване на актуализации на PKI по въздуха	Разрешаване на актуализации на PKI по въздуха

Разрешаване на пасбук, когато е заключен	Разрешаване на passbook, докато устройството е заключено
Ограничаване на проследяването на реклами	Тази функция деактивира проследяването на реклами (например рекламодателите не могат да използват проследяване на реклами, за да разпространяват персонализирани реклами).
Разрешаване на предаването	Разрешаване на предаването
Разрешаване на интернет резултати в светлината на прожекторите	Разрешаване на интернет резултати в светлината на прожекторите (например Bing или Wikipedia)
Изискване на парола при първото сдвояване с AirPlay	Изискване на парола при първото сдвояване с AirPlay
Защита на китката на часовника Force	Ако е активиран, Apple Watch е принуден да използва "Защита на китката" (разпознаване на китката).
Разрешаване на iCloud Photo Library	Позволява използването на iCloud Photo Library. Ако не е разрешено, всички снимки, които не са изтеглени напълно от iCloud, ще бъдат изтрити от локалното хранилище.
Налично в режим на наблюдение	
Разрешаване на модифицирането на акаунта	Разрешаване на модификацията "поща, контакти, календар"
Разрешаване на AirDrop	Разрешаване на AirDrop
Разрешаване на клетъчната модификация на приложението	Тази настройка блокира настройката за това на кои приложения е разрешено да използват мобилни данни. Тази настройка може например да се зададе ръчно на крайното потребителско устройство и след това това ограничението да се активира.
Позволете на Siri да прави заявки за съдържание, създадено от потребителите, от уеб	Уеб търсенето в определени уебсайтове е блокирано, например в Уикипедия, защото всеки може да прави промени, както си иска.
Активиране на филтъра за нецензурни изрази в Siri	Нецензурните изрази, които са насочени към Siri, се цензурират
Разрешаване на iBook Store	Разрешаване на iBook Store
Разрешаване на iBook Store Еротика	Разрешаване на iBook Store Еротика

Разрешаване на промяна на настройките на Find my Friends	Разрешаване на промяна на настройките на Find my Friends
Разрешаване на Game Center	Разрешаване на Game Center
Разрешаване на сдвояването на хостове	Сдвояване на контролния компютър
Разрешаване на инсталирането на профили на конфигурацията	Разрешаване на инсталирането на конфигурационни профили
Разрешаване на премахването на приложението	Премахване на приложения за контрол
Разрешаване на iMessage	Разрешаване на iMessage
Позволете изтриване на цялото съдържание и настройки	Позволява изтриване на цялото съдържание и настройки
Позволява конфигуриране на ограничения	Позволява конфигуриране на ограничения
Позволете подкаст	Позволете подкаст
Разрешаване на търсенето на дефиниции	Разрешаване на търсенето на дефиниции
Разрешаване на предсказваща клавиатура	Разрешаване на предсказваща клавиатура
Разрешаване на автоматична корекция	Разрешаване на автоматична корекция
Разрешаване на инсталирането на приложения на потребителския интерфейс	Ако е деактивирана, не могат да се инсталират приложения от публичния AppStore (иконата вече няма да се показва). Въпреки това приложенията все още могат да се инсталират чрез iTunes и Configurator
Разрешаване на бързи клавишни комбинации	Разрешаване на преки пътища от клавиатурата, ако устройството е свързано с физическа клавиатура
Разрешаване на сдвояването на Apple Watch	Забранява сдвояването между устройството и Apple Watch, като съществуващите връзки ще бъдат прекратени
Разрешаване на модификацията на паролата	Ако не е разрешено, не може да се добавя, променя или премахва парола на устройство.
Разрешаване на модификацията на името на устройството	Насоки за определяне дали името на устройството може да бъде променено
Позволете промяна на тапета	Насоки за определяне дали тапетът може да бъде сменен

Разрешаване на автоматичното изтегляне на приложения	Ако е деактивирано, закупеното приложение няма да се инсталира автоматично на други устройства. Не се отнася за актуализации за съществуващи приложения
Позволете новини	Разрешаване на новини в устройството с iOS
Разрешаване на доверието на приложението Enterprise	Ако е зададена стойност false, се предотвратява доверяването на корпоративни приложения

iCloud

Блокиране на определени функционалности по време на сдвояване с iCloud

Разрешаване на архивирането	Разрешаване на архивирането
Разрешаване на синхронизирането на документи	Разрешаване на синхронизирането на документи
Разрешаване на потока от снимки	Разрешаване на потока от снимки
Разрешаване на споделен поток от снимки	Разрешаване на споделен поток от снимки
Разрешаване на синхронизирането на ключодържателя в облака	Разрешаване на синхронизирането на ключодържателя в облака
Разрешаване на управляваните приложения да съхраняват данни	Разрешаване на управляваните приложения да съхраняват данни
Разрешаване на синхронизирането на бележки и акценти за книги на предприятието	Разрешаване на синхронизирането на бележки и акценти за книги на предприятието
Позволете архивиране на книгите на предприятието	Позволете архивиране на книгите на предприятието

Сигурност и поверителност

Блокиране на тези функционалности, свързани с диагностични данни

Разрешаване на изпращането на диагностични данни към Apple	Разрешаване на изпращането на диагностични данни към Apple
Разрешаване на потребителя да приема ненадеждни TLS сертификати	Разрешаване на потребителя да приема ненадеждни TLS сертификати
Налагане на криптирани резервни копия	Налагане на криптирани резервни копия

BYOD

Вградена защита на iOS (контейнер)

iOS винаги е можела да прави разлика между управляван (бизнес) и неуправляван (частен). Всичко, което идва от системата MDM, се третира като управлявано. Например, ако инсталирате приложение чрез MDM или конфигурирате Exchange акаунт, това ще се третира като управлявано от iOS.

Всичко останало, което се конфигурира/инсталира ръчно в устройството, ще се разглежда като неуправляемо. Например, ако потребителят инсталира WhatsApp сам или ако добавя Exchange акаунт. Това разделяне обаче никога не е засягало контактите. Но от iOS 11.3 (и по-нови версии) това беше добавено и за контактите.

Тъй като това е основна функционалност на операционната система, не е необходимо да инсталирате нещо или да настройвате специален контейнер.

Активирайте вградената функция, за да разделите личните и служебните приложения/информация/файлове. Тази настройка ще деактивира и някои други функции, които в противен случай биха могли да изключат части от това разделяне по погрешка.

Активиране

Активиране на контейнерните решения, които се поддържат от AppTec360

Активиране на контейнера Google Divide	Активиране на контейнера Google Divide
Активиране на SecurePIM контейнер	Активиране на SecurePIM контейнер

Ако сте активирали SecurePIM Container, в раздел "Активиране" ще намерите и следната точка. Освен това веднага ще се отворят още четири раздела, които са описани по-долу.

Имейл адрес за поддръжка	Имейл адрес за поддръжка, на който потребителят може да се обърне при проблеми

SecurePIM Парола

В "SecurePIM Password" можете да зададете насоки за силата на защита на паролата.

Време на сесията	Тук можете да определите след колко минути трябва да се въведе отново нова парола, след като SecurePIM работи във фонов режим.
Дължина на паролата	Дължина на паролата за достъп до SecurePIM Container
Големи букви	Минимален брой главни букви
Символи с малки букви	Минимален брой малки букви
Специални символи	Минимален брой специални символи
Цифри	Минимални цифри
Приложение за избърсване	Брой пъти, в които паролата може да бъде въведена неправилно, преди съдържанието на SecurePIM да бъде изтрито (Приложението обаче остава на устройството на крайния потребител)

SecurePIM Сигурност

В "SecurePIM Security" можете да зададете различни настройки за сигурност.

Откриване на устройства с взлом	Ако тази настройка е активирана, достъпът до SecurePIM Container ще бъде блокиран, веднага щом устройството бъде разпознато като джейлбрейкнато.
Защитени текстови полета	Съдържанието на полетата за подаване на данни ще бъде криптирано, никаква информация няма да достига до операционната система (iOS) Забележка: Докато тази настройка е активна, автоматичната корекция вече не е налична.
Експортиране на данни за контакти в устройство	Ако тази настройка е активирана, на потребителя се разрешава да експортира контактите от Exchange на своето локално устройство. Забележка: Експортират се само името и телефонният номер.
Местоположение на събитието	Ако тази настройка е активирана, местоположението на предстоящите събития ще се показва в лентата за известия.
Покажи заглавието на събитието	Ако тази настройка е активирана, местоположението на заглавието на предстоящото събитие ще се показва в лентата за известия.

Браузър SecurePIM

Тук можете да конфигурирате браузъра на SecurePIM.

Със символа можете да дефинирате нов URL адрес.

Със символа можете отново да премахнете определен URL адрес.

"URL адреси в белия списък" са URL адреси, които могат да бъдат зареждани.

"URL адреси в черния списък" са URL адреси, които не могат да бъдат заредени и по този начин са блокирани.

Имайте предвид, че записите в белия списък са с по-висок приоритет от записите в черния списък. Под "Bookmark Title" (Заглавие на отметките) можете да зададете заглавие. С "Bookmark URL" можете да свържете URL адрес със заглавието на отметките - по този начин можете да разпространявате индивидуализирани отметки на съответните потребители.

Обмен

В "Exchange" можете да конфигурирате акаунт в Exchange.

Имейл адрес на ActiveSync	Имейл адрес за обмен (обърнете внимание на "Заместващи символи")
Влизане в Exchange ActiveSync	Потребителски имена за обмен (обърнете внимание на "Заместващи символи")
ActiveSync Exchange Server	Адрес на сървъра на Exchange (FQDN)
ActiveSync Exchange домейн	Адрес на домейна на Exchange
Сертификат на потребителя	Сертификат на потребителя
Удостоверяване въз основа на сертификат	Потребителят се удостоверява с помощта на сертификат
Разрешаване на криптирането на S/MIME	Позволява на потребителя да криптира своята поща
Разрешаване на подписването с S/MIME	Позволява на потребителя да подпише своята поща
Проверка на CRL	Ако е активен, частният сертификат ще бъде сравнен с CRL (Certificate Revocation List).

Управление на връзките

Wi-Fi

Идентификатор на набора от услуги (SSID)	SSID на мрежата, която трябва да се свърже
Автоматично присъединяване	Активиране на автоматично присъединяване при присъединяване към мрежа
Скрита мрежа	Активиране, в случай че AP не излъчва SSID

Настройка на прокси сървъра

Конфигуриране на прокси за всяка точка за достъп

Няма	Установяване без пълномощно
Ръководство	Създаване на ръчно прокси
URL адрес на прокси сървър	Адрес за достъп до настройките на прокси сървъра
Пристанище	Установяване на порта за прокси сървъра
Удостоверяване	Потребителско име за удостоверяване в прокси сървъра
Парола	Парола за удостоверяване в прокси сървъра
Автоматичен	Създаване на прокси автоматично
URL адрес на прокси сървър	URL адрес за достъп до настройките на прокси сървъра

Вид сигурност

Установяване на тип сигурност за AP

WEP	
Парола	Парола за AP

WPA/WPA2	
Парола	Парола за AP

WEP Enterprise - WPA / WPA2 Enterprise - Any Enterprise			
	Протоколи		
	TLS	Активиране/деактивиране	
	TTLS	Активиране/деактивиране	
	LEAP	Активиране/деактивиране	
	PEAP	Активиране/деактивиране	
	EAP-FAST	Активиране/деактивиране	
	EAP-SIM	Активиране/деактивиране	
	Използване на PAC		Използване на PAC (Protected Access Controll)
	Осигуряване на PAC	Конфигуриране на Provision PAC	
	Анонимно предоставяне на PAC	Анонимно предоставяне на PAC	
	Вътрешни удостоверявания	Протокол за удостоверяване, който трябва да се използва: PAP, CHAP, MSCHAP, MSCHAPv2	
	Потребителско име	Потребителско име за удостоверяване	
	Не използвайте парола за свързване	Не използвайте парола за свързване	
	Сертификат за самоличност	Качване/избор на сертификат за удостоверяване	
	Външна идентичност	Идентичност, която може да се види отвън	
	Trust		
	Доверен сертификат 1	Качване на първия доверен сертификат	
	Доверен сертификат 2	Качване на втори доверен сертификат	
	Доверен сертификат 3	Качване на трети доверен сертификат	
	Имена на сертификати на доверени сървъри	Имената на очакваните сървърни сертификати	

		(в списък, разделен със запетая)	

Няма	Не установявайте сигурност

VPN

Име на връзката	Име на VPN-профила

Тип VPN

VPN

Целият мрежов трафик на устройството ще бъде пренасочен чрез VPN-връзка.

Тип на връзката	Установяване на тип VPN-връзка
IPsec (cisco)	Протокол IPsec от cisco
PPTP	Протокол PPTP
L2TP	Протокол L2TP
Cisco AnyConnect	Протокол AnyConnect
Juniper SSL	SSL протокол на Juniper
F5 SSL	SSL протокол на F5
SonicWall mConnect	SonicWall mobile Connect
Аруба VIA	Протокол Aruba VIA
Потребителски SSL	Връзка чрез потребителски SSL
OpenVPN	Протокол OpenVPN

VPN за всяко приложение

При отваряне на дадено приложение ще бъде установена VPN връзка.

Автоматично стартиране на VPN връзка за всяко приложение		Автоматично стартиране на VPN връзка за всяко приложение
Тип на връзката		Установяване на тип VPN-връзка
	Cisco AnyConnect	Протокол AnyConnect
	Juniper SSL	SSL протокол на Juniper
	F5 SSL	SSL протокол на F5
	SonicWall mConnect	SonicWall mobile Connect
	Аруба VIA	Протокол Aruba VIA
	Потребителски SSL	Връзка чрез потребителски SSL
	OpenVPN	Протокол OpenVPN

Настройка на прокси сървъра

Конфигуриране на прокси сървър за VPN-връзката

Няма	Установяване без пълномощно
Ръководство	Ръчно създаване на прокси
URL адрес на прокси сървър	Адрес за достъп до настройките на прокси сървъра
Пристанище	Установяване на порта за прокси сървъра
Удостоверяване	Потребителско име за удостоверяване в прокси сървъра
Парола	Парола за удостоверяване в прокси сървъра
Автоматичен	Създаване на прокси автоматично
URL адрес на прокси сървър	URL адрес за достъп до настройките на прокси сървъра

Показване на заместители	Показва всички налични потребителски променливи , които AppTec360 може да използва

APN

Име на точката за достъп	Име на точката за достъп
Потребителско име на точката за достъп	Потребителско име на точката за достъп
Парола на точката за достъп	Парола на точката за достъп
Прокси сървър	Адрес на прокси сървър
Пристанище	Съответният порт на прокси сървъра

Клетъчен

Активиране на роуминг на данни	Активиране на роуминг на данни
Активиране на гласовия роуминг	Активиране на гласовия роуминг
Активиране на гореща точка	Активиране на гореща точка

HTTP прокси

Тип прокси	
Ръководство	Създаване на прокси ръчно
URL адрес на прокси сървър	Адрес за достъп до настройките на прокси сървъра
Пристанище	Създаване на прокси порт
Удостоверяване	Потребителско име за удостоверяване в прокси сървъра
Парола	Парола за удостоверяване в прокси сървъра
Автоматичен	Създаване на прокси автоматично
URL адрес на прокси PAC	URL адрес на прокси PAC
Разрешаване на директна връзка, ако PAC е недостъпен	Разрешаване на директна връзка (без VPN), ако PAC е недостъпен
Позволява заобикаляне на прокси сървъра за достъп до затворени мрежи	Позволяване на заобикаляне на прокси сървъра за достъп до вътрешни мрежи

AirPrint

IP адрес	IP адрес на принтера
Път на ресурсите	Определен път до устройството AirPrint

AirPlay

Име на устройството	Име на устройството
Парола	Парола за сдвояване
Бял списък	Дефиниране на списък с устройства, с които устройството може да се свързва изключително

Управление на PIM

Exchange Active Sync

Име на сметката	Име на имейл акаунт
Exchange ActiveSync Host	Адрес/FQDN на сървъра
Разрешаване на преместването	Позволете преместването на имейли
Използвайте само в пощата	Взаимодействията могат да се осъществяват само в родното приложение Mail
Използване на SSL	Използване на SSL криптиране
Домейн	Домейн на сървъра
Потребител	Потребителско име
Електронен адрес	имейл адрес (само на ниво устройство)
Парола (само на ниво устройство)	Потребителска парола
Сертификат за самоличност	Изберете съответния сертификат за удостоверяване в сървъра
Минали дни на Mail to Sync	Брой дни, до които имейлите трябва да бъдат синхронизирани обратно. No Limit = неограничен
Активиране на S/MIME	Активиране на криптирането S/MIME
Сертификат за подписване	Качване на съответния сертификат за подписване
Сертификат за криптиране	Качване на съответния сертификат за криптиране

Електронна поща

Създаване на акаунти POP3 / IMAP на крайното потребителско устройство

Описание на сметката	Име des Имейл акаунти		
Тип на сметката	IMAP	Префикс на пътя	Префиксът на пътя за специални папки
	POP		
Потребителско име на дисплея	Потребителско име на дисплея		
Имейл адрес	Имейл адрес на потребителя		
Разрешаване на преместването	Позволете преместването на имейли		
Активиране на S/MIME	Активиране на криптирането S/MIME		
Сертификат за подписване	Качване на съответния сертификат за подписване		
Сертификат за криптиране	Качване на съответния сертификат за криптиране		

Входяща поща

Настройки на входящия сървър

Адрес на пощенския сървър	Адрес на пощенския сървър
Порт на пощенския сървър	Порт на пощенския сървър
Потребителско име	Съответно потребителско име
Тип удостоверяване	Тип удостоверяване
Няма	Не Тип удостоверяване
Парола (само на ниво устройство)	Запитване за парола
MDM предизвикателство-отговор	
NTLM	Удостоверяване на NTLM
HTTP MD5 Digest	
Използване на SSL	Използвайте SSL, ако е необходимо

Изходяща поща

Настройки на изходящия сървър

Адрес на пощенския сървър	Адрес на пощенския сървър
Порт на пощенския сървър	Порт на пощенския сървър
Потребителско име	Съответно потребителско име
Тип удостоверяване	
Няма	Няма метод за удостоверяване
Парола (само на ниво устройство)	Запитване за парола
MDM предизвикателство-отговор	
NTLM	Удостоверяване на NTLM
HTTP MD5 Digest	
Използване на SSL	Използвайте SSL, ако е необходимо
Изходящата парола е същата като входящата	Изходящата парола е същата като входящата
Използвайте само в пощата	Активирайте, ако всички изходящи имейли трябва да се изпращат чрез приложението Mail-App.

CalDav

Конфигуриране на настройката и разпространението на акаунт в CalDav

Описание на сметката	Име на профила
Име на хоста	Име на хост и/или IP адрес
Пристанище	Пристанище на акаунта в CalDav
Основен URL адрес	Основен URL адрес на сметката
Потребителско име	Съответно потребителско име на CalDav
Парола (само на ниво устройство)	Съответна парола за CalDav
Използване на SSL	Използвайте SSL, ако е необходимо

Абонирани календари

Създаване и разпространение на абонирани календари

Описание	Име на профила
URL	URL на базата данни на календара
Потребителско име	Потребителско име на абонамента за календара
Парола (само на ниво устройство)	Парола на абонамента за календара
Използване на SSL	Използвайте SSL, ако е необходимо

LDAP

В тази област настройте LDAP-връзка, за да позволите динамичен обмен на сертификати между крайното потребителско устройство и Active Directory.

Моля, обърнете внимание, че избраният потребител изисква съответното разрешение за четене.

Описание на сметката	Описание на сметката
Потребителско име на акаунта	Потребител за LDAP-достъп
Парола на акаунта	Парола за LDAP-достъп
Име на хоста на акаунта	Име на хоста/IP адрес на сървъра LDAP
Използване на SSL	Използвайте SSL, ако е необходимо

Във втората част можете да дефинирате индивидуални филтри за търсене в регистъра LDAP.

Описание	Обхват	База за търсене
Описание на филтъра	Ниво на търсене в регистъра LDAP	Определяне на индивидуалния филтър

Уеб управление

Уебклипове

На това място дефинирайте отметки с връзки към уеб страници, интранет портали и т.н., които ще бъдат видими като приложение на крайното потребителско устройство.

Етикет	Име на връзката в крайното потребителско устройство
URL	Връзка към съответния уебсайт
Сменяем	Ако е активирано, потребителят може да премахне уеб клипа
Икона	В този диалог качете лого за връзката: Размери 180x180, формат png
Предварително съставена икона	Ако е активирано, върху иконата няма да се показват допълнителни ефекти (сянка, отражение).
Пълен екран	При отваряне на уеб клипове браузърът се отваря в режим на цял екран

Филтър за уеб съдържание

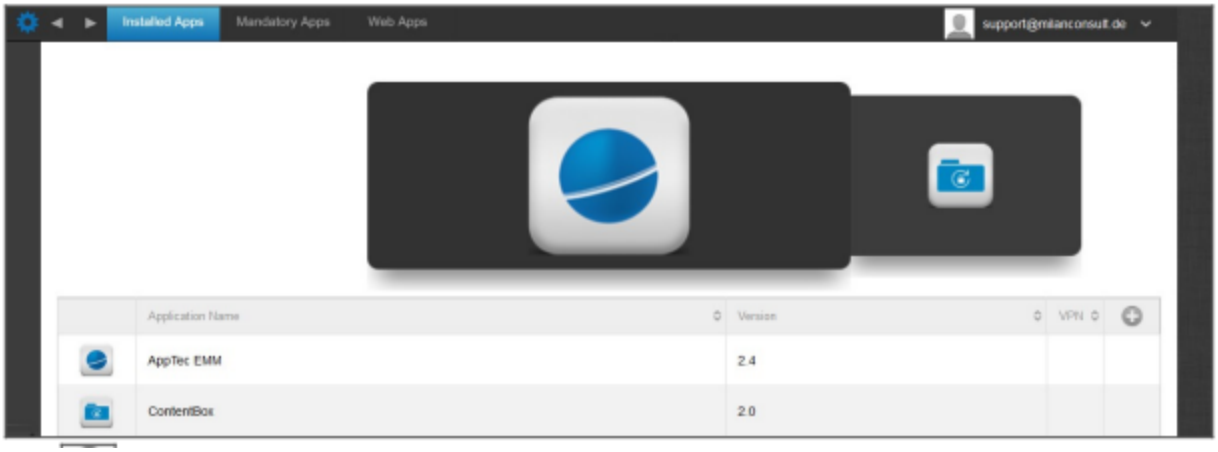
Филтърът за уеб съдържание дава възможност за ограничаване на достъпа до определени интернет страници.

Разрешени уебсайтове	
Ограничаване на съдържанието за възрастни	Уебфилтърът се прилага автоматично за съдържание за възрастни
Разрешени URL адреси	Със символа + добавете разрешени страници
URL адреси в черния списък	Със символа + добавете блокирани страници
Само конкретни уебсайтове	Може да се показва само определено съдържание, което можете да добавите със символа +.

Управление на приложения

Мениджър на корпоративни приложения

Инсталирани приложения (само на ниво устройство)



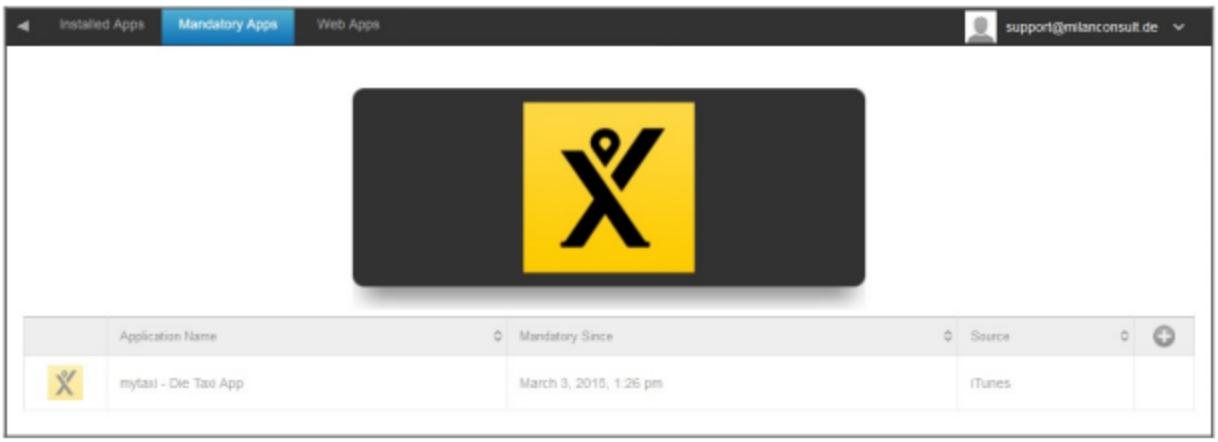
Тук можете да видите приложенията, които са инсталирани в момента на устройството.

Задължителни приложения

В раздел Задължителни приложения можете да зададете необходимите приложения.

На потребителя непрекъснато ще се напомня да инсталира това приложение.

Посредством , може да се определи задължителното приложение.



Това може да бъде приложение от Apple App Store, но и вътрешно приложение.

Ако става въпрос за контролирано устройство, приложението ще бъде инсталирано автоматично.

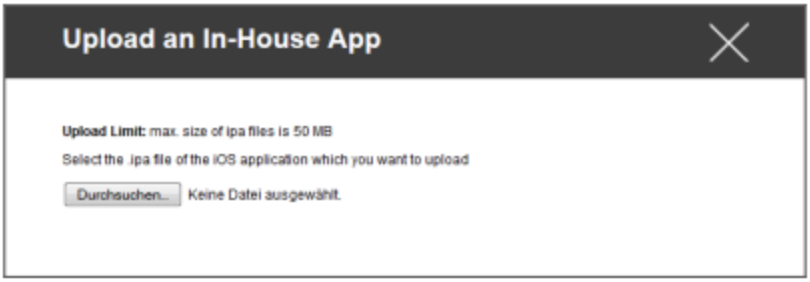
Можете да инсталирате на устройството приложение от публичния AppStore на Apple, както и вътрешно разработено приложение.

Или можете да изберете от категорията "Вътрешни приложения за iOS" и да изберете вътрешно приложение, което сте качили в "Общи настройки".

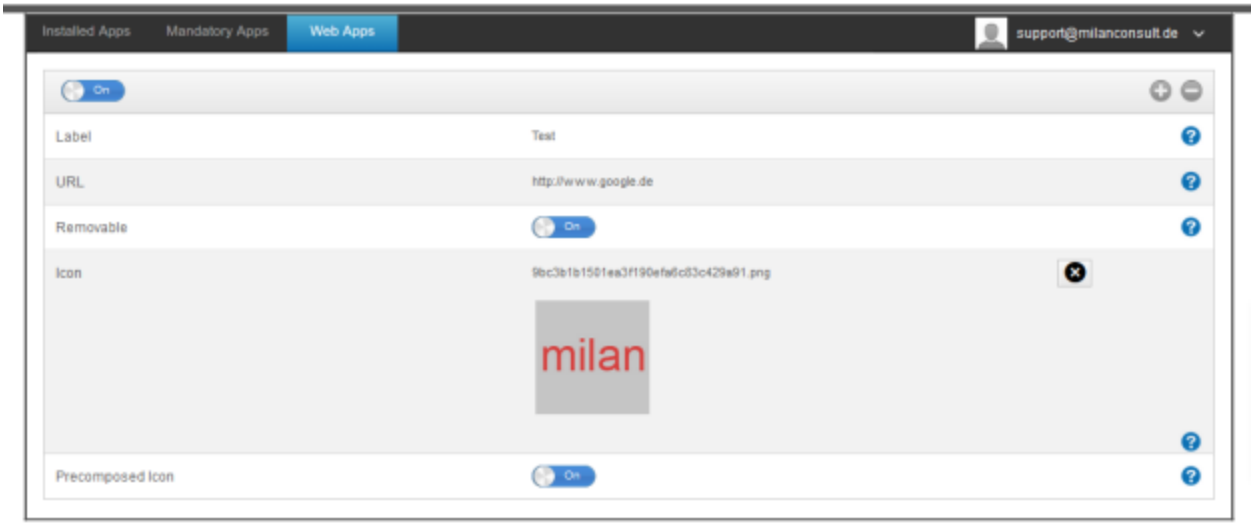
Опции за инсталиране

Поддържане на актуална информация (поддържа се само за VPP за всяко устройство)	Веднъж седмично ще се определя дали има актуализация на приложението. Ако да, тази актуализация ще бъде инсталирана. За вътрешните приложения за процеса на актуализация ще се използва целта за актуализация, конфигурирана в Общите настройки.
Изпреварване, когато не се управлява	Ако приложението вече е инсталирано, MDM ще поеме приложението и ще го управлява.
Премахване на приложението при премахване на MDM профила	В случай на премахване на управлението на устройството приложението ще бъде деинсталирано.
Предотвратяване на архивирането на данните на приложението	Няма да бъде създадено резервно копие на специфичните за приложението данни.
Настройка на приложението	В "Настройки на приложението" можете да зададете на приложението определени стойности на преден план (стига приложението да го поддържа, ако е необходимо, попитайте разработчика на приложението).

Можете също така директно да изберете и качите ipa файл чрез "Качване на вътрешно приложение".



Уеб приложения



В точката "Уеб приложения" можете, подобно на "Уеб клипове", да прехвърлите интернет страници или интранет портали като приложение на крайното потребителско устройство в областта на управлението на уеб. По подразбиране Web Apps ще се показват в режим на цял екран, който може да бъде конфигуриран в частта "Уеб клипове".

Етикет	Име на връзката в крайното потребителско устройство
URL	Връзка към съответния уебсайт
Сменяем	Ако е активиран, потребителят може да премахне Webclip
Икона	В този диалог качете лого за връзката: Размери 180x180, формат png
Предварително съставена икона	Ако е активирано, върху иконата няма да се показват допълнителни ефекти (сянка, отражение).

Ограничения и настройки

Приложения в черния списък / в белия списък

Тук можете да зададете приложенията, които са блокирани (или разрешени) в зависимост от настройките в "Общи настройки". Едно кликване върху ще доведе до търсене на известни приложения. Там можете да търсите приложенията, които искате да добавите.

Имайте предвид, че за тази функция е необходимо контролирано устройство.

Ограничения на SysApp

Блокиране на определени приложения или функции на вашето устройство

Разрешаване на използването на YouTube	Разрешаване на използването на YouTube
Разрешаване на използването на iTunes Store	Разрешаване на използването на iTunes Store
Разрешаване на използването на Safari	Разрешаване на използването на Safari
Активиране на автоматично попълване	Позволява автоматично попълване
Предупреждение за измама	Изпълнява предупреждението за измама
Активиране на JavScript	Позволява използването на JavaScript
Блокиране на изскачащи прозорци	Блокира всички видове кученца
Разрешаване на бисквитките	Изберете кога Safari да приема бисквитки

App-VPN

Чрез символа можете да дефинирате приложения, които автоматично да стартират избраната VPN връзка при стартиране.

Настройки на приложението

В "Настройки на приложението" можете да зададете на приложението определени стойности на преден план (стига приложението да го поддържа, ако е необходимо, попитайте разработчика на приложението).

Чрез символа добавяте (допълнително) приложение. Отново ще намерите познатото представяне на AppTec360 на App-Import.

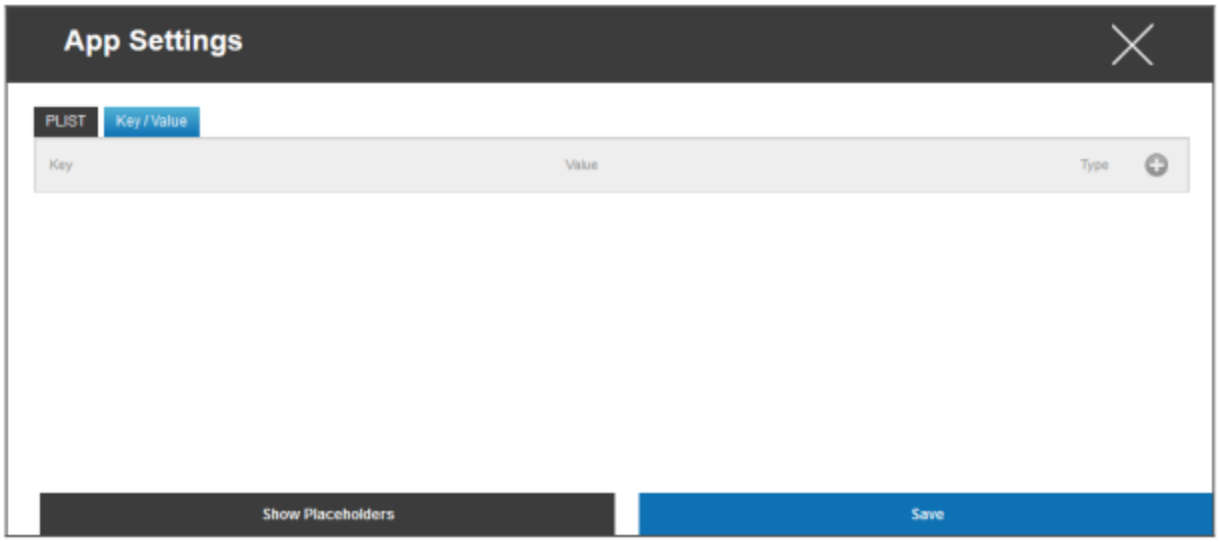
Потърсете тук приложението, което искате да конфигурирате, и го изберете. Настройките ще се прилагат само за управляваните приложения.

Ако импортирането е било успешно, ще видите следния дисплей:

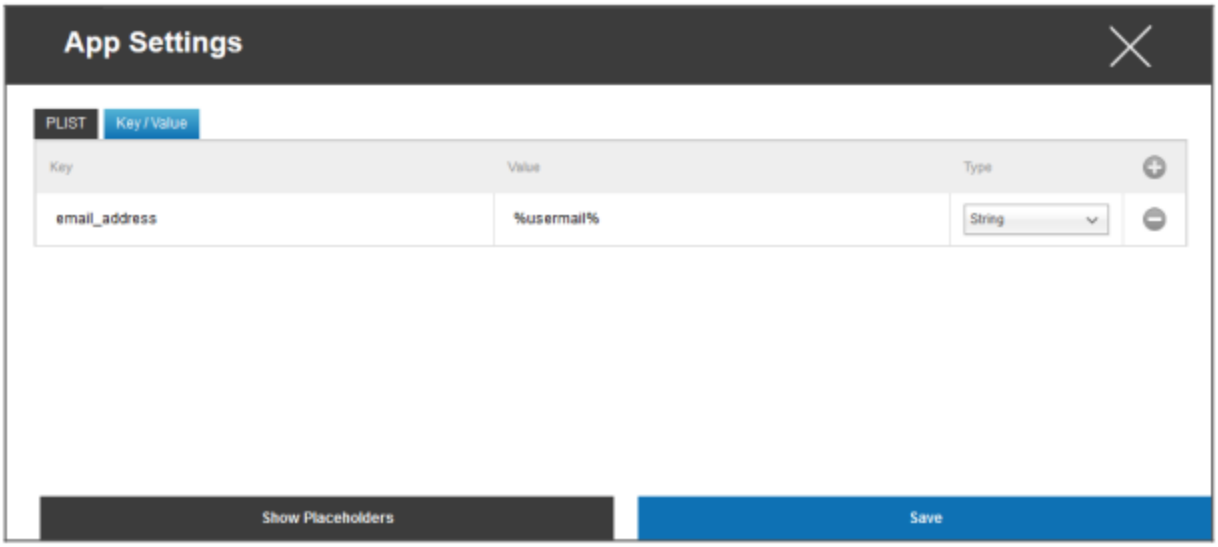
Сега с едно щракване върху , можете да извършвате различни конфигурации. След това ще получите следния преглед:

Ако вече разполагате с PLIST (изходен текст на конфигурацията), можете да го добавите тук и да запишете всичко с "Save".

В "Ключ/Стойност" можете да прикачите конкретни конфигурации към приложението



Тук можете да създадете нов ключ и неговата стойност със символа.



Разбира се, всички заместители на AppTec са на ваше разположение

Обяснение "Тип":

Редица	Текст
Булеви	Вярно/невярно
Номер	Номер

Със символа можете да премахнете дадено приложение отново.

Магазин за корпоративни приложения

Приложения на iTunes

В тази точка можете да разпространявате опционални приложения за вашия потребител.

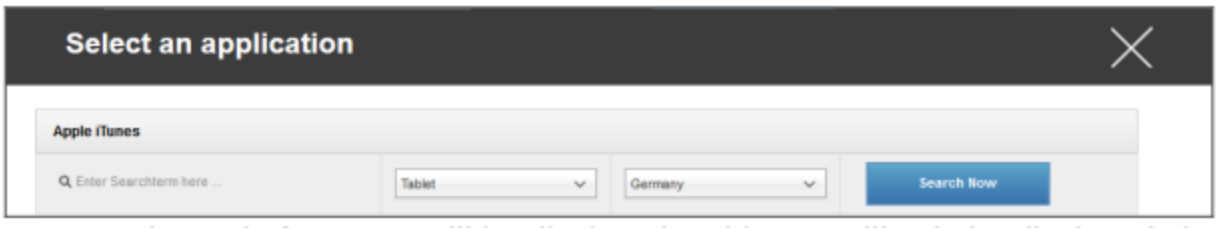
Ако тук има приложение, то ще бъде инсталирано автоматично на устройството на крайния потребител в AppTec360 Store.

Това са просто връзки към официалния магазин за приложения на Apple. Поради тази причина всяко устройство на крайния потребител трябва да бъде оборудвано с Apple ID.

На този етап препоръчваме всеки потребител да има свой собствен Apple ID.

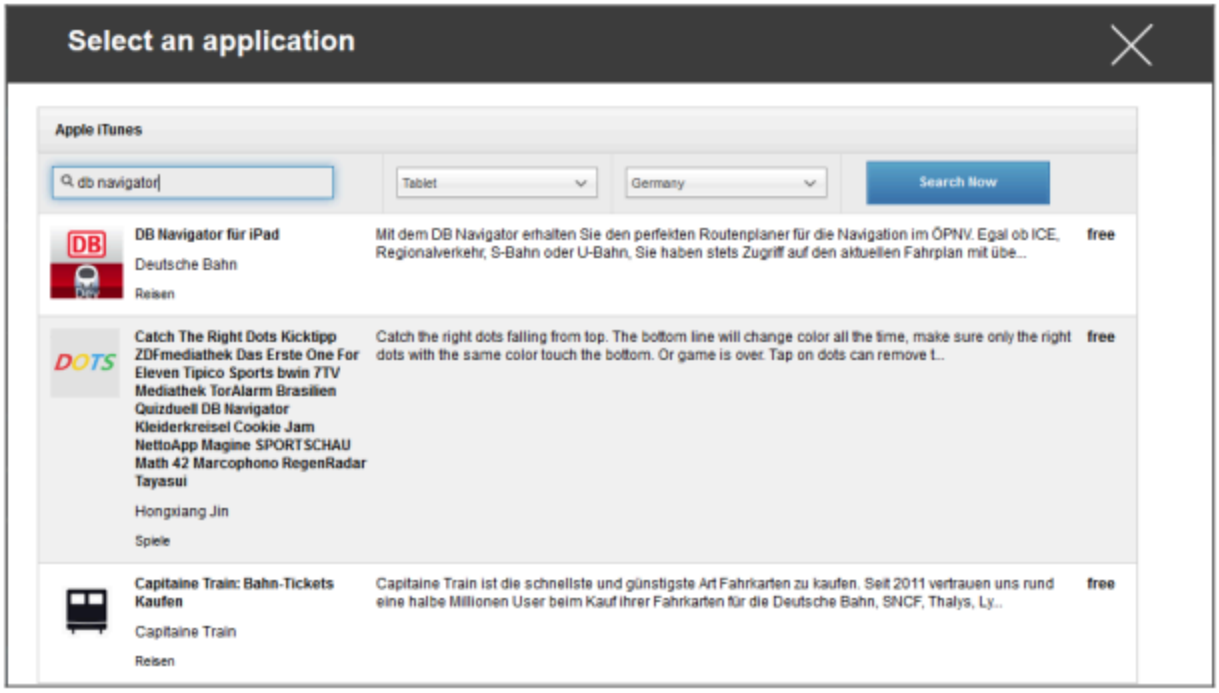
Със символа можете да добавяте допълнителни приложения.

След това ще се отвори прозорец със следния преглед.



Моля, обърнете внимание, че ще се показват само безплатни приложения, а платените ще се показват само чрез VPN.

Под "Enter Search Term here ..." можете да търсите приложение, което се намира в Apple App Store.



След като щракнете върху иконата или върху името на приложението, ще бъдете помолени отново да извършите допълнителни конфигурации.

Бъдете в крак с новостите	Веднъж седмично ще се определя дали има актуализация на приложението. Ако да, тази актуализация ще бъде инсталирана.
Премахване на приложението при премахване на MDM профила	В случай на премахване на управлението на устройството приложението ще бъде деинсталирано.
Предотвратяване на архивирането на данните на приложението	Няма да бъде създадено резервно копие на специфичните за приложението данни.

App-VPN	Изберете VPN-връзка, която ще се стартира при отваряне на приложението

След натискане на бутона "Инсталиране" приложението ще бъде добавено в Enterprise App Store и след това може да бъде инсталирано на крайното потребителско устройство чрез AppTec360 AppStore.

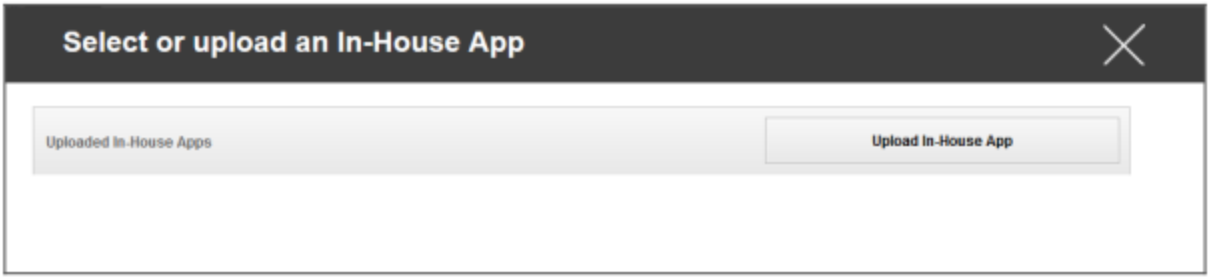
Ако импортирането в App-Store е било успешно, ще получите следния преглед:

Вътрешен

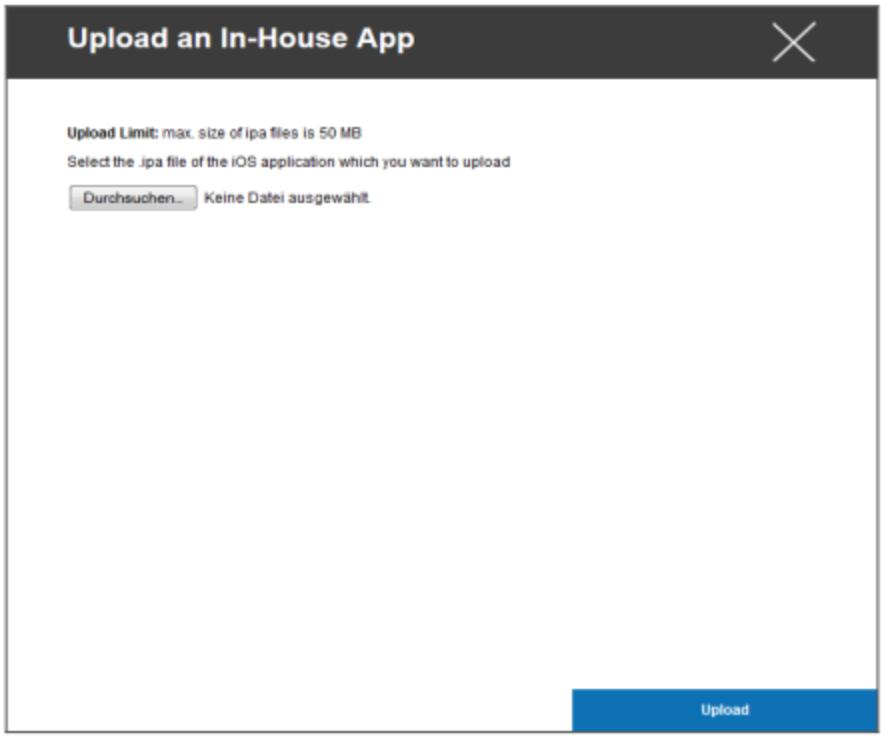
В точката "In-House" можете да качвате вътрешно разработени приложения и да ги разпространявате.

Със символа можете да разпространявате допълнителни вътрешни приложения.

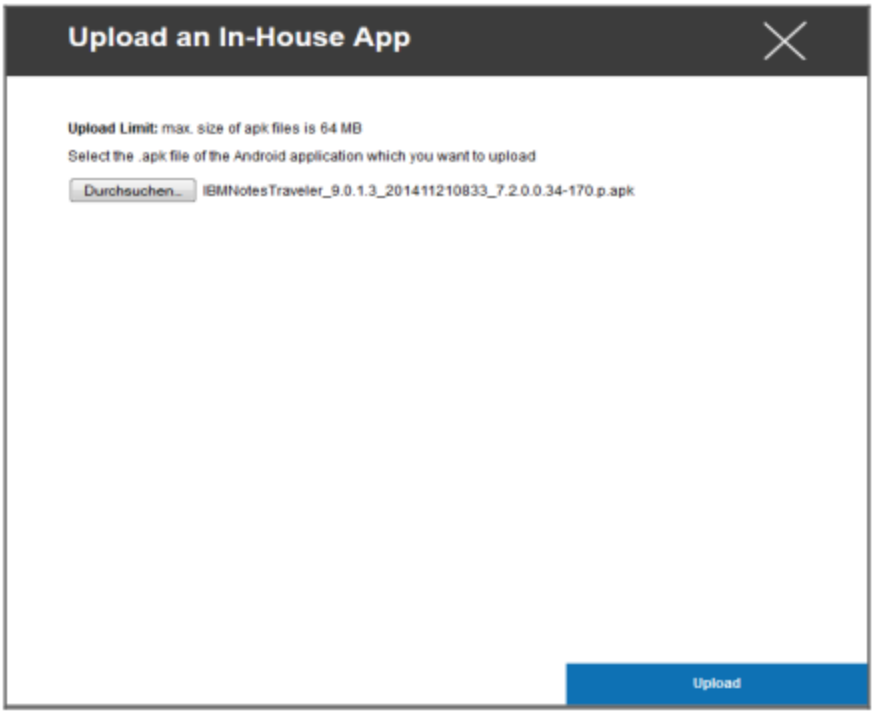
Ако никога не сте разпространявали вътрешно приложение, ще получите следния преглед:



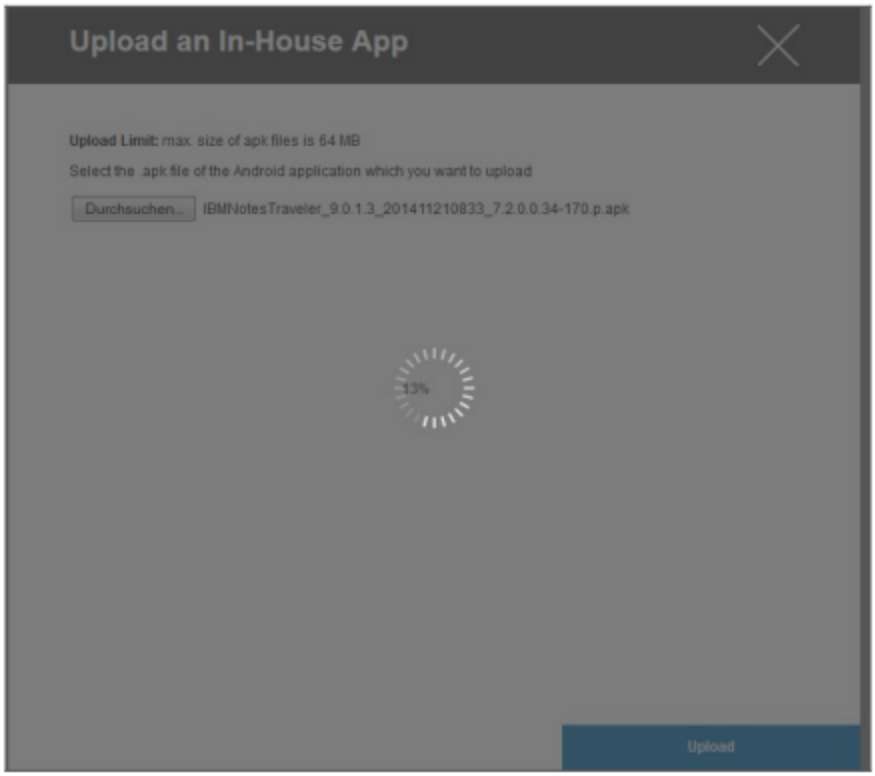
За целта щракнете върху "Upload In-House App", след което ще получите следния преглед:



Сега изберете с "Търсене...".ipa файл и щракнете върху "Качване".



Приложението ви вече ще бъде качено. В средата на кръга можете да видите процента, в който вече е качено вашето приложение.



Ако качването на вътрешното приложение е извършено успешно, ще видите новото качено приложение в каталога си с приложения.

Сега потребителят има възможност да види и инсталира това приложение в AppTec360 Store на устройството на крайния потребител, в категорията "In-House".

Поради факта, че това не включва публично приложение в Apple AppStore, потребителят не се нуждае от съхранен Apple ID на крайното потребителско устройство.

Режим на киоск

Режимът iOS Kiosk е наличен само в контролиран режим

Режимът Kiosk Mode ви позволява да дефинирате предварително приложение или URL адрес, така че да можете да стартирате/посещавате единствено това приложение/URL адрес.

Освен това можете да деактивирате различни хардуерни бутони в режим Kiosk Mode.

Тип приложение

Пакет

Ако искате да стартирате приложението в режим на киоск, изберете "Пакет" под "Тип приложение".

Приложение за киоск	Щракнете тук, за да изберете приложение, което трябва да се стартира в режим Kiosk Mode. Ще намерите текущия преглед на управлението на приложенията Можете да избирате между "Apple iTunes Apps" и "iOS In-House Apps".

URL

Ако искате да стартирате URL адрес в режим на киоск, изберете "URL адрес" под "Тип приложение".

URL	Сега задайте желания URL адрес
Политика за еднакъв произход	Ако тази функция е активна, потребителят може да сърфира само в подстраниците на предварително зададения URL адрес. Например, ако сте задали следния URL адрес: www.mypage.com, тогава потребителят може да сърфира в www.mypage.com/subpage
URL адреси в белия списък	Тук можете да поддържате бял списък, като всички тези URL адреси са разрешени. Максимум 1 URL на ред URL адресът трябва да започва с http:/ или https://
URL адреси в черния списък	Тук можете да поддържате черен списък, в който всички тези URL адреси са забранени. Максимум 1 URL на ред URL адресът трябва да започва с http:/ или https://
Изчистване на браузъра след неактивност	След неактивност кешът на браузъра ще бъде изпразнен.
Включена парола за излизане	Ако активирате тази функция, потребителят има възможност да прекрати режима на киоск с предварително зададена от вас парола.
Парола за излизане	Това е предварително зададената от вас парола.

Настройки на режима Kiosk

Планиран режим на киоск	Въз основа на времето от деня можете да настроите режима Kiosk Mode, така че режимът да се стартира и прекратява автоматично в предварително определено време.
Време на започване	Начален час
Време в минути	Време в минути, след което режимът Kiosk трябва да бъде прекратен отново
Деактивиране на докосването	Ако е активиран, сензорният екран се деактивира
Деактивиране на завъртането на устройството	Ако е активирана, автоматичната адаптация на екрана се деактивира
Деактивиране на превключвателя за звънене	Ако е активиран, превключвателят за звънене ще бъде деактивиран. От този момент нататък поведението зависи от предварително зададената функция
Деактивиране на бутоните за сила на звука	Ако са активирани, бутоните за сила на звука ще бъдат деактивирани.
Деактивиране на бутона за събуждане по време на сън	Ако е активиран, превключвателят за включване/изключване ще бъде деактивиран
Деактивиране на автоматичното заключване	Ако е активирано, устройството няма да бъде превключено в режим на готовност
Активиране на Voice Over	Ако е активиран, ще се активира Voice Over Assistant.
Активиране на увеличението	Ако е активирано, мащабирането ще се активира
Активиране на инвертиране на цветовете	Ако е активиран, ще се активира режимът на инвертиран дисплей.
Активиране на функцията Assistive Touch	Ако е активиран, AssistiveTouch ще се активира.
Активиране на избора на говорене	Ако е активиран, ще се активира изборът за говорене
Активиране на моно аудио	Ако е активирано, ще се активира монофоничното аудио.
VoiceOver	Ако е активиран, потребителят може да активира VoiceOver

Zoom	Ако е активирано, потребителят може да активира функцията Zoom
Инвертиране на цветовете	Ако е активирано, потребителят може да активира инвертирани цветове.
Помощно докосване	Ако е активирано, потребителят може да активира асистиращо докосване

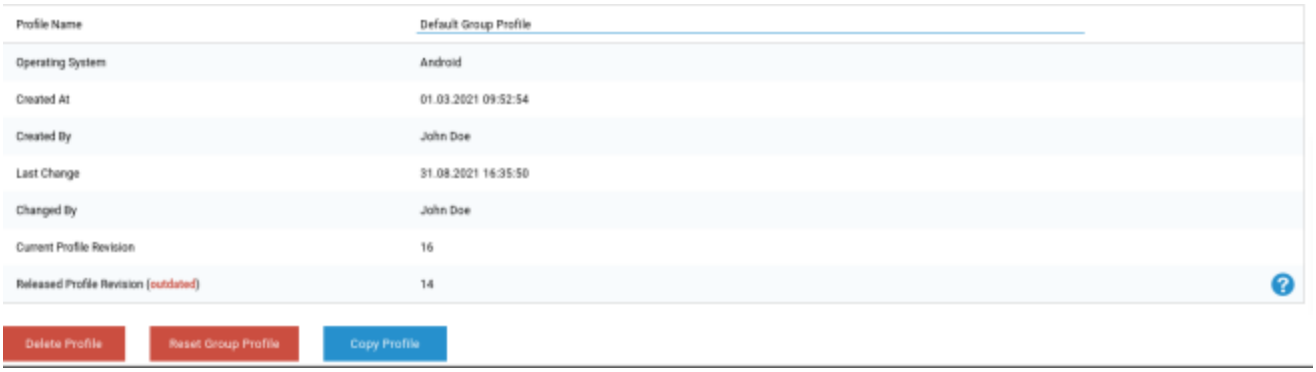
Android Enterprise – Напълно управлявано конфигуриране на устройства

В зависимост от това дали в момента сте избрали групов профил или устройство, прегледът и неговите подточки се различават - моля, обърнете внимание на това!

Обща информация

Преглед на профила на групата (само на ниво група)

При отваряне на групов профил ще получите бърз преглед на профила.



Име на профила	Име на профила (може да бъде променено тук)
Операционна система	Операционна система, за която е предназначен профилът
Създаден в	Време на създаване
Създаден от	Създател на профила
Последна промяна	Време на последната промяна в профила
Променено от	Акаунт, в който са направени последните промени

Текуща ревизия на профила	Преразглеждане на запазеното състояние на профила
Освободена ревизия на профила	Присвоена ревизия на профила ("Присвои сега"). Ако етикетът показва " (остарял)" зад текста, това означава, че сте запазили профила, но все още не сте го назначили, така че устройствата все още ще получават по-стара версия.

Преглед на устройството (само на ниво устройство)

Ако се намирате на устройство, ще получите обобщаващ преглед на избраното устройство, като тук се съдържа следното:

Име на устройството	Име на устройството
Местоположение	Координати на местоположението
Телефонен номер	Телефонен номер
Зададени задължителни приложения	Брой зададени задължителни приложения
Версия на операционната система	Версия на операционната система на устройството
Операционна система	Операционна система (Android Enterprise)
Сериен номер	Сериен номер на устройството
Притежание на устройство	Корпоративно или частно устройство
Тип устройство	Управлявано устройство AE Work
Вкоренени	Състояние, показващо дали устройството е било рутирано
Съответстващ	Съответствие с насоките
IP адрес	IP адрес на устройството
Последно видян	Точка във времето, когато устройството се е свързало за последен път с AppTec
Последен тласък	Точка във времето, в която е изпратено последното натискане към устройството
Режим на собственика на устройството AE	Да
Присвояване на потребителя	Потребителят или групата, към която е назначено това устройство

Ревизия на конфигурацията (само на ниво устройство)

Тук можете да видите кой групов профил е зададен на устройството.

Ако щракнете върху груповия профил, ще получите директен достъп до този профил и ще можете да извършвате настройки.

С този символ можете да върнете разпределените приложения към настройките на груповия профил.

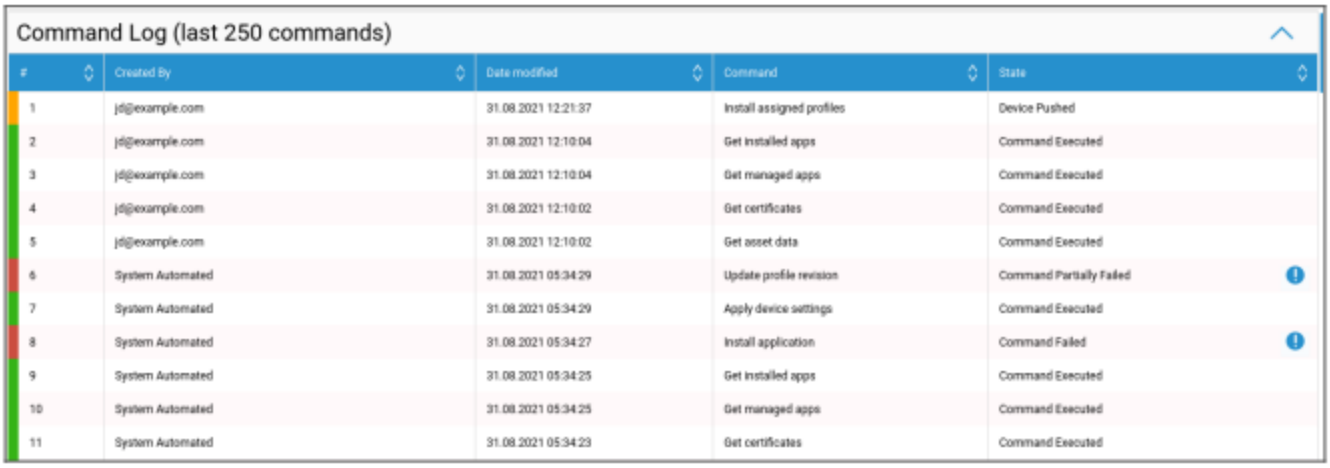
С този символ можете да върнете всички използвани приложения към настройките на груповия профил.

"Налична е по-нова ревизия" показва, че профилът на групата е променен и запазен, но не е присвоен. Груповият профил трябва да бъде присвоен с "Assign now" (Присвояване сега) на ниво група, за да се приложат промените към устройствата.

Дневник на устройството (само на ниво устройство)

Дневник на командите

Тук можете да видите кои команди са издадени за устройството и какво е тяхното състояние.



Командите, създадени от "System Automated", се създават автоматично от системата.

Възможни състояния на командата

Натиснато устройство	Изпратена е заявка за натискане до услугата за натискане (напр. APNS), за да се каже на устройството да се свърже отново със сървъра на EMM.
Създадена команда	Командата е създадена в системата.
Изпратена команда	Командата е изпратена на устройството, след като то се е свързало със сървъра.
Изпълнена команда	Командата е изпълнена успешно.
Командата е неуспешна	Командата не е изпълнена. *
Командата е частично неуспешна	В зависимост от операционната система на устройството някои команди могат да бъдат групирани заедно. При това някои части от тази група команди не успяха. *
Командата е изпълнена, но в крайна сметка е неуспешна	Командата е изпълнена, но може би не е.
Пренасочване на командата	Командата е била изпратена отново от потребител.
Изхвърлени	Командата беше отхвърлена. Например защото е била заменена от друга команда или устройството е било презаписано и старите команди са били премахнати.

Ако зад съобщението има възклицателен знак, можете да получите повече информация, като задържите курсора върху иконата.

Настройки на устройството

Конфигурация на клиента

Тук можете да извършите следните конфигурации на вашето устройство с Android:

Време за несъответствие	Ограничението на времето за отговор на потребителя, след което се прилага действието за изпълнение.
Действия по изпълнение след изтичане на срока за изпълнение	Действия по прилагане, когато потребителят не извършва действия, които водят до статус на съвместимо устройство
Честота на събиране на данни	Честота на събиране на информация за устройствата/GPS
Честота на сърдечния ритъм на устройството	Интервал, през който устройството трябва да се свърже със сървъра AppTec360 Мин. 1 минута Макс. 24 часа
Активиране на актуализациите на местоположението	Ако е активирано, устройството изпраща актуализации на местоположението към сървъра AppTec360
Време за актуализация на местоположението	Определя през какви интервали от време устройството изпраща актуализации на местоположението към AppTec360
Използване на Google Location Accuracy за актуализация на местоположението	Ако е активирано, местоположението в мрежата ще се използва за актуализации на местоположението (ако е деактивирано в "Ограничения", тази настройка няма да повлияе на нищо).
Използване на GPS местоположение за актуализиране на местоположението	Ако е активирано, GPS ще се използва за актуализации на местоположението.
Разрешаване на имитационни (фалшиви) местоположения	Позволява подправяне на информация за местоположението чрез приложения на трети страни
Действие при изгубена връзка	Ако е разрешено, можете да зададете действие в случай, че дадено устройство не получи връзка с MDM сървъра през интервала за сърдечен ритъм. Например, ако устройството има интервал на сърдечния ритъм от 5 минути, то се свързва със

	сървъра в 10:35 ч. След това устройството напуска обхвата на Wi-Fi. Следващият сърдечен ритъм в 10:40 ч. няма да успее и ще бъде изпълнено посоченото действие.
Действие	Действието, което трябва да се предприеме, когато дадено устройство стане несъответстващо на изискванията. • Устройство за заключване = устройство за заключване • Изтриване на устройството = устройството ще бъде възстановено до фабричните настройки • Изтриване на устройството и SD картата = устройството ще бъде възстановено до фабричните настройки, а паметта на SD картата ще бъде изтрита
Праг	Можете да зададете праг от неуспешни сърдечни удари, които са необходими за задействане на посоченото действие.

Режим на прилагане на политиката	По подразбиране:	Потребителите ще бъдат подканени периодично да изпълнят неизпълнени действия.
	Лениво прилагане на политики:	Потребителите никога няма да бъдат подканени да изпълнят неизпълнени действия. Всички отворени действия ще бъдат показани в AppTec360 Client.
	Агресивно прилагане на политики:	Потребителите ще бъдат подканвани непрекъснато да изпълняват неизпълнени действия.
Заключване на версията на AppTec360	Ако е разрешено, може да се зададе код на версията на AppTec360 MDM Client. Клиентът AppTec360 ще се актуализира само до посочената версия. По-новите версии ще бъдат игнорирани. Не е възможно да се извърши понижаване на версията.	
Код на версията	Код на версията на AppTec360 MDM Client, към която трябва да бъде заключен.	
Деактивиране на известието AppTec360	Ако е деактивиран, клиентът AppTec360 няма да показва известие в лентата за известия. По този начин потребителите могат да затворят AppTec360 клиента чрез мениджъра на задачите. Ако клиентът AppTec360 е затворен, няколко функции, включително Kiosk Mode (Режим на киоск) и App Black/Whitelisting (Черна/бяла листа на приложения), няма да работят правилно. Устройствата на Samsung предлагат механизъм за защита на AppTec360 Client. Известието е деактивирано по подразбиране на устройствата на	

	Samsung, които поддържат приложните програмни интерфейси KNOX. Известието не трябва да бъде деактивирано на устройства с Android 8.0 или по-нова версия.

Тапети

Задаване на персонализиран тапет	Активиране/деактивиране на персонализирания тапет
Тапети	Задаване на режима на тапета за използване на цветен код или изображение
Определяне на цвят	Посочете цвят на фона като шестнадесетична стойност, например #000000 за черно или #ffffff за бяло
Задаване на изображение като тапет	Качете файла с изображението, което искате да използвате като тапет

Управление на активи (само на ниво устройство)

Информация за устройството

Модел	Обозначение на модела на устройството
Операционна система	OS
Версия на операционната система	Версия на операционната система
Сериен номер	Сериен номер
Име на устройството	Име на устройството
Състояние на батерията	Състояние на батерията
Свободна / обща памет	Свободна / обща памет
Samsung Safe	Интерфейс Samsung SAFE, необходим за различни опции за настройка
Налична SD карта	Налична SD карта
Емулирана SD карта	Емулирана SD карта
Сменяема SD карта	Сменяема SD карта
SD Свободна / обща памет	SD Свободна / обща памет на SD картата

Wi-Fi

IP адрес	IP адрес на устройството
WiFi MAC	WiFi MAC адрес

Клетъчен

Статус	Състояние (инсталирана SIM карта)
Телефонен номер	Телефонен номер
Роуминг (глас/данни)	Роуминг за глас/данни
Състояние на роуминга	Текущо състояние на роуминга
IP адрес	IP адрес
Оператор/превозвач	Оператор/превозвач
Клетъчна технология	Клетъчна технология
IMEI	Номер на IMEI
ICCID	Това е идентификационният номер на SIM картата, често наричана също Smartcard или Integrated Circuit Card (ICC).
IMSI	Международният идентификатор на мобилния абонат (IMSI) осигурява в мобилните мрежи GSM и UMTS точна идентификация на потребителите на мрежата. IMSI се състои от максимум 15 цифри и се конфигурира по следния начин: • Код на мобилната държава (MCC), 3 цифри • Код на мобилната мрежа (MNC), 2 или 3 цифри • Идентификационен номер на мобилен абонат (MSIN), 1-10 цифри
Текущи MCC/MNC	Вижте "SIM MCC/MNC".
SIM MCC/MNC	Кодът на мобилната държава е установен идентификатор на държавата, определен от ITU съгласно стандарт E.212. Той се използва заедно с кода на мобилната мрежа (MNC) за идентифициране на мобилната мрежа. Означава кода на страната/кода на мобилната мрежа на SIM картата. Ако сте в роуминг в друга мобилна мрежа, логично е "Current MCC/MNC" и "SIM MCC/MNC" да са различни.

Bluetooth

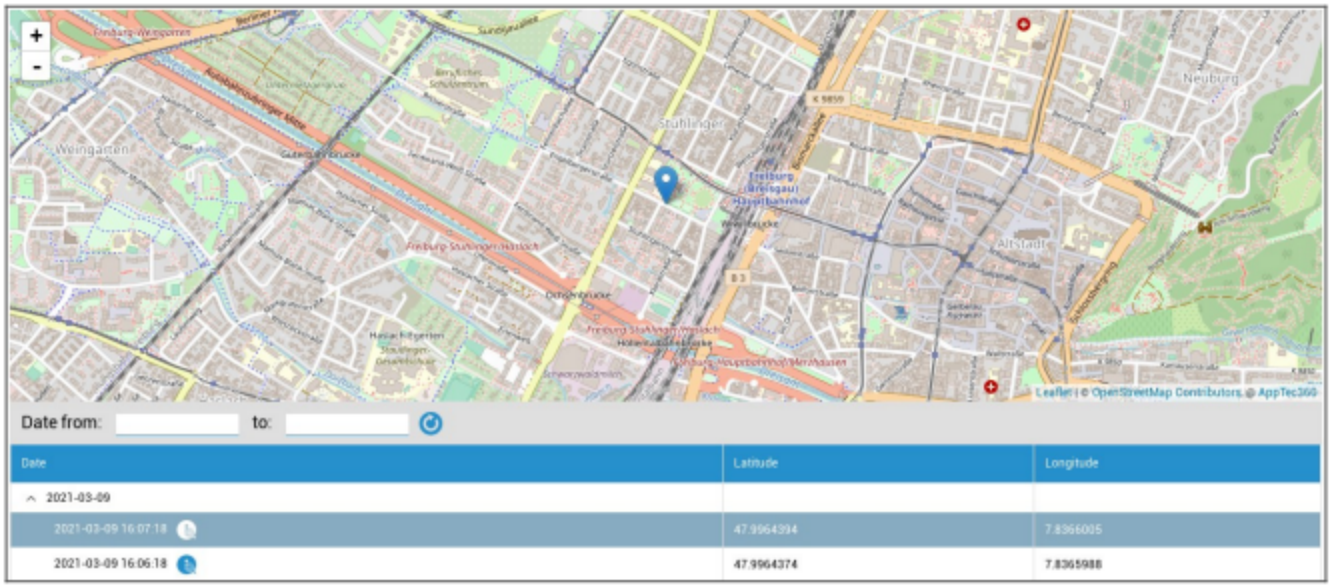
Bluetooth MAC	Bluetooth MAC адрес

Управление на сигурността

Защита от кражба (само на ниво устройство)

GPS информация (само на ниво устройство)

Тук можете да определите текущото/последното местоположение на устройството. Локализирането може да бъде защитено с една или дори две пароли - вж: Общи настройки - Поверителност - Достъп до GPS



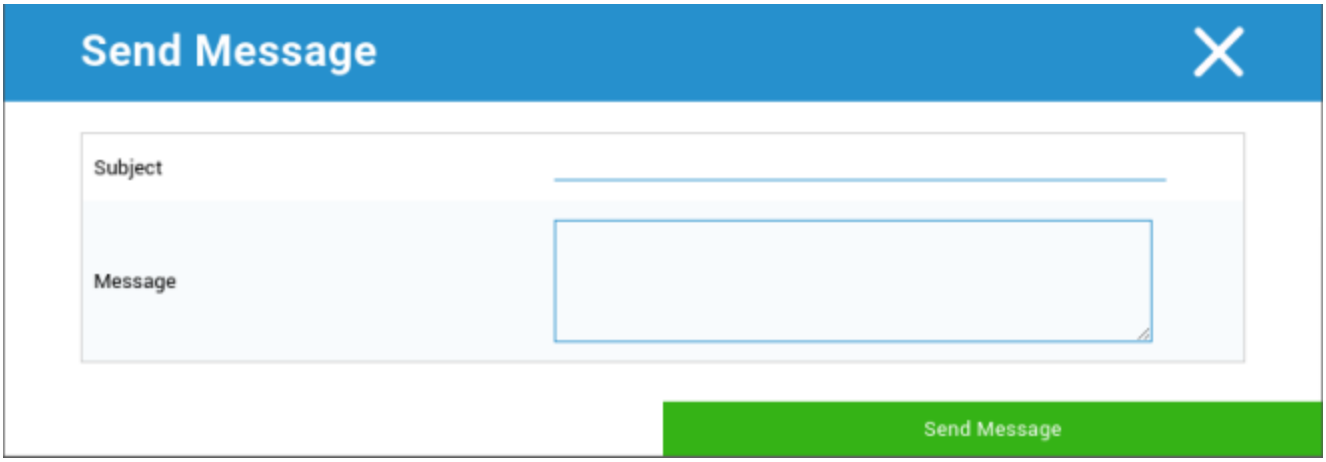
Изтриване и заключване (само на ниво устройство)

В "Изтриване и заключване" можете да извършите следните три действия:

Пълно избърсване	Устройството се възстановява до фабричните си настройки (корпоративните и личните данни се изтриват).
Изтриване на предприятието	От устройството на крайния потребител се премахват само корпоративните данни (всички приложения, данни и т.н., които са били предоставени от AppTec360)
Екран за заключване	Активирано е заключване на екрана, достатъчно е да отключите устройството с паролата на устройството/ ПИН кода.

Съобщение (само на ниво устройство)

Тук можете да попълните темата и съобщението и да го изпратите на крайно потребителско устройство.



Конфигурация на сигурността

Парола на устройството

В "Парола" можете да зададете парола на устройството, като имате на разположение следните опции за настройка

Минимална дължина на паролата	Определя минималния брой символи, които трябва да съдържа паролата.	
Качество на паролата	Неуточнено	Тази политика няма изисквания за паролата.
	Биометрични данни Слаби	Тази политика позволява използването на биометрични технологии за разпознаване с ниска степен на сигурност. Това означава технологии, които могат да разпознаят самоличността на дадено лице до около трицифрен ПИН код (фалшивото разпознаване е по-малко от 1 на 1000).
	Нещо	Тази политика изисква задаването на някакъв вид парола или шаблон, но не налага никакви конкретни правила.
	Азбучен	Потребителят трябва да е въвел парола, съдържаща поне буквени (или други символи) знаци.
	Буквено-цифрови	Потребителят трябва да е въвел парола, съдържаща поне два символа - цифров и буквен (или друг символ).
	Комплекс	Потребителят трябва да е въвел парола, която по подразбиране съдържа поне една буква, една цифра и един специален символ. С това качество на паролата може да се ограничи съдържанието на различни набори от символи, като например поне една главна буква и т.н.
Минимална дължина на паролата	Задайте необходимия брой символи за паролата. Например можете да изисквате ПИН кодът или паролите да съдържат най-малко шест знака.	
Минимален брой цифри, изисквани в паролата	Минимален брой цифри, изисквани в паролата	
Минимален брой малки букви, изисквани в паролата	Минимален брой малки букви, изисквани в паролата	

Минимален брой главни букви, изисквани в паролата	Минимален брой главни букви, изисквани в паролата
Минимален брой небуквени символи, изисквани в паролата	Минимален брой небуквени символи, изисквани в паролата
Минимален брой символи, изисквани в паролата	Минимален брой символи, изисквани в паролата

Максимално време за заключване при неактивност	Максимална неактивност на потребителя до заключване на времето
Време за изтичане на паролата	Установява, след който интервал от време паролата изтича и трябва да се издаде нова парола.
Ограничаване на историята на паролите	Брой на използваните преди това пароли, които не са разрешени
Максимален брой неуспешни опити за парола	Установява колко често паролата може да бъде въведена неправилно, преди да се извърши пълно изтриване на устройството.
Разрешаване на биометрично удостоверяване	Позволява удостоверяване чрез пръстов отпечатък или сканиране на ириса. Само за Samsung KNOX 2.1 и по-висока версия

Антивирус

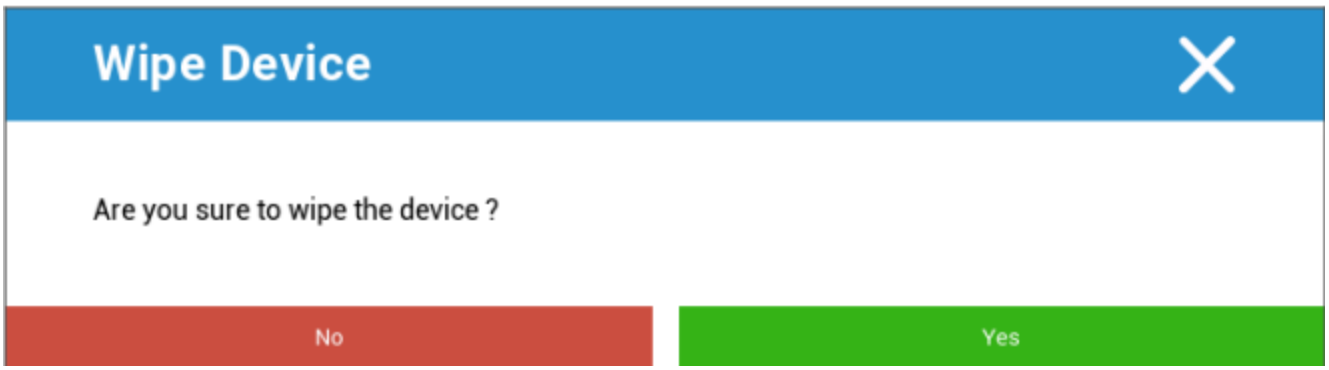
Автоматично сканиране	Активиране на периодични автоматични сканирания
Интервал на сканиране	Интервал за преглед (бърз/пълен)
Пълно автоматично сканиране	Активиране на пълно автоматично сканиране
Автоматични актуализации	Активиране на автоматични актуализации
Интервал на проверката за актуализация	Колко често трябва да се актуализират приложението и неговата база данни (вируси / повреден код)
Защита на приложенията	Активиране на автоматичното сканиране на приложения
Защита на SD картата	Активиране на автоматичното сканиране на SD картата
Актуализация само за Wi-Fi	Когато е разрешено, актуализациите ще се прилагат само когато устройството е успешно свързано с Wi-Fi мрежа.

Край на живота (само на ниво устройство)

Избърсване (само на ниво устройство)

Под "Изтриване" можете да възстановите фабричните настройки на устройството. Тук корпоративните, както и личните данни ще бъдат изтрити от устройството на крайния потребител.

След като кликнете върху символа "минус", ще получите следното съобщение:



С "Да" можете да извършите изтриването.

Под "Отчет за изтриване" могат да бъдат показани следните елементи

Изтрити от	История на лицето, извършило изтриването
Дата	Дата
Статус	Статус (например дали изтриването е извършено успешно)

Настройки на ограниченията

Ограничения

Тук могат да се ограничават и блокират различни неща.

Активиране на камерата	Разрешаване на използването на камера	
Принудителна автоматична синхронизация	На	Синхронизацията е постоянно активирана
	Изключено	Синхронизацията е постоянно деактивирана
	Избор на потребителя	Избрано от потребителя
Принудителна Bluetooth	На	Bluetooth е постоянно активиран
	Изключено	Bluetooth е постоянно деактивиран
	Избор на потребителя	Избрано от потребителя
Сила на GPS	На	GPS е постоянно активиран
	Изключено	GPS е постоянно деактивиран
	Избор на потребителя	Избрано от потребителя
Местоположение на мрежата на силите	На	Постоянно локализиране в интернет
	Изключено	Постоянно деактивиране на локализирането в интернет
	Избор на потребителя	Избрано от потребителя

Защита		
Забрана за споделяне на местоположението	Указва дали на даден потребител е забранено да включва споделяне на местоположението.	
Забрана за безопасно стартиране	Указва дали на потребителя не е разрешено да рестартира устройството в безопасен режим на зареждане.	
Забрана за нулиране на мрежата	Указва дали на даден потребител е забранено да възстановява мрежови настройки от Настройки.	
Забрана за възстановяване на фабричните настройки	Указва дали на даден потребител е забранено да нулира устройството.	
Активиране на ADB	Позволява свързване с компютър чрез ADB	
Деактивиране на функцията Keyguard	Деактивиране на функцията Keyguard	
Собственик на устройството Информация за заключен екран	Задава информацията за собственика на устройството, която да се показва на заключения екран.	
Изпълнение на изискванията	Режим Подкана Потребител	Потребителят ще бъде подканен да изпълни необходимите действия.
	Контейнер за блокиране на режима	Скриване на всички приложения, докато не бъдат изпълнени всички изисквания

Управление на приложения	
Разрешаване на свързването на приложения между профили	Позволява на приложенията в родителския профил да обработват уеб връзки от управлявания профил.
Забрана за контрол на приложенията	Указва дали на даден потребител е забранено да променя приложения в Настройки или стартиращи програми.
Забрана за инсталиране на приложения	Указва дали на даден потребител е забранено да инсталира приложения.
Забрана за деинсталиране на приложения	Указва дали на даден потребител е забранено да деинсталира приложения.
Политика за разрешаване по време на изпълнение	Указва как ще се обработват нови заявки за разрешение от приложения.
Разрешаване на неизвестни източници	Ако е разрешено, потребителите могат да зареждат приложения отстрани, като инсталират .apk файл.

Свързаност	
Забрана за конфигуриране на мобилна мрежа	Указва дали на даден потребител е забранено да конфигурира мобилни мрежи.
Конфигурация за забрана на тетеринг	Указва дали на даден потребител е забранено да конфигурира Tethering & portable hotspots.
Забрана на VPN Config	Указва дали на даден потребител е забранено да конфигурира VPN.
Забрана за конфигуриране на Wifi	Указва дали на даден потребител е забранено да променя точките за достъп до Wi-Fi.
Забрана за изходящ NFC лъч	Указва дали на потребителя не е разрешено да използва NFC за предаване на данни от приложения.
Заключване на конфигурацията на WiFi	Тази настройка контролира дали конфигурациите на Wi-Fi, създадени от приложение на собственика на устройството, трябва да бъдат заключени (т.е. да могат да се редактират или премахват само от приложението на собственика на устройството, а не дори от приложението "Настройки").
Активиране на роуминг на данни	Активира роуминг на данни

Bluetooth	
Забрана на Bluetooth	Указва дали Bluetooth е забранен на устройството. Изисква Android 8.0
Забрана за споделяне чрез Bluetooth	Указва дали изходящото споделяне на Bluetooth е забранено на устройството. Изисква Android 8.0
Забрана за конфигуриране на Bluetooth	Указва дали на даден потребител е забранено да конфигурира Bluetooth.

Управление на акаунти	
Забрана за добавяне на управляван профил	Указва дали на даден потребител е забранено да добавя управлявани профили. Изисква Android 8.0
Забрана за добавяне на потребители	Указва дали на даден потребител е забранено да добавя нови потребители.
Забрана за премахване на управляван профил	Указва дали управляваните профили на този потребител могат да бъдат премахнати, освен от собственика на профила. Изисква Android 8.0
Забрана за промяна на сметката	Указва дали на даден потребител е забранено да добавя и премахва акаунти, освен ако не са добавени програмно от Authenticator.

Телефония	
Забрана за изходящи повиквания	Указва, че на потребителя не е разрешено да извършва изходящи телефонни обаждания.
Забрана на SMS	Указва, че на потребителя не е разрешено да изпраща или получава SMS съобщения.

Система	
Забрана за създаване на прозорци	Указва, че не трябва да се създават други прозорци освен прозорците на приложението.
Забрана за задаване на потребителска икона	Указва дали на даден потребител не е позволено да променя своята икона.
Забрана за задаване на тапети	Потребителско ограничение за забрана на задаването на тапет.
Деактивиране на лентата на състоянието	Деактивирането на лентата на състоянието блокира известията, бързите настройки и други екранни наслагвания, които позволяват бягство от устройство за еднократна употреба.
Активиране на автоматично време	Настройва времето автоматично.
Активиране на автоматична часова зона	Автоматично задава часовата зона.

Останете включени, докато сте включени към мрежата	Устройството ще остане активно, докато е свързано към източник на захранване.

Съхранение	
Деактивиране на проверката на приложения	Указва дали на даден потребител е забранено да деактивира проверката на приложението.
Забрана за монтиране на физическа медия	Указва дали на даден потребител е забранено да монтира физически външни носители.
Активиране на услугата за архивиране	Услугата за архивиране управлява всички механизми за архивиране и възстановяване на устройството. Задаването на тази стойност на false ще предотврати архивирането или възстановяването на данни. Услугата за архивиране е изключена по подразбиране. Изисква Android 8.0
Активиране на USB Mass Storage	Разрешава използването на USB Mass Storage.

Клавиатура	
Забрана за автоматично попълване	Указва дали на даден потребител не е разрешено да използва услуги за автоматично попълване. Изисква Android 8.0
Забрана за копиране и поставяне между профили	Указва дали копираното в клипборда на този профил може да бъде вмъкнато в свързани профили.

Звук	
Забрана за коригиране на обема	Указва дали на даден потребител е забранено да регулира основната сила на звука.
Забрана за изключване на звука на микрофона	Указва дали на даден потребител е забранено да регулира силата на звука на микрофона.
Изключване на звука на устройството	Изключване на звука на устройството.

Управление на сертификати

Тук можете да разпространявате доверени сертификати и сертификати за идентичност към устройствата си.

Android 8 или по-нова версия се изисква за разпространение на доверени сертификати, а Android 9 или по-нова версия - за разпространение на сертификати за идентичност.

С бутона "+" можете да добавите няколко сертификата.

Достоверните сертификати трябва да са във формат PEM.

Сертификатите за самоличност трябва да бъдат във формат PKCS12.

Управление на връзките

Wifi

За тази настройка извършете предварително конфигуриране на крайните потребителски устройства за достъп до вътрешните точки за достъп

Идентификатор на набора от услуги (SSID)	SSID за мрежата, която трябва да се свърже
Скрита мрежа	Активиране, в случай че AP не излъчва SSID

Вид сигурност

Установяване на типа сигурност на AP

WEP

Парола	Парола за AP

WPA/WPA2

Парола	Парола за AP

802.1x EAP

Метод на EAP

PWD	Идентичност	Идентичност
	Парола	Парола

PEAP	Протокол за удостоверяване на фаза 2	няма	Без допълнителен протокол
		MSCHAPV2	Протокол MSCHAPV2
		GTC	Протокол на GTC
	Сертификат на CA	Сертификат на CA	
	Идентичност	Идентичност	
	Анонимна самоличност	Анонимна самоличност	
	Парола	Парола	

TTLS	Протокол за удостоверяване на фаза 2	няма	Без допълнителен протокол
		PAP	Протокол PAP
		MSCHAP	Протокол MSCHAP
		MSCHAPV2	Протокол MSCHAPV2
		GTC	Протокол на GTC
	Сертификат на CA	Сертификат на CA	
	Идентичност	Идентичност	
	Анонимна самоличност	Анонимна самоличност	
	Парола	Парола	

TLS	Сертификат на CA	Сертификат на CA
	Идентичност	Идентичност
	Парола	Парола

VPN

Име на връзката	Име на VPN връзката

Тип VPN

VPN

Клиент на VPN

AppTec360 VPN клиент	
Конфигурация на шлюза	Изберете конфигурацията на VPN шлюза (вижте **Общи настройки > Универсален шлюз > Настройки на VPN**).
Винаги включена VPN услуга	Активиране на функцията Native Lockdown
Активиране на заключването на AppTec360	Активиране на заключването на AppTec360

Вграден (наличен само в устройствата на Samsung)			
Тип на връзката	PPTP	Сървър	Сървър
		Активиране на криптирането PPTP	Активиране на криптирането PPTP
	L2TP / IPSec PSK	Сървър	Сървър
		Предварително споделен ключ на IPSec	Предварително споделен ключ на IPSec
		Активиране на L2TP Secret	Активиране на L2TP Secret
		L2TP Secret	L2TP Secret
	IPSec XAuth PSK	Сървър	Сървър
		Идентификатор на IPSec	Идентификатор на IPSec
		Предварително споделен ключ на IPSec	Предварително споделен ключ на IPSec
Домейни за търсене DNS	Домейни за търсене DNS		
Експертни настройки	DNS сървъри	DNS сървъри	
	Маршрути за препращане	Маршрути за препращане	

Отворена VPN услуга		
Сървър	Сървър	
Профил на OpenVPN	Профил на OpenVPN	
Приложение за OpenVPN	OpenVPN за Android (препоръчително)	
	Свързване с OpenVPN	
Експертни настройки	DNS сървъри	DNS сървъри
	Маршрути за препращане	Маршрути за препращане

Samsung / Strong Swan			
Тип на връзката	PPTP	Сървър	Сървър
		Потребителско име	Потребителско име
		Парола	Парола
		Активиране на криптирането PPTP	Активиране на криптирането PPTP
	L2TP / IPSec PSK	Сървър	Сървър
		Предварително споделен ключ на IPSec	Предварително споделен ключ на IPSec
		Потребителско име	Потребителско име
		Парола	Парола
		Активиране на L2TP Secret	L2TP Secret
	IPSec XAuth PSK	Сървър	Сървър
		Идентификатор на IPSec	Идентификатор на IPSec
		Предварително споделен ключ на IPSec	Предварително споделен ключ на IPSec
		Потребителско име	Потребителско име
		Парола	Парола
Експертни настройки	DNS сървъри	DNS сървъри	
	Маршрути за препращане	Маршрути за препращане	

Cisco Any Connect		
Сървър	Сървър	
Режим на сертификата	Инвалиди	Инвалиди
	Автоматичен	Автоматичен
Експертни настройки	DNS сървъри	DNS сървъри
	Маршрути за препращане	Маршрути за препращане

VPN за всяко приложение

Клиент на VPN

AppTec360 VPN клиент		
Конфигурация на шлюза	Изберете конфигурацията на VPN шлюза (вижте **Общи настройки > Универсален шлюз > Настройки на VPN**).	
VPN приложения	VPN приложения	
Винаги включена VPN услуга	Активиране на функцията Native Lockdown	Винаги включена VPN услуга
Активиране на заключването на AppTec360	Активиране на заключването на AppTec360	

Samsung / Strong Swan			
Тип на връзката	PPTP	Сървър	Сървър
		VPN приложения	VPN приложения
		Потребителско име	Потребителско име
		Парола	Парола
		Активиране на криптирането PPTP	Активиране на криптирането PPTP
	L2TP / IPSec PSK	Сървър	Сървър
		VPN приложения	VPN приложения
		Предварително споделен ключ на IPSec	Предварително споделен ключ на IPSec
		Потребителско име	Потребителско име
		Парола	Парола
		Активиране на L2TP Secret	L2TP Secret
	IPSec XAuth PSK	Сървър	Сървър
		VPN приложения	VPN приложения
		Идентификатор на IPSec	Идентификатор на IPSec
		Предварително споделен ключ на IPSec	Предварително споделен ключ на IPSec
		Потребителско име	Потребителско име
		Парола	Парола
Експертни настройки	DNS сървъри	DNS сървъри	
	Маршрути за препращане	Маршрути за препращане	

Ограничения

Тук можете да зададете ограниченията по отношение на управлението на връзката.

Разрешаване на роуминга на данни	Разрешаване на мобилните данни в роуминг
Налагане на роуминг на данни	Ако е активиран, роумингът за мобилни данни се активира за постоянно (не се препоръчва!) Тази настройка замества настройката "Разрешаване на роуминг на данни"!
Следните настройки са налични само в SAFE 2.x или по-висока версия	
Разрешаване само на спешни повиквания	Разрешаване само на спешни повиквания
Разрешаване на WiFi	Разрешаване на WiFi
Минимално ниво на сигурност на WiFi мрежата	Минимално ниво на сигурност на WiFi мрежата Отворен = разрешени са всички видове WiFi
Забрана на потребителя да добавя WiFi мрежи	Потребителят не може сам да добавя WiFi мрежа Тази настройка е възможна само ако е дефиниран WiFi профил в "Управление на връзките".
Разрешаване на SMS и MMS	Всички = Разрешен е целият SMS и MMS трафик Само входящи SMS = Разрешени са само входящи SMS съобщения Outgoing SMS Only = Разрешени са само изходящи SMS съобщения Няма = Не се разрешава SMS / MMS трафик
Разрешаване на синхронизирането по време на роуминг	Разрешаване на синхронизирането по време на роуминг Включено = активирано Изключено = деактивирано Избор на потребителя = избор на потребителя
Разрешаване на гласовия роуминг	Разрешаване на гласовия роуминг Включено = активирано Изключено = деактивирано Избор на потребителя = избор на потребителя
Използване на системен http прокси сървър	Използването на HTTP прокси сървър, което се осигурява от настройките на системата в настройките, зависи от свързаната мрежа (WiFi или APN).

Управление на PIM

Gmail Exchange

Информация: Тази конфигурация ще бъде приложена към приложението Gmail. Затова трябва да одобрите и инсталирате Gmail.

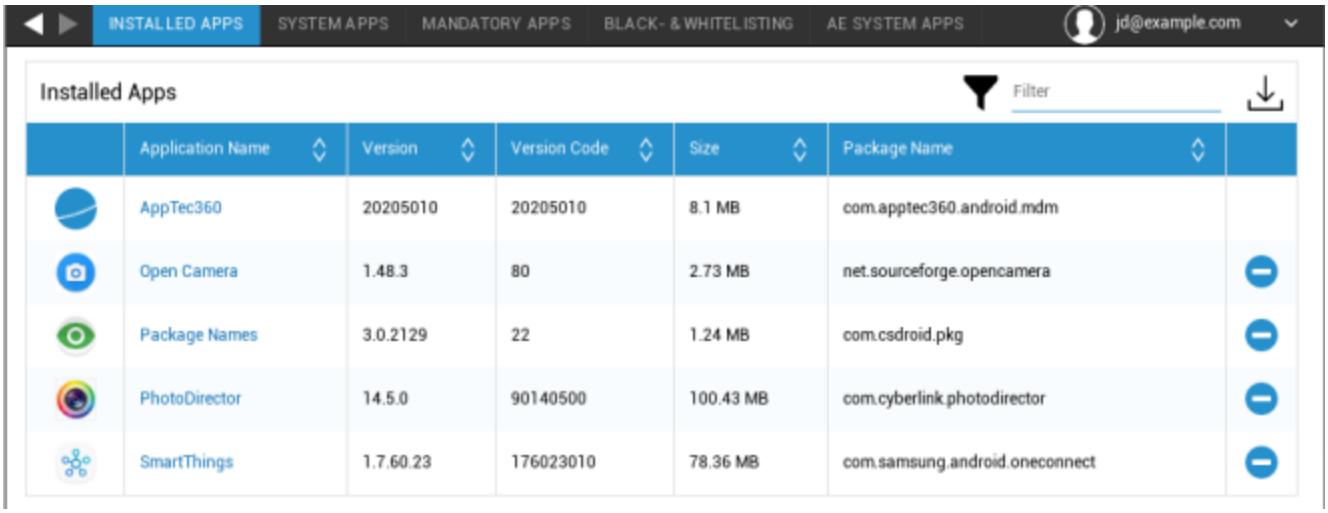
Електронен адрес	Имейл адресът на предоставения потребител Обърнете внимание на "заместителите", които можете да използвате за работа с удостоверенията и да не извършвате промени ръчно на всяко устройство. С едно кликване върху тях можете да ги покажете сами
Име на хоста на сървъра	Адрес на сървъра на вашите сървъри на Exchange
Име за вход	Името за вход за съответното устройство на крайния потребител, моля, обърнете внимание и на "Заместващи символи тук".
Подпис	Може да се приложи подпис (Съвет: Някои устройства изискват HTML форматиране на подписа).
Брой предишни дни за синхронизиране	Брой дни, определящи кога имейлите се синхронизират обратно
Идентификатор на устройството	Ein String der die EAS DeviceID enthält. Dies ist Teil des EAS Protokols und wird in einigen Umgebungen benötigt
Използване на Secure Sockets Layer (SSL)	Използване на SSL връзка
Приемане на всички сертификати	Приемат се всички сертификати. Моля, изберете тази опция, ако вашият Exchange Server използва самоподписан сертификат.

Управление на приложения

Мениджър на корпоративни приложения

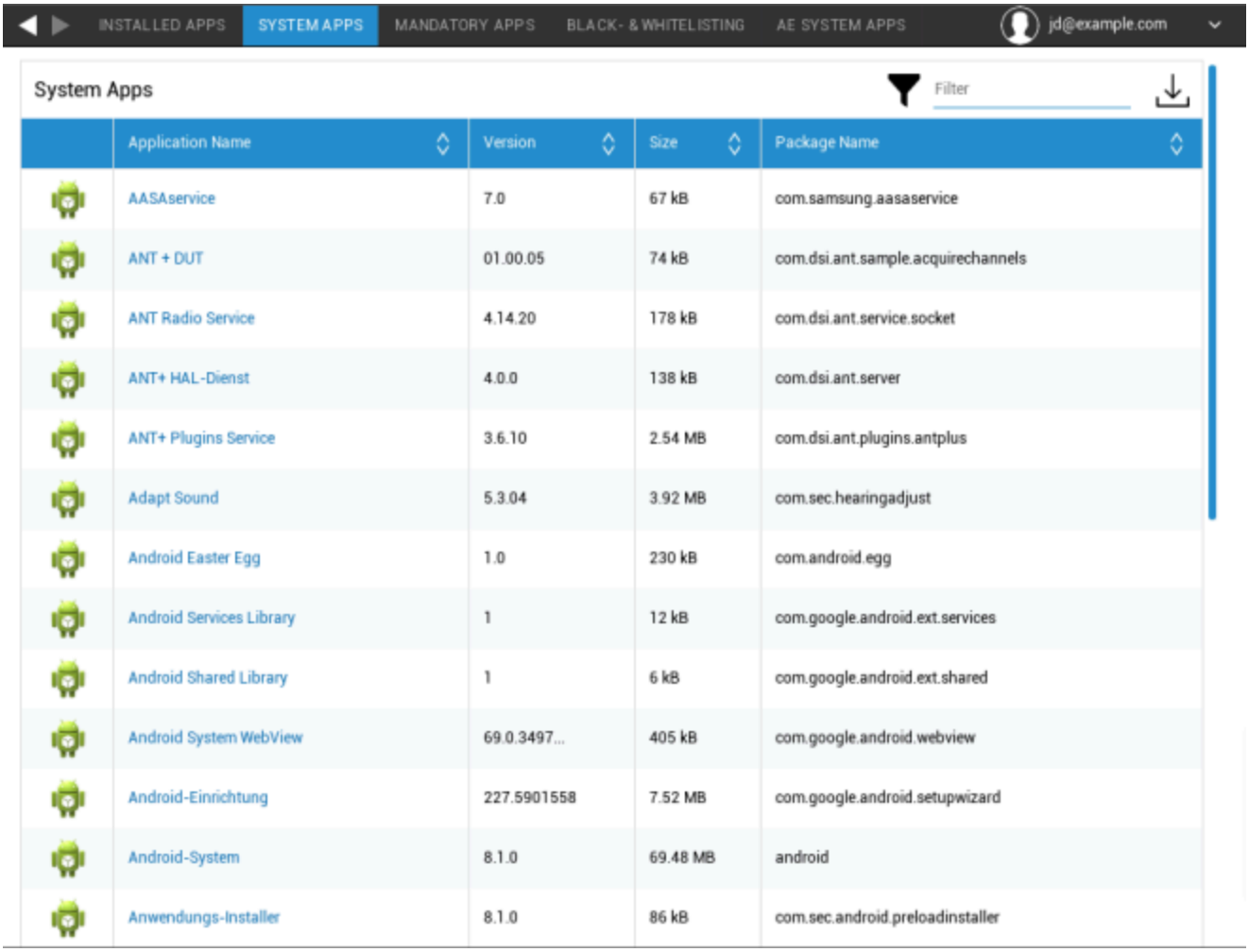
Инсталирани приложения (само на ниво устройство)

Тук ще бъдат показани всички приложения, които в момента са инсталирани на устройството на крайния потребител.



Системни приложения (само на ниво устройство)

В "Системни приложения" ще бъдат изброени всички приложения и услуги, които вече са инсталирани на крайното потребителско устройство от производителя на устройството.



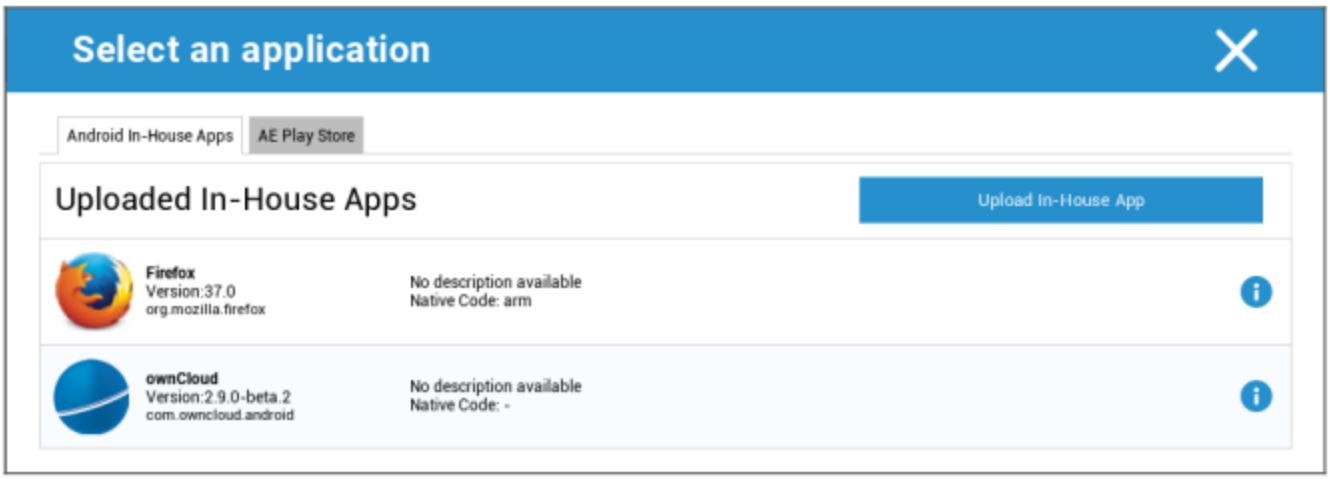
Application Name	Version	Size	Package Name
AASAservice	7.0	67 kB	com.samsung.aasaservice
ANT + DUT	01.00.05	74 kB	com.dsi.ant.sample.acquirechannels
ANT Radio Service	4.14.20	178 kB	com.dsi.ant.service.socket
ANT+ HAL-Dienst	4.0.0	138 kB	com.dsi.ant.server
ANT+ Plugins Service	3.6.10	2.54 MB	com.dsi.ant.plugins.antplus
Adapt Sound	5.3.04	3.92 MB	com.sec.hearingadjust
Android Easter Egg	1.0	230 kB	com.android.egg
Android Services Library	1	12 kB	com.google.android.ext.services
Android Shared Library	1	6 kB	com.google.android.ext.shared
Android System WebView	69.0.3497...	405 kB	com.google.android.webview
Android-Einrichtung	227.5901558	7.52 MB	com.google.android.setupwizard
Android-System	8.1.0	69.48 MB	android
Anwendungs-Installer	8.1.0	86 kB	com.sec.android.preloadinstaller

Задължителни приложения

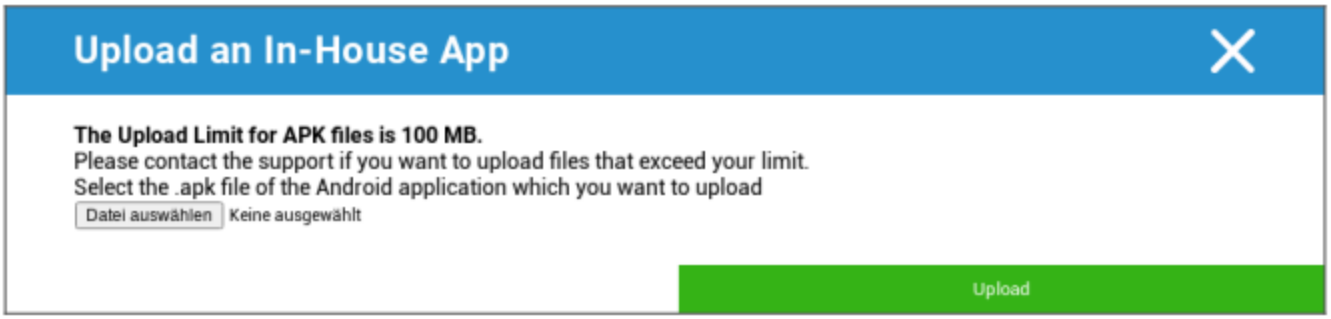
В частта Задължителни приложения можете да зададете задължителните приложения. Потребителят непрекъснато ще бъде подканван да инсталира това определено приложение.

Чрез , може да се определи задължителното изисквано приложение.

Това може да бъде вътрешно приложение от "Вътрешни приложения за Android", което сте качили в Общите настройки.

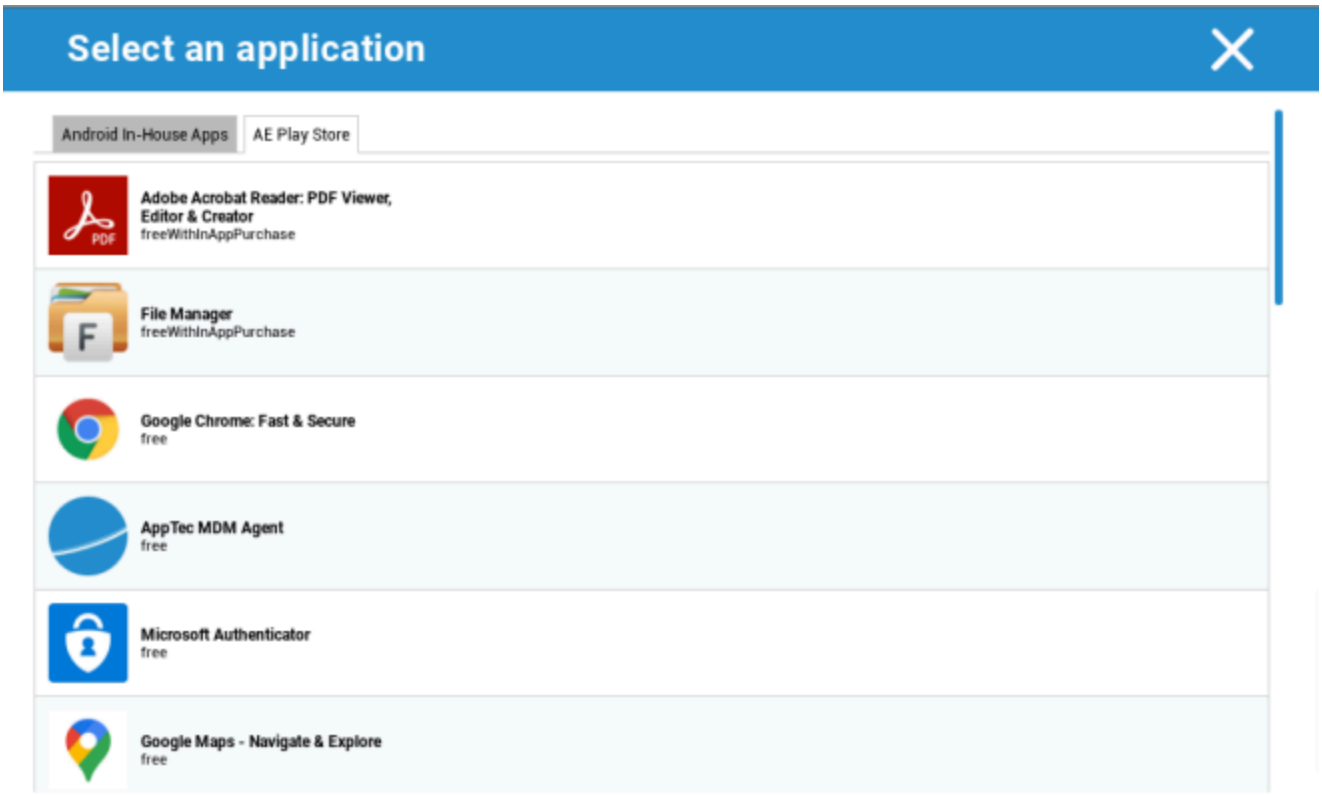


Можете също така директно да изберете и качите apk файл с "Качване на вътрешно приложение".



Ако инсталирате вътрешно приложение, ще имате възможност да активирате опцията "Keep up to date". Ако тази опция е активирана и сте определили по-нова версия в БД на вътрешното приложение, приложението ще бъде актуализирано на устройството.

Или може да бъде приложение "AE Play Store" от работния магазин Play на Google.



Само одобрените "AE Play Store Apps" ще бъдат показани в този раздел.

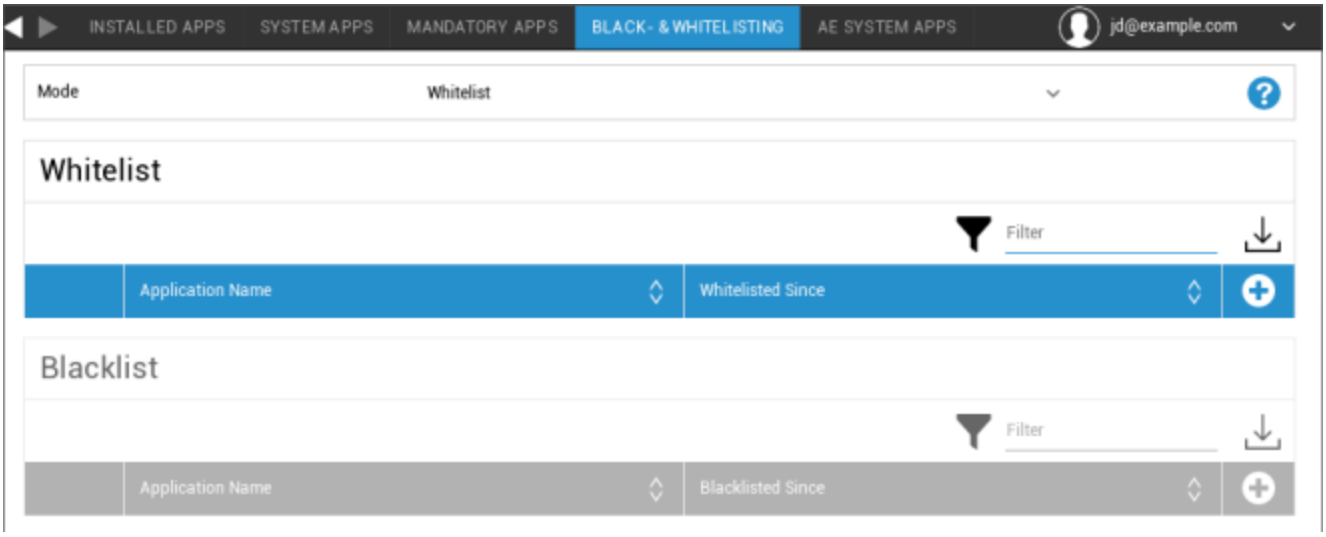
За да одобрите "AE Play Store App", моля, отидете в "Общи настройки" > "Управление на приложения" > "AE Play

Store" и добавете приложение чрез бутона, който ще ви пренасочи към раздела "Play Store Apps" (или можете
директно да отидете в раздела "Play Store Apps").

В раздела "Приложения в Play Store" можете да търсите приложения. Когато щракнете върху дадено приложение, се отваря страницата на приложението
и тук можете да одобрите приложението, като щракнете върху "Approve".

Черни и бели списъци

В "Black- & Whitelisting" (Черен и бял списък) можете да избирате между режим "Whitelist" (Бял списък) и режим "Blacklist" (Черен списък).

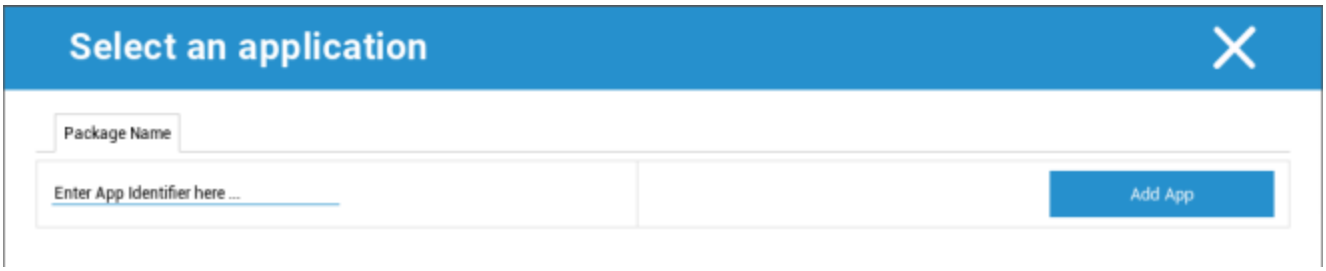


Бял списък	Само приложенията и услугите, които са добавени в списъка, могат да бъдат инсталирани на крайното потребителско устройство. Ако те вече са предварително инсталирани на устройството на крайния потребител, те ще бъдат активирани и настроени, така че потребителят да може да ги стартира.
	Всички останали приложения, които не са добавени в списъка, не могат да бъдат инсталирани на устройството на крайния потребител. Ако те вече са предварително инсталирани на устройството на крайния потребител, те ще бъдат деактивирани и настроени, така че потребителят да не може да ги стартира.
Черен списък	Приложенията и услугите, които са добавени в списъка, не могат да бъдат инсталирани на крайното потребителско устройство. Ако те вече са предварително инсталирани на устройството на крайния потребител, те ще бъдат деактивирани и настроени така, че потребителят да не може да ги стартира.
	Всички останали приложения, които не са добавени в списъка, могат да бъдат инсталирани на устройството на крайния потребител. Ако те вече са предварително инсталирани на устройството на крайния потребител, те ще бъдат активирани и настроени, така че потребителят да може да ги стартира.

Чрез бутона , добавяте допълнителни приложения или услуги към използвания в момента списък.
Чрез бутона , добавяте допълнителни приложения или услуги към неактивния в момента

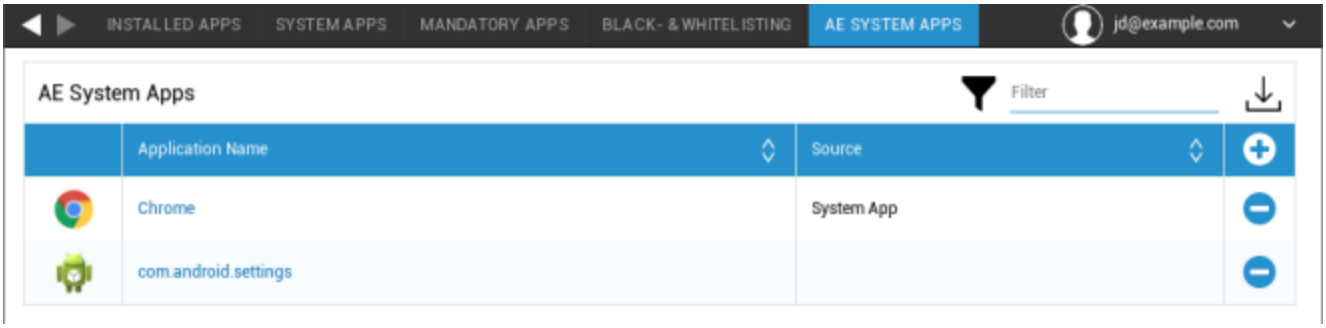
списък.

Можете да дефинирате "Пакетно име":

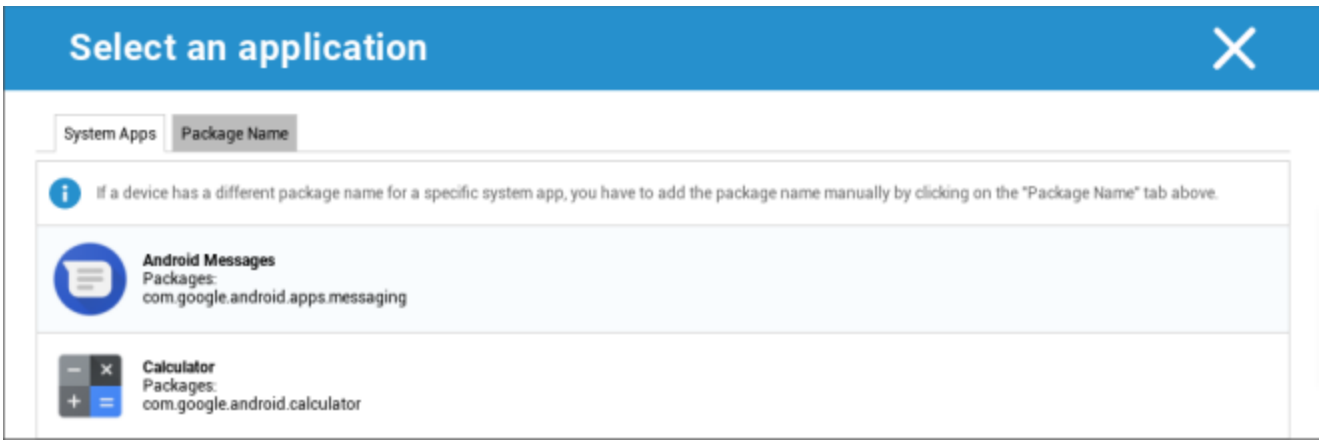


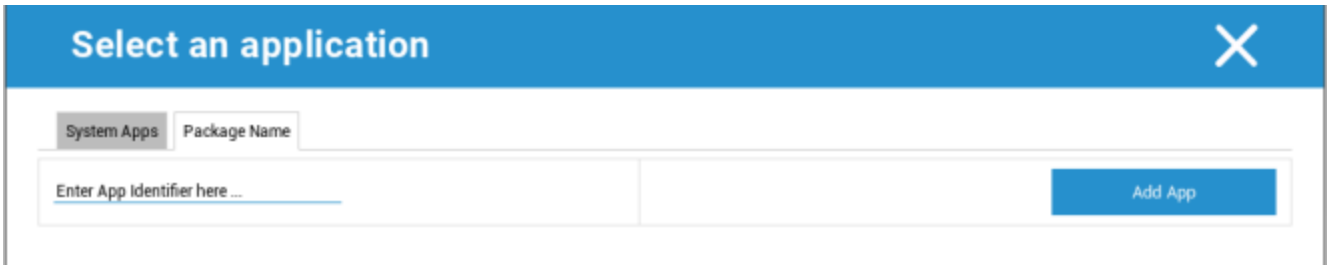
Приложения на системата AE

Тук можете да дефинирате списък, който съдържа конкретни системни приложения, които трябва да бъдат активирани на устройствата.



Ако щракнете върху бутона, можете да изберете от списък с възможни системни приложения, предоставен от Google, или директно да въведете името на пакета на системното приложение, което трябва да бъде активирано.





Имайте предвид, че системните приложения в списъка, предоставен от Google, са само приложения, които могат да бъдат системни приложения, но не е задължително да бъдат системни приложения на вашите устройства.

Този списък обаче засяга само приложения, които вече са предварително инсталирани.

Добавянето на приложения, които не са предварително инсталирани на вашите устройства, няма да се отрази на устройствата ви, независимо дали приложението е от списъка, предоставен от Google, или името на пакета на приложението е въведено директно.

Ограничения и настройки

Настройки за управление на приложения

Тук можете да конфигурирате поведението на устройството по отношение на актуализациите на приложенията.

Честота на проверките за актуализация	Посочете през какъв интервал от време AppTec360 Client ще търси актуализации на приложенията. Стойността по подразбиране е 24 часа.
Праг на Wi-Fi	Приложенията, които са по-големи от определения размер, ще бъдат изтеглени през Wi-Fi. Ако е избрана опцията "Само Wi-Fi", всички приложения ще се изтеглят чрез Wi-Fi.

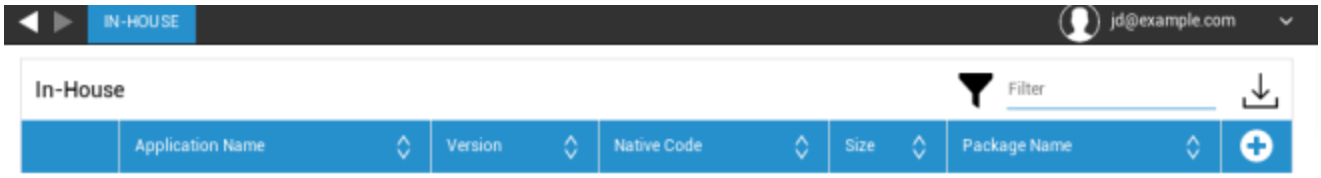
Магазин за корпоративни приложения

Вътрешен

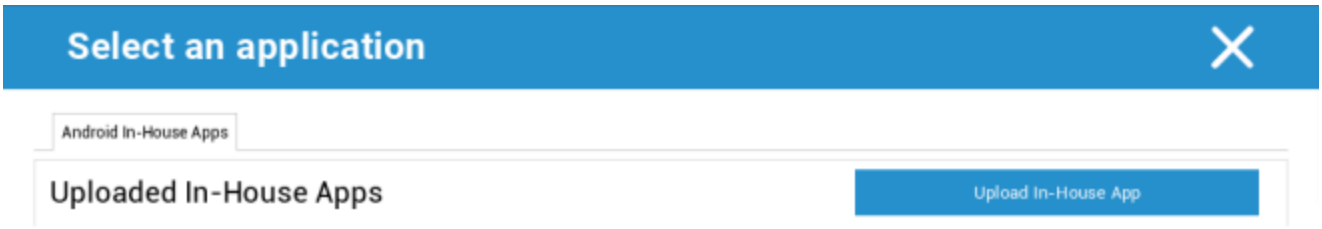
В точката "Собствени" можете да качвате и разпространявате вътрешно разработени приложения.

Със символа можете да разпространявате допълнителни вътрешни приложения.

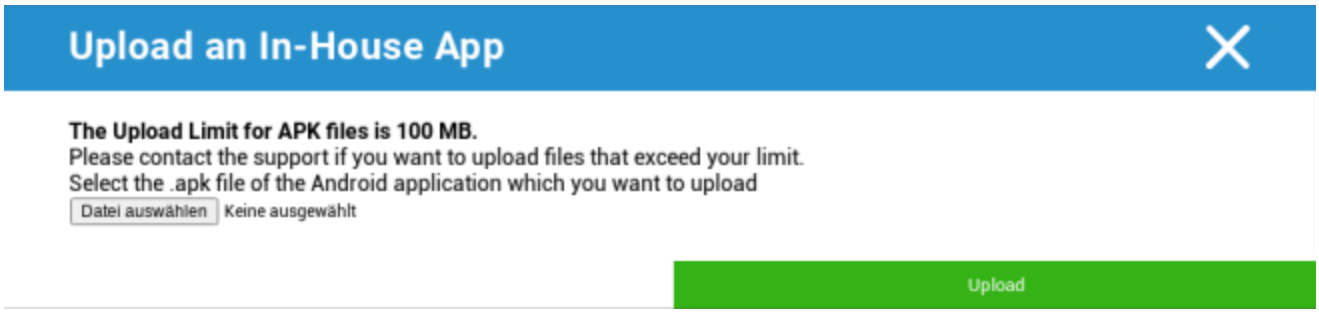
Ако инсталирате вътрешно приложение, ще имате възможност да активирате опцията "Keep up to date". Ако
това е активирано и сте дефинирали по-нова версия в БД на вътрешнофирменото приложение, приложението ще бъде
актуализирано на устройството.



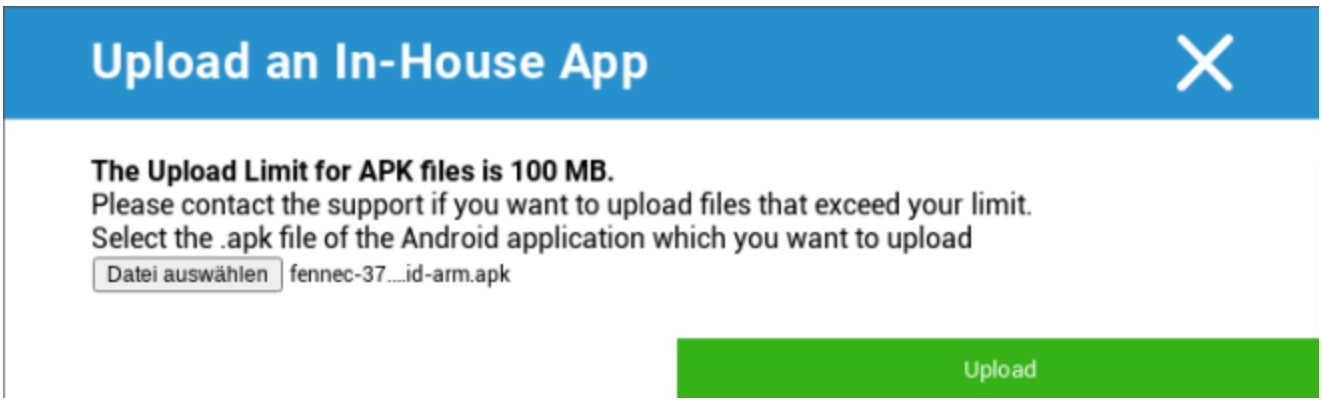
Ако не сте разпространили вътрешни приложения, ще получите следния преглед:


Select an application
Android In-House Apps
Uploaded In-House Apps
Upload In-House App

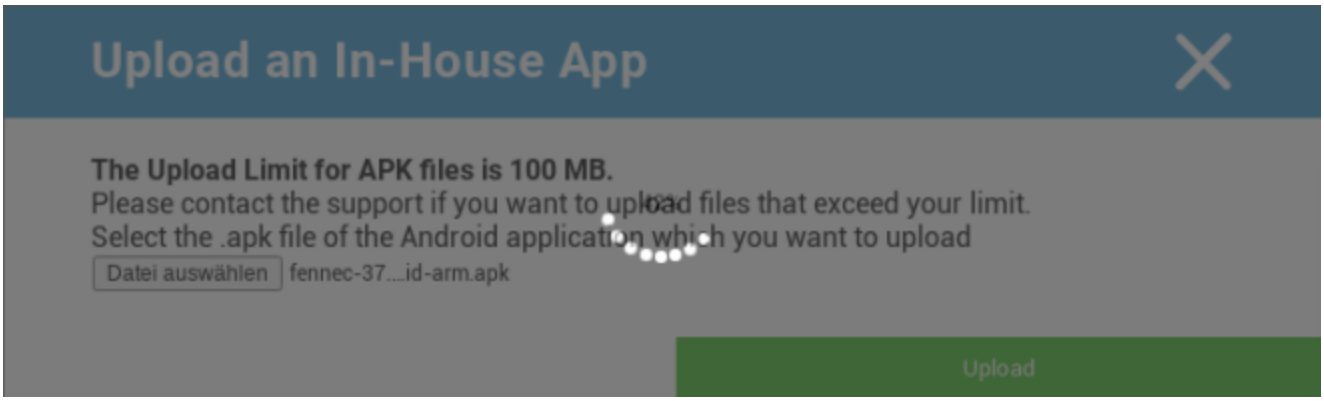
За целта кликнете върху "Upload In-House App" (Качване на вътрешно приложение), след което ще получите следния преглед:



Сега изберете с "Търсене..." .apk файл и след това кликнете върху "Качване".



Приложението ви вече ще бъде качено, а в средата на кръга ще видите индикатор за процент, който показва каква част от приложението ви вече е качена.



Ако качването на вашето вътрешно приложение е било успешно, можете да намерите каченото приложение на адрес
в каталога си с приложения.

Сега потребителят има възможност да види и инсталира това приложение в AppTec360 Store на устройството на крайния потребител
, в категорията "In-House".

Поради факта, че това не включва приложение от Google PlayStore, потребителят не се нуждае от съхранен Google
ID на съответното устройство на крайния потребител.

Магазин Play за предприятия

Магазин за игри AE

Тук можете да добавяте приложения в Android Enterprise Playstore. Моля, имайте предвид, че трябва да одобрите
Apps с вашия AE Administrator Account, преди да можете да ги добавите.

За одобряване на приложение вижте инструкциите в раздел Задължителни приложения.

Режим на киоск и стартиране

Режим на киоск

Режимът Kiosk Mode ви позволява да дефинирате предварително приложение или URL адрес. След това ще бъде възможно единствено да се стартира/посещава това приложение или URL адрес
.

По същия начин различните хардуерни бутони могат да бъдат деактивирани в разнообразния режим Kiosk Mode.

Автоматичен старт	Автоматично стартиране на режима Kiosk, веднага щом профилът достигне до крайното потребителско устройство.
Планиран режим на киоск?	Можете да планирате време за режима на киоск, който ще започва и приключва автоматично в зададено от вас време.
Време на започване	Начален час
Време в минути	Време в минути, след което режимът Kiosk трябва да приключи отново

Тип приложение

Едно приложение	Ако искате да стартирате приложението в режим на киоск, изберете Пакет" под "Тип приложение".
Приложение за киоск	Щракнете тук, за да изберете приложение, което трябва да бъде стартирано в режим Kiosk Mode. Ще намерите обичайния преглед на управлението на приложенията Можете да избирате между "Google Play Store", "Android In-House Apps" и "Packagename".

Тип приложение

URL	Ако искате да стартирате URL адрес в режим на киоск, изберете "URL адрес" под "Тип приложение". След това задайте желания URL адрес
Изчистване на браузъра след неактивност	Тук можете да зададете интервал от време в минути, след който режимът на киоск да се стартира отново.
Изчистване на уеб кеша и бисквитките	Ако активирате тази функция, след рестартиране на киоск режима уеб кешът (бисквитките и кешираните снимки) ще бъде изтрит.
Политика за еднакъв произход	Ако тази функция е активна, потребителят може да сърфира само в подстраниците на определен URL адрес. Например сте дефинирали следния URL адрес:www.mypage.com След това потребителят може да сърфира на: www.mypage.com/subpage
URL адреси в белия списък	Тук можете да поддържате бял списък, в който всички тези URL адреси са разрешени. Максимум 1 URL на ред URL адресът трябва да започва с http:/ или https://
URL адреси в черния списък	Тук можете да поддържате черен списък, в който всички тези URL адреси не са разрешени. Максимум 1 URL на ред URL адресът трябва да започва с http:/ или https://
Ориентация на екрана	Тази настройка е свързана с настройките на екрана Автоматично = автоматично Портрет = вертикален формат Landscape = пейзажен режим

Многофункционално приложение	Ако изберете режима "Multi App" Kiosk Mode, ще се наложи използването на AppTec360 Launcher.
Приложения	Приложение: Изберете Playstore или вътрешно приложение като приложение за киоск. Възможно е също така да въведете име на пакет. Избраното Kiosk Application трябва да е инсталирано на устройството. Не забравяйте да зададете приложението Kiosk Application като задължително. Пряк път на началния екран: Ако е настроено на "Вкл.", ще бъде създаден пряк път на началния екран. Ако е зададена стойност

		"Изкл.", приложението ще се показва в списъка с приложения.

Включена парола за излизане	Ако активирате тази функция, потребителят може да прекрати режима на киоск с предварително зададена от вас парола.
Парола за излизане	Това е предварително зададената от вас парола.
Автоматично сгъване на лентата на състоянието	Ако е разрешено, лентата на състоянието ще бъде автоматично подравнена. С тази опция потребителите могат да виждат информацията в лентата на състоянието, но нямат достъп до нейните функции.
Деактивиране на лентата на състоянието	Лентата на състоянието съдържа Известия, Преки пътища и Информация. Налично само за устройства на Samsung със SAFE 4.0 или по-нова версия.
Деактивиране на клавишите за сила на звука	Деактивиране на клавишите за регулиране на звука (налично само за устройства на Samsung с версия SAFE 3.0 или по-висока)
Деактивиране на превключвателя за включване и изключване	Деактивиране на превключвателя за включване/изключване (налично само за устройства на Samsung с версия SAFE 3.0 или по-висока)
Деактивиране на бутона Home	Деактивиране на бутона Home. Ако тази функция е активирана, режимът Kiosk може да бъде прекратен само в конзолата AppTec360. (достъпно само за устройства на Samsung с версия SAFE 3.0 или по-висока)
Деактивиране на лентата за навигация	С тази опция можете да деактивирате лентата за навигация (Назад / Меню). Ако тази функция е активирана, режимът Kiosk може да бъде прекратен само в конзолата AppTec360. (достъпно само за устройства на Samsung с версия SAFE 3.0 или по-висока)

AppTec360 Launcher

Активиране на AppTec360 Launcher	На: Включва стартиращото устройство AppTec360. Потребителят трябва да го зададе като стартер по подразбиране еднократно. Забележка: Ако режимът Kiosk Mode е активиран и режимът Kiosk Mode е настроен на "Multi App", използването на AppTec360 launcher ще бъде наложено.
Големи икони	На: Показване на по-голяма версия на иконите на приложенията в лентата за стартиране
Скриване на иконата на приложението AppTec360	На: Скрива напълно приложението AppTec360
Скриване на иконата на магазина AppTec360	На: Скрива напълно AppTec360 Enterprise AppStore

Настройки на AppTec360

Активиране на приложението за настройки на AppTec360	Приложението за настройки на AppTec360 осигурява управление на WiFi и Bluetooth връзките
Активиране на настройките в Multi App Режим на киоск	Ако е разрешено, потребителите могат да получат достъп до приложението AppTec360 Settings, докато режимът Multi App Kiosk Mode е активен.

Дистанционно управление

Splashtop

За да стартирате сесия за дистанционно управление на устройството си, приложението "Splashtop Streamer" трябва да бъде инсталирано на устройството, като добавите приложението към **Управление на приложенията → Мениджър на корпоративни приложения → Задължителни приложения**.

След това конфигурирайте следните настройки за Splashtop:

Активиране на Splashtop	Ако е разрешено, AppTec360 ще конфигурира приложението Splashtop, за да позволи дистанционно управление
Разгръщане на кода	Отидете на https://my.splashtop.com и влезте в акаунта си в Splashtop. Щракнете върху "Add Computer" (Добавяне на компютър) и копирайте 12-цифрения код за разполагане от получената страница.
Задаване на потребителски шлюз за внедряване?	Внедряване на шлюз
Внедряване на шлюз домейн / хост	Внедряване на шлюз
Проверка на сертификат	Проверка на сертификат

След това можете да използвате опцията Splashtop Remote Control в контекстното меню (зъбно колело до лентата за търсене, когато устройството е избрано, или щракване с десния бутон на мишката върху устройството в дървото), за да стартирате сесия за дистанционно управление.

TeamViewer

За да стартирате сесия за дистанционно управление на устройството си, приложението "TeamViewer QuickSupport" трябва да бъде инсталирано на устройството, като добавите приложението към **Управление на приложенията → Мениджър на корпоративни приложения → Задължителни приложения**.

След това можете да използвате опцията **TeamViewer Remote Control** в контекстното меню (зъбно колело до лентата за търсене, когато устройството е избрано, или щракване с десния бутон на мишката върху устройството в дървото), за да стартирате сесия за дистанционно управление.

Управление на съдържанието

ContentBox

Тук можете да активирате ContentBox.

Веднага след като превключите "Enable ContentBox" на "On", на крайното потребителско устройство автоматично ще бъде инсталирано отделно приложение ContentBox
.

Сигурен браузър

Тук можете да конфигурирате настройките за AppTec360 Secure Browser.

Щом превключите раздела в "Secure Browser" на "On", на крайното потребителско устройство автоматично ще бъде инсталирано отделно приложение за браузър
.

Изискване на парола	Изисквайте от потребителя да зададе и използва парола за достъп до браузъра.
Минимална необходима дължина на паролата	Задаване на необходимия брой символи за паролата
Изисквано качество на паролата	Задайте необходимото качество на паролата
Ограничаване на изтеглянията / Отваряне в	
Ограничаване на качванията	
Качване на бял списък	Списък с URL адреси, чието качване винаги ще бъде разрешено.
Разрешаване на копирането	Позволява копиране, изрязване или споделяне на текст в уеб страниците.
Разрешаване на заснемането на екрана	Позволява заснемане на скрийншоти.
Честота на почистване на данните	Изберете с каква честота ВСИЧКИ потребителски данни (история, кеш и т.н.) да се премахват автоматично.
Фирмени отметки	Записките ще се появят в папката "Company bookmarks" (Записки на компанията) в отметките на браузъра. Те не могат да се редактират от потребителя.
Скриване на адресната лента	
Бели списъци в браузъра (без Universal Gateway)	Активира бял списък на URL адреси от страна на клиента. • Фирмените отметки винаги са в белия списък • Поддържа се само за 100 URL адреса • Моля, използвайте Универсалния шлюз за неограничен черен и бял списък

URL адреси в белия списък	Списък на разрешените URL адреси.
Базиран на шлюз черен и бял списък	Черният списък има следните изисквания: • Работещ универсален шлюз на AppTec360 ("Общи настройки" → "Универсален шлюз") • Работеща VPN конфигурация с определен DNS сървър ("Общи настройки" → "Универсален шлюз" → "VPN настройки") • Конфигуриране на черен списък ("Общи настройки" → "Универсален шлюз" → "Черен списък на домейни") • Валидна VPN връзка в профила ("Управление на връзките" → "VPN")

Допълнителен API

Samsung KNOX

Ограничения

Разрешаване на SD карта	
Разрешаване на запис в SD картата	
Разрешаване на заснемането на екрана	
Разрешаване на клипборда	
Архивиране на настройките и данните на приложението в Google Cloud	
Възстановяване на настройките от Google Cloud при преинсталиране на приложение	
Разрешаване на дебъгването на USB	
Разрешаване на Google Crash Report	
Разрешаване на фабричното нулиране	
Разрешаване на актуализация OTA	
Разрешаване на съхранението в USB хост	Ако е разрешено, потребителят може да свърже всяко устройство за писане (преносимо USB устройство за съхранение), външен HD или четец на карти Secure Digital (SD) и то се монтира като устройство за съхранение в устройството.
Разрешаване на USB мултимедиен плейър (MTP,PTP)	
Разрешаване на микрофон	Деактивиране на микрофона за приложения на трети страни

Разрешаване на NFC (Near Field Communication)	
Разрешаване на неизвестни източници (APK Sideloading)	Ако е разрешено, страничното зареждане на приложения (APK файлове) е разрешено. След като тази настройка е деактивирана, потребителят трябва да я активира ръчно, когато разрешите инсталирането на APK файлове от непознати източници.
Разрешаване на създаването на потребители	Ако е разрешено, на потребителя се разрешава да създава множество акаунти в устройството, например акаунти за гости.

Имейл

Електронен адрес	
Протокол на входящия сървър	
Адрес на входящия сървър	
Входящ порт на сървъра	
Вход/потребителско име на входящия сървър	
Парола на входящия сървър	
Входящият сървър използва SSL	
Входящият сървър използва TLS	
Входящият сървър приема всички сертификати	
Протокол на изходящия сървър	
Адрес на изходящия сървър	
Порт на изходящия сървър	
Изходящият сървър използва допълнителни пълномощия	Ако е деактивирана, системата използва входящите идентификационни данни и за изходящия сървър.
Вход/потребителско име на изходящия сървър	
Парола на изходящия сървър	
Изходящият сървър използва SSL	
Изходящият сървър използва TLS	
Изходящият сървър приема всички сертификати	
Задаване на подпис	
Подпис	Забележка: За някои устройства подписът трябва да бъде зададен във формат HTML.
Уведомяване на потребителя при получаване на нова електронна поща	

Обмен

Електронен адрес	
Име на хоста на сървъра	Името на хоста на сървъра Exchange
Име за вход	Потребителското име, което се използва за влизане в сървъра на Exchange
Домейн	Ако е активирана конфигурация на ACL шлюза и полето Domain не е празно, AppTec360 Universal Gateway ще удостовери устройството със следното име "Domain\Login Name
Парола	
Брой предишни дни за синхронизиране	
Честота на синхронизиране на електронната поща	
Синхронизиране в роуминг	
Задаване на подпис	
Подпис	Забележка: За някои устройства подписът трябва да бъде зададен във формат HTML.
Акаунт по подразбиране	
Използване на Secure Sockets Layer (SSL)	
Използване на защита на транспортния слой (TLS)	
Приемане на всички сертификати	

APN

Наименование на APN	
Име на точката за достъп	Име на APN
Протокол на изходящия сървър	
MCC - код на мобилната държава	Оставете празно, за да използвате mmc на инсталираната SIM карта
MNC - Код на мобилната мрежа	Оставете празно, за да използвате mnc на инсталираната SIM карта
Адрес на сървъра	
Номер на порта на сървъра	
Прокси адрес на сървъра	
Адрес на MMS сървъра	Оставете празно за подразбиране
Номер на MMS порта	Оставете празно за подразбиране
MMS прокси адрес	Оставете празно за подразбиране
Потребителско име	
Парола	
Тип точка за достъп	Приетите типове са "default", "mms", "supl".
	Ако се подаде нула или празен, по подразбиране се използва "default,supl,mms".
	Оставете празно за подразбиране.
Предпочитана APN	

Bluetooth

Разрешаване на откриването на устройство чрез Bluetooth	
Разрешаване на Bluetooth сдвояване	
Разрешаване на устройства с Bluetooth слушалки	
Разрешаване на Bluetooth устройствата със свободни ръце	
Разрешаване на Bluetooth A2DP устройства	A2DP, профил за усъвършенствано разпространение на звук, позволява поточно предаване на звук между устройства
Разрешаване на изходящи повиквания	
Разрешаване на прехвърлянето на данни чрез Bluetooth	
Разрешаване на Bluetooth тетъринг	
Разрешаване на връзката с компютър чрез Bluetooth	

Връзка

Разрешаване само на спешни повикванияРазрешаване на Wi-Fi	
Минимално ниво на сигурност на Wi-Fi мрежата	
Забрана на потребителя да добавя Wi-Fi мрежи	Това ограничение може да бъде активирано само ако в раздел Управление на връзките е дефиниран поне един активен Wi-Fi профил.
Разрешаване на SMS и MMS	
Разрешаване на синхронизирането по време на роуминг	
Разрешаване на гласовия роуминг	

Android Enterprise – Напълно управлявано устройство с работен профил (COPE)

Общо обяснение на COPE

COPE е съкращение от **Corporate Owned Personally Enabled**(**корпоративно притежавана персонална услуга**).

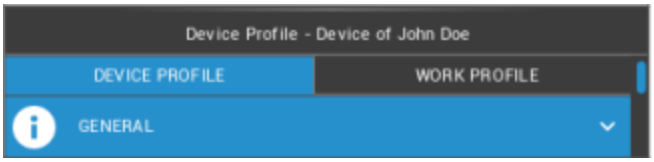
Режимът COPE позволява дадено устройство с Android да бъде записано като **Android Enterprise - напълно управлявано устройство** с интегриран профил **Android Enterprise - контейнер**.

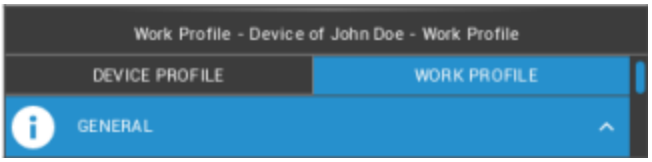
Това може да бъде или устройство с Android, което вече е регистрирано като **Android Enterprise - Напълно управляемо устройство** и на което допълнително е създаден **Android Enterprise - Контейнер**, или новорегистрирано устройство с Android, което е директно регистрирано като **Android Enterprise - Напълно управляемо устройство** заедно с **Android Enterprise - Контейнер** върху него.

Режимът COPE е наличен само за устройства с Android 8, 9 и 10

Конфигуриране на профили за устройства COPE

Тъй като за самия режим COPE няма профил за конфигуриране, конфигурирането на **Android Enterprise - напълно управлявано устройство** и **Android Enterprise - контейнер** е разделено на два профила в рамките на профила COPE. Възможно е да се превключва между двата профила за конфигурация на всеки профил, като се щракне върху съответния бутон в лявата част на конзолата:





И двата профила могат да бъдат конфигурирани, както е описано за всеки отделен профил:

Android Enterprise - Напълно управлявано устройство

Android Enterprise - Контейнер

Връщане към AE напълно управлявано устройство

Профилът **Android Enterprise - Container** може да бъде премахнат, както е описано в **Управление на мобилни устройства**.

С премахването на профила Container профилът COPE ще бъде трансформиран в профил **Android Enterprise - Fully Managed Device**.

Android Enterprise – Конфигуриране на контейнери

В зависимост от това дали в момента сте избрали групов профил или устройство, прегледът и неговите подточки се различават - моля, обърнете внимание на това!

Обща информация

Преглед на профила (само на ниво профил)

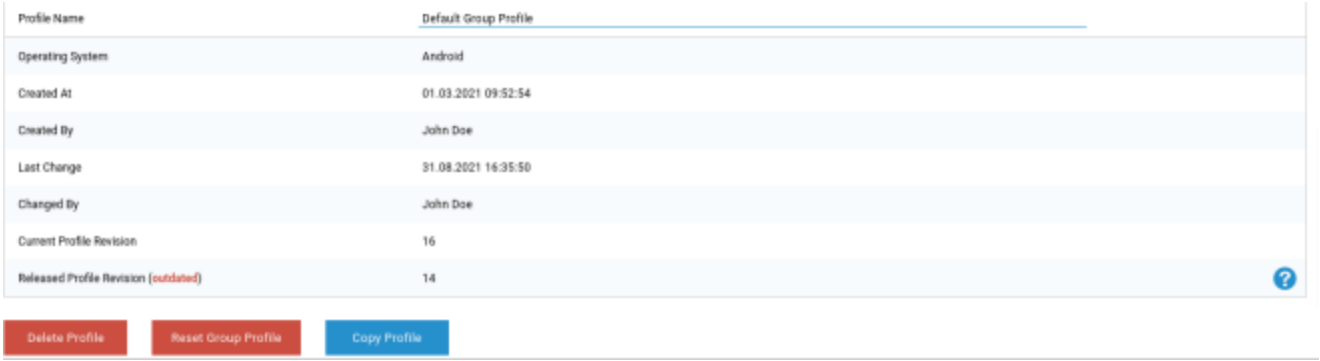
Ако се намирате в даден профил, ще получите кратък преглед на профила по отношение на име, операционна система, дата на създаване, автор и т.н.

Име на профила	Име на профила - може да се преименува директно тук
Операционна система	Валидна операционна система за профила
Създаден в	Дата на създаване
Създаден от	Създаден от
Последна промяна	Дата на последната промяна
Променено от	Потребителят, който е извършил последните промени в този профил
Текуща ревизия на профила	Брой пъти, в които профилът вече е бил актуализиран
Освободена ревизия на профила	Брой пъти, в които профилът вече е бил актуализиран и са му били присвоени устройства

Изтриване на профил	Изтриване на профил
Нулиране на профила на групата	Нулиране на профила на групата
Копиране на профил	Копиране на профил

Преглед на профила на групата (само на ниво група)

При отваряне на групов профил ще получите бърз преглед на профила.



Име на профила	Име на профила (може да бъде променено тук)
Операционна система	Операционна система, за която е предназначен профилът
Създаден в	Време на създаване
Създаден от	Създател на профила
Последна промяна	Време на последната промяна в профила
Променено от	Акаунт, в който са направени последните промени
Текуща ревизия на профила	Преразглеждане на запазеното състояние на профила
Освободена ревизия на профила	Присвоена ревизия на профила ("Присвои сега"). Ако етикетът показва " (остарял)" зад текста, това означава, че сте запазили профила, но все още не сте го назначили, така че устройствата все още ще получават по-стара версия.

Преглед на устройството (само на ниво устройство)

Ако се намирате на устройство, ще получите обобщаващ преглед на избраното устройство, като тук се съдържа следното:

Име на устройството	Име на устройството
Местоположение	Координати на местоположението
Телефонен номер	Телефонен номер
Зададени задължителни приложения	Брой зададени задължителни приложения
Версия на операционната система	Версия на операционната система на устройството
Операционна система	Операционна система (Android Enterprise)
Сериен номер	Сериен номер на устройството
Притежание на устройство	Корпоративно или частно устройство
Тип устройство	Управлявано устройство AE Work
Вкоренени	Състояние, показващо дали устройството е било рутирано
Съответстващ	Съответствие с насоките
IP адрес	IP адрес на устройството
Последно видян	Точка във времето, когато устройството се е свързало за последен път с AppTec
Последен тласък	Точка във времето, в която е изпратено последното натискане към устройството
Присвояване на потребителя	Потребителят или групата, към която е назначено това устройство

Ревизия на конфигурацията

Тук можете да видите кой групов профил е зададен на устройството.

Ако щракнете върху груповия профил, ще получите директен достъп до този профил и ще можете да извършвате настройки.

С този символ можете да върнете разпределените приложения към настройките на груповия профил.

С този символ можете да върнете всички използвани приложения към настройките на груповия профил.

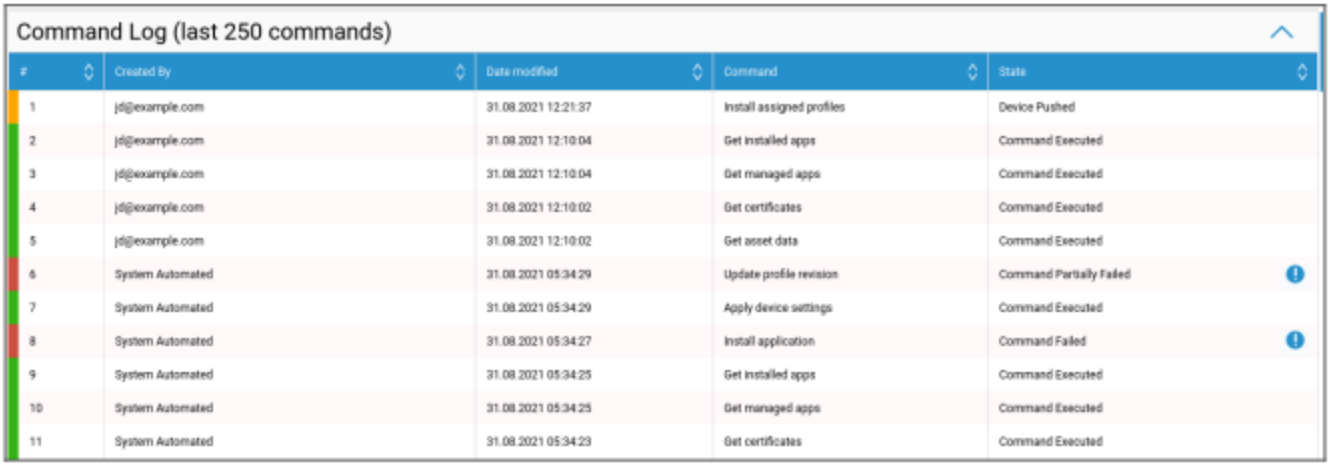
"Налична е по-нова ревизия" показва, че профилът на групата е променен и запазен, но не е присвоен. Груповият профил трябва да бъде присвоен с "Assign now" (Присвояване сега) на ниво група, за да се приложат промените към устройствата.

Дневник на устройството (само на ниво устройство)

Тук ще получите различни регистри на устройствата. Ако е необходимо, можете директно да откриете причината за дадена грешка тук.

Дневник на командите

Тук можете да видите кои команди са издадени за устройството и какво е тяхното състояние.



Възможни състояния на командата

Натиснато устройство	Изпратена е заявка за натискане до услугата за натискане (напр. APNS), за да се каже на устройството да се свърже отново със сървъра на EMM.
Създадена команда	Командата е създадена в системата.
Изпратена команда	Командата е изпратена на устройството, след като то се е свързало със сървъра.
Изпълнена команда	Командата е изпълнена успешно.
Командата е неуспешна	Командата не е изпълнена. *
Командата е частично неуспешна	В зависимост от операционната система на устройството някои команди могат да бъдат групирани заедно. При това някои части от тази група команди не успяха. *
Командата е изпълнена, но в крайна сметка е неуспешна	Командата е изпълнена, но може би не е.
Пренасочване на командата	Командата е била изпратена отново от потребител.
Изхвърлени	Командата беше отхвърлена. Например защото е била заменена от друга команда или устройството е било презаписано и старите команди са били премахнати.

*Ако зад съобщението има възклицателен знак, можете да получите повече информация, като задържите курсора върху иконата.

Настройки на устройството

Конфигурация на клиента

Тук можете да извършите следните конфигурации на вашето устройство с Android:

Време за несъответствие	Ограничението на времето за отговор на потребителя, след което се прилага действието за изпълнение.
Действия по изпълнение след изтичане на срока за изпълнение	Действия по прилагане, когато потребителят не извършва действия, които водят до статус на съвместимо устройство
Честота на събиране на данни	Честота на събиране на информация за устройствата/GPS
Честота на сърдечния ритъм на устройството	Интервал, през който устройството трябва да се свърже със сървъра AppTec Мин. 1 минута Макс. 24 часа
Активиране на актуализациите на местоположението	Ако е активирано, устройството изпраща актуализации на местоположението към сървъра AppTec
Време за актуализация на местоположението	Определя през какви интервали от време устройството изпраща актуализации на местоположението към AppTec
Използване на Google Location Accuracy за актуализация на местоположението	Ако е активирано, местоположението в мрежата ще се използва за актуализации на местоположението (ако е деактивирано в "Ограничения", тази настройка няма да повлияе на нищо).
Използване на GPS местоположение за актуализиране на местоположението	Ако е активирано, GPS ще се използва за актуализации на местоположението.
Разрешаване на имитационни (фалшиви) местоположения	Позволява подправяне на информация за местоположението чрез приложения на трети страни

Действие при изгубена връзка	Ако е разрешено, можете да зададете действие в случай, че дадено устройство не получи връзка с MDM сървъра през интервала за сърдечен ритъм. Например, ако устройството има интервал на сърдечния ритъм от 5 минути, то се свързва със сървъра в 10:35 ч. След това устройството напуска обхвата на Wi-Fi. Следващият сърдечен ритъм в 10:40 ч. няма да успее и ще бъде изпълнено посоченото действие.
Действие	Действието, което трябва да се предприеме, когато дадено устройство стане несъответстващо на изискванията. • Lock Устройство = устройство за заключване • Изтриване на устройството = устройството ще бъде възстановено до фабричните настройки • Изтриване на устройството и SD картата = устройството ще бъде възстановено до фабричните настройки, а паметта на SD картата ще бъде изтрита
Праг	Можете да зададете праг на неуспешните сърдечни удари, които са необходими за задействане на посоченото действие.

Режим на прилагане на политиката	По подразбиране:	Потребителите ще бъдат подканени периодично да изпълнят неизпълнени действия.
	Лениво прилагане на политики:	Потребителите никога няма да бъдат подканени да изпълнят неизпълнени действия. Всички отворени действия ще бъдат показани в AppTec Client.
	Агресивно прилагане на политики:	Потребителите ще бъдат подканвани непрекъснато да изпълняват неизпълнени действия.
Заключване на версията на AppTec	Ако е разрешено, може да се зададе код на версията на приложението AppTec. Клиентът на AppTec ще се актуализира само до посочената версия. По-новите версии ще бъдат игнорирани. Не е възможно да се извърши понижаване на версията.	
Код на версията	Код на версията на приложението AppTec, към която трябва да бъде заключено.	
Деактивиране на известието AppTec	Ако е деактивиран, AppTec Client няма да показва известие в лентата за известия. По този начин потребителите могат да затворят AppTec клиента чрез мениджъра на задачите. Ако клиентът AppTec е затворен, няколко	

	функции, включително Kiosk Mode (Режим на киоск) и App Black/Whitelisting (Черен/бял списък на приложения), няма да работят правилно. Устройствата на Samsung предлагат механизъм за защита на AppTec Client. Известието е деактивирано по подразбиране на устройствата на Samsung, които поддържат приложните програмни интерфейси KNOX. Известието не трябва да бъде деактивирано на устройства с Android 8.0 или по-нова версия.

Тапети

Задаване на персонализиран тапет	Активиране/деактивиране на персонализирания тапет
Тапети	Задаване на режима на тапета за използване на цветен код или изображение
Определяне на цвят	Посочете цвят на фона като шестнадесетична стойност, например #000000 за черно или #ffffff за бяло.
Задаване на изображение като тапет	Качете файла с изображението, което искате да използвате като тапет

Управление на активи (само на ниво устройство)

Информация за устройството

Модел	Обозначение на модела на устройството
Операционна система	OS
Версия на операционната система	Версия на операционната система
Сериен номер	Сериен номер
Име на устройството	Име на устройството
Състояние на батерията	Състояние на батерията
Свободна / обща памет	Свободна / обща памет
Samsung Safe	Интерфейс Samsung SAFE, необходим за различни опции за настройка
Налична SD карта	Налична SD карта
Емулирана SD карта	Емулирана SD карта
Сменяема SD карта	Сменяема SD карта
SD Свободна / обща памет	SD Свободна / обща памет на SD картата

Wi-Fi

IP адрес	IP адрес на устройството
WiFi MAC	WiFi MAC адрес

Клетъчен

Статус	Състояние (инсталирана SIM карта)
Телефонен номер	Телефонен номер
Роуминг (глас/данни)	Роуминг за глас/данни
Състояние на роуминга	Текущо състояние на роуминга
IP адрес	IP адрес
Оператор/превозвач	Оператор/превозвач
Клетъчна технология	Клетъчна технология
IMEI	Номер на IMEI
ICCID	Това е идентификационният номер на SIM картата, често наричана също Smartcard или Integrated Circuit Card (ICC).
IMSI	Международният идентификатор на мобилния абонат (IMSI) осигурява в мобилните мрежи GSM и UMTS точна идентификация на потребителите на мрежата. IMSI се състои от максимум 15 цифри и се конфигурира по следния начин: • Код на мобилната държава (MCC), 3 цифри • Код на мобилната мрежа (MNC), 2 или 3 цифри • Идентификационен номер на мобилен абонат (MSIN), 1-10 цифри
Текущи MCC/MNC	Вижте "SIM MCC/MNC".
SIM MCC/MNC	Кодът на мобилната държава е установен идентификатор на държавата, определен от ITU съгласно стандарт E.212. Той се използва заедно с кода на мобилната мрежа (MNC) за идентифициране на мобилната мрежа. Означава кода на страната/кода на мобилната мрежа на SIM картата. Ако сте в роуминг в друга мобилна мрежа, логично е "Current MCC/MNC" и "SIM MCC/MNC" да са различни.

Bluetooth

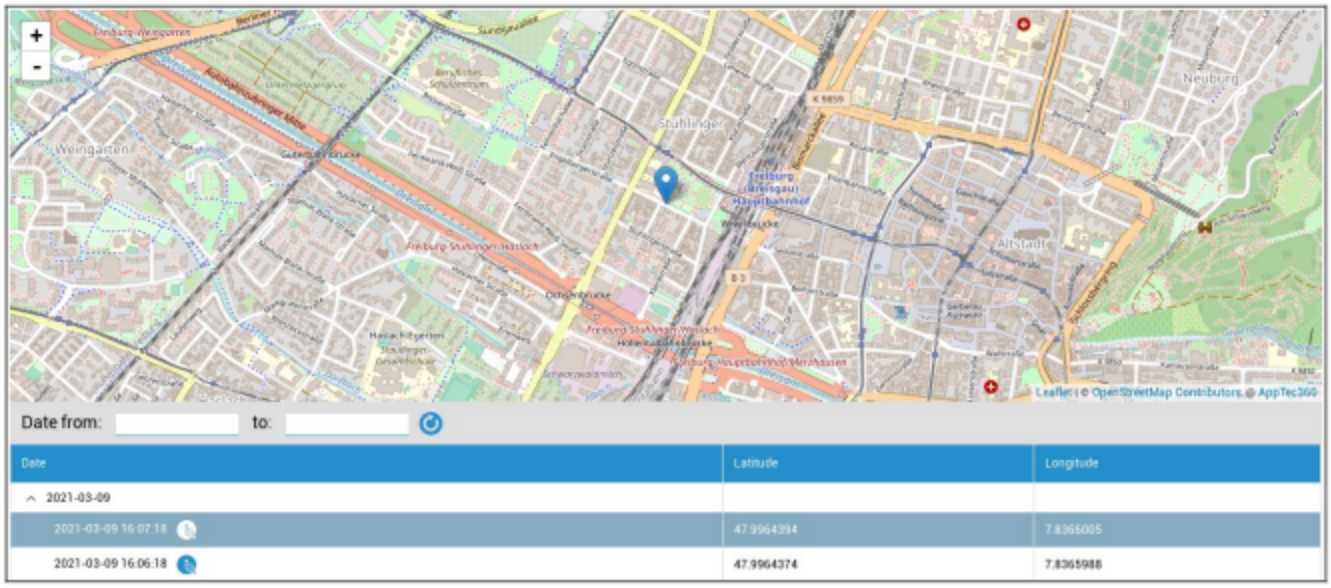
Bluetooth MAC	Bluetooth MAC адрес

Управление на сигурността

Защита от кражба (само на ниво устройство)

GPS информация (само на ниво устройство)

Тук можете да определите текущото/последното местоположение на устройството. Локализирането може да бъде защитено с една или дори две пароли - вж: Общи настройки - Поверителност - Достъп до GPS



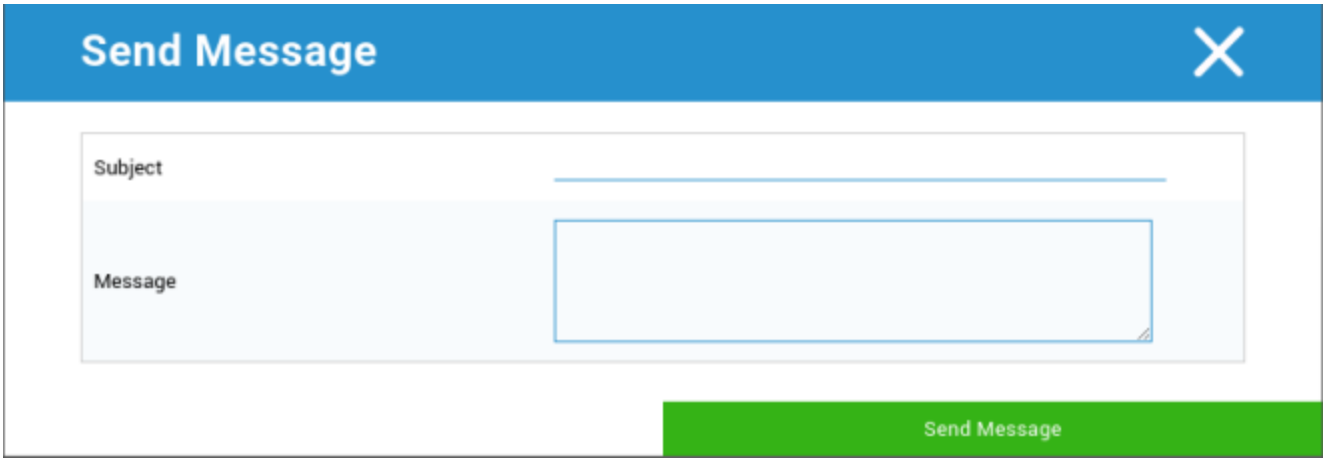
Изтриване и заключване (само на ниво устройство)

В "Изтриване и заключване" можете да извършите следните три действия:

Пълно избърсване	Устройството се възстановява до фабричните си настройки (корпоративните и личните данни се изтриват). Работи само за подобрен работен профил
Изтриване на предприятието	От устройството на крайния потребител се премахват само корпоративните данни (всички приложения, данни и т.н., които са били предоставени от AppTec)
Екран за заключване	Активирано е заключване на екрана, достатъчно е да отключите устройството с паролата на устройството/ ПИН кода.

Съобщение (само на ниво устройство)

Тук можете да попълните темата и съобщението и да го изпратите на крайно потребителско устройство.



Конфигурация на сигурността

Парола на устройството

В "Парола" можете да зададете парола на устройството, като имате на разположение следните опции за настройка

Минимална дължина на паролата	Определя минималния брой символи, които трябва да съдържа паролата.	
Качество на паролата	Неуточнено	Тази политика няма изисквания за паролата.
	Биометрични данни Слаби	Тази политика позволява използването на биометрични технологии за разпознаване с ниска степен на сигурност. Това означава технологии, които могат да разпознаят самоличността на дадено лице до около трицифрен ПИН код (фалшивото разпознаване е по-малко от 1 на 1000).
	Нещо	Тази политика изисква задаването на някакъв вид парола или шаблон, но не налага никакви конкретни правила.
	Азбучен	Потребителят трябва да е въвел парола, съдържаща поне буквени (или други символи) знаци.
	Буквено-цифрови	Потребителят трябва да е въвел парола, съдържаща поне два символа - цифров и буквен (или друг символ).
	Комплекс	Потребителят трябва да е въвел парола, която по подразбиране съдържа поне една буква, една цифра и един специален символ. С това качество на паролата може да се ограничи съдържанието на различни набори от символи, като например поне една главна буква и т.н.
Минимална дължина на паролата	Задайте необходимия брой символи за паролата. Например можете да изисквате ПИН кодът или паролите да съдържат най-малко шест знака.	
Минимален брой цифри, изисквани в паролата	Минимален брой цифри, изисквани в паролата	
Минимален брой малки букви, изисквани в паролата	Минимален брой малки букви, изисквани в паролата	

Минимален брой главни букви, изисквани в паролата	Минимален брой главни букви, изисквани в паролата
Минимален брой небуквени символи, изисквани в паролата	Минимален брой небуквени символи, изисквани в паролата
Минимален брой символи, изисквани в паролата	Минимален брой символи, изисквани в паролата

Максимално време за заключване при неактивност	Максимална неактивност на потребителя до заключване на времето
Време за изтичане на паролата	Установява, след който интервал от време паролата изтича и трябва да се издаде нова парола.
Ограничаване на историята на паролите	Брой на използваните преди това пароли, които не са разрешени
Максимален брой неуспешни опити за парола	Установява колко често паролата може да бъде въведена неправилно, преди да се извърши пълно изтриване на устройството.
Разрешаване на биометрично удостоверяване	Позволява удостоверяване чрез пръстов отпечатък или сканиране на ириса. Само за Samsung KNOX 2.1 и по-висока версия

Парола на контейнера

Под "Код за достъп" можете да зададете парола за контейнер, като имате на разположение следните опции за настройка:

Минимална дължина на паролата	Определя минималния брой символи, които трябва да съдържа паролата.	
Качество на паролата	Неуточнено	Тази политика няма изисквания за паролата.
	Биометрични данни Слаби	Тази политика позволява използването на биометрични технологии за разпознаване с ниска степен на сигурност. Това означава технологии, които могат да разпознаят самоличността на дадено лице до около трицифрен ПИН код (фалшивото разпознаване е по-малко от 1 на 1000).
	Нещо	Тази политика изисква задаването на някакъв вид парола или шаблон, но не налага никакви конкретни правила.
	Азбучен	Потребителят трябва да е въвел парола, съдържаща поне буквени (или други символи) знаци.
	Буквено-цифрови	Потребителят трябва да е въвел парола, съдържаща поне два символа - цифров и буквен (или друг символ).
	Комплекс	Потребителят трябва да е въвел парола, която по подразбиране съдържа поне една буква, една цифра и един специален символ. С това качество на паролата може да се ограничи съдържанието на различни набори от символи, като например поне една главна буква и т.н.
Минимална дължина на паролата	Задайте необходимия брой символи за паролата. Например можете да изисквате ПИН кодът или паролите да съдържат най-малко шест знака.	
Минимален брой цифри, изисквани в паролата	Минимален брой цифри, изисквани в паролата	
Минимален брой малки букви, изисквани в паролата	Минимален брой малки букви, изисквани в паролата	
Минимален брой главни букви,	Минимален брой главни букви, изисквани в паролата	

изисквани в паролата	
Минимален брой небуквени символи, изисквани в паролата	Минимален брой небуквени символи, изисквани в паролата
Минимален брой символи, изисквани в паролата	Минимален брой символи, изисквани в паролата

Максимално време за заключване при неактивност	Максимална неактивност на потребителя до заключване на времето
Време за изтичане на паролата	Установява, след който интервал от време паролата изтича и трябва да се издаде нова парола.
Ограничаване на историята на паролите	Брой на използваните преди това пароли, които не са разрешени
Максимален брой неуспешни опити за парола	Установява колко често паролата може да бъде въведена неправилно, преди да се извърши пълно изтриване на устройството.

Антивирус

Автоматично сканиране	Активиране на периодични автоматични сканирания
Интервал на сканиране	Интервал за преглед (бърз/пълен)
Пълно автоматично сканиране	Активиране на пълно автоматично сканиране
Автоматични актуализации	Активиране на автоматични актуализации
Интервал на проверката за актуализация	Колко често трябва да се актуализират приложението и неговата база данни (вируси / повреден код)
Защита на приложенията	Активиране на автоматичното сканиране на приложения
Защита на SD картата	Активиране на автоматичното сканиране на SD картата
Актуализация само за Wi-Fi	Когато е разрешено, актуализациите ще се прилагат само когато устройството е успешно свързано с Wi-Fi мрежа.

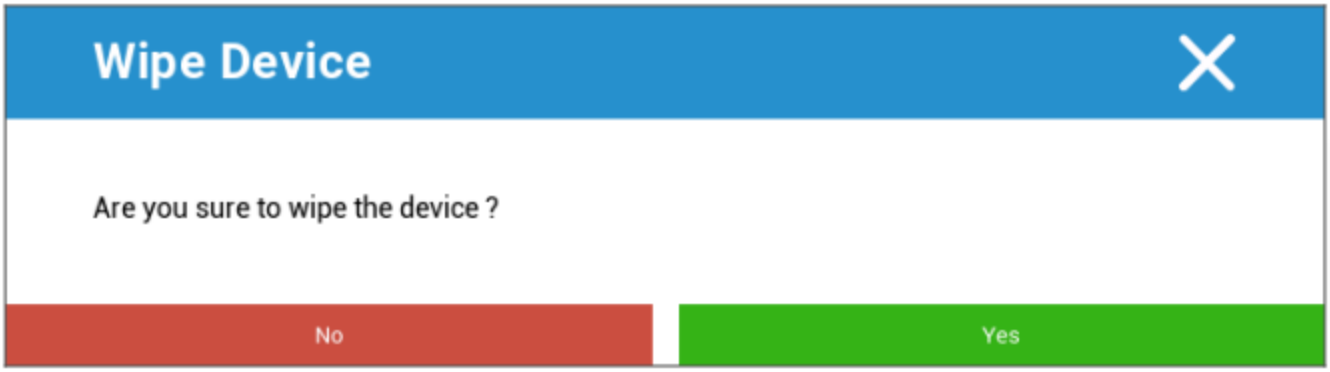
Край на живота (само на ниво устройство)

Избърсване (само на ниво устройство)

Под "Изтриване" можете да възстановите фабричните настройки на устройството (Само при подобрен работен профил).

Тук корпоративните и личните данни ще бъдат изтрити от устройството на крайния потребител.

След като кликнете върху символа "минус", ще получите следното съобщение:



С "Да" можете да извършите изтриването.

Под "Отчет за изтриване" могат да бъдат показани следните елементи

Изтрити от	История на лицето, извършило изтриването
Дата	Дата
Статус	Статус (например дали изтриването е извършено успешно)

Настройки на ограниченията

Ограничения

Тук могат да се ограничават и блокират различни неща.

Изпълнение на изискванията	Mode Prompt User - Потребителят ще бъде подканен да изпълни необходимите действия. Контейнер за блокиране на режима - скрийте всички приложения, докато не бъдат изпълнени всички изисквания
Политика за разрешаване по време на изпълнение	Подканване на потребителя за нови заявки за разрешение Винаги разрешавайте нови заявки за разрешение Винаги отказвайте нови заявки за разрешение Предупреждение: Някои приложения имат проблеми с разпознаването на разрешенията, ако те са зададени автоматично. Ако винаги предоставяте разрешения и срещате проблеми с приложенията, които казват, че липсват разрешения, задайте това на "подкани потребителя" и преинсталирайте приложението.
Разрешаване на изходящ клипборд	Позволява копиране и поставяне от вътрешността на контейнера навън
Разрешаване на резолюцията на идентификатора на повикващия	Показва името на входящо повикване въз основа на контактите в контейнера
Разрешаване на търсенето на контакти	Позволява търсене на имена в контейнера за контакти при провеждане на повиквания
Разрешаване на споделянето на контакти чрез Bluetooth	Позволява достъп до контакт с контейнер в автомобил
Забрана за изходящ NFC лъч	Деактивиране на NFC за контейнера
Разрешаване на неизвестни източници	Ако е разрешено, потребителите могат да зареждат приложения отстрани, като инсталират .apk файл.
Разрешаване на дебъгването на USB	Ако е разрешено, потребителите могат да активират USB Debugging.
Забрана за промяна на сметката	Забранява създаването, изтриването и модифицирането на акаунти в контейнера

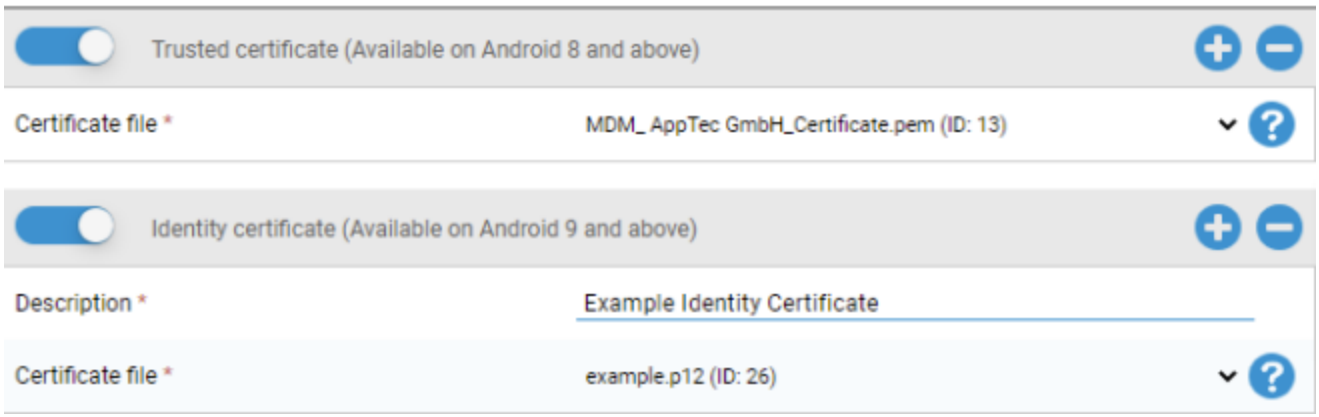
	Имайте предвид, че някои приложения трябва да създадат или модифицират акаунти, за да работят както трябва.

Ограничения на работния профил. Налично само на устройства с Android 11 и по-високи версии, с Enhanced Work Profile	
Забранете камерата	Указва дали камерата е забранена в работния профил.
Забрана на Bluetooth	Указва дали Bluetooth е забранен в работния профил.
Активиране на защитата от нулиране на фабриката	Активирайте тази опция, за да отмените защитата от фабрично нулиране на Android към акаунта в Google, който сте определили в "Общи настройки" → "Конфигурация на Android" → "Android Enterprise" → "Защита от фабрично нулиране" Ако тази опция е активирана и нулирате устройството, ще трябва да предоставите конфигурирания акаунт в Google, за да настроите устройството отново.
Актуализация на контролната операционна система	Активирайте тази опция, за да зададете поведението на актуализация като автоматично, с прозорец или отложено.
Политика за актуализиране	Автоматично: Инсталира се автоматично, веднага щом е налична актуализация. С прозорци: Инсталирайте автоматично в рамките на дневния прозорец за поддръжка. Това също така конфигурира приложенията в Play да бъдат актуализирани в рамките на прозореца. Това е силно препоръчително за киоск устройства, тъй като това е единственият начин приложенията, които са трайно прикрепени на преден план, да бъдат актуализирани от Play. Отлагане: Отложете автоматичното инсталиране до максимум 30 дни.

Ограничения на личния профил. Налично само на устройства с Android 11 и по-високи версии, с подобрен работен профил	
Забранете камерата	Указва дали камерата е забранена в личния профил.
Забрана на Bluetooth	Указва дали Bluetooth е забранен в личния профил.
Разрешаване на неизвестни източници	Ако е разрешено, потребителите на работни профили могат да зареждат приложения отстрани, като инсталират .apk файл.

Управление на сертификати

Тук можете да разпространявате доверени сертификати и сертификати за идентичност към устройствата си. За да разпространявате доверени сертификати, е необходим Android 8 или по-нов, а за да разпространявате сертификати за идентичност - Android 9 или по-нов.



С бутона "+" можете да добавите няколко сертификата.

Достоверните сертификати трябва да са във формат PEM.

Удостоверенията за идентичност трябва да са във формат PKCS12.

Управление на връзките

Wifi

За тази настройка извършете предварително конфигуриране на крайните потребителски устройства за достъп до вътрешните точки за достъп

Идентификатор на набора от услуги (SSID)	SSID за мрежата, която трябва да се свърже
Скрита мрежа	Активиране, в случай че AP не излъчва SSID

Вид сигурност

Установяване на типа на сигурност на AP

WEP

Парола	Парола за AP

WPA/WPA2

Парола	Парола за AP

802.1x EAP

Метод на EAP			
PWD	Идентичност	Идентичност	
	Парола	Парола	
PEAP	Протокол за удостоверяване на фаза 2	няма	Без допълнителен протокол
		MSCHAPV2	Протокол MSCHAPV2
		GTC	Протокол на GTC
	Сертификат на CA	Сертификат на CA	
	Идентичност	Идентичност	
	Анонимна самоличност	Анонимна самоличност	
	Парола	Парола	
TTLS	Протокол за удостоверяване на фаза 2	няма	Без допълнителен протокол
		PAP	Протокол PAP
		MSCHAP	Протокол MSCHAP
		MSCHAPV2	Протокол MSCHAPV2
		GTC	Протокол на GTC
	Сертификат на CA	Сертификат на CA	
	Идентичност	Идентичност	
	Анонимна самоличност	Анонимна самоличност	
	Парола	Парола	
TLS	Сертификат на CA	Сертификат на CA	
	Идентичност	Идентичност	
	Парола	Парола	

VPN

Име на връзката	Име на VPN връзката

Тип VPN

VPN

Клиент на VPN

Клиент за VPN на AppTec	
Конфигурация на шлюза	Изберете конфигурацията на VPN шлюза (вижте **Общи настройки > Универсален шлюз > Настройки на VPN**).
Винаги включена VPN услуга	Активиране на функцията Native Lockdown
Активиране на заключването на AppTec	Активиране на заключването на AppTec

Вграден (наличен само в устройствата на Samsung)			
Тип на връзката	PPTP	Сървър	Сървър
		Активиране на криптирането PPTP	Активиране на криптирането PPTP
	L2TP / IPSec PSK	Сървър	Сървър
		Предварително споделен ключ на IPSec	Предварително споделен ключ на IPSec
		Активиране на L2TP Secret	Активиране на L2TP Secret
		L2TP Secret	L2TP Secret
	IPSec XAuth PSK	Сървър	Сървър
		Идентификатор на IPSec	Идентификатор на IPSec
		Предварително споделен ключ на IPSec	Предварително споделен ключ на IPSec
Домейни за търсене DNS	Домейни за търсене DNS		
Експертни настройки	DNS сървъри	DNS сървъри	
	Маршрути за препращане	Маршрути за препращане	

Отворена VPN услуга		
Сървър	Сървър	
Профил на OpenVPN	Профил на OpenVPN	
Приложение за OpenVPN	OpenVPN за Android (препоръчително)	
	Свързване с OpenVPN	
Експертни настройки	DNS сървъри	DNS сървъри
	Маршрути за препращане	Маршрути за препращане

Samsung / Strong Swan			
Тип на връзката	PPTP	Сървър	Сървър
		Потребителско име	Потребителско име
		Парола	Парола
		Активиране на криптирането PPTP	Активиране на криптирането PPTP
	L2TP / IPSec PSK	Сървър	Сървър
		Предварително споделен ключ на IPSec	Предварително споделен ключ на IPSec
		Потребителско име	Потребителско име
		Парола	Парола
		Активиране на L2TP Secret	L2TP Secret
	IPSec XAuth PSK	Сървър	Сървър
		Идентификатор на IPSec	Идентификатор на IPSec
		Предварително споделен ключ на IPSec	Предварително споделен ключ на IPSec
		Потребителско име	Потребителско име
		Парола	Парола
Експертни настройки	DNS сървъри	DNS сървъри	
	Маршрути за препращане	Маршрути за препращане	

Cisco Any Connect		
Сървър	Сървър	
Режим на сертификата	Инвалиди	Инвалиди
	Автоматичен	Автоматичен
Експертни настройки	DNS сървъри	DNS сървъри
	Маршрути за препращане	Маршрути за препращане

VPN за всяко приложение

Клиент на VPN

Клиент за VPN на AppTec		
Конфигурация на шлюза	Изберете конфигурацията на VPN шлюза (вижте **Общи настройки > Универсален шлюз > Настройки на VPN**).	
VPN приложения	VPN приложения	
Винаги включена VPN услуга	Активиране на функцията Native Lockdown	Винаги включена VPN услуга
Активиране на заключването на AppTec	Активиране на заключването на AppTec	

Samsung / Strong Swan			
Тип на връзката	PPTP	Сървър	Сървър
		VPN приложения	VPN приложения
		Потребителско име	Потребителско име
		Парола	Парола
		Активиране на криптирането PPTP	Активиране на криптирането PPTP
	L2TP / IPSec PSK	Сървър	Сървър
		VPN приложения	VPN приложения
		Предварително споделен ключ на IPSec	Предварително споделен ключ на IPSec
		Потребителско име	Потребителско име
		Парола	Парола
		Активиране на L2TP Secret	L2TP Secret
	IPSec XAuth PSK	Сървър	Сървър
		VPN приложения	VPN приложения
		Идентификатор на IPSec	Идентификатор на IPSec
		Предварително споделен ключ на IPSec	Предварително споделен ключ на IPSec
		Потребителско име	Потребителско име
		Парола	Парола
Експертни настройки	DNS сървъри	DNS сървъри	
	Маршрути за препращане	Маршрути за препращане	

Ограничения

Тук можете да зададете ограниченията по отношение на управлението на връзката

Разрешаване на роуминга на данни	Разрешаване на мобилните данни в роуминг
Налагане на роуминг на данни	Ако е активиран, роумингът за мобилни данни се активира за постоянно (не се препоръчва!) Тази настройка замества настройката "Разрешаване на роуминг на данни"!
Използване на системен http прокси сървър	Използването на HTTP прокси сървър, което се осигурява от настройките на системата в настройките, зависи от свързаната мрежа (WiFi или APN).

Управление на PIM

Gmail Exchange

Информация: Тази конфигурация ще бъде приложена към приложението Gmail. Затова трябва да одобрите и инсталирате Gmail.

Електронен адрес	Имейл адресът на предоставения потребител Обърнете внимание на "заместителите", които можете да използвате за работа с удостоверенията и да не извършвате промени ръчно на всяко устройство. С едно кликване върху тях можете да ги покажете сами
Име на хоста на сървъра	Адрес на сървъра на вашите сървъри на Exchange
Име за вход	Името за вход за съответното устройство на крайния потребител, моля, обърнете внимание и на "Заместващи символи тук".
Подпис	Може да се приложи подпис (Съвет: Някои устройства изискват HTML форматиране на подписа).
Брой предишни дни за синхронизиране	Брой дни, определящи кога имейлите се синхронизират обратно
Идентификатор на устройството	Ein String der die EAS DeviceID enthält. Dies ist Teil des EAS Protokols und wird in einigen Umgebungen benötigt
Използване на Secure Sockets Layer (SSL)	Използване на SSL връзка
Приемане на всички сертификати	Приемат се всички сертификати. Моля, изберете тази опция, ако вашият Exchange Server използва самоподписан сертификат.
Разрешаване на неуправлявани акаунти	Позволете на потребителите да добавят или премахват всеки акаунт на Exchange, различен от акаунта, посочен в тази управлявана конфигурация. Ако тази настройка е разрешена, не можете да попречите на потребителите да добавят други Exchange акаунти в Gmail. Също така не можете да контролирате споделянето на данни между други приложения и Exchange акаунти, добавени от потребителите. Тази настройка трябва да бъде разрешена само ако вашите потребители трябва да поддържат повече от един работен Exchange акаунт в Gmail.

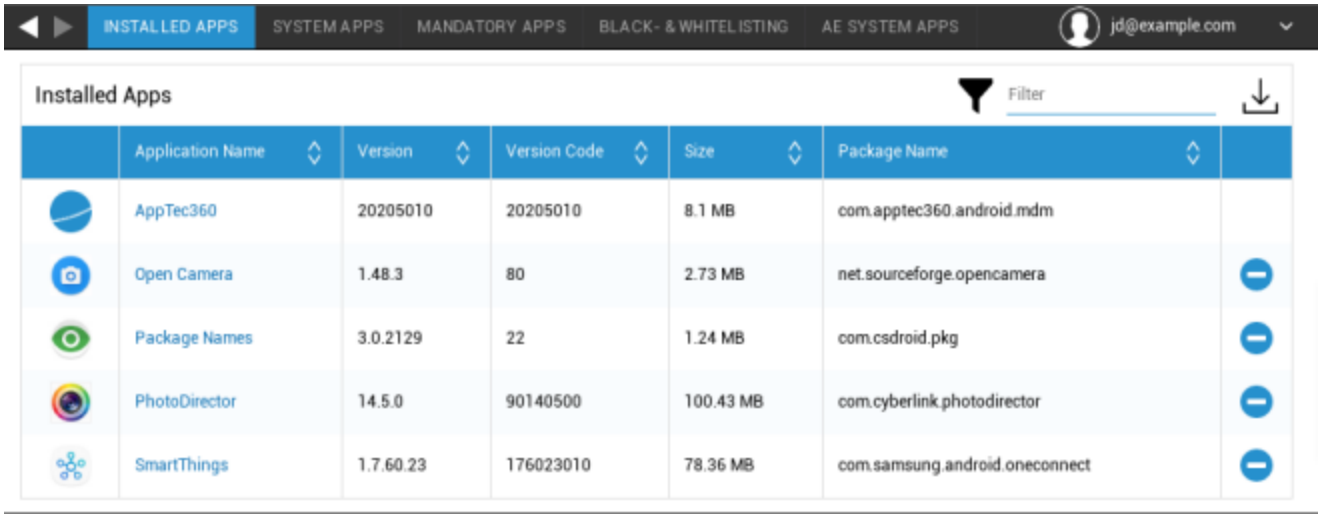
Сертификат на клиента	Клиентски сертификат. Изисква се само ако вашият пощенски сървър очаква наличието на такъв сертификат.

Управление на приложения

Мениджър на корпоративни приложения

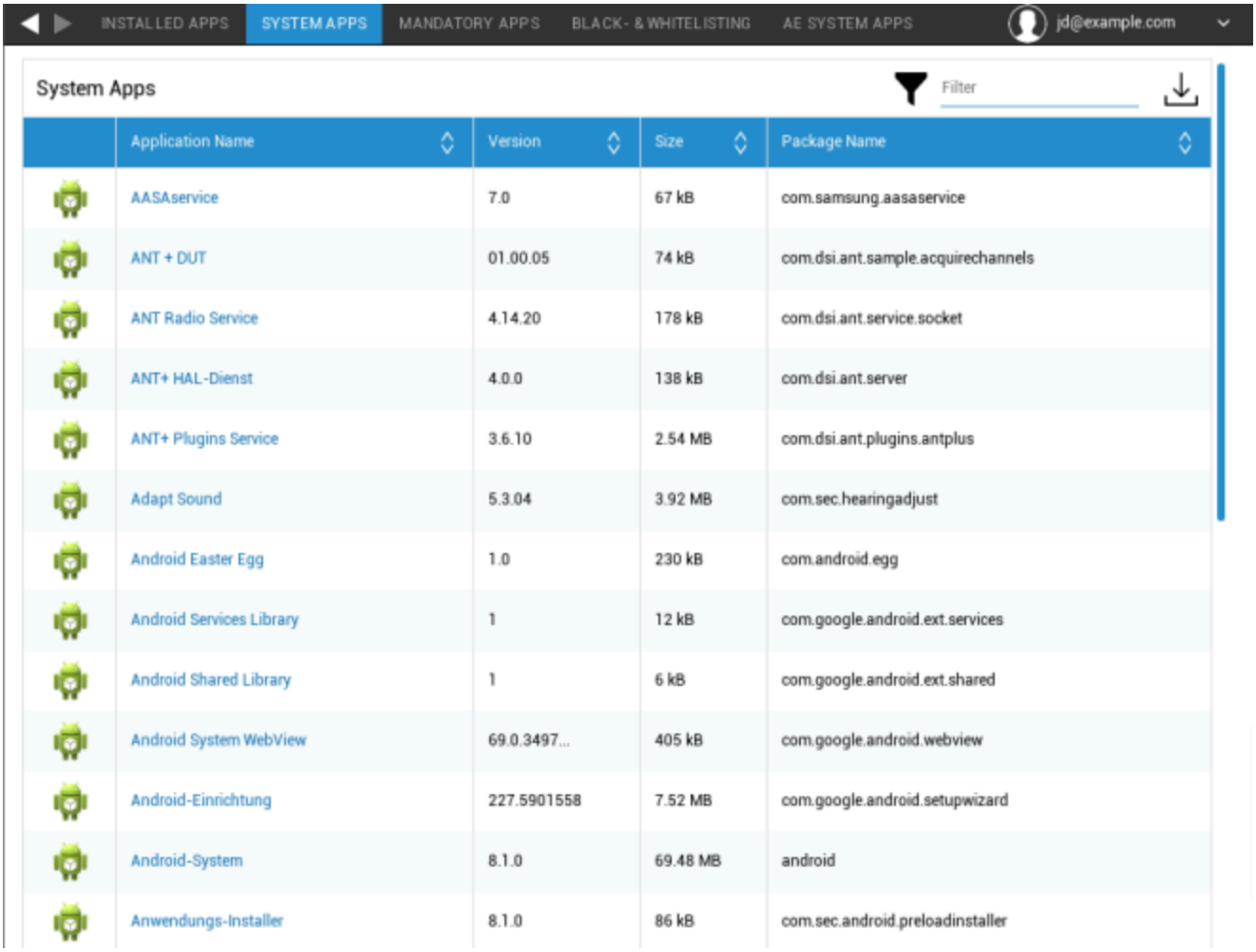
Инсталирани приложения (само на ниво устройство)

Тук ще бъдат показани всички приложения, които в момента са инсталирани в контейнера.



Системни приложения (само на ниво устройство)

В "Системни приложения" ще бъдат изброени всички приложения и услуги, които вече са инсталирани на крайното потребителско устройство от производителя на устройството.

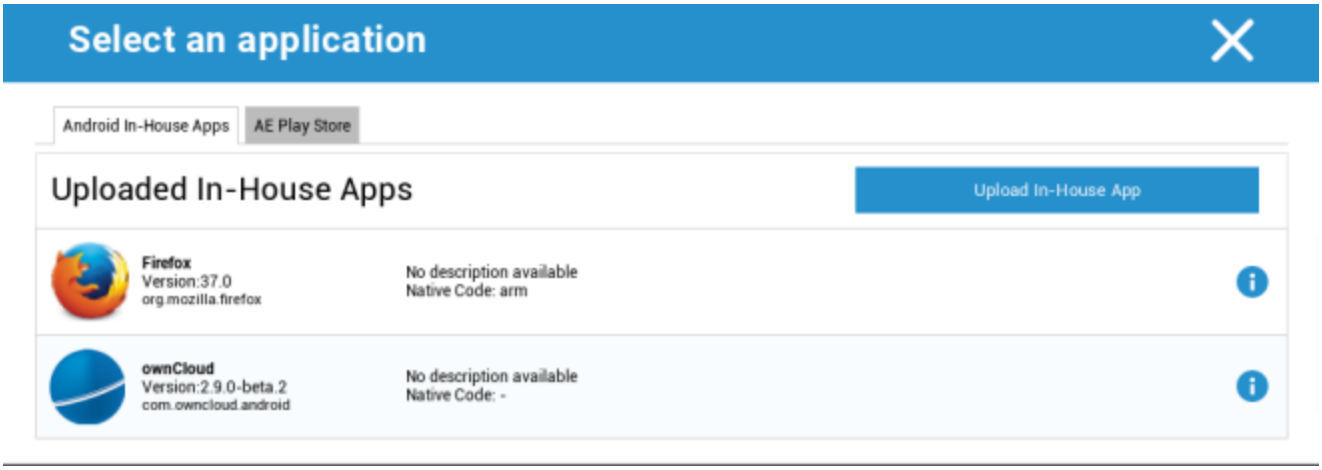


Задължителни приложения

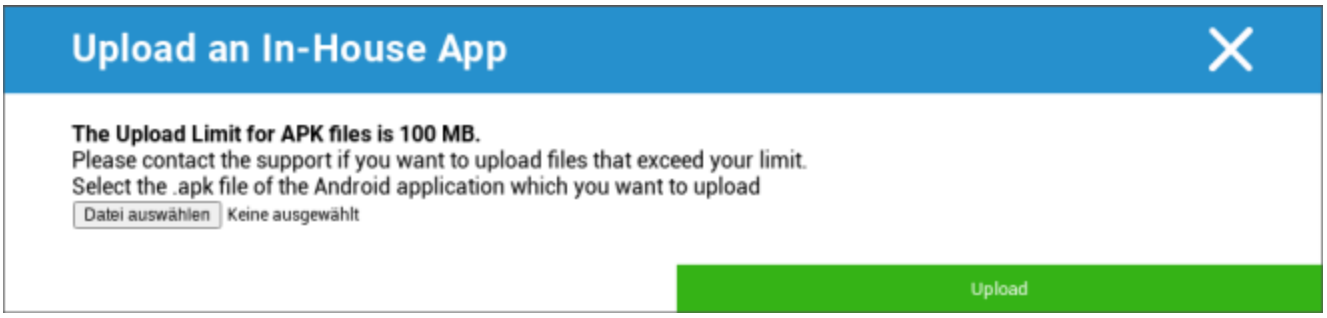
В частта Задължителни приложения можете да зададете задължителните приложения. Потребителят непрекъснато ще бъде подканян да инсталира това определено приложение, ако то е вътрешно приложение. Приложенията от Play Store ще бъдат инсталирани автоматично.

Чрез , може да се определи задължителното изисквано приложение.

Това може да бъде вътрешно приложение от "Вътрешни приложения за Android", което сте качили в Общите настройки.

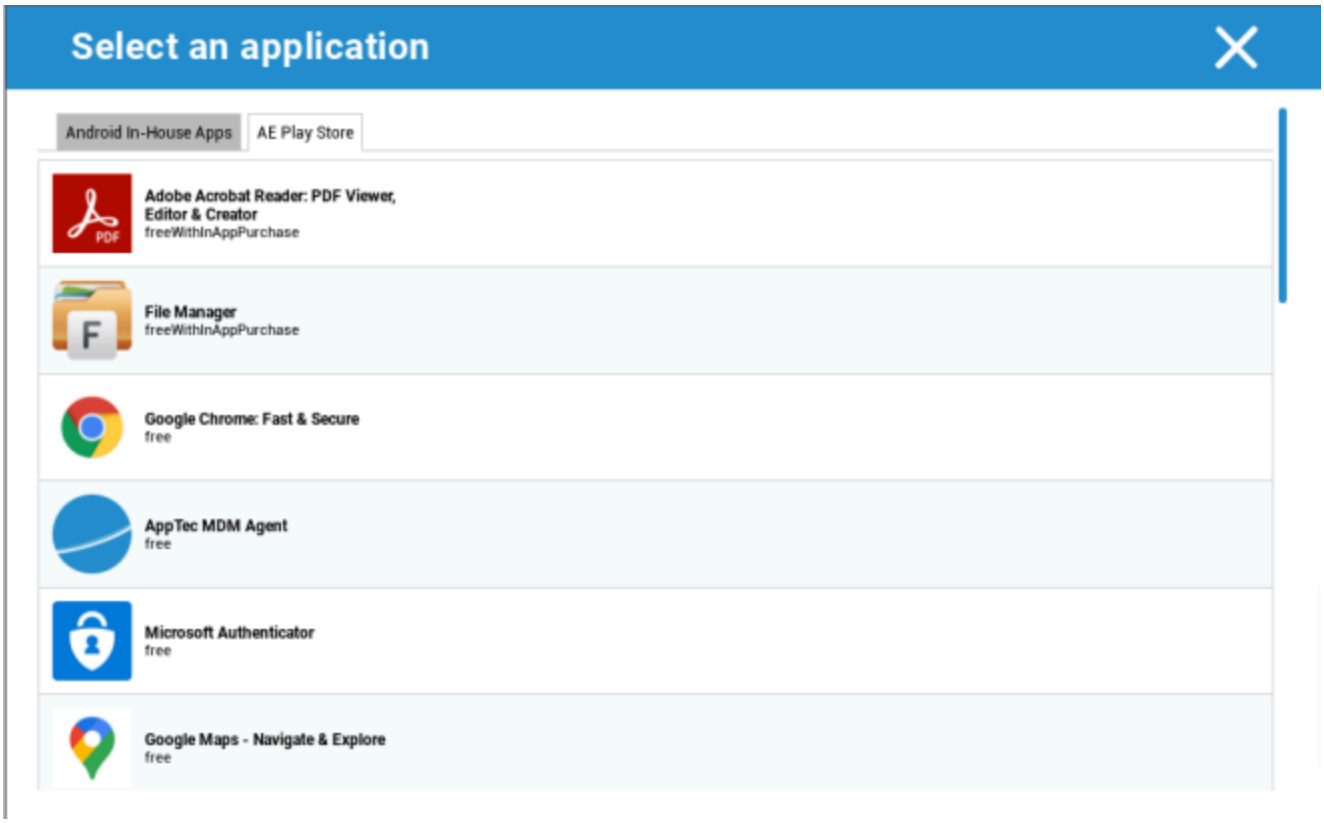


Можете също така директно да изберете и качите apk файл с "Качване на вътрешно приложение".



Ако инсталирате вътрешно приложение, ще имате възможност да активирате опцията "Keep up to date". Ако тази опция е активирана и сте определили по-нова версия в БД на вътрешното приложение, приложението ще бъде актуализирано на устройството.

Или може да бъде приложение "AE Play Store" от работния магазин Play на Google.



Само одобрените "AE Play Store Apps" ще бъдат показани в този раздел.

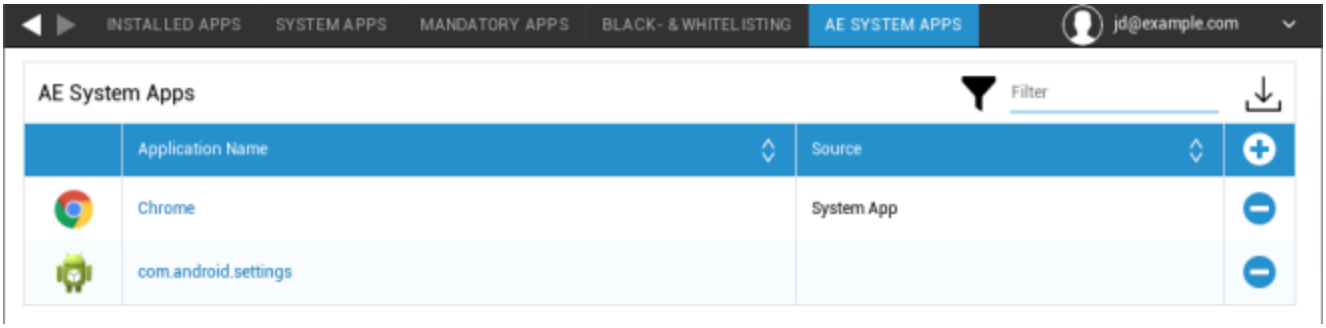
За да одобрите "AE Play Store App", моля, отидете в "Общи настройки" > "Управление на приложения" > "AE Play

Store" и добавете приложение чрез бутона, който ще ви пренасочи към раздела "Play Store Apps" (или можете директно да отидете в раздела "Play Store Apps").

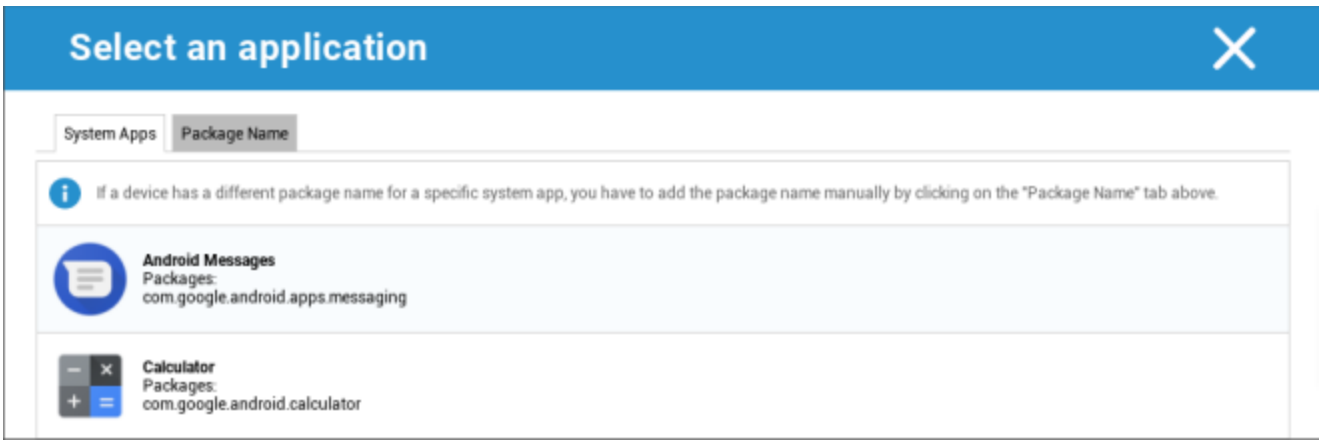
В раздела "Приложения в Play Store" можете да търсите приложения. Когато щракнете върху дадено приложение, се отваря страницата на приложението и тук можете да одобрите приложението, като щракнете върху "Approve".

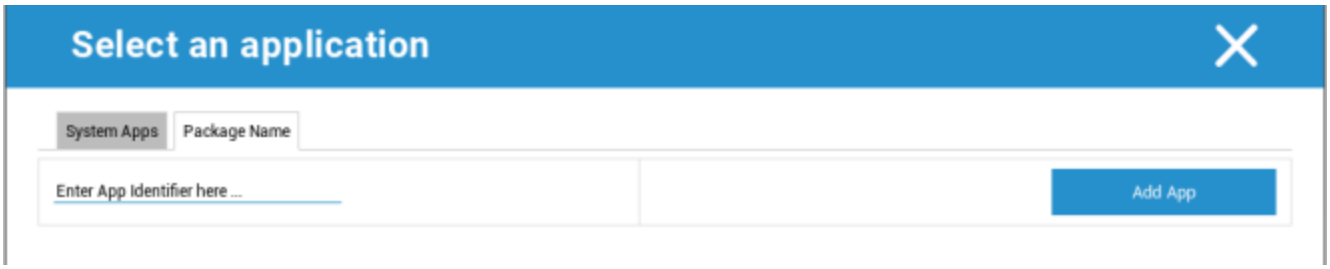
Приложения на системата AE

Тук можете да дефинирате списък, който съдържа конкретни системни приложения, които трябва да бъдат активирани на устройствата.



Ако щракнете върху бутона, можете да изберете от списък с възможни системни приложения, предоставен от Google, или директно да въведете името на пакета на системното приложение, което трябва да бъде активирано.





Имайте предвид, че системните приложения в списъка, предоставен от Google, са само приложения, които могат да бъдат системни приложения, но не е задължително да бъдат системни приложения на вашите устройства.

Този списък обаче засяга само приложения, които вече са предварително инсталирани.

Добавянето на приложения, които не са предварително инсталирани на вашите устройства, няма да се отрази на устройствата ви, независимо дали приложението е от списъка, предоставен от Google, или името на пакета на приложението е въведено директно.

Ограничения и настройки

Настройки за управление на приложения

Тук можете да конфигурирате поведението на устройството по отношение на актуализациите на приложенията.

Честота на проверките за актуализация	Посочете през какъв интервал от време AppTec Client ще търси актуализации на приложенията. Стойността по подразбиране е 24 часа.
Праг на Wi-Fi	Приложенията, които са по-големи от определения размер, ще бъдат изтеглени през Wi-Fi. Ако е избрана опцията "Само Wi-Fi", всички приложения ще се изтеглят чрез Wi-Fi.

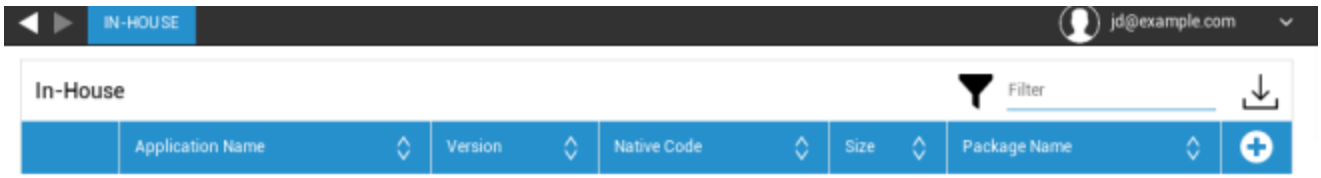
Магазин за корпоративни приложения

Вътрешен

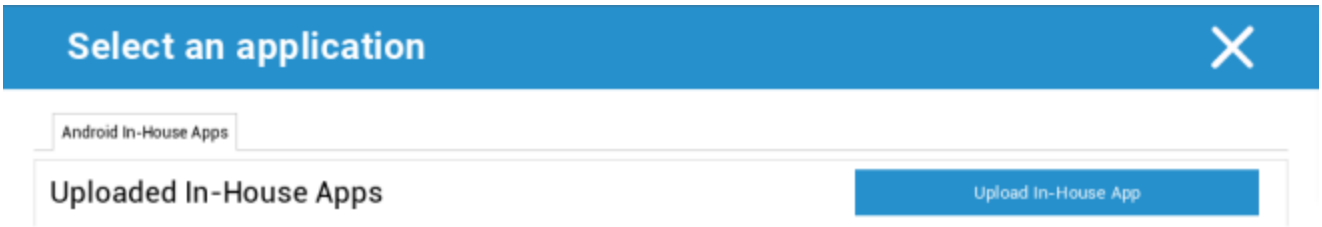
В точката "Собствени" можете да качвате и разпространявате вътрешно разработени приложения.

Със символа можете да разпространявате допълнителни вътрешни приложения.

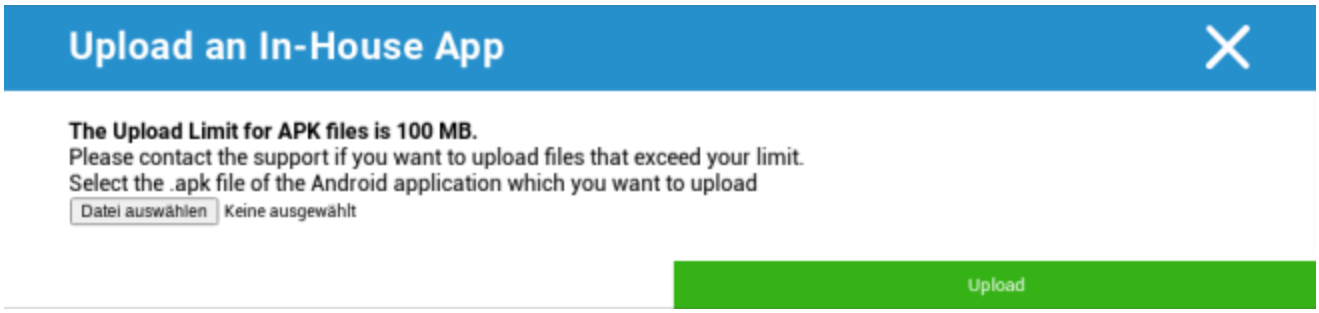
Ако инсталирате вътрешно приложение, ще имате възможност да активирате опцията "Keep up to date". Ако тази опция е активирана и сте определили по-нова версия в БД на вътрешното приложение, приложението ще бъде актуализирано на устройството.



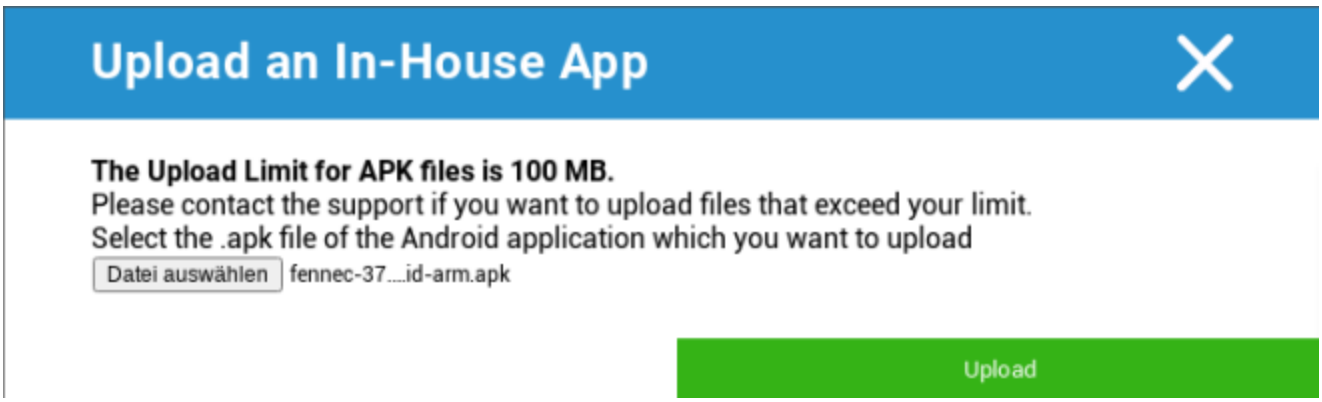
Ако не сте разпространили вътрешни приложения, ще получите следния преглед:



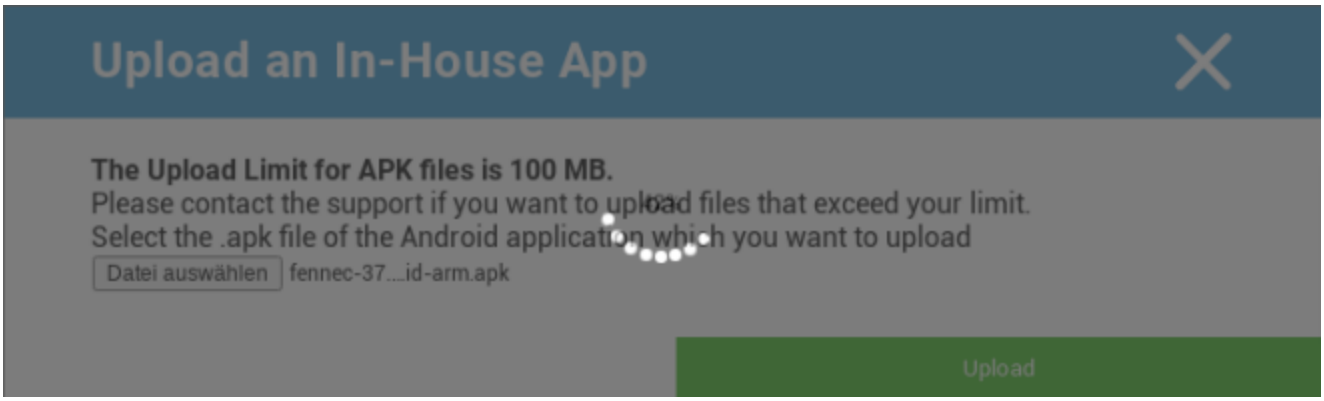
За целта кликнете върху "Upload In-House App" (Качване на вътрешно приложение), след което ще получите следния преглед:



Сега изберете с "Търсене..." .apk файл и след това кликнете върху "Качване".



Приложението ви вече ще бъде качено, като в средата на кръга ще видите индикатор за процент, който показва каква част от приложението ви вече е качена.



Ако качването на вашето вътрешно приложение е било успешно, можете да намерите каченото приложение в каталога си с приложения.

Сега потребителят има възможност да види и инсталира това приложение в AppTec Store на устройството на крайния потребител, в категорията "In-House".

Тъй като това не включва приложение от Google PlayStore, потребителят не се нуждае от съхранен Google ID на съответното устройство на крайния потребител.

Магазин Play за предприятия

Магазин за игри AE

Тук можете да добавяте приложения в Android Enterprise Playstore. Моля, имайте предвид, че преди да добавите приложения, трябва да ги одобрите с профила си на администратор на AE.

За одобряване на приложение вижте инструкциите в раздел Задължителни приложения.

Управление на съдържанието

ContentBox

Тук можете да активирате ContentBox.

Веднага след като превключите "Enable ContentBox" на "On", отделно приложение ContentBox ще бъде инсталирано автоматично на крайното потребителско устройство.

Сигурен браузър

Тук можете да конфигурирате настройките за AppTec Secure Browser.

Щом превключите раздела в "Secure Browser" (Сигурен браузър) на "On" (Вкл.), на крайното потребителско устройство автоматично ще бъде инсталирано отделно приложение за браузър.

Изискване на парола	Изисквайте от потребителя да зададе и използва парола за достъп до браузъра.
Минимална необходима дължина на паролата	Задаване на необходимия брой символи за паролата
Изисквано качество на паролата	Задайте необходимото качество на паролата
Ограничаване на изтеглянията / Отваряне в	
Ограничаване на качванията	
Качване на бял списък	Списък с URL адреси, чието качване винаги ще бъде разрешено.
Разрешаване на копирането	Позволява копиране, изрязване или споделяне на текст в уеб страниците.
Разрешаване на заснемането на екрана	Позволява заснемане на скрийншоти.
Честота на почистване на данните	Изберете с каква честота ВСИЧКИ потребителски данни (история, кеш и т.н.) да се премахват автоматично.
Фирмени отметки	Записките ще се появят в папката "Company bookmarks" (Записки на компанията) в отметките на браузъра. Те не могат да се редактират от потребителя.
Скриване на адресната лента	
Бели списъци в браузъра (без Universal Gateway)	Активира бял списък на URL адреси от страна на клиента. • Фирмените отметки винаги са в белия списък • Поддържа се само за 100 URL адреса • Моля, използвайте Универсалния шлюз за неограничен черен и бял списък
URL адреси в белия списък	Списък на разрешените URL адреси.

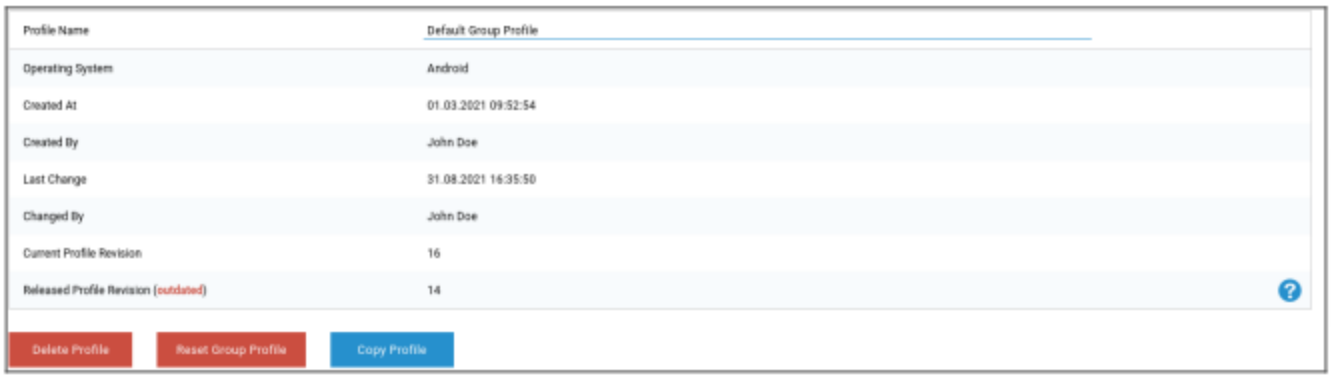
Базиран на шлюз черен и бял списък	Черният списък има следните изисквания: • Работещ универсален шлюз на AppTec ("Общи настройки" → "Универсален шлюз") • Работеща VPN конфигурация с определен DNS сървър ("Общи настройки" → "Универсален шлюз" → "VPN настройки") • Конфигуриране на черен списък ("Общи настройки" → "Универсален шлюз" → "Черен списък на домейни") • Валидна VPN връзка в профила ("Управление на връзките" → "VPN")

Конфигурация на Android

Обща информация

Преглед на профила на групата (само на ниво група)

При отваряне на групов профил ще получите бърз преглед на профила.



Име на профила	Име на профила (може да бъде променено тук)
Операционна система	Операционна система, за която е предназначен профилът
Създаден в	Време на създаване
Създаден от	Създател на профила
Последна промяна	Време на последната промяна в профила
Променено от	Акаунт, в който са направени последните промени
Текуща ревизия на профила	Преразглеждане на запазеното състояние на профила
Освободена ревизия на профила	Присвоена ревизия на профила ("Присвои сега"). Ако зад текста на етикета се показва "(остарял)", това означава, че сте запазили профила, но все още не сте го присвоили, така че устройствата все още ще получават по-стара версия.

Преглед на устройството (само на ниво устройство)

Ако се намирате на устройство, ще получите обобщаващ преглед на избраното устройство, като тук се съдържа следното:

Име на устройството	Име на устройството
Последно известно местоположение	Последните известни GPS координати
Телефонен номер	Телефонен номер
Зададени задължителни приложения	Броят на назначените задължителни приложения
Версия на операционната система	Версия на операционната система на устройството
Операционна система	Операционна система (Android / iOS / Windows Phone)
Сериен номер	Сериен номер на устройството
Притежание на устройство	Корпоративно или частно устройство
Тип устройство	Телефон или таблет
Вкоренени	Състояние, показващо дали устройството е било рутирано
Съответстващ	Съответствие с насоките
IP адрес	IP адрес
Последно видян	Точка във времето, когато устройството се е свързало за последен път с AppTec
Последен тласък	Точка във времето, в която сървърът е изпратил push към устройството
Присвояване на потребителя	Падащо меню за присвояване на устройството на друг потребител

Ревизия на конфигурацията (само на ниво устройство)

Тук ще получите преглед на груповия профил, който е зададен на устройството.

Ако щракнете върху профила на групата, ще получите директен достъп до профила и ще можете да извършвате настройки.

Със символа можете да върнете зададените приложения към настройките на груповия профил.

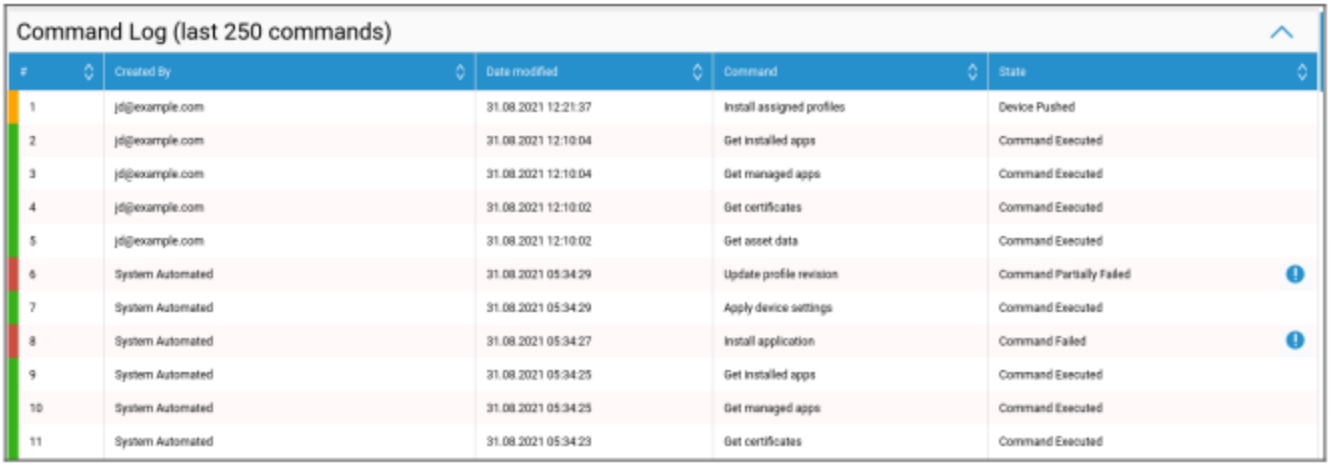
Със символа можете да нулирате профила на устройството, така че да няма никакви настройки.

"Налична е по-нова ревизия" показва, че профилът на групата е променен и запазен, но не е присвоен. Груповият профил трябва да бъде присвоен с "Assign now" (Присвояване сега) на ниво група, за да се приложат промените към устройствата.

Дневник на устройството (само на ниво устройство)

Дневник на командите

Тук можете да видите кои команди са издадени за устройството и какво е тяхното състояние.



Командите, създадени от "System Automated", се създават автоматично от системата.

Възможни състояния на командата

Натиснато устройство	Изпратена е заявка за натискане до услугата за натискане (напр. APNS), за да се каже на устройството да се свърже отново със сървъра на EMM.
Създадена команда	Командата е създадена в системата.
Изпратена команда	Командата е изпратена на устройството, след като то се е свързало със сървъра.
Изпълнена команда	Командата е изпълнена успешно.
Командата е неуспешна	Командата не е изпълнена. *
Командата е частично неуспешна	В зависимост от операционната система на устройството някои команди могат да бъдат групирани заедно. При това някои части от тази група команди не успяха. *
Командата е изпълнена, но в крайна сметка е неуспешна	Командата е изпълнена, но може би не е.
Пренасочване на командата	Командата е била изпратена отново от потребител.
Изхвърлени	Командата беше отхвърлена. Например защото е била заменена от друга команда или устройството е било презаписано и старите команди са били премахнати.

*Ако зад съобщението има възклицателен знак, можете да получите повече информация, като задържите курсора върху иконата.

Настройки на устройството

Конфигурация на клиента

Тук можете да извършите следните конфигурации на вашето устройство с Android:

Предупредително съобщение след деактивиране на управлението на устройствата	Създадено предупредително съобщение след деактивиране на управлението на устройствата
Време за несъответствие	Срок, след изтичането на който ще бъде извършено "Действие по прилагане след съответствие", ако устройството не е в съответствие. Мин. 1 минута Макс. 24 часа
Действия по изпълнение след изтичане на срока за изпълнение	Действието, което трябва да се предприеме, когато дадено устройство стане несъответстващо на изискванията. • не прави нищо = няма действие • Устройство за заключване = устройство за заключване • Изтриване на устройството = устройството ще бъде възстановено до фабричните настройки
Честота на събиране на данни	Честота на събиране на информация за устройствата/GPS
Честота на сърдечния ритъм на устройството	Интервал, през който устройството трябва да се свърже със сървъра AppTec360 Мин. 1 минута Макс. 24 часа
Активиране на актуализациите на местоположението	Ако е активирано, устройството изпраща актуализации на местоположението към сървъра AppTec360
Време за актуализация на местоположението	Определя през какви интервали от време устройството изпраща актуализации на местоположението към AppTec
Използване на Google Location Accuracy за актуализация на местоположението	Ако е активирана, за актуализациите на местоположението ще се използва услугата Google Location Accuracy (известна преди като мрежово местоположение) (ако тя е деактивирана в "Ограничения", тази настройка няма да повлияе на нищо).
Използване на GPS местоположение за	Ако е активирано, GPS ще се използва за актуализации на местоположението.

актуализиране на местоположението	
Разрешаване на имитационни (фалшиви) местоположения	Позволява подправяне на информация за местоположението чрез приложения на трети страни
Действие при изгубена връзка	Позволява ви да зададете определено действие, което ще се извърши след определен брой неуспешни сърдечни удари.
Режим на прилагане на политиката	Определя колко агресивно клиентът AppTec360 иска от потребителя да извърши определени действия, които изискват въвеждане от потребителя. Интервал (по подразбиране) = питане на интервали, така че потребителят да може да го остави във фонов режим за известно време. Без предупреждение = няма изскачащ прозорец за необходимо взаимодействие. Трябва да отворите ръчно AppTec360 Client, за да проверите дали има необходимо действие. Постоянно предупреждение = Потребителят може да извърши само необходимото действие. Клиентът на AppTec360 ще се наложи да излезе на преден план, ако потребителят се опита да го избегне
Заключване на версията на AppTec360	Позволява ви да определите версия на AppTec360 Client, която е максималната версия, до която клиентът се актуализира.

Тапети

Тук можете да зададете персонализиран тапет.

"Задаване на цвят" ви позволява да зададете цвят в шестнадесетичен формат (напр. #000000). Разрешени са само шестнадесетични стойности.

"Задаване на изображение като тапет" ви позволява да качите изображение. Моля, имайте предвид, че различните устройства с различни стартиращи програми и версии на операционната система работят по различен начин. Няма обща насока за размера и съотношението, тъй като това зависи от устройството.

Използвайте JPG (или JPEG) или PNG за файлов формат.

Управление на активи (само на ниво устройство)

Управление на активи

Информация за устройството

Модел	**Обозначение на модела на устройството**
Операционна система	OS
Версия на операционната система	Версия на операционната система
Поддръжка на AE	Поддръжка на Android Enterprise (контейнер и напълно управляван)
Сериен номер	Сериен номер
Име на устройството	Име на устройството
Състояние на батерията	Състояние на батерията
Свободна / обща памет	Свободна / обща памет
Samsung KNOX	Ниво на API на Samsung KNOX
Налична SD карта	Налична SD карта
Емулирана SD карта	Емулирана SD карта
Сменяема SD карта	Сменяема SD карта
SD Свободна / обща памет	SD Свободна / обща памет на SD картата

Wi-Fi

IP адрес	IP адрес на устройството
WiFi MAC	WiFi MAC адрес

Клетъчен

Статус	Състояние (инсталирана SIM карта)
Телефонен номер	Телефонен номер
Роуминг (глас/данни)	Роуминг за глас/данни
Състояние на роуминга	Текущо състояние на роуминга
IP адрес	IP адрес
Оператор/превозвач	Оператор/превозвач
Клетъчна технология	Клетъчна технология
IMEI	Номер на IMEI
ICCID	Това е идентификационният номер на SIM картата, често наричана също Smartcard или Integrated Circuit Card (ICC).
IMSI	Международният идентификатор на мобилния абонат (IMSI) осигурява в мобилните мрежи GSM и UMTS точна идентификация на потребителите на мрежата. IMSI се състои от максимум 15 цифри и се конфигурира по следния начин: • Код на мобилната държава (MCC), 3 цифри • Код на мобилната мрежа (MNC), 2 или 3 цифри • Идентификационен номер на мобилен абонат (MSIN), 1-10 цифри
Текущи MCC/MNC	Вижте "SIM MCC/MNC".
SIM MCC/MNC	Кодът на мобилната държава е установен идентификатор на държавата, определен от ITU съгласно E.212. Стандарт. Той работи в комбинация с кода на мобилната мрежа (MNC) за идентифициране на мобилната мрежа. Означава кода на страната/кода на мобилната мрежа на SIM картата. Ако сте в роуминг в друга мобилна мрежа, логично е "Current MCC/MNC" и "SIM MCC/MNC" да са различни.

Bluetooth

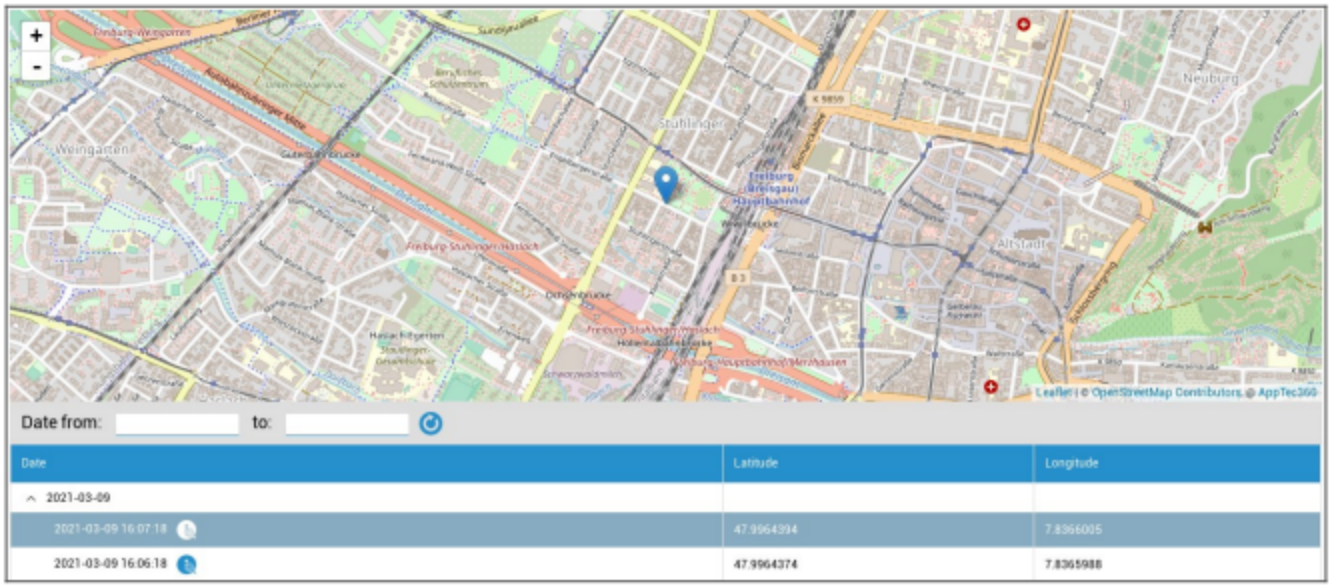
Bluetooth MAC	Bluetooth MAC адрес

Управление на сигурността

Защита от кражба (само на ниво устройство)

GPS информация (само на ниво устройство)

Тук можете да определите текущото/последното местоположение на устройството. Локализирането може да бъде защитено с една или дори две пароли - вж: Общи настройки - Поверителност - Достъп до GPS



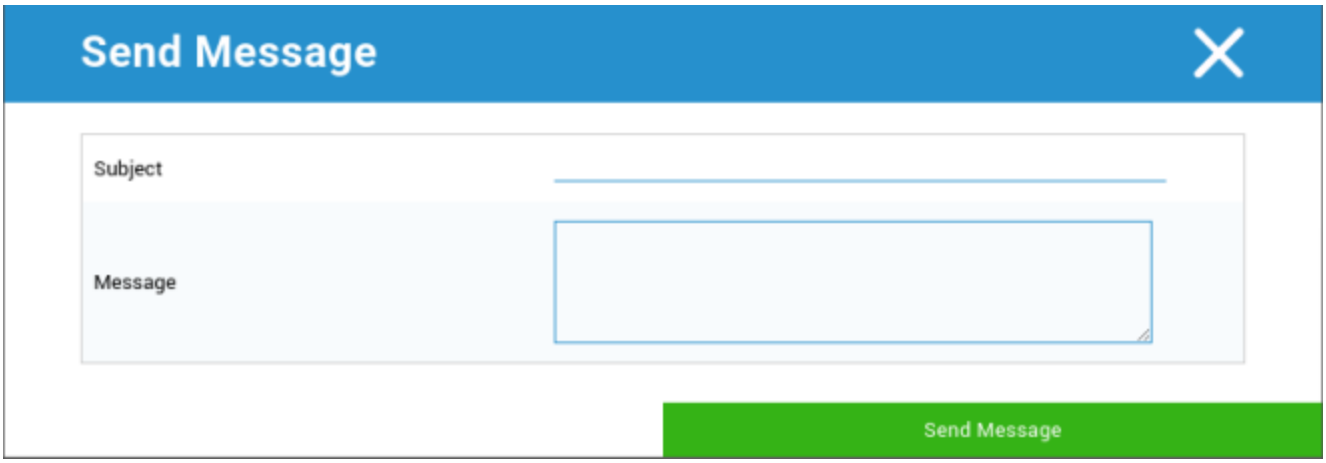
Изтриване и заключване (само на ниво устройство)

В "Изтриване и заключване" можете да извършите следните три действия:

Пълно избърсване	Устройството се възстановява до фабричните си настройки (корпоративните и личните данни се изтриват).
Изтриване на предприятието	От устройството на крайния потребител се премахват само корпоративните данни (всички приложения, данни и т.н., които са били предоставени от AppTec360)
Екран за заключване	Активирано е заключване на екрана, достатъчно е да отключите устройството с паролата на устройството/ ПИН кода.

Съобщение (само на ниво устройство)

Можете да попълните темата и съобщението и да го изпратите на крайно потребителско устройство. Това съобщение ще се покаже в AppTec360 Client.



Конфигурация на сигурността

Парола

В "Парола" можете да зададете парола на устройството, като имате на разположение следните опции за настройка

Минимална дължина на паролата	Определя минималния брой символи, които трябва да съдържа паролата.
Качество на паролата	Сила на паролата Неуточнено = не е уточнено Всяка парола е ок = всяка парола е приемлива най-малко цифрови знаци = трябва да съдържа най-малко цифрови знаци най-малко сложни символи = трябва да съдържа най-малко специални символи поне буквено-цифрови знаци = трябва да съдържа поне буквено-цифрови знаци поне азбучни знаци = трябва да съдържа поне азбучни знаци
Максимално време за заключване при неактивност	Максимално времетраене на екрана. Конфигурира се само максималната стойност, която може да бъде избрана от потребителя.
Минимален брой малки букви, изисквани в паролата	Минимален брой малки букви, изисквани в паролата
Минимален брой главни букви, изисквани в паролата	Минимален брой главни букви, изисквани в паролата
Минимален брой небуквени символи, изисквани в паролата	Минимален брой небуквени символи, изисквани в паролата
Минимален брой цифри, изисквани в паролата	Минимален брой цифри, изисквани в паролата
Минимален брой символи, изисквани в паролата	Минимален брой символи, изисквани в паролата
Време за изтичане на паролата	Установява, след който интервал от време паролата изтича и трябва да се издаде нова парола.
Ограничаване на историята на паролите	Брой на използваните преди това пароли, които не са разрешени
Максимален брой неуспешни опити за парола	Установява колко често паролата може да бъде въведена неправилно, преди да се извърши пълно изтриване на устройството.

Криптиране

В този момент можете да криптирате вътрешната памет на устройството, както и паметта на SD картата.

Изискване за криптиране на съхранението	Ако тази настройка е активирана, паметта на устройството ще бъде криптирана, стига устройството да поддържа тази функция. След като паметта на устройството бъде криптирана за първи път, вече не е възможно да бъде декриптирана. По същия начин политиката за парола ще бъде автоматично променена на 6 буквено-цифрови символа.
Изискване за криптиране на SD карта	Тази настройка се отнася само за устройства на Samsung! Ако тази настройка е активирана, външната SD карта може да бъде криптирана и може да бъде декриптирана само ръчно на устройството на крайния потребител. По същия начин политиката за парола ще бъде автоматично променена на 6 буквено-цифрови символа.

Антивирус

Включването на AntiVirus ще инсталира Ikarus на устройствата. Моля, имайте предвид, че това изисква отделен лиценз, който може да бъде въведен в Общи настройки → Управление на приложенията → Приложения на трети страни.

Автоматично сканиране	Определя дали Ikarus сканира автоматично и колко често извършва това сканиране. Активирането на "Пълно автоматично сканиране" ще извърши пълно сканиране. В противен случай ще бъде извършено бързо сканиране.
Автоматични актуализации	Активира автоматичните актуализации на вирусната база данни и задава колко често да става това.
Защита на приложенията	Позволява сканиране на приложения в допълнение към обикновеното сканиране, което сканира само файлове.
Защита на SD картата	Активира защитата на SD картата. Без това сканирането е ограничено до локалното хранилище.
Актуализация само за Wi-Fi	Ограничава актуализирането до Wi-Fi

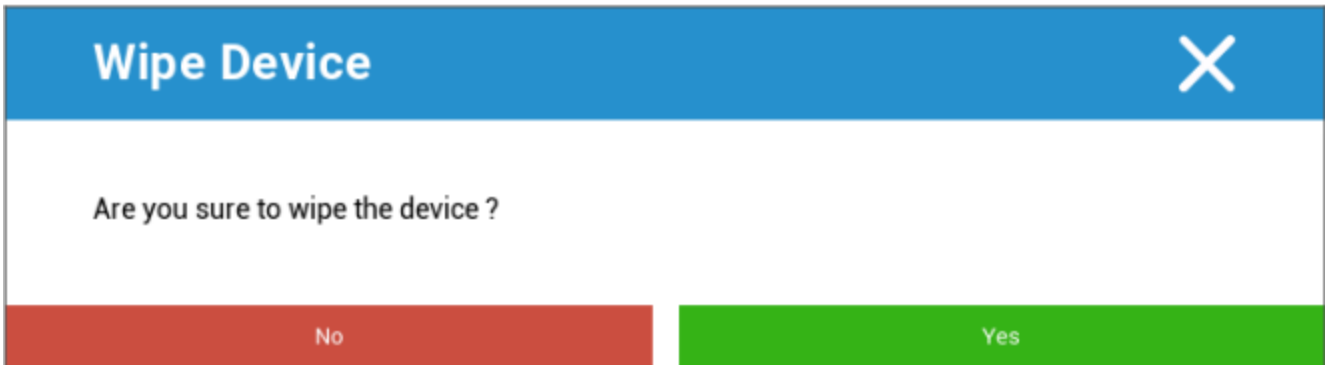
Край на живота (само на ниво устройство)

Избърсване (само на ниво устройство)

Под "Изтриване" можете да възстановите фабричните настройки на устройството. Тук корпоративните и личните данни ще бъдат изтрити от устройството на крайния потребител.

След като кликнете върху символа "минус", трябва да получите следното съобщение

Изтрийте и SD картата?	Паметта на SD-картата също ще бъде изтрита



С "Да" можете да извършите изтриването.

Под "Отчет за изтриване" могат да бъдат показани следните елементи

Изтрити от	История на лицето, извършило изтриването
Дата	Дата
Статус	Статус (например дали изтриването е извършено успешно)

Настройки на ограниченията

Ограничения

Тук могат да се ограничават и блокират различни неща.

Активиране на камерата	Разрешаване на използването на камера
Принудителна автоматична синхронизация	Свързва се с интерфейса "Синхронизация" Включено = синхронизацията е постоянно активирана Изключено = синхронизацията е постоянно деактивирана Избор на потребителя = избран от потребителя
Принудителна Bluetooth	Включено = Bluetooth е постоянно активиран Изключено = Bluetooth е постоянно деактивиран Избор на потребителя = избран от потребителя
Сила на GPS	Включено = GPS е постоянно активиран Изключено = GPS е постоянно деактивиран Избор на потребителя = избран от потребителя
Принудителна точност на местоположението в Google	Включено = Постоянно локализиране в интернет Изключено = Постоянно деактивиране на локализирането в интернет Избор на потребителя = избран от потребителя

За устройствата на Samsung с интерфейс KNOX 1.0 или по-нов са налични следните опции за настройки.

Разрешаване на SD карта	Разрешаване на SD карта
Разрешаване на запис в SD картата	Разрешаване на "запис" в SD картата
Разрешаване на заснемането на екрана	Позволете заснемане на екрана
Разрешаване на клипборда	Разрешаване на клипборда
Архивиране на настройките и данните на приложението в Google Cloud	Изключено = деактивиране на функцията за архивиране на Google Включено = активиране на Google Backup Избор на потребителя = избран от потребителя
Разрешаване на дебъгването на USB	Разрешаване на USB Debugging (използва се например за създаване на дневници на устройствата (ADB))
Разрешаване на Google Crash Report	Разрешаване на изпращането на Google Crash Report от приложенията
Разрешаване на фабричното нулиране	Позволява на потребителя да възстанови фабричните настройки на устройството
Разрешаване на актуализация OTA	Разрешаване на актуализации "по въздуха"
Разрешаване на съхранението в USB хост	Ако е активирана, може да се свърже USB памет под формата на HD или четец на SD карти.
Разрешаване на USB мултимедиен плейър (MTP,PTP)	Разрешаване на USB мултимедиен плейър (MTP,PTP)
Разрешаване на микрофон	Включено = разрешаване на микрофона за приложения на трети страни Изключено = блокиране на микрофона за приложения на трети страни Избор на потребителя = потребителите могат да избират, ако приложението на трета страна има достъп до микрофона.
Разрешаване на NFC (Near Field Communication)	Разрешаване на NFC
Разрешаване на неизвестни източници (APK Sideloading)	Ако е разрешено, страничното зареждане на приложения (APK файлове) е разрешено.

	След като тази настройка е деактивирана, потребителят трябва да я активира ръчно, когато разрешите инсталирането на APK файлове от непознати източници.
Разрешаване на създаването на потребители	Позволява създаването на множество потребители

Собственик на устройството AE

(Устройството трябва да е в режим Android Enterprise Device Owner Mode) Препоръчително е да създадете устройствата като "Android Enterprise" устройство, а не като "Android" устройство.

Защита	
Забрана за споделяне на местоположението	Указва дали на даден потребител е забранено да включва споделяне на местоположението.
Забрана за безопасно стартиране	Указва дали на потребителя не е разрешено да рестартира устройството в безопасен режим на зареждане.
Забрана за нулиране на мрежата	Указва дали на даден потребител е забранено да възстановява мрежови настройки от Настройки.
Забрана за възстановяване на фабричните настройки	Указва дали на даден потребител е забранено да нулира устройството.
Активиране на ADB	Позволява свързване с компютър чрез ADB
Деактивиране на функцията Keyguard	Деактивиране на функцията Keyguard
Собственик на устройството Информация за заключен екран	Задава информацията за собственика на устройството, която да се показва на заключения екран.
Изпълнение на изискванията	Mode Prompt User - Потребителят ще бъде подканен да изпълни необходимите действия. Контейнер за блокиране на режима - скрийте всички приложения, докато не бъдат изпълнени всички изисквания

Управление на приложения	
Разрешаване на свързването на приложения между профили	Позволява на приложенията в родителския профил да обработват уеб връзки от управлявания профил.

Забрана за контрол на приложенията	Указва дали на даден потребител е забранено да променя приложения в Настройки или стартиращи програми.
Забрана за инсталиране на приложения	Указва дали на даден потребител е забранено да инсталира приложения.
Забрана за деинсталиране на приложения	Указва дали на даден потребител е забранено да деинсталира приложения.
Политика за разрешаване по време на изпълнение	Указва как ще се обработват нови заявки за разрешение от приложения.
Разрешаване на неизвестни източници	Ако е разрешено, потребителите могат да зареждат приложения отстрани, като инсталират .apk файл.

Свързаност	
Забрана за конфигуриране на мобилна мрежа	Указва дали на даден потребител е забранено да конфигурира мобилни мрежи.
Конфигурация за забрана на тетеринг	Указва дали на даден потребител е забранено да конфигурира Tethering & portable hotspots.
Забрана на VPN Config	Указва дали на даден потребител е забранено да конфигурира VPN.
Забрана за конфигуриране на Wifi	Указва дали на даден потребител е забранено да променя точките за достъп до Wi-Fi.
Забрана за изходящ NFC лъч	Указва дали на потребителя не е разрешено да използва NFC за предаване на данни от приложения.
Заключване на конфигурацията на WiFi	Тази настройка контролира дали конфигурациите на Wi-Fi, създадени от приложение на собственика на устройството, трябва да бъдат заключени (т.е. да могат да се редактират или премахват само от приложението на собственика на устройството, а не дори от приложението "Настройки").
Активиране на роуминг на данни	Активира роуминг на данни

Bluetooth	
Забрана на Bluetooth	Указва дали Bluetooth е забранен на устройството. Изисква Android 8.0
Забрана за споделяне чрез Bluetooth	Указва дали изходящото споделяне на Bluetooth е забранено на устройството. Изисква Android 8.0
Забрана за конфигуриране на Bluetooth	Указва дали на даден потребител е забранено да конфигурира Bluetooth.

Управление на акаунти	
Забрана за добавяне на управляван профил	Указва дали на даден потребител е забранено да добавя управлявани профили. Изисква Android 8.0
Забрана за добавяне на потребители	Указва дали на даден потребител е забранено да добавя нови потребители.
Забрана за премахване на управляван профил	Указва дали управляваните профили на този потребител могат да бъдат премахнати, освен от собственика на профила. Изисква Android 8.0
Забрана за промяна на сметката	Указва дали на даден потребител е забранено да добавя и премахва акаунти, освен ако не са добавени програмно от Authenticator.

Телефония	
Забрана за изходящи повиквания	Указва, че на потребителя не е разрешено да извършва изходящи телефонни обаждания.
Забрана на SMS	Указва, че на потребителя не е разрешено да изпраща или получава SMS съобщения.

Система	
Забрана за създаване на прозорци	Указва, че не трябва да се създават други прозорци освен прозорците на приложението.
Забрана за задаване на потребителска икона	Указва дали на даден потребител не е позволено да променя своята икона.
Забрана за задаване на тапети	Потребителско ограничение за забрана на задаването на тапет.
Деактивиране на лентата на състоянието	Деактивирането на лентата на състоянието блокира известията, бързите настройки и други екранни наслагвания, които позволяват бягство от устройство за еднократна употреба.
Активиране на автоматично време	Настройва времето автоматично.
Активиране на автоматична часова зона	Автоматично задава часовата зона.

Останете включени, докато сте включени към мрежата	Устройството ще остане активно, докато е свързано към източник на захранване.

Съхранение	
Деактивиране на проверката на приложения	Указва дали на даден потребител е забранено да деактивира проверката на приложението.
Забрана за монтиране на физическа медия	Указва дали на даден потребител е забранено да монтира физически външни носители.
Активиране на услугата за архивиране	Услугата за архивиране управлява всички механизми за архивиране и възстановяване на устройството. Задаването на стойност false ще предотврати архивирането или възстановяването на данни. Услугата за архивиране е изключена по подразбиране. Изисква Android 8.0
Активиране на USB Mass Storage	Разрешава използването на USB Mass Storage.

Клавиатура	
Забрана за автоматично попълване	Указва дали на даден потребител не е разрешено да използва услуги за автоматично попълване. Изисква Android 8.0
Забрана за копиране и поставяне между профили	Указва дали копираното в клипборда на този профил може да бъде вмъкнато в свързани профили.

Звук	
Забрана за коригиране на обема	Указва дали на даден потребител е забранено да регулира основната сила на звука.
Забрана за изключване на звука на микрофона	Указва дали на даден потребител е забранено да регулира силата на звука на микрофона.
Изключване на звука на устройството	Изключване на звука на устройството.

Политика за актуализиране на системата	
Управление на актуализациите на операционната система	Активирайте тази опция, за да зададете поведението на актуализация като автоматично, с прозорец или отложено.

Контейнер BYOD

Android Enterprise

Android Enterprise

Активиране на Android Enterprise	Активиране на Android Enterprise (AE). AE се поддържа от Android 5.1 и по-нови версии.
Изпълнение на изискванията	Mode Prompt User - Потребителят ще бъде подканен да изпълни необходимите действия. Контейнер за блокиране на режима - скрийте всички приложения, докато не бъдат изпълнени всички изисквания
Политика за разрешаване по време на изпълнение	Подканване на потребителя за нови заявки за разрешение Винаги разрешавайте нови заявки за разрешение Винаги отказвайте нови заявки за разрешение Предупреждение: Някои приложения имат проблеми с разпознаването на разрешенията, ако те са зададени автоматично. Ако винаги давате разрешения и срещате проблеми с приложения, които казват, че липсват разрешения, задайте това на "подкани потребителя" и инсталирайте приложението отново.
Разрешаване на изходящ клипборд	Позволява копиране и поставяне от вътрешността на контейнера навън
Разрешаване на резолюцията на идентификатора на повикващия	Показва името на входящо повикване въз основа на контактите в контейнера
Разрешаване на търсенето на контакти	Позволява търсене на имена в контейнера за контакти при провеждане на повиквания
Разрешаване на споделянето на контакти чрез Bluetooth	Позволява достъп до контакт с контейнер в автомобил
Забрана за изходящ NFC лъч	Деактивиране на NFC за контейнера
Разрешаване на неизвестни източници	Ако е разрешено, потребителите могат да зареждат приложения отстрани, като инсталират .apk файл.

Разрешаване на дебъгването на USB	Ако е разрешено, потребителите могат да активират USB Debugging.
Забрана за промяна на сметката	Забранява създаването, изтриването и модифицирането на акаунти в контейнера Имайте предвид, че някои приложения трябва да създадат или модифицират акаунти, за да работят както трябва.

Gmail Exchange

Позволява ви да конфигурирате Gmail в контейнера. Моля, имайте предвид, че включването на тази конфигурация не води до автоматично инсталиране на приложението. Все пак трябва да добавите това приложение като задължително приложение.

Имейл адрес	Имейл адрес
Име на хоста на сървъра	Име на хоста на сървъра
Име за вход	Име за вход
Подпис	Подпис
Брой предишни дни за синхронизиране	Брой на предишните дни за синхронизиране.
Идентификатор на устройството	Идентификатор на EAS. Оставете това поле празно, ако вашата среда не изисква това.
Използване на Secure Sockets Layer (SSL)	Разрешава използването на SSL. Деактивирането на тази функция може да намали сигурността
Приемане на всички сертификати	Приема всички сертификати. Разрешаването на тази опция може да намали сигурността
Разрешаване на неуправлявани акаунти	Позволява на потребителя да добавя допълнителни акаунти
Сертификат на клиента	Качване на клиентски сертификат, ако сървърът на Exchange изисква това

Приложения на системата AE

Тук можете да активирате системните приложения за контейнера Android Enterprise. Имайте предвид, че посоченото приложение трябва да е в паметта на системата, в противен случай нищо няма да се случи.

Парола на контейнера

Само за Android 7.0 или по-нова версия

Позволява ви да зададете конкретно изискване за парола за контейнера.

Минимална дължина на паролата	Определя минималния брой символи, които трябва да съдържа паролата.
Качество на паролата	Сила на паролата Неуточнено = не е уточнено Всяка парола е ок = всяка парола е приемлива най-малко цифрови знаци = трябва да съдържа най-малко цифрови знаци най-малко сложни символи = трябва да съдържа най-малко специални символи поне буквено-цифрови знаци = трябва да съдържа поне буквено-цифрови знаци поне азбучни знаци = трябва да съдържа поне азбучни знаци
Максимално време за заключване при неактивност	Максимално време, докато контейнерът бъде заключен. Конфигурира се само максималната стойност, която може да бъде избрана от потребителя.
Минимален брой малки букви, изисквани в паролата	Минимален брой малки букви, изисквани в паролата
Минимален брой главни букви, изисквани в паролата	Минимален брой главни букви, изисквани в паролата
Минимален брой небуквени символи, изисквани в паролата	Минимален брой небуквени символи, изисквани в паролата
Минимален брой цифри, изисквани в паролата	Минимален брой цифри, изисквани в паролата
Минимален брой символи, изисквани в паролата	Минимален брой символи, изисквани в паролата
Време за изтичане на паролата	Установява, след който интервал от време паролата изтича и трябва да се издаде нова парола.
Ограничаване на историята на паролите	Брой на използваните преди това пароли, които не са разрешени
Максимален брой неуспешни опити за парола	Установява колко често може да бъде въведена неправилна парола, преди контейнерът да бъде изтрит.

Samsung KNOX

Активиране

Тук можете да активирате контейнера Samsung KNOX. Моля, имайте предвид, че това вече не се поддържа от Samsung за Android 10 или по-нови версии. Използване на контейнера Android Enterprise Container за Android 10 или по-нови версии

Код за достъп на Knox

Определяне на насоките, свързани с настройките на паролата на устройството

Минимална дължина на паролата	Определя колко символа трябва да съдържа паролата
Качество на паролата	Сила на паролата Всяка парола е наред = Всяка парола е наред Най-малко цифрови знаци = Трябва да има най-малко цифрови знаци Най-малко сложни знаци = Трябва да има минимум специални знаци Най-малко буквено-цифрови знаци = Трябва да има минимум буквено-цифрови знаци Най-малко буквени знаци = Трябва да има минимум буквени знаци
Изисква се минимален брой сложни знаци	Трябва да има минимум сложни символи
Максимално време за неактивност	Максимално време за неактивност на потребителя, преди заключване на клавиатурата
Разрешаване на удостоверяване с пръстов отпечатък	Разрешаване на удостоверяване с пръстов отпечатък
Разрешаване на удостоверяване с ирис	Разрешаване на удостоверяване чрез разпознаване на ириса
Максимална възраст на паролата	Установява след колко време изтича валидността на паролата и трябва да се издаде нова парола.
История на съхранените пароли	Брой на предишните пароли, които не са разрешени
Максимален брой неуспешни опити за парола	Установява колко често паролата може да бъде подадена неправилно, преди да се извърши пълно изтриване на устройството.

Knox Security

Ограничаване на специфични функционалности на устройството

Активиране на камерата	Разрешаване на използването на камерата
Разрешаване на Samsung KNOX App Store	Разрешаване на използването на магазина за приложения Samsung KNOX
Разрешаване на услугите на Google Play	Разрешаване на услугите на Google Play
Разрешаване на браузъра	Разрешаване на използването на родния браузър
Разрешаване на скрийншоти	Позволете създаването на снимки на екрана
Разрешаване на импортирането на контакти	Ако е активирано, достъпът до контактите на устройството от контейнера KNOX е разрешен.
Разрешаване на износа на контакти	Ако е активирано, достъпът до контактите KNOX от устройството е разрешен.
Разрешаване на импортирането на календара	Ако е активирано, достъпът до календара на устройството от контейнера KNOX е разрешен.
Разрешаване на експорта на календара	Ако е активирано, достъпът до календара KNOX от устройството е разрешен.
Разрешаване на несигурна клавиатура	Разрешаване на използването на клавиатура, която не е защитена
Активиране на импортирането на файлове	Разрешаване на импортирането на файлове в контейнера KNOX
Активиране на експортирането на файлове	Активиране на експортирането на файлове от контейнера KNOX

Knox Exchange

Тук можете да конфигурирате Exchange-профила за контейнера KNOX

Електронен адрес	Имейл адресът на предоставения потребител Обърнете внимание на "заместителите", които можете да използвате за работа с удостоверенията и да не извършвате промени ръчно на всяко устройство. С едно кликване върху **Покажи заместителите** можете да ги покажете сами.
Име на хоста на сървъра	Адрес на сървъра на вашите сървъри на Exchange
Име за вход	Името за вход за съответното устройство на крайния потребител, моля, обърнете внимание и на "заместителите" тук.
Домейн	Адрес на домейна
Парола (само на ниво устройство)	По желание на отделното устройство може да бъде предоставена парола, ако тя остане празна, потребителят ще бъде подканен да въведе паролата си за Exchange.
Брой предишни дни за синхронизиране	Брой дни, определящи кога имейлите се синхронизират обратно
Подпис	Може да се постави подпис.
Сметка по подразбиране	установява, че този имейл акаунт е стандартният акаунт
Използване на Secure Sockets Layer (SSL)	Използване на SSL връзка
Използване на защита на транспортния слой (TLS)	Използване на връзка TLS
Приемане на всички сертификати	Приемат се всички сертификати. Моля, изберете тази опция, ако вашият Exchange Server използва самоподписан сертификат.

Електронна поща на Нокс

Електронен адрес	Имейл адресът на предоставения потребител Обърнете внимание на "заместителите", които можете да използвате за работа с удостоверенията и да не извършвате промени ръчно на всяко устройство. С едно кликване върху **Покажи заместителите** можете да ги покажете сами.
Протокол на входящия сървър	Протокол на входящия сървър IMAP или POP
Адрес на входящия сървър	Адрес на входящия сървър
Входящ порт на сървъра	Входящ порт на сървъра
Вход/потребителско име на входящия сървър	Вход/потребителско име на входящия сървър
Парола на входящия сървър	Парола на входящия сървър
Входящият сървър използва SSL	Входящият сървър използва SSL
Входящият сървър използва TLS	Входящият сървър използва TLS
Входящият сървър приема всички сертификати	Входящият сървър приема всички видове сертификати
Протокол на изходящия сървър	Протокол на изходящия сървър SMTP
Порт на изходящия сървър	Порт на изходящия сървър
Изходящият сървър използва допълнителни пълномощия	Допълнителни пълномощия за изходящия сървър. Ако тази стойност е "изключена", ще се използват настройките на входящия сървър.
Вход/потребителско име на изходящия сървър	Вход/потребителско име на изходящия сървър
Парола на изходящия сървър	Парола на изходящия сървър
Изходящият сървър използва SSL	Изходящият сървър използва SSL
Изходящият сървър използва TLS	Изходящият сървър използва TLS
Изходящият сървър приема всички сертификати	Изходящият сървър приема всички видове сертификати
Подпис	Тук може да се постави подпис.

Уведомяване на потребителя при получаване на нова електронна поща	Уведомяване на потребителя при получаване на нова електронна поща

Приложения Knox

Създайте тук приложенията, които искате да разпространявате на крайните потребителски устройства. След това те ще бъдат налични в контейнера KNOX. За да добавите приложение, процедирайте както в менюто Задължителни приложения

Име на приложението	Име на приложението
Задължително от	Момент във времето, когато е добавено приложението
Източник:	Източник на приложението (Play Store | Собствен)

С натискане на символа съответното приложение може да бъде премахнато отново.

Управление на връзките

Wifi

За тази настройка извършете предварително конфигуриране на крайните потребителски устройства за достъп до вътрешните точки за достъп.

Идентификатор на набора от услуги (SSID)	SSID за мрежата, която трябва да се свърже
Скрита мрежа	Активиране, в случай че AP не излъчва SSID
Вид сигурност	Установяване на типа на сигурност на AP

Вид сигурност

WEP

Парола	Парола за AP

WPA/WPA2

Парола	Парола за AP

802.1x EAP

Метод на EAP	

PWD	Идентичност	Идентичност
	Парола	Парола

PEAP	Протокол за удостоверяване на фаза 2	няма	Без допълнителен протокол
		MSCHAPV2	Протокол MSCHAPV2
		GTC	Протокол на GTC
	Сертификат на CA	Сертификат на CA	
	Идентичност	Идентичност	
	Анонимна самоличност	Анонимна самоличност	
	Парола	Парола	

Метод на EAP	

TTLS	Протокол за удостоверяване на фаза 2	няма	Без допълнителен протокол
		PAP	Протокол PAP
		MSCHAP	Протокол MSCHAP
		MSCHAPV2	Протокол MSCHAPV2
		GTC	Протокол на GTC
	Сертификат на CA	Сертификат на CA	
	Идентичност	Идентичност	
	Анонимна самоличност	Анонимна самоличност	
	Парола	Парола	

TLS	Сертификат на CA	Сертификат на CA
	Идентичност	Идентичност
	Парола	Парола

VPN

Тип на връзката	**Установяване на тип VPN-връзка**

Ако изберете "Per-App VPN" като VPN Type, наличните VPN клиенти ще се променят. Per-App VPN ограничава VPN до определени приложения и стартира VPN връзката автоматично, ако се стартира определено приложение.

AppTec360 VPN клиент	Използва AppTec360 VPN Client в комбинация с Universal Gateway
Име на връзката	Име на VPN връзката
Конфигурация на шлюза	Изберете VPN конфигурацията на универсалния шлюз
Винаги включена VPN услуга	Налага VPN мрежата да бъде винаги активна, така че целият трафик да преминава през нея.
Активиране на функцията Native Lockdown	Блокира всички мрежи, когато устройството не е свързано към VPN. Използвайте тази опция внимателно, тъй като тя може да доведе до пълна загуба на връзката, ако не е конфигурирана правилно. Само за Android Enterprise с Android 7 или по-нова версия
Активиране на заключването на AppTec360	Блокира използването на всички приложения, докато не се стартира VPN връзката

Cisco AnyConnect	
Име на връзката	Име на VPN връзката
Сървър	Адрес на сървъра
Режим на сертификата	Disabled = деактивиран Автоматично = автоматично

L2TP (само за KNOX)	Предлага се само за устройства на Samsung
Име на връзката	Име на връзката
Сървър	Адрес на сървъра
Активиране на L2TP Secret	
Домейни за търсене DNS	DNS търсене на домейни

Тип на връзката	**Установяване на тип VPN-връзка**

PPTP (само за KNOX)	Предлага се само за устройства на Samsung
Име на връзката	Име на VPN връзката
Сървър	Адрес на сървъра
Активиране на криптирането	Активиране на криптирането
Домейни за търсене DNS	DNS търсене на домейни

L2TP / IPSec PSK (само за KNOX)	Предлага се само за устройства на Samsung
Име на връзката	Име на VPN връзката
Сървър	Адрес на сървъра
Предварително споделен ключ на IPSec	Предварително споделен ключ за удостоверяване
Активиране на L2TP Secret	
L2TP Secret	
Домейни за търсене DNS	DNS търсене на домейни

IPSec XAuth PSK (само за KNOX)	Предлага се само за устройства на Samsung
Име на връзката	Име на VPN връзката
Сървър	Адрес на сървъра
Идентификатор на IPSec	Потребителско име за връзката
Предварително споделен ключ на IPSec	Парола за връзката
Домейни за търсене DNS	DNS търсене на домейни

OpenVPN	
Име на връзката	Име на връзката

Профил на OpenVPN	Ето къде ще бъде копирано съдържанието на файла .ovpn
Приложение за OpenVPN	Съществуват две различни приложения за използване на OpenVPN Препоръчваме приложението "OpenVPN за Android". Но като алтернатива може да се използва приложението "OpenVPN Connect".

Ограничения

Тук можете да зададете ограниченията по отношение на управлението на връзката.

Разрешаване на роуминга на данни	Разрешаване на мобилните данни в роуминг
Налагане на роуминг на данни	Ако е активиран, роумингът за мобилни данни се активира за постоянно (не се препоръчва!) Тази настройка замества настройката "Разрешаване на роуминг на данни"!
Следните настройки са налични само при Samsung KNOX 2.0 или по-висока версия	
Разрешаване само на спешни повиквания	Разрешаване само на спешни повиквания
Разрешаване на WiFi	Разрешаване на WiFi
Минимално ниво на сигурност на WiFi мрежата	Минимално ниво на сигурност на WiFi мрежата Отворен = разрешени са всички видове WiFi
Забрана на потребителя да добавя WiFi мрежи	Потребителят не може сам да добавя WiFi мрежа Тази настройка е възможна само ако е дефиниран WiFi профил в "Управление на връзките".
Разрешаване на SMS и MMS	Всички = Разрешен е целият SMS и MMS трафик Само входящи SMS = Разрешени са само входящи SMS съобщения Outgoing SMS Only = Разрешени са само изходящи SMS съобщения Няма = Не се разрешава SMS / MMS трафик
Разрешаване на синхронизирането по време на роуминг	Разрешаване на синхронизирането по време на роуминг Включено = активирано Изключено = деактивирано Избор на потребителя = избор на потребителя
Разрешаване на гласовия роуминг	Разрешаване на гласовия роуминг Включено = активирано Изключено = деактивирано Избор на потребителя = избор на потребителя
Използване на системен http прокси сървър	Използването на HTTP прокси сървър, което се осигурява от настройките на системата в настройките, зависи от свързаната мрежа (WiFi или APN).

APN

Следните настройки са налични само в Samsung SAFE 2.0 или по-висока версия!

Наименование на APN	Наименование на APN	
Име на точката за достъп	Име на APN	
Протокол на изходящия сървър	Не е зададено	
	Няма	
	PAP	Протокол PAP
	CHAP	Протокол CHAP
	PAP или CHAP	Протокол PAP или CHAP
MCC - код на мобилната държава	Тук се въвежда MCC, оставете това поле празно, ако трябва да се използва MCC на поставената SIM карта.	
MNC - Код на мобилната мрежа	Тук се въвежда MNC, оставете това поле празно, ако трябва да се използва MCC на поставената SIM карта.	
Адрес на сървъра	Адрес на сървъра	
Номер на порта на сървъра	Номер на порта на сървъра	
Прокси адрес на сървъра	Прокси адрес на сървъра	
Адрес на MMS сървъра	Адрес на сървъра за MMS, за Standard моля, оставете празен.	
Номер на MMS порта	Номер на MMS порта	
MMS прокси адрес	MMS прокси адрес	
Потребителско име	Потребителско име	
Парола	Парола	
Тип точка за достъп	Позволените типове са: "default", "mms", "supl" Ако това поле е оставено празно, ще се използват "default,supl,mms".	
Предпочитана APN	Предпочита се APN	

Bluetooth

Тук могат да се извършват различни настройки на Bluetooth.

Следните настройки са налични само при Samsung KNOX 1.0 или по-висока версия!

Разрешаване на откриването на устройство чрез Bluetooth	Разрешаване на откриването на устройства чрез Bluetooth
Разрешаване на Bluetooth сдвояване	Разрешаване на сдвояването чрез Bluetooth
Разрешаване на устройства с Bluetooth слушалки	Разрешаване на устройства с Bluetooth слушалки
Разрешаване на Bluetooth устройствата със свободни ръце	Разрешаване на Bluetooth устройствата със свободни ръце
Разрешаване на Bluetooth A2DP устройства	Разрешаване на Bluetooth A2DP аудио стрийминг между устройства
Разрешаване на изходящи повиквания	Разрешаване на изходящи повиквания чрезBT
Разрешаване на прехвърлянето на данни чрез Bluetooth	Разрешаване на прехвърлянето на данни чрез Bluetooth
Разрешаване на Bluetooth тетъринг	Позволява използването на устройството като модем (Bluetooth интернет връзка)
Разрешаване на връзката с компютър чрез Bluetooth	Разрешаване на връзката с компютър чрез Bluetooth

Управление на PIM

Обмен

Предлага се само за Samsung KNOX 1.0 или по-висока версия!

Електронен адрес	Имейл адресът на предоставения потребител Обърнете внимание на "заместителите", които можете да използвате за работа с удостоверенията и да не извършвате промени ръчно на всяко устройство. С едно кликване върху **Покажи заместителите** можете да ги покажете сами.
Име на хоста на сървъра	Адрес на сървъра на вашите сървъри на Exchange
Име за вход	Името за вход за съответното устройство на крайния потребител, моля, обърнете внимание и на "Заместващи символи тук".
Домейн	Адрес на домейна
Парола (само на ниво устройство)	По желание на отделното устройство може да бъде предоставена парола, ако тя остане празна, потребителят ще бъде подканен да въведе паролата си за Exchange.
Брой предишни дни за синхронизиране	Брой дни, определящи кога имейлите се синхронизират обратно
Подпис	Може да се приложи подпис (Съвет: Някои устройства изискват HTML форматиране на подписа).
Сметка по подразбиране	Установява, че този имейл акаунт е стандартният акаунт
Използване на Secure Sockets Layer (SSL)	Използване на SSL връзка
Използване на защита на транспортния слой (TLS)	Използване на връзка TLS
Приемане на всички сертификати	Приемат се всички сертификати. Моля, изберете тази опция, ако вашият Exchange Server използва самоподписан сертификат.

Електронна поща

Тук можете да разпределяте IMAP и POP акаунти към съответните крайни потребителски устройства.

Следните настройки са налични само при Samsung KNOX 1.0 или по-висока версия!		
Електронен адрес	Имейл адресът на предоставения потребител Обърнете внимание на "заместителите", които можете да използвате за работа с удостоверенията и да не извършвате промени ръчно на всяко устройство. С едно кликване върху **Покажи заместителите** можете да ги покажете сами.	
Протокол на входящия сървър	Протокол на входящия сървър	IMAP или POP
Адрес на входящия сървър	Адрес на входящия сървър	
Входящ порт на сървъра	Входящ порт на сървъра	
Вход/потребителско име на входящия сървър	Вход/потребителско име на входящия сървър	
Парола на входящия сървър (само на ниво устройство)	Парола на входящия сървър (само на ниво устройство)	
Входящият сървър използва SSL	Входящият сървър използва SSL	
Входящият сървър използва TLS	Входящият сървър използва TLS	
Входящият сървър приема всички сертификати	Входящият сървър приема всички видове сертификати	
Протокол на изходящия сървър	Протокол на изходящия сървър	SMTP
Порт на изходящия сървър	Порт на изходящия сървър	
Изходящият сървър използва допълнителни пълномощия	Допълнителни пълномощия за изходящия сървър. Ако тази стойност е "изключена", ще се използват настройките на входящия сървър.	
Вход/потребителско име на изходящия сървър	Вход/потребителско име на изходящия сървър	
Парола на изходящия сървър (само на ниво устройство)	Парола на изходящия сървър	

Изходящият сървър използва SSL	Изходящият сървър използва SSL
Изходящият сървър използва TLS	Изходящият сървър използва TLS
Изходящият сървър приема всички сертификати	Изходящият сървър приема всички видове сертификати
Подпис	Подписът може да бъде прикачен тук (Съвет: Някои устройства изискват HTML форматиране на подписа).
Уведомяване на потребителя при получаване на нова електронна поща	Уведомява потребителя за получаване на нов имейл

AE Gmail Exchange

Информация: Тази конфигурация ще бъде приложена към приложението Gmail. Затова трябва да одобрите и инсталирате Gmail.

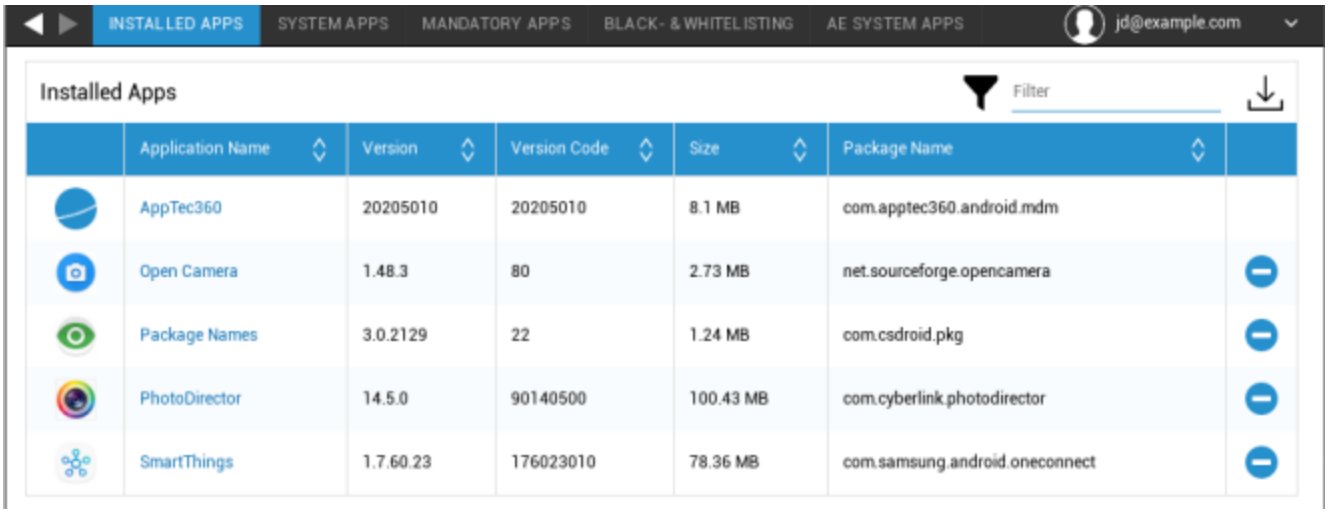
Електронен адрес	Имейл адресът на предоставения потребител Обърнете внимание на "заместителите", които можете да използвате за работа с удостоверенията и да не извършвате промени ръчно на всяко устройство. С едно кликване върху Покажи заместителите можете да ги покажете сами.
Име на хоста на сървъра	Адрес на сървъра на вашите сървъри на Exchange
Име за вход	Името за вход за съответното устройство на крайния потребител, моля, обърнете внимание и на "Заместващи символи тук".
Подпис	Може да се приложи подпис (Съвет: Някои устройства изискват HTML форматиране на подписа).
Брой предишни дни за синхронизиране	Брой дни, определящи кога имейлите се синхронизират обратно
Идентификатор на устройството	Идентификатор на EAS. Оставете това поле празно, ако вашата среда не изисква това.
Използване на Secure Sockets Layer (SSL)	Използване на SSL връзка
Приемане на всички сертификати	Приемат се всички сертификати. Моля, изберете тази опция, ако вашият Exchange Server използва самоподписан сертификат.
Разрешаване на неуправлявани акаунти	Позволява на потребителя да добавя допълнителни акаунти
Сертификат на клиента	Качване на клиентски сертификат, ако сървърът на Exchange изисква това

Управление на приложения

Мениджър на корпоративни приложения

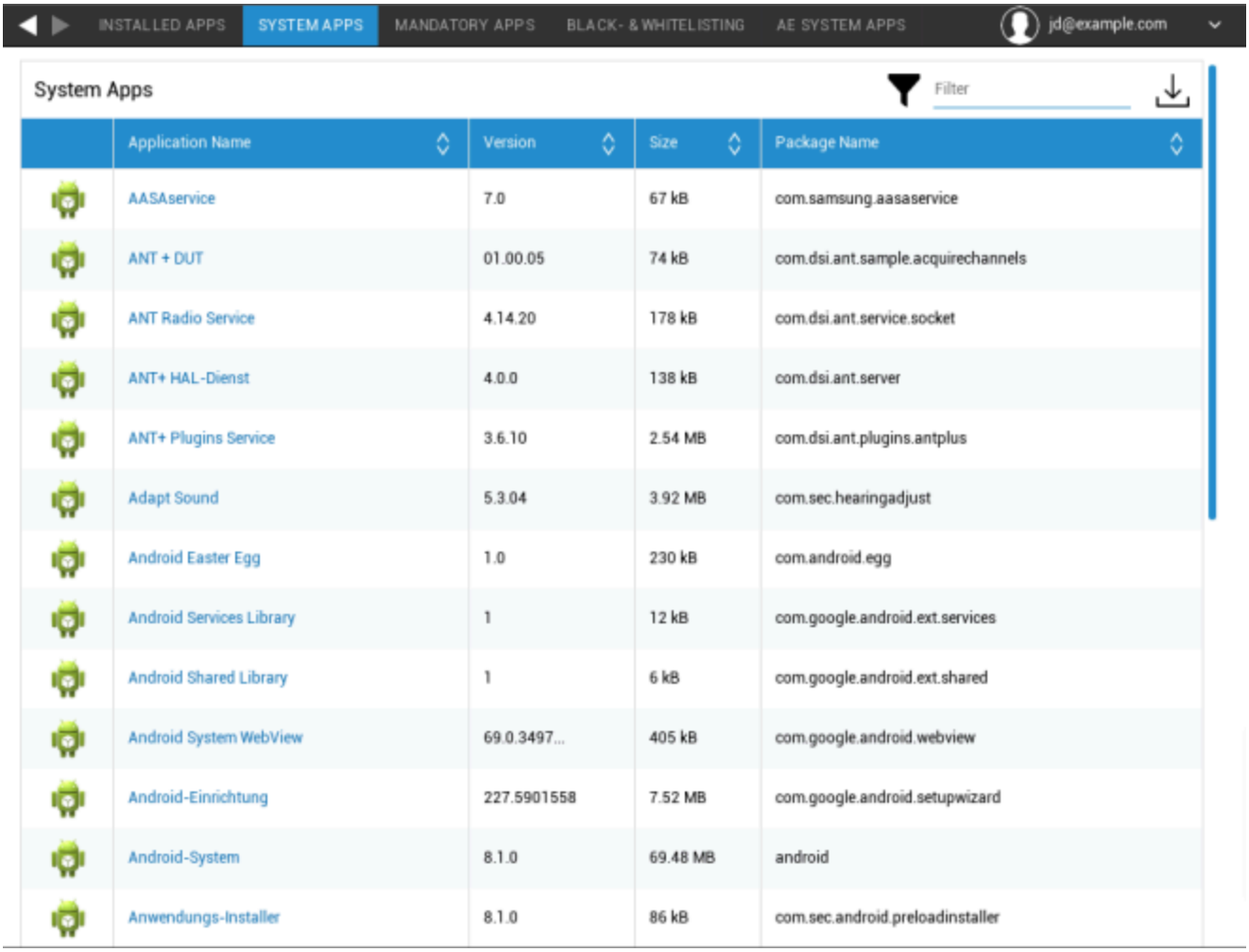
Инсталирани приложения (само на ниво устройство)

Тук ще бъдат показани всички приложения, които в момента са инсталирани на крайното потребителско устройство.


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

Системни приложения (само на ниво устройство)

В "Системни приложения" ще бъдат изброени всички предварително инсталирани системни приложения с името на пакета и версията му.



Application Name	Version	Size	Package Name
AASAservice	7.0	67 kB	com.samsung.aasaservice
ANT + DUT	01.00.05	74 kB	com.dsi.ant.sample.acquirechannels
ANT Radio Service	4.14.20	178 kB	com.dsi.ant.service.socket
ANT+ HAL-Dienst	4.0.0	138 kB	com.dsi.ant.server
ANT+ Plugins Service	3.6.10	2.54 MB	com.dsi.ant.plugins.antplus
Adapt Sound	5.3.04	3.92 MB	com.sec.hearingadjust
Android Easter Egg	1.0	230 kB	com.android.egg
Android Services Library	1	12 kB	com.google.android.ext.services
Android Shared Library	1	6 kB	com.google.android.ext.shared
Android System WebView	69.0.3497...	405 kB	com.google.android.webview
Android-Einrichtung	227.5901558	7.52 MB	com.google.android.setupwizard
Android-System	8.1.0	69.48 MB	android
Anwendungs-Installer	8.1.0	86 kB	com.sec.android.preloadinstaller

Задължителни приложения

В "Задължителни приложения" можете да определите кои приложения трябва да бъдат инсталирани на устройството. В зависимост от конфигурацията и устройството приложението ще се инсталира автоматично или потребителят ще бъде подканен да го инсталира.

Моля, имайте предвид, че се препоръчва да използвате Android Enterprise за лесно управление на приложенията.

Сценариите са изброени по-долу:

Обикновени приложения за Play Store

Инсталирането на приложения в Playstore винаги се нуждае от взаимодействие с потребителя. Освен това в устройството трябва да бъде конфигуриран акаунт в Google.

Инсталиране на приложения в дома

На устройствата на Samsung тези приложения ще бъдат инсталирани безшумно. Единственото изключение е контейнерът, при който потребителят трябва да потвърди инсталацията.

При всеки друг сценарий потребителят трябва да потвърди инсталирането на приложението.

Android Enterprise Play Store приложения

Тези приложения винаги ще се инсталират безшумно, без взаимодействие с потребителя.

За да добавите задължително приложение, щракнете върху "+" и изберете желаното приложение от списъка. Моля, имайте предвид, че не можете да инсталирате приложения от раздела "Google Play Store", ако устройството е конфигурирано с Android Enterprise като напълно управлявано или като контейнер.

Ако използвате Android Enterprise, изберете приложенията от раздела "AE Play Store". За да направите приложенията достъпни тук, потвърдете ги в магазина на Google Enterprise Play, като отидете на General Settings → AE Play Store → Play Store Apps.

Когато премахвате задължително приложение, то също ще бъде деинсталирано от устройството.

Можете да щракнете върху името на приложението в списъка със задължителни приложения и да отидете в раздела "Конфигуриране", за да конфигурирате приложението. Това изисква използването на Android Enterprise и приложението трябва да го поддържа. Затова наличните опции зависят от избраното приложение.

Приложения на системата AE

Тук можете да активирате системните приложения за устройствата с Android Enterprise. Имайте предвид, че посоченото приложение трябва да е в паметта на системата, в противен случай нищо няма да се случи. 296

Ограничения и настройки

Черни и бели списъци

Тук можете да дефинирате черен или бял списък. Всички приложения в черния списък ще бъдат блокирани. Всички приложения, които не са в белия списък, ще бъдат блокирани. Празен черен списък не блокира нищо, а празен бял списък блокира всичко*

**Всички задължителни приложения и приложения от Enterprise App Store ще бъдат автоматично включени в белия списък. Не е необходимо да ги добавяте ръчно.*

Когато щракнете върху "+", можете да потърсите приложение, което искате да добавите към черния или белия списък, или да въведете името на пакета ръчно.

Ограничения на системните приложения

В "Sys App Restrictions" можете, наред с други неща, да блокирате предварително инсталирани приложения и услуги, както желаете.

Деактивиране на браузъра	Деактивиране на стандартния браузър
Деактивиране на календара	Деактивиране на родния календар
Деактивиране на калкулатора	Деактивиране на калкулатора
Деактивиране на браузъра Chrome	Деактивиране на браузъра Chrome
Деактивиране на часовника	Деактивиране на часовника
Деактивиране на контактите	Деактивиране на контактите
Деактивиране на телефонния указател	Деактивиране на родния диалер
Деактивиране на електронната поща	Деактивиране на имейл
Деактивиране на Exchange	Деактивиране на акаунти на Exchange
Деактивиране на Facebook	Деактивиране на приложението Facebook
Деактивиране на галерията	Деактивиране на родното приложение за галерия
Деактивиране на Gmail	Деактивиране на Gmail
Деактивиране на Google Books	Деактивиране на Google Books
Деактивиране на Google Play Kiosk	Деактивиране на Google Play Kiosk
Деактивиране на Google Maps	Деактивиране на Google Maps
Деактивиране на Google Music	Деактивиране на Google Music
Деактивиране на филмите на Google	Деактивиране на филмите на Google
Деактивиране на Google Play Store	Деактивиране на Google Play Store (публичен App Store)
Деактивиране на Google Plus	Деактивиране на Google Plus
Деактивиране на търсенето в Google	Деактивиране на търсенето в Google
Деактивиране на Google Talk / Google Hangouts	Деактивиране на Google Talk / Google Hangouts
Деактивиране на музикалния плейър	Деактивиране на родното приложение за музикален плейър
Деактивиране на настройките	Деактивиране на настройките на устройството
Деактивиране на Sim Toolkit	Деактивиране на услугите на Sim Toolkit
Деактивиране на SMS / MMS	Деактивиране на SMS / MMS
Деактивиране на Street View	Деактивиране на услугите на Street View
Деактивиране на Youtube	Деактивиране на Youtube

Приложения на Samsung

В "Samsung Apps" можете да определите допълнителни настройки и/или ограничения за устройствата Samsung.

Деактивиране на AllShare Play / Samsung Link	Деактивиране на AllShare Play / Samsung Link
Деактивиране на ChatON	Деактивиране на ChatON
Деактивиране на центъра за игри	Деактивиране на центъра за игри
Деактивиране на груповата игра	Деактивиране на груповата игра
Деактивиране на Помощ	Деактивиране на Samsung Help
Деактивиране на KNOX	Деактивиране на контейнера Samsung KNOX
Деактивиране на бележката	Деактивиране на гласовата бележка
Деактивиране на моите файлове	Деактивиране на моите файлове
Деактивиране на оптичния четец	Деактивиране на оптичния четец
Деактивиране на Polaris Office	Деактивиране на Polaris Office
Деактивиране на Readers Hub / Samsung Books	Деактивиране на Readers Hub / Samsung Books
Деактивиране на S Memo	Деактивиране на приложението Samsung Memo
Деактивиране на преводача S	Деактивиране на приложението Samsung Translator
Деактивиране на S Voice	Деактивиране на гласовия асистент S
Деактивиране на приложенията на Samsung	Деактивиране на Samsung App Store
Деактивиране на Samsung Hub	Деактивиране на магазините за развлечения на Samsung
Деактивиране на видео плейъра	Деактивиране на видео плейъра
Деактивиране на гласовия записвач	Деактивиране на гласовия записвач
Деактивиране на WatchON	Деактивиране на WatchON (симулира дистанционно управление)

Приложения на Huawei

Под "Huawei Apps" можете да определите допълнителни настройки и/или ограничения на устройството Huawei.

Деактивиране на DLNA	Деактивиране на DLNA
Деактивиране на инсталатора на приложения	Деактивиране на инсталатора на приложения
Деактивиране на файловия мениджър	Деактивиране на файловия мениджър
Деактивиране на мениджъра за архивиране	Деактивиране на мениджъра за архивиране
Деактивиране на системния актуализатор	Деактивиране на системния актуализатор
Деактивиране на кутията с инструменти	Деактивиране на кутията с инструменти
Деактивиране на времето	Деактивиране на времето
Деактивиране на FM радиото	Деактивиране на FM радиото

Настройки за управление на приложения

Тук можете да определите поведението на актуализация на приложенията InHouse Apps.

Честотата на проверката на актуализациите определя колко често приложението AppTec360 търси актуализации за приложенията на InHouse. След като бъде открита нова версия, тя ще бъде изтеглена и инсталирана.

Wi-Fi Threshold определя дали изтеглянето трябва да бъде ограничено до Wi-Fi връзки, ако приложението е по-голямо от конфигурирания от вас Threshold. Ако тя е по-малка или не сте определили праг, приложението ще се изтегли в Wi-Fi и в клетъчна мрежа.

Магазин за корпоративни приложения

Моля, имайте предвид, че добавянето на приложения тук (Enterprise App Store) НЕ води до автоматичното им инсталиране на устройството(ата). Потребителят трябва да отвори Enterprise App Store на устройството и да инсталира приложението ръчно.

Ако искате автоматично да инсталирате приложения на устройството, отидете в "Управление на приложенията" → "Мениджър на корпоративни приложения" → "Задължителни приложения" и добавете желаните приложения там.

В тази точка можете да разпространявате опционални приложения сред потребителите си.

Playstore

Кликнете върху "+", за да добавите приложение в магазина за игри. Ако използвате Android Enterprise, моля, отидете на "App Management Enterprise Play Store". Също така имайте предвид, че за да инсталирате определените тук приложения, на → устройството трябва да бъде конфигуриран акаунт в Google.

Вътрешен

В точката "Собствени" можете да качвате и разпространявате вътрешно разработени приложения.

Щракнете върху "+", за да добавите приложение InHouse в магазина за приложения на предприятието, което след това може да бъде инсталирано от потребителя. В този диалог можете също така да качите ново приложение на InHouse.

Магазин Play за предприятия

Моля, имайте предвид, че добавянето на приложения тук (Enterprise Play Store) НЕ води до автоматичното им инсталиране на устройството (устройствата). Потребителят трябва да отвори Play Store на устройството и да инсталира приложението ръчно.

Ако искате автоматично да инсталирате приложения на устройството, отидете в "Управление на приложенията" → "Мениджър на корпоративни приложения" → "Задължителни приложения" и добавете желаните приложения там.

В тази точка можете да разпространявате опционални приложения сред потребителите си.

Тук можете да добавяте приложения в Android Enterprise Playstore. Моля, имайте предвид, че трябва да одобрите приложенията в Общи настройки → AE Play Store → Play Store Apps. Тези приложения ще бъдат добавени в нормалния магазин на Google Play.

Също така имайте предвид, че първо трябва да дефинирате макет с приложения в Общи настройки → Управление на приложения → Магазин за приложения → Магазин за приложения → Макет на магазина.

Преди да добавите успешно приложения в магазина, те трябва да са в Layout.

Режим на киоск и стартиране

Режим на киоск

Режимът Kiosk Mode ви позволява да дефинирате предварително приложение или URL адрес. Тогава ще бъде възможно единствено да стартирате/посещавате това приложение и/или URL адрес.

По същия начин различните хардуерни бутони могат да бъдат деактивирани в разнообразния режим Kiosk Mode.

Автоматичен старт	Автоматично стартиране на режима Kiosk, веднага щом профилът достигне до крайното потребителско устройство.
Планиран режим на киоск?	Можете да планирате време за режима на киоск, който ще започва и приключва автоматично в зададено от вас време.
Време на започване	Начален час
Време в минути	Време в минути, след което режимът Kiosk трябва да приключи отново

Тип приложение

Едно приложение	Ако искате да стартирате приложението в режим на киоск, изберете Пакет" под "Тип приложение".
Приложение за киоск	Щракнете тук, за да изберете приложение, което трябва да бъде стартирано в режим Kiosk Mode. Ще намерите обичайния преглед на управлението на приложенията Можете да избирате между "Google Play Store", "Android In-House Apps" и "Packagename".

Тип приложение

URL	Ако искате да стартирате URL адрес в режим на киоск, изберете "URL адрес" под "Тип приложение". След това задайте желания URL адрес
Изчистване на браузъра след неактивност	Тук можете да зададете интервал от време в минути, след който режимът на киоск да се стартира отново.
Изчистване на уеб кеша и бисквитките	Ако активирате тази функция, след рестартиране на киоск режима уеб кешът (бисквитките и кешираните снимки) ще бъде изтрит.
Политика за еднакъв произход	Ако тази функция е активна, потребителят може да сърфира само в подстраниците на определен URL адрес. Например сте дефинирали следния URL адрес:www.mypage.com След това потребителят може да сърфира на: www.mypage.com/subpage
URL адреси в белия списък	Тук можете да поддържате бял списък, в който всички тези URL адреси са разрешени. Максимум 1 URL на ред URL адресът трябва да започва с http:/ или https://
URL адреси в черния списък	Тук можете да поддържате черен списък, в който всички тези URL адреси не са разрешени. Максимум 1 URL на ред URL адресът трябва да започва с http:/ или https://
Ориентация на екрана	Тази настройка е свързана с настройките на екрана Автоматично = автоматично Портрет = вертикален формат Landscape = пейзажен режим

Многофункционално приложение	Ако изберете режима "Multi App" Kiosk Mode, ще се наложи използването на AppTec360 Launcher.
Приложения	Приложение: Изберете Playstore или вътрешно приложение като приложение за киоск. Възможно е също така да въведете име на пакет. Избраното приложение за киоск трябва да е инсталирано на устройството. Не забравяйте да зададете приложението Kiosk като задължително. Пряк път на началния екран: Ако е настроено на "Вкл.", ще бъде създаден пряк път на началния екран. Ако е зададена стойност

		"Изкл.", приложението все пак ще се показва в списъка с приложения.

Включена парола за излизане	Ако активирате тази функция, потребителят може да прекрати режима на киоск с предварително зададена от вас парола.
Парола за излизане	Това е предварително зададената от вас парола.
Автоматично сгъване на лентата на състоянието	Ако е разрешено, лентата на състоянието ще бъде автоматично подравнена. С тази опция потребителите могат да виждат информацията в лентата на състоянието, но нямат достъп до нейните функции.
Деактивиране на лентата на състоянието	Лентата на състоянието съдържа Известия, Преки пътища и Информация. Предлага се само за устройства на Samsung с KNOX 1.0 или по-нова версия.
Деактивиране на клавишите за сила на звука	Деактивиране на клавишите за сила на звука (налично само за устройства на Samsung с KNOX 1.0 или по-висока версия)
Деактивиране на превключвателя за включване и изключване	Деактивиране на превключвателя за включване/изключване (налично само за устройства на Samsung с KNOX 1.0 или по-висока версия)
Деактивиране на бутона Home	Деактивиране на бутона Home. Ако тази функция е активирана, режимът Kiosk може да бъде прекратен само в конзолата AppTec360. (налично само за устройства на Samsung с KNOX 1.0 или по-висока версия)
Деактивиране на лентата за навигация	С тази опция можете да деактивирате лентата за навигация (Назад / Меню). Ако тази функция е активирана, режимът Kiosk може да бъде прекратен само в конзолата AppTec360. (налично само за устройства на Samsung с KNOX 1.0 или по-висока версия)

Настройки за актуализиране на приложенията	
Разрешаване на актуализациите на приложенията	Потребителите ще бъдат подканени да извършат актуализации на приложенията, дори когато режимът Kiosk е активен. На устройства със Samsung KNOX приложенията ще бъдат актуализирани безшумно.
Прозорец за актуализиране	Задайте интервал, през който потребителите ще бъдат подканени да инсталират актуализации на приложения.

TeamViewer

Активиране на необслужван достъп	Ако е разрешено, администраторите могат да управляват устройството от разстояние без взаимодействие с потребителя. Приложението TeamViewer Host трябва да бъде инсталирано на устройството.

AppTec360 Launcher

Активиране на AppTec360 Launcher	На: Включва стартиращото устройство AppTec360. Потребителят трябва да го зададе по подразбиране като стартер еднократно. Забележка: Ако режимът Kiosk Mode е активиран и режимът Kiosk Mode е настроен на "Multi App", използването на AppTec360 launcher ще бъде наложено.
Големи икони	На: Показване на по-голяма версия на иконите на приложенията в лентата за стартиране
Скриване на иконата на приложението AppTec360	На: Скрива напълно приложението AppTec360
Скриване на иконата на магазина AppTec360	На: Скрива напълно AppTec360 Enterprise AppStore

Настройки на AppTec360

Активиране на приложението за настройки на AppTec360	Приложението за настройки на AppTec360 осигурява управление на WiFi и Bluetooth връзките
Активиране на настройките в Multi App Режим на киоск	Ако е разрешено, потребителите могат да получат достъп до приложението AppTec360 Settings, докато режимът Multi App Kiosk Mode е активен.

Дистанционно управление

Splashtop

Показва текущото състояние на настройката на Splashtop. Тук ще видите стъпките, които трябва да извършите, за да осъществите отдалечен достъп до устройството чрез Splashtop. Тук трябва да въведете и кода за разполагане, който можете да получите от уебсайта на Splashtop. Кодът за внедряване е необходим за свързване с устройството.

Teamviewer

Показва текущото състояние на настройката на Teamviewer. Тук ще видите стъпките, които трябва да извършите, за да осъществите отдалечен достъп до устройството чрез Teamviewer.

Управление на съдържанието

Поле за съдържание

Тук можете да активирате Contentbox за това устройство. След като бъде активирано, приложението Contentbox ще бъде инсталирано на устройството.

Сигурен браузър

Тук можете да активирате защитения браузър за това устройство. След като бъде активирано, приложението Secure Browser ще бъде инсталирано на устройството. Този браузър може да бъде конфигуриран така, че да предлага уеб браузър на устройството, който е ограничен според вашите нужди.

Изискване на парола	Изисквайте от потребителя да зададе и използва парола за достъп до браузъра.
Ограничаване на изтеглянията / Отваряне в	Блокира изтегляния от уебсайтове
Ограничаване на качванията	Ограничава качването до определени URL адреси. Не предоставяйте URL адрес, за да блокирате изцяло качването
Разрешаване на копирането	Позволява копиране, изрязване или споделяне на текст в уеб страниците.
Разрешаване на заснемането на екрана	Позволява заснемане на скрийншоти.
Честота на почистване на данните	Изберете с каква честота ВСИЧКИ потребителски данни (история, кеш и т.н.) да се премахват автоматично.
Фирмени отметки	Записките ще се появят в папката "Company bookmarks" (Записки на компанията) в отметките на браузъра. Те не могат да се редактират от потребителя.
Скриване на адресната лента	Скрива адресната лента, така че потребителят да не вижда URL адреса, който посещава.
Бели списъци в браузъра (без Universal Gateway)	Активира бял списък на URL адреси от страна на клиента. - Фирмените отметки винаги са включени в бял списък - Поддържа се само за 100 URL адреса - Моля, използвайте универсалния шлюз за неограничен брой черни и бели списъци

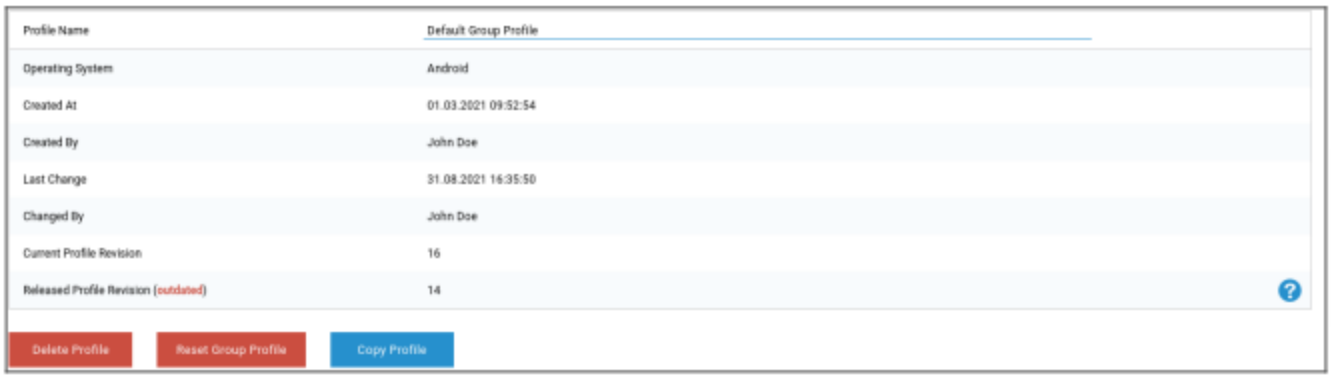
Базиран на шлюз черен и бял списък	Черният списък има следните изисквания: - Работещ универсален шлюз на AppTec360 ("Общи настройки" → "Универсален шлюз") - Работеща VPN конфигурация с определен DNS сървър ("Общи настройки" → "Универсален шлюз" → "VPN настройки") - Конфигурация на черния списък ("Общи настройки" → "Универсален шлюз" → "Черен списък на домейни") - Валидна VPN връзка в профила ("Управление на връзките" → "VPN")

Конфигуриране на компютър с Windows 10

Обща информация

Преглед на профила на групата (само на ниво група)

При отваряне на групов профил ще получите бърз преглед на профила.



Име на профила	Име на профила (може да бъде променено тук)
Операционна система	Операционна система, за която е предназначен профилът
Създаден в	Време на създаване
Създаден от	Създател на профила
Последна промяна	Време на последната промяна в профила
Променено от	Акаунт, в който са направени последните промени
Текуща ревизия на профила	Преразглеждане на запазеното състояние на профила
Освободена ревизия на профила	Присвоена ревизия на профила ("Присвои сега"). Ако зад текста на етикета се показва "(остарял)", това означава, че сте запазили профила, но все още не сте го присвоили, така че устройствата все още ще получават по-стара версия.

Преглед на устройството (само на ниво устройство)

Обобщен преглед на устройството, който съдържа следното:

Име на компютъра	Име на компютъра
Клиент	Устройствата тип Windows
Последно известно местоположение	Географска ширина и дължина на последното известно местоположение на устройствата
Зададени задължителни приложения	Брой на задължителните приложения, назначени за устройството
UID НА КОМПЮТЪРА	UID на компютъра
Издание за операционна система	Показва вашето издание на Windows
Версия на операционната система	Текущо инсталирана версия на Windows
Изграждане на операционна система	Текуща версия на Windows
Операционна система	Текущо инсталирана операционна система
Сериен номер	Сериен номер на устройството
Притежание на устройство	Конфигурираният тип собственост
Тип устройство	Типът на устройството
Вкоренени	Показва дали устройството е вкоренено
Съответстващ	Показва дали устройството е съвместимо
Последно видян	Дата и час, когато са направени промените в профила
Присвояване на потребителя	Показва потребителя или групата, към която това устройство е прикрепено в момента. Можете да преместите устройството, като изберете друг потребител или група от падащия списък.

Настройки

Разрешаване на автоматичното актуализиране	Разрешаване или забраняване на автоматичните актуализации на Os.

Ревизия на конфигурацията (само на ниво устройство)

Тук ще получите преглед на груповия профил, който е зададен на устройството.

Ако щракнете върху профила на групата, ще получите директен достъп до профила и ще можете да извършвате настройки.

Със символа можете да върнете зададените приложения към настройките на груповия профил.

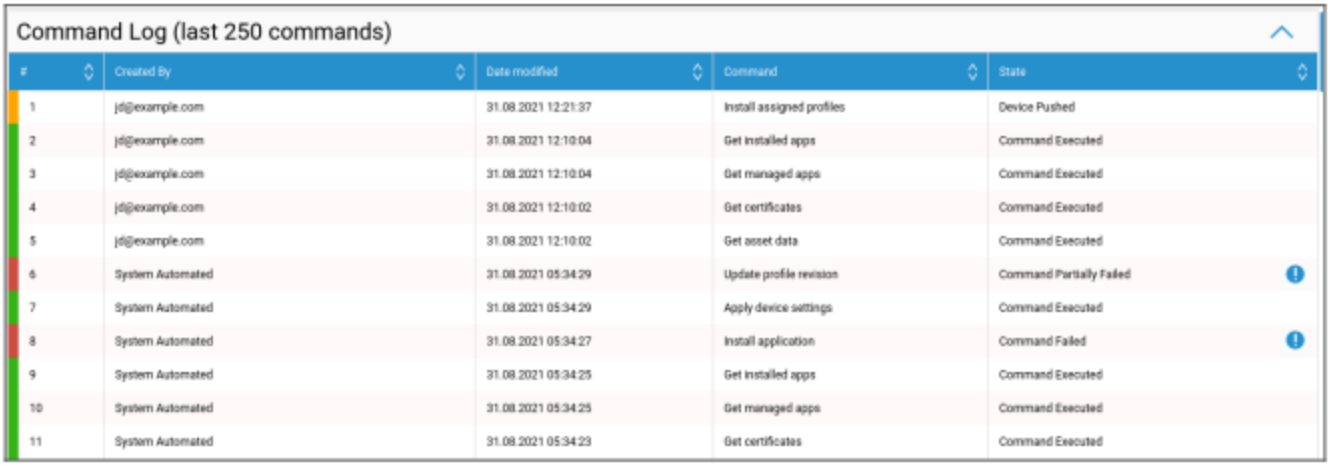
Със символа можете да нулирате профила на устройството, така че да няма никакви настройки.

"Налична е по-нова ревизия" показва, че профилът на групата е променен и запазен, но не е присвоен. Груповият профил трябва да бъде присвоен с "Assign now" (Присвояване сега) на ниво група, за да се приложат промените към устройствата.

Дневник на устройството (само на ниво устройство)

Дневник на командите

Тук можете да видите кои команди са издадени за устройството и какво е тяхното състояние.



Командите, създадени от "System Automated", се създават автоматично от системата.

Възможни състояния на командата

Натиснато устройство	Изпратена е заявка за натискане до услугата за натискане (напр. APNS), за да се каже на устройството да се свърже отново със сървъра на EMM.
Създадена команда	Командата е създадена в системата.
Изпратена команда	Командата е изпратена на устройството, след като то се е свързало със сървъра.
Изпълнена команда	Командата е изпълнена успешно.
Командата е неуспешна	Командата не е изпълнена. *
Командата е частично неуспешна	В зависимост от операционната система на устройството някои команди могат да бъдат групирани заедно. При това някои части от тази група команди не успяха. *
Командата е изпълнена, но в крайна сметка е неуспешна	Командата е изпълнена, но може би не е.
Пренасочване на командата	Командата е била изпратена отново от потребител.
Изхвърлени	Командата беше отхвърлена. Например защото е била заменена от друга команда или устройството е било презаписано и старите команди са били премахнати.

*Ако зад съобщението има възклицателен знак, можете да получите повече информация, като задържите курсора върху иконата.

Управление на активи (само на ниво устройство)

Информация за устройството

Производител	Производител на устройството
Модел	Модел на устройството
Номер на модела	Номер на модела
Операционна система	Операционна система
Версия на операционната система	Версия на операционната система
Сериен номер	Сериен номер
ExchangeID	ExchangeID
Общо RAM	Общо RAM
Резолюция на дисплея	Резолюция на дисплея
Език на телефона	Език на устройството
Версия на фърмуера	Версия на фърмуера
Версия на клиента DM	Версия на клиента за управление на устройства
Версия на хардуера	Версия на хардуера на устройството
Архитектура на процесора	Архитектура на процесора (тип процесор)

Клетъчен

Мрежа на оператора на SIM	Преносна мрежа
Телефонен номер	Телефонен номер
Състояние на роуминга	Състояние на роуминга
IMEI	IMEI
IMSI	IMSI
Фърмуер на модема	Фърмуер на модема

Информация за синхронизиране

Незабавна връзка с DM	Устройството трябва незабавно да създаде връзка с AppTec
Първоначално време за повторение	Първоначално време за повторение за тази първа връзка
Повторения на връзката	Брой на повторните опити за нова връзка след прекъсване на връзката от мениджъра на връзките или грешка на ниво WinInet
Максимално време за сън	Максимално време за престой след грешка при изпращане на пакета
Първи повторения на синхронизацията	Време за първия етап след записването
Интервал за първо повторение	Време за първия етап след записването
Втори повторения на синхронизацията	Време за втория етап след записването
Интервал на повторение на секундата	Време за втория етап след записването
Редовни повторения на синхронизацията	Време за допълнителните етапи след записването
Редовен интервал на повторение	Време за допълнителните етапи след записването

Управление на сигурността

Защита от кражба (само на ниво устройство)

GPS информация (само на ниво устройство)

Тук можете да определите текущото/последното местоположение на устройството. Локализирането може да бъде защитено с една или дори две пароли - вж: "Общи настройки" > "Поверителност" > "Достъп до GPS"

Настройки на GPS

Активиране на GPS проследяване	Разрешаване на редовна синхронизация на GPS информацията.
Интервал на проследяване	Задайте интервала за синхронизиране на GPS информацията.

Конфигурация на сигурността

Парола

Минимална дължина на паролата	Минимална дължина на паролата	
Състав на паролата	Определя броя на специфичните символи, които трябва да съдържа паролата. Те се състоят от главни букви, малки букви, цифри и специални символи.	
Качество на паролата	Тук можете да зададете качеството на паролата	
	Буквено-цифрови	Само цифри и букви
	Цифрови данни	Само числа
	Цифрови или буквено-цифрови	Цифри или цифри и букви
Максимално време на неактивност	Брой минути на неактивност на потребителя в устройството, след които устройството ще бъде заключено. След изтичането на този период потребителят трябва да отключи устройството, като въведе паролата на устройството си.	
Изтичане на паролата	Задаване на времето, за което трябва да се зададе нова парола	
Ограничение на историята на паролите	Брой на използваните преди пароли, които не са разрешени	
Максимален брой неуспешни опити за парола	Брой пъти, в които паролата може да бъде въведена неправилно, преди да се извърши пълно изтриване на устройството	

Антивирусна програма

Антивирусни настройки - Задаване на конфигурация за сканиране	
Вид сканиране	Избира дали да се извърши бързо или пълно сканиране
Задаване на начало на сканиране	Избира времето от деня, в което Windows Defender ще започне сканирането.
Честота на сканиране	Избира деня, в който трябва да се стартира сканирането на Windows Defender
Честота на актуализиране на подписите	Определя интервала в часове, който ще се използва за проверка за подписи

Конфигуриране на типа на файловете за сканиране	
Разрешаване на сканирането на архивни файлове	Разрешаване или забраняване на сканирането на архиви (например .zip) при достъп.
Разрешаване на сканирането на скриптове	Разрешава или забранява функцията за сканиране на скриптове на Windows Defender.
Разрешаване на сканирането на имейли	Разрешаване или забраняване на сканирането на имейли.
Разрешаване на сканирането на мрежови файлове	Разрешаване или забраняване на сканирането на мрежови файлове.
Разрешаване на пълно сканиране на картографирани мрежови дискове	Разрешаване или забраняване на сканирането на картографирани мрежови дискове (разрешава се само когато е разрешено пълно сканиране).
Управление на двупосочното сканиране	Контролира кои набори от файлове трябва да се наблюдават.
Разрешаване на пълно сканиране на сменяеми устройства	Разрешаване или забраняване на пълното сканиране на сменяеми дискове. Започва се само при пълно сканиране.

Вид на файловете, които да бъдат изключени от сканирането	
Игнориране на типовете файлове за сканиране	Дефиниране на набор от типове разширения на файлове. Всяко разширение на файла за всяко поле.
Игнориране на пътищата към директориите	Дефинирайте набор от пътища към директории, за да не ги сканирате. По една пътека на поле. Примери: Примери: "C:\Example", "C:\Windows" или "C:\Users".
Изключване на процеси от сканиране	Изключване на файлове, които са били отворени от определени процеси, от антивирусни сканирания на Microsoft Defender. . По една пътека на поле. Примери: "C:\myFile.exe", "C:\Windows\myProcess.exe", "C:\myScript.bat

Допълнителни настройки	
Позволете наблюдение в реално време	Разрешаване или забраняване на функцията за наблюдение в реално време на Windows Defender
Позволете мониторинг на поведението	Разрешаване или забраняване на функцията за наблюдение на поведението на Windows
Разрешаване на защитата в облака	Разрешаване или забраняване на Windows Defender да изпраща информация на Microsoft за всеки открит проблем. Microsoft ще анализира тази информация, ще научи повече за проблема, който засяга устройството, и ще предложи подобрени решения.
	Поведение за изпращане на проби
Разрешаване на защитата IOAV на Windows Defender	Разрешаване или забраняване на защитата Windows Defender IOAV
Разрешаване на достъпа до потребителския интерфейс на Defenders "Защита при достъп"	
Среден коефициент на натоварване на процесора	Представлява средния коефициент на натоварване на процесора за сканирането на Windows Defender (в проценти).

Обработка на зловреден софтуер	
Ниска тежест	За всяко ниво на сериозност можете да определите как устройството да обработва зловреден софтуер. Наличните опции са: • Clean • Карантина • Премахване на • Позволете • Дефинирано от потребителя • Блок
Умерена тежест	
Голяма тежест	
Тежка тежест	
Дни за задържане на почистения зловреден софтуер	Период от време в дни, през който файловете/позициите от карантината ще се съхраняват в системата. Стойността по подразбиране е 0, което

	запазва елементите в карантината и не ги премахва автоматично. Максималната стойност е 90.

Център за сигурност

Център за сигурност на Windows - Настройки за сигурността на Windows	
Деактивиране на потребителския интерфейс за защита от вируси и заплахи	
Скриване на рансъмуер Потребителски интерфейс за възстановяване на данни	
Деактивиране на потребителския интерфейс за защита на профила	
Деактивиране на защитната стена и на потребителския интерфейс за мрежова защита	
Деактивиране на потребителския интерфейс за управление на приложения и браузъри	
Забрана за промени в защитата от експлоатиране	Да се забрани на потребителя да прави промени в настройките за защита от експлоатиране
Деактивиране на потребителския интерфейс за сигурност на устройството	
Скриване на отстраняване на проблеми с TPM	Скриване на настройките за отстраняване на неизправности в TPM
Деактивиране на бутона Clear TPM	
Деактивиране на потребителския интерфейс за производителността и състоянието на устройството	
Деактивиране на потребителския интерфейс на семейните опции	

Персонализиране на тостове	
Активиране на персонализирана информация за поддръжка	Разрешете показването на персонализирана информация за контакт с поддръжката на вашата компания в долния десен ъгъл на приложението "Център за сигурност".
Адрес на електронна поща	Задаване на имейл адреса на компанията
Име на компанията	Задайте името на компанията
Телефон на компанията	Задаване на телефон на компанията
URL адрес за помощ	Задайте URL адрес за помощ на компанията

Допълнителни настройки	
Деактивиране на известията	Деактивиране на показването на известията от Центъра за сигурност на Windows Defender.
Скриване на препоръките за актуализация на фърмуера на TPM	Скриване на препоръката за актуализиране на фърмуера на TPM, когато е открит уязвим фърмуер.
Показвайте името на компанията и опциите за контакт	Показвайте името на фирмата си и опциите за контакт в картата с контакти в Центъра за сигурност на Windows Defender.
Скриване на Secure Boot	Скриване на зоната за зареждане на сигурността.
Скриване на контрола на зоната за уведомяване за сигурността	Скриване на контрола на зоната за известия на Windows Security.

Конфигуриране на защитната стена

Конфигурация на защитната стена - Глобални настройки	
Игнориране на набора за удостоверяване	Игнориране на целия набор от удостоверения, ако те не поддържат всички набори от удостоверения, посочени в набора.
Вид на опашката от пакети	Указва как се активира мащабирането на софтуера от страната на получаването както за криптираното получаване, така и за изчистването на пътя за препращане за сценария на IPsec тунелен шлюз.
Деактивиране на извършването на щатното филтриране на FTP	Ако е деактивирана, няма да се извършва филтриране на FTP (File Transfer Protocol), за да се разрешат вторични връзки.
Време на бездействие на асоциацията за сигурност	В това поле се конфигурира времето за бездействие на асоциацията за сигурност в секунди. Асоциациите за сигурност се изтриват, след като не се наблюдава мрежов трафик за този определен период от време.
Кодиране на предварително потвърден ключ	Задаване на кодирането на предварително потвърдения ключ
Изключения от IPSec	Конфигуриране на изключенията на интернет протокола
Проверка на списъка с отзовани удостоверения	

Профили на защитната стена (профил на домейна / личен профил / публичен профил)	
Активиране на защитната стена за този профил	
Деактивиране на известията	Деактивиране на показването на известие на потребителя, когато дадено приложение е блокирано да слуша на даден порт.
Блокиране на уникаст отговори на мултикаст излъчвания	
Прилагане на правила за защитната стена за разрешени приложения	Ако не е наложена, правилата на защитната стена за разрешени приложения в локалния магазин се игнорират и не се прилагат.
Прилагане на глобални правила за защитна стена на портовете	Ако не е наложена, правилата на глобалната защитна стена за портове в локалния магазин се пренебрегват и не се прилагат. Настройката има значение само ако е зададена или изброена в хранилището на груповата политика или ако е изброена от GroupPolicyRSoPStore
Прилагане на правилата на защитната стена	Ако не е наложена, правилата на защитната стена от локалния магазин се игнорират и не се прилагат.
Прилагане на правила за сигурност на връзката	Ако не е наложена, правилата за сигурност на връзката от локалния магазин се игнорират и не се прилагат.
Изходящо действие по подразбиране	Действието, което защитната стена извършва по подразбиране при изходящи връзки
Входящо действие по подразбиране	Действието, което защитната стена извършва по подразбиране при входящи връзки
Деактивиране на режима Stealth	Скритият режим е механизъм в защитната стена на Windows, който помага на злонамерени потребители да не откриват информация за мрежовите компютри и изпълняваните от тях услуги.
Деактивиране на предотвратяването на отговора на непоискан трафик	Ако е деактивирана, правилата за скрит режим на защитната стена не трябва да пречат на хост компютъра да отговаря на непоискан мрежов трафик, ако този трафик е защитен чрез IPsec.

Правила на защитната стена

Правила на защитната стена	
Име	Наименование на правилото
Описание	Описание на правилото
Действие	Посочете дали това правило ще блокира трафика, или ще го разреши. Моля, имайте предвид, че опцията "Блокиране" може също така да блокира трафика (в зависимост от останалата част от конфигурацията) между сървъра MDM и устройството.
Посока	
Активиране на обхождането на ръбове (налично само когато е зададено **направление** за **входящ трафик**)	Показва, че на определен входящ трафик е разрешено да се тунелира през NAT и други крайни устройства, като се използва технологията за тунелиране Teredo.

Програми и услуги	
Определяне на приложения, всички останали	Ако не е разрешено, ще се разглеждат всички приложения.
Име на семейството на пакета	Името на фамилията пакети, за която ще се прилага правилото.
Пътят на файла на приложението	Пълното приложение, например C:\Windows\System\Notepad.exe, за което ще се прилага правилото
Напълно квалифицирано двоично име	Напълно квалифицираното двоично име, за което ще се прилага правилото. FQBN е низ в следната форма: {Издател\Продукт\Филеново име,Версия}
Име на услугата	Въведете името на услугата (напр. "EventLog"). Можете да получите списък с имената на услугите в Powershell, като изпълните командата "Get-Service".

Протоколи и портове				
Протокол	Протоколът, използван от правилото.			
	Налични стойности: - Всеки - Потребителски - HOPORT - ICMPv4 - IGMP - TCP - UDP - IPv6 - IPv6-маршрут - IPv6-Frag - GRE - ICMPv6 - IPv6-NoNxt - IPv6-Opts - VRRP - PGM - L2TP	Когато е зададена стойност Custom	Въведете номер на протокола между 0 и 255	Номерът на протокола
		Когато е зададена стойност TCP или UDP	Посочете локални портове, в противен случай ще се използват всички	Локални портове, които правилото ще използва, разрешени са и портове от обхвата.
			Местно пристанище	Единичен порт или набор от портове. Например 100-120, 200, 300-320.
			Посочете отдалечени портове, в противен случай ще се използват всички	Отдалечени портове, които правилото ще използва, разрешени са и портове от обхвата.
			Отдалечен порт	Единичен порт или набор от портове. Например 100-120, 200, 300-320.

Обхват	
Посочете местни IP адреси, в противен случай - всеки IP адрес	Набор от локални IP адреси, може да бъде и диапазон от IP адреси, разделени с -
Местен IP адрес	Набор от единични IP адреси или обхват от IP адреси, разделени с -
Посочете отдалечени IP адреси, в противен случай всеки отдалечен IP адрес	Посочете набор от отдалечени IP адреси, като това може да бъде и диапазон от IP адреси, разделени с "-".
Отдалечен IP адрес	Задаване на единични IP адреси или диапазон от IP адреси
Токени	Токени, които могат да бъдат зададени заедно с отдалечени адреси. Tokens Intranet, RmtIntranet и Ply2Renders се поддържат в Windows 10, версия 1809 и по-нова.

Разширени настройки	
Посочете профилите, в противен случай ще се използват всички	Ако е изключено, ще се използват всички профили.
Домейн	Профил на домейна
Частна	Личен профил
Публичен	Публичен профил
Посочете интерфейси, в противен случай ще се използват всички.	Ако е изключено, ще се използват всички интерфейси.
Локална мрежа	Интерфейс на локалната мрежа
Отдалечен достъп	Интерфейс за отдалечен достъп
Безжичен	Безжичен интерфейс

Местни директори	
Добавяне на оторизирани местни потребители	Разрешаване на добавянето на списък с местни потребители, които ще използват това правило
Оторизирани потребители	Списък на оторизираните местни потребители за това правило. Потребителят трябва да е във формат SDDL (Security Description Definition language), например PC_NAME\USERNAME. Това поле не трябва да се попълва, ако името на услугата е зададено да използва това правило.

Настройки на ограниченията

Функционалност на устройството

Разрешаване на SD карта	Разрешаване на използването на SD карта
Разрешаване на камерата	Разрешаване на използването на камерата
Разрешаване на услугата за местоположение	Разрешаване на услугата за местоположение на устройството
Разрешаване на странично зареждане на приложения	Разрешаване на инсталирането на приложения от непознати източници
Разрешаване на режима за разработчици	Позволява режим за разработчици
Разрешаване на роуминга на клетъчни данни	Разрешаване на роуминг на клетъчни данни
Разрешаване на Cortana	Разрешаване на гласовия асистент Cortana
Разрешаване на търсенето да използва местоположението	Позволете на търсенето да използва местоположението
Разрешаване на добавянето на имейл акаунт, различен от този на Microsoft	Посочете дали на потребителя е разрешено да добавя имейл акаунти, които не са MSA.
Разрешаване на връзката с акаунта на Microsoft	Посочете дали да разрешите използването на MSA акаунт за удостоверяване и услуги, които не са свързани с имейл.
Разрешаване на синхронизирането на моите настройки	Позволява синхронизиране на настройките в цялото устройство

Защитени имена на домейни на предприятия	Посочва имената на домейни на предприятието, разделени с ";".
Разрешаване на потребителя да забрани възстановяването на системата	Позволява на потребителя да забрани възстановяването на системата. **ПРЕДУПРЕЖДЕНИЕ!** Тази функция трябва да се използва само на устройства, които са собственост или са предоставени от предприятието или организацията, или на устройство, собственост на потребителя, когато потребителят разрешава устройството да се управлява изцяло от предприятието. Ако деактивирате тази настройка на политиката, Възстановяване на системата е изключено и съветникът за възстановяване на системата не може да бъде достъпен. Опцията за конфигуриране на Възстановяване на системата или създаване на точка за възстановяване чрез Защита на системата също е деактивирана.
Разрешаване на отписването на потребители	Позволява на потребителя да премахне корпоративната част от устройството и по този начин да се изключи от сървърите на AppTec360. Ако това се случи, управлението на устройството ще бъде невъзможно. **ПРЕДУПРЕЖДЕНИЕ!** Тази функция трябва да се използва само на устройства, които са собственост или са предоставени от предприятието или организацията, или на устройство, собственост на потребителя, когато потребителят разрешава устройството да се управлява изцяло от предприятието. Ако деактивирате тази настройка на политиката, потребителите няма да могат да премахват MDM записвания. Посочете дали на потребителя е разрешено да изтрие акаунта на работното място чрез контролния панел на работното място. MDM сървърът винаги може да изтрие акаунта от разстояние.

BitLocker

Конфигурация на BitLocker

Общи настройки	
Изискване за криптиране на устройството	Поискайте от потребителите да разрешат криптирането на устройството.В зависимост от изданието на Windows и системната конфигурация, потребителите може да бъдат помолени: - За да потвърдите, че криптирането от друг доставчик не е разрешено. - Изключване на функцията BitLocker Drive Encryption и повторно включване на функцията BitLocker.
Методи за криптиране	
Метод за криптиране на дискове на операционната система	
Метод за криптиране на фиксирани дискове с данни	
Метод за криптиране на преносими дискове с данни	
Деактивиране на предупреждението за криптиране на дискове от трети страни	Деактивиране на предупредителния сигнал за услугата за криптиране на дискове на трета страна, която се използва на устройството. От версия 1803 на Windows 10 тази настройка се поддържа само за устройства, присъединени към Azure Active Directory.
Разрешаване на стартирането на криптиране, докато потребител, който не е администратор, е влязъл в системата	Поддържа се само за устройства, присъединени към Azure Active Directory

AppTec360 разширения	
Безшумно криптиране	Ако е избрано заедно с "Изискване за криптиране на устройствата", услугата за управление на AppTec360 ще стартира автоматично безшумно криптиране на дисковете на устройствата.
Автоматично генериране на потребителски пълномощия	Криптираният диск на операционната система ще бъде защитен с автоматично генерирани потребителски данни. Или TPM PIN код, когато е наличен TPM, или шестцифрена текстова парола. Генерираните идентификационни данни се изпращат на имейл адреса, регистриран за дадено устройство. Ако тази опция е изключена, единствената възможна защита за безшумно криптиране е използването на TPM. В този случай за устройства без TPM тихото криптиране ще се провали.
Криптиране на фиксирани дискове	Всички налични фиксирани дискове с данни също ще бъдат криптирани и защитени с "Автоматично отключване", като се използва ключ, съхранен на диска на операционната система.

Настройки на диска на операционната система

Изискване за допълнително удостоверяване при стартиране	Тази настройка ви позволява да конфигурирате дали BitLocker да изисква удостоверяване при всяко стартиране на компютъра. Тази настройка се прилага по време на настройката на BitLocker. Ако разрешите тази настройка, потребителите могат да конфигурират разширени опции за стартиране в съветника за настройка на BitLocker.
Блокиране на BitLocker без съвместим TPM	
Само TPM	
TPM и PIN	
TPM и ключ	
TPM, ключ и PIN	Ако искате да изисквате използването на ПИН код и USB флаш устройство (ключ), потребителят трябва да конфигурира BitLocker, като използва инструмента за команден ред "manage-bde" вместо съветника за конфигуриране на BitLocker Drive Encryption.

Изискване за минимална дължина на ПИН кода

	Минимален брой символи

Конфигуриране на съобщението и URL адреса за възстановяване преди зареждане	Конфигурирайте цялото съобщение за възстановяване или заменете съществуващия URL адрес, който се показва на екрана за възстановяване с ключ преди стартиране, когато устройството на операционната система е заключено. Забележка: Не всички знаци и езици се поддържат при предварително зареждане. Силно се препоръчва да проверите дали използваните от вас символи се появяват правилно на екрана за възстановяване преди стартиране на системата.
	Опция за съобщение за възстановяване преди стартиране на системата
	Потребителско съобщение за възстановяване
	Потребителски URL адрес за възстановяване

Опции за възстановяване на дискове с операционна система		Тази настройка ви позволява да контролирате начина, по който се възстановяват защитени с BitLocker дискове на операционни системи при липса на необходимите пълномощия. Тази настройка се прилага по време на настройката на BitLocker. По подразбиране е разрешен агент за възстановяване на данни, базиран на сертификат, като опциите за възстановяване могат да бъдат зададени от потребителя, включително паролата за възстановяване и ключа за възстановяване, а информацията за възстановяване не се архивира в AD DS.
	Агент за възстановяване на данни, базиран на блок сертификат	Посочете дали агентът за възстановяване на данни може да се използва със защитени с BitLocker дискове на операционната система. Преди да може да се използва агент за възстановяване на данни, той трябва да бъде добавен от елемента Политики на публичния ключ в Конзолата за управление на групови политики или в редактора на локални групови политики. За повече информация относно добавянето на агенти за възстановяване на данни направете справка с Ръководството за внедряване на BitLocker Drive Encryption в Microsoft TechNet.
	Настройки на паролата за възстановяване на BitLocker	
	Настройки на ключа за възстановяване на BitLocker	
	Записване на информация за възстановяване на BitLocker в Active Directory Domain Services	
	Конфигурация на хранилището за възстановяване на AD DS BitLocker	Съхраняването на пакета с ключове подпомага възстановяването на данни от диск, който е бил физически повреден.
	Изискване за съхранение на данни за възстановяване в AD DS	Предотвратяване на активирането на BitLocker от потребителите, освен ако компютърът не е свързан към домейна и

Фиксирани настройки на задвижването	
Опции за възстановяване на фиксирани дискове	Тази настройка ви позволява да контролирате начина, по който защитените с BitLocker фиксирани дискове се възстановяват при липса на необходимите пълномощия. Тази настройка се прилага по време на настройката на BitLocker. По подразбиране е разрешен агент за възстановяване на данни, базиран на сертификат, като опциите за възстановяване могат да бъдат зададени от потребителя, включително паролата за възстановяване и ключа за възстановяване, а информацията за възстановяване не се архивира в AD DS.
Агент за възстановяване на данни, базиран на блок сертификат	
Настройки на паролата за възстановяване на BitLocker	
Настройки на ключа за възстановяване на BitLocker	
Записване на информация за възстановяване на BitLocker в Active Directory Domain Services	
Конфигурация на хранилището за възстановяване на AD DS BitLocker	Съхраняването на пакета с ключове подпомага възстановяването на данни от диск, който е бил физически повреден.
Изискване за съхранение на данни за възстановяване в AD DS	Предотвратете активирането на BitLocker от потребителите, освен ако компютърът не е свързан с домейна и архивирането на информацията за възстановяване на BitLocker в AD DS е успешно. Забележка: Паролата за възстановяване се генерира автоматично.
Отказване на достъп за запис до незащитени фиксирани дискове	

Настройки на преносимо устройство	
Отказване на достъп за запис до незащитени сменяеми дискове	Отказване на достъп за запис до сменяеми дискове с данни, които не са защитени от Bitlocker. Забележка: Ако "Removable Disks: Deny write access" е разрешена в груповата политика, тази настройка на политиката ще бъде пренебрегната.
Отказване на достъп за запис до устройства, конфигурирани в друга организация	Само на дискове с идентификационни полета, които съвпадат с идентификационните полета на компютъра, ще бъде предоставен достъп за запис. Тези полета се определят от настройката на груповата политика "Предоставяне на уникални идентификатори за вашата организация".

Състояние на BitLocker

Тук можете да видите текущото състояние на криптираните с BitLocker дискове

C [OS Drive]
Статус на криптиране
Криптирани (%)
Статус на защита
Метод на криптиране
Протектори за ключове
Парола за възстановяване

С едно щракване върху бутона "Rotate recovery password" можете да завъртите паролата за възстановяване на BitLocker.

Управление на сертификати

Списък на сертификатите

Тук е представен списък на сертификатите, които са инсталирани на показваното устройство.

Конфигурация на сертификата

Тук можете да конфигурирате сертификатите и начина, по който те ще бъдат инсталирани на устройството.

Доверен сертификат	
Описание	Описание на сертификата
Обхват	Обхват на разгръщане на сертификата: Текущ потребител срещу устройство
Съхранение на сертификати	"Ненадеждни сертификати" е налична само при стартиране на Windows 10, версия 1803
Файл със сертификат	Качване на файл PKCS#1

Сертификат за самоличност			
Описание	Описание на сертификата		
Обхват	Обхват на разгръщане на сертификата: Текущ потребител срещу устройство		
Ключово местоположение	Доставчикът за съхранение на ключове, в който да се инсталира частният ключ.		
		TPM. Отказ, ако няма TPM	
	TPM. Ако няма TPM, се преминава към софтуерен KSP		
	Доставчик на софтуерни ключове за съхранение		Маркиране на частния ключ като експортируем
	Windows Hello за бизнеса	Име на контейнера	Посочва името на контейнера Windows Hello for Business (известен преди като Microsoft Passport for Work).
		Текст на съобщението за ПИН	Определя персонализирания текст, който да се показва в подкана за въвеждане на ПИН код на Windows Hello for Business по време на записването на сертификат.

Удостоверение	Качване на файл PKCS#12

SCEP

Описание	Описание на сървъра SCEP		
Обхват на внедряване	Обхват на разгръщане на сертификата: Текущо устройство срещу потребител		
URL адреси на сървъра SCEP	Един или повече сървъри, които издават сертификати чрез SCEP		
Тема	Представяне на име в X.500. Например "C=US, O=Microsoft Corporation, CN=foo, 1.2.5.3=bar"		
Алтернативни наименования на предмета	Тип	Имейл адрес	
		DNS	
		URI	
		Основно име на потребител (UPN)	
Пръстови отпечатъци на CA	Пръстовият отпечатък SHA1 на сертификата на удостоверяващия орган. E.g. 31:8F:1E:78:5C:D5:12:9F:7E:3B:AD:F3:1C:C0:19:03:96:43:A9:E5		
Период на валидност единици	Дни, месеци или години		
Период на валидност			
Предизвикателство	Използва се като предварително споделена тайна за автоматично записване		
Повторения	Броят на повторните опити на устройството, ако сървърът изпрати отговор PENDING. Стойността по подразбиране е 5. Максималната стойност е 30.		
Забавяне на повторението	Брой минути за изчакване преди повторен опит. Стойността по подразбиране е 5. Минималната стойност е 1.		
Размер на ключа	Размер на ключа в битове		
Алгоритъм за хеш	Семейство алгоритъми за бърз достъп		
Ключова употреба	Разширението за използване на ключа определя предназначението (напр. шифроване, подписване) на ключа, съдържащ се в сертификата. Трябва да се избере поне една от опциите "Цифров подпис" или "Шифроване на ключове".		
Разширено използване на	Определя разширените употреби на ключове.В зависимост от конфигурацията на сървъра SCEP. Посочете списъка със съответните		

ключовете	OID, например 1.3.6.1.5.5.7.3.2 (Удостоверяване на клиента)		
Ключово местоположение	Доставчикът за съхранение на ключове, в който да се инсталира частният ключ.		
		TPM. Отказ, ако няма TPM	
	TPM. Ако няма TPM, се преминава към софтуерен KSP		
	Доставчик на софтуерни ключове за съхранение		
	Windows Hello за бизнеса	Име на контейнера	Посочва името на контейнера Windows Hello for Business (известен преди като Microsoft Passport for Work).
		Текст на съобщението за ПИН	Определя персонализирания текст, който да се показва в подкана за въвеждане на ПИН код на Windows Hello for Business по време на записването на сертификат.

Управление на връзките

Wifi

При тази настройка се извършва предварителна конфигурация на крайните потребителски устройства за достъп до вътрешните точки за достъп.

Идентификатор на набора от услуги (SSID)	SSID на мрежата, към която ще бъде установена връзката
Автоматично присъединяване	Активиране на автоматично присъединяване към мрежата
Скрита мрежа	Активиране, в случай че AP не излъчва SSID

Вид сигурност

Установяване на типа сигурност на AP

Отворена система WEP	
Парола	Парола за AP

WPA PSK	
Парола	Парола за AP

WPA EAP	
Тип удостоверяване	Тип удостоверяване, възможно само с "PEAP-MSCAHPv2"
Бързо възстановяване на връзката	Устройствата могат да превключват между точките за достъп, без да се налага да се удостоверяват отново.
Достъп за гости	Потребителят няма акаунт и затова трябва да се регистрира като гост
Проверки за карантина	Клиентът трябва да извърши проверка на NAP (Network Access Protection) и да сподели резултатите със системата, която след това решава дали клиентът може да се свърже.
Изискване за криптографско свързване	Удостоверяването е възможно само чрез Crypto Binding
Утвърждаване на сървъра	Клиентът проверява дали сертификатът на сървъра е валиден. Ако случаят е такъв, ще бъде установена връзка.
Изискване за сертификати	Позволява на потребителя да приема ненадеждни сертификати
Имена на сървъри	Възможност за показване на името на RADIUS-сървъра, който предлага мрежовото удостоверяване и оторизиране.

WPA2-PSK	
Парола	Парола за AP

WPA2 EAP	
Тип удостоверяване	Тип удостоверяване, възможно само с "PEAP-MSCAHPv2"
Бързо възстановяване на връзката	
Достъп за гости	
Проверки за карантина	Активира защитата на достъпа до мрежата NAP
Изискване за криптографско свързване	Удостоверяването е възможно само чрез Crypto Binding
Утвърждаване на сървъра	
Изискване за сертификати	Запитва за валидиран сертификат на сървъра, име или удостоверяване на коренен сертификат (CA)
Имена на сървъри	Списък на сървърите, на които устройствата трябва да се доверяват
Няма	Няма установена сигурност
Използване на прокси сървър	Използване на прокси сървър
Адрес на сървъра	Адрес на прокси сървър
Порт на сървъра	Порт на сървъра на прокси сървъра

Използване на прокси сървър

Разрешаване на използването на прокси сървър.

Адрес на сървъра	Адрес на прокси сървър, използван от тази мрежа.
Порт на сървъра	Портът на прокси сървъра, използван от тази мрежа.

Ограничения за Wi-Fi

Тук можете да зададете различни ограничения за Wifi.

Разрешаване на WiFi	Разрешаване/забрана на Wi-Fi
Разрешаване на споделянето на интернет	Разрешаване на използването на гореща точка
Разрешаване на автоматичното свързване с горещи точки на WiFi Sense	Разрешаване на автоматичното свързване с горещи точки на WiFi Sense
Разрешаване на ръчно конфигуриране на WiFi	Разрешаване на потребителя да се свързва с WiFi мрежи, които не са дефинирани от AppTec
Честота на сканиране на WLAN	Установява интервала на сканиране на WLAN. Тук по-високата стойност повишава способността за разпознаване на WIFI мрежи.

VPN

Извършете подходящите настройки тук, за да конфигурирате VPN връзките.

Име на връзката	Посочено име на връзката		
Тип VPN	VPN връзката за всяко приложение се използва за защита на трафика на определени приложения.		
	VPN	Винаги включено	Това автоматично ще свърже VPN услугата при влизане и ще остане свързана, докато потребителят не прекъсне връзката ръчно.
	VPN за всяко приложение	VPN приложения	Определяне на приложенията, които използват тази VPN връзка
		Блокиране за всяко приложение	Забраната за всяко приложение прави така, че избраните приложения да имат връзка само чрез тази VPN връзка. Тази функция зависи от защитната стена на Windows Defender.
	Профил на WIP	WIP домейн за тази връзка	Идентификатор на предприятието, който се изисква за свързване на този VPN профил с политика за защита на информацията на Windows (WIP).

Вид на връзката

AppTec360 VPN	
За "AppTec360 VPN" е необходимо да е разрешено страничното зареждане на приложения. Моля, разрешете "Allow App Sideloading" в "Управление на сигурността" → "Restriction Settings" → "Device Functionality".	
Конфигурация на шлюза	За да конфигурирате VPN връзка с черен списък, изберете VPN конфигурация с определен DNS сървър. Можете да настроите VPN конфигурация в "Общи настройки" → "Универсален шлюз" → "VPN настройки".

IKEv2		
Сървъри	Списък с VPN сървъри	
Тунел за устройства	Разрешаване на връзката преди влизане на потребителя.	
Метод на удостоверяване	EAP	EAP XML
	Сертификати за машини	
Алгоритъм за криптиране		
Алгоритъм за проверка на интегритета		
Група на Дифи-Хелман		
Алгоритъм за трансформиране на шифъра		
Алгоритъм за преобразуване на удостоверяването		
Група с перфектна тайна на препращане (PFS)		

PPTP		
Сървъри	Списък с VPN сървъри	
Метод на удостоверяване	EAP	EAP XML

L2TP		
Сървъри	Списък с VPN сървъри	
Метод на удостоверяване	EAP	EAP XML
Алгоритъм за криптиране		
Алгоритъм за проверка на интегритета		
Група на Дифи-Хелман		
Алгоритъм за трансформиране на шифъра		
Алгоритъм за преобразуване на удостоверяването		
Група с перфектна тайна на препращане (PFS)		

Автоматичен		
Сървъри	Списък с VPN сървъри	
Метод на удостоверяване	EAP	EAP XML

Общи конфигурации на VPN

Запомняне на идентификационните данни при всяко влизане в системата	
Регистриране на IP адреси с вътрешния DNS	
Правила за филтриране на мрежовия трафик	Ограничаване на VPN връзката до определения набор от правила.
Списък за търсене на суфикси на DNS	DNS суфикси за добавяне към списъка за търсене на DNS за маршрутизиране на кратки имена.
Правила на таблицата за политика за разрешаване на имена (NRPT)	Правилата на таблицата за политика за преобразуване на имена (NRPT) определят как DNS преобразува имената при свързване към VPN.
Откриване на доверена мрежа	Списък с DNS суфикси за идентифициране на доверена мрежа.
Разделяне на тунели	Разделеното тунелиране означава, че трафикът може да преминава през всеки интерфейс, определен от мрежовия стек.
Разделяне на маршрути за тунелиране	Списък на маршрутите, които трябва да се добавят към таблицата за маршрутизация за VPN интерфейса.
Настройка на прокси сървъра	Конфигурира прокси сървъра, използван в тази мрежа
Адрес на пълномощното	Адрес на прокси сървър като пълно квалифицирано име на хост или IP адрес.
Пристанище	Портът на прокси сървъра.
URL адрес за автоматична конфигурация на прокси сървъра	URL адрес за автоматично извличане на настройките на прокси сървъра.

Ограничения за VPN

Тук можете да зададете различни ограничения за VPN.

Разрешаване на настройките на VPN	Тази насока позволява/забранява на потребителя да деактивира и променя настройките на VPN
Разрешаване на VPN през клетъчна мрежа	Разрешава/забранява на устройството да установи VPN връзка, ако устройството използва мобилни данни
Разрешаване на VPN роуминг през клетъчната мрежа	Разрешава/забранява на устройството да установи VPN връзка, ако устройството е в роуминг

Bluetooth

Тук можете да определите дали Bluetooth да бъде разрешен/забранен.

Разрешаване на Bluetooth	Активиране/деактивиране на Bluetooth

Управление на PIM

Exchange Active Sync

Настройка на акаунта ActiveSync в устройството на крайния потребител

Име на сметката	Име на имейл акаунт
Име на хоста на сървъра	Адрес на сървъра/FQDN
Име на домейна	Домейн на сървъра
Имейл адрес	Имейл адрес
Потребителско име	Потребителско име
Парола на потребителя	По желание тук вече можете да прикачите парола към потребителя.
Използване на SSL	Използване на SSL връзка
Интервал на синхронизация	Тук може да се определи интервалът на синхронизация. Ръчна синхронизация = Потребителят трябва да изтегли имейлите си и да извърши ръчна синхронизация.
Филтър за възрастта на пощата	Време, за което имейлите трябва да се синхронизират Без филтър = неограничен
Ниво на дневника	Установяване на нивата на регистриране на трафика на ActiveSync
Синхронизиране на имейл	Активирано = имейлите се синхронизират
Синхронизиране на контакти	Активирано = контактите са синхронизирани
Синхронизиране на календара	Активиран = календарът е синхронизиран
Синхронизиране на задачи	Активирано = задачите са синхронизирани

Електронна поща

Създаване на POP3/IMAP4 акаунти на крайното потребителско устройство.

Описание на сметката	Име на имейл акаунт
Име на подателя	Показано име на подателя
Име на домейна	Име на домейна за имейл акаунта
Имейл адрес	Имейл адрес на потребителя
Потребителско име	Потребителско име
Парола на потребителя	По желание тук вече можете да прикачите парола към потребителя.
Алтернативни идентификационни данни на изходящия сървър	Тук може да се зададе, ако за изходящия сървър се изискват други данни.
Име на изходящ домейн	Име на изходящ домейн
Потребителско име на изходящия сървър	Потребителско име на изходящия сървър
Парола на изходящия сървър	Парола на изходящия сървър
Протокол за електронна поща	POP3 или IMAP4, може да се използва като протокол
Име на хоста на входящия пощенски сървър	Име на хоста на сървъра за входяща поща
Използване на SSL за входящи писма	Използване на SSL за входящи имейли
Име на хоста на изходящия пощенски сървър	Име на хоста на сървъра за изходяща поща
Използване на SSL за изходящи писма	Използване на SSL за изходящи имейли
Удостоверяване на изходящия сървър	Изисква се удостоверяване на изходящия сървър
Интервал на синхронизация	Тук може да се определи интервалът на синхронизация. Ръчна синхронизация = Потребителят трябва да изтегли имейлите си и да извърши ръчна синхронизация.
Филтър за възрастта на пощата	Време, за което имейлите трябва да се синхронизират Без филтър = неограничен

Управление на приложения

Мениджър на корпоративни приложения

Инсталирани приложения

Тук е представен списък на приложенията, които са инсталирани в момента на показваното устройство.

Задължителни приложения

Тук можете да конфигурирате списък с приложения, които са задължителни за устройството.

Този списък ще бъде проверяван всеки път, когато устройството се свърже с MDM, и ще бъдат инсталирани всички приложения от този списък, които не са инсталирани на устройството, независимо дали приложението е било деинсталирано или никога не е било инсталирано преди това.

Можете да качите вътрешни приложения на Windows 10 и след това да ги добавите в този списък или да добавите конфигурации на Microsoft Office, които трябва да бъдат конфигурирани предварително в "Общи настройки" > "Управление на приложения" > "Microsoft Office".

Ограничения на системните приложения

Приложения за входяща поща
Разрешаване на аларми и часовник
Позволете калкулатор
Разрешаване на камерата
Разрешаване на поддръжката за контакт
Разрешаване на Cortana
Разрешаване на File Explorer
Позволете да започнете
Позволете Groove Music
Разрешаване на карти
Разрешаване на изпращането на съобщения
Разрешаване на Microsoft Edge
Позволете филми и телевизия
Позволете пари
Позволете новини
Разрешаване на OneDrive
Разрешаване на OneNote
Разрешаване на календара и пощата на Outlook
Позволете на хората
Разрешаване на телефона
Разрешаване на снимки
Позволете Powerpoint
Разрешаване на настройките
Разрешаване на Skype
Позволете спорт
Позволете магазин
Разрешаване на гласовия рекордер
Разрешаване на портфейла
Позволете времето

Разрешаване на хъба за обратна връзка на Windows
Разрешаване на Word
Разрешаване на Xbox

Задаване на страници
Разрешаване на акаунти на работното място
Разрешаване на разширена информация
Разрешаване на ъгъла с приложения
Позволете блокиране и филтриране
Разрешаване на цветовия профил
Разрешаване на режима на шофиране
Разрешаване на имейли и акаунти
Позволете Equalizer
Разрешаване на клавиатурата
Разрешаване на лентата за навигация
Разрешаване на самолетния режим на мрежата
Разрешаване на споделянето на интернет в мрежата
Разрешаване на мрежови услуги
Разрешаване на мрежата Wi-Fi
Разрешаване на Bluetooth в системата на компютъра
Позволете оценка на вашето устройство
Разрешаване на актуализация на възстановяването
Разрешаване на споделянето
Разрешаване на стартирането
Позволете време Език
Позволете време Регион
Разрешаване на заключване на екрана по подразбиране на Windows
Разрешаване на работа или училищна сметка

Черни и бели списъци

В "Black- & Whitelisting" (Черен и бял списък) можете да избирате между режим "Whitelist" (Бял списък) и режим "Blacklist" (Черен списък).

Бял списък	Само приложенията и услугите, които са добавени в списъка, могат да бъдат инсталирани на крайното потребителско устройство. Ако те вече са предварително инсталирани на устройството на крайния потребител, те ще бъдат активирани и настроени, така че потребителят да може да ги изпълнява.
	Всички останали приложения, които не са добавени в списъка, не могат да бъдат инсталирани на устройството на крайния потребител. Ако те вече са предварително инсталирани на устройството на крайния потребител, те ще бъдат деактивирани и настроени така, че потребителят да не може да ги стартира.
Черен списък	Приложенията и услугите, които са добавени в списъка, не могат да бъдат инсталирани на крайното потребителско устройство. Ако те вече са предварително инсталирани на устройството на крайния потребител, те ще бъдат деактивирани и настроени така, че потребителят да не може да ги стартира.
	Всички останали приложения, които не са добавени в списъка, могат да бъдат инсталирани на устройството на крайния потребител. Ако те вече са предварително инсталирани на устройството на крайния потребител, те ще бъдат активирани и настроени, така че потребителят да може да ги изпълнява.

Чрез бутона , добавяте допълнителни приложения или услуги към списъка на използваните в момента.

Чрез бутона , добавяте допълнителни приложения или услуги към неактивния в момента списък.

Можете да добавите приложение от "Windows App Store" или директно да въведете "Идентификатор на приложение", за да го добавите към черния или белия списък.

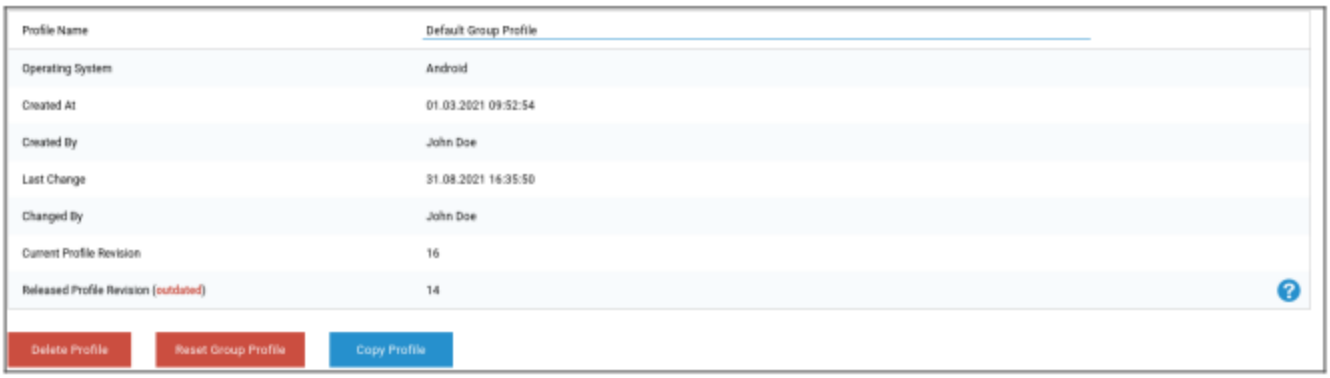
Конфигурация на MacOS

В зависимост от това дали сте избрали профил или устройство, дисплеят и неговите подточки са различни - моля, обърнете внимание на това!

Обща информация

Преглед на профила на групата (само на ниво група)

При отваряне на групов профил ще получите бърз преглед на профила.



Име на профила	Име на профила (може да бъде променено тук)
Операционна система	Операционна система, за която е предназначен профилът
Създаден в	Време на създаване
Създаден от	Създател на профила
Последна промяна	Време на последната промяна в профила
Променено от	Акаунт, в който са направени последните промени
Текуща ревизия на профила	Преразглеждане на запазеното състояние на профила
Освободена ревизия на профила	Присвоена ревизия на профила ("Присвои сега"). Ако зад текста на етикета се показва "(остарял)", това означава, че сте запазили профила, но все още не сте го присвоили, така че устройствата все още ще получават по-стара версия.

Преглед на устройството (само на ниво устройство)

Обобщен преглед на устройството.

Име на устройството	Име на устройството
Модел	Модел
Операционна система	Операционна система
Сериен номер	Сериен номер на устройството
Притежание на устройство	Конфигурираният тип собственост
Тип устройство	Типът на устройството
Съответстващ	Показва дали устройството е съвместимо
IP адрес	IP адресът, от който устройството е свързано със сървъра
Последно видян	Време на последната връзка от устройството
Последен тласък	Време на последното натискане, изпратено до устройството
Задание	Тук можете да преместите устройството към друг потребител или група

Ревизия на конфигурацията (само на ниво устройство)

Тук ще получите преглед на груповия профил, който е зададен на устройството.

Ако щракнете върху профила на групата, ще получите директен достъп до профила и ще можете да извършвате настройки.

Със символа можете да върнете зададените приложения към настройките на груповия профил.

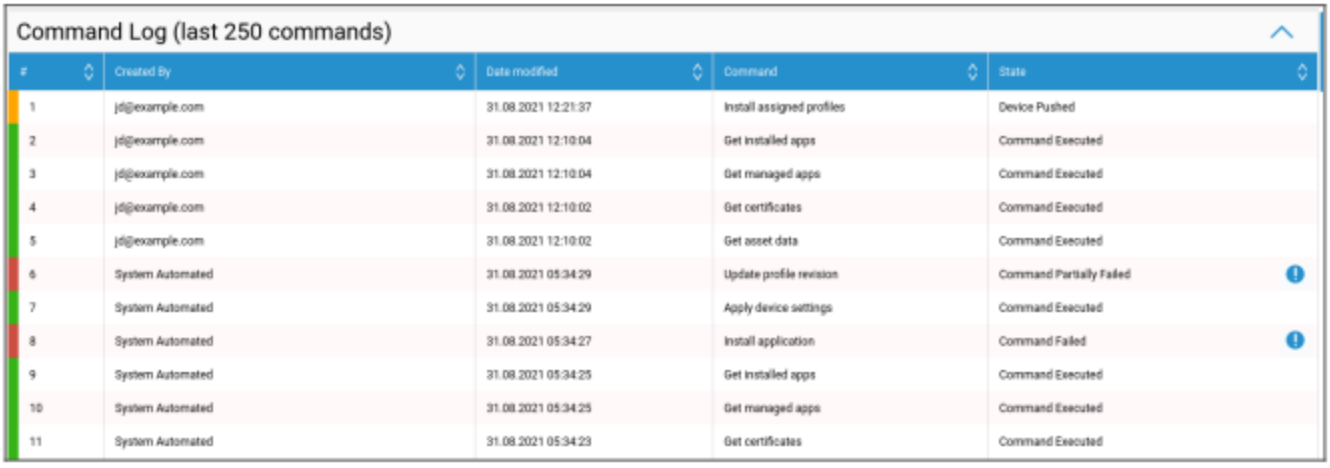
Със символа можете да нулирате профила на устройството, така че да няма никакви настройки.

"Налична е по-нова ревизия" показва, че профилът на групата е променен и запазен, но не е присвоен. Груповият профил трябва да бъде присвоен с "Assign now" (Присвояване сега) на ниво група, за да се приложат промените към устройствата.

Дневник на устройството (само на ниво устройство)

Дневник на командите

Тук можете да видите кои команди са издадени за устройството и какво е тяхното състояние.



Командите, създадени от "System Automated", се създават автоматично от системата.

Възможни състояния на командата

Натиснато устройство	Изпратена е заявка за натискане до услугата за натискане (напр. APNS), за да се каже на устройството да се свърже отново със сървъра на EMM.
Създадена команда	Командата е създадена в системата.
Изпратена команда	Командата е изпратена на устройството, след като то се е свързало със сървъра.
Изпълнена команда	Командата е изпълнена успешно.
Командата е неуспешна	Командата не е изпълнена. *
Командата е частично неуспешна	В зависимост от операционната система на устройството някои команди могат да бъдат групирани заедно. При това някои части от тази група команди не успяха. *
Командата е изпълнена, но в крайна сметка е неуспешна	Командата е изпълнена, но може би не е.
Пренасочване на командата	Командата е била изпратена отново от потребител.
Изхвърлени	Командата беше отхвърлена. Например защото е била заменена от друга команда или устройството е било презаписано и старите команди са били премахнати.

*Ако зад съобщението има възклицателен знак, можете да получите повече информация, като задържите курсора върху иконата.

Управление на активи (само на ниво устройство)

Информация за устройството

Номер на модела	Номер на модела
Име на хоста	Име на хоста
Местно име на хост	Местно име на хост
Операционна система	Операционна система
Версия на операционната система	Версия на операционната система
UDID	UDID
Свободна / обща памет	Свободна / обща памет

WiFi

IP адрес	IP адрес
WiFi MAC	WiFi MAC

Клетъчен

Телефонен номер	Телефонен номер
Състояние на роуминга	Състояние на роуминга
Роуминг (глас/данни)	Роуминг (глас/данни)
IP адрес	IP адрес
Оператор/превозвач	Оператор/превозвач
Мрежа на оператора на SIM	Преносна мрежа
Версия на носителя	Версия на носителя
ICCID	ICCID
Текущи MCC/MNC	Текущи MCC/MNC
SIM MCC/MNC	SIM MCC/MNC

Bluetooth

Bluetooth MAC	Bluetooth MAC

Управление на актуализациите (само на ниво устройство)

Актуализиране на информацията

Този раздел показва информация за настройките за актуализация на системата на устройството.

Разрешена е функцията Autocheck	Ако системата проверява за актуализация автоматично.
Разрешено е автоматично обновяване на приложенията	Ако системата ще инсталира актуализациите на приложенията автоматично.
Разрешени автоматични актуализации на операционната система	Ако системата ще инсталира актуализациите на Os автоматично.
Разрешени автоматични актуализации на сигурността	Ако системата ще инсталира актуализации на сигурността автоматично.
Актуализация на приложенията Изтегляне на заден план е разрешено	Ако системата ще изтегля актуализации на приложения във фонов режим.
URL адрес на каталога	URL адресът на каталога с актуализации на софтуера, който клиентът използва.
е каталог по подразбиране	Ако е "да", Каталогът е каталогът по подразбиране.
Извършване на периодична проверка	Ако отговорът е "да", започнете ново сканиране.
Дата на предишното сканиране	Датата на последното сканиране за актуализация на софтуера.
Резултат от предишно сканиране	Кодът на резултата от последното сканиране за актуализация на софтуера.

Управление на сигурността

Защита от кражби

Избърсване и заключване

Пълно избърсване	Изпращане на команда за нулиране на фабричните настройки на устройството
Изтриване на предприятието	Премахване на MDM от устройството и премахване на всички данни от MDM (напр. акаунти, приложения)
Екран за заключване	Накарайте устройството да се върне в заключения екран

Конфигурация на сигурността

Парола

Разрешено е деактивиране на кода	Определя дали потребителят е принуден да зададе ПИН код. Простото задаване на тази стойност (а не на други) принуждава потребителя да въведе код за достъп, без да се налага дължина или качество.
Позволете проста стойност	Позволете на потребителя да използва еднакви, ескалиращи и редуциращи се поредици от номера (например 1234, 1111)
Изискване за буквено-цифрова стойност	Паролите трябва да съдържат поне една буква.
Минимална дължина на кода за достъп	Минимална дължина на паролата
Минимален брой сложни символи	Минимален брой буквено-цифрови символи в паролата
Максимална възраст на кода за достъп	Брой дни, след които паролата трябва да бъде променена
Максимално автоматично заключване	Максимално време, след което устройството се заключва
Максимален гратисен период за заключване на устройството	Времето, за което устройството може да бъде заключено, без да се изисква въвеждане на парола при отключване
Максимална възраст на кода за достъп (1-730 дни или никаква)	Дни, след които кодът за достъп трябва да бъде променен
История на паролите (1-50 пароли или нито една)	Брой уникални пароли преди повторно използване

Сертификат

PKCS#1	
Описание	Въведете описание на сертификата
Удостоверение	Качване на файл pkcs1

PKCS#12	
Описание	Въведете описание на сертификата
Удостоверение	Качване на файл pkcs12

Настройки на ограниченията

Функционалност на устройството

Разрешаване на камерата	Разрешаване на използването на камерата
Разрешаване на Game Center	Когато е невярно, Game Center се деактивира и иконата му се премахва от Начален екран.
Разрешаване на мултиплейър игри	Когато е невярно, забранява игрите за няколко играчи.
Разрешаване на добавянето на приятели в Game Center	Когато е невярно, се забранява добавянето на приятели в Game Center.
Разрешаване на iCloud Photo Library	Ако е зададена стойност false, се деактивира iCloud Photo Library. Всички снимки, които не са изцяло изтеглени от iCloud Photo Library в устройството, ще бъдат премахнати от локалното хранилище.
Разрешаване на Touch ID	Ако е невярно, предотвратява отключването на устройството с Touch ID.

iCloud

Блокиране на определени функционалности по време на сдвояване с iCloud

Разрешаване на синхронизирането на документи	Разрешаване на синхронизирането на документи
Разрешаване на синхронизирането на iCloud Keychain	Разрешаване на синхронизирането на iCloud Keychain
Разрешаване на бележките в iCloud	Когато е невярно, се забраняват услугите на MacOS iCloud Notes
Разрешаване на iCloud BTMM	Когато е невярно, се забранява услугата iCloud в MacOS Back to My Mac.
Разрешаване на iCloud FMM	Когато е невярно, се забранява услугата iCloud на MacOS Find My Mac.
Разрешаване на отметките в iCloud	Когато е невярно, се забранява синхронизирането на MacOS iCloud Bookmark.
Разрешаване на iCloud Mail	Когато е невярно, се забраняват услугите iCloud на MacOS Mail.

Разрешаване на календара на iCloud	Когато е невярно, се забраняват услугите iCloud в MacOS Cloud.
Разрешаване на напомнянията в iCloud	Когато е невярно, забранява услугите на iCloud Reminder.
Разрешаване на iCloud Addressbook	Когато е невярно, забранява услугите на MacOS iCloud Address Book.

Управление на медиите

Изхвърляне при излизане от системата	Изхвърляне на всички сменяеми носители при излизане от системата
Разрешаване на мрежата	Разрешаване на достъпа за мрежови носители
Разрешаване на вътрешния диск	Разрешаване на достъпа до вътрешния диск.
Изискване на удостоверяване	Изискване за удостоверяване на автентичността при използване на тази медия
Само за четене	Потребителят може само да чете данни от носителя
Разрешаване на външен диск	Разрешаване на достъпа до външен диск.
Изискване на удостоверяване	Изискване за удостоверяване на автентичността при използване на тази медия
Само за четене	Потребителят може само да чете данни от носителя
Разрешаване на използването на дискови изображения	Разрешаване на достъпа за изображения.
Изискване на удостоверяване	Изискване за удостоверяване на автентичността при използване на тази медия
Само за четене	Потребителят може само да чете данни от носителя
Разрешаване на използването на DVD-RAM	Разрешаване на достъпа до DVD-RAM диска.
Изискване на удостоверяване	Изискване за удостоверяване на автентичността при използване на тази медия
Само за четене	Потребителят може само да чете данни от носителя
Разрешаване на използването на DVD дискове	Разрешаване на достъпа до DVD диска.
Изискване на удостоверяване	Изискване за удостоверяване на автентичността при използване на тази медия
Разрешаване на използването на компактдискове	Разрешаване на достъпа до CD диска.
Изискване на удостоверяване	Изискване за удостоверяване на автентичността при използване на тази медия

Управление на връзките

Wi-Fi

Тук можете да добавяте и конфигурирате Wi-Fi връзки

Идентификатор на набора от услуги (SSID)	SSID на мрежата, към която ще бъде установена връзката
Автоматично присъединяване	Разрешаване на автоматичното присъединяване към мрежата
Скрита мрежа	Разрешаване, в случай че AP не излъчва SSID
Настройка на прокси сървъра	Конфигуриране на прокси за всяка точка за достъп
Няма	Не използвайте прокси сървър
Ръководство	Създаване на ръчно прокси
URL адрес на прокси сървър	Адрес за достъп до настройките на прокси сървъра
Пристанище	Установяване на порта за прокси сървъра
Удостоверяване	Потребителско име за удостоверяване в прокси сървъра
Парола	Парола за удостоверяване в прокси сървъра
Автоматичен	Създаване на прокси автоматично
URL адрес на прокси сървър	URL адрес за файла с настройките на прокси сървъра
Вид сигурност	Установяване на тип сигурност за AP
WEP	
Парола	Парола за AP
WPA/WPA2	
Парола	Парола за AP
WEP Enterprise - WPA / WPA2 Enterprise / Всяко предприятие	Вижте таблица Грешка: Reference source not found below
Няма	Не установявайте сигурност
Деактивиране на случайното	Деактивира случайното разпределение на MAC адресите за тази Wi-Fi мрежа, докато е свързана с нея. Това също така показва

разпределение на MAC адресите	предупреждение за поверителност в Настройки, което показва, че мрежата е намалила защитата на поверителността.

Конфигуриране на Wi-Fi в предприятието

Забележка: Налично е само когато "Тип сигурност" е зададен на тип Enterprise.

Протоколи	Протокол за удостоверяване, поддържан в целевата мрежа
TLS	Активиране / деактивиране на употребата
TTLS	Активиране / деактивиране на употребата
Вътрешни удостоверявания	Протокол за удостоверяване, който трябва да се използва: PAP, CHAP, MSCHAP, MSCHAPv2
LEAP	Активиране / деактивиране на употребата
PEAP	Активиране / деактивиране на употребата
EAP-FAST	Активиране / деактивиране на употребата
EAP-SIM	Активиране / деактивиране на употребата
Използване на PAC	Използване на PAC (защитен контрол на достъпа)
Осигуряване на PAC	Конфигуриране на Provision PAC
Анонимно предоставяне на PAC	Анонимно предоставяне на PAC
Удостоверяване	
Потребителско име	Потребителско име за удостоверяване
Не използвайте На връзка Парола	Не използвайте парола за свързване
Парола	Паролата, която се използва
Сертификат за самоличност	Качване/избор на сертификат за удостоверяване
Външна идентичност	Идентичност, която може да се види отвън
Trust	
Доверен сертификат 1	Качване на първия доверен сертификат
Доверен сертификат 2	Качване на втори доверен сертификат
Доверен сертификат 3	Качване на трети доверен сертификат

Доверен сървър Имена на сертификати	Имената на очакваните сървърни сертификати (в списък, разделен със запетая)

VPN

В зависимост от избрания Тип на връзката може да се виждат различни полета.

Име на връзката	Име на VPN-профила
Тип VPN	
VPN	Целият мрежов трафик на устройството ще бъде пренасочен чрез VPN-връзка.
Тип на връзката	Установяване на тип VPN-връзка
IPsec (cisco)	Протокол IPsec от cisco
L2TP	Протокол L2TP
Потребителски SSL	Връзка чрез потребителски SSL
IKEv2	Протокол IKEv2
Настройка на прокси сървъра	Конфигуриране на прокси сървър за VPN-връзката
Няма	Установяване без пълномощно
Ръководство	Ръчно създаване на прокси
URL адрес на прокси сървър	Адрес за достъп до настройките на прокси сървъра
Пристанище	Установяване на порта за прокси сървъра
Удостоверяване	Потребителско име за удостоверяване в прокси сървъра
Парола	Парола за удостоверяване в прокси сървъра
Автоматичен	Създаване на прокси автоматично
URL адрес на прокси сървър	URL адрес за достъп до настройките на прокси сървъра

HTTP прокси

Тип прокси	
Ръководство	Създаване на прокси ръчно
URL адрес на прокси сървър	Адрес за достъп до настройките на прокси сървъра
Пристанище	Създаване на прокси порт
Удостоверяване	Потребителско име за удостоверяване в прокси сървъра
Парола	Парола за удостоверяване в прокси сървъра
Автоматичен	Създаване на прокси автоматично
URL адрес на прокси PAC	URL адрес на прокси PAC
Разрешаване на директна връзка, ако PAC е недостъпен	Разрешаване на директна връзка (без VPN), ако PAC е недостъпен
Позволява заобикаляне на прокси сървъра за достъп до затворени мрежи	Позволяване на заобикаляне на прокси сървъра за достъп до вътрешни мрежи

AirPrint

IP адрес	IP адрес на принтера
Път на ресурсите	Определен път до устройството AirPrint

AirPlay

Име на устройството	Име на устройството
Парола	Парола за сдвояване
Бял списък	Дефиниране на списък с устройства, с които устройството може да се свързва изключително

Управление на PIM

Exchange Active Sync

Име на сметката	Име на сметката.
Електронен адрес	Адресът на сметката (напр. max@company.com)
Име на хоста на сървъра	Вътрешно име на хост
Име за вход	"Домейн" и "Име за вход" трябва да са празни, за да може устройството да поиска потребител.
Домейн	"Домейн" и "Име за вход" трябва да са празни, за да може устройството да поиска потребител. Ако е активирана конфигурация на ACL шлюза и полето Domain не е празно, AppTec360 Universal Gateway ще удостовери устройството със следното име "Domain\Login Name".
Парола	Паролата за акаунта (напр. secretUserPassword)
Минали дни на Mail to Sync	Броят на пощата от последните дни за синхронизиране
Използване на SSL	Използване на SSL за вътрешния хост на Exchange
Разширена опция	Показване на разширени опции
Порт на сървъра	Вътрешен порт
Път на сървъра	Вътрешен път
Външно име на хост	Външен хост
Външен порт	Външен порт
Външен път	Външен път
Използване на SSL за външни Exchange Host	Използване на SSL за външен хост на Exchange

Електронна поща

Създаване на акаунти POP3 / IMAP на крайното потребителско устройство

Описание на сметката	Име des Имейл акаунти
Тип на сметката	
IMAP	
Префикс на пътя	Префиксът на пътя за специални папки
POP	
Потребителско име на дисплея	Потребителско име на дисплея
Имейл адрес	Имейл адрес на потребителя

Входяща поща	Настройки на входящия сървър
Адрес на пощенския сървър	Адрес на пощенския сървър
Порт на пощенския сървър	Порт на пощенския сървър
Потребителско име	Съответно потребителско име
Тип удостоверяване	Тип удостоверяване
Няма	Не Тип удостоверяване
Парола (само на ниво устройство)	Запитване за парола
MDM предизвикателство-отговор	
NTLM	Удостоверяване на NTLM
HTTP MD5 Digest	
Използване на SSL	Използвайте SSL, ако е необходимо

Изходяща поща	Настройки на изходящия сървър
Адрес на пощенския сървър	Адрес на пощенския сървър
Порт на пощенския сървър	Порт на пощенския сървър
Потребителско име	Съответно потребителско име
Тип удостоверяване	
Няма	Няма метод за удостоверяване
Парола (само на ниво устройство)	Запитване за парола
MDM предизвикателство-отговор	
NTLM	Удостоверяване на NTLM
HTTP MD5 Digest	
Използване на SSL	Използвайте SSL, ако е необходимо
Изходящата парола е същата като входящата	Изходящата парола е същата като входящата
Използвайте само в пощата	Активирайте, ако всички изходящи имейли трябва да се изпращат чрез приложението Mail-App.

CalDav

Конфигуриране на настройката и разпространението на акаунт в CalDav

Описание на сметката	Име на профила
Име на хоста	Име на хост и/или IP адрес
Пристанище	Пристанище на акаунта в CalDav
Основен URL адрес	Основен URL адрес на сметката
Потребителско име	Съответно потребителско име на CalDav
Парола (само на ниво устройство)	Съответна парола за CalDav
Използване на SSL	Използвайте SSL, ако е необходимо

CardDav

Конфигуриране на създаването и разпространението на акаунт в CardDav

Описание на сметката	Име на профила
Име на хоста	Име на хост и/или IP адрес
Пристанище	Пристанище на акаунта CardDav
Основен URL адрес	Основен URL адрес на сметката
Потребителско име	Съответно потребителско име на CardDav
Парола (само на ниво устройство)	Съответна парола за CardDav
Използване на SSL	Използвайте SSL, ако е необходимо

LDAP

В тази област настройте LDAP-връзка, за да позволите динамичен обмен на сертификати между крайното потребителско устройство и Active Directory.

Моля, обърнете внимание, че избраният потребител изисква съответното разрешение за четене.

Описание на сметката	Описание на сметката
Потребителско име на акаунта	Потребител за LDAP-достъп
Парола на акаунта	Парола за LDAP-достъп
Име на хоста на акаунта	Име на хоста/IP адрес на сървъра LDAP
Използване на SSL	Използвайте SSL, ако е необходимо

Във втората част можете да дефинирате индивидуални филтри за търсене в регистъра LDAP.

Описание	Обхват	База за търсене
Описание на филтъра	Ниво на търсене в регистъра LDAP	Определяне на индивидуалния филтър

Информационно табло и отчитане

Настройки на таблото за управление

Тук можете да видите кои информационни табла съществуват, да ги редактирате или да създадете нови. Всяко табло за управление има собствен набор от данни за показване и конфигурация на графиката.

Контрол на настройките на таблото за управление

Публичен	Задава публичност на таблото за управление, така че други потребители да могат да го виждат. Потребителите, разбира се, трябва да могат да влизат в системата и да преглеждат таблата за управление. Ако "Публично" не е активирано, само създателят може да го види.
По подразбиране	Задава таблото за управление като подразбиране, така че то да се отваря автоматично при следващия достъп до изгледа на таблото за управление.
	Показване на информационното табло и неговите графики
	Изтриване на таблото за управление
	Редактиране на името и настройките на таблото за управление
	Направете копие на информационното табло
	Добавяне на изцяло ново табло за управление

Изглед на таблото за управление

Това показва данните и графиките на избраното табло за управление и ви позволява да ги промените.

Контрол на таблото за управление

	Позволява ви да определите кои данни да се показват в таблото за управление, количеството данни, които да се показват, и размера, в който да се показват тези данни.
	Връща ви обратно в Преглед на таблото за управление
	Възстановяване на текущо отвореното табло за управление до настройките по подразбиране
	Запазва всички промени, които сте направили в текущо отвореното табло (например кои данни да се показват).
	Промяна на типа на диаграмата към стълбова диаграма
	Промяна на типа на диаграмата към кръгова диаграма
	Промяна на типа на диаграмата към диаграма на поничка
	Промяна на типа на диаграмата към диаграма на полярна област
	Промяна на реда на сортиране

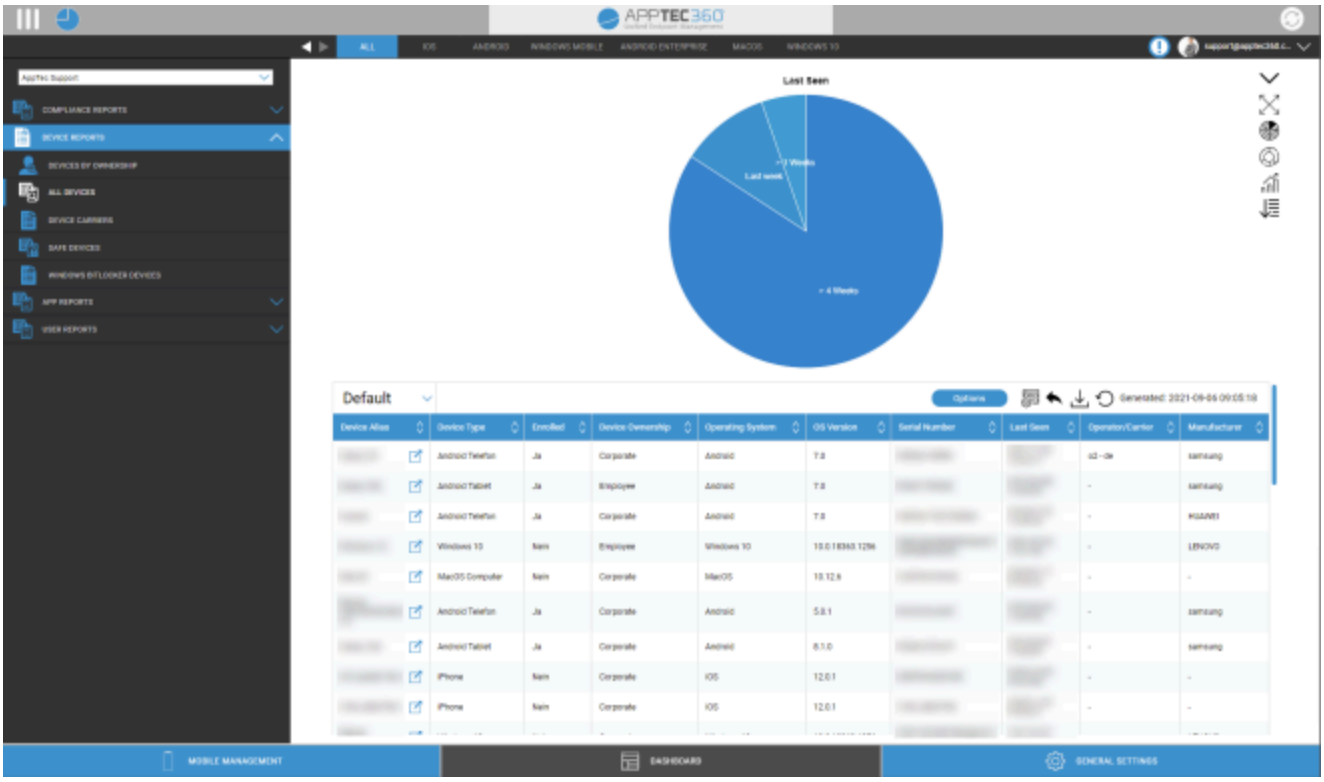
Разширено отчитане

"Разширено отчитане" предлага подробни прегледи и графики за информация за устройствата и потребителите.

Има няколко отчета по подразбиране, но всички те могат да се променят ръчно, за да се добавят или премахнат данни, които да се показват.

Моля, имайте предвид, че можете само ръчно да променяте кои данни се показват. Избраната категория на отчета определя данните, на които той се основава. Например никога няма да можете да видите устройства с Android в отчета за iOS в Отчети за устройства Всички устройства iOS

В горния ляв ъгъл можете да ограничите данните от отчетите до определена група (и всички нейни подгрупи). По подразбиране това е зададено за вашия основен възел, така че се вземат предвид ВСИЧКИ устройства и потребители.



Разширен контрол на отчитането

Във всеки преглед можете да използвате следните функции, за да промените отчета по желания от вас начин:

	Скриване на диаграмата (Ако диаграмата е показана)
	Показване на диаграма (Ако диаграмата е скрита)
	Разширяване на диаграмата (Ако диаграмата е сгъната)
	Свиване на диаграма (Ако диаграмата е разширена)
	Промяна на типа на диаграмата към стълбова диаграма
	Промяна на типа на диаграмата към кръгова диаграма
	Промяна на типа на диаграмата към диаграма на поничка
	Промяна на типа на диаграмата към диаграма на полярна област
	Промяна на реда на сортиране
	Променете следните части на показания преглед: • Добавяне/премахване на колони • Определяне на реда, в който се показват колоните • Показване/скриване на диаграмата над таблицата • Изберете колоната, която се използва за диаграмата • Филтриране на данните в таблицата
	Отворете мениджъра на настройките, за да запазвате и зареждате различни отчети
	Възстановяване на текущо отворения отчет по подразбиране
	Експортиране на текущия отчет като .csv файл
	Регенериране на данни и презареждане на текущия отчет

Списък на всички отчети по подразбиране можете да намерите на следващите страници.

Доклади за съответствие

Вкоренени устройства

Преглед на устройствата, които са били рутирани/ джейлбрейкнати.

Колони по подразбиране на този отчет:

Псевдоним на устройство
Собственик на устройството
Електронна поща
Операционна система
Телефонен номер
Последно видян
Производител

Устройства в роуминг

Преглед на всички устройства, които са в роуминг

Колони по подразбиране на този отчет:

Псевдоним на устройство
Собственик на устройството
Електронна поща
Тип устройство
Операционна система
Телефонен номер
Последно видян

Устройства с разрешен роуминг

Преглед на всички устройства, които са активирали роуминг, но не е задължително да са в роуминг в момента.

Колони по подразбиране на този отчет:

Псевдоним на устройство
Собственик на устройството
Електронна поща
Тип устройство
Операционна система
Телефонен номер
Последно видян

Контролирани устройства

Преглед на всички устройства, които са под наблюдение в режим на наблюдение (само за iOS)

Колони по подразбиране на този отчет:

Псевдоним на устройство
Собственик на устройството
Електронна поща
Тип устройство
Последно видян

Неактивни устройства

Преглед на всички устройства, които не са се свързвали със сървъра през последните 7 дни

Колони по подразбиране на този отчет:

Псевдоним на устройство
Собственик на устройството
Електронна поща
Тип устройство
Операционна система
Последно видян

Доклади за устройства

Устройства по собственост

Тук можете да видите колко устройства са внедрени в момента като корпоративни (корпоративни устройства) и като устройства на служителите (частни устройства).

Колони по подразбиране на този отчет:

Псевдоним на устройство
Собственик на устройството
Тип устройство
Притежание на устройство
Операционна система

Всички устройства

Тук можете да видите преглед на всички устройства с най-важната информация.

Колони по подразбиране на този отчет:

Псевдоним на устройство
Тип устройство
Записани на
Притежание на устройство
Операционна система
Версия на операционната система
Сериен номер
Последно видян
Оператор/превозвач
Производител

Носители на устройства

Тук можете да видите преглед на оператора (мобилния оператор).

Колони по подразбиране на този отчет:

Псевдоним на устройство
Собственик на устройството
Електронна поща
Операционна система
Версия на операционната система
Оператор/превозвач

Устройства SAFE

Тук можете да видите преглед на устройствата, които използват версията SAFE.

Тъй като прегледът и/или SAFE са достъпни само за устройствата на Samsung, няма да видите обичайните раздели в тази точка.

Колони по подразбиране на този отчет:

Псевдоним на устройство
Собственик на устройството
Електронна поща
Тип устройство
Последно видян
Версия SAFE

Устройства с Windows BitLocker

Тук можете да видите преглед на устройствата с Windows, които използват BitLocker.

Колони по подразбиране на този отчет:

Псевдоним на устройство
Собственик на устройството
Електронна поща

Състояние на BitLocker

Доклади за приложения

Тук можете да получите различни прегледи на приложенията. Във всички тези отчети можете да щракнете върху даден запис, за да видите допълнително кои версии са инсталирани на устройствата и колко често. В този изглед можете отново да щракнете върху определена версия, за да видите на кои устройства е инсталирана тази конкретна версия.

Забележка: Може да отнеме известно време, докато системата получи актуална информация от устройството. Освен това докладите не се актуализират всяка минута. Може да се наложи да проявите търпение, за да видите текущото състояние, ако току-що сте назначили ново приложение или версия. Ръчното презареждане на отчета ще го накара да покаже най-актуалните налични данни.

Инсталирани приложения

Тук ще получите преглед на всички инсталирани приложения.

Колони по подразбиране на този отчет:

Име	Име на съответното приложение и/или услуга
Идентификатор	Определен идентификатор на приложение/услуга
Общ брой	Колко често това приложение/услуга е било инсталирано на устройствата на крайния потребител

Най-инсталирани приложения

Тук можете да видите най-инсталираните приложения.

Колони по подразбиране на този отчет:

Име	Име на съответното приложение и/или услуга
Идентификатор	Определен идентификатор на приложение/услуга
Общ брой	Колко често това приложение/услуга е било инсталирано на устройствата на крайния потребител

Задължителни приложения

Тук ще получите преглед на задължителните (задължителни) приложения.

Колони по подразбиране на този отчет:

Име	Име на съответното приложение и/или услуга
Идентификатор	Определен идентификатор на приложение/услуга
Източник на приложения	Кой AppStore участва: • Google PlayStore (Android) • iTunes AppStore (iOS)
OS	Операционна система

Приложения в черния списък

Тук ще получите преглед на всички дефинирани приложения в черния списък.

Колони по подразбиране на този отчет:

Име	Име на съответното приложение и/или услуга
Идентификатор	Определен идентификатор на приложение/услуга
Източник на приложения	Кой AppStore участва: • Google PlayStore (Android) • iTunes AppStore (iOS)
OS	Операционна система

Доклади на потребителите

Тарифа

Тук можете да получите преглед на телефонните тарифи и SIM картите на потребителите.

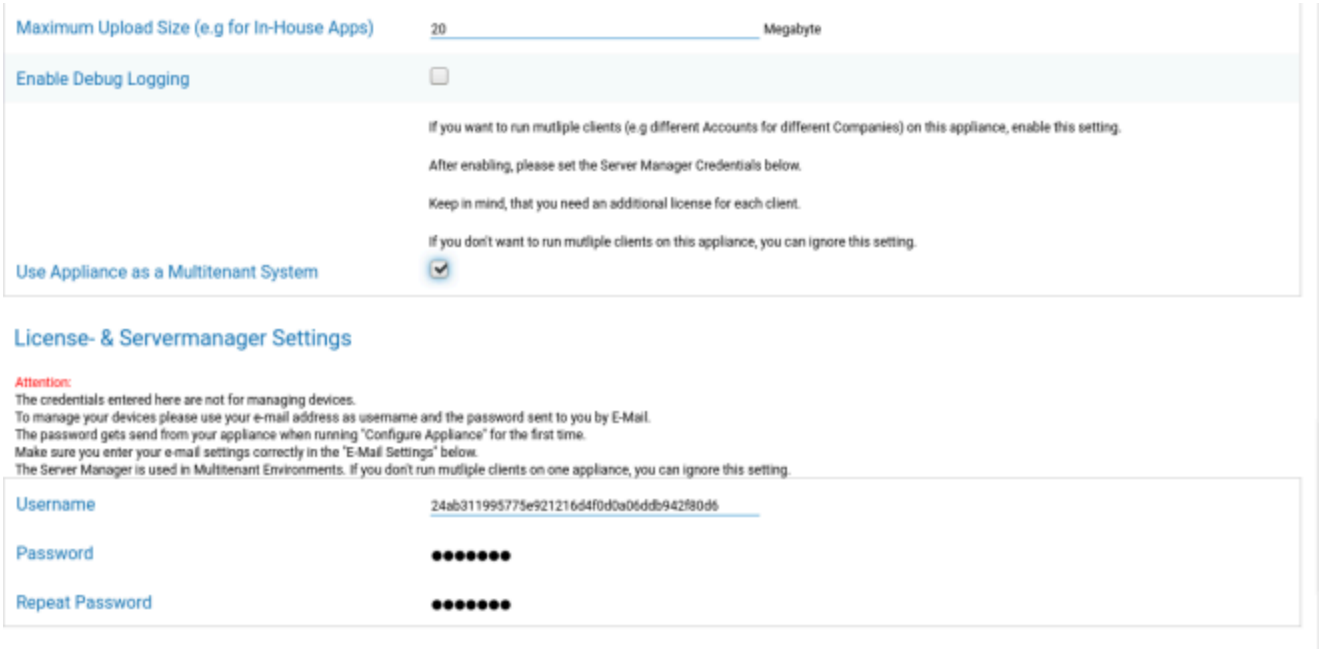
Колони по подразбиране на този отчет:

Електронна поща
Име
phoneNumber
превозвач
тарифа
опция
цена
contractCancelled
contractStart
duringTime
mobileAndData
dataVolume
multiSIM
тип
simCardSerial1
simCardSerial2
simCardSerial3
pin1
щифт2
puk1
puk2
бележка

Управление на множество наематели

AppTec360 EMM може да хоства множество отделни наематели, всеки от които има свои собствени потребители и групи, разрешения и глобални настройки.

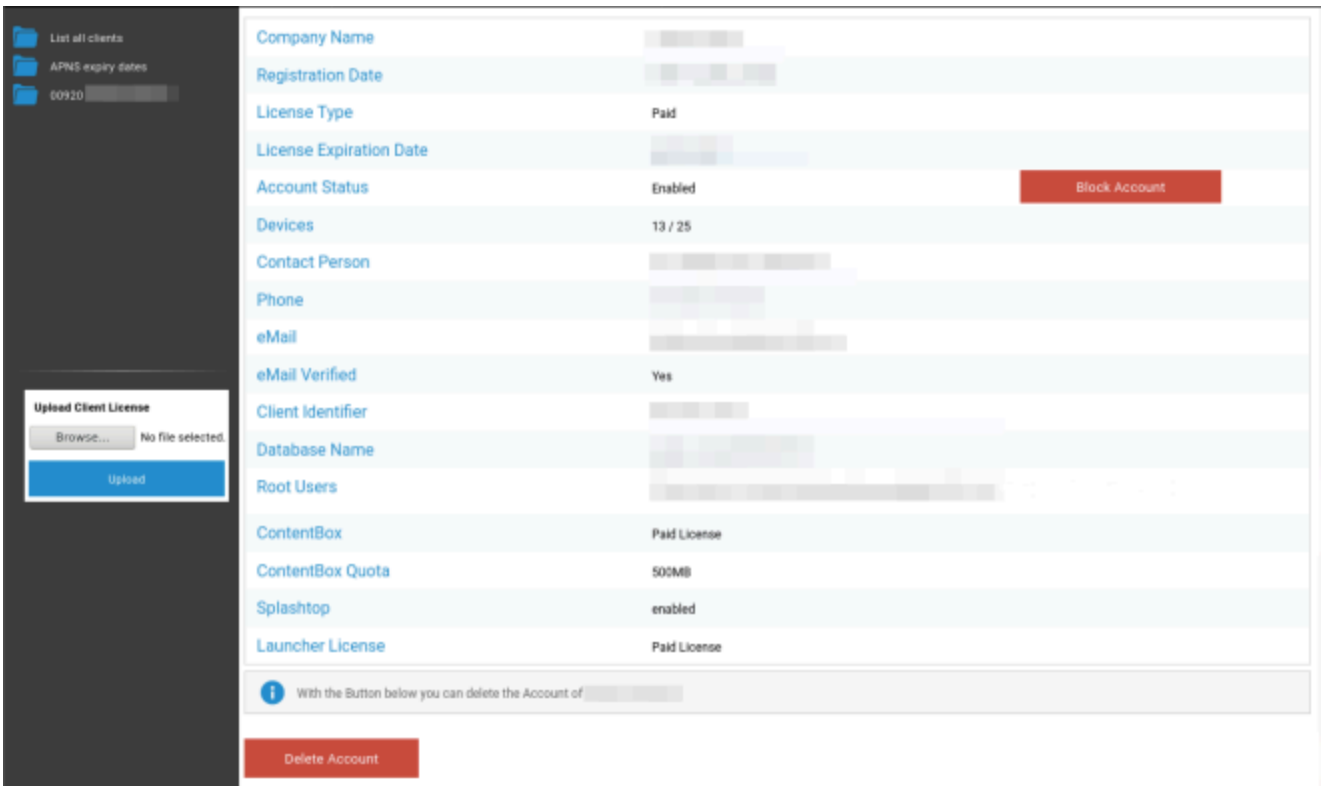
За да активирате функцията Multitenant, трябва да я включите в интерфейса за конфигуриране на устройството в "Трета стъпка - Настройки на сървъра".



В новото меню задайте потребителско име и парола за Servermanager. Запазете настройките и стартирайте "Configure Appliance" (Конфигуриране на устройството) в "Стъпка пет - Лицензионно споразумение", за да приложите настройките.

Когато конфигурацията е завършена, вече можете да влезете със зададените идентификационни данни през нормалния интерфейс за управление на мобилни устройства.

След влизане в системата можете да видите следния изглед.



Вляво можете да видите всички наематели (в този случай само един с идентификатор 920), а вдясно - информацията за този клиент. Имате също така възможност да блокирате достъпа до акаунта, както и да изтриете клиента (ВНИМАНИЕ: Това ще премахне всички данни, свързани с този клиент).

Вляво можете да качите нов клиентски лиценз, който може да бъде актуализация на лиценз за съществуващ клиент или нов лиценз, който автоматично създава нов клиент. При създаването на нов клиент автоматично се изпраща имейл, съдържащ паролата за вход, на имейл адреса, за който е издаден лицензът.

За да получите нов или актуализиран клиентски лиценз (напр. при нужда от повече лицензи за устройства), се свържете с вашия търговски представител.

Допълнителни изгледи

Списък на всички клиенти

Показва преглед на всички клиенти в системата.

Идентификатор на клиента	Идентификатор на клиента
Идентификатор	Идентификатор на клиента
База данни	База данни
Име на компанията	Име на компанията
Електронна поща	Лице за контакт Електронна поща
Проверено	Дали електронната поща на лицето за контакт е проверена или не
Държава	Държава
Устройства	Брой регистрирани устройства
Дата на регистрация	Момент на възлагане на лицензa
Последно влизане	Последно влизане в акаунта на администратора
Лиценз	Показване на типа лиценз (безплатен|платен)
CB лиценз	Тип на лиценза на ContentBox (безплатен|платен)
Статус	Текущо състояние на AppTec-Client
Изтекъл срок на валидност	Показва, ако лицензът е изтекъл
iOS	Брой устройства с iOS
Android	Брой устройства с Android
Windows Mobile	Брой устройства с Windows Mobile
MacOS	Брой устройства с MacOS
Windows 10	Брой устройства с Windows 10
Android Enterprise	Брой на устройствата с Android в предприятията
IOS BYOD (записване на потребители)	Брой устройства IOS BYOD (записване на потребители)
IoT	Брой на IoT устройствата

Дати на изтичане на валидността на APNS

Показва преглед на всички дати на изтичане на валидността на сертификатите APNS на всички клиенти.

Идентификатор на клиента	Идентификатор на клиента
Име на компанията	Име на компанията
Дата на изтичане	Дата на изтичане на валидността на сертификата Apple APNS
Информация	Информация за изтичането на срока на валидност

Свържете се с

Допълнителни въпроси? Свържете се с нас под следния адрес:

За общи технически въпроси

support@apptec360.com

+41 61 511 3210

За въпроси, свързани с инсталирането на виртуален уред

consulting@apptec360.com

+41 61 511 3214

Отказ от отговорност