AppTec360 Enterprise Mobile Manager i ContentBox

Podręcznik administratora | Wersja 5.0 (202110)

Spis treści

- Przegląd ogólny
  - Wprowadzenie do AppTec360
  - Obsługiwane systemy operacyjne urządzeń
  - Obsługiwane katalogi LDAP
  - Wyjaśnienie „trybu nadzorowanego” na urządzeniach Apple
    - Dostępne w trybie nadzorowanym
    - Aktywacja trybu nadzorowanego
    - Dodawanie urządzenia do DEP
  - Wyjaśnienie Android Enterprise
    - Czym jest Android Enterprise?
    - Jakie są wymagania do korzystania z Android Enterprise?
    - Jakie są dostępne tryby w Android Enterprise?
    - Jak mogę przypisać aplikacje do urządzeń Android Enterprise?
  - Przesyłanie własnych aplikacji do sklepu Google Play
- Wymagania i instalacja
  - Wymagania
    - Wymagania systemowe
    - Klucz licencyjny
    - Rozpoznawanie adresów IP i DNS
    - Certyfikat SSL
    - Serwer SMTP
    - Reguły zapory sieciowej
  - Aktualizacje zabezpieczeń
    - Domyślne hasła urządzenia wirtualnego
  - Konfiguracja urządzenia wirtualnego
    - Przygotowanie
      - Konfiguracja z zewnętrznego hosta
    - Krok pierwszy – Licencja na urządzenie
    - Krok drugi – Certyfikat SSL
      - Automatyczny

- Niestandardowe
- Krok trzeci – Ustawienia serwera
- Krok czwarty – Konfiguracja MySQL
- Krok piąty – Umowa licencyjna
- Rozwiązywanie problemów
- Zalecenia dotyczące bezpieczeństwa

Ustawienia ogólne

Przegląd konta

- Informacje o koncie
  - Przegląd
  - Raport o błędzie
  - Żądanie funkcji

Konfiguracja globalna

- Ustawienia eMail
- Szablony wiadomości eMail
- Rejestracja SMS

Prywatność

- Dostęp GPS

Dostęp oparty na rolach

- Zarządzanie rolami
- Przypisanie ról
  - Przypisanie roli
- Dostęp API
  - Dostęp do AppTec360 REST API
  - Zasady ogólne
  - Przykład żądania
  - Zapytania
  - Przykładowy kod w Python3

Konfiguracja Apple

- Certyfikat APNS
  - Krok 1
  - Krok 2
  - Krok 3
- Dostęp zarządzany

- Rejestracja użytkownika
- Współdzielony iPad
- DEP
- Konfigurator i adres URL
  - Adresy URL rejestracji puli
  - Profil MDM – konfigurator Apple

Konfiguracja systemu Android

- Konfiguracja systemu Android
- Automatyczna rejestracja
- Android Enterprise
  - Pierwsza metoda: Konto Android Enterprise (konto Google)
  - Druga metoda: Konto G-Suite
  - Ochrona przed przywróceniem ustawień fabrycznych
- AE Rejestracja
  - Metoda 1: Rejestracja za pomocą kodu QR
  - Metoda 2: Rejestracja NFC
  - Metoda 3: Konto Google
- Zapisy KNOX
- Zero-Touch

Konfiguracja systemu Windows

- Konfiguracja systemu Windows

ContentBox

- Konfiguracja

Konfiguracja LDAP

- Przegląd protokołu LDAP

Zarządzanie aplikacjami

- Wewnętrzny DB aplikacji
  - Android
  - iOS
  - macOS
  - Windows 10
- Ustawienia aplikacji
  - Ustawienia aplikacji iOS
  - Ustawienia aplikacji na Androida

- Aplikacje innych firm
  - Android
  - iOS
- VPP / KNOX Premium
  - Licencje VPP
  - Token VPP
  - Klucz KNOX Premium
- Ustawienia App Store
  - Region i język
- Sklep AE Play
  - Zatwierdzone aplikacje
  - Aplikacje ze Sklepu Play
  - Aplikacje prywatne
  - Aplikacje internetowe
  - Układ sklepu
- Zestaw aplikacji

Pilot zdalnego sterowania

- TeamViewer
  - TeamViewer Connector
  - Zainstaluj TeamViewer QuickSupport
  - Zdalne sterowanie urządzeniem
  - Dostęp nienadzorowany
- Splashtop

Zarządzanie kartami SIM

- Import zbiorczy CSV
- Przewoźnik i taryfa

Zarządzanie subskrypcjami

- Zarządzanie subskrypcjami

Ogólny dziennik kontroli

- Dziennik kontroli
- Ustawienia dziennika inspekcji

Zarządzanie certyfikatami

Zarządzanie urządzeniami mobilnymi

Ekran zarządzania urządzeniami mobilnymi

- Filtr urządzenia
- Okno wyszukiwania
- Opcje sprzętu
- Strzałki nawigacyjne

Ustawienia konta administracyjnego

- Informacje o użytkowniku
- Ustawienia konsoli
- Dziennik logowania

Administracja korporacyjna (węzeł główny) w zarządzaniu urządzeniami mobilnymi

- Tworzenie podgrupy
- Zmiana nazwy węzła głównego
- Masowa rejestracja
- Przydział masowy
- Szybka administracja aplikacjami
- Import użytkownika CSV

Zarządzanie grupami w zarządzaniu urządzeniami mobilnymi

- Tworzenie podgrupy
- Edytuj wybraną grupę
- Usuń wybraną grupę
- Utwórz użytkownika
  - Utwórz nowego użytkownika admin

Zarządzanie użytkownikami w zarządzaniu urządzeniami mobilnymi

- Dodawanie i rejestrowanie urządzenia

Zarządzanie profilami w zarządzaniu urządzeniami mobilnymi

- Utwórz profil
- Edytuj profil
- Kopiuj profil
- Usuń profil
- Dziedziczenie profili

Zarządzanie urządzeniami w zarządzaniu urządzeniami mobilnymi

- IOS
  - Edytuj urządzenie

- Wyczyść kod dostępu
- Urządzenie blokujące
- Urządzenie wyłączające
- Restart urządzenia
- Alarm i tryb utracony | Wyłącz tryb utracony
- Usuń urządzenie
- Czyszczenie urządzenia
- Enterprise Wipe | Usuń MDM
- Wyślij wiadomość
- Zdalne sterowanie TeamViewer
- Wyślij prośbę o rejestrację

Android

- Edytuj urządzenie
- Wyczyść kod dostępu
- Urządzenie blokujące
- Usuń urządzenie
- Czyszczenie urządzenia
- Usuń MDM
- Wyślij wiadomość
- Przekształcenie w tryb COPE
- Wyślij prośbę o rejestrację
- Migracja starszego urządzenia

Windows

- Edytuj urządzenie
- Usuń urządzenie
- Enterprise Wipe | Usuń MDM
- Zdalne sterowanie TeamViewer
- Wyślij prośbę o rejestrację

Zarządzanie treścią

- Pliki grupowe
- Eksplorator plików
- Ścieżka audytu
- Śmieci
- Pamięć zewnętrzna

Dziennik kontroli

Konfiguracja iOS

Ogólne

- Przegląd profilu grupy (tylko na poziomie grupy)
- Informacje ogólne
- Ustawienia
- Wersja konfiguracji
- Dziennik urządzenia (tylko na poziomie urządzenia)
  - Dziennik poleceń
  - Możliwe statusy poleceń

Zarządzanie zasobami (tylko na poziomie urządzenia)

- Zarządzanie zasobami (tylko na poziomie urządzenia)
  - Informacje o urządzeniu
  - Wi-Fi
  - Komórkowy
  - Bluetooth

Zarządzanie bezpieczeństwem

- Ochrona przed kradzieżą (tylko na poziomie urządzenia)
  - Informacje GPS (tylko na poziomie urządzenia)
  - Wipe & Lock (tylko na poziomie urządzenia)
  - Wiadomość (tylko na poziomie urządzenia)
- Konfiguracja zabezpieczeń
  - Kod dostępu
  - Certyfikat (tylko na poziomie urządzenia)
  - Szyfrowanie
  - Pojedyncze logowanie
- Koniec życia (tylko na poziomie urządzenia)
  - Wipe (tylko na poziomie urządzenia)
- Ustawienia ograniczeń
  - Funkcjonalność urządzenia
  - iCloud
  - Bezpieczeństwo i prywatność

BYOD

- Wbudowane zabezpieczenia iOS (kontener)
  - Aktywacja

- Hasło SecurePIM
- Bezpieczeństwo SecurePIM
- Przeglądarka SecurePIM
- Wymiana

Zarządzanie połączeniami

- Wi-Fi
  - Konfiguracja proxy
  - Typ zabezpieczenia
- VPN
  - Typ VPN
    - VPN
    - VPN dla poszczególnych aplikacji
  - Konfiguracja proxy
- APN
- Komórkowy
- Serwer proxy HTTP
- AirPrint
- AirPlay

Zarządzanie PIM

- Exchange Active Sync
- eMail
  - Poczta przychodząca
  - Poczta wychodząca
- CalDav
- Subskrybowane kalendarze
- LDAP

Zarządzanie siecią

- Klipy internetowe
- Filtr treści internetowych

Zarządzanie aplikacjami

- Menedżer aplikacji dla przedsiębiorstw
  - Zainstalowane aplikacje (tylko na poziomie urządzenia)
  - Aplikacje obowiązkowe
    - Opcje instalacji

- Aplikacje internetowe
- Ograniczenia i ustawienia
  - Aplikacje na czarnej / białej liście
  - Ograniczenia aplikacji SysApp
  - App-VPN
  - Ustawienia aplikacji
- Sklep z aplikacjami dla przedsiębiorstw
  - Aplikacje iTunes
  - Wewnątrz firmy
- Tryb kiosku
  - Typ aplikacji
    - Pakiet
    - URL
  - Ustawienia trybu kiosku

Android Enterprise – w pełni zarządzana konfiguracja urządzeń

Ogólne

- Przegląd profilu grupy (tylko na poziomie grupy)
- Przegląd urządzeń (tylko na poziomie urządzenia)
- Wersja konfiguracji (tylko na poziomie urządzenia)
- Dziennik urządzenia (tylko na poziomie urządzenia)
  - Dziennik poleceń
  - Możliwe statusy poleceń
- Ustawienia urządzenia
  - Konfiguracja klienta
  - Tapeta

Zarządzanie zasobami (tylko na poziomie urządzenia)

- Informacje o urządzeniu
  - Wi-Fi
- Komórkowy
- Bluetooth

Zarządzanie bezpieczeństwem

- Ochrona przed kradzieżą (tylko na poziomie urządzenia)
  - Informacje GPS (tylko na poziomie urządzenia)
  - Wipe & Lock (tylko na poziomie urządzenia)

- Wiadomość (tylko na poziomie urządzenia)
- Konfiguracja zabezpieczeń
  - Kod dostępu urządzenia
  - Antywirus
- Koniec życia (tylko na poziomie urządzenia)
  - Wipe (tylko na poziomie urządzenia)
- Ustawienia ograniczeń
  - Ograniczenia
- Zarządzanie certyfikatami

Zarządzanie połączeniami

- Wifi
  - Typ zabezpieczenia
    - WEP
    - WPA/WPA2
    - 802.1x EAP
- VPN
  - Typ VPN
    - VPN
    - VPN dla poszczególnych aplikacji
- Ograniczenia

Zarządzanie PIM

- Gmail Exchange

Zarządzanie aplikacjami

- Menedżer aplikacji dla przedsiębiorstw
  - Zainstalowane aplikacje (tylko na poziomie urządzenia)
  - Aplikacje systemowe (tylko na poziomie urządzenia)
  - Aplikacje obowiązkowe
  - Czarna i biała lista
  - Aplikacje systemowe AE
- Ograniczenia i ustawienia
  - Ustawienia zarządzania aplikacjami
- Sklep z aplikacjami dla przedsiębiorstw
  - Wewnątrz firmy
- Sklep Play dla przedsiębiorstw
  - Sklep AE Play

- Tryb kiosku i program uruchamiający
  - Tryb kiosku
  - AppTec360 Launcher
  - Ustawienia AppTec360
- Pilot zdalnego sterowania
  - Splashtop
  - TeamViewer
- Zarządzanie treścią
  - ContentBox
  - Bezpieczna przeglądarka
- Dodatkowy interfejs API
  - Samsung KNOX
    - Ograniczenia
    - E-mail
    - Wymiana
    - APN
    - Bluetooth
    - Połączenie

Android Enterprise – w pełni zarządzane urządzenie z profilem pracy (COPE)

- Ogólne wyjaśnienie COPE
- Konfiguracja profili dla urządzeń COPE
- Powrót do w pełni zarządzanego urządzenia AE

Android Enterprise – konfiguracja kontenera

- Ogólne
  - Przegląd profilu (tylko na poziomie profilu)
  - Przegląd profilu grupy (tylko na poziomie grupy)
  - Przegląd urządzeń (tylko na poziomie urządzenia)
  - Wersja konfiguracji
  - Dziennik urządzenia (tylko na poziomie urządzenia)
    - Dziennik poleceń
    - Możliwe statusy poleceń
  - Ustawienia urządzenia

- Konfiguracja klienta
- Tapeta

Zarządzanie zasobami (tylko na poziomie urządzenia)

- Informacje o urządzeniu
  - Wi-Fi
- Komórkowy
- Bluetooth

Zarządzanie bezpieczeństwem

- Ochrona przed kradzieżą (tylko na poziomie urządzenia)
  - Informacje GPS (tylko na poziomie urządzenia)
  - Wipe & Lock (tylko na poziomie urządzenia)
  - Wiadomość (tylko na poziomie urządzenia)
- Konfiguracja zabezpieczeń
  - Kod dostępu urządzenia
  - Kod dostępu do kontenera
  - Antywirus
- Koniec życia (tylko na poziomie urządzenia)
  - Wipe (tylko na poziomie urządzenia)
- Ustawienia ograniczeń
  - Ograniczenia
- Zarządzanie certyfikatami

Zarządzanie połączeniami

- Wifi
  - Typ zabezpieczenia
    - WEP
    - WPA/WPA2
    - 802.1x EAP
- VPN
  - Typ VPN
    - VPN
    - VPN dla poszczególnych aplikacji
- Ograniczenia

Zarządzanie PIM

- Gmail Exchange

Zarządzanie aplikacjami

- Menedżer aplikacji dla przedsiębiorstw
  - Zainstalowane aplikacje (tylko na poziomie urządzenia)
  - Aplikacje systemowe (tylko na poziomie urządzenia)
  - Aplikacje obowiązkowe
  - Aplikacje systemowe AE
- Ograniczenia i ustawienia
  - Ustawienia zarządzania aplikacjami
- Sklep z aplikacjami dla przedsiębiorstw
  - Wewnątrz firmy
- Sklep Play dla przedsiębiorstw
  - Sklep AE Play

Zarządzanie treścią

- ContentBox
- Bezpieczna przeglądarka

Konfiguracja systemu Android

Ogólne

- Przegląd profilu grupy (tylko na poziomie grupy)
  - Przegląd urządzeń (tylko na poziomie urządzenia)
- Wersja konfiguracji (tylko na poziomie urządzenia)
- Dziennik urządzenia (tylko na poziomie urządzenia)
  - Dziennik poleceń
  - Możliwe statusy poleceń
- Ustawienia urządzenia
  - Konfiguracja klienta
  - Tapeta

Zarządzanie zasobami (tylko na poziomie urządzenia)

- Zarządzanie aktywami
  - Informacje o urządzeniu
  - Wi-Fi
  - Komórkowy
  - Bluetooth

Zarządzanie bezpieczeństwem

- Ochrona przed kradzieżą (tylko na poziomie urządzenia)
  - Informacje GPS (tylko na poziomie urządzenia)

- Wipe & Lock (tylko na poziomie urządzenia)
- Wiadomość (tylko na poziomie urządzenia)
- Konfiguracja zabezpieczeń
  - Kod dostępu
  - Szyfrowanie
  - Antywirus
- Koniec życia (tylko na poziomie urządzenia)
  - Wipe (tylko na poziomie urządzenia)
- Ustawienia ograniczeń
  - Ograniczenia
  - Właściciel urządzenia AE

Kontener BYOD

- Android Enterprise
  - Android Enterprise
  - Gmail Exchange
  - Aplikacje systemowe AE
  - Kod dostępu do kontenera
- Samsung KNOX
  - Aktywacja
  - Kod dostępu Knox
  - Knox Security
  - Knox Exchange
  - Knox eMail
  - Knox Apps

Zarządzanie połączeniami

- Wifi
  - Typ zabezpieczenia
    - WEP
    - WPA/WPA2
    - 802.1x EAP
- VPN
- Ograniczenia
- APN
- Bluetooth

Zarządzanie PIM

- Wymiana
- eMail
- AE Gmail Exchange

Zarządzanie aplikacjami

- Menedżer aplikacji dla przedsiębiorstw
  - Zainstalowane aplikacje (tylko na poziomie urządzenia)
  - Aplikacje systemowe (tylko na poziomie urządzenia)
  - Aplikacje obowiązkowe
  - Aplikacje systemowe AE
- Ograniczenia i ustawienia
  - Czarna i biała lista
  - Ograniczenia aplikacji systemowych
    - Samsung Apps
    - Aplikacje Huawei
  - Ustawienia zarządzania aplikacjami
- Sklep z aplikacjami dla przedsiębiorstw
  - Sklep Play
  - Wewnątrz firmy
- Sklep Play dla przedsiębiorstw
- Tryb kiosku i program uruchamiający
  - Tryb kiosku
  - AppTec360 Launcher
  - Ustawienia AppTec360

Pilot zdalnego sterowania

- Splashtop
- Teamviewer

Zarządzanie treścią

- Contentbox
- Bezpieczna przeglądarka

Konfiguracja komputera z systemem Windows 10

Ogólne

- Przegląd profilu grupy (tylko na poziomie grupy)
- Przegląd urządzeń (tylko na poziomie urządzenia)
- Ustawienia

- Wersja konfiguracji (tylko na poziomie urządzenia)
- Dziennik urządzenia (tylko na poziomie urządzenia)
  - Dziennik poleceń
  - Możliwe statusy poleceń
- Zarządzanie zasobami (tylko na poziomie urządzenia)
  - Informacje o urządzeniu
  - Komórkowy
  - Informacje o synchronizacji
- Zarządzanie bezpieczeństwem
  - Ochrona przed kradzieżą (tylko na poziomie urządzenia)
    - Informacje GPS (tylko na poziomie urządzenia)
    - Ustawienia GPS
  - Konfiguracja zabezpieczeń
    - Kod dostępu
    - Antywirus
    - Centrum bezpieczeństwa
    - Konfiguracja zapory sieciowej
    - Reguły zapory sieciowej
  - Ustawienia ograniczeń
    - Funkcjonalność urządzenia
  - BitLocker
    - Konfiguracja funkcji BitLocker
    - Stan funkcji BitLocker
  - Zarządzanie certyfikatami
    - Lista certyfikatów
    - Konfiguracja certyfikatu
    - SCEP
- Zarządzanie połączeniami
  - Wifi
    - Typ zabezpieczenia
    - Użyj serwera proxy
  - Ograniczenia Wi-Fi
  - VPN
    - Typ połączenia
    - Ogólne konfiguracje VPN
  - Ograniczenia VPN
  - Bluetooth

- Zarządzanie PIM
  - Exchange Active Sync
  - eMail
- Zarządzanie aplikacjami
  - Menedżer aplikacji dla przedsiębiorstw
    - Zainstalowane aplikacje
    - Aplikacje obowiązkowe
    - Ograniczenia aplikacji systemowych
    - Czarna i biała lista

Konfiguracja macOS

Ogólne

- Przegląd profilu grupy (tylko na poziomie grupy)
- Przegląd urządzeń (tylko na poziomie urządzenia)
- Wersja konfiguracji (tylko na poziomie urządzenia)
- Dziennik urządzenia (tylko na poziomie urządzenia)
  - Dziennik poleceń
  - Możliwe statusy poleceń

Zarządzanie zasobami (tylko na poziomie urządzenia)

- Informacje o urządzeniu
- WiFi
- Komórkowy
- Bluetooth

Zarządzanie aktualizacjami (tylko na poziomie urządzenia)

- Informacje o aktualizacji

Zarządzanie bezpieczeństwem

- Ochrona przed kradzieżą
  - Wipe & Lock
- Konfiguracja zabezpieczeń
  - Kod dostępu
  - Certyfikat
- Ustawienia ograniczeń
  - Funkcjonalność urządzenia
  - iCloud
  - Zarządzanie mediami

- Zarządzanie połączeniami
  - Wi-Fi
    - Konfiguracja sieci Wi-Fi w przedsiębiorstwie
  - VPN
  - Serwer proxy HTTP
  - AirPrint
  - AirPlay
- Zarządzanie PIM
  - Exchange Active Sync
  - eMail
  - CalDav
  - CardDav
  - LDAP

Pulpit nawigacyjny i raportowanie

- Ustawienia pulpitu nawigacyjnego
- Widok pulpitu nawigacyjnego
- Rozszerzone raportowanie
  - Raporty zgodności
    - Zrootowane urządzenia
    - Urządzenia w roamingu
    - Urządzenia z włączonym roamingiem
    - Nadzorowane urządzenia
    - Nieaktywne urządzenia
  - Raporty o urządzeniach
    - Urządzenia według własności
    - Wszystkie urządzenia
    - Nośniki urządzeń
    - Bezpieczne urządzenia
    - Urządzenia Windows BitLocker
  - Raporty aplikacji
    - Zainstalowane aplikacje
    - Najczęściej instalowane aplikacje
    - Aplikacje obowiązkowe
    - Aplikacje na czarnej liście

- Raporty użytkowników
  - Taryfa
- Zarządzanie wieloma dzierżawcami
  - Dodatkowe widoki
    - Lista wszystkich klientów
    - Daty wygaśnięcia APNS
- Kontakt
  - Ogólne pytania techniczne
  - W przypadku pytań związanych z instalacją urządzenia wirtualnego
- Zastrzeżenie

Przegląd ogólny

Wprowadzenie do AppTec360

Rozwiązanie AppTec Enterprise-Mobile-Management-Solution oferuje opcję zarządzania i konfigurowania wszystkich urządzeń mobilnych za pomocą intuicyjnej konsoli zarządzania. W tym scenariuszu serwer EMM może działać we własnym środowisku lub można skorzystać z naszego rozwiązania opartego na chmurze.

Nawet jeśli chodzi o centralną instalację aplikacji korporacyjnych na smartfonach, trafiłeś we właściwe miejsce. Enterprise Mobile Manager umożliwia dystrybucję firmowych aplikacji i dokumentów na urządzenia w ciągu kilku sekund lub blokowanie niepożądanych aplikacji za pomocą białej/czarnej listy.

Korzystanie z prywatnych urządzeń w firmach stanowi nowe wyzwanie dla zabezpieczenia smartfonów i tabletów. Ze względu na fakt, że pracownicy chcą coraz częściej korzystać ze swoich smartfonów, administratorzy IT muszą chronić dużą liczbę różnych typów urządzeń. Pomożemy Ci zabezpieczyć wszystkie urządzenia i przechowywane na nich wrażliwe dane oraz zarządzać nimi z poziomu intuicyjnej konsoli.

Obsługiwane systemy operacyjne urządzeń

AppTec360 oferuje wsparcie dla urządzeń z systemami iOS, Android i Windows. Należy pamiętać, że wydajność funkcji wymienionych platform może się różnić w zależności od systemu operacyjnego.

- Apple iOS 11.0 lub nowszy*
- Apple macOS 10.11 lub nowszy
- Google Android 4.4 lub nowszy** w wersji Cloud
- Google Android 4.1 lub nowszy** w wersji OnPrem
- MS Windows 10 lub nowszy*** (komputer stacjonarny, notebook i tablet)

**Należy pamiętać, że urządzenia z systemem iOS 10 lub starszym nie mogą zostać zarejestrowane ze względu na drastyczne zmiany wprowadzone przez Apple w procesie rejestracji.*

***Urządzenia mogą być podłączone i skonfigurowane, nawet jeśli korzystają z wersji, która nie jest już obsługiwana przez producenta. Należy pamiętać, że niektóre funkcje mogą wymagać określonej wersji systemu Android. W przypadkach wsparcia postępujemy zgodnie z oficjalnym wsparciem producenta. W przypadku problemów lub błędów spowodowanych przez przestarzałą wersję, która nie jest już wspierana przez producenta, zastrzegamy sobie prawo do oferowania jedynie ograniczonego wsparcia.*

**** Domowa wersja systemu Windows nie jest obsługiwana ze względu na ograniczenia systemu operacyjnego. Zdecydowanie zalecamy korzystanie z wersji systemu operacyjnego, która jest nadal obsługiwana przez producenta. Nie tylko ze względu na kompatybilność, ale także ze względów bezpieczeństwa. Dlatego zalecamy system iOS 12 lub nowszy oraz Android 9 lub nowszy.*

Obsługiwane katalogi LDAP

- Microsoft Active Directory
- Otwórz LDAP

Aktualne informacje na temat "Obsługiwanych systemów operacyjnych urządzeń" i "Obsługiwanych katalogów LDAP" można znaleźć tutaj:

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

Wyjaśnienie „trybu nadzorowanego” na urządzeniach Apple

Tryb nadzorowany stanowi rozszerzony interfejs dla urządzeń z systemem iOS.

Na odpowiednio skonfigurowanym urządzeniu można zastosować dodatkowe ograniczenia dotyczące funkcjonalności urządzenia użytkownika końcowego. Są one również zawarte w podręczniku administracyjnym i oznaczone banerem.

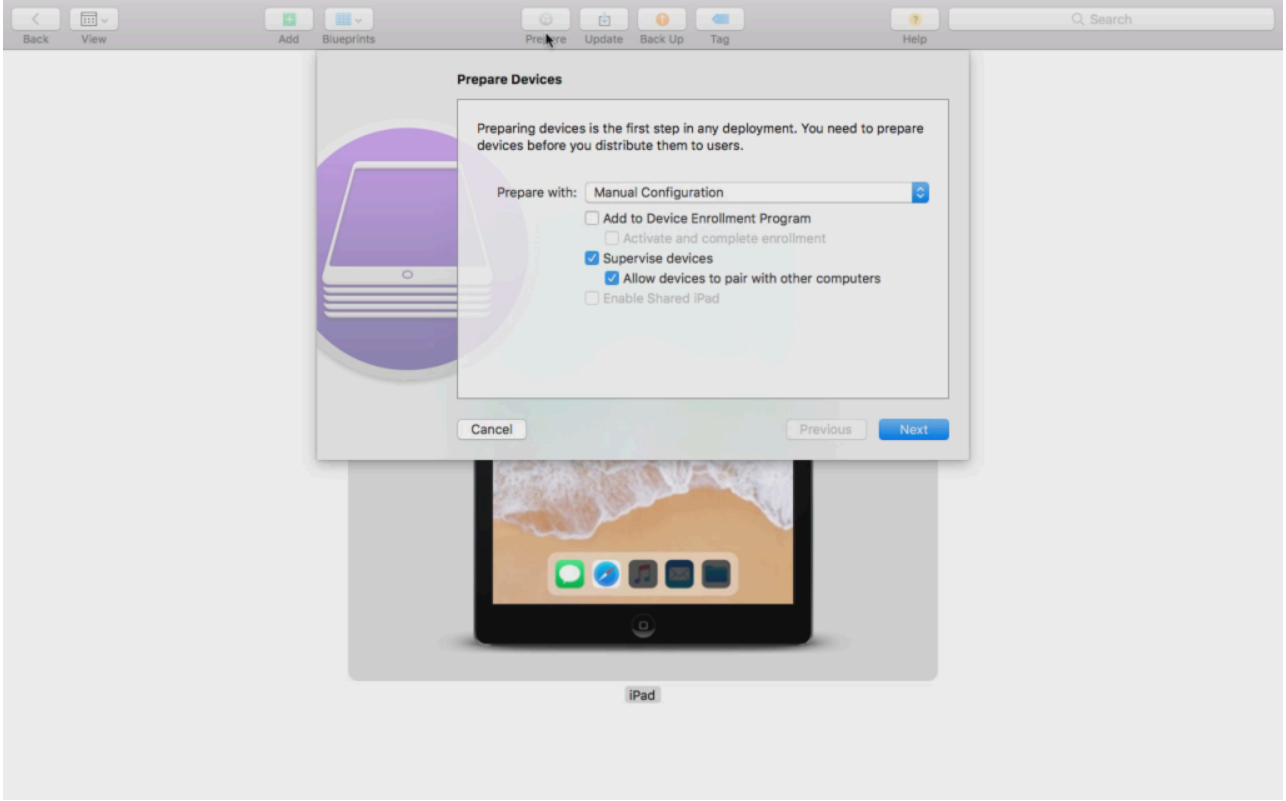
Dostępne w trybie nadzorowanym

Tryb nadzorowany" można aktywować za pomocą programu "Apple Configurator". Apple Configurator może ustawić domyślne ustawienia na nowych urządzeniach iOS jako narzędzie konfiguracyjne (za pośrednictwem interfejsu USB).

Narzędzie może nie tylko instalować profile konfiguracyjne, ale także aplikacje. Jest ona bezpłatna, ale wymaga komputera Mac.

Aktywacja trybu nadzorowanego

1. Otwórz aplikację Apple Configurator



2. Kliknij urządzenie i wybierz opcję "Przygotuj".
3. Wybierz "Konfiguracja ręczna" i "Nadzoruj urządzenia".
4. Kliknij "Dalej"
5. (Opcjonalnie) Teraz można dodać serwer MDM, na którym urządzenie zostanie zarejestrowane. Link do tego można znaleźć w "Ustawienia ogólne - Konfiguracja iOS - Konfigurator i adres URL" Wybierz swoją organizację lub utwórz nową.
6. Wybierz swoją organizację lub utwórz nową
7. Wybierz, które kroki należy pominąć w początkowej konfiguracji i kliknij "Dalej" (UWAGA: kontynuowanie spowoduje usunięcie urządzenia!).

Teraz urządzenie zostanie przełączone w tryb nadzorowany. Może to zająć kilka minut. Po zakończeniu urządzenie uruchomi się ponownie.

Teraz urządzenie jest nadzorowane!

Dodawanie urządzenia do DEP

Urządzenia z systemem iOS 11 lub nowszym można również dodawać do programu DEP (Device Enrollment Programm) za pomocą aplikacji Apple Configurator.

Więcej informacji o DEP: https://www.apple.com/business/dep/

Wykonaj te same kroki, jak w przypadku nadzorowania urządzenia i dodatkowo zaznacz opcję "Add to Device Enrollment Programm". Zostaniesz poproszony o podanie danych logowania do DEP, jeśli nigdy wcześniej nie logowałeś się do DEP za pomocą Apple Configurator.

Po zakończeniu procesu urządzenie można znaleźć na serwerze DEP "Devices Added by Apple Configurator 2". Można teraz użyć tego serwera i podłączyć go do konsoli zarządzania lub przenieść urządzenie do już istniejącego serwera.

Urządzenie zostało pomyślnie dodane do DEP!

Wyjaśnienie Android Enterprise

Czym jest Android Enterprise?

Android Enterprise oferuje lepszą kontrolę nad urządzeniami roboczymi, które są zarządzane za pomocą MDM. Pozwala to administratorom mieć pełną kontrolę nad urządzeniami z Androidem lub oddzielić dane firmowe od danych prywatnych na urządzeniach kontenerowych. Dodatkowo Android Enterprise pozwala na łatwiejszą rejestrację urządzeń i łatwą dystrybucję aplikacji.

Jakie są wymagania do korzystania z Android Enterprise?

Android Enterprise może być używany za darmo przez każdego. Wystarczy podłączyć konto Google do MDM, aby włączyć wszystkie funkcje Android Enterprise. Więcej informacji na ten temat można znaleźć w sekcji Android Enterprise.

Android Enterprise może być używany na urządzeniach z systemem Android 5.1 lub nowszym, z wyjątkiem Enhanced Work Profile (patrz poniżej). Zalecamy co najmniej system Android 7 lub nowszy w celu łatwiejszej rejestracji lub Android 11 w celu wykorzystania wszystkich dostępnych funkcji.

Jakie są dostępne tryby w Android Enterprise?

Podczas korzystania z Android Enterprise dostępne są 3 różne tryby.

AE Urządzenie w pełni zarządzane (Work Managed): W pełni zarządzane urządzenie, które jest używane tylko do pracy. Pozwala to administratorowi na pełną kontrolę nad urządzeniem. Nie pozwala to na prywatne korzystanie z urządzenia. Aby zarejestrować urządzenia w tym trybie, należy je zresetować i zarejestrować za pomocą kodu QR (patrz Rejestracja AE) lub zarejestrować za pomocą rejestracji Knox lub Zero Touch.

AE BYOD Container: Kontener BYOD (bring your own device) umożliwia użytkownikom dostęp do danych firmowych na ich prywatnym telefonie w oddzielnym kontenerze. W tym trybie prywatne aplikacje nie widzą danych i aplikacji firmowych i odwrotnie. Aby zarejestrować urządzenia w tym trybie, należy pobrać aplikację AppTec i zeskanować kod QR. Utwórz urządzenie w konsoli i wybierz "AE Container (BYOD & Enahnced Work Profile)" jako typ urządzenia. Kliknij kod QR na nowo wygenerowanym urządzeniu, aby uzyskać kod QR i ustawić pierwszy przełącznik na "Legacy & BYOD".

AE Enhanced Work Profile: (wymaga systemu Android 11 lub nowszego) Podczas gdy wyżej wspomniany kontener BYOD przenosi dane firmowe na prywatne urządzenie, Enhanced Work Profile robi to samo, ale na urządzeniu należącym do firmy. Tworzy ten sam kontener, ale daje administratorowi nieco większą kontrolę nad urządzeniem, więc użytkownik nie może po prostu usunąć MDM z urządzenia. Utwórz urządzenie w konsoli i wybierz "AE Container (BYOD & Enahnced

Work Profile)" jako typ urządzenia. Kliknij kod QR na nowo wygenerowanym urządzeniu, aby uzyskać kod QR i ustawić pierwszy przełącznik na "Enhanced Work Profile". Ten kod QR można zeskanować po zresetowaniu urządzenia i stuknięciu 6 razy w ekran, jak wyjaśniono w Metodzie 1 w rejestracji AE.

Jak mogę przypisać aplikacje do urządzeń Android Enterprise?

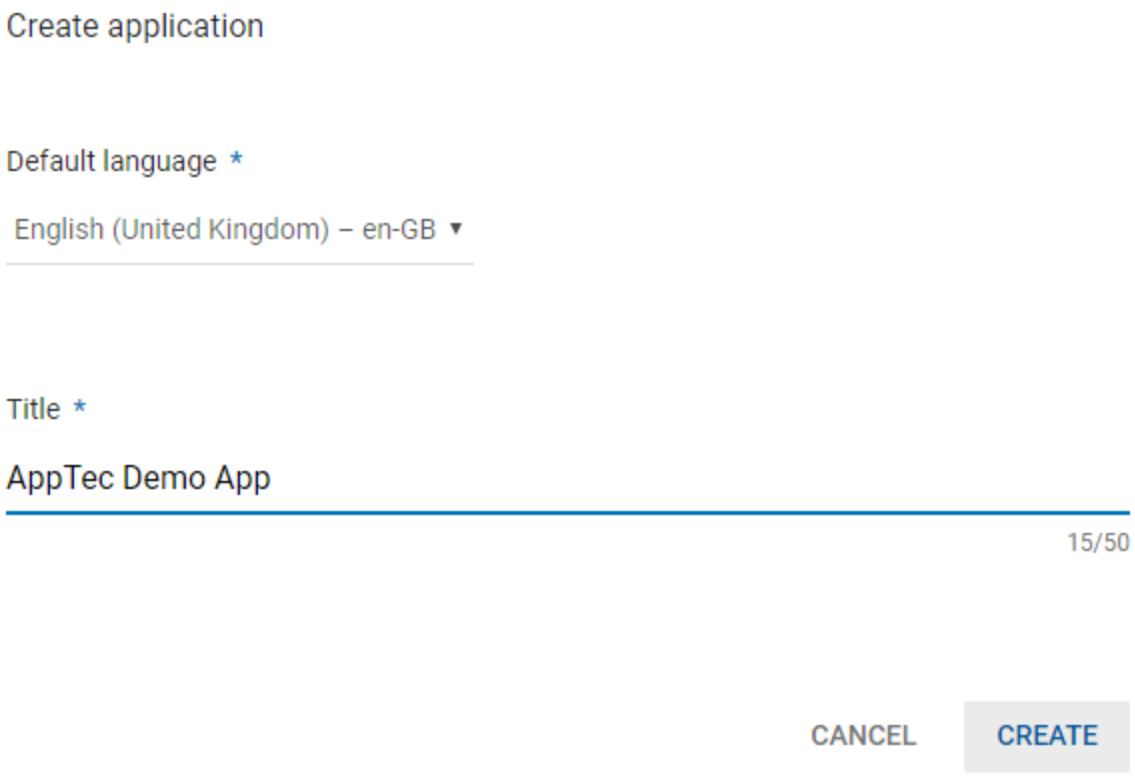
Najpierw musisz zatwierdzić aplikacje, których chcesz używać w Ustawieniach ogólnych → Zarządzanie aplikacjami → Sklep AE Play → Aplikacje Sklepu Play. Po zatwierdzeniu aplikacji możesz przypisać ją do listy obowiązkowych aplikacji → swojego profilu, klikając "+" i wybierając aplikację z zakładki "AE Play Store". Spowoduje to automatyczne pobranie i zainstalowanie aplikacji. Nie jest wymagane konto Google na urządzeniu, a użytkownik nie musi potwierdzać ani zezwalać na to.

Przesyłanie własnych aplikacji do sklepu Google Play

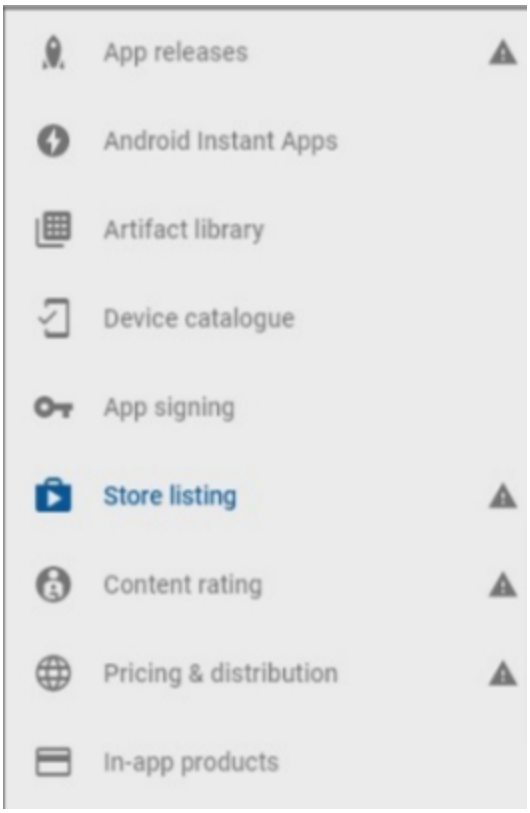
Możliwe jest przesyłanie aplikacji wewnętrznych do Sklepu Google Play. W ten sposób można korzystać z różnych zalet, takich jak mechanizm aktualizacji Sklepu Play.

Aby to zrobić, potrzebujesz konta Google Developer. Zaloguj się za pomocą Konsoli Google Play(https://play.google.com/apps/publish).

Kliknij "Utwórz aplikację". Wybierz domyślny język i tytuł aplikacji.



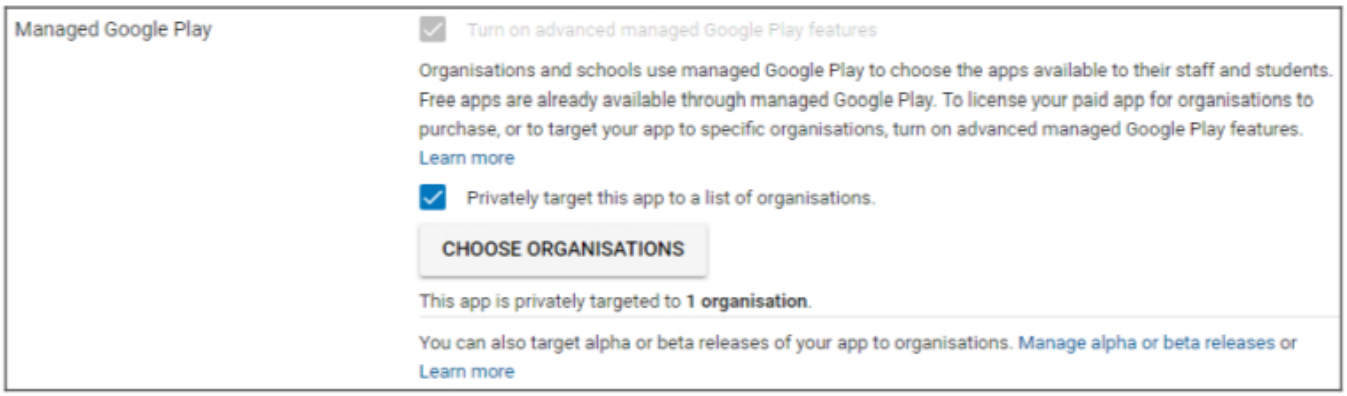
Na następnej stronie zostaniesz poproszony o wprowadzenie różnych szczegółów dotyczących Twojej aplikacji.



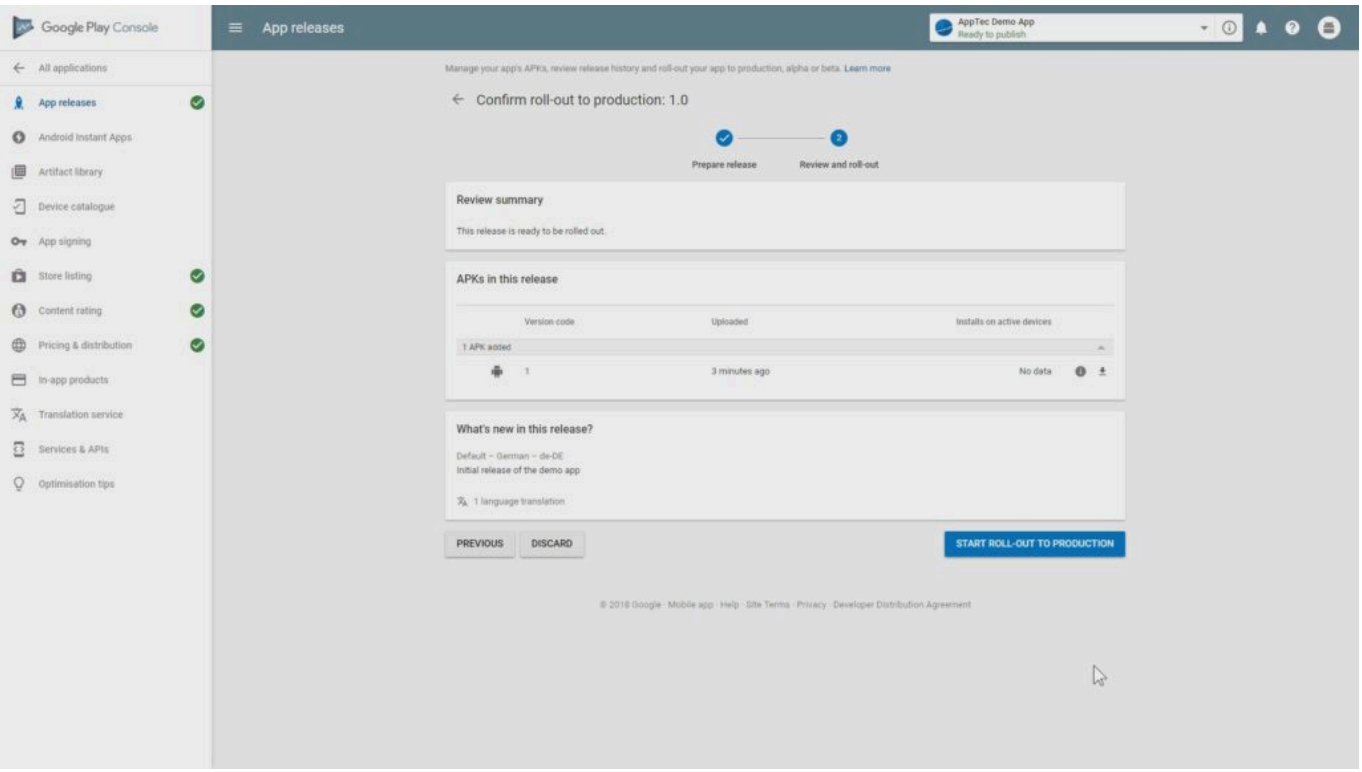
Po wprowadzeniu wszystkich szczegółów, po lewej stronie pojawią się różne symbole podpowiedzi.

Najedź na nie kursorem, aby zobaczyć, które kroki pozostały do wykonania i wykonaj je w dowolnej kolejności.

Uwaga: Upewnij się, że zaznaczone są dwa pola wyboru "Zarządzane Google Play" w sekcji "Ceny i dystrybucja". W przeciwnym razie aplikacja będzie publiczna i dostępna dla wszystkich. Upewnij się również, że wybrałeś kraj dystrybucji.



Po wykonaniu wszystkich kroków możesz przejść do "Wydania aplikacji". Kliknij "Review" i "Start Roll-Out to Production", aby sfinalizować wersję roboczą i opublikować aplikację.



Może minąć trochę czasu, zanim aplikacja będzie dostępna w Sklepie Play. Po zakończeniu procesu można wyszukać aplikację w sklepie Play for Work i zatwierdzić ją. Następnie możesz po prostu przypisać aplikację do urządzeń za pomocą konsoli EMM, tak jak robisz to z innymi aplikacjami.

Wymagania i instalacja

Wymagania

Wymagania systemowe

Urządzenie wirtualne jest dostępne w formacie Open Virtualization Format (VMWare, VirtualBox, Citrix Xen Server) oraz jako skompresowany plik .vhdx (Hyper-V)*.

*Uwaga: W przypadku korzystania z Hyper-V maszyna musi zostać utworzona w Generacji 1.

Dysk wirtualny ma docelowy rozmiar 20 GB, a maszyna wymaga 4 GB pamięci RAM.

Urządzenie jest oparte na systemie Debian 9 64bit

Zaktualizuj zaimportowaną maszynę do najnowszej wersji kompatybilności (np. w VMWare) i upewnij się, że typ systemu operacyjnego maszyny jest prawidłowo ustawiony w hiperwizorze.

Klucz licencyjny

Aby pomyślnie aktywować i zainstalować serwer, potrzebny jest ważny plik licencyjny. Można go uzyskać bezpośrednio od AppTec360 i/lub od odpowiedniego sprzedawcy.

Rozpoznawanie adresów IP i DNS

Urządzenie AppTec360 musi być osiągalne przez urządzenie przy użyciu nazwy hosta, dla której wydano licencję.

Aby zarejestrować urządzenia z systemem Windows 10, należy również skonfigurować dodatkową subdomenę w postaci "enterpriseenrollment.", wskazującą na urządzenie.

Certyfikat SSL

Ponieważ wszystkie połączenia z i do urządzeń muszą być zabezpieczone przy użyciu protokołu SSL, wymagany jest ważny certyfikat dla nazwy hosta wydany przez zaufany przez urządzenie urząd certyfikacji. Klucz prywatny certyfikatu musi zostać przesłany bez zabezpieczenia hasłem. W większości przypadków wymagany jest pośredni certyfikat urzędu certyfikacji, aby urządzenia mogły rozpoznać certyfikat serwera.

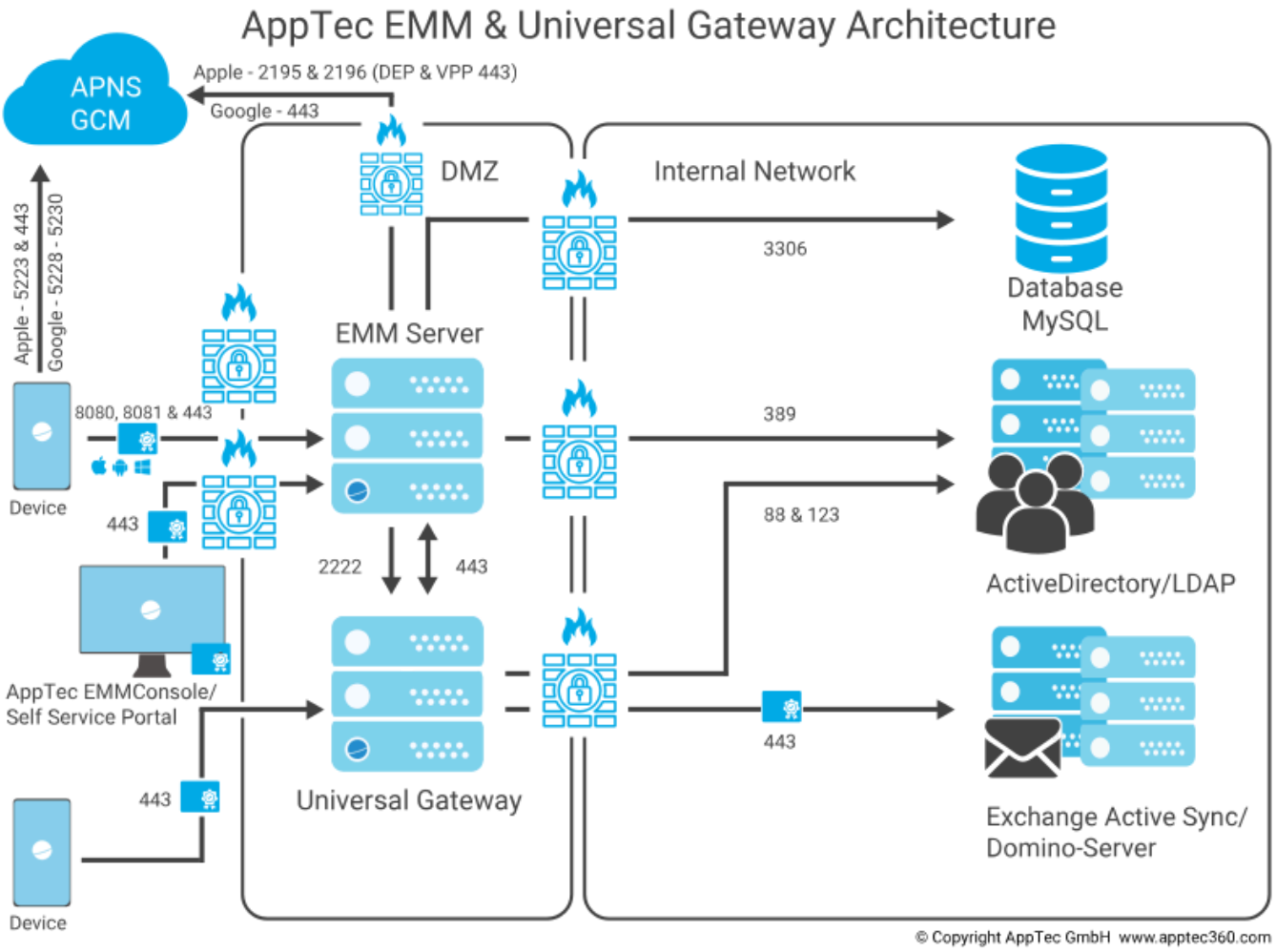
Urządzenia z systemem Windows 10 będą wymagały specjalnego certyfikatu dla subdomeny enterpriseenrollment.

Począwszy od wersji appliance 202104 można również korzystać z certyfikatów Let's Encrypt, które są generowane automatycznie (opisane w kroku drugim - Certyfikat SSL).

Serwer SMTP

Wymagany jest serwer e-mail i/lub przekaźnik e-mail, aby umożliwić AppTec360 EMM wysyłanie wiadomości e-mail (np. w celu rejestracji urządzenia i weryfikacji konta).

Reguły zapory sieciowej



Ten schemat pokazuje, które połączenie jest wymagane w zależności od usług, z których chcesz korzystać.

Bardziej szczegółowy opis znajduje się w tabeli na następnej stronie.

Dowolny (zewnętrzny/urządzenia)	→	**AppTec360 Appliance / emmconsole.com**
Porty	443	Zarządzanie, Enterprise AppStore i Windows Phone Communication
	8080	Komunikacja w systemach Android i iOS
	80	Pierwsza konfiguracja Let's Encrypt. Następnie używa 443.
Dowolny (urządzenia)	→	**Dowolny (zewnętrzny)**
Porty	5223, 443	Usługa Apple Push, musi być dostępna bez proxy, 443 jako Fallback, patrz https://support.apple.com/en-us/HT203609.
	5228-5230	Usługa Android Push (FCM) musi być dostępna bez serwera proxy.
AppTec360 Appliance	→	**Kontroler domeny**
Porty	389, (LDAPS 636)	Synchronizacja użytkowników z LDAP
AppTec360 Appliance	→	**Dowolny**
Port	443	Używany dla usługi Android Push Service (GCM) Wyszukiwanie w AppStore/Sklepie Play
AppTec360 Appliance	→	**emmconsole.com**
Porty	443	Aktualizacje AppTec360 Appliance, generowanie certyfikatów APNS
AppTec360 Appliance	→	**Sieć Apple (17.0.0.0/8)**
Porty	2195, 2196	Usługa Apple Push Service i usługa przekazywania opinii
	443	DEP I VPP

Aktualizacje zabezpieczeń

System operacyjny Debian powinien być regularnie aktualizowany, aby otrzymywać najnowsze poprawki bezpieczeństwa. Upewnij się jednak, że nie aktualizujesz ręcznie do nowszej wersji Debiana. Gdy AppTec360 EMM będzie kompatybilny z nowszą wersją główną, dodamy sposób aktualizacji w aktualizacji urządzenia.

Domyślne hasła urządzenia wirtualnego

Użytkownik logowania (logowanie root jest wyłączone. Użyj "sudo" do zadań administracyjnych)

apptec

Hasło logowania

apptec

Użytkownik główny MySQL

korzeń

Hasło główne MySQL

apptec

Domyślny użytkownik MySQL

AppTec

Domyślne hasło użytkownika MySQL

AppTec

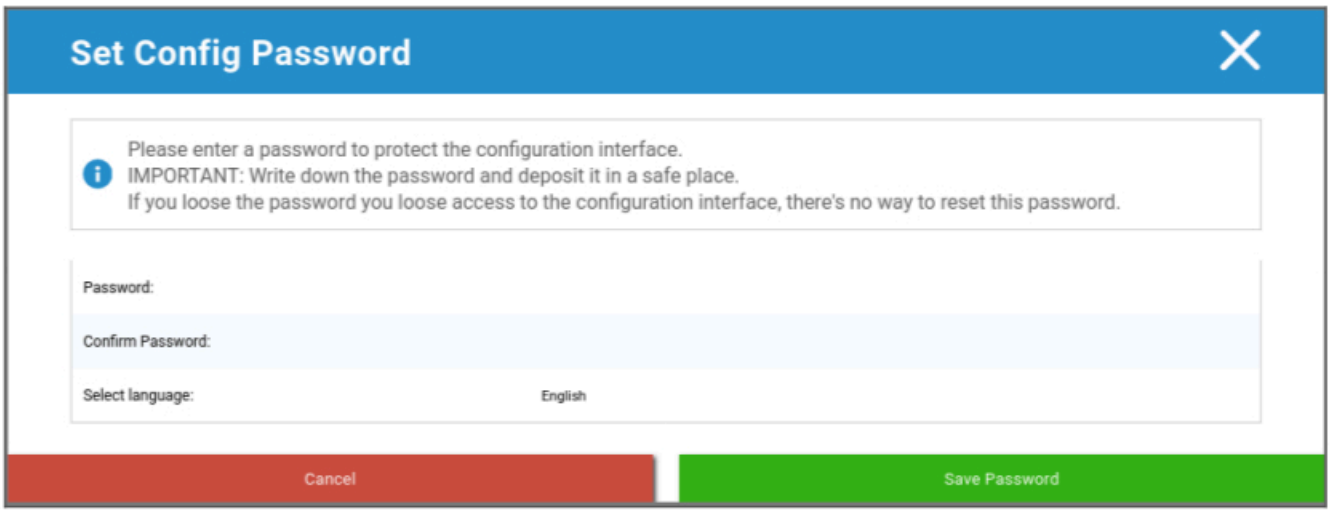
Konfiguracja urządzenia wirtualnego

Ważne: Przed rozpoczęciem konfiguracji urządzenia wirtualnego rozdzielczość ekranu powinna wynosić co najmniej 1280 x 800 pikseli.

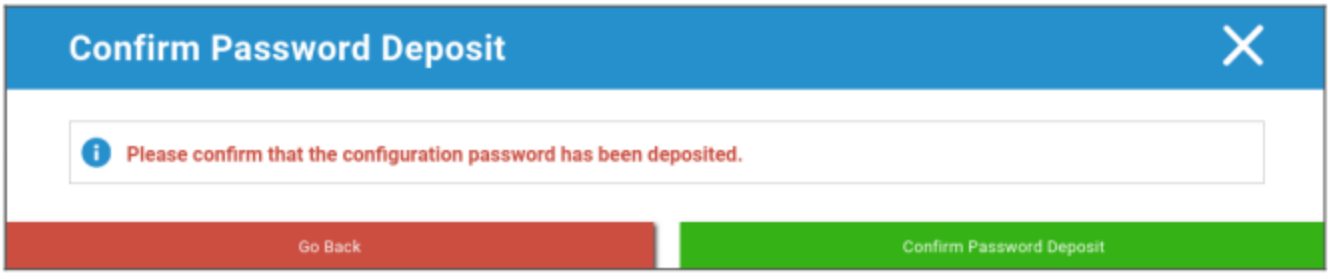
Po zalogowaniu się do urządzenia, Firefox powinien uruchomić się automatycznie i wyświetlić interfejs konfiguracyjny.

Przygotowanie

Najpierw należy podać hasło do interfejsu konfiguracyjnego. Hasło to służy do szyfrowania wszystkich informacji i plików wprowadzanych w interfejsie konfiguracyjnym. W tym miejscu można również ustawić język, w którym ma być wyświetlany interfejs (można go zmienić później).

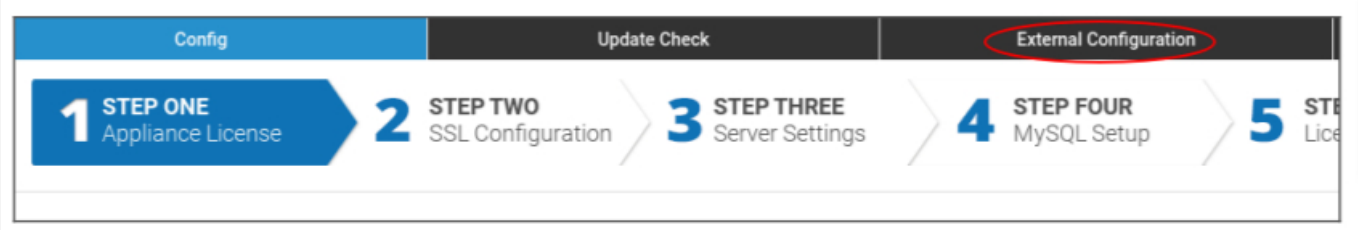


Hasło może zostać zresetowane tylko przez dział wsparcia AppTec360, więc upewnij się, że zdeponowałeś je w bezpiecznym miejscu i potwierdziłeś nadchodzące wyskakujące okienko.



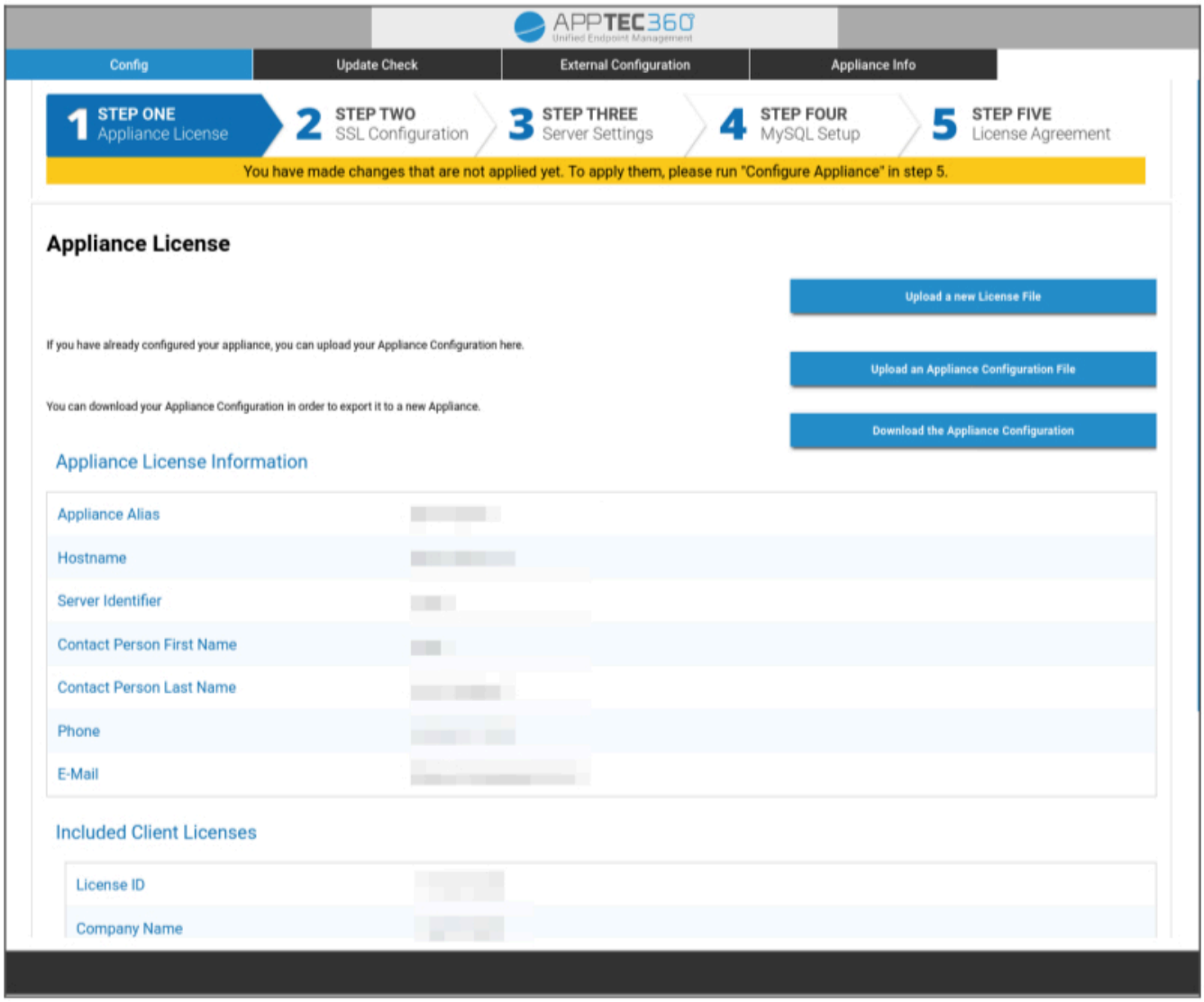
Konfiguracja z zewnętrznego hosta

Aby ułatwić proces konfiguracji, można udostępnić stronę konfiguracji zdalnie. Aby to zrobić, wykonaj kroki opisane w sekcji "Konfiguracja z zewnętrznego hosta".



Krok pierwszy – Licencja na urządzenie

1. Prześlij plik licencji otrzymany od AppTec.
2. Jeśli plik licencji został przesłany pomyślnie, możesz zobaczyć informacje o licencji urządzenia, jak na poniższym zrzucie ekranu.



Krok drugi – Certyfikat SSL

Możesz skorzystać z automatycznej konfiguracji certyfikatu za pomocą Let's Encrypt lub dostarczyć certyfikaty samodzielnie (więcej informacji można znaleźć w sekcji Certyfikat SSL).

Automatyczny

Certyfikat zostanie wygenerowany automatycznie przy użyciu usługi Let's Encrypt.

AppTec360 EMM wykorzystuje wyzwanie HTTP-01 do walidacji domeny, co oznacza, że port HTTP musi być otwarty z Internetu dla pierwszego żądania certyfikatu. Kolejne żądania odnowienia mogą być walidowane przez HTTPS.

Przełącz przyciski opcji na "Automatycznie (Let's Encrypt)" i naciśnij "ZAPISZ WARTOŚCI". Certyfikat zostanie automatycznie zażądany podczas stosowania konfiguracji w kroku piątym - Umowa licencyjna. W razie potrzeby certyfikat zostanie automatycznie odnowiony, a użytkownik otrzyma wiadomość e-mail, jeśli certyfikat wkrótce wygaśnie (co oznacza, że odnowienie mogło się nie powieść).

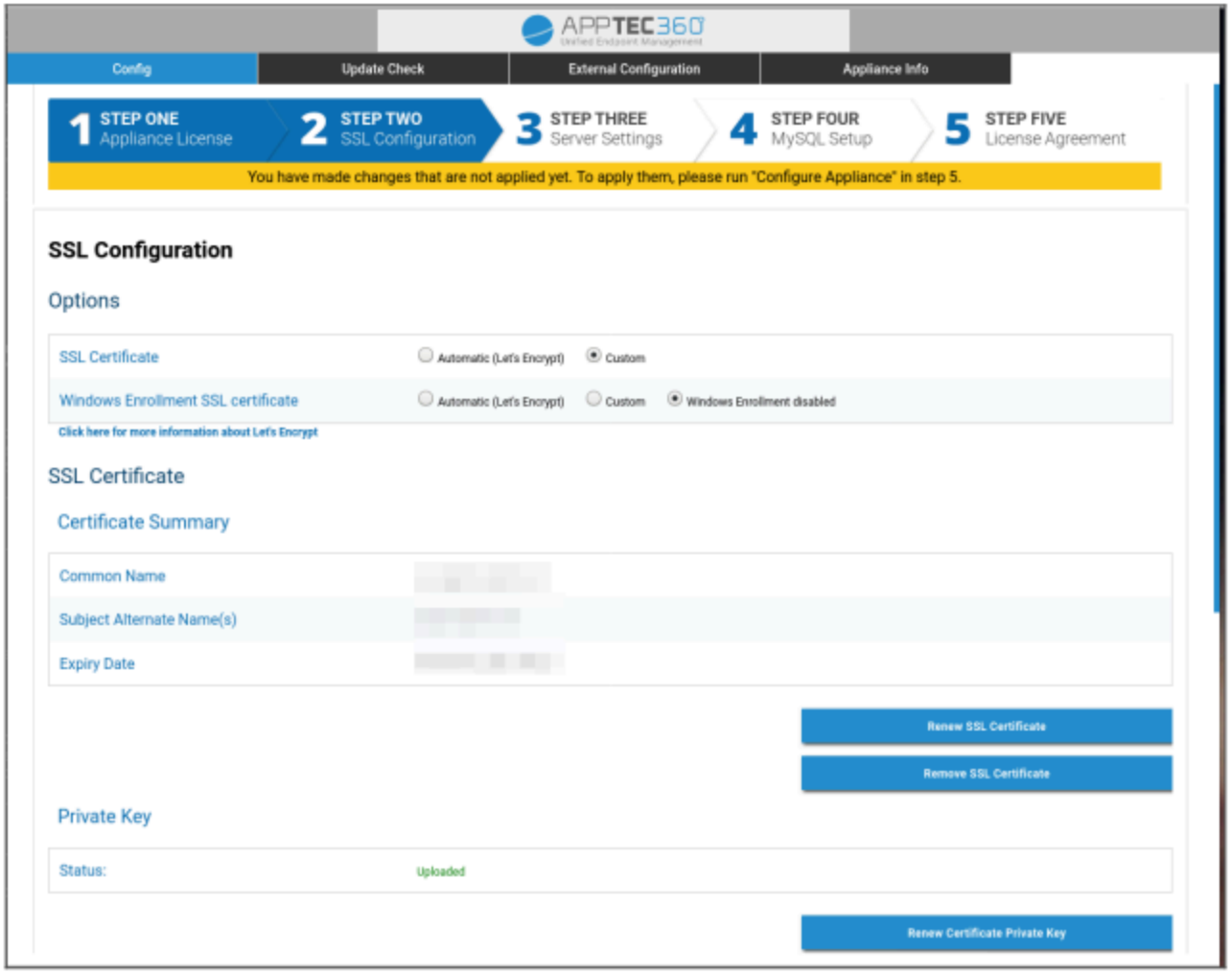
Niestandardowe

1. Prześlij certyfikat SSL dla licencjonowanej nazwy hosta. Nazwę hosta można sprawdzić w kroku pierwszym - Licencja urządzenia.

2. Prześlij również klucz prywatny certyfikatu i w razie potrzeby certyfikat pośredni.

Ważne: Klucz nie może być chroniony hasłem. Jeśli tak, usuń hasło przed przesłaniem.

Wskazówka: Jeśli chcesz również korzystać z urządzeń z systemem Windows 10, musisz włączyć opcję "Windows Enrollment SSL certificate" i przesłać certyfikat, klucz prywatny i certyfikat pośredni dla swojej subdomeny (opisane w sekcji Przesyłanie adresów IP i rozpoznawanie DNS) na dole strony.



Krok trzeci – Ustawienia serwera

1. Wprowadź globalny adres e-mail pomocy technicznej. Ten adres będzie używany w wiadomościach e-mail do użytkowników, aby wiedzieli, z kim się skontaktować w przypadku jakichkolwiek problemów związanych z ich urządzeniem.
2. Podaj ustawienia wiadomości e-mail, które będą używane przez system do wysyłania wiadomości e-mail. Ustawienia te będą używane do wysyłania wiadomości e-mail do użytkownika, a także do wysyłania raportów o błędach i żądań funkcji na adres"support@apptec360.com".Po zapisaniu ustawień poczty e-mail należy je zweryfikować, klikając "Testuj konfigurację poczty e-mail" i postępując zgodnie z instrukcjami.

Krok czwarty – Konfiguracja MySQL

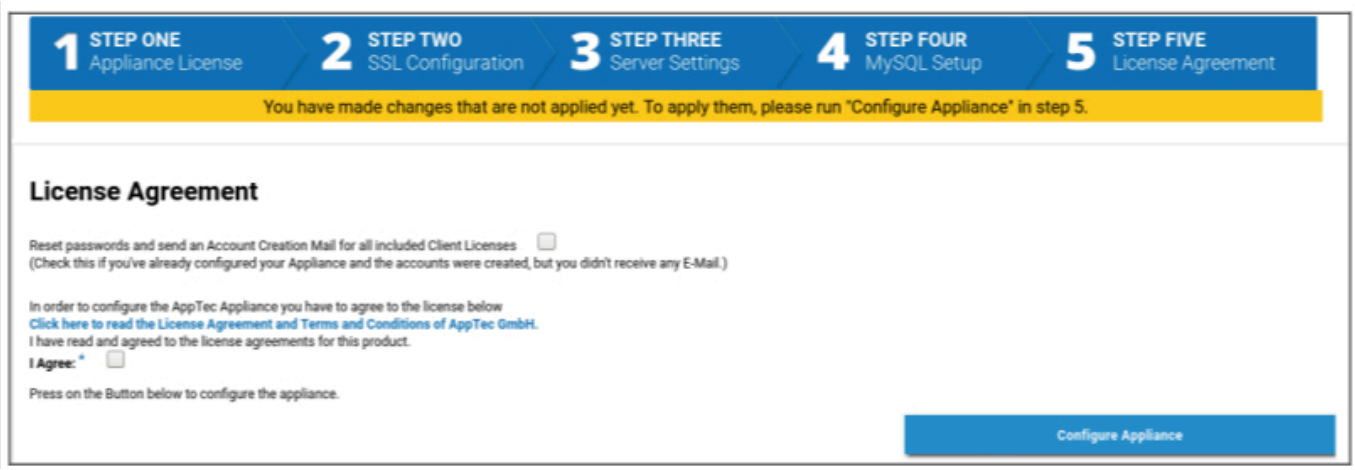
1. Jeśli chcesz korzystać z wewnętrznej bazy danych, możesz pominąć ten krok. W przeciwnym razie możesz wprowadzić informacje o połączeniu z zewnętrznym serwerem bazy danych.


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)

Krok piąty – Umowa licencyjna

1. Prosimy o zapoznanie się z umową licencyjną.
2. Zaznacz "Zgadzam się" i naciśnij przycisk "Konfiguruj urządzenie", aby zastosować ustawienia.

Wskazówka: Za każdym razem, gdy zmienisz ustawienia w 5 krokach, będziesz musiał uruchomić "Configure Appliance", aby zastosować ustawienia.



Gratulacje!

Konfiguracja urządzenia wirtualnego została zakończona.

Wiadomość e-mail zawierająca hasło została wysłana na adres podany dla licencji (widoczny w sekcji "Dołączone licencje klienta" w kroku pierwszym - Licencja urządzenia).

Możesz teraz zalogować się do konsoli przy użyciu tego hasła i adresu e-mail, na który je otrzymałeś.

Aby zalogować się do konsoli, należy wpisać nazwę hosta konsoli w pasku adresu przeglądarki.

Nazwę hosta urządzenia można znaleźć w kroku pierwszym - Licencja urządzenia.

Rozwiązywanie problemów

1. Nie otrzymałeś wiadomości e-mail podczas konfigurowania urządzenia w kroku piątym - Umowa licencyjna:

Upewnij się, że ustawienia poczty e-mail w kroku trzecim - Ustawienia serwera są prawidłowe. Aby ponownie wysłać hasło, zaznacz opcję "Reset passwords and send an Account Creation Mail for all included Client Licenses" w kroku piątym - Umowa licencyjna przed ponownym uruchomieniem opcji "Configure Appliance".

2. Otrzymałeś błąd w odniesieniu do Let's Encrypt podczas konfiguracji w kroku piątym - Umowa licencyjna:

Upewnij się, że urządzenie jest osiągalne przez nazwę domeny na porcie 80. Let's encrypt zapisuje również dziennik do "/var/log/letsencrypt", który może pomóc w dalszym rozwiązywaniu problemów.

Zalecenia dotyczące bezpieczeństwa

Zaleca się wykonanie następujących kroków w celu zabezpieczenia urządzenia AppTec360.

Nie jest to pełny zestaw instrukcji, a jedynie zalecenie dotyczące podstawowej konfiguracji.

- Zmiana hasła dla użytkownika AppTec360
- Zmień hasło dla użytkowników MySQL "root" i "AppTec" i odpowiednio zaktualizuj Krok czwarty - Konfiguracja MySQL
- Zmiana domyślnego portu serwera SSH
- Zablokuj port 80 w konsoli i nie zezwalaj na przychodzący ruch HTTP, używaj tylko HTTPS. Po skonfigurowaniu możliwa jest również zewnętrzna konfiguracja przez HTTPS.
- Ogranicz dostęp do interfejsu zarządzania tylko do niektórych Ips w dolnej części kroku trzeciego - Ustawienia serwera.
- Konfiguracja zapory sieciowej

Ustawienia ogólne

Przegląd konta

Informacje o koncie

Przegląd

Tutaj możesz zobaczyć przegląd swojego konta AppTec360.

Nazwa firmy	Nazwa firmy
Data utworzenia	Data utworzenia konta
Typ licencji	Płatna = płatna licencja Darmowa = nieodpłatna licencja Uwaga: Konta na urządzeniu OnPremise będą zawsze wyświetlane jako opłacone z przyczyn technicznych.
Identyfikator klienta	Identyfikator konta (NIE jest to numer klienta)
Data wygaśnięcia licencji	Data wygaśnięcia licencji AppTec360
Licencja ContentBox	Free = darmowa licencja na 25 urządzeń Płatna = płatna licencja na x urządzeń
Launcher	Pokazuje, czy można używać niestandardowego programu uruchamiającego dla systemu Android.
Urządzenia	Liczba aktualnie używanych licencji / całkowita liczba licencji
Osoba kontaktowa	Podana osoba kontaktowa
Telefon	Podany numer telefonu
eMail*	Podany adres e-mail
Użytkownik root	Użytkownicy root, którzy mogą się zalogować
Wersja oprogramowania	Aktualna wersja oprogramowania

**Uwaga: Podany tutaj adres e-mail jest adresem wprowadzonym podczas rejestracji konta. Na tej podstawie w drzewie użytkowników/urządzeń zostanie utworzony użytkownik, którego można modyfikować. Edycja tego użytkownika spowoduje zmianę adresu e-mail, którego należy użyć do zalogowania się, ale nie zmieni informacji w przeglądzie konta. .*

Raport o błędzie

Raport o błędzie może zostać wysłany bezpośrednio do pomocy technicznej w celu zgłoszenia problemów lub błędów i zawiera informacje i dzienniki dotyczące konta i konfiguracji.

Przedmiot	Temat zgłoszenia błędu. Dołącz numer zgłoszenia, jeśli chcesz dodać je do istniejącego zgłoszenia do pomocy technicznej.
Oczekiwane zachowanie	Opisz szczegółowo, co zrobiłeś i czego oczekiwałeś.
Rzeczywiste zachowanie	Opisz szczegółowo, co dokładnie się stało. Prosimy o DOKŁADNE cytowanie komunikatów o błędach. Pomocne będzie również dodanie zrzutów ekranu do załącznika.
Kiedy wystąpił problem?	Podaj dokładny czas, w którym pojawił się konkretny komunikat o błędzie/problem. W najlepszym przypadku uwzględnij także sekundy, np. 18:55:27.
Czy problem można powtórzyć? Jeśli tak, to w jaki sposób (szczegółowo)?	Opisz szczegółowo, w jaki sposób możesz odtworzyć problem.
Czy ta funkcja działała wcześniej zgodnie z oczekiwaniami? Jeśli tak, to do kiedy?	Pozostaw puste, jeśli nie wiesz.
Czy przed wystąpieniem tego problemu wprowadzono jakieś konkretne zmiany w systemie? Jeśli tak, jakie zmiany (szczegółowo)?	Zawsze wspominaj o ostatniej zmianie lub działaniu przed pojawieniem się problemu, nawet jeśli uważasz, że jest to nieistotne.
Jeśli dotyczy: Których modeli urządzeń i wersji systemu operacyjnego to dotyczy?	Zawsze podawaj dokładną wersję systemu operacyjnego (np. iOS 14.7.1 lub Android 11).
Jeśli dotyczy: Jaki jest publiczny adres IP i/lub numer seryjny urządzenia?	Wymień przynajmniej jedno, nawet jeśli dotyczy to wszystkich urządzeń.
Dołącz pliki dziennika	Zaznacz, aby wysłać plik dziennika wraz z raportem o błędzie. Jest to zalecane.
Pobranie aktualnego stanu VPP od Apple i dołączenie do zgłoszenia błędu	Zawiera informacje o przypisaniach licencji VPP. Aktywuj tę opcję tylko wtedy, gdy zostaniesz o to poproszony przez pomoc techniczną lub jeśli Twój problem dotyczy VPP.

Załącznik	Dołącz dowolny plik, który może być przydatny (np. zrzuty ekranu komunikatu o błędzie).

Żądanie funkcji

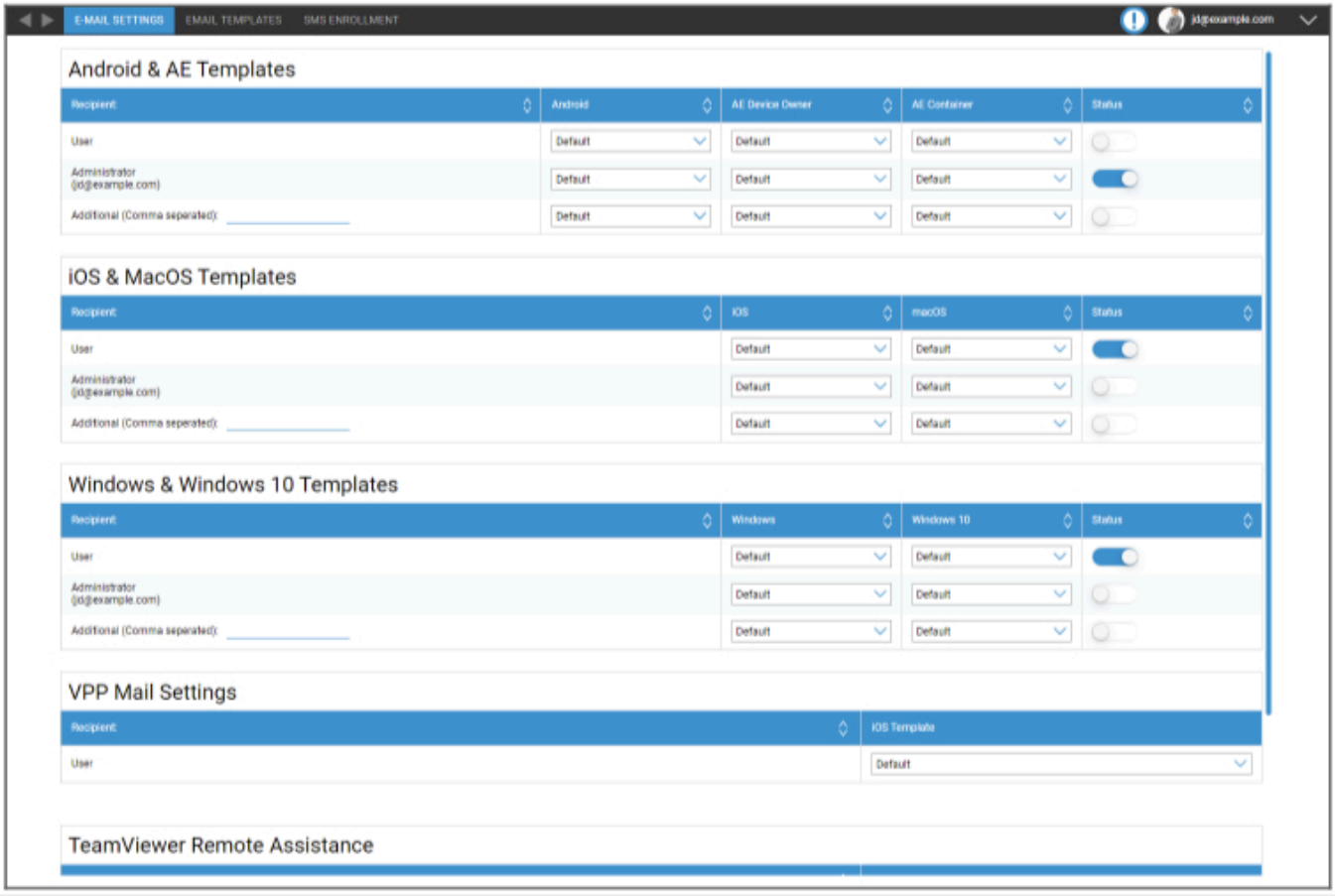
Żądanie funkcji można wysłać bezpośrednio do pomocy technicznej. Może ono zawierać prośbę o konkretną funkcję lub ulepszenie dla

Podsumowanie	Krótkie streszczenie problemu
Opis	Szczegółowy opis problemu, możliwie jak najbardziej konkretny
Załącznik	Dołączanie plików do raportu o błędzie

Konfiguracja globalna

Ustawienia eMail

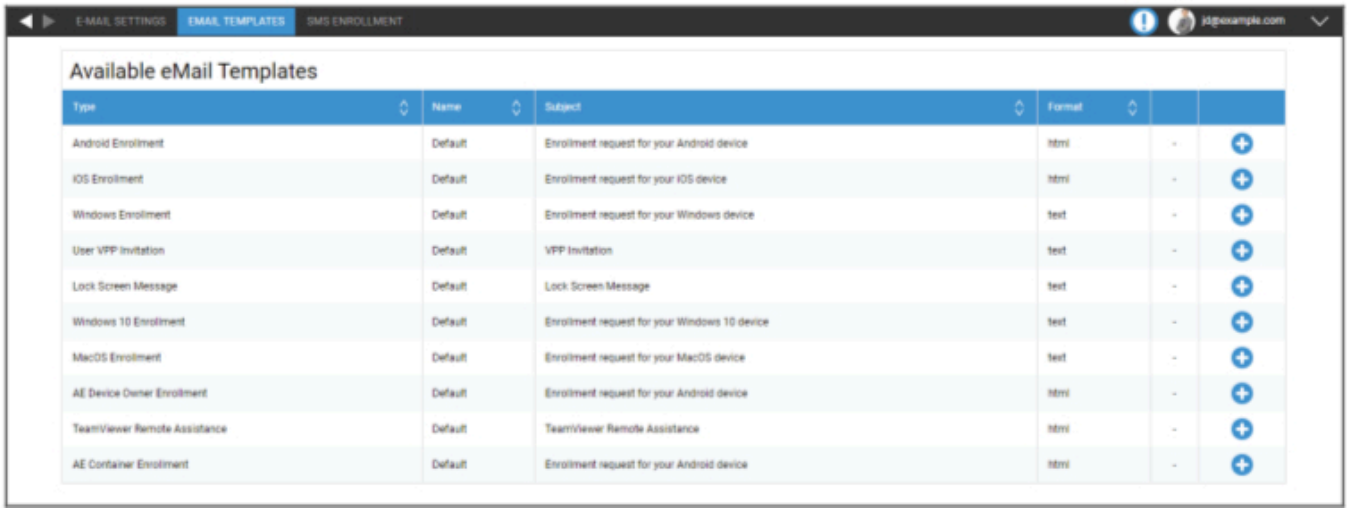
W tym miejscu można zdefiniować, kto otrzyma wiadomość e-mail po wygenerowaniu żądania rejestracji i jaki szablon tekstu zostanie użyty w tej wiadomości.



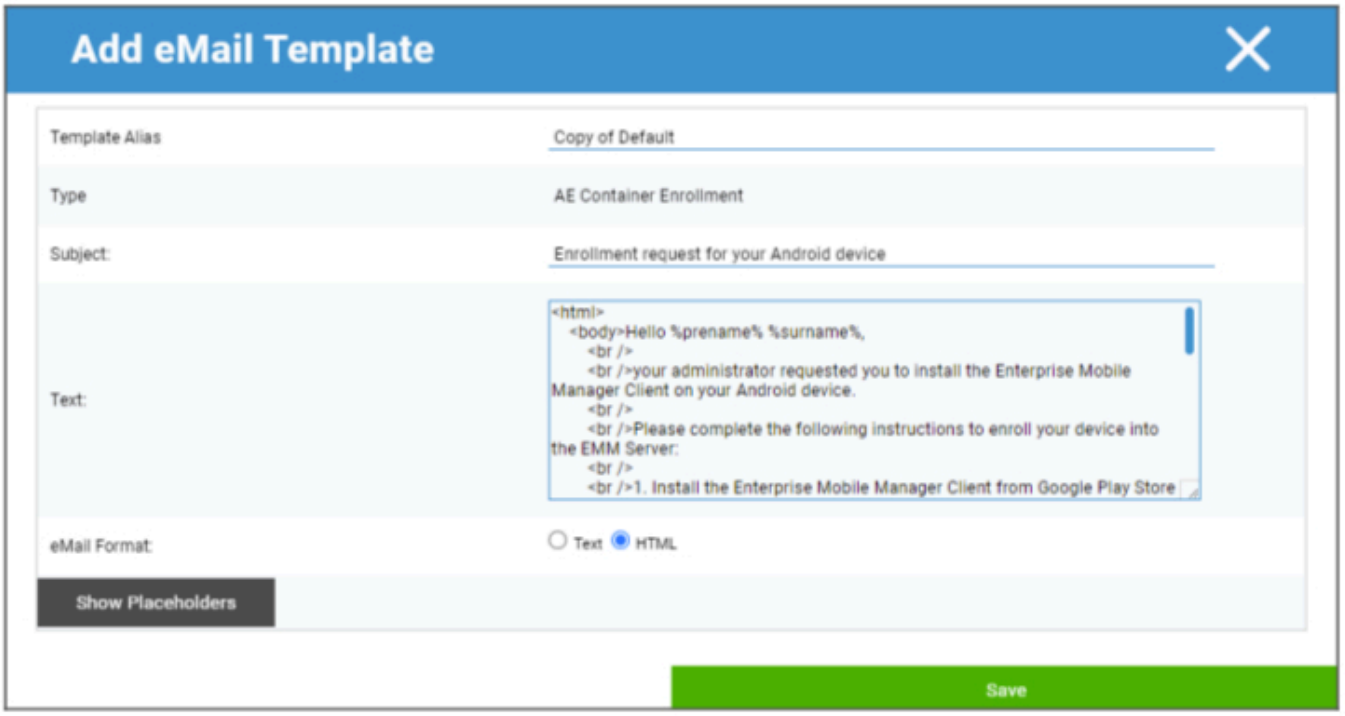
Szablony wiadomości eMail

Tutaj można generować i edytować szablony dla różnych scenariuszy. Mogą one mieć postać zwykłego tekstu lub HTML. W przypadku HTML można lepiej kontrolować formatowanie tekstu.

Domyślnych szablonów nie można edytować ani usuwać.



Można również użyć symboli zastępczych jako zmiennych, które zostaną automatycznie zastąpione. Kliknij "Pokaż symbole zastępcze" podczas edycji, aby zobaczyć dostępne symbole zastępcze. Różne kategorie mają różne symbole zastępcze.



Rejestracja SMS

W tym miejscu można wykonać/aktywować proces rejestracji SMS.

(Domyślnie: wyłączone)

Wyświetli się również informacja, ile kredytów SMS jest jeszcze dostępnych.

Kredyty SMS należy zakupić osobno.

Prywatność

Dostęp GPS

W tym miejscu można zabezpieczyć widok GPS dla każdego urządzenia za pomocą 1 lub 2 haseł (zasada czterech oczu). Przy każdej próbie uzyskania dostępu do lokalizacji urządzenia zostanie wyświetlony monit o wprowadzenie hasła (haseł).

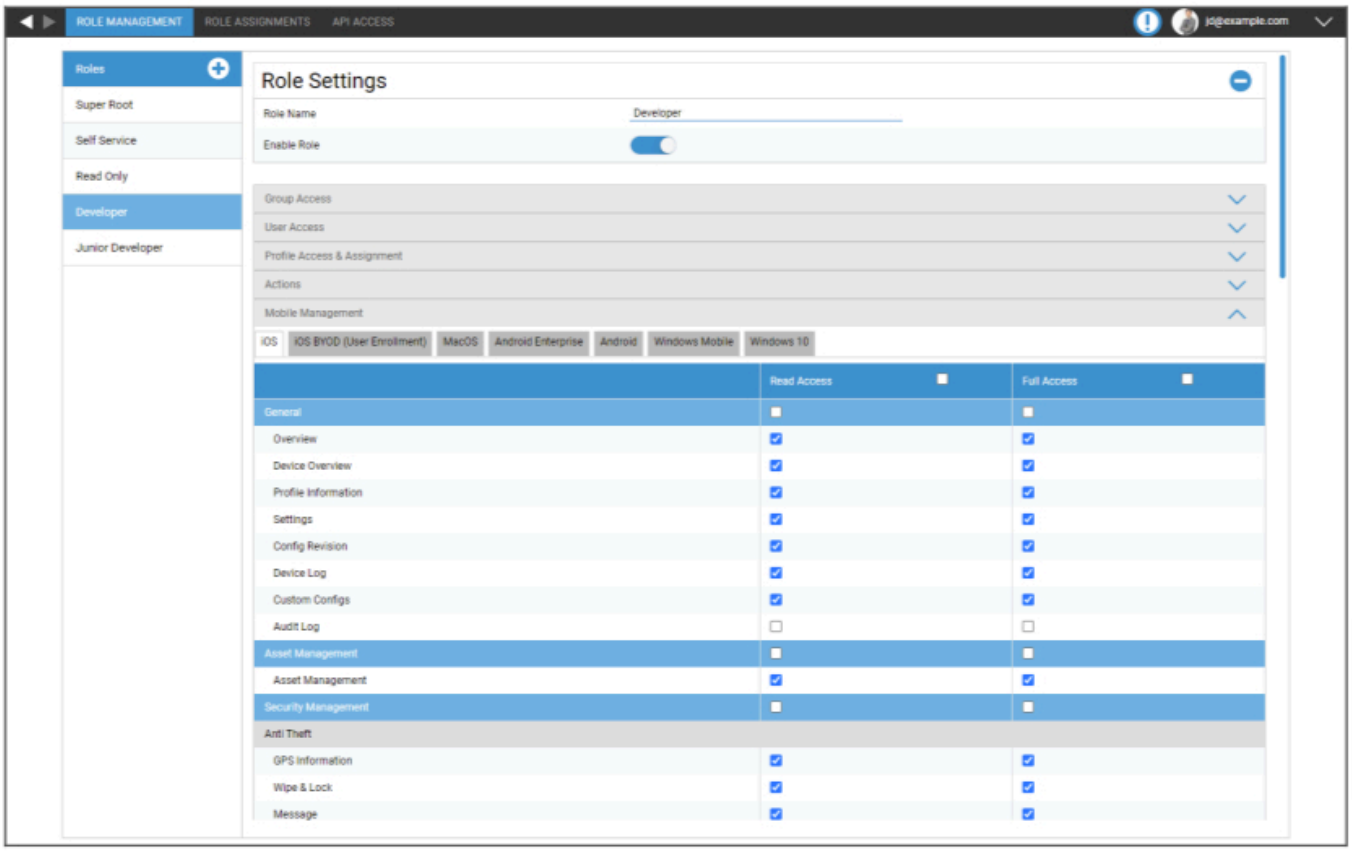
Ograniczenie dostępu do ustawień GPS	Off = funkcja jest wyłączona, a hasło nie jest wymagane do lokalizacji.
	On = funkcja jest włączona, a do lokalizacji wymagane jest hasło.
Metoda ochrony	Użyj jednego hasła = użyj jednego hasła do lokalizacji
	Użyj dwóch haseł = użyj dwóch haseł do lokalizacji
Wprowadź hasło (1)	Wprowadź wybrane hasło
Powtórz hasło (1)	Ponownie wprowadź wybrane hasło
opcjonalnie: Wprowadź hasło 2	Wprowadź drugie wybrane hasło
opcjonalnie: Powtórz hasło 2	Ponownie wprowadź drugie wybrane hasło

Uwaga: Po ustawieniu kodu (kodów) należy wprowadzić go ponownie przed całkowitym włączeniem.

Dostęp oparty na rolach

Zarządzanie rolami

Role definiują, co użytkownik może zobaczyć i zrobić po zalogowaniu się do konsoli zarządzania. Pozwala to na tworzenie użytkowników, którzy mogą się logować, ale mają ograniczoną funkcjonalność.



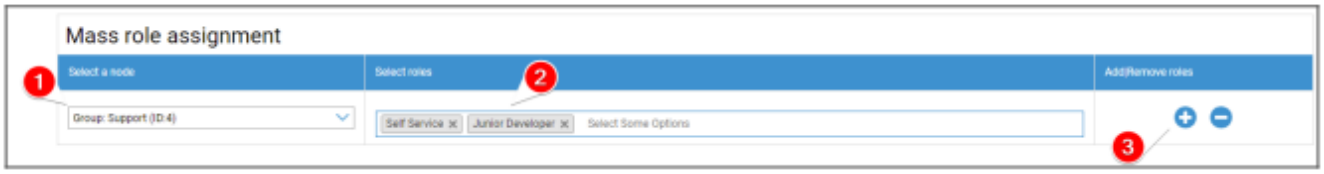
Rola Super Root jest domyślną rolą, która zawsze może widzieć i zmieniać wszystko. Nie można jej zmienić ani usunąć. Rola samoobsługowa może widzieć tylko własnych użytkowników i urządzenia. Można połączyć Self Service i rolę niestandardową, aby np. umożliwić użytkownikom logowanie i rejestrowanie urządzeń samodzielnie i tylko dla ich użytkownika.

Role niestandardowe można ręcznie włączyć lub wyłączyć. Nowe role są domyślnie wyłączone. Użytkownicy z wyłączoną rolą działają tak, jakby jej nie mieli. Pozwala to np. tymczasowo ograniczyć działania danej roli.

Wszystkie uprawnienia są podzielone na "Dostęp do odczytu" i "Pełny dostęp". Przyznanie roli dostępu do odczytu pozwala jej zobaczyć określoną część konsoli. Nadanie im Pełnego dostępu pozwala Roli widzieć i zmieniać określoną część konsoli.

Przypisanie ról

Tutaj można uzyskać przegląd wszystkich użytkowników, którzy mają rolę i zobaczyć, którą z nich mają. Można tu również przypisać rolę do użytkowników lub całych grup:

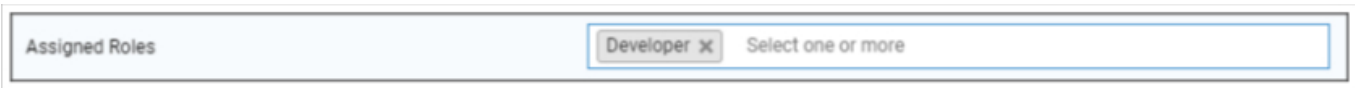


1. Wybierz grupę lub użytkownika, dla którego chcesz dodać lub usunąć role. Można wybrać pojedynczego użytkownika lub grupę. W przypadku wybrania grupy zmiana będzie miała wpływ na wszystkich użytkowników w ramach tej grupy i wszystkich użytkowników podgrup w ramach wybranej grupy.
2. Wybierz rolę, którą chcesz dodać lub usunąć. Możesz wybrać jedną lub wiele ról.
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. Zapisz, aby zakończyć proces. Użytkownicy, którzy wcześniej nie mieli roli i wyłączonej opcji "Can Login", automatycznie otrzymają wiadomość e-mail z linkiem do ustawienia hasła.

Poniżej masowego przypisywania ról znajduje się przegląd przypisanych ról. Można tam również ręcznie zmienić role dla określonych użytkowników.

Przypisanie roli

Aby przypisać rolę do użytkownika, należy przejść do Mobile Management, gdzie znajduje się drzewo grup, użytkowników i urządzeń. Edytuj użytkownika, aby przypisać rolę. Alternatywnie można również użyć powyższej metody tylko dla pojedynczych użytkowników.



Dostęp API

Dostęp do AppTec360 REST API

Interfejs API AppTec360 REST wymaga tokena uwierzytelniającego (klucza API) i klucza prywatnego, które należy wygenerować w konsoli zarządzania.

Aby to zrobić, zaloguj się do AppTec360 EMM i przejdź do

Ustawienia ogólne → Dostęp oparty na rolach → Dostęp API i dodaj nowy klucz.

Musisz wybrać użytkownika, którego uprawnienia będą miały zastosowanie do klucza API.

Klucz prywatny można pobrać tylko raz. Po rozpoczęciu pobierania klucz zostanie usunięty, a przycisk "Pobierz" zniknie.

W przypadku utraty klucza prywatnego należy wygenerować nowy klucz API.

Zasady ogólne

- Interfejs API REST jest dostępny poniżej podstawowego adresu URL:

/public/external/api

- Wszystkie żądania muszą być wysyłane metodą POST.
- Interfejs API REST obsługuje tylko żądania za pośrednictwem protokołu HTTPS.
- Żądania muszą zawierać następujące nagłówki:

Nazwa nagłówka	Wartość nagłówka	Opis
Typ zawartości	application/json	stały
auth	123...xyz	Klucz API z zakładki "Dostęp API"
podpis	Podpis zakodowany w Base64	Podpis ładunku wygenerowanego za pomocą klucz prywatny z zakładki "Dostęp API"

- Treść żądania musi być zakodowanym obiektem json, który musi zawierać następujące wartości:

Pole	Pole Przykład Wartość	Opis
api	v2/device/listdevices	Nazwa interfejsu API
czas	1529662725	Unix Timestamp (UTC) komputera klienckiego. Maksymalna dozwolona różnica czasu między klientem a serwerem wynosi 30 minut.

- W przypadku powodzenia API zwraca żądane dane (patrz Zapytania poniżej) i kod statusu HTTP 200.
- Jeśli wystąpi błąd, kod statusu HTTP będzie wynosił od 4xx do 5xx w zależności od błędu, a obiekt odpowiedzi będzie zawierał tablicę z kluczem "errors", która zawiera listę komunikatów o błędach czytelnych dla człowieka.
- Jeśli nie ma pasujących danych dla urządzenia, zwrócona zostanie pusta tablica.
- Jeśli identyfikator urządzenia nie istnieje, zwrócone dane będą miały wartość null.

Przykład żądania

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]}}

Zapytania

Lista wszystkich urządzeń

Funkcjonalność: Zwraca listę wszystkich urządzeń zawierającą ID urządzenia, IMEI i Serial
API URI: v2/device/listdevices
Parametry obowiązkowe: brak
Parametry opcjonalne: brak

Przykładowa treść żądania


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


Przykładowa treść odpowiedzi


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

Pobierz listę pozycji (GPS)

Funkcjonalność: Zwraca listę wszystkich zapisanych wpisów dziennika pozycji dla identyfikatorów urządzeń
API URI: v2/device/listposition
Parametry obowiązkowe: "ids" - tablica identyfikatorów urządzeń
Parametry opcjonalne: brak

Przykładowa treść żądania


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


Przykładowa treść odpowiedzi


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

Pobierz mapę zasobów

Funkcjonalność:
Zwraca listę wszystkich przechowywanych możliwych zasobów, których można zażądać za pomocą funkcji Get any asset data.
Do żądania danych można użyć formularza czytelnego dla człowieka lub znacznika zasobu.
API URI: v2/device/getassetmap
Parametry obowiązkowe: brak
Parametry opcjonalne: brak

Przykładowa treść żądania

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

Przykładowa treść odpowiedzi

Ta odpowiedź została skrócona dla czytelności.

{
"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": []
}

Pobierz dowolne dane zasobów

Funkcjonalność: Zwraca listę żądanych danych zasobów dla identyfikatorów urządzeń
API URI: v2/device/getassetdata
Parametry obowiązkowe: "ids" - tablica identyfikatorów urządzeń
Parametry opcjonalne:
"assetkeys" - klucze danych zasobów do zwrócenia. Jeśli nie zostaną określone, zwrócone zostaną wszystkie dostępne dane zasobów
. Listę kluczy zasobów można uzyskać za pomocą Get asset map.

Przykładowa treść żądania


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


Przykładowa treść odpowiedzi


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

Przykładowy kod w 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)
```

Konfiguracja Apple

Certyfikat APNS

Tutaj możesz przesłać certyfikat APNS. Jest to wymagane do zarządzania urządzeniami iOS i MacOS.

Uwaga: Certyfikat APNS jest ważny tylko przez rok. Należy go odnowić przed wygaśnięciem. Proces odnowienia jest identyczny z procesem tworzenia (patrz poniżej) i zajmuje tylko kilka minut.

Jeśli zapomnisz odnowić ją na czas, nie będziesz mógł wprowadzać zmian w już zarejestrowanych urządzeniach. **i trzeba ponownie zarejestrować wszystkie urządzenia.**.

Krok 1

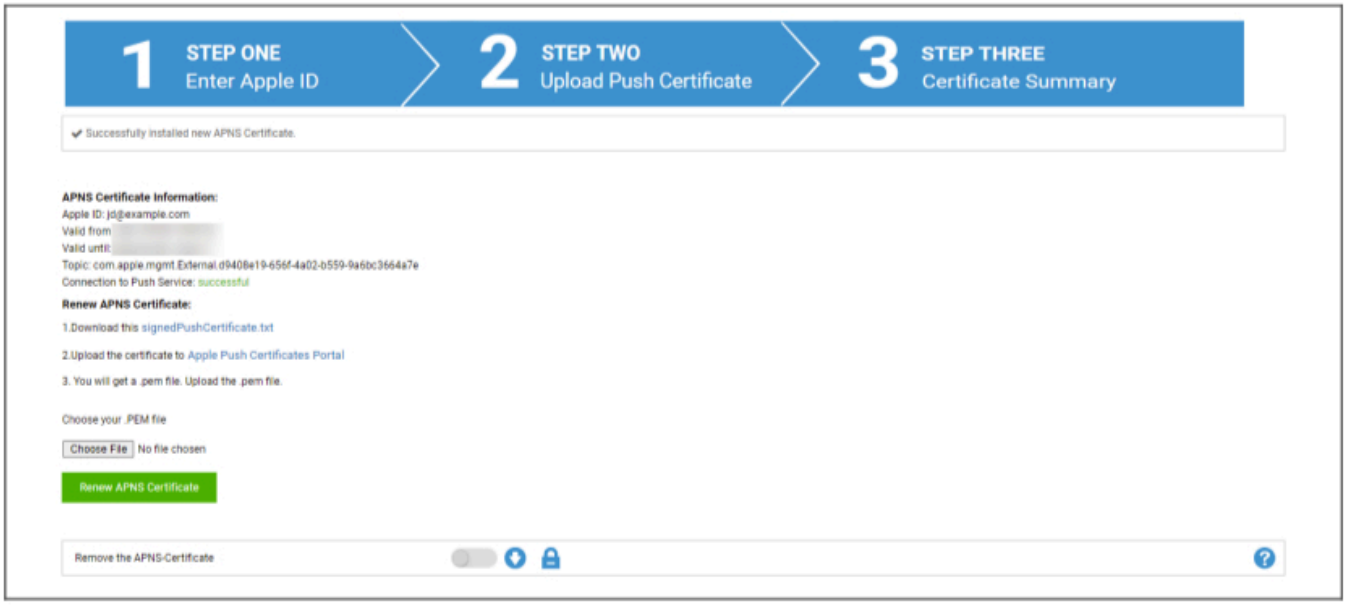
- Najpierw wprowadź swój identyfikator Apple ID, którego chcesz użyć do utworzenia certyfikatu APNS.

Uwaga: Ten Apple ID jest używany tylko do tworzenia certyfikatu APNS. Ten Apple ID nie ma nic wspólnego z urządzeniami i urządzenia nie będą o nim wiedzieć. Ponadto dostęp do tego Apple ID jest również potrzebny do odnowienia certyfikatu APNS. Dlatego zaleca się użycie jakiegoś ogólnego Apple ID i udokumentowanie danych logowania. Przypomnienie jest wysyłane na używany adres e-mail Apple ID przed wygaśnięciem certyfikatu APNS.

- Kliknij "Następny krok", aby kontynuować.
- (opcjonalnie) Można również odzyskać wcześniej usunięty certyfikat APNS, jeśli został on usunięty przez przypadek

Krok 2

- Pobierz plik signedPushCertificate.txt
- Przejdź na stronę https://identity.apple.com/pushcert/ i zaloguj się za pomocą Apple ID z kroku 1.
- Kliknij "Utwórz certyfikat"
- (opcjonalnie) wprowadź notatkę. Może to być pomocne w przypadku zarządzania wieloma najemcami w celu ich łatwej identyfikacji.
- Kliknij "Wybierz plik", aby wybrać wcześniej pobrany plik signedPushCertificate.txt.
- Kliknij przycisk "Prześlij".
- Zostanie wyświetlone potwierdzenie utworzenia certyfikatu APNS.
- Kliknij "Pobierz" i zapisz plik.
- Wróć do konsoli zarządzania.
- Kliknij "Wybierz plik" i wybierz certyfikat APNS, który chcesz przesłać.
- Kliknij "Prześlij"



Krok 3

Pomyślnie skonfigurowałeś certyfikat APNS i możesz teraz zarządzać urządzeniami iOS i MacOS.

W kroku 3 zobaczysz przegląd aktualnie używanego certyfikatu APNS.

Masz również możliwość odnowienia certyfikatu APNS, wykonując czynności pokazane na ekranie. Należy pamiętać, aby odnowić go przed wygaśnięciem.

Podczas odnawiania certyfikatu APNS należy pamiętać o zalogowaniu się za pomocą Apple ID pokazanego w kroku 3, a także o odnowieniu wcześniej używanego certyfikatu, a NIE tworzeniu nowego. Zobaczysz "temat" certyfikatu APNS w kroku 3 i po kliknięciu "i" w portalu Apple Push Certificate Portal. Jest to unikalny identyfikator, który identyfikuje certyfikat. Pomoże to zidentyfikować i odnowić właściwy certyfikat.

Gdy pojawi się komunikat "Błąd: Certyfikat Push ma inny temat!" podczas odnawiania, oznacza to, że odnowiłeś inny certyfikat lub utworzyłeś nowy.

Jeśli chcesz przesłać nowy certyfikat, np. jeśli nie możesz już uzyskać dostępu do poprzednio używanego Apple ID, musisz najpierw usunąć aktualnie przesłany certyfikat.

W każdym razie usunięcie certyfikatu APNS oznacza, że nie można już wprowadzać zmian dla aktualnie zarejestrowanych urządzeń, dopóki nie zarejestrujesz ich ponownie. Upewnij się więc, że jesteś na to przygotowany i usuń certyfikat tylko wtedy, gdy nie ma innego sposobu.

Dostęp zarządzany

W tym miejscu można włączyć rejestrację użytkowników dla urządzeń z systemem iOS i udostępnianie iPada dla urządzeń z systemem iOS.

Rejestracja użytkownika

"Rejestracja użytkownika" włącza specjalny tryb dla urządzeń BYOD.

Dla każdego użytkownika należy utworzyć zarządzany identyfikator Apple-ID w portalu Apple Business Portal.

Podczas procesu rejestracji użytkownicy zostaną poproszeni o podanie swoich danych uwierzytelniających Apple-ID.

"Rejestracja użytkownika" gwarantuje maksymalne bezpieczeństwo użytkownika, ponieważ pozwala na skonfigurowanie przez MDM tylko ograniczonego zestawu ustawień i ograniczeń.

Zarządzana domena:

Domena używana do mapowania adresu e-mail użytkownika na jego zarządzany identyfikator Apple-ID (musi być w formacie: "@appleid.company.com"). Np. john.doe@example.com zostanie zmapowany na john.doe@appleid.company.com.

Sprawdź w Apple Business Manager swoją zarządzaną domenę

Współdzielony iPad

Współdzielony iPad to urządzenie DEP skonfigurowane ze specjalnym profilem DEP.

Umożliwia to wielu użytkownikom logowanie się do urządzenia przy użyciu zarządzanego identyfikatora Apple-ID.

Zarządzany identyfikator Apple-ID musi zostać utworzony w Apple Business Portal lub Apple School Manager.

Użytkownicy, którzy logują się do współdzielonego iPada, są proszeni o podanie swoich zarządzanych poświadczeń Apple-ID.

Zarządzana domena:

Domena używana do mapowania adresu e-mail użytkownika na jego zarządzany identyfikator Apple-ID (musi być w formacie: "@appleid.company.com"). Np. john.doe@example.com zostanie zmapowany na john.doe@appleid.company.com.

Sprawdź w Apple Business Manager swoją zarządzaną domenę

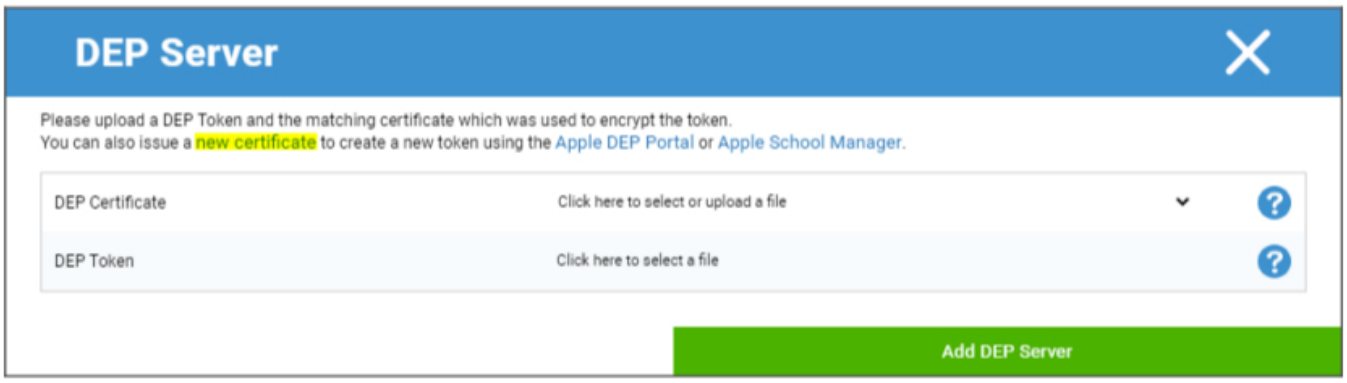
DEP

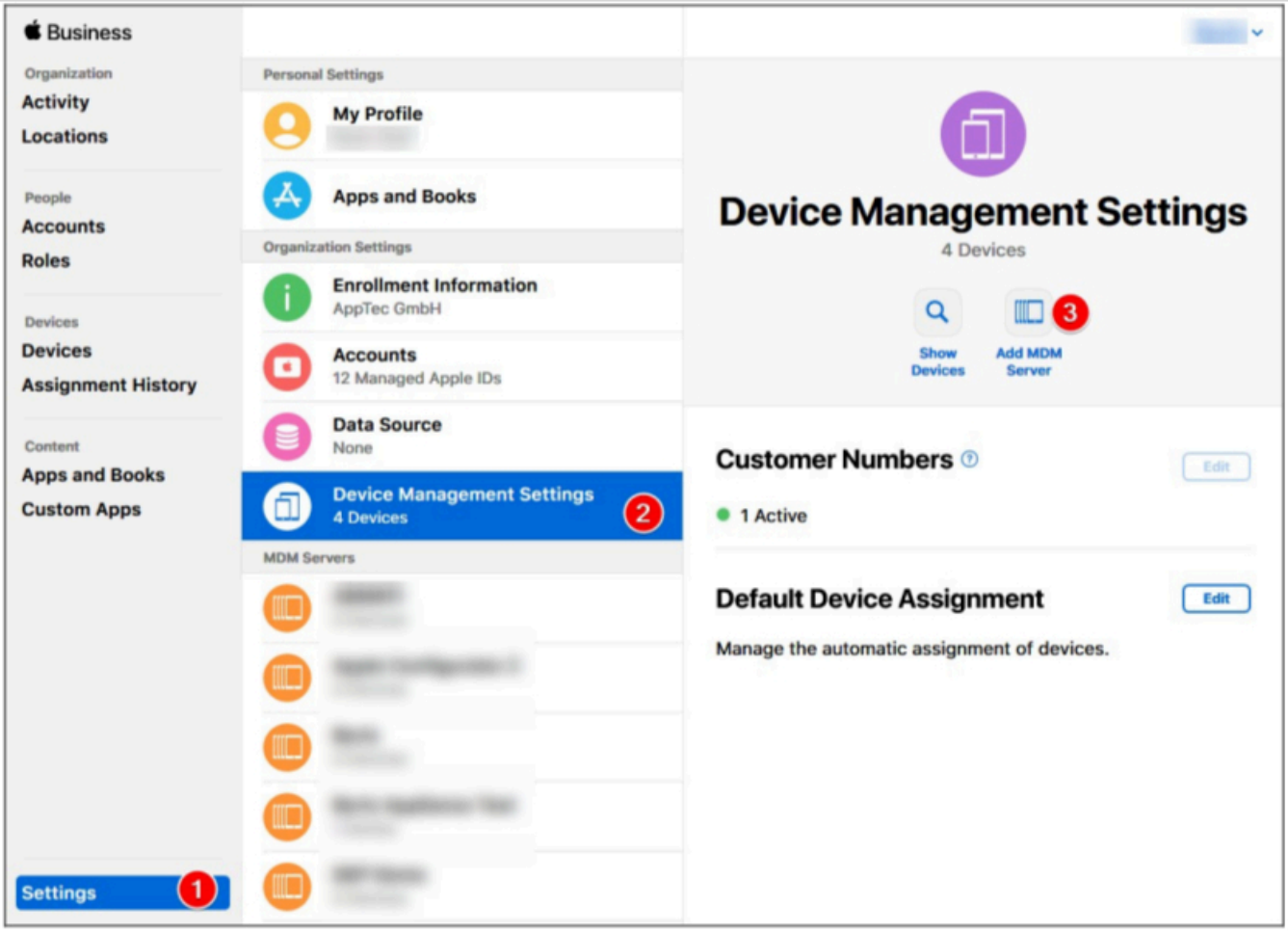
DEP (Device Enrollment Program) umożliwia łatwe rejestrowanie urządzeń w systemie MDM. Podczas korzystania z DEP urządzenia będą automatycznie podłączane do MDM podczas konfigurowania urządzenia. Można również pominąć prawie wszystkie kroki konfiguracji, które są zwykle obowiązkowe w systemie iOS.

Należy pamiętać, że urządzenia należy kupować od sprzedawcy, który obsługuje DEP. Więcej informacji można uzyskać u sprzedawcy lub w firmie Apple.

Więcej informacji o DEP: https://www.apple.com/business/dep/

Kliknij "+", aby dodać token DEP. W wyskakującym okienku kliknij "nowy certyfikat" w tekście (zaznaczony na żółto na poniższym obrazku). Spowoduje to wygenerowanie i pobranie certyfikatu DEP. Następnie przejdź do Apple Business Manager(https://business.apple.com/) lub Apple School Manager(https://school.apple.com/).

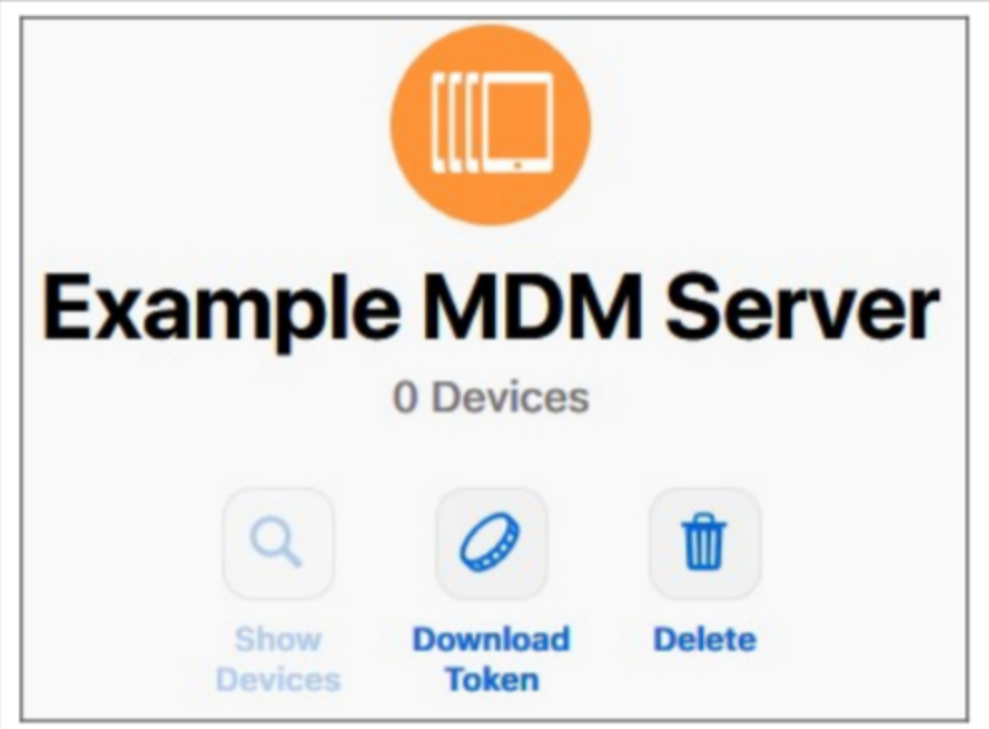




W Apple Business Manager wykonaj kroki pokazane na powyższym obrazku. Ustawienia → Ustawienia zarządzania urządzeniami → Dodaj serwer MDM.

Nadaj serwerowi dowolną nazwę i prześlij wcześniej pobrany certyfikat DEP w Ustawieniach serwera MDM → Prześlij klucz publiczny i kliknij "Zapisz".

Pojawi się teraz opcja "Pobierz token". Kliknij ją i zapisz. Token jest ważny tylko przez 1 rok. Ale ponowne kliknięcie opcji "Pobierz token" spowoduje wydanie nowego tokena, co bardzo ułatwia jego odnowienie.



Możesz teraz wrócić do MDM, gdzie wcześniej pobrałeś certyfikat DEP. Jeśli karta nie została zamknięta, wyskakujące okienko dodawania serwera DEP powinno być nadal otwarte, a certyfikat DEP powinien być już wybrany. Możesz teraz przesłać swój token w polu "DEP Token" i kliknąć DEP Server.

W kolumnie "**Urządzenia**" zostanie wyświetlona liczba urządzeń przypisanych do tego serwera DEP. Urządzenia dodane do tego serwera DEP zostaną automatycznie utworzone w puli DEP w Zarządzaniu urządzeniami mobilnymi.

Możesz kliknąć ten numer, aby uzyskać przegląd wszystkich urządzeń DEP i ich statusu.

Uwaga: W zależności od przepływu pracy lub konfiguracji w Business Manager może być konieczne ręczne przypisanie tych urządzeń do serwera DEP. Można również ustawić domyślny serwer DEP w Apple Business Manager dla nowych urządzeń.

W kolumnie "**Profile**" wyświetlana jest liczba posiadanych profili DEP. Możesz również kliknąć ten numer, aby zobaczyć szczegóły dotyczące profili DEP i możesz tutaj usunąć stare/nieużywane profile. Obecnie nie ma możliwości ich zmiany. Jeśli chcesz dokonać zmiany, musisz utworzyć nowy profil.

W kolumnie "**Ostatnia synchronizacja**" możesz ręcznie zsynchronizować serwer DEP (np. jeśli właśnie dodałeś nowe urządzenie do DEP) i zobaczyć datę ostatniej udanej synchronizacji.

W kolumnie "**Profil automatyczny**" można ustawić profil DEP jako automatyczny profil domyślny. Profil ten będzie automatycznie przypisywany do nowych urządzeń. Jeśli nie ustawisz profilu automatycznego, musisz za każdym razem ręcznie przypisać profil do nowych urządzeń.

W kolumnie "**Dodaj profil**" można dodać nowy profil DEP. Urządzenie otrzyma go na początku konfiguracji. Profil DEP określa, w jaki sposób urządzenie jest konfigurowane i które kroki konfiguracji zostaną pominięte.

Uwaga: po zarejestrowaniu urządzenia ustawienia te można zmienić tylko poprzez przywrócenie ustawień fabrycznych i zarejestrowanie urządzenia z nowym profilem. Jest to szczególnie istotne w przypadku opcji "**Removable**" i "**Allow pairing**". W przypadku opcji "**Zezwalaj na parowanie**" zaleca się jej włączenie, ponieważ można ją wyłączyć za pomocą ograniczeń MDM, ale nie można jej ponownie włączyć, jeśli została wyłączona w profilu DEP.

W kolumnie "**Edytuj**" można przesłać nowy token, np. podczas odnawiania tokena.

Konfigurator i adres URL

Adresy URL rejestracji puli

W tym miejscu można utworzyć adres URL rejestracji i kod QR rejestracji, który jest ważny przez określoną liczbę rejestracji i do określonej daty. Umożliwia to rejestrację wielu urządzeń za pomocą jednego łącza lub kodu QR.

Urządzenia zarejestrowane za pomocą tego adresu URL lub kodu QR znajdą się w puli w Zarządzaniu urządzeniami mobilnymi, a następnie należy ręcznie przypisać je do grupy lub użytkownika.

Uwaga: dotyczy to tylko ręcznej rejestracji. Nie używaj tego adresu URL, jeśli rejestrujesz urządzenia za pomocą Apple Configurator

Profil MDM – konfigurator Apple

Tutaj można uzyskać adres URL potrzebny do rejestrowania urządzeń za pośrednictwem Apple Configurator. Podczas przygotowywania urządzeń za pomocą Apple Configurator można dodać urządzenia do MDM w tym samym procesie. Apple Configurator wymaga w tym celu tego adresu URL.

Urządzenia dodane za pomocą Apple Configurator znajdą się w puli w Zarządzaniu urządzeniami mobilnymi, a następnie należy ręcznie przypisać je do grupy lub użytkownika.

Znajdziesz tu również plik .mobileconfig, który może być użyty do rejestracji urządzeń za pośrednictwem Apple Configurator. W każdym razie zaleca się korzystanie z adresu URL.

Konfiguracja systemu Android

Konfiguracja systemu Android

Odinstaluj ochronę	Jeśli ta funkcja jest włączona, użytkownik nie może dezaktywować administratora urządzenia bez wprowadzenia hasła ustawionego przez administratora MDM. Hasło jest ustawiane podczas rejestracji, więc urządzenia muszą zostać ponownie zarejestrowane, aby zaktualizować hasło. Istnieją dwie opcje usuwania administratorów urządzeń: 1. Ręcznie na urządzeniu ◦ Otwórz aplikację EMM na urządzeniu ◦ Przejdź do karty Status ◦ Stuknij w "Odinstaluj ochronę" ◦ Możesz użyć Revision, aby uzyskać prawidłowe hasło z "Historii haseł" w konsoli. ◦ Przewiń w dół i dotknij nowo dodanego punktu "Dotknij, aby odinstalować aplikację AppTec360 MDM" (masz 20 sekund na wykonanie tego zadania). ◦ Potwierdź okno dialogowe "Uninstall AppTec360 MDM App" przyciskiem "ok". Spowoduje to wyrejestrowanie urządzenia z konsoli. ◦ Aby usunąć aplikację z urządzenia, potwierdź dialog "AppTec360 MDM zostanie odinstalowany" za pomocą "UNINSTALL". 2. automatyczny (konsola) ◦ Wybierz urządzenie w konsoli ◦ Kliknij niebieską ikonę koła zębatego i wybierz "Enterprise Wipe". Uwaga: Dostępne tylko z systemem Android 4.x i niższymi wersjami lub na urządzeniach z interfejsem API KNOX (urządzenia Samsung).

Hasło dezinstalacji (wersja x)	Ustanowione hasło, za pomocą którego użytkownik może usunąć administratora urządzenia. Revision x = licznik, jak często hasło było już zmieniane Ważne jest, jakiego hasła potrzebuje użytkownik, ponieważ możliwe jest, że urządzenie nie skomunikowało się z serwerem AppTec360 i dlatego najnowsze hasło nie zostało jeszcze przesłane.
Historia haseł	Po kliknięciu niebieskiego przycisku ("Pokaż historię") można wyświetlić wcześniej ustalone hasła
Rozszerzona ochrona przed odinstalowaniem	Opcja ta zapewnia ochronę przed urządzeniami innymi niż SAFE Dopóki to ustawienie jest aktywne, nie ma możliwości łatwej dezaktywacji administratora urządzenia
Monitować użytkownika o odinstalowanie zablokowanych aplikacji?	Jeśli to możliwe, zablokowane aplikacje będą nie tylko blokowane, ale także automatycznie odinstalowywane. Jeśli automatyczne odinstalowanie nie jest możliwe, użytkownik zostanie poproszony o odinstalowanie zablokowanych aplikacji.
Inteligentny system blokowania aplikacji	Jeśli włączona jest funkcja Whitelisting, klient Android MDM blokuje wszystkie aplikacje zainstalowane przez użytkownika. Włącz to ustawienie, aby blokować wszystkie uruchamialne aplikacje systemowe w trybie Whitelisting.

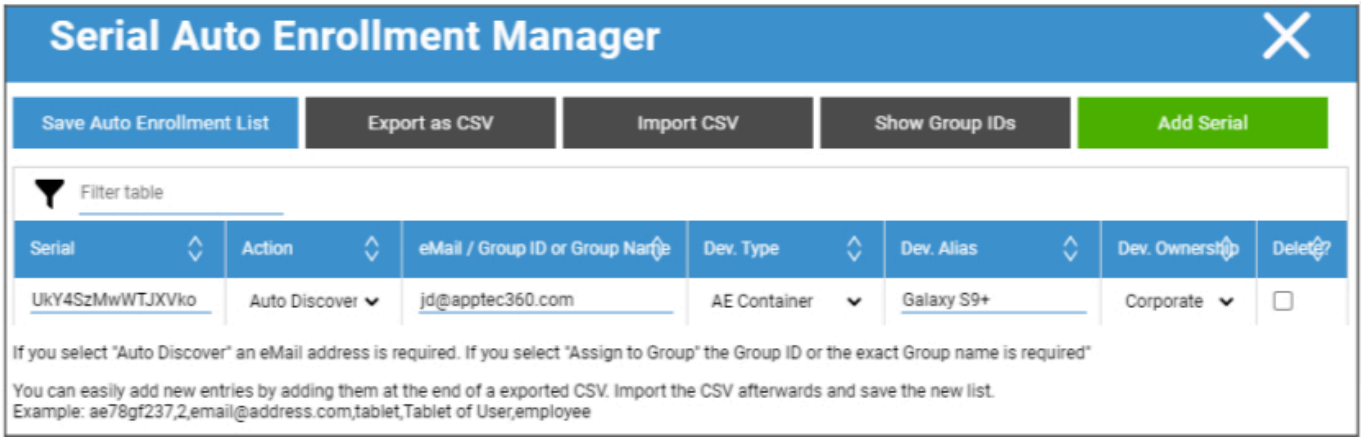
Automatyczna rejestracja

W tym miejscu można włączyć funkcję automatycznej rejestracji, aby rejestrować urządzenia automatycznie po otwarciu klienta AppTec360 MDM na urządzeniu.

Ważne: Ta metoda rejestracji jest przestarzała i nie działa już na systemie Android 10 lub nowszym. W każdym razie podczas korzystania z systemu Android 7 lub nowszego należy zarejestrować urządzenia jako w pełni zarządzane Android Enterprise. Jeśli chcesz korzystać z kontenera Android Enterprise BYOD i korzystasz z systemu Android 10 lub nowszego, musisz ręcznie zarejestrować urządzenie za pomocą poświadczeń, kodu QR lub wiadomości SMS. W każdym razie lista automatycznej rejestracji jest nadal używana do automatyzacji procesu rejestracji, np. rejestracji AE, rejestracji Knox itp.

W każdym razie lista automatycznej rejestracji jest nadal używana do automatyzacji procesu rejestracji, np. rejestracji AE, rejestracji Knox itp.

Klikając na "Serial Manager" lub "IMEI Manager" możesz dodać odpowiednio Serial lub IMEI swoich urządzeń. Nie jest wymagane dodanie obu urządzeń, wystarczy jedno.



Akcja określa, czy urządzenia zostaną zapisane do puli, użytkownika czy grupy.

Możesz także eksportować i importować plik .csv oraz filtrować wpisy według słów kluczowych.

Android Enterprise

Tutaj możesz skonfigurować Android Enterprise. Jest to niezbędne do korzystania ze wszystkich funkcji Android Enterprise.

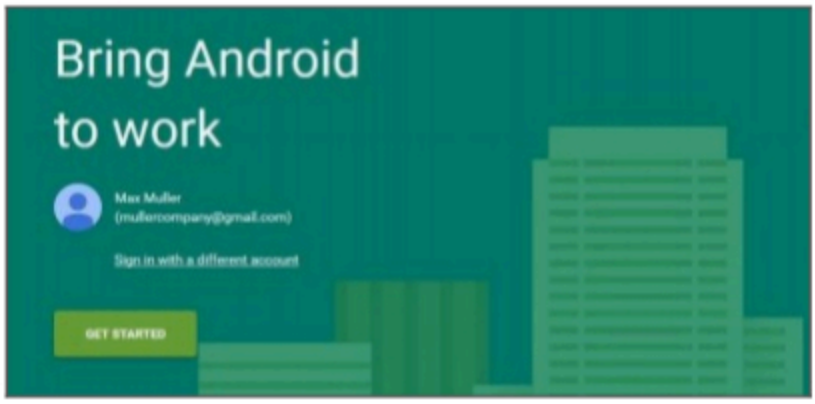
Pierwsza metoda: Konto Android Enterprise (konto Google)

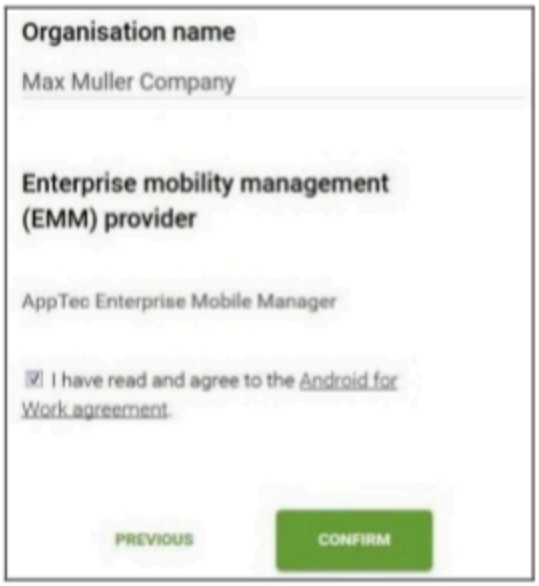
Najpierw należy nacisnąć przycisk "Prepare Setup", a po krótkiej chwili powinien pojawić się przycisk "Start Setup".

Spowoduje to przejście do strony konfiguracji Google Android Enterprise.

Zaloguj się za pomocą konta Google, którego chcesz użyć, jeśli nie jesteś jeszcze zalogowany i naciśnij "Rozpocznij".

Teraz możesz wprowadzić nazwę swojej firmy. Następnie zaznacz pole wyboru i naciśnij "Potwierdź".





W ostatnim kroku możesz zakończyć rejestrację i powinieneś wrócić do konsoli. Jeśli wszystko zadziałało, powinno to wyglądać następująco:

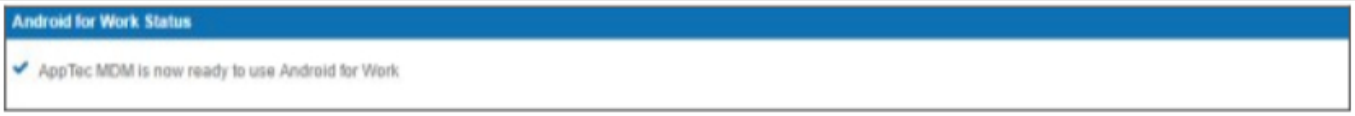
Teraz możesz rozpocząć konfigurację Android Enterprise Container.

Druga metoda: Konto G-Suite

Naciśnij "Użyj G-Suite" i zaloguj się na swoje konto administratora Google. Tam przejdź do "Security" -> "Show more" -> "Manage EMM provider for Android" i wygeneruj Token. Uwaga: Jeśli nie widzisz ustawień Android Enterprise na swoim koncie G-Suite, musisz przejść do "Pobierz więcej aplikacji i usług" i dodać zarządzanie urządzeniami z Androidem. Teraz wprowadź Token i swoją podstawową domenę w naszej konsoli i kliknij "Zapisz zmiany". Po zakończeniu kliknij "Użyj konta Android Enterprise".

Teraz powinieneś zobaczyć przycisk "Utwórz konto usługi". Kliknij go. Proces ten może zająć kilka chwil.

Jeśli wszystko zadziałało, powinno to wyglądać następująco:



Teraz możesz rozpocząć konfigurację Android Enterprise Container.

Ochrona przed przywróceniem ustawień fabrycznych

Dzięki funkcji Factory Reset Protection możesz powiązać swoje urządzenie z wybranym przez siebie kontem Google, co również zastępuje wszelkie istniejące powiązania z kontem Google. Aby skorzystać z funkcji Factory Reset Protection, należy najpierw skonfigurować ją tutaj, a następnie aktywować w swoich profilach.

Aby skonfigurować ochronę przed przywróceniem ustawień fabrycznych, kliknij "FRP Setup" i postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

UWAGA: Uważnie przeczytaj i wykonaj wszystkie kroki. Zalecamy wykonanie tej czynności w nowym oknie przeglądarki incognito, aby uniknąć automatycznego logowania na niewłaściwe konto Google. Możesz całkowicie zablokować sobie dostęp do urządzenia, jeśli wprowadzisz nieprawidłowy identyfikator lub utracisz dostęp do używanego konta Google!

AE Rejestracja

Tutaj można aktywować Android Enterprise Ernollment. Użycie tej metody spowoduje włączenie urządzenia do trybu właściciela urządzenia Android Enterprise. W tym trybie będziesz mieć pełną kontrolę nad urządzeniem.

Włącz rejestrację AE	Aktywuje rejestrację AE Uwaga: Jeśli wyłączysz AE Enrollment, istniejące kody QR i już skonfigurowane urządzenia programatora NFC przestaną działać. Jeśli ponownie włączysz AE Enrollment, będziesz musiał ponownie wysłać konfiguracje NFC push / wygenerować nowe kody QR.
Włącz automatyczne wykrywanie	Gdy urządzenie zarejestruje się poprzez "AE Enrollment", system spróbuje przypisać je do użytkownika na podstawie informacji ustawionych w Serial / IMEI Whitelist ("General Settings" > "Android Configuration" > "Auto Enrollment").
Blokowanie nieznanych urządzeń	Tylko urządzenia, które znajdują się na białej liście Serial / IMEI Whitelist ("Ustawienia ogólne" > "Konfiguracja Androida" > "Automatyczna rejestracja") mogą się zarejestrować.

Uwaga dotycząca metod 1 i 2: "Ekran powitalny" odnosi się do pierwszego ekranu wyświetlanego po przywróceniu ustawień fabrycznych. Może on wyglądać inaczej w zależności od używanej wersji Androida i/lub modelu urządzenia.

Metoda 1: Rejestracja za pomocą kodu QR

(wymaga systemu Android 7.0 lub nowszego) Zalecamy korzystanie z tej metody, jeśli używasz systemu Android 7 lub nowszego.

1. Przywracanie ustawień fabrycznych urządzenia
2. Wygeneruj kod QR dla rejestracji, korzystając z jednej z dwóch poniższych metod:
    - Kliknij w "Ustawienia ogólne -> Konfiguracja Androida -> Rejestracja AE" na "Generuj kod QR". Wybierz, czy chcesz pominąć szyfrowanie pamięci i/lub usunąć wszystkie aplikacje systemowe.
    - (alternatywnie) Wybierz istniejące urządzenie. W "Przeglądzie urządzenia" kliknij wyświetlony tam kod QR. Wybierz, czy chcesz pominąć szyfrowanie pamięci i/lub usunąć wszystkie aplikacje systemowe.
3. Teraz stuknij 6 razy w ekran powitalny urządzenia. Powinno to uruchomić tryb rejestracji QR.
4. Teraz połącz się z siecią bezprzewodową i poczekaj chwilę, aż czytnik kodów QR zostanie zainstalowany
5. Teraz zeskanuj kod QR
6. To wszystko. Twoje urządzenie jest teraz zarejestrowane w Android Enterprise Device Mode.
    - a. Jeśli użyłeś kodu QR w "Ustawieniach ogólnych", możesz znaleźć swoje urządzenie w "Pula -> Urządzenia właściciela urządzenia AE". (Wskazówka: Możliwe, że będziesz

musiał przeładować stronę, aby zobaczyć urządzenia). Jeśli zaznaczyłeś opcję "Enable Auto Discover" (Włącz funkcję automatycznego wykrywania), znajdziesz je w ramach swojego użytkownika Auto Discover.

- Jeśli użyto kodu QR istniejącego profilu urządzenia, urządzenie zostanie zarejestrowane w tym profilu.

Metoda 2: Rejestracja NFC

(wymaga NFC i systemu Android 6.0 lub nowszego)

Przygotowanie: Wprowadź informacje o swoim WiFi w "General Settings -> Android Configuration -> AE Enrollment -> Data for NFC provisioning". Teraz użyj "NFC Device", aby wyszukać urządzenie, które stanie się programatorem. To urządzenie będzie używane do wysyłania informacji o rejestracji do innych urządzeń za pośrednictwem NFC.

1. Przywracanie ustawień fabrycznych urządzenia
2. Otwórz aplikację do parowania NFC z AppTec360 na swoim programatorze
3. Wybierz, czy chcesz pominąć szyfrowanie pamięci i/lub usunąć wszystkie aplikacje systemowe.
4. Przytrzymaj oba urządzenia plecami do siebie
5. Teraz Android Enterprise Enrollment powinien stać się gwiazdą
6. Urządzenie znajduje się teraz w konsoli
    - a. W puli, jeśli nie skonfigurowano automatycznego wykrywania
    - b. W ramach użytkownika skonfigurowanego dla funkcji Auto Discover
    - c. Wskazówka: Możliwe, że będziesz musiał przeładować stronę, aby zobaczyć urządzenia

Metoda 3: Konto Google

(wymaga systemu Android 5.1 lub nowszego)

(Uwaga: Jeśli korzystasz z tej metody, urządzenie nie zostanie zarejestrowane automatycznie. Zamiast tego należy zarejestrować je ręcznie lub zautomatyzować proces za pomocą funkcji automatycznej rejestracji).

1. Przywracanie ustawień fabrycznych urządzenia
2. Przejdź przez kroki konfiguracji, aż będziesz mógł zalogować się za pomocą konta Google.
3. Wprowadź "afw#apptec" jako nazwę użytkownika/adres e-mail
4. Stuknij w "Dalej"
5. Twoje urządzenie jest teraz urządzeniem Android Enterprise

Zapisy KNOX

Tutaj można aktywować KNOX Enrollment i znaleźć informacje potrzebne do utworzenia KNOX Enrollment Profile w KNOX Deployment Portal. Do skonfigurowania i korzystania z tej funkcji potrzebne jest konto w portalu KNOX Deployment Portal.

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

Włącz rejestrację KNOX	Aktywuje rejestrację KNOX. Uwaga: Po wyłączeniu funkcji KNOX Enrollment istniejące profile MDM przestaną działać. Jeśli ponownie włączysz KNOX Enrollment, będziesz musiał zaktualizować pole "Custom JSON Data" w swoim profilu MDM.
Włącz automatyczne wykrywanie	Gdy urządzenie zarejestruje się poprzez "KNOX Enrollment", system spróbuje przypisać je do użytkownika na podstawie informacji ustawionych w Serial / IMEI Whitelist ("General Settings" > "Android Configuration" > "Auto Enrollment").

1. Zaloguj się do portalu Samsung KNOX Mobile Enrollment Portal https://eukme.samsungknox.com/itadmin
2. Przejdź do "Profile MDM"
3. Kliknij "Dodaj"
4. Wybierz "Server URI not required for my MDM" i kliknij "Next".
5. Teraz utwórz profil z informacjami wyświetlanymi w konsoli zarządzania

Teraz ten profil rejestracji KNOX może być bezpośrednio zainstalowany na urządzeniu przez firmę Samsung, jeśli nabędziesz urządzenia bezpośrednio od firmy Samsung.

Alternatywnie można pobrać aplikację KNOX Deployment App, zalogować się za pomocą konta KNOX Deployment Account i wysłać profil KNOX Enrollment Profile za pośrednictwem NFC do innych urządzeń.

Jeśli urządzenie ma zainstalowany profil rejestracji KNOX, pobierze naszą aplikację i zarejestruje urządzenie, jeśli ma działające połączenie internetowe.

Rejestrację urządzeń poprzez KNOX Enrollment można znaleźć w "Pool -> KNOX Enrollment" lub w ramach użytkownika określonego w Auto Discover.

Zero-Touch

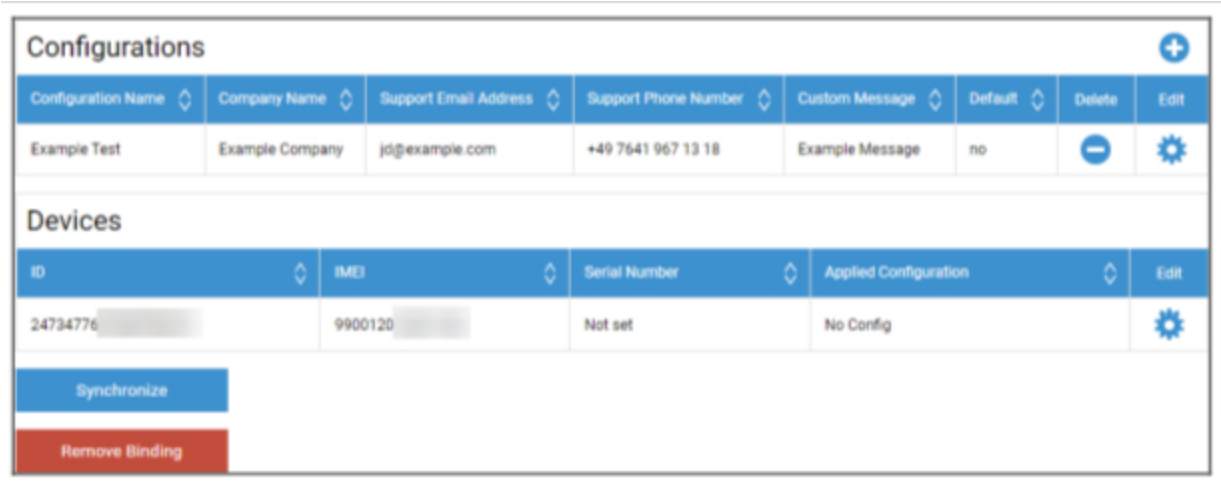
Dzięki Zero-Touch możesz łatwo zarejestrować swoje urządzenia bez konieczności ich dotykania lub konfigurowania czegokolwiek na samym urządzeniu. Wystarczy je włączyć, przejść przez normalną konfigurację, a urządzenie otrzyma wszystkie informacje o tym, jak skonfigurować i połączyć się z MDM całkowicie automatycznie.

Aby korzystać z Zero-Touch, musisz kupić urządzenia od sprzedawcy, który obsługuje Zero-Touch. Ten sam sprzedawca tworzy również konto użytkownika w portalu Zero-Touch. Skontaktuj się ze sprzedawcą, aby uzyskać więcej informacji na temat procedury lub w przypadku problemów z dostępem do portalu Zero-Touch.

Kliknij "Rozpocznij konfigurację", aby rozpocząć konfigurację. Zostaniesz przekierowany na stronę logowania, gdzie musisz wybrać swoje konto Google, które ma dostęp do portalu Zero-Touch.

UWAGA: Możliwe jest wybranie DOWOLNEGO konta. Upewnij się więc, że w tym kroku wybrałeś właściwe konto. Jeśli nie widzisz swoich urządzeń/konfiguracji, najprawdopodobniej użyłeś niewłaściwego konta.

Po zakończeniu logowania będzie on wyglądał następująco:



Kliknij "+", aby dodać Konfigurację i wypełnij pola w sposób przedstawiony na ekranie. Jeśli włączysz konfigurację jako konfigurację domyślną, zostanie ona automatycznie przypisana do nowych urządzeń. Utworzenie lub ustawienie konfiguracji domyślnej nie powoduje przypisania jej do już istniejących urządzeń.

Jeśli urządzenie nie ma przypisanej konfiguracji, zostanie skonfigurowane jako zwykłe urządzenie i nie połączy się z MDM. Dlatego należy upewnić się, że urządzenia mają przypisaną konfigurację.

Po połączeniu konta, urządzenia są widoczne i przypisano do nich konfigurację, można rozpocząć konfigurację urządzeń.

Urządzenia można dodać do listy automatycznego rejestrowania, dzięki czemu będą one automatycznie rejestrowane do określonej grupy lub użytkownika. Jeśli nie skonfigurowano niczego na liście automatycznej rejestracji, urządzenia zostaną zarejestrowane w puli.

Konfiguracja systemu Windows

Konfiguracja systemu Windows

W tym miejscu można włączyć następujące konfiguracje na komputerze z systemem Windows 10:

Natychmiastowe połączenie DM	
Początkowy czas ponawiania próby	Ustanawia pierwszą próbę połączenia z urządzeniem, wartość ta rośnie wykładniczo
Próby połączenia	Wskazuje, ile prób połączenia powinien wykonać klient DM podczas błędu połączenia.
Maksymalny czas uśpienia	Wskazuje maksymalny czas uśpienia po błędzie połączenia.
Pierwsze próby synchronizacji	Odstępy czasu, w których urządzenie ma komunikować się z serwerem po pierwszym połączeniu
Interwał pierwszej próby	Odnosi się do "Pierwszych ponownych prób synchronizacji" Tutaj czasy są podane w minutach Na przykład w polu "First Sync Retries" (Pierwsza próba synchronizacji) podana jest wartość "2", a w polu "First Retry Interval" (Interwał pierwszej próby) podana jest wartość "4 Minutes" (4 minuty), dzięki czemu urządzenie komunikuje się 2 razy co 4 minuty, po pierwszym połączeniu.
Druga próba synchronizacji	Odstępy czasu, w których urządzenie powinno komunikować się z serwerem po zakończeniu "Pierwszych prób synchronizacji".
Drugi interwał ponawiania próby	Ta sama zasada, co w przypadku "Interwału pierwszej próby" - tylko że tutaj dotyczy to "Drugich prób synchronizacji".
Regularne próby synchronizacji	Interwały, jak często urządzenie powinno komunikować się z serwerem w przyszłości Domyślnie: "Nieskończony" Zalecamy, aby nie zmieniać tej wartości, ponieważ jeśli wprowadzisz "10", urządzenie będzie komunikować się z serwerem 10 razy, a następnie przestanie. Dlatego komunikacja z serwerem AppTec360 zostanie przerwana!
Regularny interwał ponawiania prób	Ta sama zasada, co w przypadku "First/Second Retry Interval" - tylko, że tutaj stosuje ustawienia na przyszłość.
Regularny interwał ponawiania prób	Ta sama zasada, co w przypadku "First/Second Retry Interval" - tylko, że tutaj stosuje ustawienia na przyszłość.

ContentBox

Konfiguracja

Tutaj można skonfigurować ContentBox. W ContentBox można umieszczać pliki dla grup, do których można uzyskać dostęp za pomocą aplikacji ContentBox na urządzeniu.

Włącz ContentBox	Włącz ContentBox. Wyłączenie tej opcji, jeśli nie korzystasz z ContentBox, może zaoszczędzić zasoby na komputerach OnPremise.
Użyj zewnętrznej instalacji ContentBox	ContentBox może być również obsługiwany za pomocą własnej chmury Nextcloud.
URL	Pełny adres URL jednostki Nextcloud
Użytkownik root	Użytkownik główny konta Nextcloud
Hasło główne	Hasło główne do konta Nextcloud
Domyślne uprawnienia do folderów grupowych	Domyślne uprawnienia do folderów grupowych, mogą być indywidualnie modyfikowane przez grupę (w Zarządzaniu urządzeniami mobilnymi).
Udostępnianie folderu grupy podgrupom	Jeśli jest aktywna, każda podgrupa może odczytywać wszystkie foldery grupy głównej, można ją również skonfigurować indywidualnie dla każdej grupy (Zarządzanie urządzeniami mobilnymi).
Uprawnienia dla podgrup	Uprawnienia dla podgrup można skonfigurować indywidualnie dla każdej grupy (Mobile Management)
Zezwalaj na udostępnianie	Umożliwia użytkownikowi udostępnianie treści za pośrednictwem linków, które można indywidualnie skonfigurować dla każdej grupy.
Maksymalny rozmiar przesyłanego pliku w MB	Maksymalny rozmiar pliku Standard: 512 MB Maksymalna konfiguracja: 2048
Poświadczenia WebDAV	
Adres URL WebDAV	ContentBox można również otworzyć za pomocą WebDAV. Pod żadnym pozorem nie usuwaj następujących folderów: /apptecgroups /apptecgroups/AppTecGroup-X
Użytkownik root	Nazwa użytkowników głównych
Hasło	Hasło użytkowników głównych

Synchronizacja z ContentBox odbywa się automatycznie. Można jednak wykonać ręczną synchronizację za pomocą opcji "Synchronizuj ContentBox".

Dodatkowo można tutaj aktywować/dezaktywować ContentBox na każdym urządzeniu.

Jest to istotne tylko wtedy, gdy nie posiadasz dodatkowej licencji ContentBox, wtedy nadal masz dostęp do 25 urządzeń, na których możesz przetestować ContentBox - tutaj możesz aktywować to dla odpowiednich urządzeń.

Konfiguracja LDAP

Przegląd protokołu LDAP

W tym miejscu można nawiązać połączenie z usługą Active Directory za pośrednictwem protokołu LDAP w celu masowego importowania użytkowników i grup. Synchronizacja musi być wykonana ręcznie. Można skonfigurować wiele połączeń LDAP do różnych systemów lub z różnymi konfiguracjami/filtrami.

Nazwa serwera	Wyświetlana nazwa serwera
Typ	Obecnie obsługiwane są tylko katalogi aktywne obsługujące protokół LDAP
Domena LDAP	Podstawowa domena LDAP (np. example.com)
Host LDAP	Konieczne tylko wtedy, gdy host LDAP nie jest osiągalny w danej domenie LDAP.
Port	Pozostaw puste, aby użyć standardowego portu (389 lub 636 dla SSL).
Nazwa użytkownika	Np. CN=John,OU=Users,DC=EXAMPLE,DC=COM Uwaga: Większość systemów wymaga nazwy użytkownika w tym formacie i nie akceptuje "John" jako nazwy użytkownika.
Hasło	
Potwierdź hasło	
Bezpieczeństwo połączeń	Uwaga: w przypadku korzystania z protokołu SSL lub TLS zostanie sprawdzony certyfikat usługi Active Directory. Jeśli jest on podpisany samodzielnie, należy dodać główny urząd certyfikacji do magazynu zaufania maszyny OnPremise. Jeśli korzystasz z chmury, Active Directory musi zapewnić zaufany certyfikat, w przeciwnym razie połączenie będzie działać tylko bez szyfrowania.
Automatyczna synchronizacja.	Włącza automatyczną synchronizację katalogu LDAP w przedziale czasu określonym w ogólnych ustawieniach LDAP.
Bazowy DN	Jeśli nie chcesz synchronizować całego katalogu, możesz określić tutaj jednostkę organizacyjną, np. OU=AndroidUsers,OU=Users,DC=EXAMPLE,DC=COM
Członek	Wszyscy zaimportowani użytkownicy zostaną dodani do wybranej grupy.
Tylko aktywowani użytkownicy?	Po włączeniu, atrybut userAccountControl będzie brany pod uwagę, użytkownicy bez tego atrybutu nie będą importowani.
Filtr LDAP	Za pomocą filtra LDAP można filtrować, którzy użytkownicy zostaną zaimportowani

Filtr Regex	Możesz użyć filtra Regex, aby filtrować, którzy użytkownicy zostaną zaimportowani
Połączenie testowe	Testuje połączenie podczas zapisywania konfiguracji
Zresetować strukturę katalogów podczas synchronizacji?	Jeśli to prawda, wszystkie wpisy LDAP zostaną przeniesione z powrotem do ich pierwotnej lokalizacji w drzewie LDAP. Zalecane włączenie.
Ponownie zaimportować usuniętych użytkowników i grupy?	Po włączeniu tej opcji usunięci użytkownicy i grupy zostaną ponownie utworzeni. Zalecane włączenie.
Usuwanie synchronizacji?	Po włączeniu tej opcji grupy i użytkownicy będą usuwani, gdy zostaną usunięci z serwera LDAP. Usunięte zostaną również urządzenia usuniętych użytkowników.

Poniżej listy konfiguracji LDAP można zdefiniować okres, w którym system będzie synchronizowany automatycznie. Do automatycznej synchronizacji używane są tylko te konfiguracje LDAP, w których aktywowano odpowiednią opcję.

Zarządzanie aplikacjami

Wewnętrzny DB aplikacji

Android

W tym miejscu można przesyłać aplikacje na Androida opracowane przez firmę i dystrybuować je później w usłudze Mobile Management w profilach urządzeń lub grup.

Należy pamiętać, że radzimy dystrybuować w ten sposób tylko aplikacje, które nie są dostępne w sklepie Google Play.

Kliknij "+", aby przesłać plik APK aplikacji, którą chcesz przesłać. Obecnie obsługiwany jest tylko format APK.

Limit przesyłania w urządzeniach OnPremise można zwiększyć w kroku 3 konfiguracji urządzenia. Jeśli chcesz zwiększyć limit przesyłania w chmurze, skontaktuj się z pomocą techniczną, aby uzyskać więcej informacji.

Należy pamiętać, że zazwyczaj pliki APK są nieco mniejsze niż ich zawartość. Może się zdarzyć, że przesyłanie nie powiedzie się z tego powodu, ponieważ plik APK jest rozpakowywany w trakcie procesu. Np. możliwe jest, że plik APK o rozmiarze 95 MB nie powiedzie się przy limicie przesyłania 100 MB. W takim przypadku należy zwiększyć limit przesyłania, jak wspomniano powyżej.

Radzimy również najpierw ręcznie przenieść plik APK na jedno urządzenie testowe (np. przez USB) i spróbować zainstalować go ręcznie za pomocą aplikacji Pliki na urządzeniu. Jeśli to nie zadziała z jakiegokolwiek powodu, nie powiedzie się również za pośrednictwem MDM.

Cel aktualizacji

Za pomocą funkcji "Cel aktualizacji" można wybrać, która wersja aplikacji powinna zostać zainstalowana lub do której wersji aplikacja powinna zostać zaktualizowana, jeśli aktywowano opcję "Aktualizuj" dla aplikacji.

Jeśli nie wybrano celu aktualizacji, użyta zostanie najwyższa wersja.

Należy pamiętać, że Android nie może obniżać wersji aplikacji. Należy również pamiętać, że "Kod wersji" określa, czy wersja jest wyższa, niższa lub taka sama. Upewnij się więc, że poprawnie zwiększyłeś tę wersję w swojej aplikacji podczas tworzenia aktualizacji.

iOS

W tym miejscu można przesyłać opracowane aplikacje iOS i dystrybuować je później w aplikacji Mobile Management w profilu urządzenia lub grupy.

Kliknij "+", aby przesłać IPA aplikacji, którą chcesz przesłać. Obecnie obsługiwany jest tylko format IPA.

Limit przesyłania w urządzeniach OnPremise można zwiększyć w kroku 3 konfiguracji urządzenia. Jeśli chcesz zwiększyć limit przesyłania w chmurze, skontaktuj się z pomocą techniczną, aby uzyskać więcej informacji.

Cel aktualizacji

Za pomocą funkcji "Cel aktualizacji" można wybrać, która wersja aplikacji powinna zostać zainstalowana lub do której wersji aplikacja powinna zostać zaktualizowana, jeśli aktywowano opcję "Aktualizuj" dla aplikacji.

Jeśli nie wybrano celu aktualizacji, użyta zostanie najwyższa wersja.

macOS

W tym miejscu można przesyłać opracowane aplikacje MacOS i dystrybuować je później w aplikacji Mobile Management w profilu urządzenia lub grupy.

Kliknij "+", aby przesłać PKG aplikacji, którą chcesz przesłać. Obecnie obsługiwany jest tylko format PKG.

Limit przesyłania w urządzeniach OnPremise można zwiększyć w kroku 3 konfiguracji urządzenia. Jeśli chcesz zwiększyć limit przesyłania w chmurze, skontaktuj się z pomocą techniczną, aby uzyskać więcej informacji.

Cel aktualizacji

Za pomocą funkcji "Update Target" można wybrać, która wersja aplikacji powinna zostać zainstalowana lub do której wersji aplikacja powinna zostać zaktualizowana, jeśli aktywowano opcję "Keep up to date" dla aplikacji.

Jeśli nie wybrano celu aktualizacji, użyta zostanie najwyższa wersja.

Windows 10

W tym miejscu można przesyłać aplikacje Windows 10 i dystrybuować je później w aplikacji Zarządzanie urządzeniami mobilnymi w profilu urządzenia lub grupy.

Kliknij "+", aby przesłać APPX, APPXBUNDLE lub MSI aplikacji, którą chcesz przesłać. Obecnie obsługiwany jest tylko format APPX, APPXBUNDLE lub MSI.

Można również przesyłać i definiować zależności dla aplikacji, które będą automatycznie dystrybuowane i instalowane przed zainstalowaniem żądanej aplikacji.

Limit przesyłania w urządzeniach OnPremise można zwiększyć w kroku 3 konfiguracji urządzenia. Jeśli chcesz zwiększyć limit przesyłania w chmurze, skontaktuj się z pomocą techniczną, aby uzyskać więcej informacji.

Cel aktualizacji

Za pomocą funkcji "Update Target" można wybrać, która wersja aplikacji powinna zostać zainstalowana lub do której wersji aplikacja powinna zostać zaktualizowana, jeśli aktywowano opcję "Keep up to date" dla aplikacji.

Jeśli nie wybrano celu aktualizacji, użyta zostanie najwyższa wersja.

Pakiet Win32 (.exe)

Możesz także dystrybuować pliki .exe/instalatory na swoje urządzenia.

Nazwa pakietu	Nazwa, która będzie wyświetlana w MDM
Opis	Opis wyświetlany w MDM
Plik pakietu	Dozwolone są tylko pliki .zip. Umieść pliki, które chcesz wdrożyć w tym pliku zip.
Kontekst wdrożenia	**System**: Polecenie instalacji jest uruchamiane z uprawnieniami systemowymi, czyli wyższymi niż "Użytkownik". Ponadto, gdy używany jest "System", proces nie ma interfejsu użytkownika, więc będzie cichy, a profil użytkownika, np. zmienne środowiskowe, takie jak %AppDat%, nie są dostępne. **Użytkownik**: Polecenie instalacji ma dostęp do profilu użytkownika i w razie potrzeby może wyświetlić interfejs użytkownika. Uwaga: Niektóre procesy mogą działać tylko w jednym kontekście. Np. jeśli oprogramowanie instaluje się w AppData, będzie działać tylko po wybraniu "Użytkownik"
Polecenie instalacji	Polecenie używane do instalacji programu. Na przykład polecenie instalacji dla pliku zip zawierającego "setup.exe" w jego katalogu głównym, który obsługuje parametr "/s" dla cichej instalacji, polecenie instalacji brzmiałoby "setup.exe /s". Należy pamiętać, że różne programy mogą mieć różne parametry.
Polecenie odinstalowania	Polecenie do uruchomienia w celu odinstalowania oprogramowania przez MDM. Zwykle wskazuje na deinstalator. Na przykład "C:\Program Files\ExampleSoftware\uninstall.exe".
Wymagania	
Uwaga: Aby oprogramowanie zostało zainstalowane, muszą zostać spełnione wszystkie określone wymagania. W przeciwnym razie nie zostanie ono zainstalowane. Niektóre pola mogą być obowiązkowe. Jeśli dla danego wymagania nie zostanie ustawiona żadna wartość, zostanie ono zignorowane.	
Architektura systemu operacyjnego	Architektura systemu operacyjnego
Minimalna wersja systemu operacyjnego	Minimalna wersja systemu operacyjnego
Minimalna ilość wolnego miejsca na dysku (MB)	Minimalna ilość wolnego miejsca na dysku (MB)
Min. pamięć fizyczna (MB)	Min. pamięć fizyczna (MB)

Minimalna liczba procesorów logicznych	Minimalna liczba procesorów logicznych
Minimalna szybkość procesora (MHz)	Minimalna szybkość procesora (MHz)
Dodatkowe wymagania	Możesz także ręcznie zdefiniować reguły lub przesłać tutaj skrypt, aby przeprowadzić dodatkowe kontrole wymagań, jeśli chcesz.
Zasady wykrywania	
Metoda wykrywania	Tutaj można zdefiniować sposób wykrywania, czy aplikacja jest zainstalowana na urządzeniu. Polecenia instalacji będą uruchamiane tylko wtedy, gdy te reguły wykryją, że aplikacja NIE jest zainstalowana. Polecenia odinstalowania będą uruchamiane tylko wtedy, gdy te reguły wykryją, że aplikacja nie jest zainstalowana. **Ręcznie z**definiuj **reguły**: Umożliwia ręczne zdefiniowanie jednej lub więcej reguł w celu sprawdzenia na przykład obecności określonego pliku, folderu, MSI lub klucza rejestru. Jeśli wszystkie podane reguły wykrywania są prawdziwe, aplikacja zostanie uznana za obecną. **Użyj skryptu**: Prześlij własny skrypt z własnymi kontrolami. Jeśli skrypt zwróci "$TRUE", aplikacja zostanie uznana za obecną.
Zasady wykrywania	

Ustawienia aplikacji

Ustawienia aplikacji iOS

W tym miejscu można zdefiniować domyślne ustawienia dodawania aplikacji do sklepu z aplikacjami obowiązkowymi lub sklepu z aplikacjami dla przedsiębiorstw.

Uwaga: Ustawia to tylko to, co jest domyślnie wybrane podczas dodawania aplikacji. NIE zmienia to istniejących ustawień dla aplikacji, które zostały już dodane w obowiązkowych aplikacjach lub sklepie z aplikacjami dla przedsiębiorstw.

Bądź na bieżąco	Automatycznie aktualizuje aplikację. Należy pamiętać, że aktualizacja aplikacji może potrwać do 7 dni od wydania aktualizacji.
Wyprzedzanie, gdy nie jest zarządzane	Jeśli aplikacja jest już zainstalowana jako niezarządzana (przez użytkownika), zostanie ona przejęta i będzie zarządzana przez MDM.
Usuń aplikację po usunięciu profilu MDM	Odinstalowuje aplikację po usunięciu MDM.
Zapobieganie tworzeniu kopii zapasowych danych aplikacji	Zapobiega tworzeniu kopii zapasowych danych aplikacji.

Ustawienia aplikacji na Androida

W tym miejscu można zdefiniować domyślne ustawienia dodawania aplikacji do sklepu z aplikacjami obowiązkowymi lub sklepu z aplikacjami dla przedsiębiorstw.

Uwaga: Ustawia to tylko to, co jest domyślnie wybrane podczas dodawania. NIE zmienia to ustawień aplikacji, które zostały już dodane w obowiązkowych aplikacjach lub sklepie z aplikacjami dla przedsiębiorstw.

Bądź na bieżąco	Automatycznie aktualizuje aplikację. Dostępne tylko dla aplikacji InHouse.
Aktualizacja klienta kontrolowanego AppTec360 EMM	Jeśli jest włączona, administratorzy mogą określić cel aktualizacji dla AppTec360 EMM Client. Lista wszystkich dostępnych wersji AppTec360 EMM Client zostanie wyświetlona w "Ustawieniach ogólnych" → "Zarządzanie aplikacjami" → "Wewnętrzna baza aplikacji" → "Android".

Aplikacje innych firm

Android

Tutaj możesz ustawić swój kod aktywacyjny dla Ikarus.

Ustaw tę opcję na "Użyj kodu aktywacyjnego" i wprowadź tutaj swój kod aktywacyjny.

Uwaga: Po wprowadzeniu i zapisaniu kodu nie zostanie on jeszcze dodany do profilu wysyłanego do urządzenia. Aby kod został dodany do profilu, należy dokonać dowolnej zmiany w profilu. Np. zmienić dowolny przełącznik w profilu z off → on → off - Save → Assign now.

iOS

Tutaj możesz wprowadzić swoją licencję SecurePIM. Po wprowadzeniu licencji naciśnij "Zapisz zmiany" i możesz korzystać z opcji SecurePIM.

VPP / KNOX Premium

Apples Volume Purchase Program (VPP) umożliwia łatwą dystrybucję płatnych i bezpłatnych aplikacji na urządzenia. Jest to wysoce zalecane, ponieważ nie potrzebujesz Apple ID na urządzeniach, użytkownicy nie muszą potwierdzać instalacji (nadzorowanej), użytkownicy nie będą musieli wprowadzać hasła Apple ID i możesz łatwo dystrybuować płatne aplikacje bez kupowania ich ponownie na każdym urządzeniu.

Aby korzystać z VPP należy zarejestrować się w Apple Business Manager.

Licencje VPP

W tym miejscu można uzyskać przegląd posiadanych aplikacji VPP, liczby używanych i dostępnych licencji.

Kliknięcie kółka pozwala zobaczyć, które urządzenia mają przypisaną licencję i jaki jest status tego przypisania.

Kliknięcie przycisku odświeża pamięć podręczną VPP, która porównuje licencje przypisane w MDM z licencjami przypisanymi po stronie Apple. W niektórych przypadkach może to rozwiązać problemy z licencjami.

Token VPP

Tutaj możesz przesłać swój token VPP, który można znaleźć w Apple Business Manager w Ustawienia → Aplikacje i książki. Możesz przesłać wiele tokenów VPP.

Token można odnowić, po prostu pobierając nowy w Apple Business Manager, klikając kółko "Edytuj" i przesyłając nowy.

"Tryb VPP" decyduje o sposobie obsługi przypisania licencji. W zależności od scenariusza należy użyć różnych trybów:

"Device based" musi być używane podczas rejestrowania urządzeń za pomocą kodu QR, łącza, Apple Configurator lub DEP.

"User based" jest wymagane, jeśli urządzenia są zarejestrowane z User Enrollment lub jako Shared iPad.

Po włączeniu opcji "Automatyczne zarządzanie licencjami" użytkownicy przenoszeni z jednej grupy do drugiej będą automatycznie przypisywani do licencji Apple VPP na podstawie profilu grupy, do której zostali przeniesieni.

Istniejące licencje Apple VPP z grupy, z której zostali przeniesieni, nie zostaną cofnięte.

Nowi użytkownicy dodani do grupy zostaną automatycznie przypisani do licencji Apple VPP w oparciu o odpowiedni profil grupy.

Klucz KNOX Premium

W tym miejscu można wprowadzić klucz KNOX Premium, aby korzystać z kontenera Samsung KNOX.

Należy pamiętać, że nie jest to już obsługiwane od Androida 10. Zamiast tego należy użyć Android Enterprise Container.

Ustawienia App Store

Region i język

W tym miejscu można ustawić domyślny język i region wyszukiwania aplikacji w aplikacji Zarządzanie aplikacjami.

Należy pamiętać, że ustawienia iTunes określają również sposób, w jaki system pobiera informacje o niektórych aplikacjach. Jeśli napotkasz aplikacje na swoich listach, które są wyświetlane w dziwny sposób (np. brak ikony), być może ustawiłeś region, w którym dana aplikacja nie jest dostępna.

Sklep AE Play

Tutaj można znaleźć wszystkie opcje Sklepu Play dla urządzeń Android Enterprise, aby zatwierdzać aplikacje, przesyłać własne aplikacje do Sklepu Play lub tworzyć własne aplikacje internetowe.

Zatwierdzone aplikacje

Tutaj można uzyskać przegląd wszystkich zatwierdzonych aplikacji.

Aplikacje ze Sklepu Play

Spowoduje to załadowanie ramki iFrame pokazującej Sklep Play. Wyszukaj dowolną aplikację, kliknij ją i zatwierdź. Podczas zatwierdzania aplikacji można również zdefiniować, że zatwierdzenie zostanie cofnięte, jeśli wymagane uprawnienia ulegną zmianie. Zalecamy pozostawienie tych ustawień domyślnych podczas zatwierdzania aplikacji.

Po zatwierdzeniu aplikacji można dodać ją do swoich profili.

Przycisk "Zatwierdź" zmieni się na "Cofnij zatwierdzenie" po zatwierdzeniu, więc zawsze możesz usunąć aplikacje, jeśli już ich nie potrzebujesz.

Aplikacje prywatne

Tutaj możesz przesłać własną aplikację jako aplikację prywatną do Sklepu Google Play. Pozwala to na dystrybucję aplikacji za pośrednictwem usług Google i aktualizowanie jej za ich pośrednictwem. Ma to

również tę zaletę, że własne aplikacje mogą być instalowane bez potwierdzenia użytkownika, które zwykle jest konieczne.

Aplikacje internetowe

Tutaj można tworzyć aplikacje internetowe, które są linkami do określonych stron internetowych, które można przypisać jak aplikacje.

Możesz również nadać tej ikonie niestandardową ikonę i dodatkowo zdefiniować sposób jej wyświetlania.

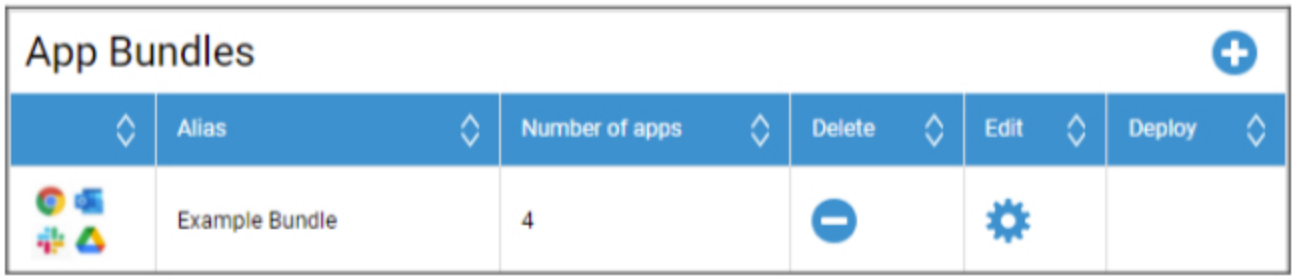
Układ sklepu

Układ Sklepu definiuje sposób wyświetlania aplikacji w Sklepie Play lub to, czy są one w ogóle wyświetlane.

Pamiętaj, że jeśli chcesz wyświetlać aplikacje w Sklepie Play, aby użytkownik mógł je ręcznie zainstalować, należy je dodać tutaj w układzie. **ORAZ** w profilu do sklepu Enterprise Play Store. Jeśli aplikacja zostanie dodana tylko do jednego z nich, nie będzie wyświetlana.

Zestaw aplikacji

Dzięki App Bundles można definiować grupy aplikacji, które można przypisać do profili urządzeń lub grup za pomocą jednego kliknięcia.



Kliknij "+", aby utworzyć nowy App Bundle. Po utworzeniu App Bundle możesz kliknąć "Edit", aby dodać do niego aplikacje z różnych źródeł.

Pakiety można dodawać do profili jak każdą inną aplikację. Podczas dodawania aplikacji pojawi się dodatkowa karta o nazwie "App Bundles", w której znajdują się pakiety.

Jeśli dokonasz jakiejkolwiek zmiany w pakiecie aplikacji, pojawi się przycisk w kolumnie "Deploy". Umożliwi to przesłanie tych zmian do wszystkich profili zawierających ten pakiet. Należy więc pamiętać, że trzeba to zrobić ręcznie po dodaniu lub usunięciu aplikacji w pakiecie.

Pilot zdalnego sterowania

TeamViewer

TeamViewer Connector

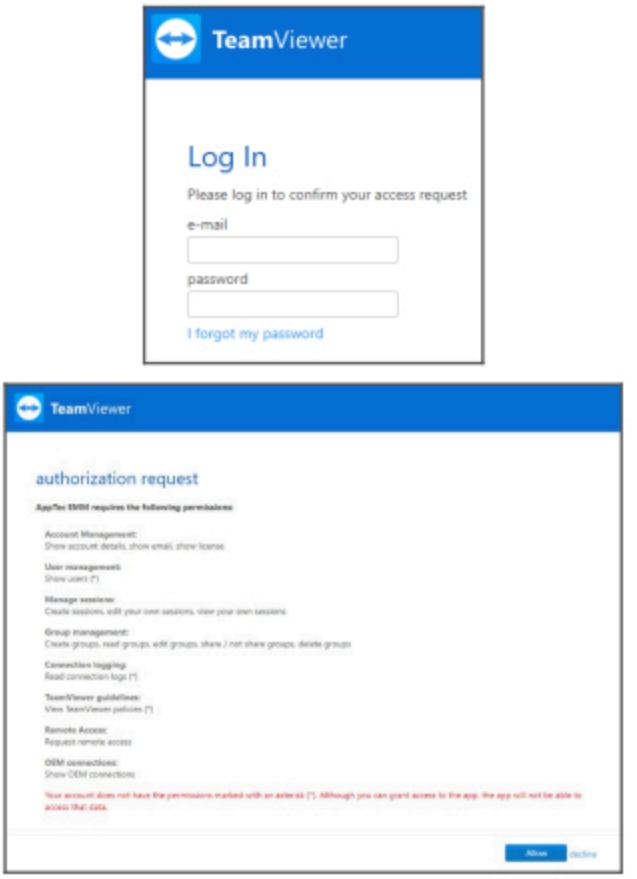
Uwaga: W bezpłatnej wersji próbnej naszej wersji w chmurze nie ma możliwości podłączenia konta TeamViewer. Zamiast tego zostanie automatycznie połączone bezpłatne konto demo.

Przejdź do Ustawienia ogólne -> Zdalne sterowanie -> TeamViewer. Tutaj możesz połączyć swoje konto TeamViewer z konsolą lub zobaczyć informacje o aktualnie połączonym koncie. Możesz także wyświetlić wszystkie aktualnie aktywne sesje, przechodząc do zakładki "Aktywne sesje".

Aby połączyć swoje konto, kliknij "Rozpocznij konfigurację".

Spowoduje to przekierowanie do nowej strony, na której należy zalogować się przy użyciu konta TeamViewer.

Po zalogowaniu należy autoryzować AppTec360 MDM do korzystania z tego konta. Po potwierdzeniu należy odczekać kilka sekund, a konto zostanie połączone.


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

Zainstaluj TeamViewer QuickSupport

Dodaj aplikację "TeamViewer QuickSupport" do obowiązkowych aplikacji w profilu urządzenia lub profilu grupy i kliknij przycisk "Przypisz teraz". Poczekaj, aż aplikacja zostanie zainstalowana na urządzeniu.

Jeśli spróbujesz uzyskać dostęp do urządzenia, na którym aplikacja nie jest zainstalowana, zostanie ona zainstalowana lub zostaniesz poproszony o jej zainstalowanie, w zależności od konfiguracji urządzenia.

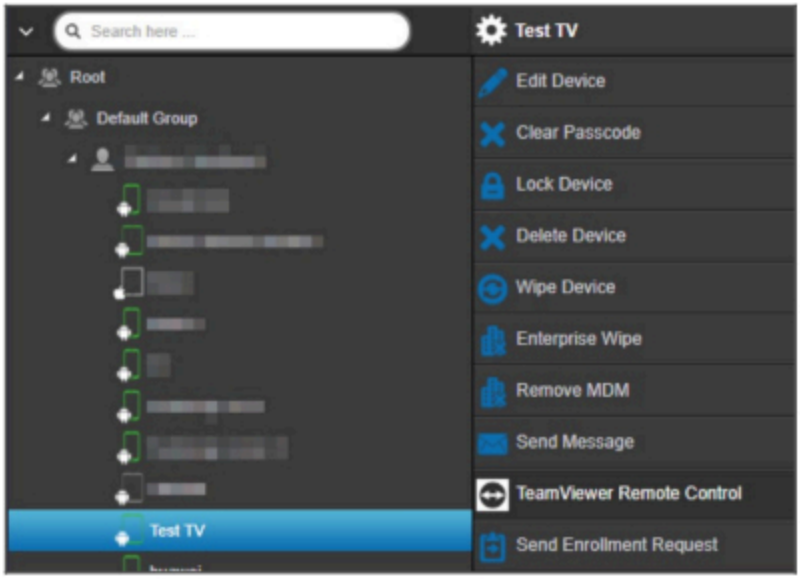
Zdalne sterowanie urządzeniem

Aby zdalnie sterować urządzeniem, wybierz urządzenie, kliknij kółko i wybierz "TeamViewer Remote Control".

Jeśli istnieje już aktywna sesja, można użyć starej sesji lub utworzyć nową.

Potwierdź, że chcesz utworzyć nową sesję TeamViewer.

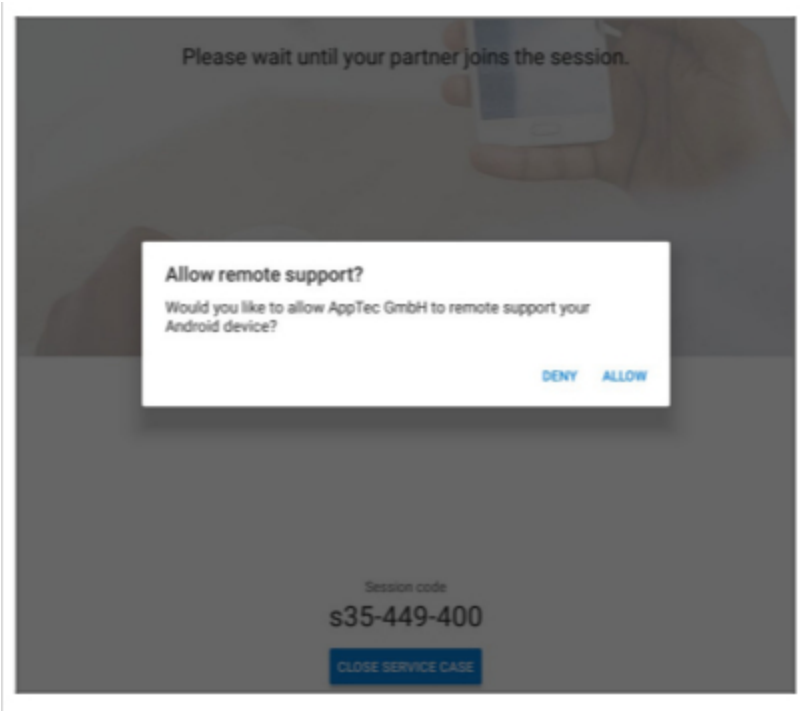
Po kilku sekundach pojawi się link do sesji TeamViewer. Możesz kliknąć "Start", aby otworzyć ten link w nowym oknie.


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

To łącze otworzy zainstalowaną aplikację TeamViewer i połączy użytkownika z urządzeniem.

Teraz musisz potwierdzić połączenie na samym urządzeniu, aby móc nim zdalnie sterować.

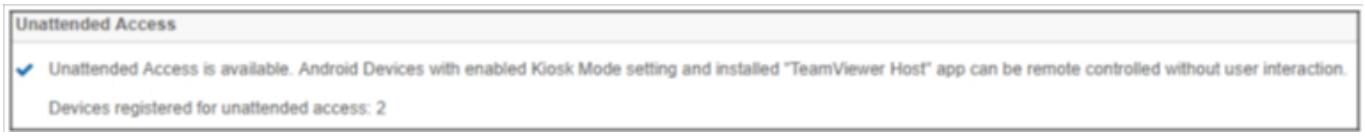


Jeśli korzystasz z iOS, otrzymasz wiadomość w AppTec360 MDM Client. Za pomocą tego linku urządzenie dołączy do sesji zdalnej. W zależności od ustawień powiadomień urządzenia możliwe jest, że nie otrzymasz powiadomienia i będziesz musiał ręcznie otworzyć AppTec360 MDM Client.

Na niektórych urządzeniach z systemem Android (np. Samsung) wymagane jest zainstalowanie dodatkowej aplikacji jako dodatku. Aplikacja TeamViewer na urządzeniu poinformuje Cię o tym, jeśli jest to konieczne na Twoim urządzeniu.

Dostęp nienadzorowany

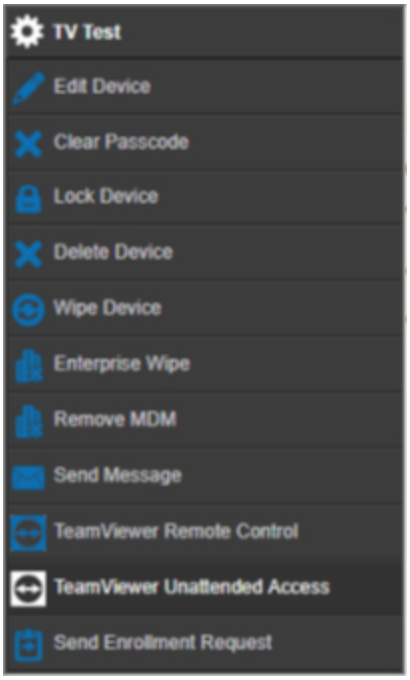
Uwaga: Dostęp nienadzorowany jest możliwy tylko na urządzeniach z systemem Android.



Możesz łączyć się ze swoimi urządzeniami bez akceptowania połączenia na urządzeniu tylko wtedy, gdy Twoje konto TeamViewer korzysta z licencji "Tensor" lub "Corporate".

Można to sprawdzić po połączeniu konta w "Ustawieniach ogólnych"

Aby korzystać z dostępu nienadzorowanego, należy zainstalować aplikację "TeamViewer Host" i aktywować opcję "Enable Unattended Access" w sekcji "Kiosk Mode & Launcher" w swoim profilu. Należy pamiętać, że jest to możliwe tylko w przypadku korzystania z trybu kiosku.



Teraz możesz wybrać dostęp nienadzorowany, jeśli wybierzesz swoje urządzenie i klikniesz kółko. Spowoduje to połączenie z urządzeniem bez konieczności potwierdzania na samym urządzeniu. Należy pamiętać, że uzyskanie łącza dostępu do urządzenia może zająć kilka chwil.

Splashtop

Jeśli włączysz opcję Splashtop, zobaczysz opcje konfiguracji Splashtop w swoich profilach.

Aby korzystać ze Splashtop, musisz ustawić Splashtop Streamer (com.splashtop.streamer.csrs) jako obowiązkową aplikację w swoim profilu. Następnie możesz włączyć konfigurację Splashtop w swoim profilu w sekcji "Zdalne sterowanie". Włączenie tej opcji spowoduje skonfigurowanie aplikacji Splashtop Streamer. Jeśli używasz Splashtop Streamer, ale nie w połączeniu z MDM, powinieneś pozostawić to wyłączone.

W swoim profilu w sekcji "Zdalne sterowanie" musisz również ustawić kod wdrożenia. Wejdź na stronę https://my.splashtop.com i zaloguj się na swoje konto Splashtop. Kliknij "Dodaj komputer" i skopiuj 12-cyfrowy kod wdrożeniowy z wyświetlonej strony.

Bez Deploy Code zdalne sterowanie NIE jest możliwe.

Po wykonaniu tej czynności można kliknąć urządzenie prawym przyciskiem myszy i rozpocząć sesję zdalną, klikając "Splashtop Remote Control".

Zarządzanie kartami SIM

Import zbiorczy CSV

Pokazuje przegląd przypisanych kart SIM i wszystkie informacje na ich temat. Pomaga to mieć wszystkie informacje, nie tylko o urządzeniach, ale także o kartach SIM w jednym systemie.

UWAGA: Jest to ręczne zarządzanie/dokumentacja. Nie jest możliwe automatyczne uzyskanie tych danych z urządzeń ze względu na mechanizmy prywatności/bezpieczeństwa systemów operacyjnych.

Można również zaimportować tę listę jako CSV.

Przewoźnik i taryfa

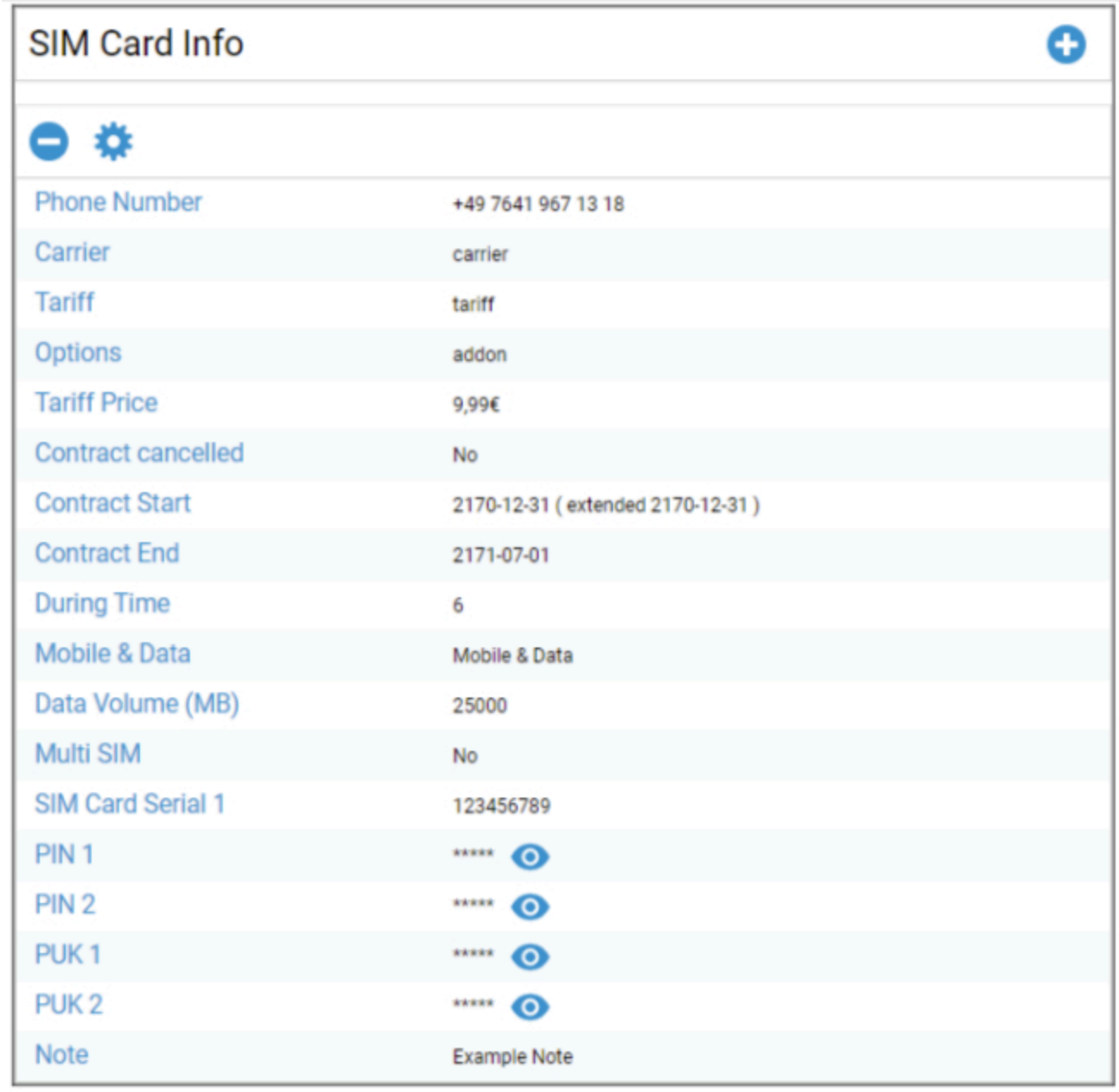
Aby dodać kartę SIM, najpierw kliknij przycisk dodawania jednego lub wielu operatorów.

Następnie kliknij przycisk "+" w sekcji "Informacje o taryfie", aby dodać taryfę do przewoźnika.

Opcjonalnie możesz dodać opcjonalne dodatki poniżej, jeśli masz coś takiego.

Przygotowano tu wszystko, czego potrzeba do dodania rzeczywistej karty SIM. Karty SIM są obecnie przypisane do użytkownika. Dlatego przejdź do Zarządzania urządzeniami mobilnymi, wybierz Użytkownika i przejdź do "Przeglądu kart SIM".

Tutaj wyświetlane są karty SIM użytkowników. Jeśli taka istnieje, można ją edytować lub usunąć. Użytkownicy mogą mieć wiele kart SIM.

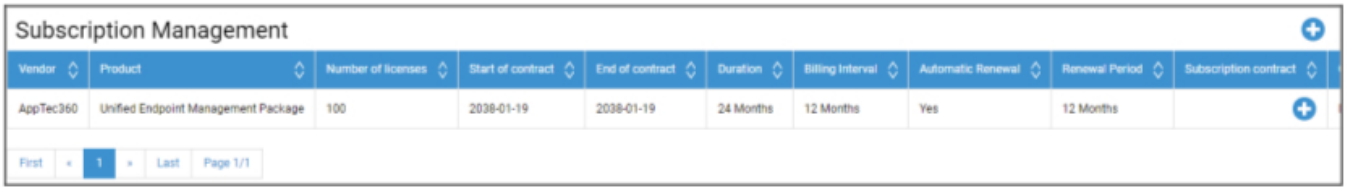


Kliknij "+", aby dodać kartę SIM i dodać wszystkie potrzebne informacje. Te karty Sim będą również wymienione na liście wszystkich kart Sim w Ustawieniach ogólnych → Zarządzanie kartami Sim.

Zarządzanie subskrypcjami

Zarządzanie subskrypcjami

W tym miejscu można dokumentować bieżące subskrypcje, ich szczegóły, a także przechowywać różne pliki, np. podpisaną umowę, pismo o rozwiązaniu umowy itp. Możesz także skonfigurować przypomnienia, które będą przypominać Ci pocztą przed zakończeniem subskrypcji i być może przedłużą ją automatycznie.



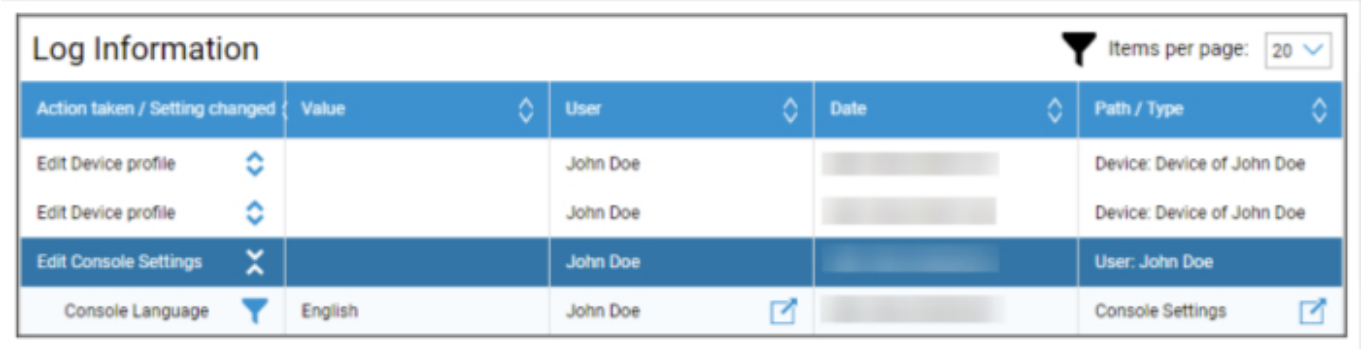
Kliknij "+" u góry, aby dodać subskrypcję. Możesz dodać dowolną liczbę subskrypcji.

Kliknij "+" w różnych polach, aby przesłać pliki dotyczące tej subskrypcji. Technicznie możesz przesłać dowolny typ pliku, ale pamiętaj, że nie każdy typ pliku można wyświetlić w przeglądarce.

Ogólny dziennik kontroli

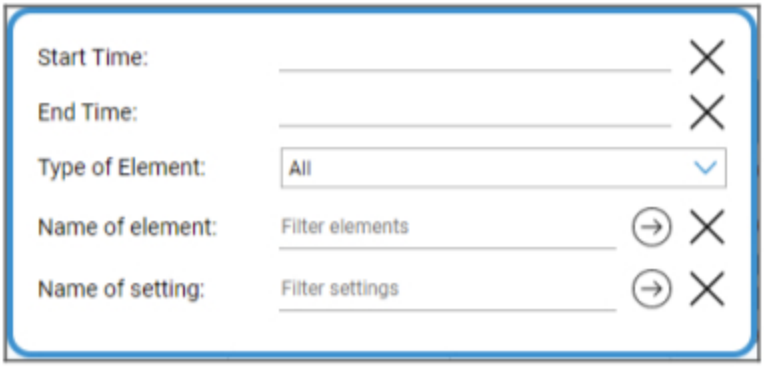
Dziennik kontroli

Tutaj znajduje się ogólny dziennik audytu, który pokazuje wszystkie wprowadzone zmiany. Podczas gdy dziennik audytu użytkownika lub grupy pokazuje tylko zmiany dotyczące tego użytkownika lub grupy, ten pokazuje KAŻDĄ zmianę dokonaną w dowolnym miejscu konsoli.



Możesz zobaczyć, co zostało zmienione, przez kogo, kiedy i gdzie. W niektórych przypadkach można również rozszerzyć wpis, aby zobaczyć więcej szczegółów.

Możliwe jest kliknięcie użytkownika lub wpisu w "Ścieżka / Typ", aby przejść do lokalizacji, w której dokonano zmiany.



W prawym górnym rogu można również zdefiniować filtr, który może pomóc w znalezieniu określonych zmian w środowisku, w którym zachodzi wiele zmian.

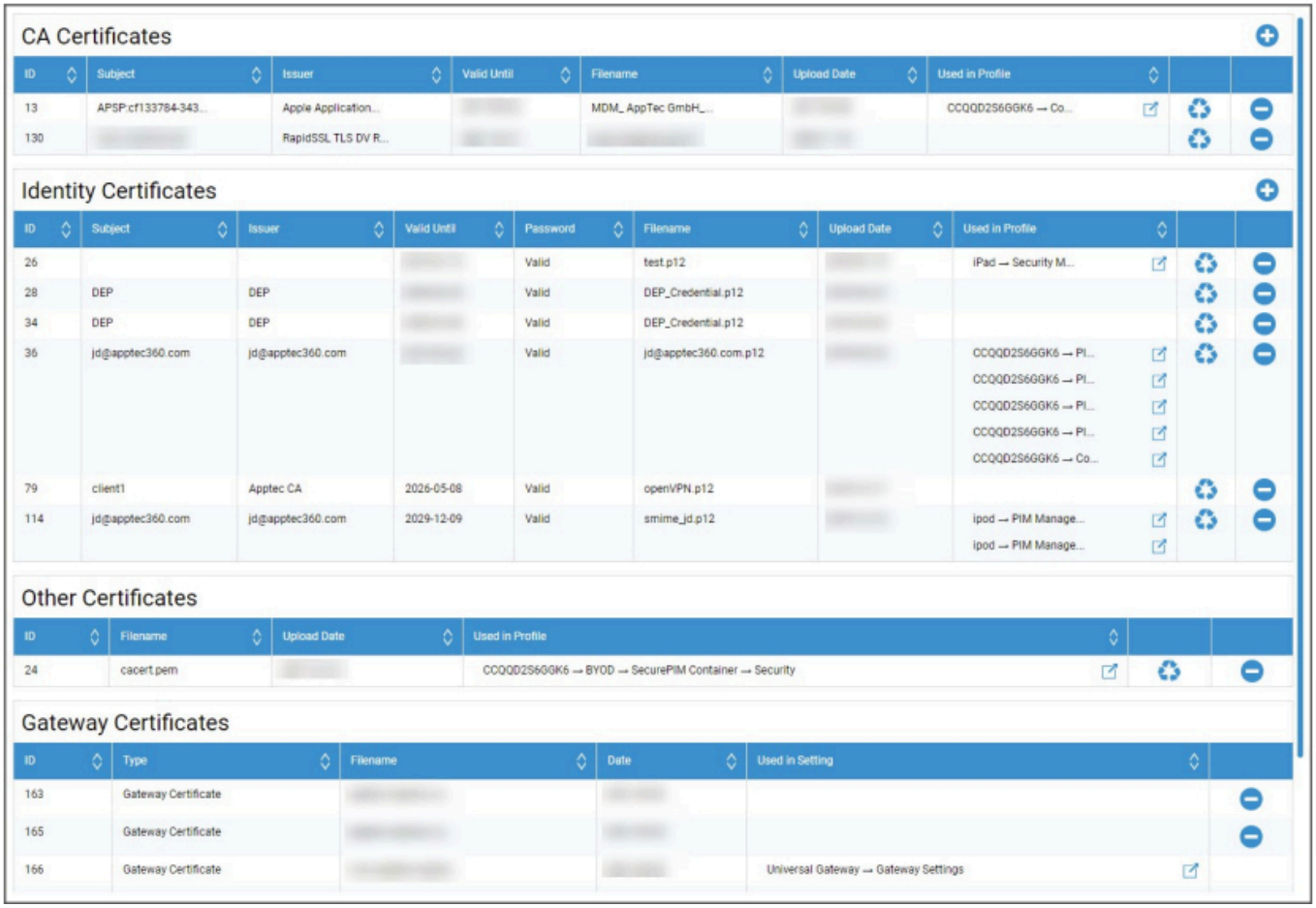
Ustawienia dziennika inspekcji

"Okres przechowywania dziennika audytu" określa, jak długo dzienniki audytu powinny być przechowywane przed usunięciem.

Zarządzanie certyfikatami

Tutaj znajdziesz przegląd wszystkich certyfikatów przesłanych i używanych w konsoli. Jest to tylko przegląd. Rzeczywista konfiguracja np. certyfikatów Wi-Fi jest nadal wykonywana w profilu w odpowiedniej lokalizacji.

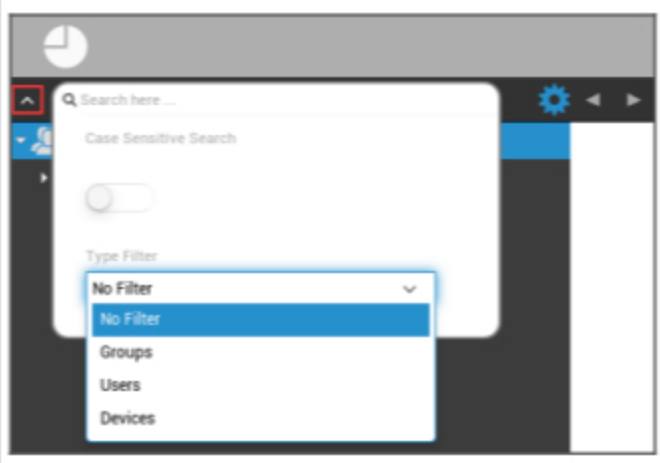
Tutaj można również usunąć lub zaktualizować certyfikaty, co zostanie automatycznie odzwierciedlone w odpowiednich profilach. Kliknij informacje w sekcji "Używany w profilu", aby zobaczyć, gdzie dokładnie jest przypisany certyfikat.



Zarządzanie urządzeniami mobilnymi

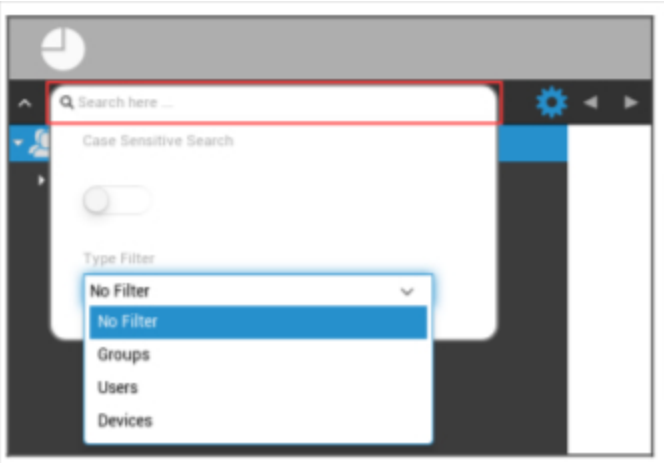
Ekran zarządzania urządzeniami mobilnymi

Filtr urządzenia



Po kliknięciu w lewym górnym rogu ekranu można znaleźć różne filtry do wyświetlania urządzeń.

Okno wyszukiwania



Okno wyszukiwania umożliwia przeszukiwanie wszystkich urządzeń i/lub użytkowników za pomocą określonego słowa kluczowego.

Opcje sprzętu

Po kliknięciu odpowiedniego symbolu wyświetlona zostanie lista dostępnych opcji.

Zmieniają się one wraz z każdym bieżącym oknem i są wyjaśnione w odpowiednich rozdziałach.

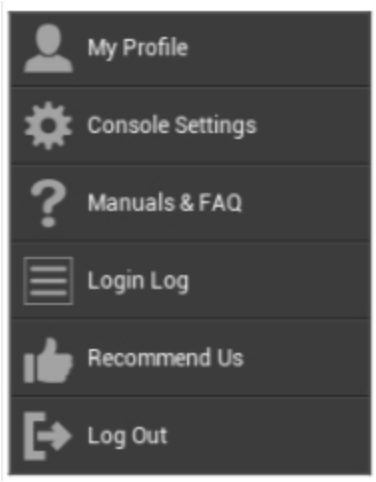
Strzałki nawigacyjne

Kliknięcie strzałki w lewo spowoduje przejście do poprzedniej strony.

Następnie, klikając strzałkę w prawo, zostaniesz przeniesiony na stronę, którą właśnie opuściłeś.

Ustawienia konta administracyjnego

Kliknięcie adresu e-mail, jak pokazano powyżej, powoduje wyświetlenie następującego menu:



Mój profil	Edytuj szczegóły konta administratora
Ustawienia konsoli	Konfiguracja ustawień konsoli dla konta administratora
Podręczniki i FAQ	Wyświetl stronę "Instrukcje i FAQ" w "Ustawieniach ogólnych".
Dziennik logowania	Dostęp do "Dziennika logowania"
Poleć nas	Wyświetl stronę "Poleć nas" w "Ustawieniach ogólnych".
Wyloguj się	Wyloguj się z konsoli MDM

Informacje o użytkowniku

W tym miejscu można edytować dane konta aktualnie zalogowanego administratora.

Nazwa użytkownika	Nazwa użytkownika i/lub adres e-mail konta
Nazwa	Imię i nazwisko administratora
Nazwisko	Nazwisko administratora
Nazwa logowania	Nazwa logowania administratorów
Adres e-mail	Adres e-mail administratorów
Alternatywny adres e-mail	Alternatywny adres e-mail administratora
Zdjęcie	Zdjęcie profilowe
Numer telefonu	Numer telefonu administratora
Numer telefonu komórkowego	Numer telefonu komórkowego administratora
Rozszerzenie telefonu	Rozszerzenie telefonu
Lokalizacja	Lokalizacja
Pozycja	Stanowisko w firmie
Grupa użytkowników	Wybierz grupę użytkowników, do której chcesz przypisać konto administratora.
Komentarz	Wprowadź komentarz
Wprowadź nowe hasło	Wprowadź hasło w celu zmiany hasła
Powtórz nowe hasło	Powtórz nowe hasło, aby je potwierdzić

Należy pamiętać, że dostęp administracyjny może być również złożony jako konto użytkownika lokalnego w strukturze hierarchii. Bez ustanowienia dodatkowego administratora, ten nie powinien zostać usunięty!

Ustawienia konsoli

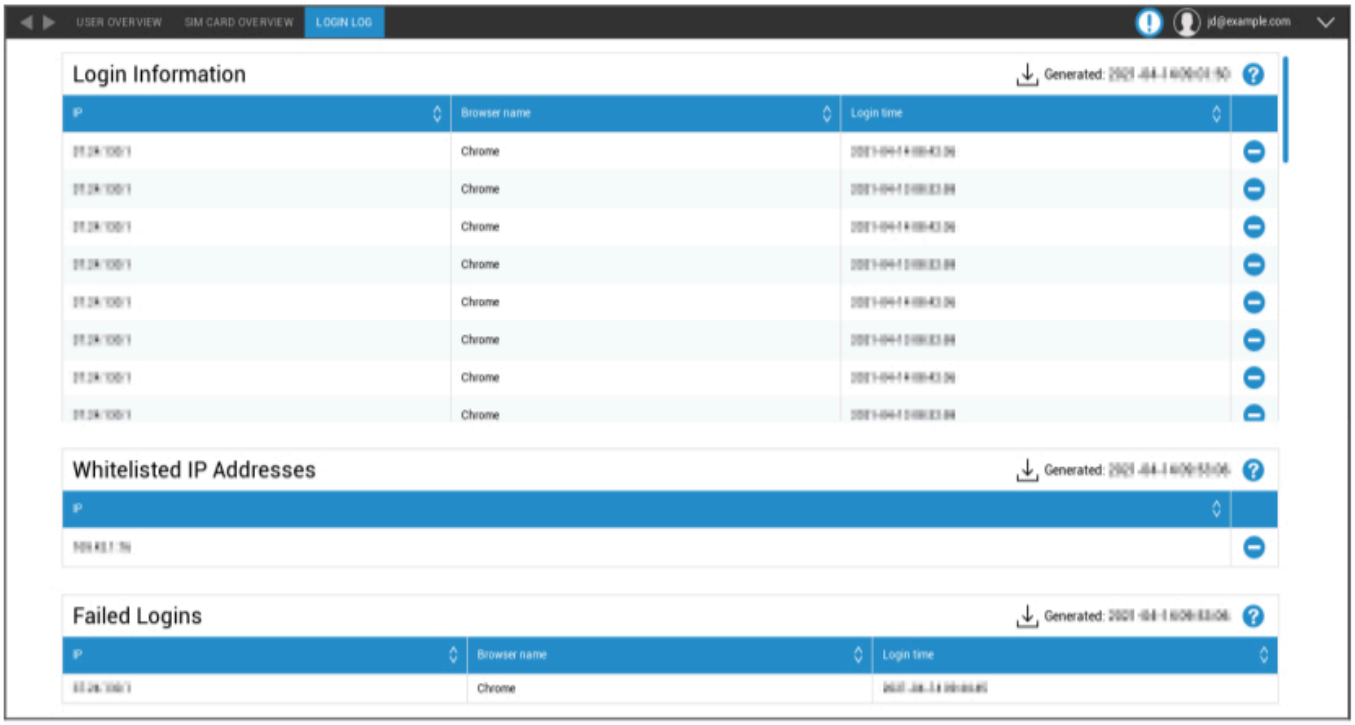
W tym miejscu można skonfigurować następujące ustawienia konsoli dla konta administratora:

Opcje wyświetlania użytkownika katalogu	Definiowanie sposobu oznaczania użytkowników w drzewie
Opcje wyświetlania urządzenia katalogowego	Definiowanie sposobu oznaczania urządzeń w drzewie
Limit czasu sesji	Jeśli użytkownik nie wykona żadnej czynności w określonym czasie, zostanie wylogowany. Domyślną wartością jest 60 minut. Po zmianie tego ustawienia należy się wylogować i zalogować ponownie.
Strefa czasowa	Wybierz używaną strefę czasową
Format czasu	Wybierz sposób wyświetlania znaczników czasu
Język konsoli	Wybierz język, w którym ma być wyświetlana konsola. Dostępne są języki angielski i niemiecki.
Kolor główny	Możesz ustawić kolor, który będzie używany jako podstawa schematu kolorów konsoli. Możesz użyć selektora kolorów lub wprowadzić kolor w notacji HTML HEX. Formatory RGB, takie jak "różowy", "żółty" również działają.
Polecenie Zapisz	Kombinacja klawiszy uruchamiająca zapis bez naciskania przycisku "Zapisz".
Uwierzytelnianie dwuskładnikowe	Włącz uwierzytelnianie dwuskładnikowe podczas logowania. Po zalogowaniu otrzymasz wiadomość e-mail z kodem, który musisz wprowadzić, aby się zalogować.
Limit czasu uwierzytelniania dwuskładnikowego	Ustaw okres czasu, w którym użytkownik nie będzie proszony o uwierzytelnienie dwuskładnikowe po udanym uwierzytelnieniu.
Wyślij kod weryfikacyjny przez	Kod weryfikacyjny zostanie wysłany do wybranych opcji. Wiadomość o urządzeniu zostanie wyświetlona w aplikacji AppTec360 MDM na wszystkich urządzeniach z systemem Android i iOS należących do użytkownika.
Wyślij wiadomość po zalogowaniu	Jeśli opcja ta jest włączona, wiadomość e-mail będzie wysyłana w przypadku każdego logowania z adresu IP, który nie znajduje się na białej liście.

	Wiadomość e-mail zawiera informacje o logowaniu (np. IP, przeglądarka).

Dziennik logowania

W tym miejscu można zobaczyć informacje dotyczące loginów aktualnie zalogowanego konta administratora.



Informacje o logowaniu	Lista zawierająca loginy aktualnie zalogowanego konta administratora, które zostały zarejestrowane przez konsolę. Ta lista pokazuje wszystkie udane logowania w ciągu ostatnich 30 dni.
Adresy IP na białej liście	Jest to lista wszystkich adresów IP znajdujących się na białej liście. Jeśli zalogujesz się z adresu IP, który jest wymieniony tutaj, nie otrzymasz komunikatu logowania. Adres IP można dodać do tej listy, klikając przycisk obok wpisu na powyższej liście "Informacje o logowaniu". Adres IP można usunąć z tej listy, klikając przycisk obok wpisu na tej liście lub na liście "Informacje o logowaniu" powyżej.
Nieudane logowania	Jest to lista wszystkich nieudanych prób logowania w ciągu ostatnich 30 dni. Jeśli nie udało się wprowadzić poprawnego hasła co najmniej 3 razy w ciągu 20 minut, wpis pojawi się na tej liście. Użytkownik będzie również informowany o nieudanych próbach logowania za pośrednictwem wiadomości e-mail.

Administracja korporacyjna (węzeł główny) w zarządzaniu urządzeniami mobilnymi

Po przejściu do węzła głównego (pierwszej grupy) można wykonać różne ustawienia dla firmy w odniesieniu do zarządzania urządzeniami mobilnymi.

Tworzenie podgrupy	Utwórz podgrupę
Zmiana nazwy węzła głównego	Zmiana nazwy węzła głównego (np. nazwa firmy)
Masowa rejestracja	Rejestracja wielu urządzeń/użytkowników jednocześnie
Przydział masowy	Przypisanie profilu dla odpowiednich grup, z jednym wyglądem
Szybka administracja aplikacjami	Wysyłanie żądań (nie)instalacji aplikacji do odpowiednich grup urządzeń
Import użytkownika CSV	Importowanie użytkowników z CSV do odpowiedniej grupy

Tworzenie podgrupy

Za pomocą opcji "Utwórz podgrupę" można utworzyć dodatkową podgrupę.

Można ustalić, do której grupy ma zostać przypisana podgrupa.

(Domyślnie tworzona jest nowa grupa, która jest przypisana jako podgrupa w węźle głównym).

Zmiana nazwy węzła głównego

Tutaj można zmienić nazwę główną. W tym przypadku często używana jest nazwa firmy.

Masowa rejestracja

Dzięki funkcji "Mass Enrollment" można zarejestrować wiele urządzeń i użytkowników.

Możesz bezpośrednio wybrać, w jaki sposób użytkownik ma otrzymać rejestrację (eMail; alternatywny eMail; SMS).

W zależności od urządzenia, z którego będzie korzystał użytkownik (iOS, Android, Windows Phone), można to bezpośrednio zaznaczyć tutaj.

Rozróżnienie, czy jest to smartfon, czy tablet, można również skonfigurować tutaj, co należy wybrać poprawnie, zaznaczając znacznik wyboru.

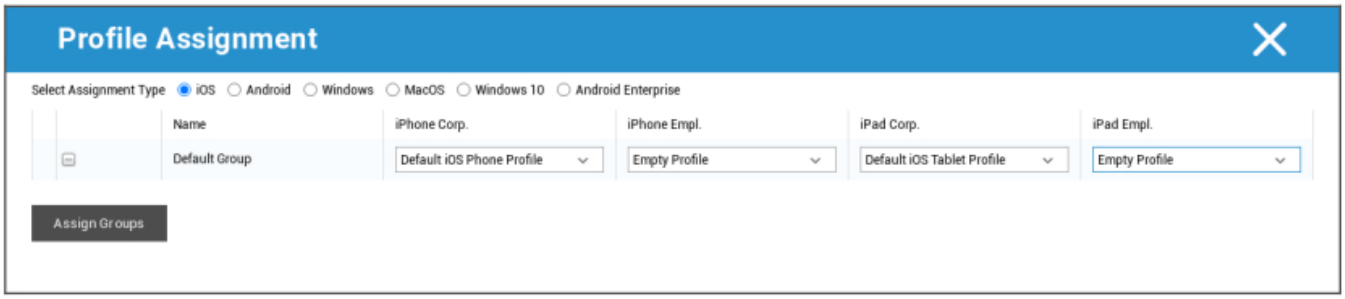
Ostatnim krokiem jest ustalenie, czy dane urządzenie jest firmowe czy prywatne (BYOD).

Za pomocą opcji "Eksportuj jako CSV" można wyeksportować informacje jako plik danych CSV. W zamian można również zaimportować plik danych CSV za pomocą opcji "Import CSV", plik powinien wyglądać jak na poniższym przykładzie:

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

Przydział masowy

W sekcji Przypisanie masowe można przypisać profil do wszystkich grup, które są podzielone na iOS - Android - Windows - MacOS - Windows 10 - Android Enterprise.

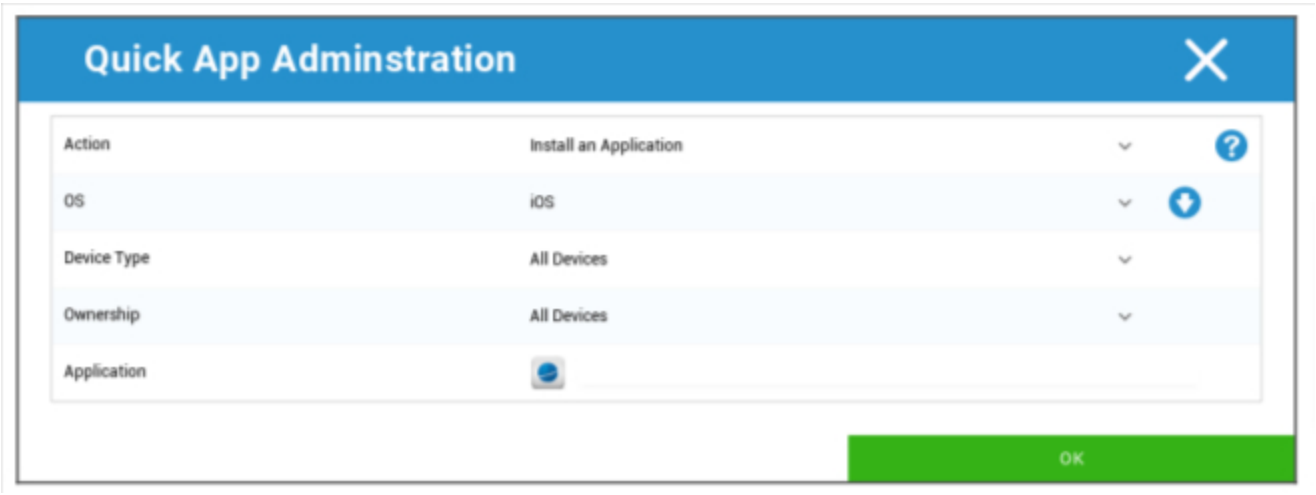


Windows - MacOS - Windows 10 - Android Enterprise

Szybka administracja aplikacjami

W Quick App Administration można wysyłać żądania instalacji lub dezinstalacji określonej aplikacji do wybranego systemu operacyjnego.

Można również określić, czy żądanie ma być wysyłane do wszystkich typów urządzeń wybranego systemu operacyjnego, czy tylko do określonego typu urządzenia.



Import użytkownika CSV

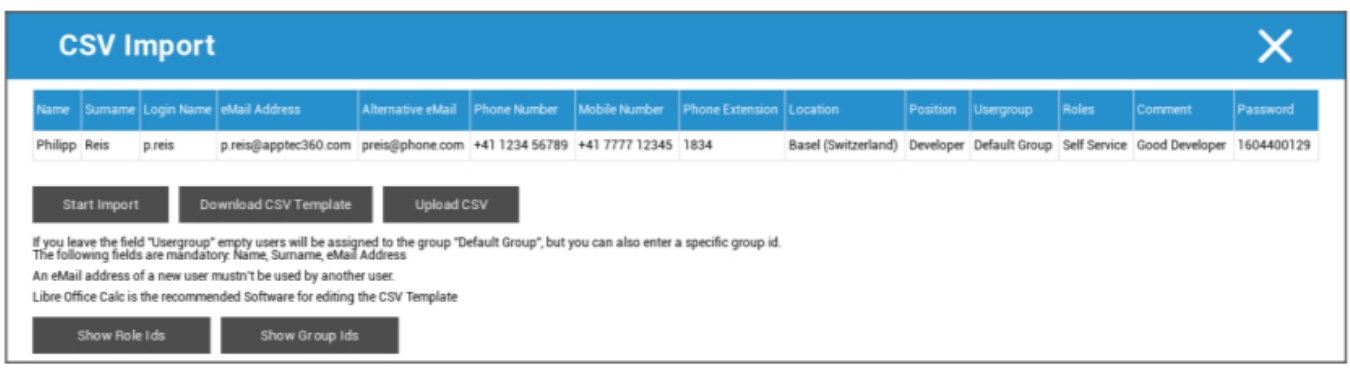
Importuj użytkowników z CSV do odpowiedniej grupy.

Za pomocą opcji "Pobierz szablon CSV" można wyeksportować plik szablonu CSV, który można wypełnić (lub wykorzystać jako odniesienie).

Można również użyć opcji "Pokaż identyfikatory ról" i "Pokaż identyfikatory grup" jako odniesienia do utworzenia własnego pliku CSV.

Plik CSV można przesłać do MDM za pomocą opcji "Prześlij CSV".

Ostatnim krokiem jest rozpoczęcie importu poprzez kliknięcie przycisku "Rozpocznij import".



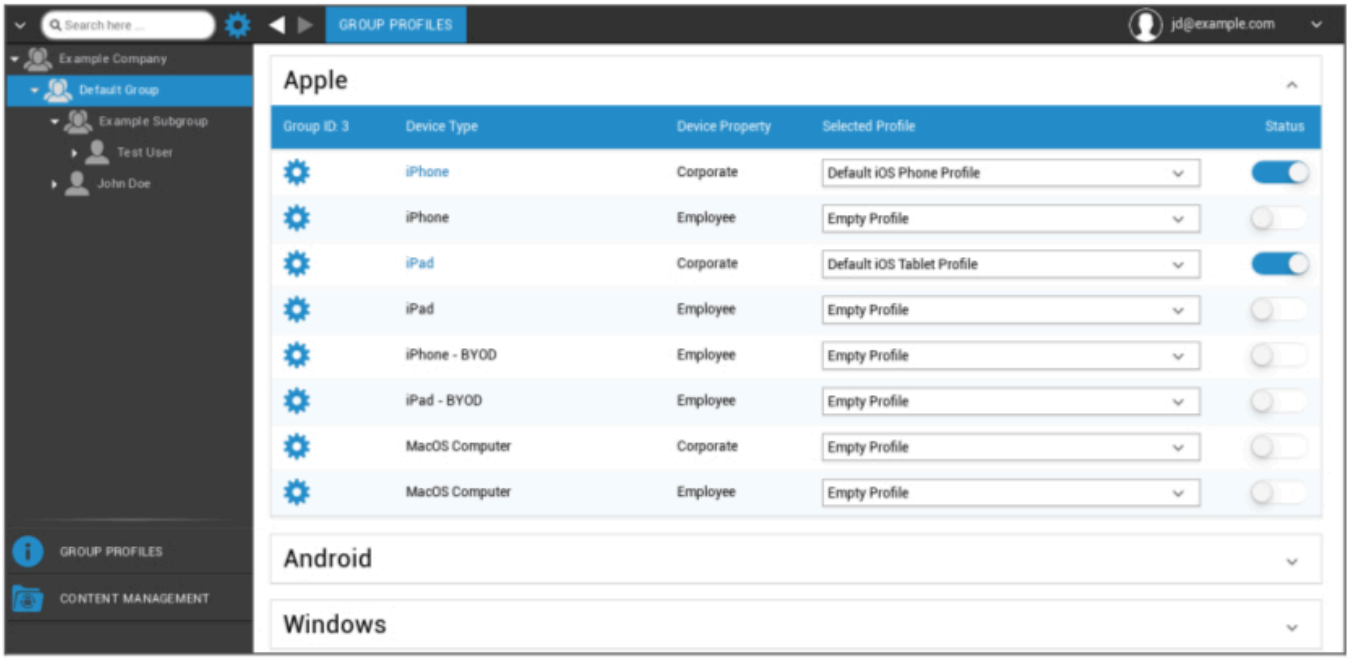
Zarządzanie grupami w zarządzaniu urządzeniami mobilnymi

Jedno kliknięcie na przegląd wyświetla różne profile konfiguracji dla poszczególnych platform.

Jeden profil zawiera wszystkie opcje ustawień, które można wcześniej skonfigurować za pomocą AppTec360 na urządzeniu użytkownika końcowego. Na każdej platformie można tworzyć profile dla urządzeń firmowych (Corporate) lub urządzeń typu Bring-Your-Own-Device (Employee).

W celu rozróżnienia konfiguracji dla grup urządzeń, na przykład na podstawie lokalizacji lub funkcji, zaleca się utworzenie kilku podgrup.

Zwróć uwagę na Zarządzanie profilami w Zarządzaniu urządzeniami mobilnymi



W menu narzędzi można skonfigurować różne ustawienia dla danej (pod)grupy.

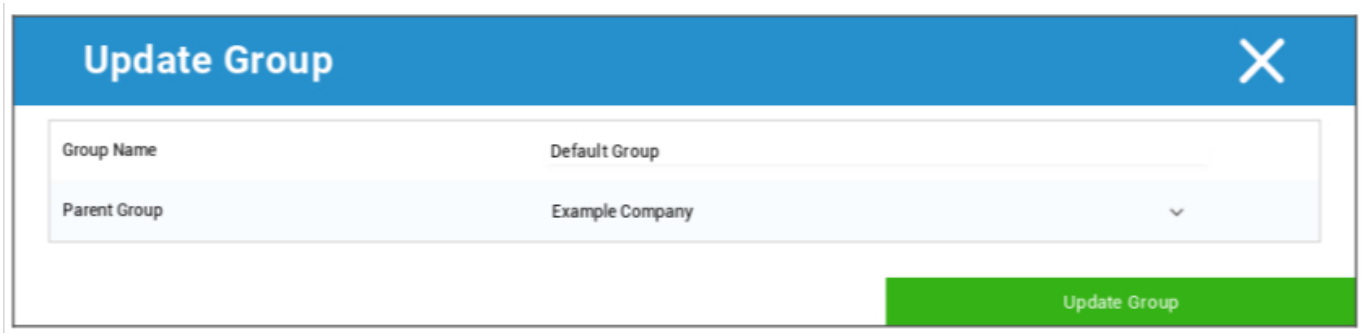
Tworzenie podgrupy	Utwórz podgrupę dla odpowiedniej (pod)grupy
Edytuj wybraną grupę	Edytuj wybraną grupę
Usuń wybraną grupę	Usuń wybraną grupę
Masowa rejestracja	Rejestracja wielu urządzeń/użytkowników jednocześnie dla wybranego profilu
Przydział masowy	Przypisywanie profili do aktualnie wybranej grupy
Tworzenie podgrupy	Utwórz podgrupę dla odpowiedniej (pod)grupy
Utwórz użytkownika	Utwórz użytkownika dla odpowiedniej (pod)grupy

Tworzenie podgrupy

Za pomocą opcji "Utwórz podgrupę" można utworzyć dodatkową podgrupę.

Można ustalić, do której grupy ma zostać przypisana podgrupa (domyślnie podgrupa jest przypisywana do aktualnie wybranej grupy).

Edytuj wybraną grupę



Tutaj można edytować profil - możliwe są następujące ustawienia:

- Nazwę grupy można zmienić
- Grupa nadrzędna może zostać zmieniona

Usuń wybraną grupę

W sekcji "Usuń wybraną grupę" wyświetlane są listy wszystkich użytkowników i urządzeń należących do danej grupy. Tutaj masz możliwość ich usunięcia.

Dla jednego użytkownika można wykonać następujące polecenia usunięcia:

Usuń użytkownika	Użytkownik został usunięty
Przenieś użytkownika do grupy:	Możesz przenieść użytkownika do innej grupy (następna kolumna, np. "Administratorzy").

Dla jednego urządzenia można wykonać następujące polecenia usunięcia:

Wipe & Delete	Czyszczenie i usuwanie urządzenia
Usuń z systemu	Usuń urządzenie tylko z AppTec

Odniesienie: Masowa rejestracja

Odniesienie: Przydział masy

Utwórz użytkownika

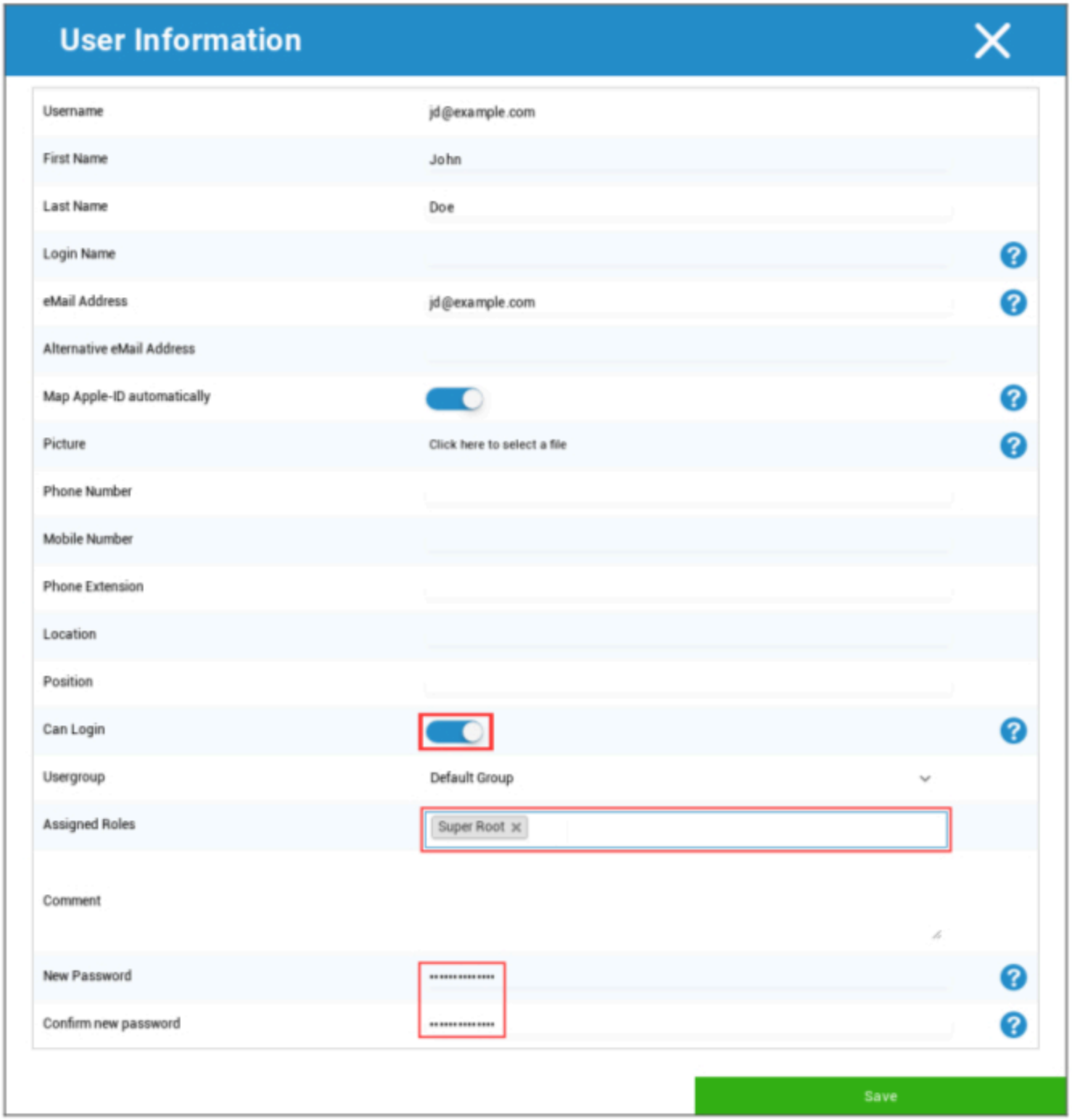
Za pomocą opcji "Utwórz użytkownika" można dodać nowego użytkownika.

Utwórz nowego użytkownika admin

Użytkownika można ustawić jako Admin-User. Da mu to uprawnienia do logowania się do konsoli, a także do zmiany użytkowników/grup/urządzeń.

Utwórz zwykłego użytkownika lub użyj istniejącego. Wybierz użytkownika, któremu chcesz nadać uprawnienia administratora, kliknij kółko i wybierz "Edytuj użytkownika":

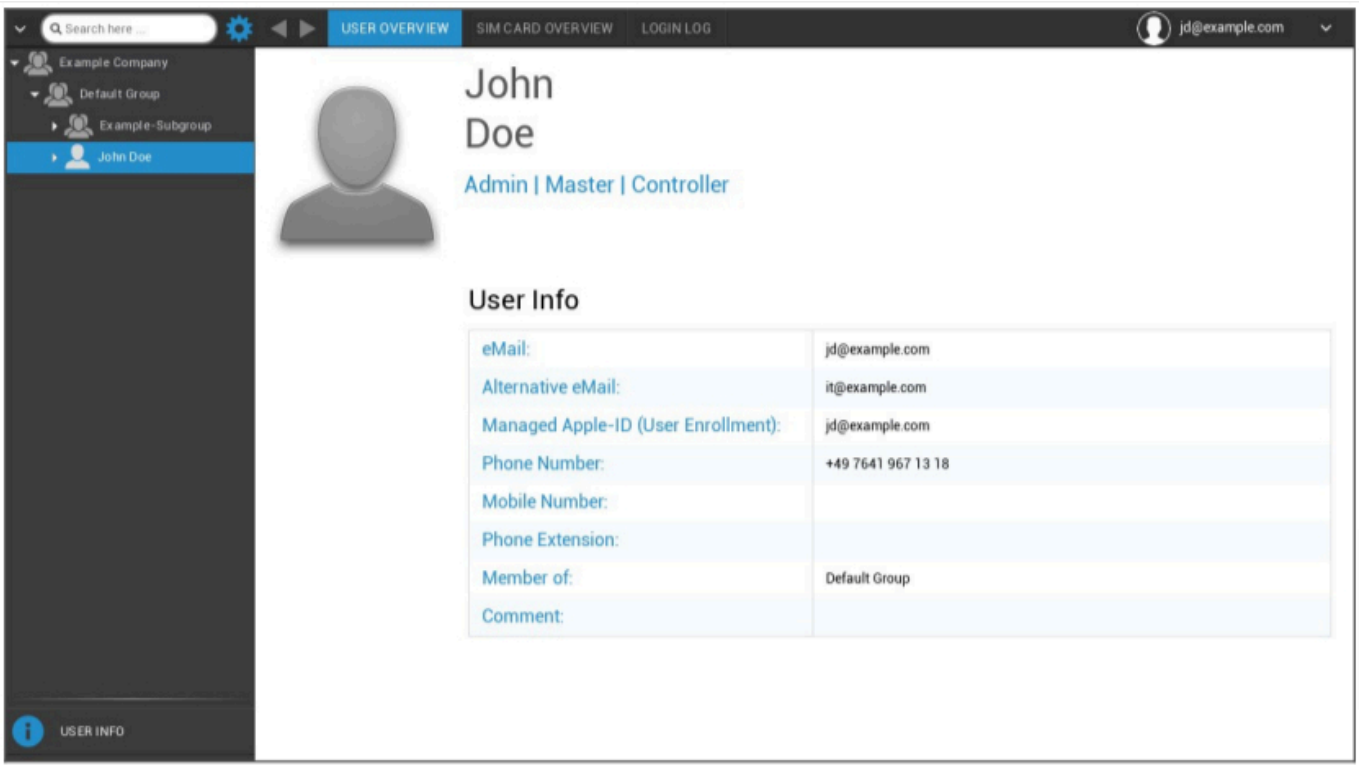
Aktywuj przełącznik "Can Login", przypisz rolę "Super-Root" do użytkownika i ustaw hasło.



Zapisz to, a użytkownik może teraz zalogować się przy użyciu nazwy użytkownika i hasła.

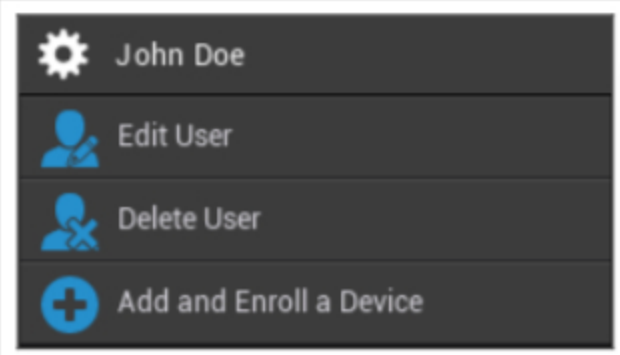
Zarządzanie użytkownikami w zarządzaniu urządzeniami mobilnymi

Po wybraniu określonego użytkownika zobaczysz następujący przegląd:



Zostanie wyświetlony przegląd wszystkich informacji wprowadzonych wcześniej w sekcji "Utwórz użytkownika".

Za pomocą sprzętu zainstalowanego na górze można wykonać następujące konfiguracje:



Nazwa użytkownika	Nazwa użytkownika wybranego użytkownika
Edytuj użytkownika	Edycja informacji o użytkowniku

Usuń użytkownika	Usuń użytkownika • Delete from System = urządzenie zostanie usunięte z AppTec • Wipe & Delete = Urządzenie zostanie przywrócone do ustawień fabrycznych i usunięte z AppTec.
Dodawanie i rejestrowanie urządzenia	Zarejestruj urządzenie dla wybranego użytkownika

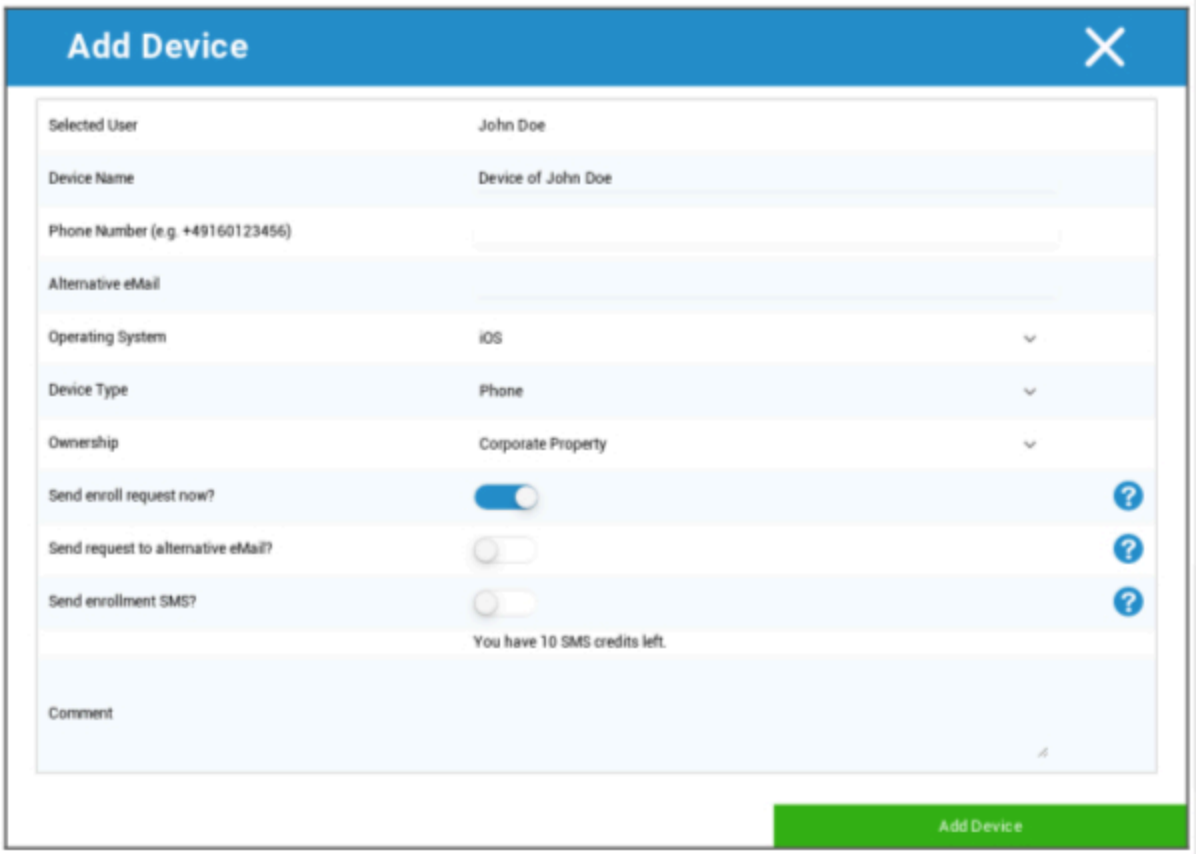
Należy pamiętać, że dostęp administracyjny może być również złożony jako konto użytkownika lokalnego w strukturze hierarchii. Bez ustanowienia dodatkowego administratora, ten nie powinien zostać usunięty!

Dodawanie i rejestrowanie urządzenia

W tym miejscu można wybrać urządzenie dla wybranego zastosowania.

Alternatywnie można bezpośrednio zarejestrować urządzenia w grupie. Aby to zrobić, kliknij grupę, kliknij kółko i wybierz opcję "Dodaj i zarejestruj urządzenie".

Powinieneś zobaczyć następujący przegląd:



W zależności od rodzaju urządzenia, które ma zostać zarejestrowane, należy przeprowadzić następujące konfiguracje:

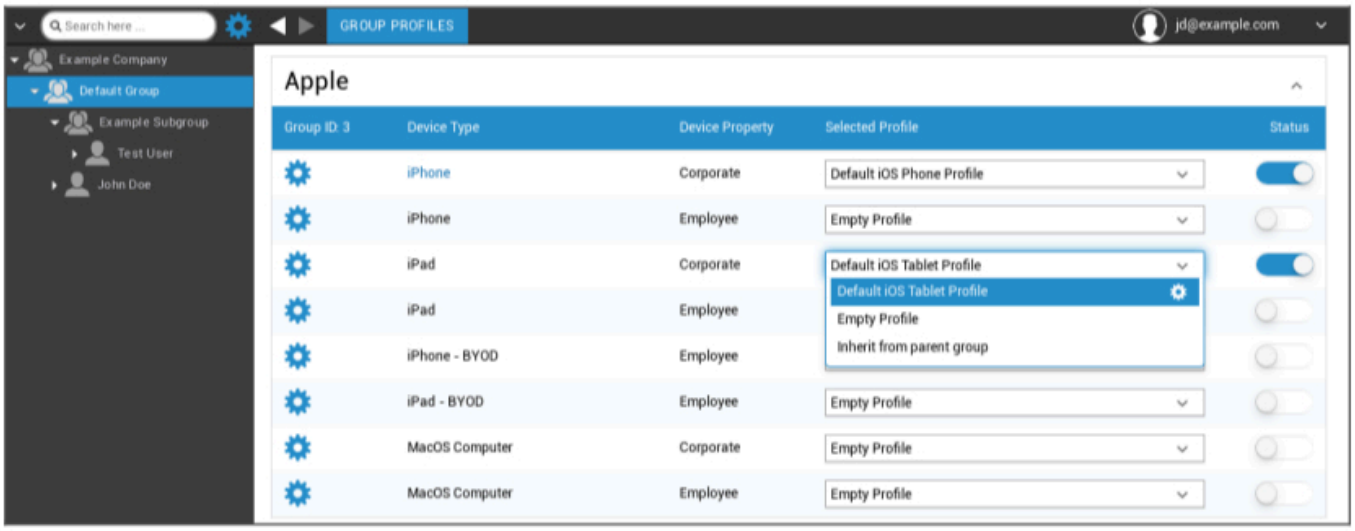
Wybrany użytkownik	Wybrany użytkownik (zostanie wypełniony automatycznie)
Nazwa urządzenia	Zostanie wypełniony automatycznie (urządzenie dla "nazwy użytkownika") - można go jednak zmienić.
Numer telefonu	Numer telefonu, zostanie wypełniony automatycznie (o ile został podany przez użytkownika) - tutaj jednak można go dodać lub zmienić.
Alternatywny e-mail	Alternatywny adres e-mail, zostanie wypełniony automatycznie (o ile został podany przez użytkownika) - tutaj jednak można go dodać lub zmienić.
Właściciel urządzenia	Własność korporacyjna = urządzenie korporacyjne Własność pracownika = urządzenie BYOD
Wybierz system operacyjny	Tutaj można wybrać jeden z następujących systemów operacyjnych: • iOS • iOS BYOD (rejestracja użytkowników) • macOS • Android Enterprise • Android • Windows Mobile • Windows 10
Wysłać prośbę o rejestrację?	Wiadomość e-mail jest wysyłana natychmiast na główny adres e-mail, a użytkownik jest proszony o podłączenie urządzenia
Wysłać prośbę na alternatywny adres e-mail?	Wyślij wiadomość e-mail dodatkowo lub wyłącznie (w przypadku, gdy opcja "Wyślij prośbę o rejestrację?" została wyłączona) na alternatywny adres e-mail (adres e-mail różni się od "normalnego" adresu e-mail z prośbą o rejestrację).
Wysłać SMS rekrutacyjny?	Wyślij prośbę o rejestrację za pośrednictwem wiadomości SMS (należy wprowadzić "Numer telefonu").

Po wysłaniu żądania rejestracji urządzenie zostanie natychmiast wyświetlone (zaznaczone na czerwono).

Gdy tylko urządzenie zostanie pomyślnie podłączone, wkrótce potem zostanie oznaczone kolorem zielonym i będzie gotowe do odbierania ograniczeń, aplikacji itp.

Zarządzanie profilami w zarządzaniu urządzeniami mobilnymi

Po kliknięciu grupy zostanie wyświetlony przegląd wszystkich platform urządzeń, które mają zostać skonfigurowane, oraz odpowiednio przypisanych profili.



	Przeprowadzenie konfiguracji dla wybranego profilu
Typ urządzenia	Typ i/lub model urządzenia
Właściwość urządzenia	Właściciel urządzenia (korporacyjny = własność korporacyjna, pracownik = prywatne urządzenie pracownika)
Wybrany profil	Wybrany profil (koło zębate otwiera okno dialogowe konfiguracji profilu)
Status	On/Off (profil jest włączony/wyłączony)

Po wybraniu biegu dostępne będą następujące opcje:

Utwórz profil

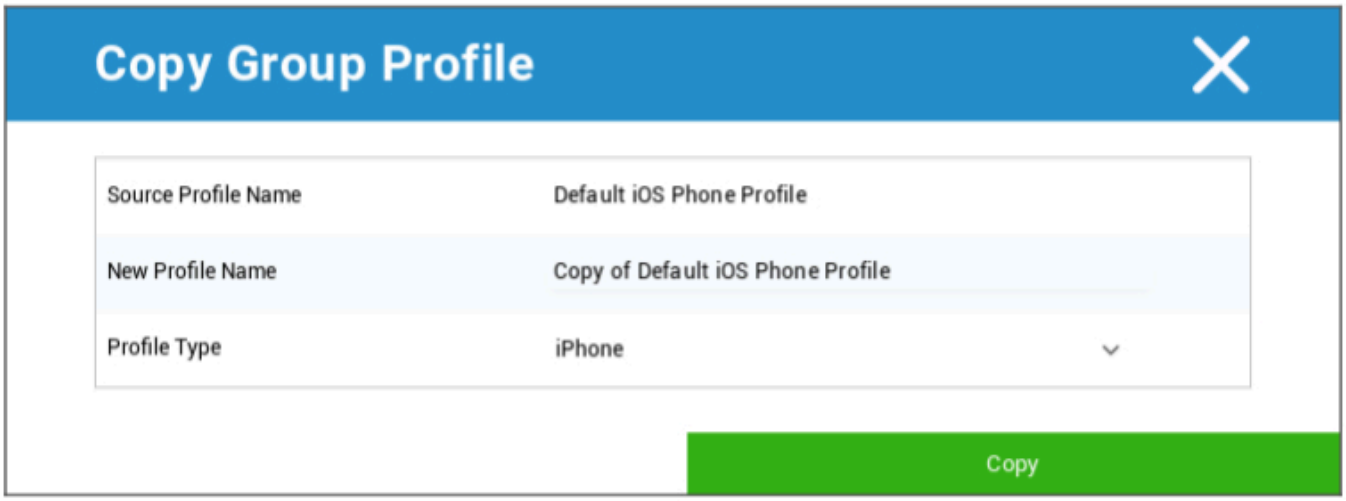
Można utworzyć i skonfigurować nowy profil dla każdego wpisu i/lub platformy. Po kliknięciu tego podpunktu profil zostanie utworzony natychmiast i można od razu rozpocząć konfigurację systemu iOS, Android i Windows Phone.

Edytuj profil

Po kliknięciu przycisku "Edytuj profil" zostanie wyświetlony ekran konfiguracji danego profilu, w którym można ustawić konfiguracje.

Kopiuj profil

Za pomocą funkcji "Kopiuj profil" można skopiować ustawienia/konfiguracje z już istniejącego profilu i dodać je do nowego profilu.

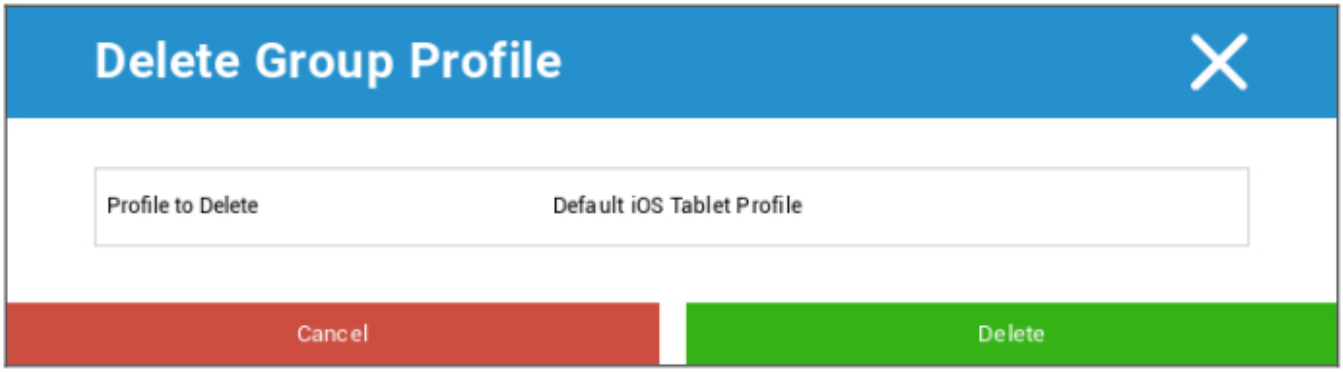


Nazwa profilu źródłowego	Nazwa profilu, który ma zostać skopiowany
Nowa nazwa profilu	Nazwa nowego profilu
Typ profilu	Typ profilu (telefon/tablet)

Po kliknięciu przycisku "Kopiuj" profil zostanie utworzony i będzie można go przypisać do grupy.

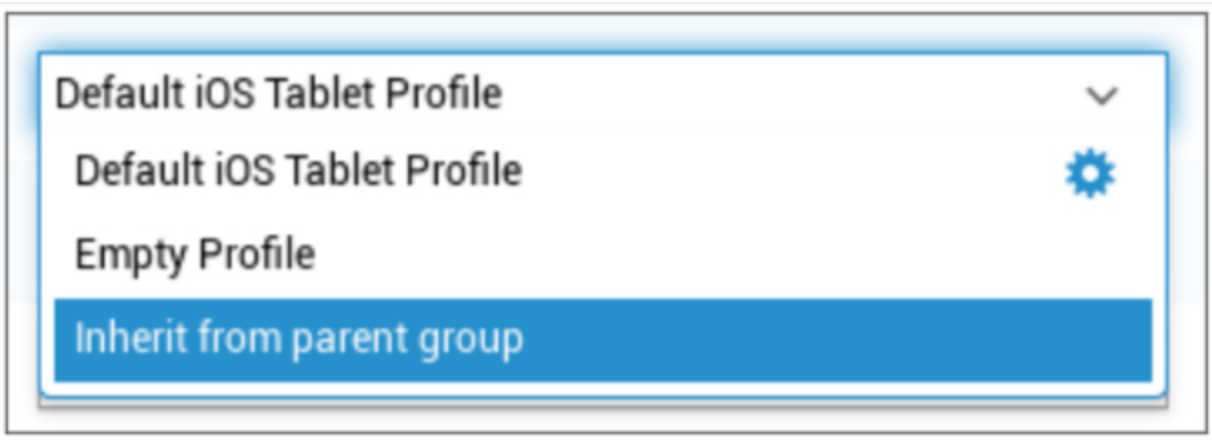
Usuń profil

Tutaj można trwale usunąć profil. Należy pamiętać, że podczas procesu usuwania i następującego po nim procesu "Przypisz teraz" dla profilu, konfiguracja zniknie na odpowiednich urządzeniach danej grupy i nie będzie można jej odzyskać!


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

Dziedziczenie profili

Podczas wyboru profili dostępna jest opcja "Dziedzicz z grupy nadrzędnej".



Gdy profil zostanie aktywowany, profil grupy nadrzędnej zostanie użyty dla odpowiednio wybranego urządzenia (i odpowiedniego typu urządzenia). Należy również pamiętać, że zmiany w tym profilu mogą mieć wpływ na wiele grup.

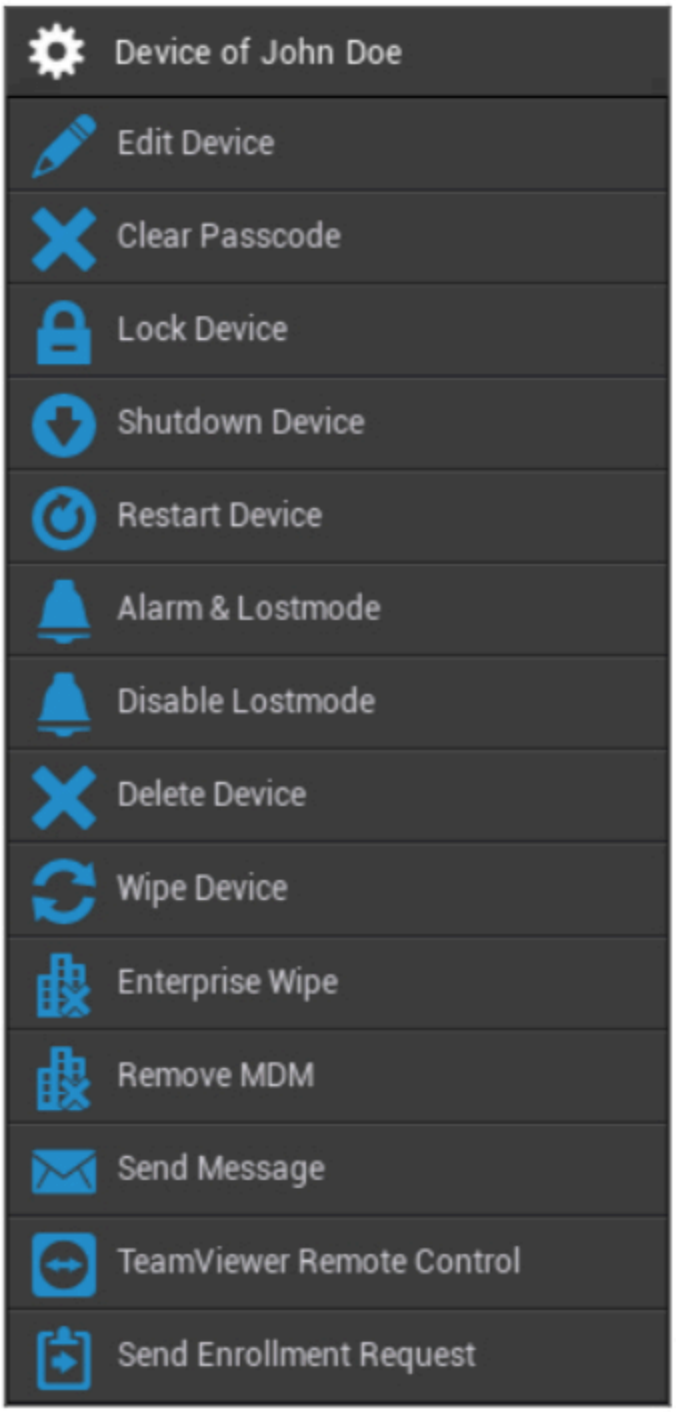
Ta konfiguracja jest ustawiana jako wartość domyślna, gdy tworzona jest nowa podgrupa.

Dostępna jest również konfiguracja "Pusty profil", która odpowiada pustemu profilowi, co oznacza, że ostatecznie na urządzeniu użytkownika końcowego nie zostaną przeprowadzone żadne nowe konfiguracje.

Zarządzanie urządzeniami w zarządzaniu urządzeniami mobilnymi

Po wybraniu urządzenia można wykonywać różne zadania za pomocą "koła zębatego". Są one różne w zależności od platformy systemu operacyjnego (iOS, Android Enterprise, Android, Windows Mobile, Windows 10).

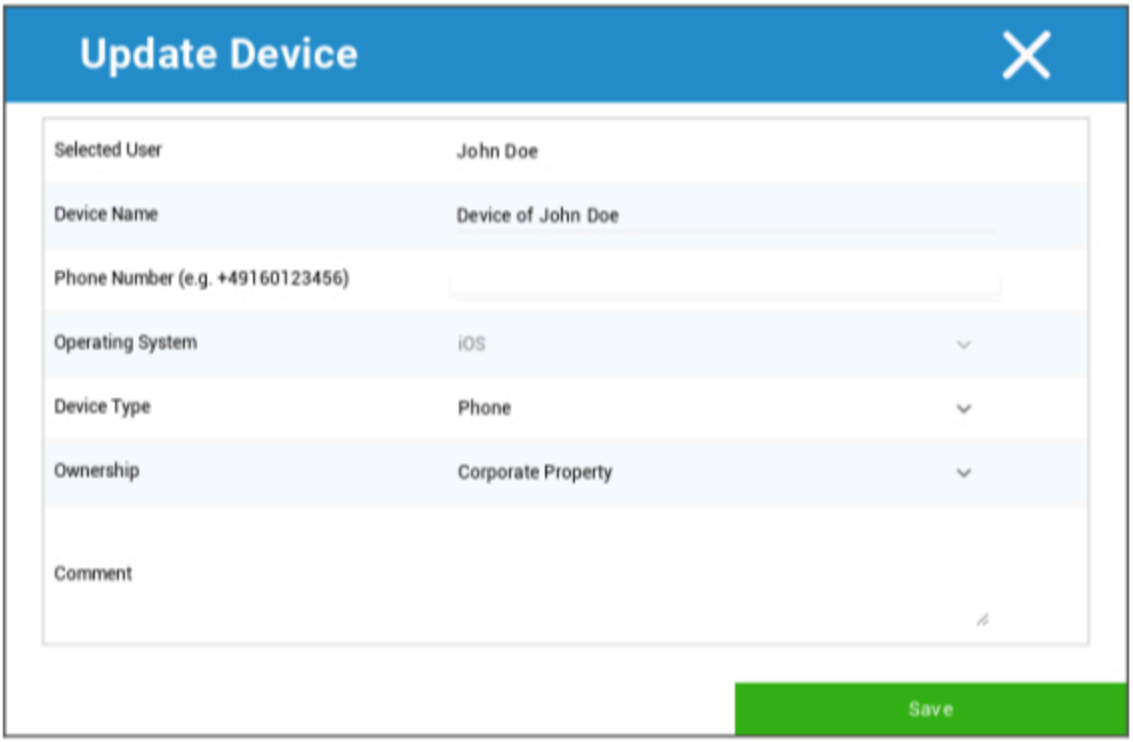
IOS



Edytuj urządzenie	Edytuj urządzenie
Wyczyść kod dostępu	Kod urządzenia zostanie usunięty
Urządzenie blokujące	Blokada urządzenia (ekran blokady)
Urządzenie wyłączające	Urządzenie wyłączające

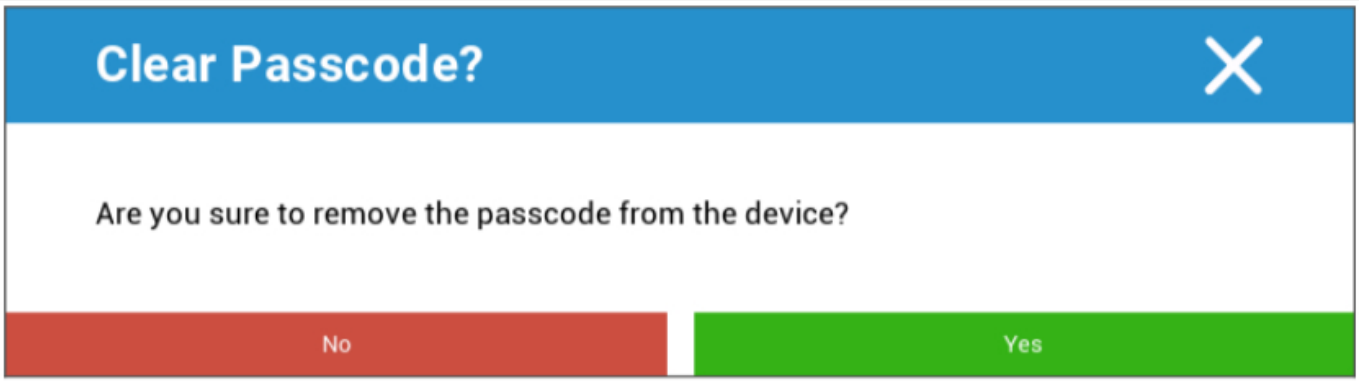
Restart urządzenia	Uruchom ponownie urządzenie
Alarm i Lostmode	Uruchom alarm i tryb Lostmode
Wyłącz tryb Lostmode	Wyłącz tryb Lostmode
Usuń urządzenie	Usuń urządzenie z AppTec
Czyszczenie urządzenia	Przywracanie ustawień fabrycznych urządzenia
Enterprise Wipe	Informacje, aplikacje i profile dostarczone przez AppTec360 są usuwane (urządzenie jest oddzielone od MDM).
Usuń MDM	
Wyślij wiadomość	Wysyłanie powiadomień push do urządzenia Wiadomość zostanie wyświetlona w aplikacji AppTec360 (zakładka Wiadomość).
Zdalne sterowanie TeamViewer	Rozpoczęcie sesji zdalnego sterowania przy użyciu TeamViewer
Wyślij prośbę o rejestrację	Wyślij (powtórzone) żądanie rejestracji

Edytuj urządzenie



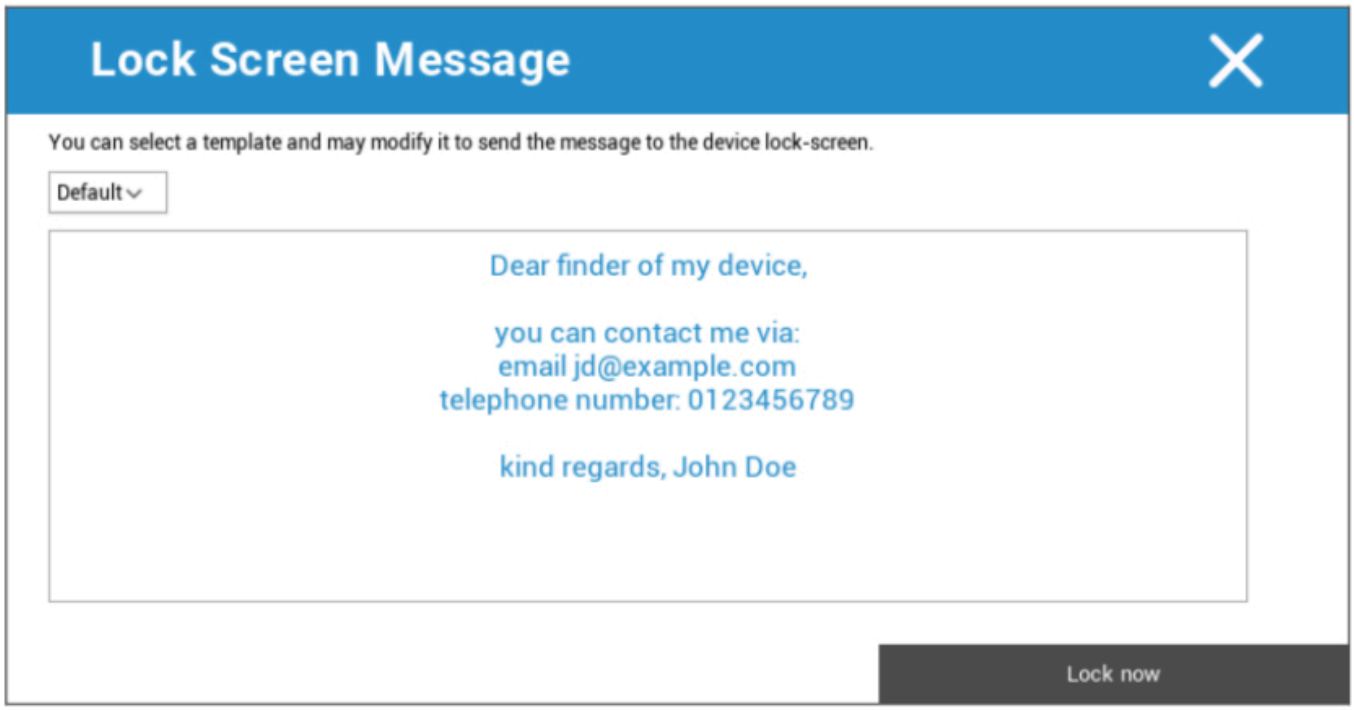
Tutaj można zaktualizować różne informacje o urządzeniu.

Wyczyść kod dostępu



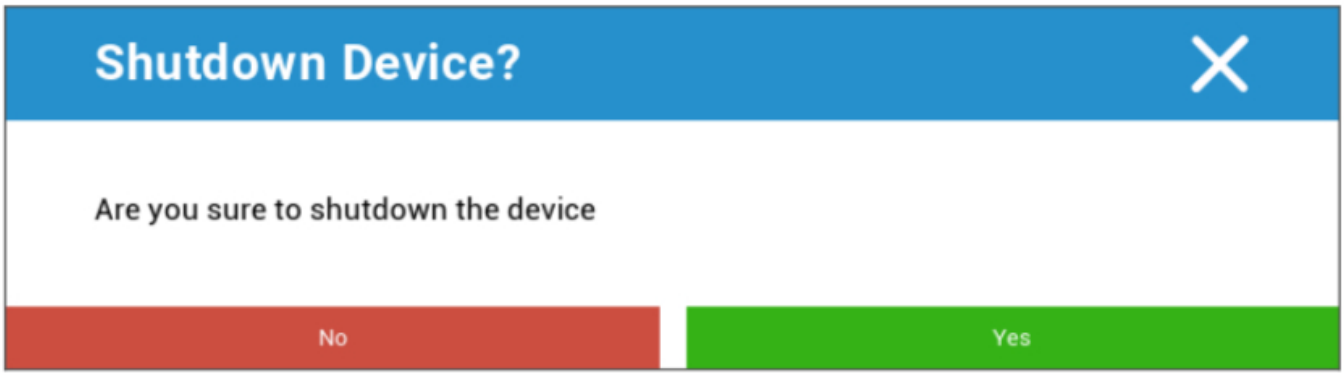
W sekcji "Wyczyść hasło" można zdalnie usunąć hasło z urządzenia. Następnie użytkownik zostanie poproszony o podanie nowego hasła (w zależności od wytycznych Passcode).

Urządzenie blokujące



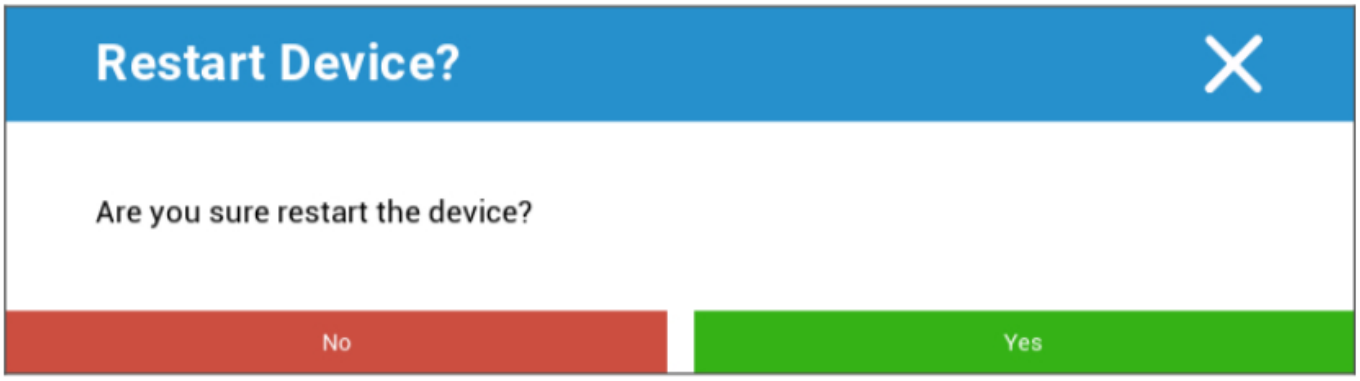
Tutaj polecenie blokady jest wysyłane do urządzenia użytkownika końcowego (ekran blokady).

Urządzenie wyłączające



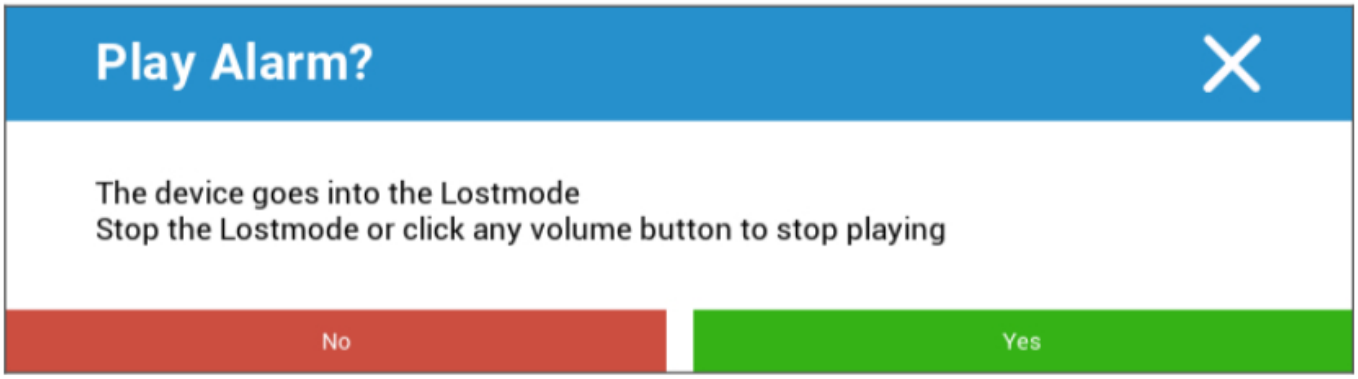
Tutaj polecenie wyłączenia jest wysyłane do urządzenia użytkownika końcowego.

Restart urządzenia

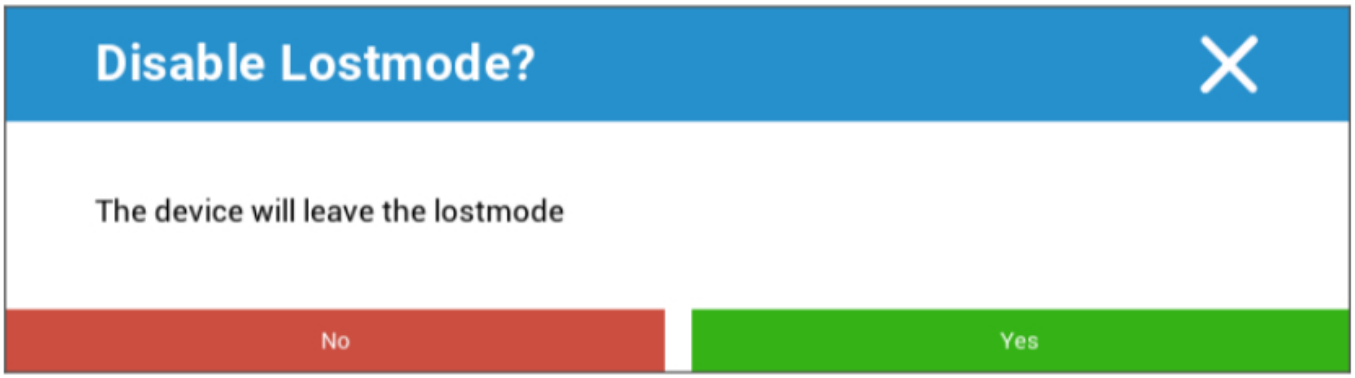


Tutaj polecenie restartu jest wysyłane do urządzenia użytkownika końcowego.

Alarm i tryb utracony | Wyłącz tryb utracony



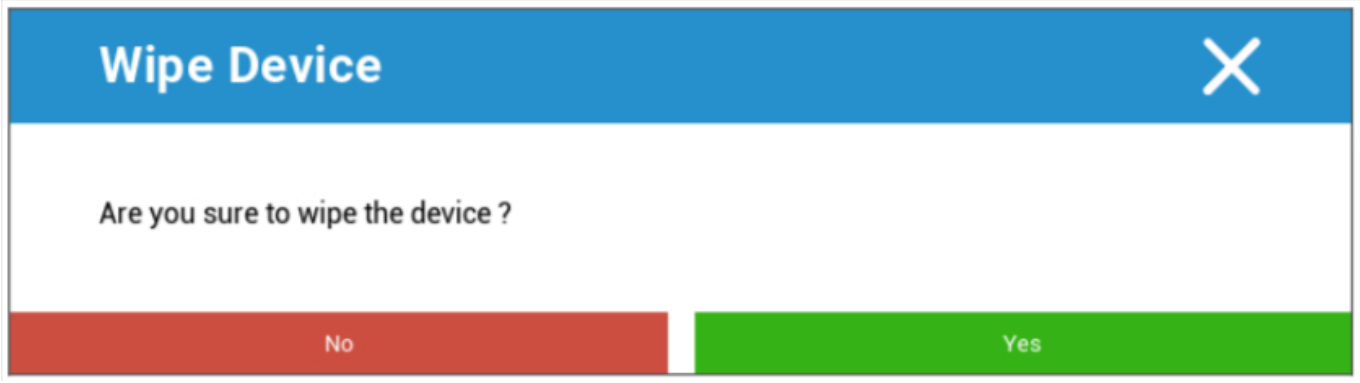
Tutaj urządzenie można ustawić w tryb Lostmode, który ustawia urządzenie na ciągłe odtwarzanie dźwięku alarmu. Tryb Lostmode można wyłączyć, naciskając dowolny przycisk głośności urządzenia lub zdalnie, klikając opcję "Disable Lostmode":



Usuń urządzenie

Tutaj można wykonać polecenie usunięcia. Możesz ponownie zdecydować, czy urządzenie ma zostać usunięte tylko z AppTec360 ("Delete from System"), czy też urządzenie ma zostać usunięte z AppTec360 i przywrócone do ustawień fabrycznych ("Wipe & Delete").

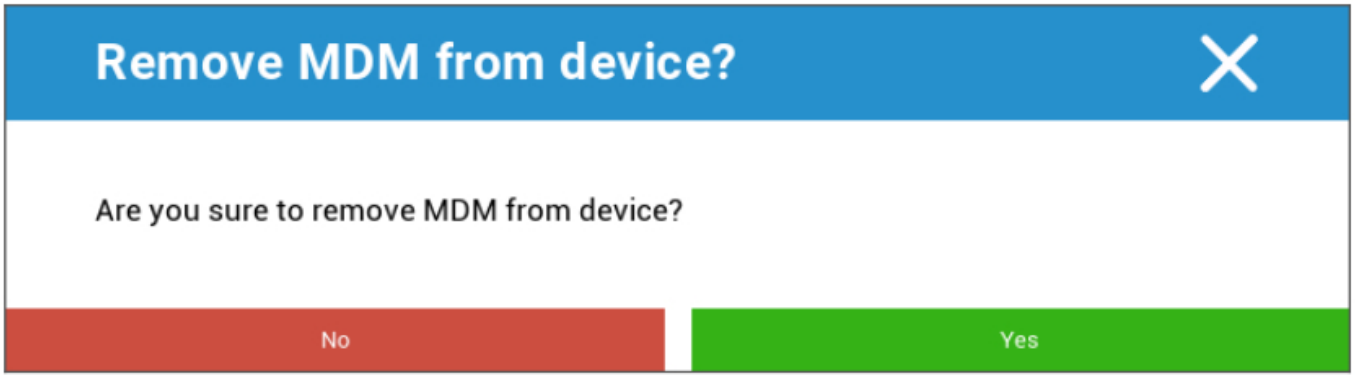
Czyszczenie urządzenia



W sekcji "Wipe Device" (Wyczyść urządzenie) można wykonać całkowite czyszczenie urządzenia. Urządzenie zostanie przywrócone do ustawień fabrycznych.

Enterprise Wipe | Usuń MDM

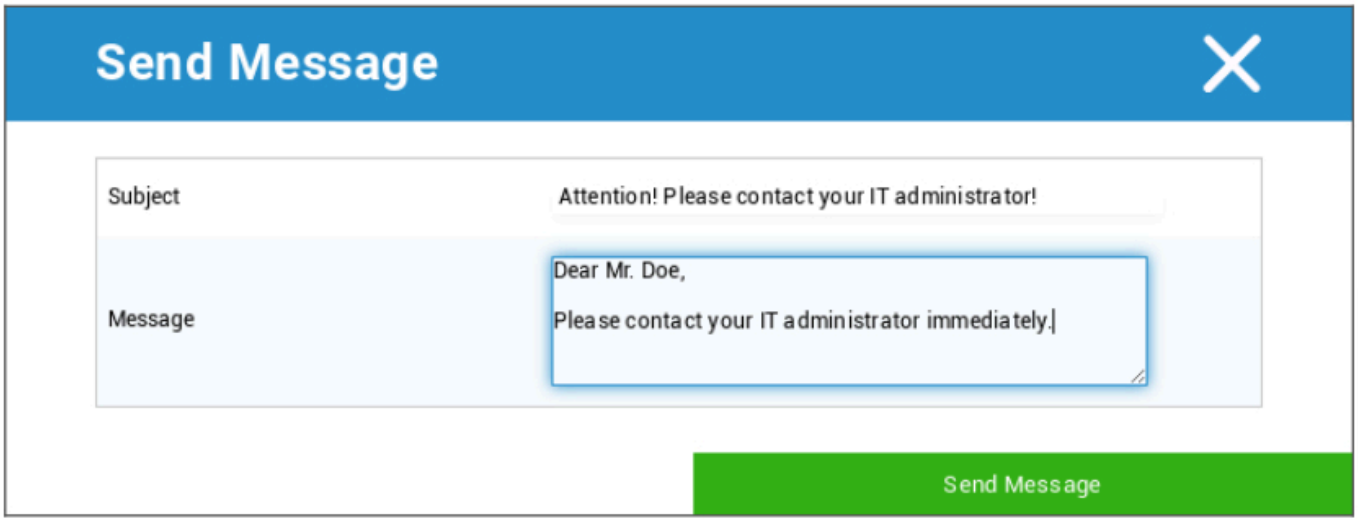
Usuwane są tylko informacje, aplikacje i profile dostarczone przez AppTec360. W ten sposób dane firmowe nie będą już dostępne na urządzeniu użytkownika końcowego. Obszar prywatny pozostaje nienaruszony i nadal pozostaje na urządzeniu użytkownika końcowego.



Za pomocą opcji "Remove MDM" można usunąć profil MDM na urządzeniu użytkownika końcowego i wszystkie inne elementy dostarczone przez AppTec.

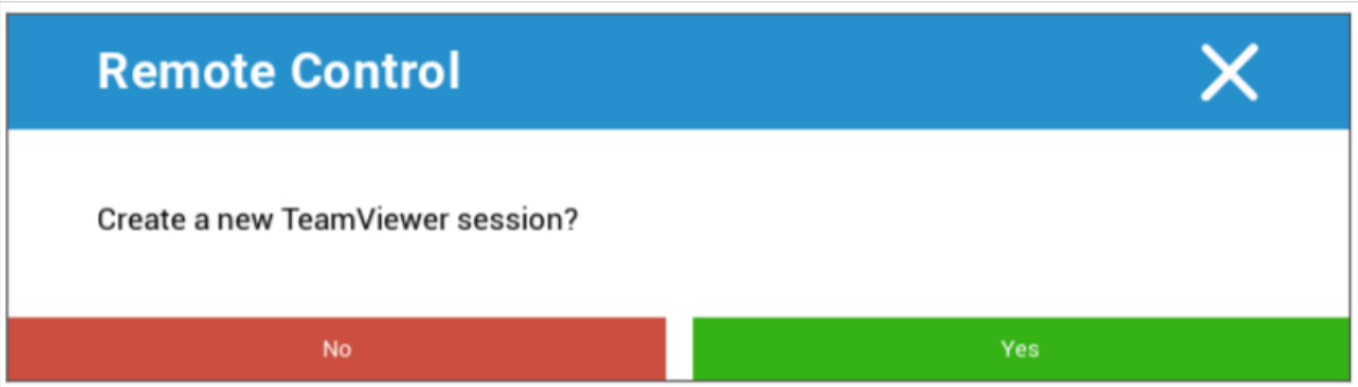
Polecenie to wykonuje tę samą czynność, co "Enterprise Wipe".

Wyślij wiadomość



W tym miejscu można wysłać powiadomienie Push na odpowiednie urządzenie.

Zdalne sterowanie TeamViewer



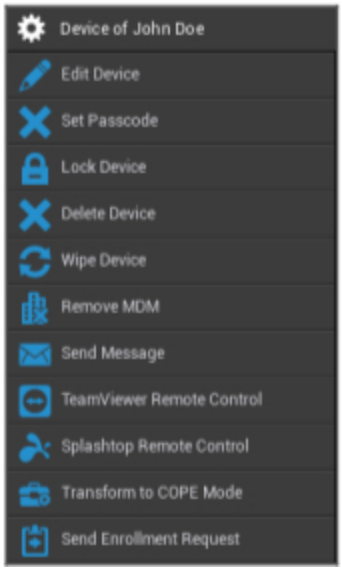
Tutaj można rozpocząć sesję zdalnego sterowania Teamviewer.

Wyślij prośbę o rejestrację

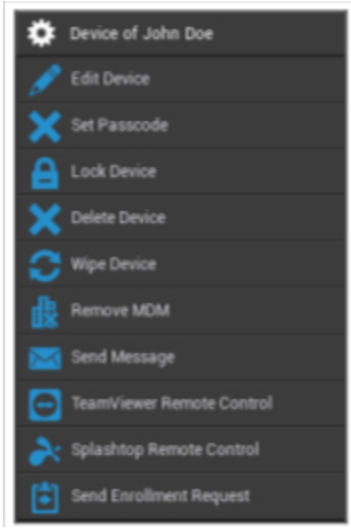
Za pomocą opcji "Send Enrollment Request" (Wyślij prośbę o rejestrację) można wysłać prośbę o rejestrację (ponownie) do danego użytkownika.

Android

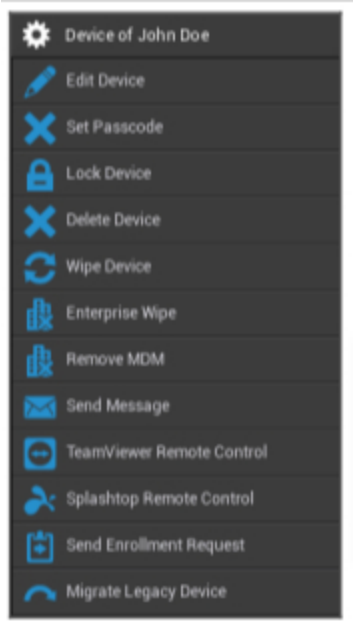
W pełni zarządzane urządzenie AE (Work Managed)



Profil pracy AE (kontener)



Telefon | Tablet z systemem Android

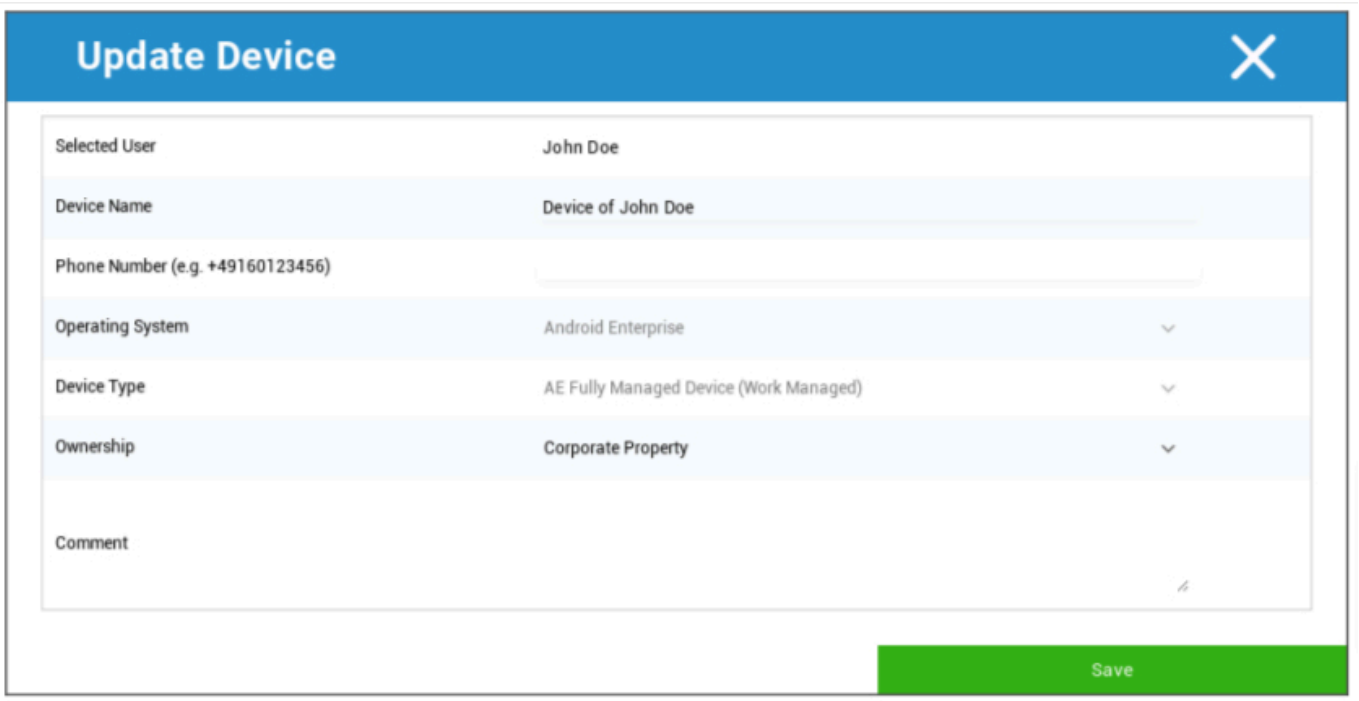


Edytuj urządzenie	Edycja informacji o urządzeniu
Ustawianie kodu dostępu	Ustawianie hasła urządzenia
Urządzenie blokujące	Blokada urządzenia (ekran blokady)
Usuń urządzenie	Usuń urządzenie z AppTec
Czyszczenie urządzenia	Przywracanie ustawień fabrycznych urządzenia
Enterprise Wipe	Informacje, aplikacje, profile dostarczane przez AppTec360 są usuwane (urządzenie zostanie oddzielone od MDM).
Usuń MDM	
Wyślij wiadomość	Wysyłanie powiadomień Push do urządzenia Wiadomość zostanie wyświetlona w aplikacji AppTec360 (zakładka Wiadomość).
Zdalne sterowanie TeamViewer	Uruchom sesję zdalnego sterowania dla tego urządzenia za pomocą TeamViewer
Pilot zdalnego sterowania Splashtop	Uruchom sesję zdalnego sterowania dla tego urządzenia za pomocą Splashtop
Przekształcenie w tryb COPE (tylko na w pełni zarządzanym urządzeniu AE (Work Managed))	Utwórz profil roboczy na tym w pełni zarządzanym urządzeniu AE (Work Managed)

Wyślij prośbę o rejestrację	Wyślij (powtórzone) żądanie rejestracji
Migracja starszego urządzenia (tylko na telefonie / tablecie z systemem Android, jeśli zarejestrowano je przy użyciu udostępniania w trybie właściciela urządzenia)	Migracja profilu telefonu / tabletu z systemem Android do profilu w pełni zarządzanego urządzenia AE (Work Managed)

Edytuj urządzenie

Tutaj można zaktualizować różne informacje o urządzeniu.



Wybrany użytkownik	Użytkownik urządzenia
Nazwa urządzenia	Nazwa urządzenia
Numer telefonu	Numer telefonu urządzenia
System operacyjny	Android Enterprise Android
Typ urządzenia	Android Enterprise: • W pełni zarządzane urządzenie AE (Work Managed) • Tryb profilu roboczego AE (tylko kontener) • AE W pełni zarządzane urządzenie z profilem pracy (COPE) Android: • Telefon • Tablet
Własność	Korporacyjny = własność korporacyjna

	Pracownik = właściwość pracownika
Komentarz	Dodatkowe opisy urządzenia

Wyczyść kod dostępu

Tutaj można usunąć hasło urządzenia na wybranym urządzeniu. Domyślnie w systemie Android hasło będzie ustawione na "123456" - użytkownik może i powinien je później zmienić.

Urządzenie blokujące

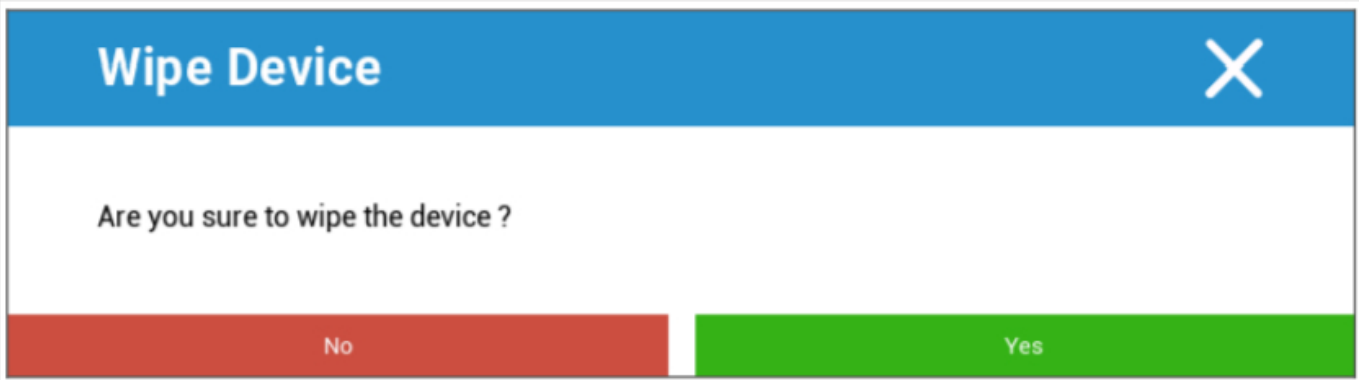
W tym miejscu do urządzenia zostanie wysłane polecenie blokady urządzenia (ekranu blokady).

Usuń urządzenie

Tutaj można wykonać polecenie usunięcia. Możesz ponownie zdecydować, czy urządzenie ma zostać usunięte tylko z AppTec360 ("Delete from System"), czy też urządzenie ma zostać usunięte z AppTec360 i dodatkowo przywrócone do ustawień fabrycznych ("Wipe & Delete").

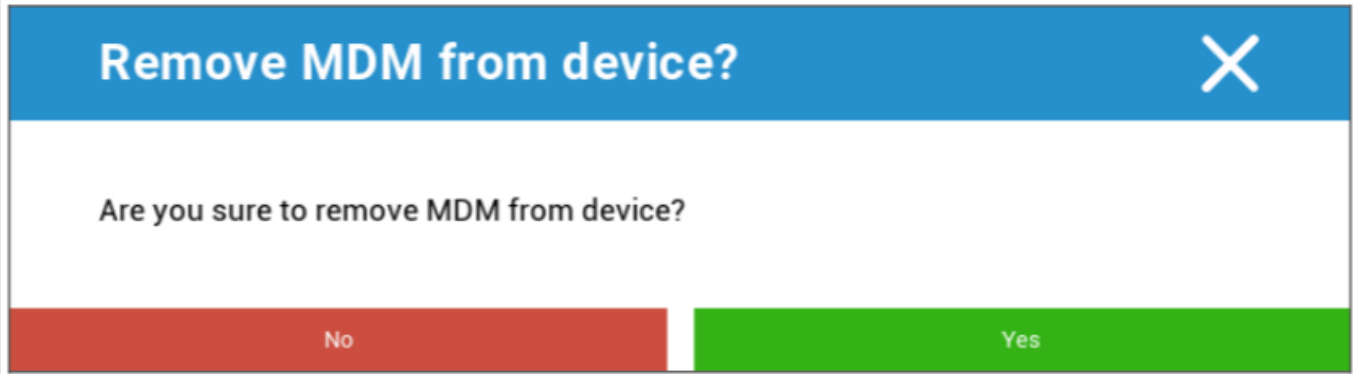
Czyszczenie urządzenia

W sekcji "Wipe Device" można wykonać całkowite wyczyszczenie urządzenia. Urządzenie zostanie przywrócone do ustawień fabrycznych.



Dodatkowo, jeśli urządzenie zawiera kartę SD, można ją wymazać. Można to zrobić, ustawiając opcję "Wyczyścić również kartę SD? " na "Wł.".

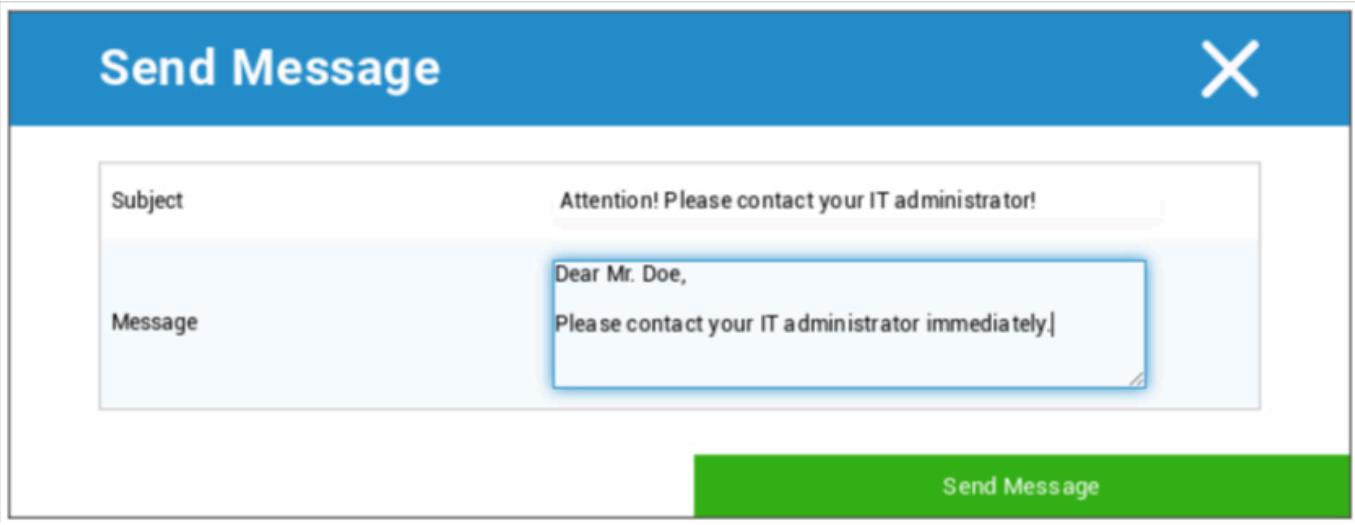
Usuń MDM



Jest to zalecana metoda tworzenia separacji od MDM.

Usuwane są tylko informacje, aplikacje i profile dostarczone przez AppTec360, co oznacza, że wszystkie dane firmowe nie będą już dostępne na urządzeniu użytkownika końcowego. Nie ma to jednak wpływu na sferę prywatną, która nadal pozostaje na urządzeniu użytkownika końcowego.

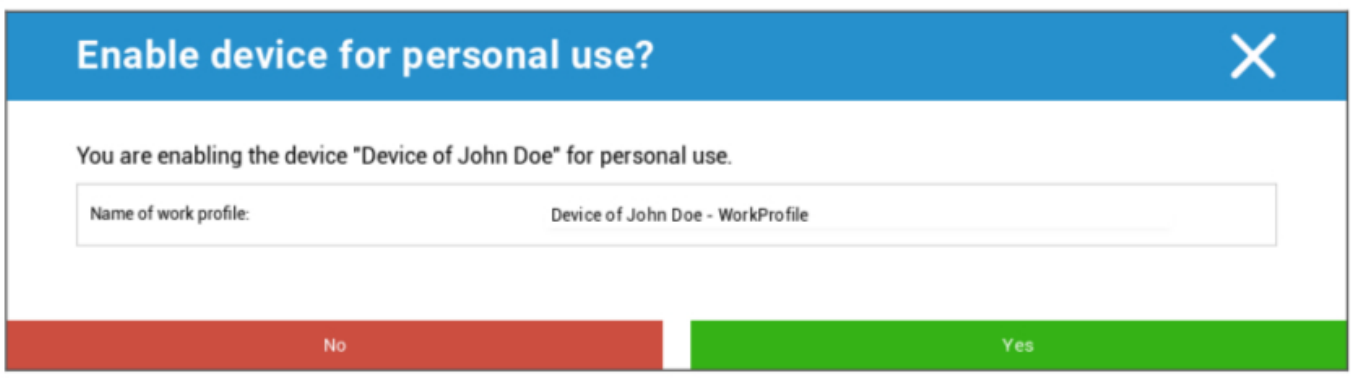
Wyślij wiadomość



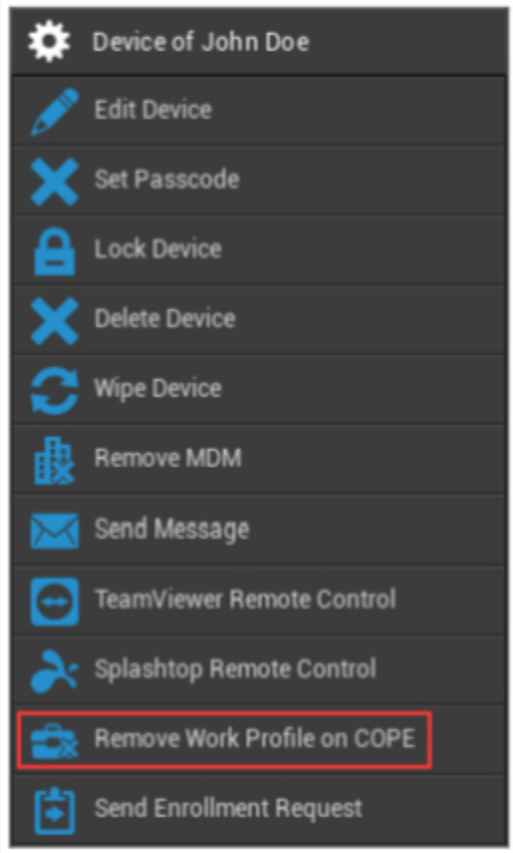
W tym miejscu można wysłać powiadomienie Push na odpowiednie urządzenie użytkownika końcowego.

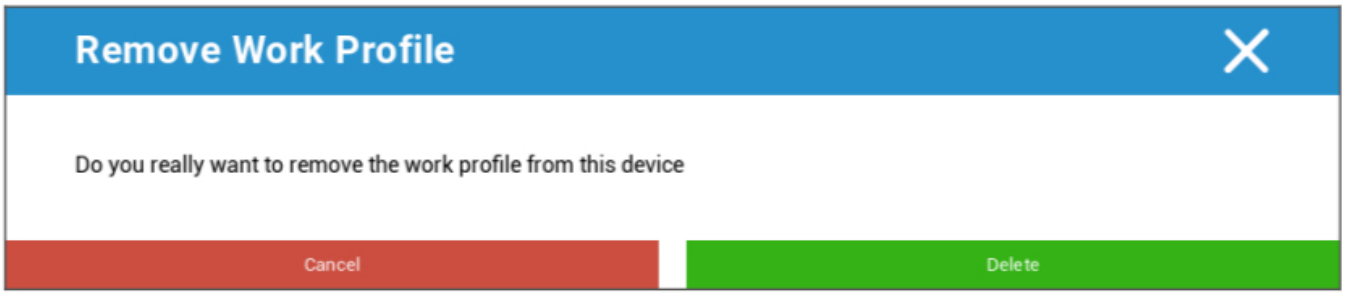
Przekształcenie w tryb COPE

Utwórz profil roboczy na tym w pełni zarządzanym urządzeniu AE (Work Managed)



Po przekształceniu urządzenia w tryb **COPE** można usunąć profil roboczy, klikając opcję koła zębatego **Usuń profil roboczy w COPE:**




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

Wyślij prośbę o rejestrację

Za pomocą opcji "Send Enrollment Request" (Wyślij prośbę o rejestrację) można wysłać prośbę o rejestrację (ponownie) do danego użytkownika.

Należy pamiętać, że ważny jest tylko najnowszy wniosek o rejestrację.

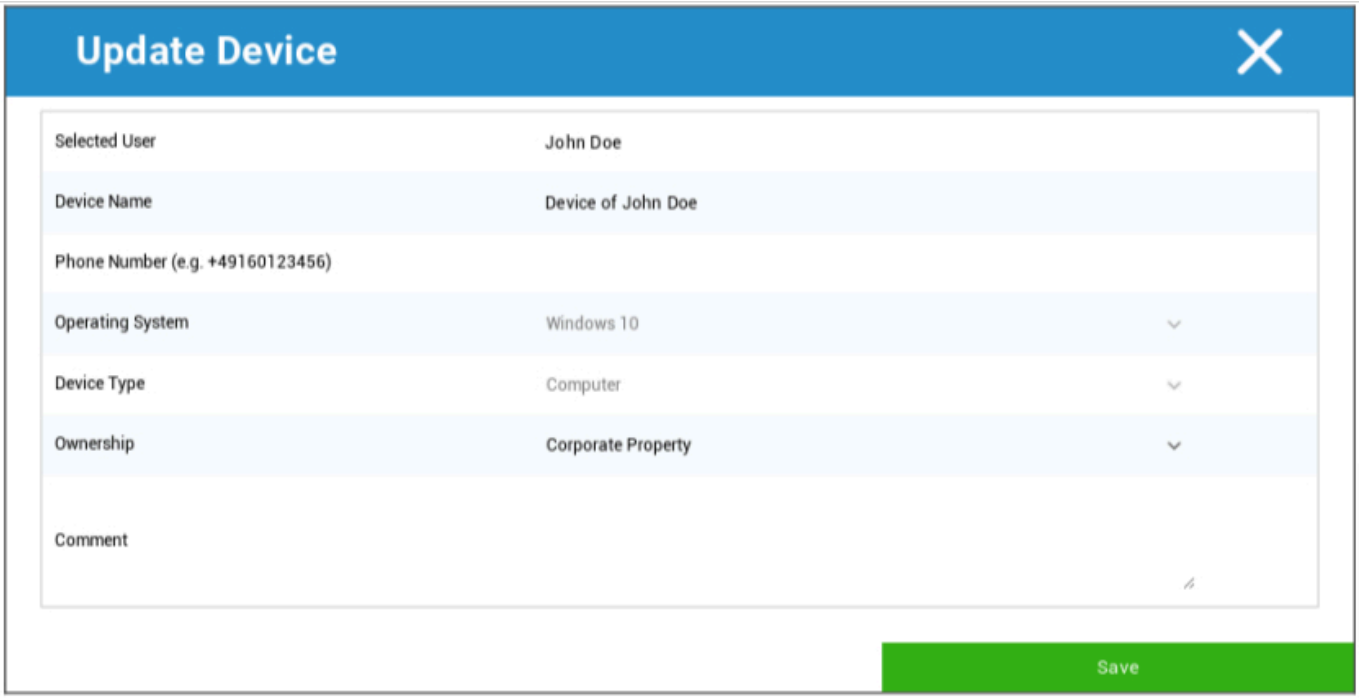
Migracja starszego urządzenia

Migracja profilu telefonu / tabletu z systemem Android do profilu w pełni zarządzanego urządzenia AE (Work Managed)

Windows

Nazwa urządzenia	Nazwa wybranego urządzenia
Edytuj urządzenie	Edytuj urządzenie
Usuń urządzenie	Usuń urządzenie z AppTec
Enterprise Wipe	Informacje, aplikacje i profile dostarczone przez AppTec360 są usuwane
Usuń MDM	
Zdalne sterowanie TeamViewer	Zdalne sterowanie urządzeniem za pomocą TeamViewer
Wyślij prośbę o rejestrację	Wyślij żądanie rejestracji (ponownie)

Edytuj urządzenie

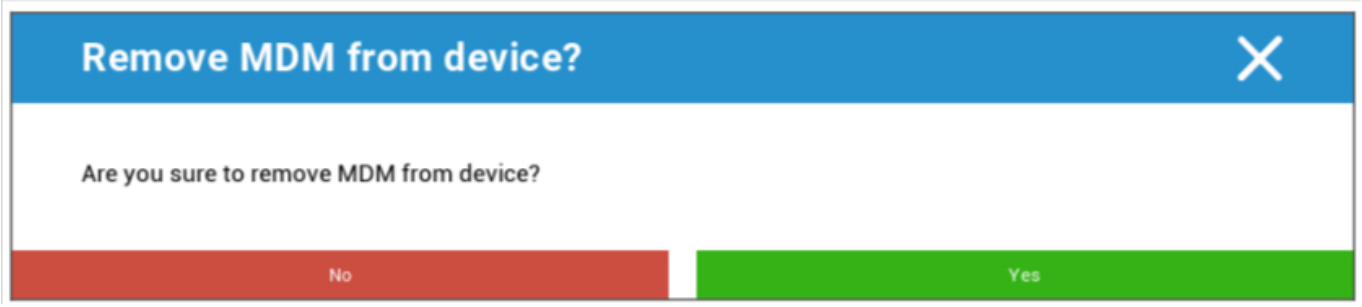


Tutaj można zaktualizować różne informacje o urządzeniu.

Usuń urządzenie

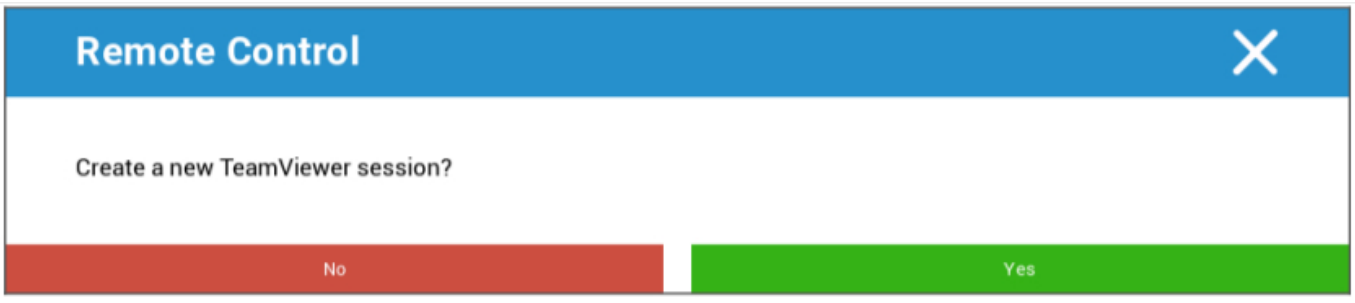
Tutaj można wykonać polecenie usuwania, które usuwa urządzenie z AppTec360.

Enterprise Wipe | Usuń MDM



Usuwane są tylko informacje, aplikacje i profile dostarczone przez AppTec360. W ten sposób dane firmowe nie będą już dostępne na urządzeniu użytkownika końcowego. Obszar prywatny pozostaje nienaruszony i nadal pozostaje na urządzeniu użytkownika końcowego.

Zdalne sterowanie TeamViewer



Tutaj możesz rozpocząć sesję zdalnego sterowania TeamViewer dla tego urządzenia.

Wyślij prośbę o rejestrację

Za pomocą opcji "Send Enrollment Request" (Wyślij prośbę o rejestrację) można wysłać prośbę o rejestrację (ponownie) do danego użytkownika.

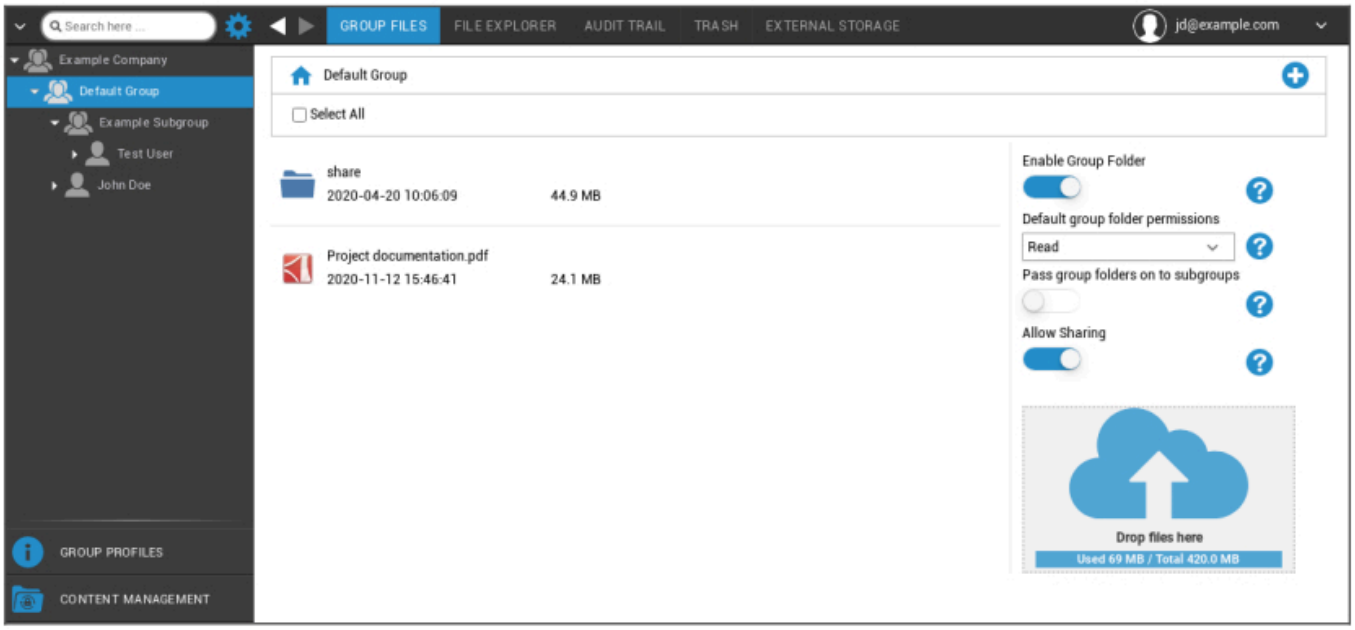
Zarządzanie treścią

Gdy jesteś w grupie, możesz zarządzać AppTec ContentBox za pomocą "Content Management".

Content Box umożliwia bezpieczną dystrybucję dokumentów i innych danych firmowych na urządzenia użytkowników końcowych.

Pliki grupowe

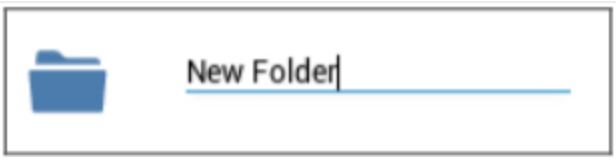
"Pliki grupowe" stanowią podstawową część ContentBox. Tutaj można wprowadzać ustawienia, przesyłać dokumenty, tworzyć nowe foldery itp.



Za pomocą symbolu w prawym górnym rogu można tworzyć nowe foldery, które są przypisane do odpowiedniej grupy za pomocą opcji "Dodaj folder".

Za pomocą symbolu w prawym górnym rogu można utworzyć nowy folder za pomocą opcji "Dodaj folder", który należy przypisać do odpowiedniej grupy.

Folderowi można nadać dowolną nazwę.



Poprzez "Upload Files" można przesyłać dane. Tutaj zostanie otwarty Standard-Explorer. Te dwie czynności można oczywiście wykonać w każdym (pod)folderze.

Za pomocą symbolu w lewym górnym rogu można powrócić do menu głównego.

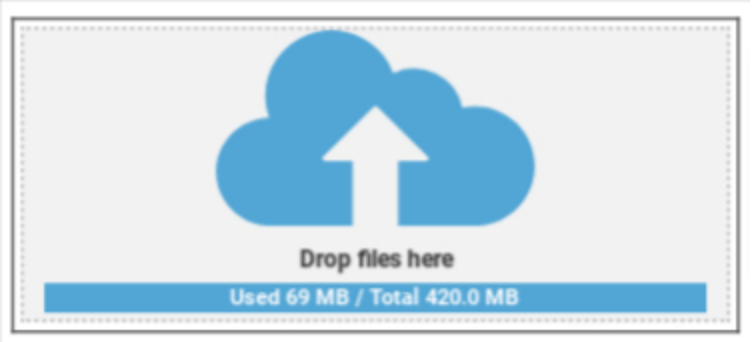
Możesz wybrać kilka folderów i plików i pobrać je klikając "Pobierz" lub usunąć je klikając "Usuń".

Można również zaznaczyć wszystkie pliki i foldery i wykonać polecenia "Pobierz" i "Usuń".

Po najechaniu myszą na folder lub plik wyświetlony zostanie następujący widok:

- Za pomocą opcji "Zmień nazwę" można zmienić nazwę folderu/pliku
- Za pomocą opcji "Pobierz" można pobrać folder/plik
- Za pomocą opcji "Usuń" można usunąć folder/plik

Włącz folder grupy	Jeśli jest aktywna, wszyscy członkowie grupy mają dostęp do danego folderu
Domyślne uprawnienia do folderów grupowych	Uprawnienia użytkowników w wybranej grupie: Read = uprawnienie tylko do odczytu Aktualizacja = uprawnienie do aktualizacji Utwórz = uprawnienie tworzenia Delete = uprawnienie do usuwania
Przekazywanie folderów grupowych do podgrup	Po aktywacji odpowiednie podgrupy mogą mieć dostęp do nadrzędnych plików danych
Uprawnienia dla podgrup	Uprawnienia użytkowników w wybranej podgrupie: Read = uprawnienie tylko do odczytu Aktualizacja = uprawnienie do aktualizacji Utwórz = uprawnienie tworzenia Delete = uprawnienie do usuwania
Zezwalaj na udostępnianie	Po aktywacji użytkownik może udostępniać pliki za pośrednictwem łącza



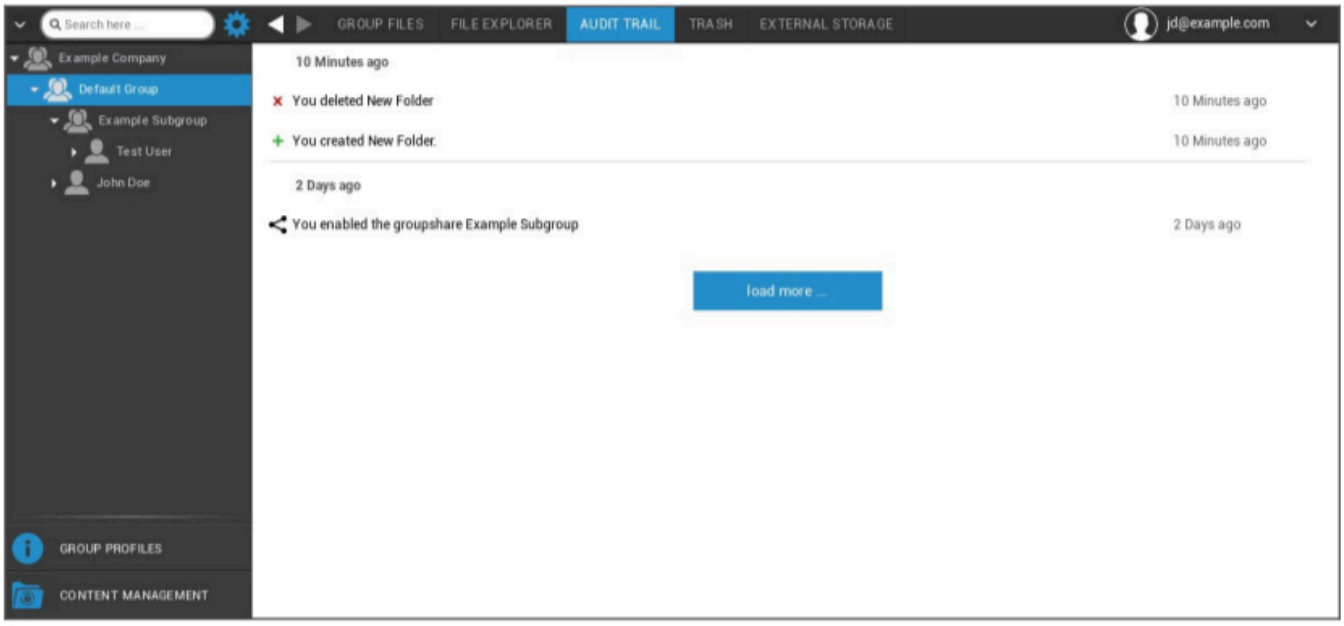
Aby przesłać pliki, można użyć tego pola, przeciągając plik metodą "przeciągnij i upuść" do tego okna. Można również kliknąć to pole, aby wybrać i przesłać plik za pomocą przeglądarki Internet Explorer.

Eksplorator plików

Za pomocą "Eksploratora plików" można zarządzać wszystkimi folderami i plikami - niezależnie od grupy, w której się znajdują.

Znajdziesz tu również ustawienia i przyciski, o których dowiedziałeś się w sekcji "Pliki grupowe".

Ścieżka audytu



W "Audit Trail" można zobaczyć z historii, który użytkownik co utworzył, usunął lub udostępnił. W ten sposób można w dowolnym momencie ustalić, co zostało zrobione z danymi firmowymi.

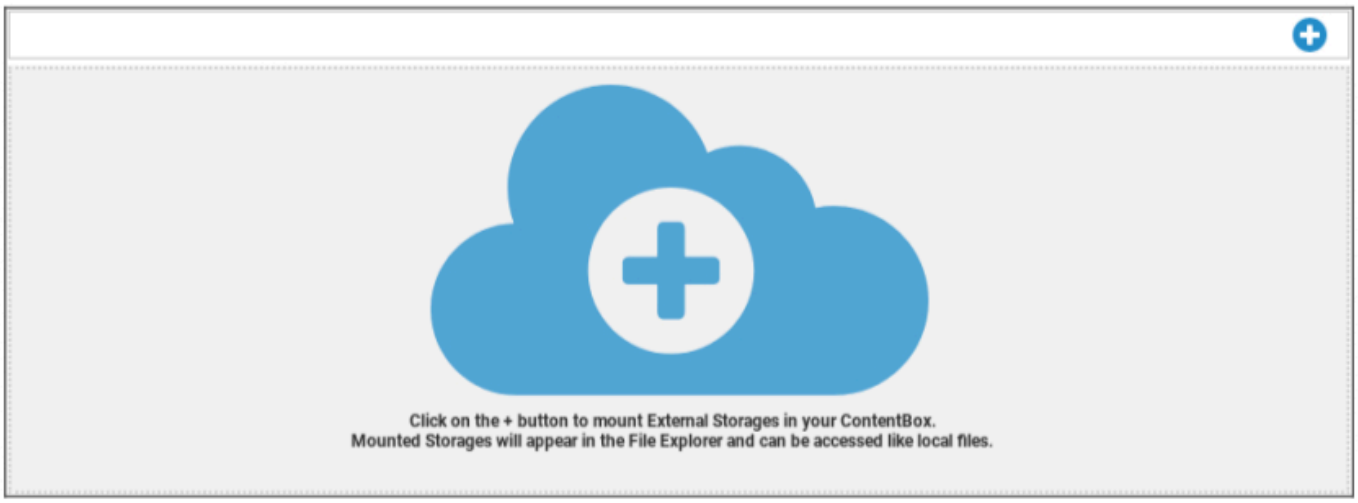
Śmieci

Jeśli coś zostało usunięte (przez przypadek), możesz zobaczyć foldery i pliki w "Koszu" i odzyskać je zgodnie z własnymi życzeniami.

- Dzięki funkcji "Cofnij usunięcie" można odzyskać dane/folder.
- Polecenie "Usuń" umożliwia trwałe usunięcie danych/folderu - należy ponownie potwierdzić polecenie usunięcia.

Należy pamiętać, że pojemność pamięci masowej wykorzystywana w koszu zmniejsza "Całkowitą dostępną przestrzeń" - jest to wymóg ownCloud.

Pamięć zewnętrzna



Pod nagłówkiem "External Storage" można podłączyć zewnętrzną pamięć masową.

Za pomocą symbolu można dodać (dodatkową) pamięć.

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

Amazon S3	
Wyświetlana nazwa	Wyświetlana nazwa
Klucz dostępu	Klucz dostępu
Tajny klucz	Klucz bezpieczeństwa
Wiadro	Określona tożsamość podfolderu, który został przypisany do użytkownika.
Nazwa hosta (opcjonalnie)	Nazwa hosta (opcjonalnie)
Port (opcjonalnie)	Port (opcjonalnie)
Region	Region (opcjonalnie)
Włącz SSL	Włącz SSL
Włącz styl ścieżki	Clear Path Address, który został przypisany do użytkownika

FTP	
Wyświetlana nazwa	Wyświetlana nazwa
Gospodarz	Adres hosta
Nazwa użytkownika	Nazwa użytkownika
Hasło	Hasło
Korzeń	Menu główne
Bezpieczny ftps://	

SFTP	
Wyświetlana nazwa	Wyświetlana nazwa
Gospodarz	Adres hosta
Nazwa użytkownika	Nazwa użytkownika
Hasło	Hasło
Korzeń	Menu główne

ownCloud	
Wyświetlana nazwa	Wyświetlana nazwa
URL	Adres URL ownCloud
Nazwa użytkownika	Nazwa użytkownika
Hasło	Hasło
Podfolder zdalny	Folder standardowy
Bezpieczne https://	

WebDAV	
Wyświetlana nazwa	Wyświetlana nazwa
URL	Adres URL WebDAV
Nazwa użytkownika	Nazwa użytkownika
Hasło	Hasło
Korzeń	Menu główne
Bezpieczne https://	
Windows Share	Wsparcie dla Windows Share będzie dostępne wkrótce
SharePoint	Wsparcie dla Microsoft SharePoint będzie dostępne wkrótce

Dziennik kontroli

Tutaj można znaleźć dziennik, który rejestruje informacje o działaniach wykonywanych w konsoli MDM.

Ikona filtra umożliwia zastosowanie filtrów do wyświetlanej listy.

Za pomocą rozwijanego menu **Items per page (Pozycje na stronę**) można wybrać liczbę pozycji wyświetlanych na jednej stronie listy.

Podjęte działania / zmienione ustawienia	Podjęte działanie / zmienione ustawienie
Wartość	Wartość podjętego działania / zmienionego ustawienia
Użytkownik	Nazwa użytkownika, który podjął działanie / zmienił ustawienie.
Data	Znacznik czasu, kiedy ta akcja została podjęta / to ustawienie zostało zmienione.
Ścieżka / Typ	Ścieżka do miejsca, w którym podjęto tę akcję / zmieniono to ustawienie.

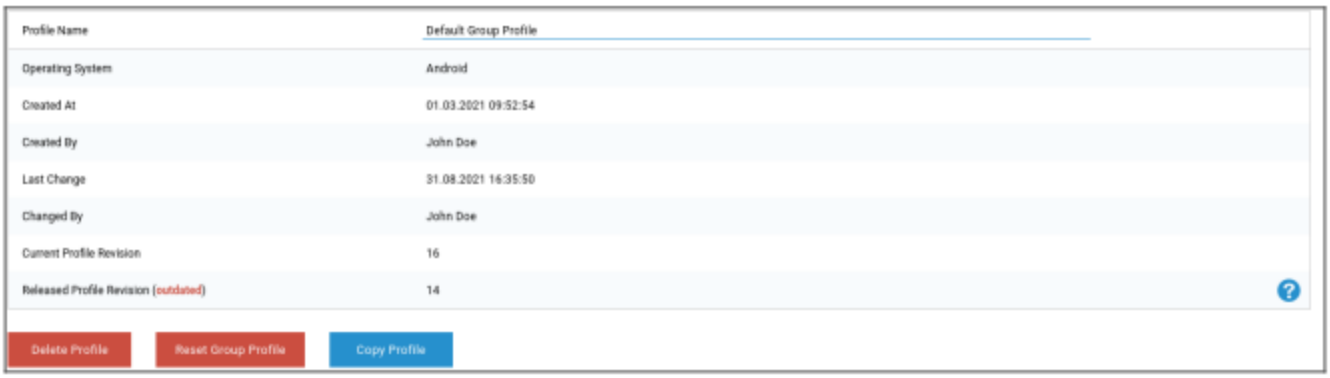
Konfiguracja iOS

Ogólne

W zależności od tego, czy aktualnie wybrano grupę, czy urządzenie, wyświetlacz i jego podpunkty różnią się - należy zwrócić na to szczególną uwagę!

Przegląd profilu grupy (tylko na poziomie grupy)

Po otwarciu profilu grupy wyświetlony zostanie szybki przegląd profilu



Nazwa profilu	Nazwa profilu (można ją zmienić tutaj)
System operacyjny	System operacyjny, dla którego przeznaczony jest profil
Utworzono w	Czas stworzenia
Utworzony przez	Twórca profilu
Ostatnia zmiana	Czas ostatniej zmiany profilu
Zmienione przez	Konto, które wprowadziło ostatnie zmiany
Aktualna wersja profilu	Zmiana zapisanego stanu profilu
Wydana wersja profilu	Wersja przypisanego profilu ("Przypisz teraz"). Jeśli etykieta pokazuje "(nieaktualne)" za tekstem, oznacza to, że profil został zapisany, ale nie został jeszcze przypisany, więc urządzenia nadal będą otrzymywać starszą wersję.

Informacje ogólne

Jeśli jesteś bezpośrednio na urządzeniu, otrzymasz krótki przegląd wybranego urządzenia.

Nazwa urządzenia	Nazwa urządzenia
Numer telefonu	Numer telefonu urządzenia
Model	Numer modelu
System operacyjny	OS
Numer seryjny	Numer seryjny urządzenia
Własność urządzenia	Urządzenie firmowe lub prywatne Korporacyjny = urządzenie korporacyjne Pracownik = urządzenie prywatne
Typ urządzenia	Typ urządzenia (tablet lub telefon)
Jailbroken	Jeśli na urządzeniu jest zainstalowany Jailbreak
Nadzorowany	Wskazuje, czy jest to urządzenie nadzorowane.
Zgodność	Jeśli jakiekolwiek wytyczne zostały naruszone
Ostatnio widziany	Status ostatniej komunikacji urządzenia z serwerem AppTec360.

Ustawienia

Ustawienia te zawierają nazwę urządzenia i predefiniowane tło.

Nazwa urządzenia do nazwy systemu	Nazwa, która zostanie nadana w konsoli AppTec360 (w lewej strukturze hierarchii), będzie taka sama jak na odpowiednim urządzeniu użytkownika końcowego (można ją wyświetlić w ustawieniach urządzenia).
Używanie niestandardowej tapety (tylko urządzenia pod nadzorem)	W tym miejscu można wstępnie zdefiniować tło, które powinno być wyświetlane na urządzeniu użytkownika końcowego (np. dla rodzaju brandingu korporacyjnego dla urządzenia). Jest dostępny tylko w trybie nadzorowanym!
Automatyczne aktualizacje systemu operacyjnego	Wymusza aktualizacje systemu operacyjnego, jeśli są dostępne. Tylko dla urządzeń DEP w trybie nadzorowanym.
Niestandardowe czcionki	Tutaj można dodać niestandardowe czcionki.
Nazwa	Opcjonalnie. Widoczna dla użytkownika nazwa czcionki. To pole jest zastępowane rzeczywistą nazwą czcionki po instalacji.
Czcionka	Prześlij plik czcionki (.otf lub .ttf).

Wersja konfiguracji

W tym miejscu wyświetlany jest przegląd profili grupowych przypisanych do urządzenia.

Jeśli klikniesz profil grupy, uzyskasz do niego bezpośredni dostęp i będziesz mógł dokonać ustawień.

Za pomocą symbolu można przywrócić przypisane aplikacje do ustawień profilu grupy.

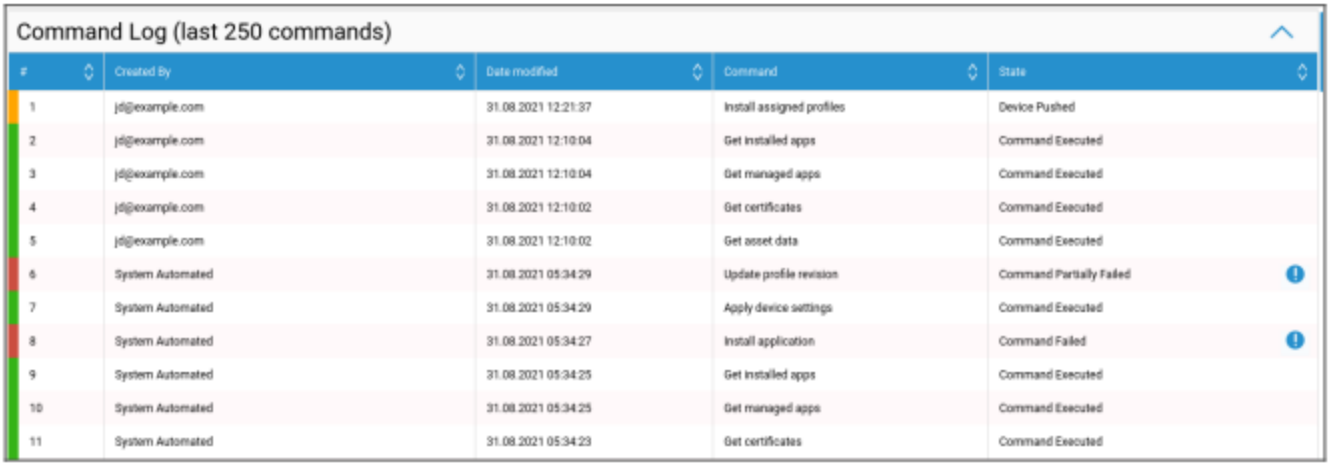
Za pomocą symbolu można zresetować profil urządzenia, aby nie miał żadnych ustawień.

"Newer Revision available" oznacza, że profil grupy został zmieniony i zapisany, ale nie został przypisany. Profil grupy musi zostać przypisany za pomocą opcji "Przypisz teraz" na poziomie grupy, aby zastosować zmiany do urządzeń.

Dziennik urządzenia (tylko na poziomie urządzenia)

Dziennik poleceń

Tutaj można sprawdzić, które polecenia zostały wydane dla urządzenia i jaki jest ich status.



Polecenia utworzone przez "System Automated" są automatycznie tworzone przez system.

Możliwe statusy poleceń

Urządzenie wciśnięte	Żądanie push zostało wysłane do usługi push (np. APNS), aby poinformować urządzenie o konieczności połączenia się z serwerem EMM.
Utworzone polecenie	Polecenie zostało utworzone w systemie.
Wysłane polecenie	Polecenie zostało wysłane do urządzenia po nawiązaniu połączenia z serwerem.
Polecenie wykonane	Polecenie zostało pomyślnie wykonane.
Polecenie nie powiodło się	Polecenie nie powiodło się. *
Polecenie częściowo nieudane	W zależności od systemu operacyjnego urządzenia niektóre polecenia mogą zostać zgrupowane. W tym przypadku niektóre części tej grupy poleceń nie powiodły się. *
Polecenie wykonane, ostatecznie nieudane	Polecenie zostało wykonane, ale być może nie.
Przesunięcie polecenia	Polecenie zostało powtórzone przez użytkownika.
Odrzucony	Polecenie zostało odrzucone. Na przykład dlatego, że zostało zastąpione przez inne polecenie lub urządzenie zostało ponownie zarejestrowane, a stare polecenia zostały usunięte.

Jeśli za wiadomością znajduje się wykrzyknik, można uzyskać więcej informacji, najeżdżając kursorem na ikonę.

Zarządzanie zasobami (tylko na poziomie urządzenia)

Zarządzanie zasobami (tylko na poziomie urządzenia)

Informacje o urządzeniu

Model	Numer modelu urządzenia
System operacyjny	OS
Wersja systemu operacyjnego	Wersja systemu operacyjnego
Numer seryjny	Numer seryjny
UDID	Identyfikator UDID urządzenia
Nazwa urządzenia	Nazwa urządzenia
Nadzorowany	Wyświetla, czy urządzenie jest nadzorowane
Stan akumulatora	Stan akumulatora

Wi-Fi

Adres IP	Adres IP urządzenia
WiFi MAC	Adres MAC WiFi

Komórkowy

Status	Status (obecna karta SIM)
Numer telefonu	Numer telefonu
Status roamingu	Bieżący status roamingu
Roaming (połączenia głosowe/dane)	Status roamingu dla połączeń głosowych/danych
Adres IP	Adres IP
IMEI	Numer IMEI
Operator/Przewoźnik	Dostawca usług komórkowych
SIM Sieć operatora	Sieć operatora SIM
Wersja dla przewoźników	Wersja dla przewoźników
Oprogramowanie sprzętowe modemu	Oprogramowanie układowe modemu
Obecny MCC/MNC	Patrz "SIM MCC/MNC"
SIM MCC/MNC	Kod kraju sieci komórkowej jest identyfikatorem kraju ustalonym przez ITU zgodnie ze standardem E.212, który w połączeniu z kodem sieci komórkowej (MNC) jest używany do identyfikacji sieci komórkowej (=kod kraju). Po przejściu do innej sieci komórkowej "Bieżący MCC/MNC" i "SIM MCC/MNC" są zatem różne.

Bluetooth

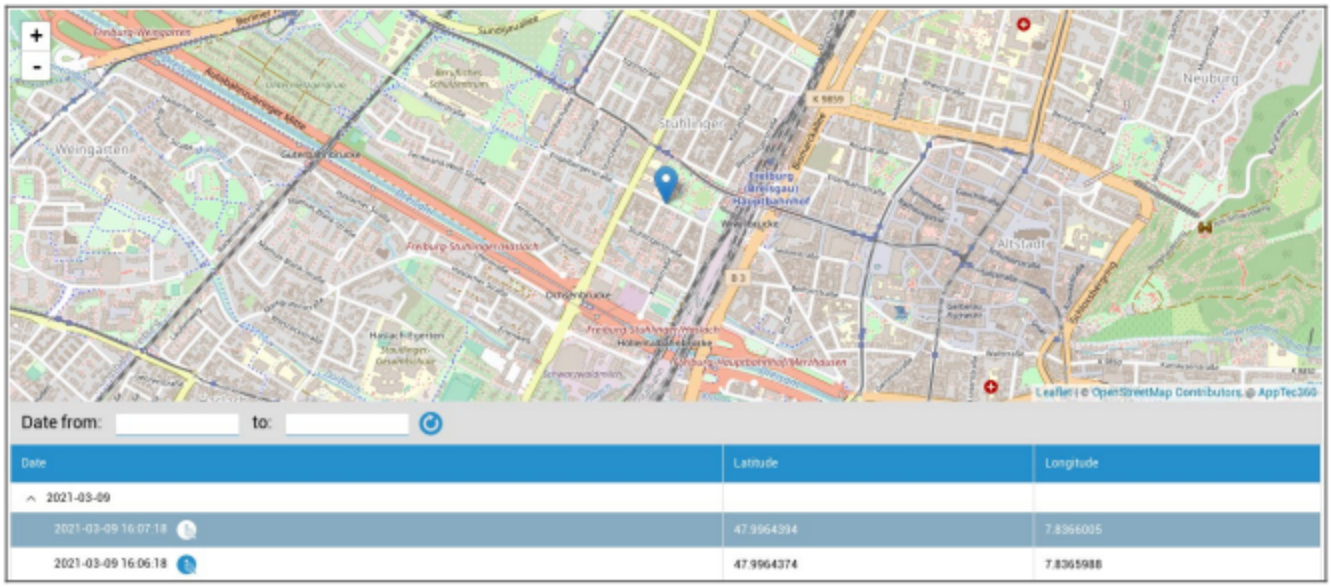
Bluetooth MAC	Adres MAC Bluetooth

Zarządzanie bezpieczeństwem

Ochrona przed kradzieżą (tylko na poziomie urządzenia)

Informacje GPS (tylko na poziomie urządzenia)

Tutaj można ocenić bieżącą/ostatnią lokalizację urządzenia. Lokalizacja może być chroniona jednym lub nawet dwoma hasłami - patrz: Ustawienia ogólne - Prywatność - Dostęp GPS



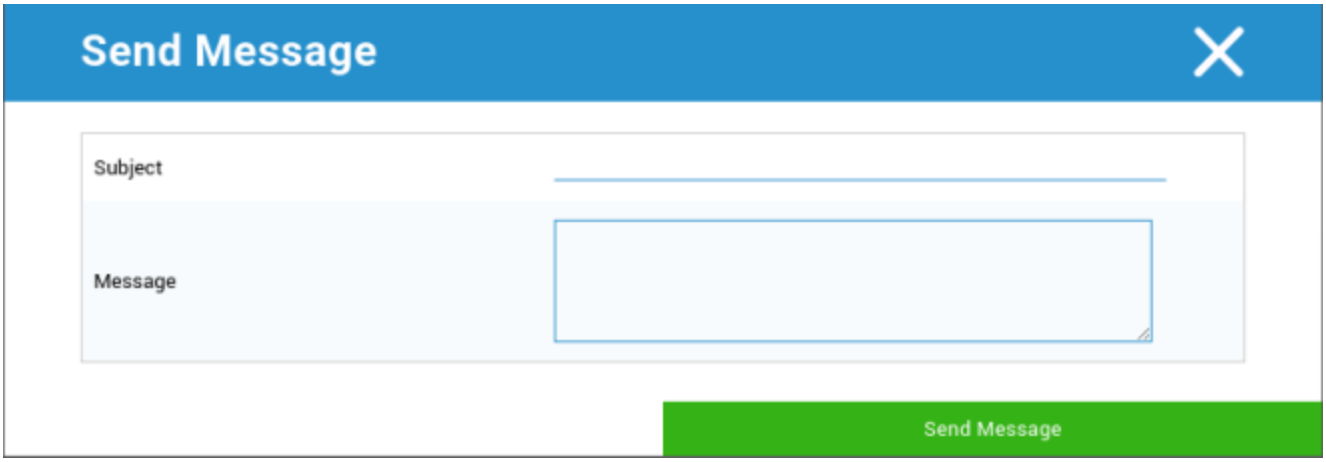
Wipe & Lock (tylko na poziomie urządzenia)

W sekcji "Wyczyść i zablokuj" można wykonać następujące trzy czynności:

Pełne wytarcie	Urządzenie jest przywracane do ustawień fabrycznych (dane firmowe i osobiste są usuwane).
Enterprise Wipe	Z urządzenia użytkownika końcowego usuwane są tylko dane firmowe (wszystkie aplikacje, dane itp. dostarczone przez AppTec).
Ekran blokady	Blokada ekranu jest aktywna, wystarczy odblokować urządzenie za pomocą hasła / kodu PIN urządzenia.
Blokada kryminalistyczna (tylko urządzenia nadzorowane)	Jeśli funkcja ta zostanie aktywowana za pomocą symbolu  , urządzenie zostanie zablokowane poprzez wyświetlenie komunikatu, którego nie można zamknąć. Pracownik nie może również odblokować urządzenia. Tylko administrator może odblokować urządzenie w konsoli za pomocą symbolu odblokowania  .
Zezwalaj na blokadę aktywacji (tylko urządzenia nadzorowane)	Jeśli ta funkcja zostanie aktywowana, urządzenie zostanie zablokowane, gdy tylko funkcja "Znajdź mój iPhone" zostanie aktywowana w ustawieniach iCloud

Wiadomość (tylko na poziomie urządzenia)

W poniższym oknie można wpisać temat i wiadomość, a następnie wysłać ją na urządzenie użytkownika końcowego:



Konfiguracja zabezpieczeń

Kod dostępu

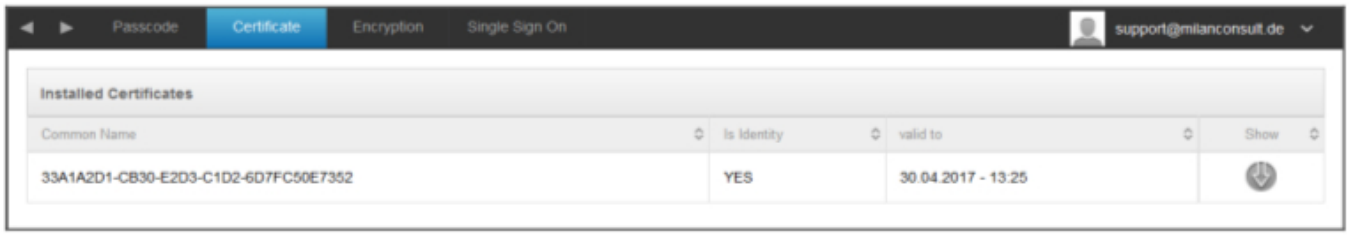
W tym miejscu można określić ustawienia hasła urządzenia

Dozwolona dezaktywacja kodu	Gdy to ustawienie jest aktywne, nie jest wyświetlany monit o wprowadzenie hasła Po ustanowieniu hasła nie można go dezaktywować
Zezwalaj na prostą wartość	Zezwalanie użytkownikowi na używanie tych samych, rosnących i malejących ciągów numerów (np. 1234, 1111).
Wymagana wartość alfanumeryczna	Hasła muszą zawierać co najmniej jedną literę
Minimalna długość kodu dostępu	Minimalna długość hasła
Minimalna liczba złożonych znaków	Minimalna liczba symboli alfanumerycznych w haśle
Maksymalny wiek kodu dostępu	Liczba dni, po których hasło musi zostać zmienione
Maksymalna automatyczna blokada	Maksymalny czas, po którym urządzenie zostanie zablokowane
Maksymalny okres karencji dla blokady urządzenia	Czas, po którym urządzenie przechodzi do zablokowanego trybu gotowości
Maksymalna liczba nieudanych prób	Ustala, jak często hasło może być wprowadzane niepoprawnie, zanim zostanie wykonane całkowite czyszczenie urządzenia.
Maksymalny wiek kodu dostępu (1-730 dni)	Maksymalny wiek hasła
Historia kodów dostępu (1-50 kodów dostępu)	Użycie starego hasła jest dozwolone po tej liczbie

Kliknięcie na kosz otwiera okno dialogowe resetowania hasła, za pomocą którego można usunąć zapomniane hasło urządzenia.

Certyfikat (tylko na poziomie urządzenia)

Wyświetla certyfikaty dostępne na urządzeniu


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

Szyfrowanie

Wymóg szyfrowania pamięci masowej	Aktywacja funkcji szyfrowania zainstalowanego urządzenia

Pojedyncze logowanie

W punkcie "Single Sign-On" można skonfigurować uwierzytelnianie Kerberos.

W tym miejscu ustala się poświadczenia dostępu i odpowiednie adresy URL / aplikacje, które mogą korzystać z tokenów Kerberos.

Dostępne w trybie nadzorowanym	
Nazwa konta	Nazwa konta
Imię i nazwisko	Unikalna tożsamość, do której można dystrybuować bilety Kerberos
Królestwo	Obszar Kerberos, który ma być używany (np. domena)

Za pomocą Symbolu można utworzyć dodatkowe adresy URL.

Wzorzec URL używany do ograniczenia tego konta	Do ustalenia adresy URL, do których można dystrybuować bilety Kerberos.

Za pomocą Symbolu można utworzyć dodatkowe aplikacje.

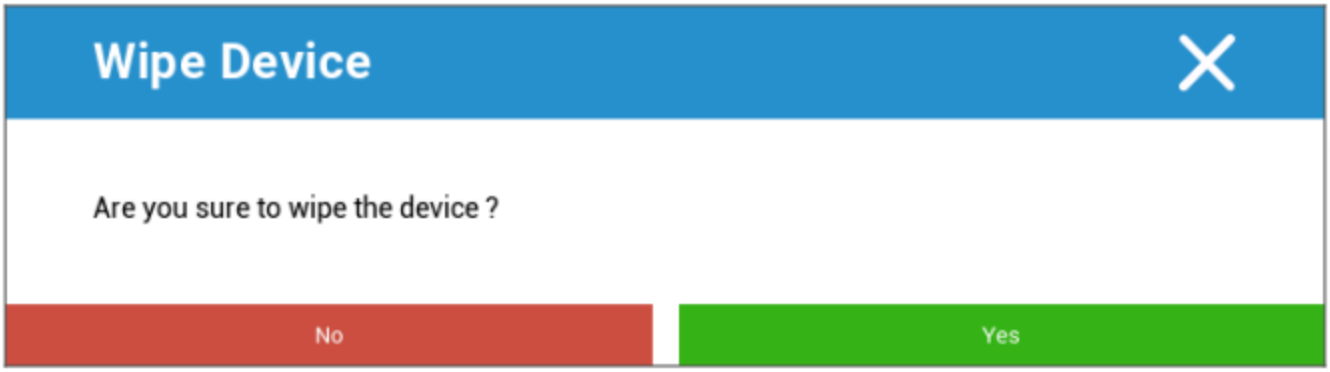
Aplikacje ograniczające to konto	Do ustalenia Aplikacje, do których można dystrybuować bilety Kerberos

Koniec życia (tylko na poziomie urządzenia)

Wipe (tylko na poziomie urządzenia)

W sekcji "Wipe" można przywrócić urządzenie do ustawień fabrycznych. W tym przypadku dane firmowe i prywatne zostaną usunięte z urządzenia użytkownika końcowego.

Po kliknięciu na "Symbol minus" powinieneś otrzymać następujący komunikat



Po wybraniu opcji "Tak" można wykonać czyszczenie.

W sekcji "Wipe Report" można wyświetlić następujące elementy

Wymazane przez	Historia tego, kto wykonał czyszczenie
Data	Data
Status	Status (np. czy czyszczenie zostało wykonane pomyślnie)

Ustawienia ograniczeń

Funkcjonalność urządzenia

Tutaj można zablokować poszczególne funkcje urządzenia użytkownika końcowego

Zezwalaj na instalowanie aplikacji	Zezwalaj na instalowanie aplikacji
Zezwalaj na kamerę	Zezwalaj na korzystanie z kamery
Zezwalaj na FaceTime	Zezwalaj na FaceTime
Zezwalaj na przechwytywanie ekranu	Zezwalaj na przechwytywanie ekranu
Zezwalaj na automatyczną synchronizację w roamingu	Zezwalaj na automatyczną synchronizację w roamingu
Zezwól Siri	Zezwól Siri
Zezwalaj na wybieranie głosowe	Zezwalaj na wybieranie głosowe
Zezwalaj na zakupy w aplikacji	Zezwalaj na zakupy w aplikacji
Wymaganie hasła iTunes Store dla wszystkich zakupów	Wymaganie hasła iTunes Store dla wszystkich zakupów
Umożliwienie gry wieloosobowej	Umożliwienie gry wieloosobowej
Zezwalaj na dodawanie znajomych z Game Center	Zezwalaj na dodawanie znajomych z Game Center
Zezwól na otwarcie z zarządzanego do niezarządzanego	Zezwalanie na otwieranie zawartości aplikacji zarządzanych w aplikacjach niezarządzanych
Zezwalaj na otwarcie z trybu niezarządzanego na zarządzany	Zezwalanie na otwieranie zawartości aplikacji niezarządzanych w aplikacjach zarządzanych
Zezwalaj na widok dnia dzisiejszego na ekranie blokady	Gdy to ustawienie jest aktywne, widok "Dzisiaj" będzie wyświetlany w Centrum powiadomień na ekranie blokady
Zezwalaj na centrum sterowania na ekranie blokady	Zezwalaj na Centrum sterowania na ekranie blokady
Zezwalaj na TouchID	Zezwalaj na TouchID
Zezwalanie na bezprzewodowe aktualizacje PKI	Zezwalanie na bezprzewodowe aktualizacje PKI

Zezwalaj na korzystanie z książeczki podczas blokady	Zezwalanie na korzystanie z książki haseł, gdy urządzenie jest zablokowane
Ograniczenie śledzenia reklam	Funkcja ta dezaktywuje śledzenie reklam (np. reklamodawcy nie mogą używać śledzenia reklam w celu rozpowszechniania spersonalizowanych reklam).
Zezwalaj na przekazywanie	Zezwalaj na przekazywanie
Zezwalaj na wyniki internetowe w centrum uwagi	Zezwalaj na wyniki internetowe w centrum uwagi (np. Bing lub Wikipedia)
Wymagaj kodu przy pierwszym parowaniu AirPlay	Wymagaj kodu przy pierwszym parowaniu AirPlay
Ochrona nadgarstka zegarka Force Watch	W przypadku aktywacji, Apple Watch jest zmuszony do korzystania z "Ochrony nadgarstka" (rozpoznawanie nadgarstka).
Zezwalanie na korzystanie z biblioteki zdjęć iCloud	Zezwala na korzystanie z biblioteki zdjęć iCloud. Jeśli nie jest to dozwolone, wszystkie zdjęcia, które nie zostały całkowicie pobrane z usługi iCloud, zostaną usunięte z pamięci lokalnej.
Dostępne w trybie nadzorowanym	
Zezwalaj na modyfikację konta	Zezwalaj na modyfikację "poczty, kontaktów, kalendarza"
Zezwalaj na AirDrop	Zezwalaj na AirDrop
Zezwalaj na modyfikację komórkową aplikacji	To ustawienie blokuje ustawienie, które aplikacje mogą korzystać z danych mobilnych To ustawienie można na przykład ustawić ręcznie na urządzeniu użytkownika końcowego, a następnie aktywować to ograniczenie
Umożliwienie Siri odpytywania treści generowanych przez użytkowników w Internecie	Wyszukiwanie w niektórych witrynach jest zablokowane, np. w Wikipedii, ponieważ każdy może wprowadzać zmiany według własnego uznania.
Włącz filtr wulgaryzmów Siri	Wulgaryzmy skierowane do Siri są cenzurowane
Zezwalaj na iBook Store	Zezwalaj na iBook Store
Erotyka w iBook Store	Erotyka w iBook Store
Zezwalaj na modyfikowanie ustawień usługi Znajdź moich znajomych	Zezwalaj na modyfikowanie ustawień usługi Znajdź moich znajomych
Zezwól na Game Center	Zezwól na Game Center
Zezwalaj na parowanie hostów	Parowanie komputera sterującego

Zezwalaj na instalowanie profili konfiguracji	Zezwalaj na instalowanie profili konfiguracji
Zezwalaj na usuwanie aplikacji	Usuwanie aplikacji sterujących
Zezwalaj na iMessage	Zezwalaj na iMessage
Zezwalaj na wymazanie całej zawartości i ustawień	Umożliwienie usunięcia całej zawartości i ustawień
Zezwalaj na konfigurowanie ograniczeń	Zezwalaj na konfigurowanie ograniczeń
Pozwól na podcast	Pozwól na podcast
Zezwalaj na wyszukiwanie definicji	Zezwalaj na wyszukiwanie definicji
Zezwalaj na klawiaturę predykcyjną	Zezwalaj na klawiaturę predykcyjną
Zezwalaj na automatyczną korektę	Zezwalaj na automatyczną korektę
Zezwalaj na instalację aplikacji UI	Po dezaktywacji nie można instalować aplikacji z publicznego sklepu AppStore (ikona nie będzie już wyświetlana). Aplikacje można jednak nadal instalować za pośrednictwem iTunes i konfiguratora
Zezwalaj na skróty klawiaturowe	Zezwalaj na skróty klawiaturowe, jeśli urządzenie jest podłączone do fizycznej klawiatury.
Zezwalaj na parowanie Apple Watch	Zabrania parowania urządzenia z zegarkiem Apple Watch, a istniejące połączenia zostaną przerwane.
Zezwalaj na modyfikację kodu dostępu	Jeśli nie jest to dozwolone, żadne hasło urządzenia nie może zostać dodane, zmienione ani usunięte.
Zezwalaj na modyfikację nazwy urządzenia	Wytyczne określające, czy można zmienić nazwę urządzenia
Zezwalaj na modyfikację tapet	Wytyczne określające, czy tapetę można zmienić
Zezwalaj na automatyczne pobieranie aplikacji	W przypadku dezaktywacji zakupiona aplikacja nie będzie automatycznie instalowana na innych urządzeniach. Nie dotyczy aktualizacji istniejących aplikacji
Zezwalaj na wiadomości	Zezwalaj na wiadomości na urządzeniu z systemem iOS
Zezwalaj na zaufanie aplikacji Enterprise	Jeśli ustawiona na false, zapobiega ufaniu aplikacjom korporacyjnym.

iCloud

Blokowanie niektórych funkcji podczas parowania iCloud

Zezwalaj na tworzenie kopii zapasowych	Zezwalaj na tworzenie kopii zapasowych
Zezwalaj na synchronizację dokumentów	Zezwalaj na synchronizację dokumentów
Zezwalaj na strumień zdjęć	Zezwalaj na strumień zdjęć
Zezwalaj na udostępnianie strumienia zdjęć	Zezwalaj na udostępnianie strumienia zdjęć
Zezwalaj na synchronizację pęku kluczy w chmurze	Zezwól na synchronizację pęku kluczy w chmurze
Zezwalanie zarządzanym aplikacjom na przechowywanie danych	Zezwalanie zarządzanym aplikacjom na przechowywanie danych
Zezwalaj na synchronizację notatek i wyróżnień dla książek korporacyjnych	Zezwalaj na synchronizację notatek i podkreśleń dla książek korporacyjnych
Umożliwienie tworzenia kopii zapasowych ksiąg przedsiębiorstwa	Umożliwienie tworzenia kopii zapasowych ksiąg przedsiębiorstwa

Bezpieczeństwo i prywatność

Blokowanie tych funkcji związanych z danymi diagnostycznymi

Umożliwienie wysyłania danych diagnostycznych do Apple	Umożliwienie wysyłania danych diagnostycznych do Apple
Zezwalanie użytkownikowi na akceptowanie niezaufanych certyfikatów TLS	Zezwalaj użytkownikowi na akceptowanie niezaufanych certyfikatów TLS
Wymuś szyfrowane kopie zapasowe	Wymuś szyfrowane kopie zapasowe

BYOD

Wbudowane zabezpieczenia iOS (kontener)

iOS zawsze był w stanie odróżnić zarządzane (biznesowe) od niezarządzanych (prywatnych). Wszystko, co pochodzi z systemu MDM, jest traktowane jako zarządzane. Na przykład, jeśli zainstalujesz aplikację za pośrednictwem MDM lub skonfigurujesz konto Exchange, będzie to traktowane jako zarządzane przez iOS.

Wszystko inne, co zostanie skonfigurowane/zainstalowane ręcznie na urządzeniu, będzie traktowane jako niezarządzane. Na przykład, jeśli użytkownik sam zainstaluje WhatsApp lub doda konto Exchange. Jednak ta separacja nigdy nie miała wpływu na kontakty. Ale od iOS 11.3 (i nowszych) zostało to również dodane dla kontaktów.

Ponieważ jest to podstawowa funkcjonalność systemu operacyjnego, nie trzeba niczego instalować ani konfigurować specjalnego kontenera.

Aktywuj wbudowaną funkcję oddzielania prywatnych i służbowych aplikacji/informacji/plików. To ustawienie wyłączy również niektóre inne funkcje, które w przeciwnym razie mogłyby omyłkowo wyłączyć część tej separacji.

Aktywacja

Aktywuj rozwiązania kontenerowe obsługiwane przez AppTec360

Włącz Google Divide Container	Włącz Google Divide Container
Włącz kontener SecurePIM	Włącz kontener SecurePIM

Jeśli aktywowałeś SecurePIM Container, znajdziesz również następujący punkt w sekcji "Aktywacja". Dodatkowo od razu zostaną otwarte cztery kolejne zakładki, które zostały opisane poniżej.

Adres e-mail pomocy technicznej	Adres e-mail pomocy technicznej, na który użytkownik może się zwrócić z problemami

Hasło SecurePIM

W sekcji "SecurePIM Password" można ustalić wytyczne dotyczące siły zabezpieczeń hasła.

Limit czasu sesji	W tym miejscu można ustalić, po ilu minutach należy ponownie wprowadzić nowe hasło, gdy program SecurePIM działa w tle
Długość hasła	Długość hasła dostępu do kontenera SecurePIM
Wielkie litery	Minimalna wielkość liter
Małe litery	Minimum małych liter
Znaki specjalne	Minimalna liczba znaków specjalnych
Cyfry	Minimalne cyfry
Aplikacja do wycierania	Ile razy hasło może zostać wprowadzone niepoprawnie, zanim zawartość SecurePIM zostanie usunięta. (Aplikacja pozostaje jednak na urządzeniu użytkownika końcowego).

Bezpieczeństwo SecurePIM

W sekcji "SecurePIM Security" można określić różne ustawienia zabezpieczeń.

Wykrywanie urządzeń po jailbreaku	Jeśli to ustawienie zostanie aktywowane, dostęp do SecurePIM Container zostanie zablokowany, gdy tylko urządzenie zostanie wykryte jako jailbreakowane
Bezpieczne pola tekstowe	Zawartość pól zgłoszeń będzie zaszyfrowana, żadne informacje nie dotrą do systemu operacyjnego (iOS). Uwaga: Dopóki to ustawienie jest aktywne, automatyczna korekta nie jest już dostępna.
Eksportowanie danych kontaktu do urządzenia	Jeśli to ustawienie zostanie aktywowane, użytkownik będzie mógł eksportować kontakty Exchange na swoje urządzenie lokalne Uwaga: Eksportowane są tylko nazwa i numer telefonu.
Lokalizacja wydarzenia	Jeśli to ustawienie jest aktywne, lokalizacja nadchodzących wydarzeń będzie wyświetlana na pasku powiadomień
Pokaż tytuł wydarzenia	Jeśli to ustawienie jest aktywne, lokalizacja tytułu nadchodzącego wydarzenia będzie wyświetlana na pasku powiadomień

Przeglądarka SecurePIM

Tutaj można skonfigurować przeglądarkę SecurePIM.

Za pomocą symbolu można zdefiniować nowy adres URL.

Za pomocą symbolu można ponownie usunąć zdefiniowany adres URL.

"Adresy URL z białej listy" to adresy URL, które mogą zostać załadowane.

"Adresy URL z czarnej listy" to adresy URL, które nie mogą zostać załadowane, a tym samym są blokowane.

Należy pamiętać, że wpisy na białej liście mają wyższy priorytet niż wpisy na czarnej liście. W sekcji "Tytuł zakładki" można nadać jej tytuł. Za pomocą opcji "Adres URL zakładki" można powiązać adres URL z tytułem zakładki - w ten sposób można dystrybuować zindywidualizowane zakładki do odpowiednich użytkowników.

Wymiana

W sekcji "Exchange" można skonfigurować konto Exchange.

Adres e-mail ActiveSync	Exchange email address (zwróć uwagę na "Placeholders")
ActiveSync Exchange Login	Wymiana nazw użytkowników (zwróć uwagę na "symbole zastępcze")
ActiveSync Exchange Server	Adres serwera Exchange (FQDN)
Domena ActiveSync Exchange	Adres domeny Exchange
Certyfikat użytkownika	Certyfikat użytkownika
Uwierzytelnianie oparte na certyfikatach	Użytkownik uwierzytelnia się za pomocą certyfikatu
Zezwalaj na szyfrowanie S/MIME	Umożliwia użytkownikowi szyfrowanie poczty.
Zezwalaj na podpisywanie S/MIME	Umożliwia użytkownikowi podpisywanie poczty
Sprawdzenie listy CRL	Jeśli jest aktywny, certyfikat prywatny zostanie porównany z listą CRL (Certificate Revocation List).

Zarządzanie połączeniami

Wi-Fi

Identyfikator zestawu usług (SSID)	SSID sieci, z którą ma zostać nawiązane połączenie
Automatyczne dołączanie	Aktywacja automatycznego dołączania podczas dołączania do sieci
Ukryta sieć	Aktywuj, jeśli punkt dostępowy nie rozgłasza identyfikatora SSID

Konfiguracja proxy

Konfiguracja serwera proxy dla każdego punktu dostępowego

Brak	Ustanowienie braku proxy
Podręcznik	Ustanowienie ręcznego pełnomocnika
Adres URL serwera proxy	Adres dostępu do ustawień serwera proxy
Port	Ustalenie portu dla serwera proxy
Uwierzytelnianie	Nazwa użytkownika do uwierzytelniania na serwerze proxy
Hasło	Hasło do uwierzytelniania na serwerze proxy
Automatyczny	Automatyczne ustanowienie serwera proxy
Adres URL serwera proxy	Adres URL umożliwiający dostęp do ustawień serwera proxy

Typ zabezpieczenia

Ustalenie typu zabezpieczeń dla punktu dostępowego

WEP	
Hasło	Hasło do punktu dostępowego

WPA/WPA2	
Hasło	Hasło do punktu dostępowego

WEP Enterprise - WPA / WPA2 Enterprise - Any Enterprise			
	Protokoły		
	TLS	Aktywuj/Dezaktywuj	
	TTLS	Aktywuj/Dezaktywuj	
	LEAP	Aktywuj/Dezaktywuj	
	PEAP	Aktywuj/Dezaktywuj	
	EAP-FAST	Aktywuj/Dezaktywuj	
	EAP-SIM	Aktywuj/Dezaktywuj	
	Korzystanie z PAC		Korzystanie z PAC (kontrolera chronionego dostępu)
	Przepis PAC	Konfiguracja Provision PAC	
	Udostępnianie PAC anonimowo	Anonimowe dostarczanie PAC	
	Uwierzytelnianie wewnętrzne	Protokół uwierzytelniania, który powinien być używany: PAP, CHAP, MSCHAP, MSCHAPv2	
	Nazwa użytkownika	Nazwa użytkownika uwierzytelniania	
	Nie używaj hasła na połączenie	Nie używaj hasła na połączenie	
	Certyfikat tożsamości	Prześlij/wybierz certyfikat uwierzytelniania	
	Tożsamość zewnętrzna	Tożsamość widoczna na zewnątrz	
	Zaufanie		
	Zaufany certyfikat 1	Prześlij pierwszy zaufany certyfikat	
	Zaufany certyfikat 2	Prześlij drugi zaufany certyfikat	
	Zaufany certyfikat 3	Prześlij trzeci zaufany certyfikat	
	Nazwy certyfikatów zaufanego serwera	Nazwy oczekiwanych certyfikatów serwera (na liście oddzielonej przecinkami)	

Brak	Brak zabezpieczeń

VPN

Nazwa połączenia	Nazwa profilu VPN

Typ VPN

VPN

Cały ruch sieciowy urządzenia będzie kierowany przez połączenie VPN.

Typ połączenia	Ustanowienie typu połączenia VPN
IPsec (cisco)	Protokół IPsec firmy cisco
PPTP	Protokół PPTP
L2TP	Protokół L2TP
Cisco AnyConnect	Protokół AnyConnect
Juniper SSL	Protokół SSL Juniper
F5 SSL	Protokół F5 SSL
SonicWall mConnect	SonicWall mobile Connect
Aruba VIA	Protokół Aruba VIA
Niestandardowy SSL	Połączenie przez niestandardowy protokół SSL
OpenVPN	Protokół OpenVPN

VPN dla poszczególnych aplikacji

Po otwarciu określonej aplikacji zostanie nawiązane połączenie VPN

Automatyczne uruchamianie połączenia VPN dla aplikacji		Automatyczne uruchamianie połączenia VPN dla aplikacji
Typ połączenia		Ustanowienie typu połączenia VPN
	Cisco AnyConnect	Protokół AnyConnect
	Juniper SSL	Protokół SSL Juniper
	F5 SSL	Protokół F5 SSL
	SonicWall mConnect	SonicWall mobile Connect
	Aruba VIA	Protokół Aruba VIA
	Niestandardowy SSL	Połączenie przez niestandardowy protokół SSL
	OpenVPN	Protokół OpenVPN

Konfiguracja proxy

Konfiguracja serwera proxy dla połączenia VPN

Brak	Ustanowienie braku proxy
Podręcznik	Ręczne ustanowienie serwera proxy
Adres URL serwera proxy	Adres dostępu do ustawień proxy
Port	Ustalenie portu dla serwera proxy
Uwierzytelnianie	Nazwa użytkownika do uwierzytelniania na serwerze proxy
Hasło	Hasło do uwierzytelniania na serwerze proxy
Automatyczny	Automatyczne ustanowienie serwera proxy
Adres URL serwera proxy	Adres URL umożliwiający dostęp do ustawień serwera proxy

Pokaż symbole zastępcze	Wyświetla wszystkie dostępne zmienne użytkownika, których może używać AppTec360

APN

Nazwa punktu dostępu	Nazwa punktu dostępu
Nazwa użytkownika punktu dostępu	Nazwa użytkownika punktu dostępu
Hasło punktu dostępu	Hasło punktu dostępu
Serwer proxy	Adres serwera proxy
Port	Odpowiedni port proxy

Komórkowy

Włącz roaming danych	Włącz roaming danych
Włącz roaming głosowy	Włącz roaming głosowy
Włącz Hotspot	Włącz Hotspot

Serwer proxy HTTP

Typ proxy	
Podręcznik	Ręczne ustanowienie serwera proxy
Adres URL serwera proxy	Adres dostępu do ustawień serwera proxy
Port	Ustanowienie portu proxy
Uwierzytelnianie	Nazwa użytkownika do uwierzytelniania na serwerze proxy
Hasło	Hasło do uwierzytelniania na serwerze proxy
Automatyczny	Automatyczne ustanowienie serwera proxy
Adres URL serwera proxy PAC	Adres URL serwera proxy PAC
Zezwalaj na bezpośrednie połączenie, jeśli PAC jest nieosiągalny	Zezwalaj na bezpośrednie połączenie (bez VPN), jeśli PAC jest nieosiągalny.
Zezwalanie na omijanie proxy w celu uzyskania dostępu do sieci wewnętrznych	Zezwalanie na omijanie proxy w celu uzyskania dostępu do wewnętrznych sieci captive

AirPrint

Adres IP	Adres IP drukarki
Ścieżka zasobów	Określona ścieżka do urządzenia AirPrint

AirPlay

Nazwa urządzenia	Nazwa urządzenia
Hasło	Hasło parowania
Biała lista	Zdefiniuj listę urządzeń, z którymi urządzenie może się sparować na wyłączność.

Zarządzanie PIM

Exchange Active Sync

Nazwa konta	Nazwa konta e-mail
Host Exchange ActiveSync	Adres/FQDN serwera
Zezwalaj na ruch	Zezwalaj na przenoszenie wiadomości e-mail
Używaj tylko w korespondencji	Interakcje mogą występować tylko w natywnej aplikacji Mail.
Używanie protokołu SSL	Używanie szyfrowania SSL
Domena	Domena serwera
Użytkownik	Nazwa użytkownika
Adres e-mail	adres e-mail (tylko na poziomie urządzenia)
Hasło (tylko na poziomie urządzenia)	Hasło użytkownika
Certyfikat tożsamości	Wybierz odpowiedni certyfikat do uwierzytelniania na serwerze
Poprzednie dni Mail to Sync	Liczba dni, do których wiadomości e-mail powinny zostać zsynchronizowane z powrotem. Bez limitu = bez ograniczeń
Włącz S/MIME	Włącz szyfrowanie S/MIME
Certyfikat podpisywania	Prześlij odpowiedni certyfikat podpisywania
Certyfikat szyfrowania	Prześlij odpowiedni certyfikat szyfrowania

eMail

Konfiguracja kont POP3 / IMAP na urządzeniu użytkownika końcowego

Opis konta	Nazwa konta e-mail		
Typ konta	IMAP	Prefiks ścieżki	Prefiks ścieżki dla folderów specjalnych
	POP		
Wyświetlana nazwa użytkownika	Wyświetlana nazwa użytkownika		
Adres e-mail	Adres e-mail użytkownika		
Zezwalaj na ruch	Zezwalaj na przenoszenie wiadomości e-mail		
Włącz S/MIME	Włącz szyfrowanie S/MIME		
Certyfikat podpisywania	Prześlij odpowiedni certyfikat podpisywania		
Certyfikat szyfrowania	Prześlij odpowiedni certyfikat szyfrowania		

Poczta przychodząca

Ustawienia serwera przychodzącego

Adres serwera pocztowego	Adres serwera pocztowego
Port serwera poczty	Port serwera poczty
Nazwa użytkownika	Odpowiednia nazwa użytkownika
Typ uwierzytelniania	Typ uwierzytelniania
Brak	Brak typu uwierzytelniania
Hasło (tylko na poziomie urządzenia)	Monit o hasło
Wyzwanie - odpowiedź MDM	
NTLM	Uwierzytelnianie NTLM
HTTP MD5 Digest	
Używanie protokołu SSL	W razie potrzeby użyj protokołu SSL

Poczta wychodząca

Ustawienia serwera wychodzącego

Adres serwera pocztowego	Adres serwera pocztowego
Port serwera poczty	Port serwera poczty
Nazwa użytkownika	Odpowiednia nazwa użytkownika
Typ uwierzytelniania	
Brak	Brak metody uwierzytelniania
Hasło (tylko na poziomie urządzenia)	Monit o hasło
Wyzwanie - odpowiedź MDM	
NTLM	Uwierzytelnianie NTLM
HTTP MD5 Digest	
Używanie protokołu SSL	W razie potrzeby użyj protokołu SSL
Hasło wychodzące takie samo jak przychodzące	Hasło wychodzące takie samo jak przychodzące
Używać tylko w korespondencji	Aktywuj, jeśli wszystkie wychodzące wiadomości e-mail mają być wysyłane za pośrednictwem aplikacji Mail.

CalDav

Konfiguracja konfiguracji i dystrybucji konta CalDav

Opis konta	Wyświetlana nazwa konta
Nazwa hosta	Nazwa hosta i/lub adres IP
Port	Port konta CalDav
Główny adres URL	Główny adres URL konta
Nazwa użytkownika	Odpowiednia nazwa użytkownika CalDav
Hasło (tylko na poziomie urządzenia)	Odpowiednie hasło CalDav
Używanie protokołu SSL	W razie potrzeby użyj protokołu SSL

Subskrybowane kalendarze

Konfiguracja i dystrybucja subskrybowanych kalendarzy

Opis	Wyświetlana nazwa konta
URL	Adres URL bazy danych kalendarza
Nazwa użytkownika	Nazwa użytkownika subskrypcji kalendarza
Hasło (tylko na poziomie urządzenia)	Hasło subskrypcji kalendarza
Używanie protokołu SSL	W razie potrzeby użyj protokołu SSL

LDAP

W tym obszarze należy skonfigurować połączenie LDAP, aby umożliwić dynamiczną wymianę certyfikatów między urządzeniem użytkownika końcowego a usługą Active Directory.

Należy pamiętać, że wybrany użytkownik wymaga odpowiednich uprawnień do odczytu.

Opis konta	Opis konta
Nazwa użytkownika konta	Użytkownik dla dostępu LDAP
Hasło do konta	Hasło dostępu do protokołu LDAP
Nazwa hosta konta	Nazwa hosta/adres IP serwera LDAP
Używanie protokołu SSL	W razie potrzeby użyj protokołu SSL

W drugiej części można zdefiniować indywidualne filtry do wyszukiwania w rejestrze LDAP.

Opis	Zakres	Baza wyszukiwania
Opis filtra	Poziom wyszukiwania w rejestrze LDAP	Zdefiniuj filtr indywidualny

Zarządzanie siecią

Klipy internetowe

W tym miejscu można zdefiniować zakładki z linkami do stron internetowych, portali intranetowych itp., które będą widoczne jako aplikacja na urządzeniu użytkownika końcowego.

Etykieta	Nazwa połączenia na urządzeniu użytkownika końcowego
URL	Link do odpowiedniej strony internetowej
Zdejmowany	Jeśli jest aktywna, użytkownik może usunąć klip internetowy
Ikona	W tym oknie dialogowym można przesłać logo połączenia: Wymiary 180x180, format png
Wstępnie skomponowana ikona	Jeśli jest aktywna, na ikonie nie będą wyświetlane żadne dodatkowe efekty (cień, odbicie).
Pełny ekran	Podczas otwierania klipów internetowych przeglądarka otwiera się w trybie pełnoekranowym.

Filtr treści internetowych

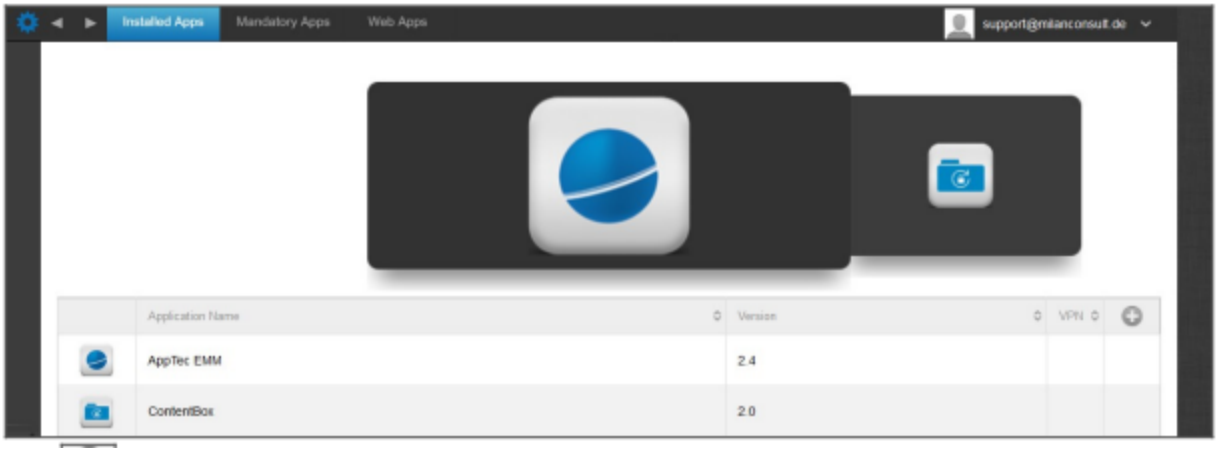
Filtr treści internetowych umożliwia ograniczenie dostępu do określonych stron internetowych.

Dozwolone strony internetowe	
Ograniczenie treści dla dorosłych	Webfilter jest automatycznie stosowany w przypadku treści dla dorosłych
Dozwolone adresy URL	Za pomocą symbolu + dodaj dozwolone strony
Adresy URL na czarnej liście	Za pomocą symbolu + dodaj zablokowane strony
Tylko określone strony internetowe	Wyświetlana może być tylko określona zawartość, którą można dodać za pomocą symbolu +.

Zarządzanie aplikacjami

Menedżer aplikacji dla przedsiębiorstw

Zainstalowane aplikacje (tylko na poziomie urządzenia)



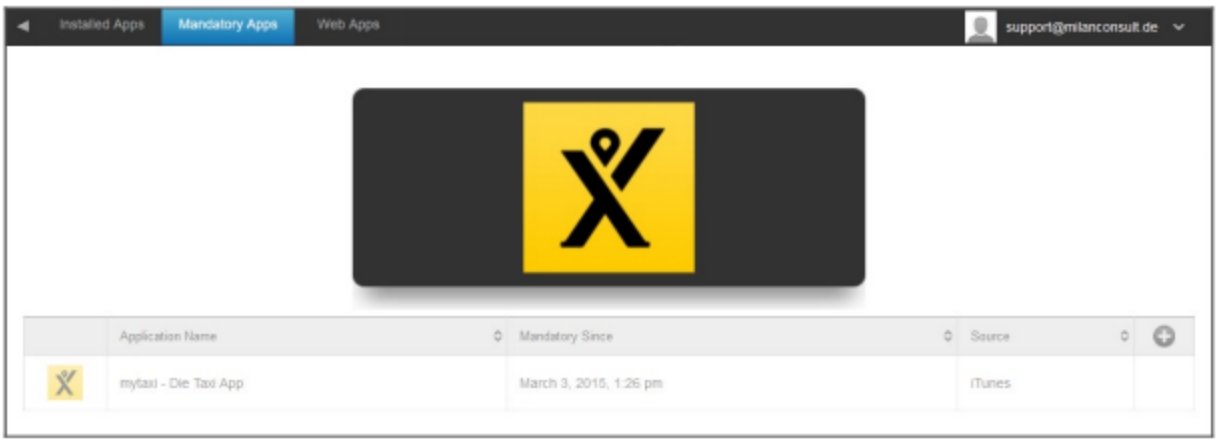
Tutaj możesz zobaczyć aplikacje, które są obecnie zainstalowane na urządzeniu.

Aplikacje obowiązkowe

W sekcji Aplikacje obowiązkowe można określić niezbędne aplikacje.

Użytkownik będzie stale monitowany o zainstalowanie wspomnianej aplikacji.

Aplikację można zdefiniować za pomocą przycisku .



Może to być aplikacja Apple App Store, ale także aplikacja wewnętrzna.

Jeśli dotyczy to nadzorowanego urządzenia, aplikacja zostanie zainstalowana automatycznie.

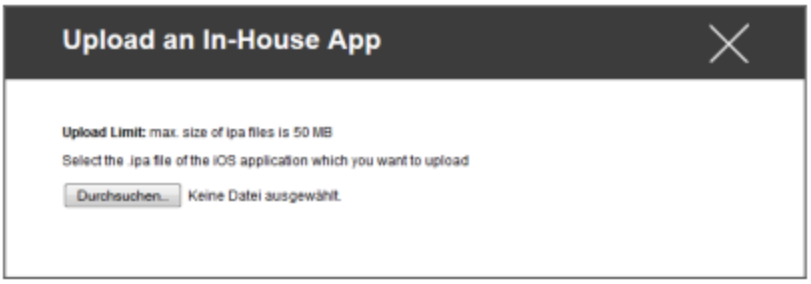
Na urządzenie można przesłać aplikację "Apple AppStore" z publicznego sklepu AppStore, a także wewnętrznie opracowaną aplikację wewnętrzną.

Możesz też wybrać kategorię "Aplikacje wewnętrzne iOS" i wybrać aplikację wewnętrzną, którą przesłałeś w Ustawieniach ogólnych.

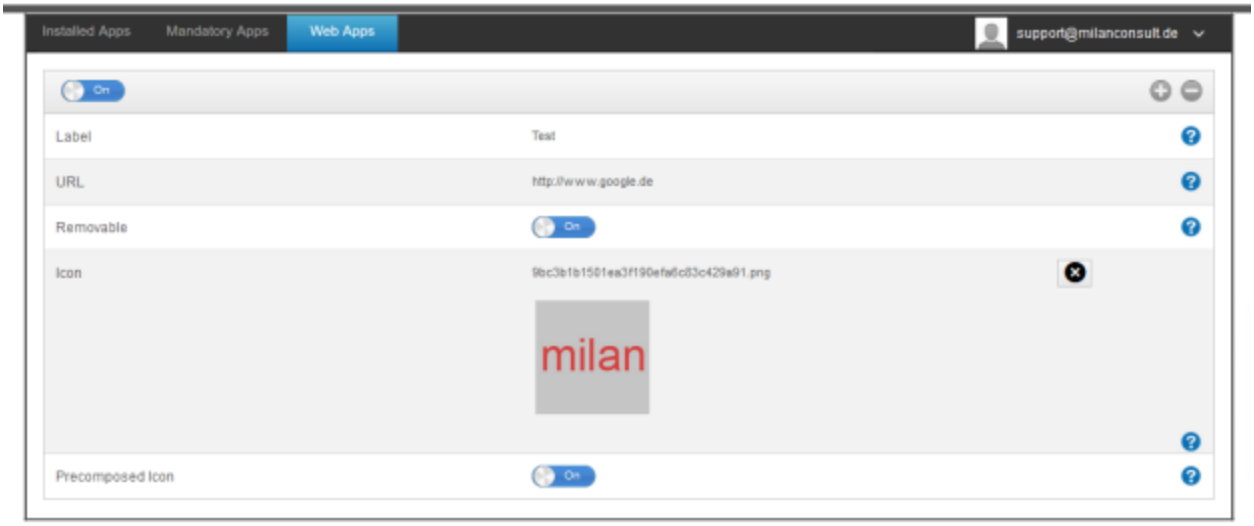
Opcje instalacji

Aktualizuj (obsługiwane tylko dla VPP na urządzenie)	Raz w tygodniu będzie sprawdzane, czy dostępna jest aktualizacja aplikacji. Jeśli tak, aktualizacja zostanie zainstalowana W przypadku aplikacji wewnętrznych do procesu aktualizacji zostanie użyty cel aktualizacji skonfigurowany w ustawieniach ogólnych.
Wyprzedzanie, gdy nie jest zarządzane	Jeśli aplikacja jest już zainstalowana, MDM przejmie ją i będzie nią zarządzać
Usuń aplikację po usunięciu profilu MDM	W przypadku usunięcia zarządzania urządzeniem aplikacja zostanie odinstalowana
Zapobieganie tworzeniu kopii zapasowych danych aplikacji	Kopia zapasowa danych aplikacji nie zostanie utworzona.
Ustawienia aplikacji	W sekcji "Ustawienia aplikacji" można przypisać aplikacji określone wartości do pierwszego planu (o ile aplikacja to obsługuje, w razie potrzeby należy zapytać jej twórcę).

Możesz także bezpośrednio wybrać i przesłać plik ipa, korzystając z opcji "Prześlij aplikację wewnętrzną".



Aplikacje internetowe



W punkcie "Web Apps" można, podobnie jak w przypadku "Web Clips", przesyłać strony internetowe lub portale intranetowe jako aplikację na urządzenie użytkownika końcowego w obszarze Web Management. Domyślnie aplikacje internetowe będą wyświetlane w trybie pełnoekranowym, który można skonfigurować w sekcji Webclips.

Etykieta	Nazwa połączenia na urządzeniu użytkownika końcowego
URL	Link do odpowiedniej strony internetowej
Zdejmowany	Jeśli jest aktywna, użytkownik może usunąć Webclip
Ikona	W tym oknie dialogowym można przesłać logo połączenia: Wymiary 180x180, format png
Wstępnie skomponowana ikona	Jeśli jest aktywna, na ikonie nie będą wyświetlane żadne dodatkowe efekty (cień, odbicie).

Ograniczenia i ustawienia

Aplikacje na czarnej / białej liście

Tutaj można ustawić aplikacje, które są blokowane (lub dozwolone) w zależności od ustawień w "Ustawieniach ogólnych". Kliknięcie spowoduje wyświetlenie wyszukiwania znanych aplikacji. Możesz tam wyszukać aplikacje, które chcesz dodać.

Należy pamiętać, że do działania tej funkcji niezbędne jest urządzenie nadzorowane

Ograniczenia aplikacji SysApp

Blokowanie określonych aplikacji lub funkcji urządzenia

Zezwalaj na korzystanie z YouTube	Zezwalaj na korzystanie z YouTube
Zezwalanie na korzystanie z iTunes Store	Zezwalanie na korzystanie z iTunes Store
Zezwalaj na korzystanie z Safari	Zezwalaj na korzystanie z Safari
Włącz autouzupełnianie	Umożliwia autouzupełnianie
Ostrzeżenie o oszustwach siłowych	Wymusza ostrzeżenie o oszustwie
Włącz JavScript	Umożliwia korzystanie z JavaScript
Blokowanie wyskakujących okienek	Blokuje wszystkie rodzaje pup-upów
Zezwalaj na pliki cookie	Wybierz, kiedy Safari ma akceptować pliki cookie

App-VPN

Za pomocą symbolu można zdefiniować aplikacje, które będą automatycznie uruchamiać wybrane połączenie VPN przy starcie.

Ustawienia aplikacji

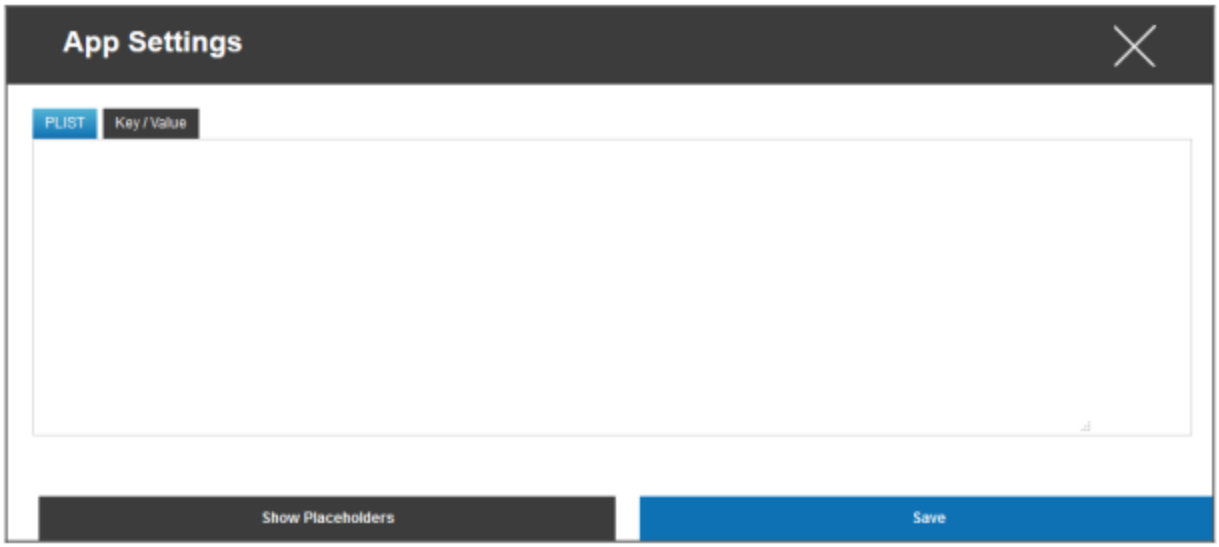
W sekcji "Ustawienia aplikacji" można przypisać aplikacji określone wartości do pierwszego planu (o ile aplikacja to obsługuje, w razie potrzeby należy zapytać jej twórcę).

Za pomocą symbolu dodajesz (dodatkową) aplikację. Ponownie znajdziesz znaną reprezentację AppTec360 App-Import.

Wyszukaj tutaj aplikację, którą chcesz skonfigurować i wybierz ją. Ustawienia będą miały zastosowanie tylko do zarządzanych aplikacji.

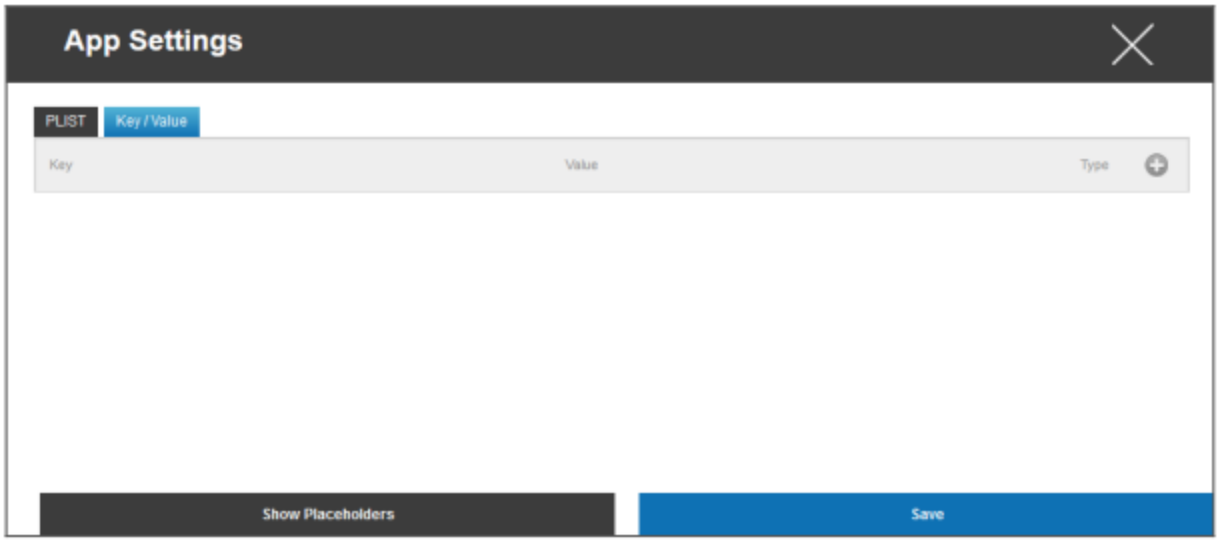
Jeśli import się powiedzie, zostanie wyświetlony następujący ekran:

Teraz wystarczy kliknąć przycisk , aby przeprowadzić różne konfiguracje. Zostanie wyświetlony następujący przegląd:

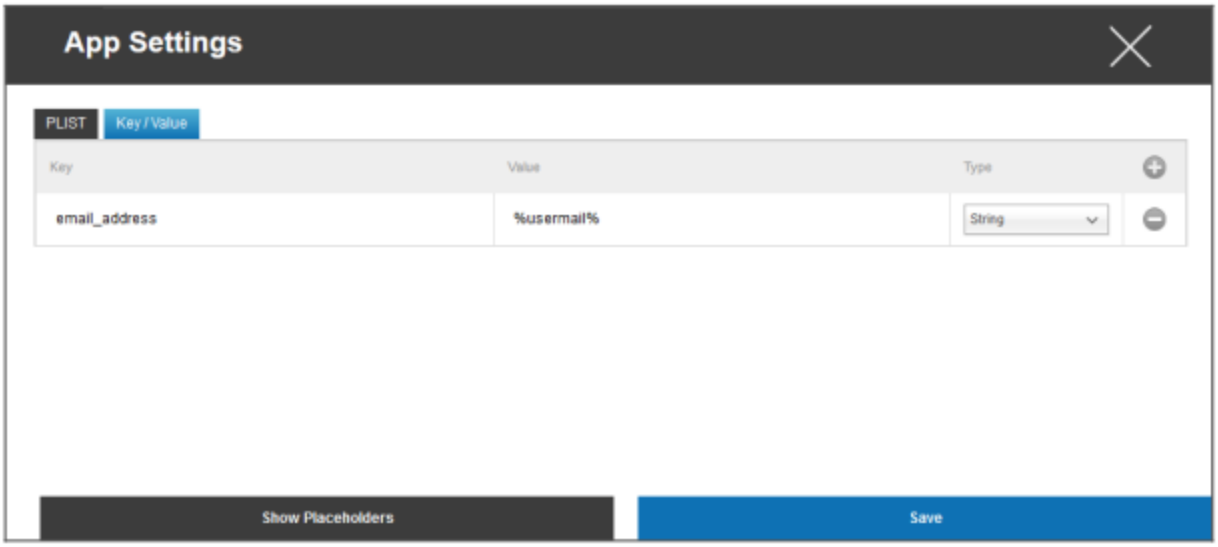


Jeśli masz już PLISTĘ (tekst źródłowy konfiguracji), możesz dodać ją tutaj i zapisać wszystko za pomocą "Zapisz".

W sekcji "Klucz/Wartość" można dołączyć określone konfiguracje do aplikacji



W tym miejscu można utworzyć nowy klucz i jego wartość za pomocą symbolu.



Oczywiście wszystkie symbole zastępcze AppTec są do Twojej dyspozycji

Wyjaśnienie "Typ":

String	Tekst
Wartość logiczna	Prawda/Fałsz
Liczba	Liczba

Za pomocą symbolu można ponownie usunąć aplikację.

Sklep z aplikacjami dla przedsiębiorstw

Aplikacje iTunes

W tym punkcie możesz dystrybuować opcjonalne aplikacje dla swojego użytkownika.

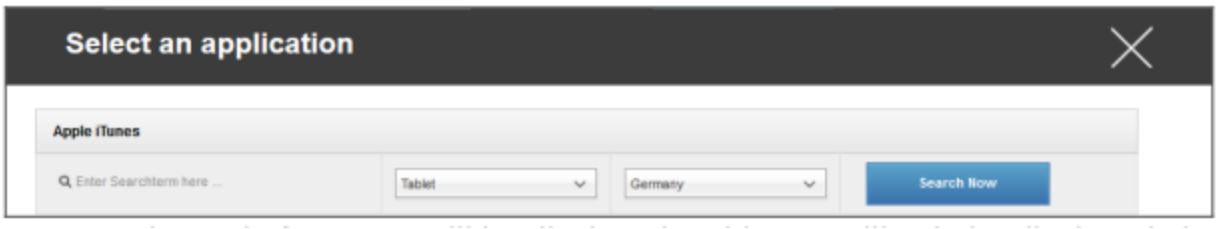
Jeśli aplikacja znajduje się tutaj, zostanie ona automatycznie zainstalowana na urządzeniu użytkownika końcowego AppTec360 Store.

Są to po prostu linki do oficjalnego sklepu Apple App Store. Z tego powodu każde urządzenie użytkownika końcowego musi być wyposażone w Apple ID.

W tym momencie zalecamy, aby każdy użytkownik miał własny identyfikator Apple ID.

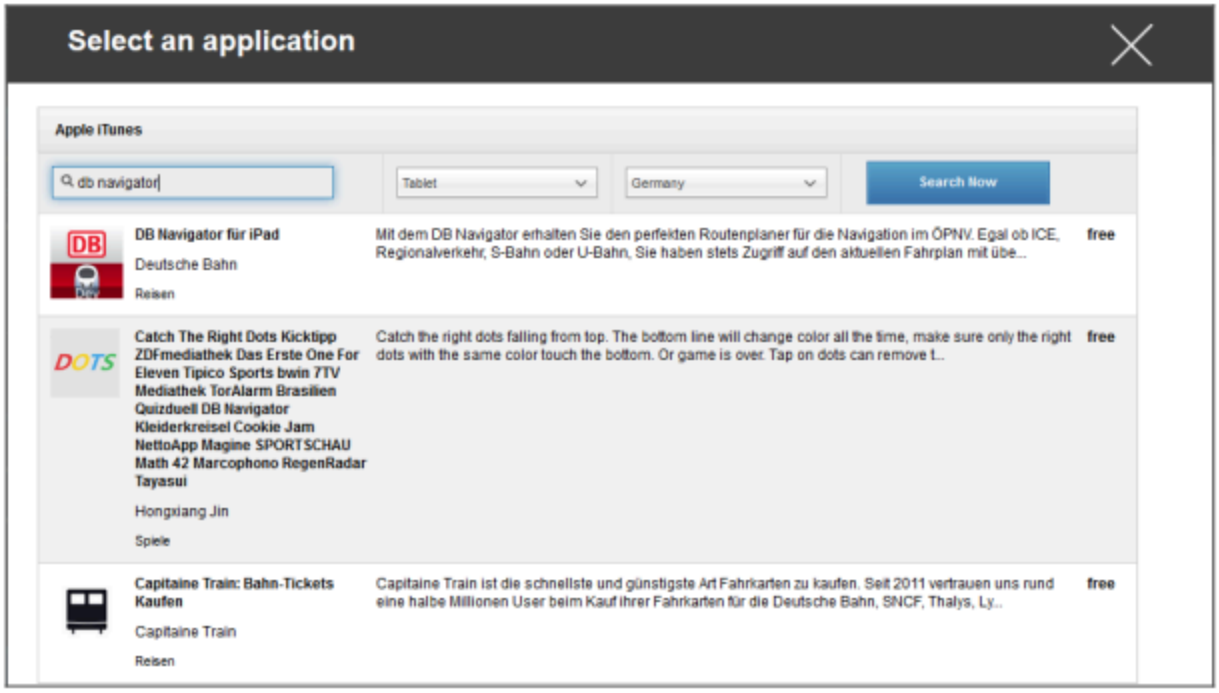
Za pomocą symbolu można dodać dodatkowe aplikacje.

Następnie powinno otworzyć się okno z następującym przeglądem.



Należy pamiętać, że wyświetlane będą tylko bezpłatne aplikacje, płatne aplikacje będą wyświetlane tylko przez VPN.

W sekcji "Enter Search Term here ..." można wyszukać aplikację dostępną w sklepie Apple App Store.



Po kliknięciu ikony lub nazwy aplikacji zostaniesz ponownie poproszony o przeprowadzenie dodatkowej konfiguracji.

Bądź na bieżąco	Raz w tygodniu będzie sprawdzane, czy dostępna jest aktualizacja aplikacji. Jeśli tak, aktualizacja zostanie zainstalowana
Usuń aplikację po usunięciu profilu MDM	W przypadku usunięcia zarządzania urządzeniem aplikacja zostanie odinstalowana
Zapobieganie tworzeniu kopii zapasowych danych aplikacji	Kopia zapasowa danych aplikacji nie zostanie utworzona.

App-VPN	Wybierz połączenie VPN, które zostanie uruchomione po otwarciu aplikacji.

Po kliknięciu przycisku "Zainstaluj" aplikacja zostanie dodana do Enterprise App Store, a następnie może zostać zainstalowana na urządzeniu użytkownika końcowego za pośrednictwem AppStore AppTec360.

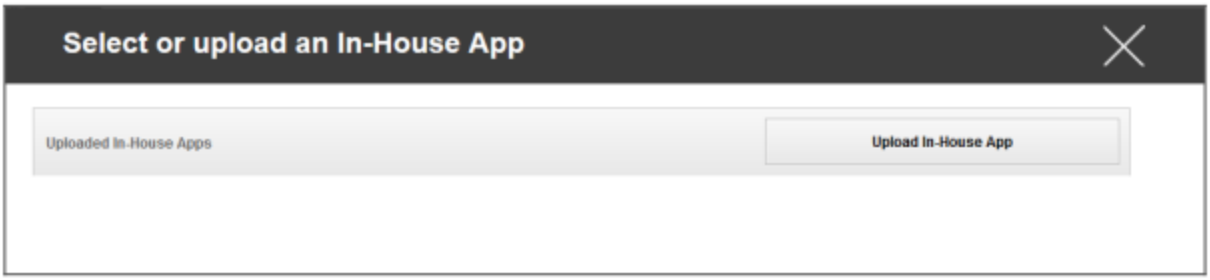
Jeśli import do App-Store zakończy się pomyślnie, otrzymasz następujący przegląd:

Wewnątrz firmy

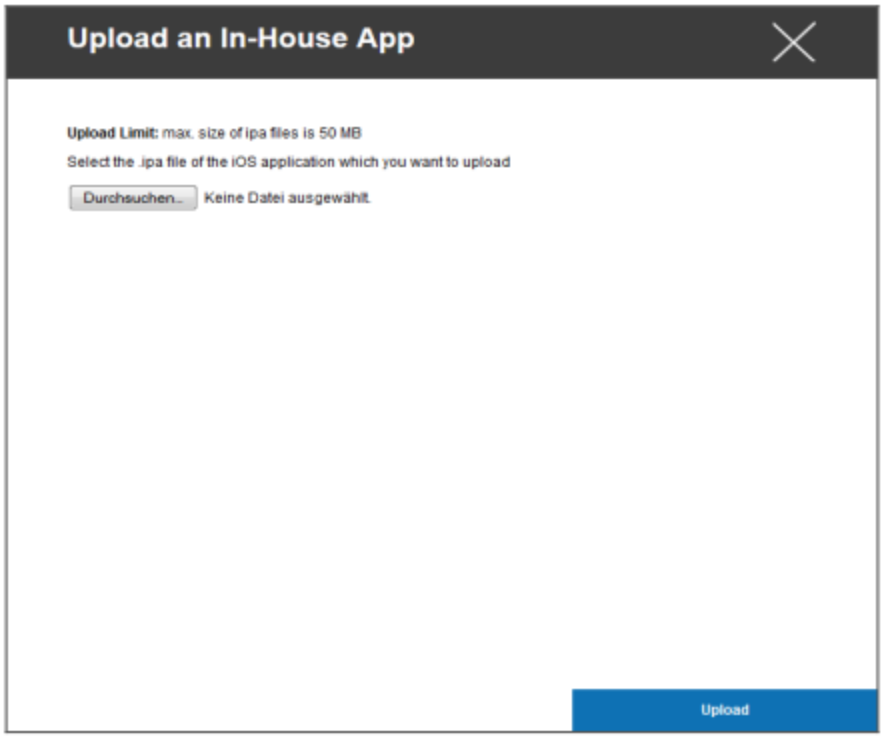
W punkcie "In-House" można przesyłać i dystrybuować wewnętrznie opracowane aplikacje.

Symbol ten umożliwia dystrybucję dodatkowych aplikacji wewnętrznych.

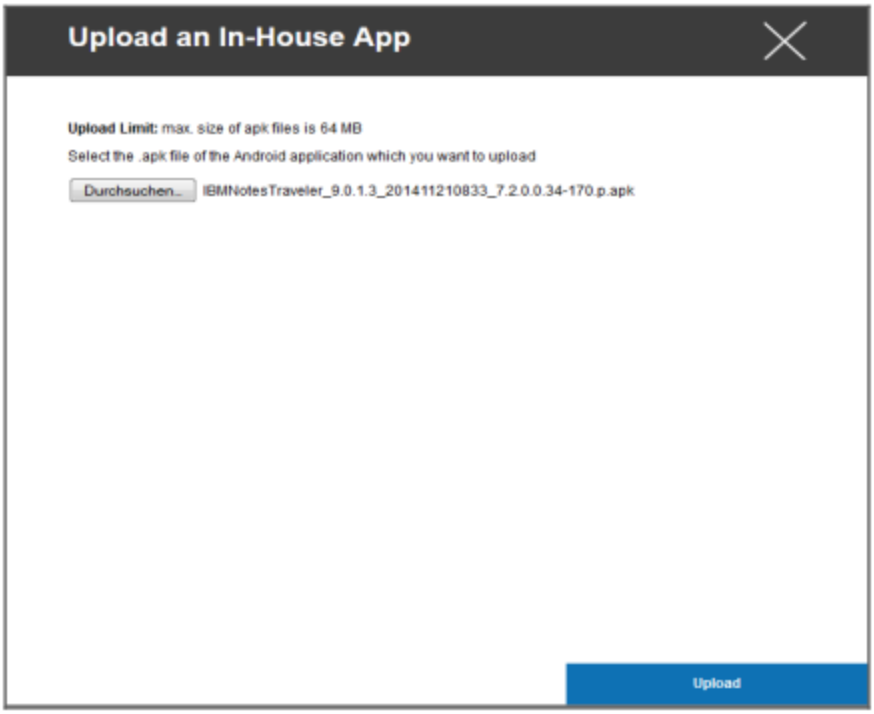
Jeśli nigdy nie dystrybuowałeś aplikacji In-House, otrzymasz następujący przegląd:



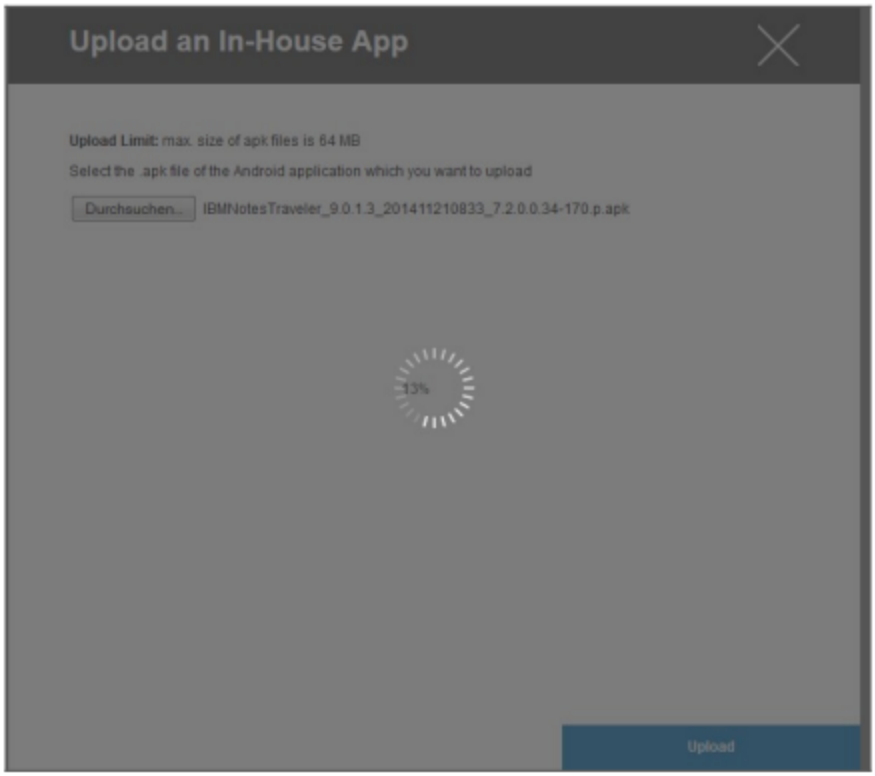
W tym celu kliknij "Prześlij aplikację wewnętrzną", a następnie otrzymasz następujący przegląd:



Teraz wybierz za pomocą "Szukaj..." plik .ipa, a następnie kliknij "Prześlij".



Aplikacja zostanie teraz przesłana. W środku okręgu możesz zobaczyć procentową ilość aplikacji, która została już przesłana.



Jeśli przesyłanie aplikacji wewnętrznej zakończy się powodzeniem, nowo przesłana aplikacja zostanie wyświetlona w katalogu aplikacji.

Użytkownik ma teraz możliwość wyświetlenia i zainstalowania tej aplikacji w AppTec360 Store na urządzeniu użytkownika końcowego, w kategorii "In-House".

Ze względu na fakt, że nie wiąże się to z publiczną aplikacją Apple AppStore, użytkownik nie potrzebuje przechowywanego identyfikatora Apple ID na urządzeniu końcowym.

Tryb kiosku

Tryb kiosku iOS jest dostępny tylko w trybie nadzorowanym

Tryb kiosku umożliwia wstępne zdefiniowanie aplikacji lub adresu URL, dzięki czemu możliwe będzie uruchamianie/odwiedzanie wyłącznie tej aplikacji/URL.

Ponadto w trybie kiosku można dezaktywować różne przyciski sprzętowe.

Typ aplikacji

Pakiet

Jeśli chcesz uruchomić aplikację w trybie kiosku, wybierz "Pakiet" w sekcji "Typ aplikacji".

Aplikacja kiosku	Kliknij tutaj, aby wybrać aplikację, która powinna zostać uruchomiona w trybie kiosku. Znajdziesz tu aktualny przegląd zarządzania aplikacjami Możesz wybrać pomiędzy "Apple iTunes Apps" i "iOS In-House Apps".

URL

Jeśli chcesz uruchomić adres URL w trybie kiosku, wybierz "URL" w sekcji "Typ aplikacji".

URL	Teraz należy zdefiniować żądany adres URL
Polityka tego samego pochodzenia	Jeśli ta funkcja jest aktywna, użytkownik może przeglądać tylko podstrony predefiniowanego adresu URL Na przykład, jeśli zdefiniowano następujący adres URL: www.mypage.com, użytkownik może przeglądać stronę www.mypage.com/subpage
Adresy URL na białej liście	Tutaj można prowadzić białą listę, wszystkie te adresy URL są dozwolone Maksymalnie 1 adres URL w wierszu Adres URL musi zaczynać się od http:/ lub https://.
Adresy URL na czarnej liście	Tutaj można utworzyć czarną listę, na której wszystkie te adresy URL są niedozwolone. Maksymalnie 1 adres URL w wierszu Adres URL musi zaczynać się od http:/ lub https://.
Wyczyść przeglądarkę po braku aktywności	Po braku aktywności pamięć podręczna przeglądarki zostanie opróżniona.
Hasło wyjścia włączone	Po aktywowaniu tej funkcji użytkownik ma możliwość zakończenia trybu kiosku za pomocą hasła, które zostało wcześniej zdefiniowane przez użytkownika
Hasło wyjścia	Jest to hasło wstępnie zdefiniowane przez użytkownika

Ustawienia trybu kiosku

Zaplanowany tryb kiosku	W oparciu o porę dnia można ustawić tryb kiosku, tak aby był on uruchamiany i kończony automatycznie o określonej wcześniej godzinie
Godzina rozpoczęcia	Czas rozpoczęcia
Czas w minutach	Czas w minutach, po którym tryb kiosku powinien zostać ponownie zakończony.
Wyłączanie dotyku	W przypadku aktywacji ekran dotykowy jest dezaktywowany
Wyłącz obracanie urządzenia	Jeśli funkcja ta jest włączona, automatyczne dostosowanie ekranu jest wyłączone
Wyłącznik dzwonka	W przypadku aktywacji przełącznik dzwonka zostanie wyłączony. Od tego momentu zachowanie zależy od wcześniej ustawionej funkcji
Wyłączanie przycisków głośności	W przypadku aktywacji przyciski głośności zostaną wyłączone
Wyłącz przycisk usypiania i budzenia	W przypadku aktywacji, włącznik/wyłącznik zostanie dezaktywowany
Wyłącz automatyczną blokadę	W przypadku aktywacji urządzenie nie zostanie przełączone w tryb gotowości
Włącz funkcję Voice Over	Jeśli funkcja ta jest włączona, aktywowany zostanie asystent Voice Over Assistant
Włącz zoom	W przypadku aktywacji, zoom zostanie włączony
Włącz odwrócenie kolorów	W przypadku aktywacji, włączony zostanie odwrócony tryb wyświetlania
Włączanie funkcji Assistive Touch	W przypadku aktywacji funkcja AssistiveTouch zostanie włączona
Włącz wybór mowy	Jeśli opcja ta jest włączona, aktywowany zostanie wybór mówienia
Włącz dźwięk mono	Jeśli opcja ta zostanie aktywowana, włączone zostanie Mono Audio
VoiceOver	W przypadku aktywacji użytkownik może włączyć funkcję VoiceOver
Zoom	W przypadku aktywacji użytkownik może włączyć funkcję Zoom
Odwróć kolory	Jeśli opcja ta jest aktywna, użytkownik może włączyć odwrócone kolory
Assistive Touch	Po aktywacji użytkownik może włączyć asystenta dotyku

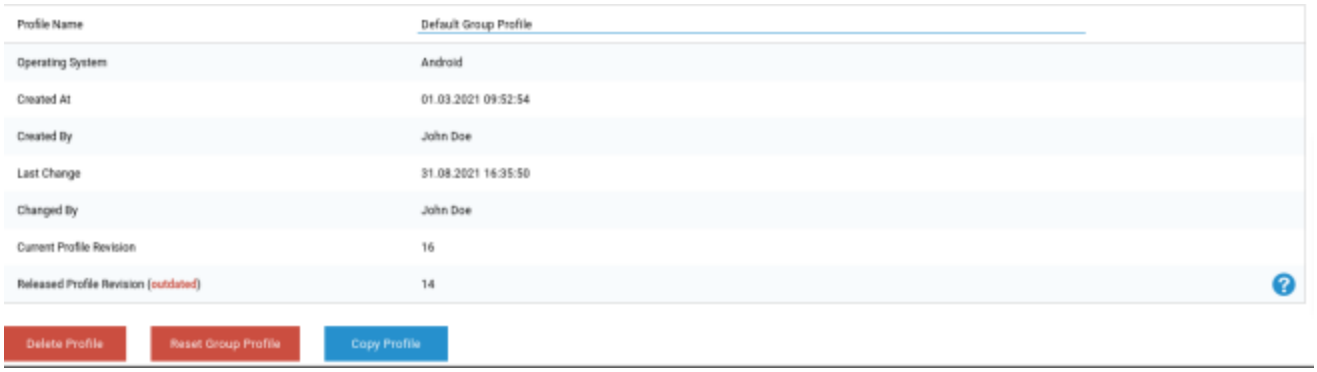
Android Enterprise – w pełni zarządzana konfiguracja urządzeń

W zależności od tego, czy aktualnie wybrano profil grupy, czy urządzenie, przegląd i jego podpunkty różnią się - należy to dokładnie rozważyć!

Ogólne

Przegląd profilu grupy (tylko na poziomie grupy)

Po otwarciu profilu grupy wyświetlony zostanie szybki przegląd profilu.



Nazwa profilu	Nazwa profilu (można ją zmienić tutaj)
System operacyjny	System operacyjny, dla którego przeznaczony jest profil
Utworzono w	Czas stworzenia
Utworzony przez	Twórca profilu
Ostatnia zmiana	Czas ostatniej zmiany profilu
Zmienione przez	Konto, które wprowadziło ostatnie zmiany
Aktualna wersja profilu	Zmiana zapisanego stanu profilu
Wydana wersja profilu	Wersja przypisanego profilu ("Przypisz teraz"). Jeśli etykieta pokazuje "(nieaktualne)" za tekstem, oznacza to, że profil został zapisany, ale nie został jeszcze przypisany, więc urządzenia nadal będą otrzymywać starszą wersję.

Przegląd urządzeń (tylko na poziomie urządzenia)

Jeśli jesteś na urządzeniu, otrzymasz podsumowanie wybranego urządzenia, które zawiera następujące informacje:

Nazwa urządzenia	Nazwa urządzenia
Lokalizacja	Współrzędne lokalizacji
Numer telefonu	Numer telefonu
Przypisane aplikacje obowiązkowe	Liczba przypisanych aplikacji obowiązkowych
Wersja systemu operacyjnego	Wersja systemu operacyjnego urządzenia
System operacyjny	System operacyjny (Android Enterprise)
Numer seryjny	Numer seryjny urządzenia
Własność urządzenia	Urządzenie firmowe lub prywatne
Typ urządzenia	Urządzenie zarządzane AE Work
Zakorzeniony	Status, wskazujący, czy urządzenie zostało zrootowane.
Zgodność	Zgodność z wytycznymi
Adres IP	Adres IP urządzenia
Ostatnio widziany	Punkt w czasie, kiedy urządzenie ostatnio łączyło się z AppTec
Last Push	Punkt w czasie, w którym do urządzenia wysłano ostatnią wiadomość push.
Tryb właściciela urządzenia AE	Tak
Przypisanie użytkownika	Użytkownik lub grupa, do której przypisane jest urządzenie

Wersja konfiguracji (tylko na poziomie urządzenia)

W tym miejscu można sprawdzić, który profil grupy jest przypisany do urządzenia.

Jeśli klikniesz profil grupy, uzyskasz bezpośredni dostęp do tego profilu i będziesz mógł dokonać ustawień.

Za pomocą tego symbolu można przywrócić rozproszone aplikacje do ustawień profilu grupy.

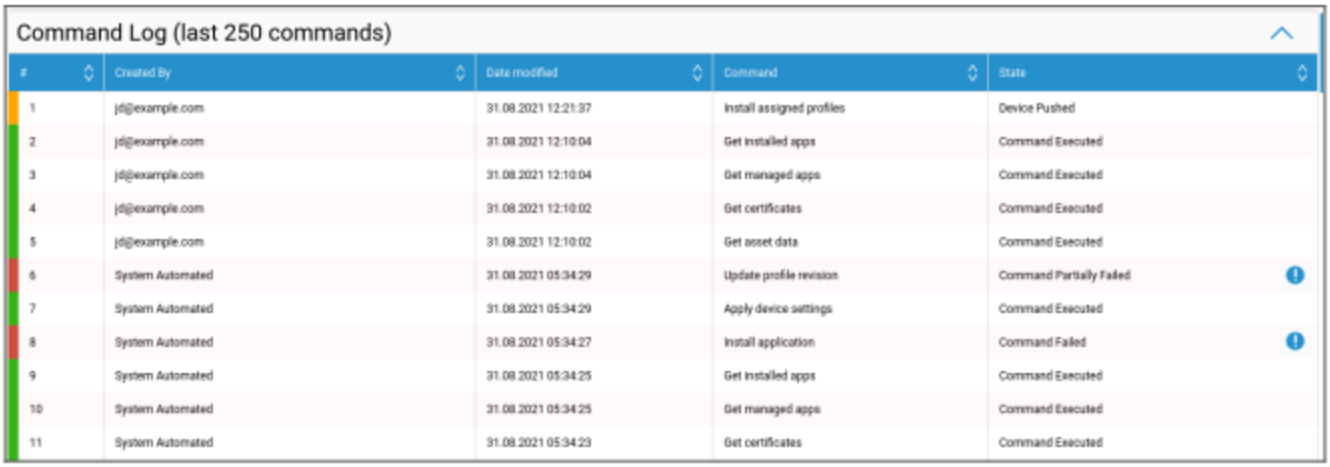
Za pomocą tego symbolu można przywrócić wszystkie używane aplikacje do ustawień profilu grupy.

"Newer Revision available" oznacza, że profil grupy został zmieniony i zapisany, ale nie został przypisany. Profil grupy musi zostać przypisany za pomocą opcji "Przypisz teraz" na poziomie grupy, aby zastosować zmiany do urządzeń.

Dziennik urządzenia (tylko na poziomie urządzenia)

Dziennik poleceń

Tutaj można sprawdzić, które polecenia zostały wydane dla urządzenia i jaki jest ich status.



Polecenia utworzone przez "System Automated" są automatycznie tworzone przez system.

Możliwe statusy poleceń

Urządzenie wciśnięte	Żądanie push zostało wysłane do usługi push (np. APNS), aby poinformować urządzenie o konieczności połączenia się z serwerem EMM.
Utworzone polecenie	Polecenie zostało utworzone w systemie.
Wysłane polecenie	Polecenie zostało wysłane do urządzenia po nawiązaniu połączenia z serwerem.
Polecenie wykonane	Polecenie zostało pomyślnie wykonane.
Polecenie nie powiodło się	Polecenie nie powiodło się. *
Polecenie częściowo nieudane	W zależności od systemu operacyjnego urządzenia niektóre polecenia mogą zostać zgrupowane. W tym przypadku niektóre części tej grupy poleceń nie powiodły się. *
Polecenie wykonane, ostatecznie nieudane	Polecenie zostało wykonane, ale być może nie.
Przesunięcie polecenia	Polecenie zostało powtórzone przez użytkownika.
Odrzucony	Polecenie zostało odrzucone. Na przykład dlatego, że zostało zastąpione przez inne polecenie lub urządzenie zostało ponownie zarejestrowane, a stare polecenia zostały usunięte.

Jeśli za wiadomością znajduje się wykrzyknik, można uzyskać więcej informacji, najeżdżając kursorem na ikonę.

Ustawienia urządzenia

Konfiguracja klienta

W tym miejscu można przeprowadzić następujące konfiguracje na urządzeniu z systemem Android:

Czas niezgodności	Limit czasu odpowiedzi użytkownika, po którym stosowana jest akcja wymuszania.
Działania egzekucyjne po przekroczeniu limitu czasu zgodności	Egzekwowanie działań, gdy użytkownik nie wykonuje czynności, które prowadzą do stanu zgodnego urządzenia
Częstotliwość zbierania danych	Częstotliwość gromadzenia informacji o urządzeniu/GPS
Częstotliwość uderzeń serca urządzenia	Interwał, w którym urządzenie powinno kontaktować się z serwerem AppTec360 Min. 1 minuta Maks. 24 godziny
Włącz aktualizacje lokalizacji	W przypadku aktywacji urządzenie wysyła aktualizacje lokalizacji do serwera AppTec360.
Czas aktualizacji lokalizacji	Określa, w jakich odstępach czasu urządzenie wysyła aktualizacje lokalizacji do AppTec360.
Użyj dokładności lokalizacji Google do aktualizacji lokalizacji	Jeśli jest włączona, lokalizacja sieciowa będzie używana do aktualizacji lokalizacji (jeśli została wyłączona w sekcji "Ograniczenia", to ustawienie to nie będzie miało żadnego wpływu).
Używanie lokalizacji GPS do aktualizacji lokalizacji	Jeśli jest włączona, GPS będzie używany do aktualizacji lokalizacji
Zezwalaj na fałszywe lokalizacje	Umożliwia fałszowanie informacji o lokalizacji za pośrednictwem aplikacji innych firm.
Akcja Utracone połączenie	Jeśli opcja ta jest włączona, można określić działanie w przypadku, gdy urządzenie nie uzyska połączenia z serwerem MDM w interwale pulsu. Na przykład, jeśli urządzenie ma czas bicia serca wynoszący 5 minut, łączy się z serwerem o godzinie 10:35. Następnie urządzenie opuszcza zasięg Wi-Fi. Następne bicie serca o 10:40 nie powiedzie się i zostanie wykonana określona akcja.

Działanie	Działanie, które należy podjąć, gdy tylko urządzenie stanie się niezgodne. • Urządzenie blokujące = urządzenie blokujące • Wipe Device = urządzenie zostanie przywrócone do ustawień fabrycznych. • Wipe Device & SD Card = urządzenie zostanie przywrócone do ustawień fabrycznych, a pamięć karty SD zostanie usunięta.
Próg	Można określić próg nieudanych uderzeń serca, które są niezbędne do wyzwolenia określonej akcji.

Tryb egzekwowania zasad	Domyślnie:	Użytkownicy będą okresowo monitowani o wykonanie zaległych działań
	Leniwe egzekwowanie zasad:	Użytkownicy nigdy nie będą proszeni o wykonanie zaległych akcji. Wszystkie otwarte akcje będą wyświetlane w kliencie AppTec360.
	Agresywne egzekwowanie zasad:	Użytkownicy będą nieustannie proszeni o wykonanie zaległych działań
Blokada wersji AppTec360	Jeśli ta opcja jest włączona, można określić kod wersji dla AppTec360 MDM Client. Klient AppTec360 będzie aktualizowany tylko do określonej wersji. Nowsze wersje będą ignorowane. Obniżenie wersji NIE jest możliwe.	
Kod wersji	Kod wersji klienta AppTec360 MDM, który ma zostać zablokowany.	
Wyłączanie powiadomień AppTec360	Jeśli opcja ta zostanie wyłączona, klient AppTec360 nie będzie wyświetlał powiadomienia na pasku powiadomień. W ten sposób użytkownicy mogą zamknąć klienta AppTec360 za pośrednictwem menedżera zadań. Jeśli klient AppTec360 jest zamknięty, kilka funkcji, w tym tryb kiosku i czarna/biała lista aplikacji, nie będzie działać poprawnie. Urządzenia Samsung oferują mechanizm ochrony dla klienta AppTec360. Powiadomienie jest domyślnie wyłączone na urządzeniach Samsung obsługujących API KNOX. Powiadomienie nie powinno być wyłączone na urządzeniach z systemem Android 8.0 lub nowszym.	

Tapeta

Ustaw niestandardową tapetę	Włączanie/wyłączanie niestandardowej tapety
Tapeta	Ustawienie trybu tapety na użycie kodu koloru lub obrazu
Określ kolor	Określ kolor tła jako wartość szesnastkową, np. #000000 dla czarnego lub #ffffff dla białego.
Ustaw obraz jako tapetę	Prześlij plik obrazu, którego chcesz użyć jako tapety.

Zarządzanie zasobami (tylko na poziomie urządzenia)

Informacje o urządzeniu

Model	Oznaczenie modelu urządzenia
System operacyjny	OS
Wersja systemu operacyjnego	Wersja systemu operacyjnego
Numer seryjny	Numer seryjny
Nazwa urządzenia	Nazwa urządzenia
Stan akumulatora	Stan akumulatora
Pamięć wolna / całkowita	Pamięć wolna / całkowita
Samsung Safe	Interfejs Samsung SAFE, wymagany dla różnych opcji ustawień
Dostępna karta SD	Dostępna karta SD
Emulowana karta SD	Emulowana karta SD
Wyjmowana karta SD	Wyjmowana karta SD
SD Free / Pamięć całkowita	Wolna pamięć SD / całkowita pamięć karty SD

Wi-Fi

Adres IP	Adres IP urządzenia
WiFi MAC	Adres MAC sieci Wi-Fi

Komórkowy

Status	Status (zainstalowana karta SIM)
Numer telefonu	Numer telefonu
Roaming (połączenia głosowe / transmisja danych)	Roaming dla połączeń głosowych / transmisji danych
Status roamingu	Bieżący status roamingu
Adres IP	Adres IP
Operator/Przewoźnik	Operator/Przewoźnik
Technologia komórkowa	Technologia komórkowa
IMEI	Numer IMEI
ICCID	Jest to identyfikator karty SIM, często również karty Smartcard lub Integrated Circuit Card (ICC).
IMSI	International Mobile Subscriber Identity (IMSI) zapewnia w sieciach GSM i UMTS jednoznaczną identyfikację użytkowników sieci. IMSI składa się z maksymalnie 15 cyfr i jest konfigurowany w następujący sposób: • Kod kraju sieci komórkowej (MCC), 3 cyfry • Kod sieci komórkowej (MNC), 2 lub 3 cyfry • Numer identyfikacyjny abonenta sieci komórkowej (MSIN), 1-10 cyfr
Obecny MCC/MNC	Patrz "SIM MCC/MNC"
SIM MCC/MNC	Kod kraju sieci komórkowej to ustalony identyfikator kraju, określony przez ITU zgodnie ze standardem E.212. Działa on w połączeniu z kodem sieci komórkowej (MNC) w celu identyfikacji sieci komórkowej. Oznacza kod kraju/sieci komórkowej karty SIM. Jeśli korzystasz z roamingu w innej sieci komórkowej, logicznie rzecz biorąc, "Bieżące MCC/MNC" i "SIM MCC/MNC" będą się różnić.

Bluetooth

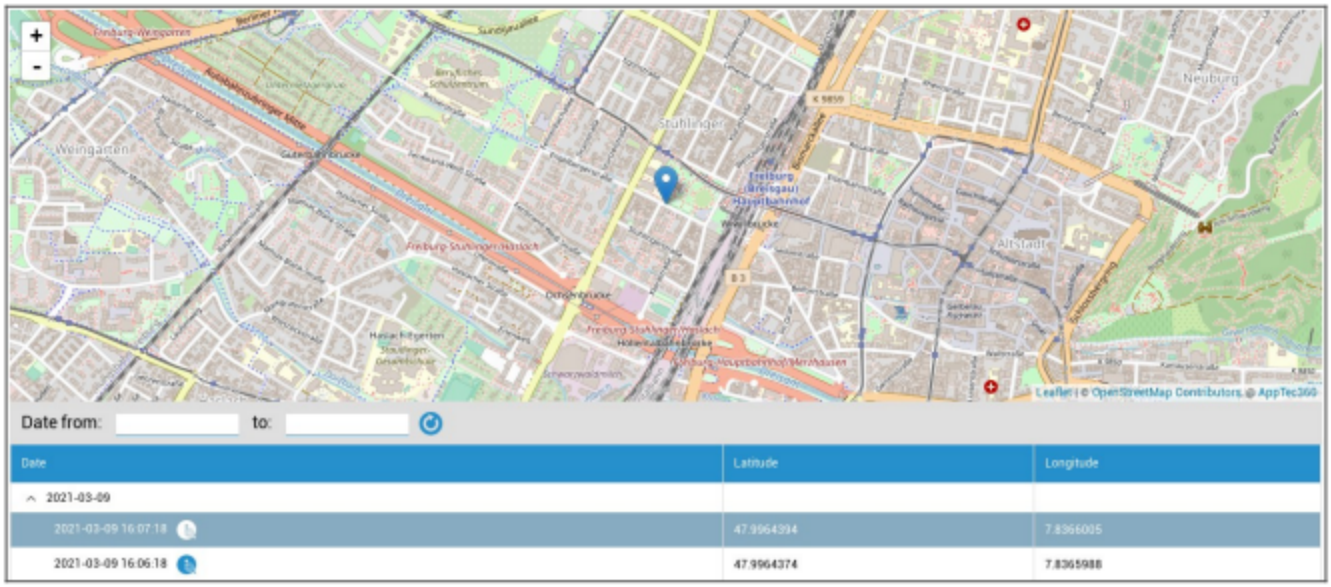
Bluetooth MAC	Adres MAC Bluetooth

Zarządzanie bezpieczeństwem

Ochrona przed kradzieżą (tylko na poziomie urządzenia)

Informacje GPS (tylko na poziomie urządzenia)

Tutaj można ustalić bieżącą/ostatnią lokalizację urządzenia. Lokalizacja może być chroniona jednym lub nawet dwoma hasłami - patrz: Ustawienia ogólne - Prywatność - Dostęp GPS



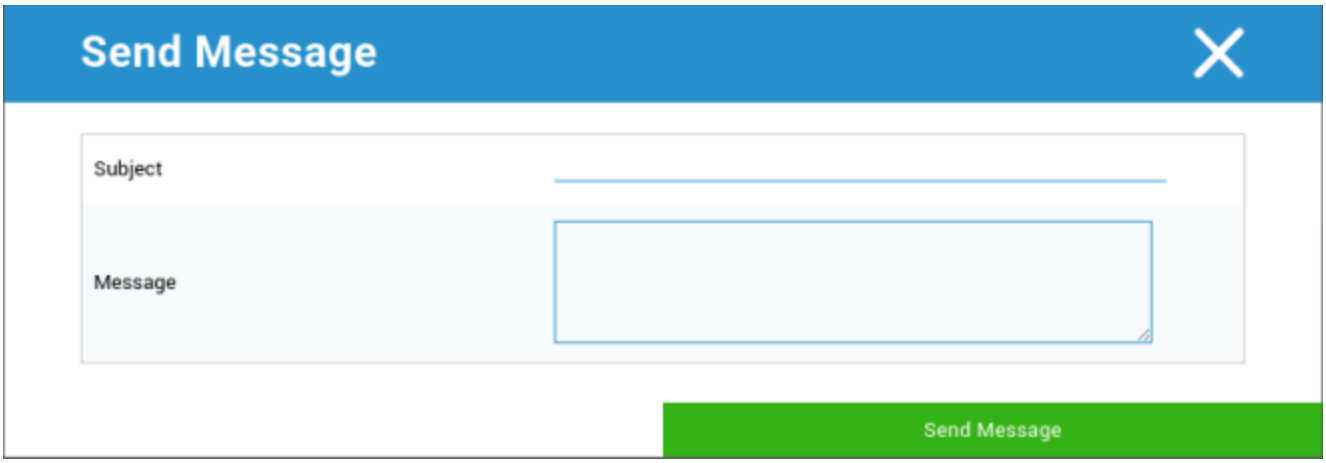
Wipe & Lock (tylko na poziomie urządzenia)

W sekcji "Wyczyść i zablokuj" można wykonać następujące trzy czynności:

Pełne wytarcie	Urządzenie jest przywracane do ustawień fabrycznych (dane firmowe i osobiste są usuwane).
Enterprise Wipe	Z urządzenia użytkownika końcowego usuwane są wyłącznie dane firmowe (wszystkie aplikacje, dane itp. dostarczone przez AppTec360).
Ekran blokady	Blokada ekranu jest aktywna, wystarczy odblokować urządzenie za pomocą hasła / kodu PIN urządzenia.

Wiadomość (tylko na poziomie urządzenia)

Tutaj można wpisać temat i wiadomość, a następnie wysłać ją na urządzenie użytkownika końcowego.



Konfiguracja zabezpieczeń

Kod dostępu urządzenia

W sekcji "Kod dostępu" można ustawić hasło urządzenia, dostępne są następujące opcje ustawień

Minimalna długość hasła	Ustala minimalną liczbę symboli, które musi zawierać hasło	
Jakość hasła	Nieokreślony	Niniejsza polityka nie zawiera żadnych wymagań dotyczących hasła.
	Słabość biometryczna	Polityka ta zezwala na stosowanie technologii rozpoznawania biometrycznego o niskim poziomie bezpieczeństwa. Oznacza to technologie, które mogą rozpoznać tożsamość osoby do około 3-cyfrowego kodu PIN (fałszywe wykrycie jest mniejsze niż 1 na 1000).
	Coś	Ta polityka wymaga ustawienia pewnego rodzaju hasła lub wzorca, ale nie wymusza żadnych konkretnych reguł.
	Alfabetyczny	Użytkownik musi wprowadzić hasło zawierające co najmniej znaki alfabetu (lub inne symbole).
	Alfanumeryczne	Użytkownik musi wprowadzić hasło zawierające co najmniej znaki numeryczne i alfabetyczne (lub inne symbole).
	Kompleks	Domyślnie użytkownik musi wprowadzić hasło zawierające co najmniej literę, cyfrę i symbol specjalny. Dzięki tej jakości hasła można ograniczyć do różnych zestawów znaków, takich jak co najmniej wielka litera itp.
Minimalna długość hasła	Ustaw wymaganą liczbę znaków dla hasła. Można na przykład wymagać, aby kod PIN lub hasło miały co najmniej sześć znaków.	
Minimalne cyfry wymagane w haśle	Minimalne cyfry wymagane w haśle	
Minimalne małe litery wymagane w haśle	Minimalne małe litery wymagane w haśle	
Minimalne wielkie litery wymagane w haśle	Minimalne wielkie litery wymagane w haśle	

Minimalna liczba znaków nieliterowych wymaganych w haśle	Minimalna liczba znaków nieliterowych wymaganych w haśle
Minimalne symbole wymagane w haśle	Minimalne symbole wymagane w haśle

Maksymalna blokada czasu nieaktywności	Maksymalny czas nieaktywności użytkownika do blokady czasowej
Limit czasu wygaśnięcia hasła	Ustala, po jakim czasie hasło wygasa i musi zostać wydane nowe hasło.
Ograniczenie historii haseł	Liczba poprzednio używanych haseł, które nie są dozwolone
Maksymalna liczba nieudanych prób podania hasła	Ustala, jak często hasło może być wprowadzane niepoprawnie, zanim zostanie wykonane całkowite czyszczenie urządzenia.
Zezwalaj na uwierzytelnianie biometryczne	Umożliwia uwierzytelnianie za pomocą odcisku palca lub skanu tęczówki. Tylko dla Samsung KNOX 2.1 i nowszych wersji

Antywirus

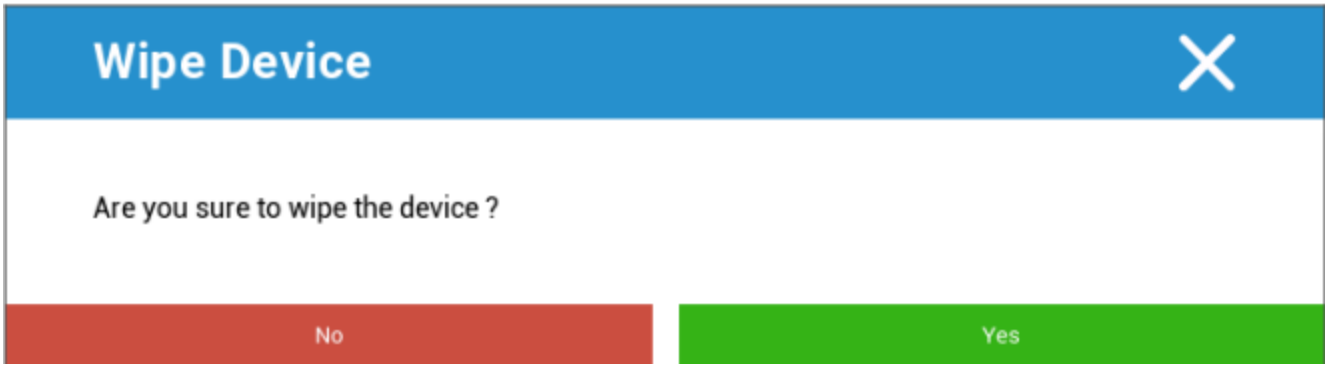
Automatyczne skanowanie	Włącz okresowe automatyczne skanowanie
Interwał skanowania	Interwał badania (szybki / pełny)
Pełne automatyczne skanowanie	Włącz w pełni automatyczne skanowanie
Automatyczne aktualizacje	Włącz automatyczne aktualizacje
Interwał sprawdzania aktualizacji	Jak często aplikacja i jej baza danych powinny być aktualizowane (wirusy / uszkodzony kod)?
Ochrona aplikacji	Włącz automatyczne skanowanie aplikacji
Ochrona karty SD	Włącz automatyczne skanowanie karty SD
Aktualizacja tylko przez Wi-Fi	Po włączeniu tej opcji aktualizacje będą stosowane tylko wtedy, gdy urządzenie zostanie pomyślnie połączone z siecią Wi-Fi.

Koniec życia (tylko na poziomie urządzenia)

Wipe (tylko na poziomie urządzenia)

W sekcji "Wipe" można przywrócić urządzenie do ustawień fabrycznych. W tym przypadku dane firmowe i prywatne zostaną usunięte z urządzenia użytkownika końcowego.

Kliknięcie na "Symbol minus" spowoduje wyświetlenie następującego komunikatu:



Po wybraniu opcji "Tak" można wykonać czyszczenie.

W sekcji "Wipe Report" można wyświetlić następujące elementy

Wymazane przez	Historia tego, kto wykonał czyszczenie
Data	Data
Status	Status (np. czy czyszczenie zostało wykonane pomyślnie)

Ustawienia ograniczeń

Ograniczenia

Tutaj różne rzeczy mogą być ograniczane i blokowane.

Włącz kamerę	Zezwalaj na korzystanie z kamery	
Wymuś automatyczną synchronizację	Na	Synchronizacja jest włączona na stałe
	Wył.	Synchronizacja jest trwale wyłączona
	Wybór użytkownika	Wybrany przez użytkownika
Force Bluetooth	Na	Bluetooth jest włączony na stałe
	Wył.	Bluetooth jest trwale wyłączony
	Wybór użytkownika	Wybrany przez użytkownika
Force GPS	Na	GPS jest aktywowany na stałe
	Wył.	GPS jest trwale wyłączony
	Wybór użytkownika	Wybrany przez użytkownika
Lokalizacja sieci sił	Na	Stała lokalizacja w Internecie
	Wył.	Trwała dezaktywacja lokalizacji internetowej
	Wybór użytkownika	Wybrany przez użytkownika

Bezpieczeństwo		
Nie zezwalaj na udostępnianie lokalizacji	Określa, czy użytkownik nie może włączyć udostępniania lokalizacji.	
Nie zezwalaj na bezpieczny rozruch	Określa, czy użytkownik nie może ponownie uruchomić urządzenia w trybie bezpiecznego rozruchu.	
Nie zezwalaj na resetowanie sieci	Określa, czy użytkownik nie może resetować ustawień sieciowych w Ustawieniach.	
Nie zezwalaj na przywracanie ustawień fabrycznych	Określa, czy użytkownik nie może resetować urządzenia.	
Włącz ADB	Umożliwia połączenie z komputerem PC przez ADB	
Wyłącz Keyguard	Wyłącza Keyguard	
Właściciel urządzenia Informacje o ekranie blokady	Ustawia informacje o właścicielu urządzenia wyświetlane na ekranie blokady.	
Egzekwowanie zgodności	Tryb Monituj użytkownika	Użytkownik zostanie poproszony o wykonanie niezbędnych czynności.
	Pojemnik z blokadą trybu	Ukryj wszystkie aplikacje do momentu spełnienia wszystkich wymagań

Zarządzanie aplikacjami	
Zezwalaj na łączenie aplikacji między profilami	Umożliwia aplikacjom w profilu nadrzędnym obsługę łączy internetowych z profilu zarządzanego.
Nie zezwalaj na kontrolę aplikacji	Określa, czy użytkownik nie może modyfikować aplikacji w ustawieniach lub programach uruchamiających.
Nie zezwalaj na instalację aplikacji	Określa, czy użytkownik nie może instalować aplikacji.
Nie zezwalaj na odinstalowywanie aplikacji	Określa, czy użytkownik nie może odinstalowywać aplikacji.
Polityka uprawnień środowiska uruchomieniowego	Określa sposób obsługi nowych żądań uprawnień od aplikacji.
Zezwalaj na nieznane źródła	Jeśli opcja ta jest włączona, użytkownicy mogą pobierać aplikacje poprzez instalację pliku .apk.

Łączność	
Nie zezwalaj na konfigurację sieci komórkowej	Określa, czy użytkownik nie może konfigurować sieci komórkowych.
Wyłącz konfigurację tetheringu	Określa, czy użytkownik nie może konfigurować tetheringu i przenośnych hotspotów.
Nie zezwalaj na konfigurację VPN	Określa, czy użytkownik nie może konfigurować sieci VPN.
Nie zezwalaj na konfigurację Wi-Fi	Określa, czy użytkownik nie może zmieniać punktów dostępu WiFi.
Nie zezwalaj na wychodzącą wiązkę NFC	Określa, czy użytkownik nie może używać NFC do przesyłania danych z aplikacji.
Zablokuj konfigurację WiFi	To ustawienie kontroluje, czy konfiguracje WiFi utworzone przez aplikację właściciela urządzenia powinny być zablokowane (tj. edytowalne lub usuwalne tylko przez aplikację właściciela urządzenia, nawet przez aplikację Ustawienia).
Włącz roaming danych	Aktywuje roaming danych

Bluetooth	
Wyłącz Bluetooth	Określa, czy bluetooth jest niedozwolony na urządzeniu. Wymaga systemu Android 8.0
Wyłącz udostępnianie Bluetooth	Określa, czy wychodzące udostępnianie Bluetooth jest niedozwolone na urządzeniu. Wymaga systemu Android 8.0
Wyłącz konfigurację Bluetooth	Określa, czy użytkownik nie może konfigurować bluetooth.

Zarządzanie kontem	
Nie zezwalaj na dodawanie profilu zarządzanego	Określa, czy użytkownik nie może dodawać zarządzanych profili. Wymaga systemu Android 8.0
Nie zezwalaj na dodawanie użytkowników	Określa, czy użytkownik nie może dodawać nowych użytkowników.
Nie zezwalaj na usuwanie profilu zarządzanego	Określa, czy zarządzane profile tego użytkownika mogą być usuwane w inny sposób niż przez właściciela profilu. Wymaga systemu Android 8.0
Nie zezwalaj na modyfikację konta	Określa, czy użytkownik nie może dodawać i usuwać kont, chyba że zostały one dodane programowo przez Authenticator.

Telefonia	
Nie zezwalaj na połączenia wychodzące	Określa, że użytkownik nie może wykonywać wychodzących połączeń telefonicznych.
Nie zezwalaj na SMS-y	Określa, że użytkownik nie może wysyłać ani odbierać wiadomości SMS.

System	
Nie zezwalaj na tworzenie okien	Określa, że okna poza oknami aplikacji nie powinny być tworzone.
Nie zezwalaj na ustawianie ikony użytkownika	Określa, czy użytkownik nie może zmienić swojej ikony.
Nie zezwalaj na ustawianie tapet	Ograniczenie użytkownika uniemożliwiające ustawienie tapety.
Wyłącz pasek stanu	Wyłączenie paska stanu blokuje powiadomienia, szybkie ustawienia i inne nakładki ekranowe, które umożliwiają ucieczkę z urządzenia jednorazowego użytku.
Włącz automatyczny czas	Automatycznie ustawia godzinę.
Włącz automatyczną strefę czasową	Automatycznie ustawia strefę czasową.
Pozostaje włączony po podłączeniu	Urządzenie pozostanie aktywne po podłączeniu do źródła zasilania.

Przechowywanie	
Nie zezwalaj na wyłączanie weryfikacji aplikacji	Określa, czy użytkownik nie może wyłączyć weryfikacji aplikacji.
Nie zezwalaj na montowanie nośników fizycznych	Określa, czy użytkownik nie może montować fizycznych nośników zewnętrznych.
Włącz usługę kopii zapasowej	Usługa kopii zapasowych zarządza wszystkimi mechanizmami tworzenia kopii zapasowych i przywracania danych na urządzeniu. Ustawienie tej opcji na wartość false uniemożliwi tworzenie kopii zapasowych lub przywracanie danych. Usługa kopii zapasowej jest domyślnie wyłączona. Wymaga systemu Android 8.0
Włączanie pamięci masowej USB	Umożliwia korzystanie z pamięci masowej USB.

Klawiatura	
Wyłącz autouzupełnianie	Określa, czy użytkownik nie może korzystać z usług autouzupełniania. Wymaga systemu Android 8.0
Nie zezwalaj na kopiowanie i wklejanie między profilami	Określa, czy zawartość skopiowana do schowka tego profilu może zostać wklejona do powiązanych profili.

Dźwięk	
Nie zezwalaj na korektę głośności	Określa, czy użytkownik nie może regulować głośności głównej.
Wyłącz wyciszenie mikrofonu	Określa, czy użytkownik nie może regulować głośności mikrofonu.
Urządzenie wyciszające	Urządzenie wyciszające.

Zarządzanie certyfikatami

Tutaj możesz dystrybuować zaufane certyfikaty i certyfikaty tożsamości na swoje urządzenia.

System Android 8 lub nowszy jest wymagany do dystrybucji zaufanych certyfikatów, a system Android 9 lub nowszy jest wymagany do dystrybucji certyfikatów tożsamości.

Za pomocą "+" można dodać wiele certyfikatów.

Zaufane certyfikaty muszą być w formacie PEM.

Certyfikaty tożsamości muszą być w formacie PKCS12

Zarządzanie połączeniami

Wifi

W przypadku tego ustawienia należy przeprowadzić wstępną konfigurację urządzeń użytkowników końcowych w celu uzyskania dostępu do wewnętrznych punktów dostępu

.

Identyfikator zestawu usług (SSID)	SSID dla sieci, która ma być połączona
Ukryta sieć	Aktywuj, jeśli punkt dostępowy nie rozgłasza identyfikatora SSID

Typ zabezpieczenia

Ustalenie typu zabezpieczeń punktu dostępowego

WEP

Hasło	Hasło do punktu dostępowego

WPA/WPA2

Hasło	Hasło do punktu dostępowego

802.1x EAP

Metoda EAP

PWD	Tożsamość	Tożsamość
	Hasło	Hasło

PEAP	Protokół uwierzytelniania fazy 2	brak	Brak dodatkowego protokołu
		MSCHAPV2	Protokół MSCHAPV2
		GTC	Protokół GTC
	Certyfikat CA	Certyfikat CA	
	Tożsamość	Tożsamość	
	Anonimowa tożsamość	Anonimowa tożsamość	
	Hasło	Hasło	

TTLS	Protokół uwierzytelniania fazy 2	brak	Brak dodatkowego protokołu
		PAP	Protokół PAP
		MSCHAP	Protokół MSCHAP
		MSCHAPV2	Protokół MSCHAPV2
		GTC	Protokół GTC
	Certyfikat CA	Certyfikat CA	
	Tożsamość	Tożsamość	
	Anonimowa tożsamość	Anonimowa tożsamość	
	Hasło	Hasło	

TLS	Certyfikat CA	Certyfikat CA
	Tożsamość	Tożsamość
	Hasło	Hasło

VPN

Nazwa połączenia	Nazwa połączenia VPN

Typ VPN

VPN

Klient VPN

Klient VPN AppTec360	
Konfiguracja bramy	Wybierz konfigurację Gateway VPN (patrz **Ustawienia ogólne > Universal Gateway > Ustawienia VPN**).
Always On VPN	Włącz blokadę natywną
Włącz blokadę AppTec360	Włącz blokadę AppTec360

Wbudowany (dostępny tylko w urządzeniach Samsung)			
Typ połączenia	PPTP	Serwer	Serwer
		Włącz szyfrowanie PPTP	Włącz szyfrowanie PPTP
	L2TP / IPSec PSK	Serwer	Serwer
		Klucz wstępny IPSec	Klucz wstępny IPSec
		Włącz L2TP Secret	Włącz L2TP Secret
		L2TP Secret	L2TP Secret
	IPSec XAuth PSK	Serwer	Serwer
		Identyfikator IPSec	Identyfikator IPSec
		Klucz wstępny IPSec	Klucz wstępny IPSec
Domeny wyszukiwania DNS	Domeny wyszukiwania DNS		
Ustawienia eksperckie	Serwery DNS	Serwery DNS	
	Trasy przekazywania	Trasy przekazywania	

Open VPN		
Serwer	Serwer	
Profil OpenVPN	Profil OpenVPN	
Aplikacja OpenVPN	OpenVPN dla systemu Android (zalecane)	
	OpenVPN Connect	
Ustawienia eksperckie	Serwery DNS	Serwery DNS
	Trasy przekazywania	Trasy przekazywania

Samsung / Strong Swan			
Typ połączenia	PPTP	Serwer	Serwer
		Nazwa użytkownika	Nazwa użytkownika
		Hasło	Hasło
		Włącz szyfrowanie PPTP	Włącz szyfrowanie PPTP
	L2TP / IPSec PSK	Serwer	Serwer
		Klucz wstępny IPSec	Klucz wstępny IPSec
		Nazwa użytkownika	Nazwa użytkownika
		Hasło	Hasło
		Włącz L2TP Secret	L2TP Secret
	IPSec XAuth PSK	Serwer	Serwer
		Identyfikator IPSec	Identyfikator IPSec
		Klucz wstępny IPSec	Klucz wstępny IPSec
		Nazwa użytkownika	Nazwa użytkownika
		Hasło	Hasło
Ustawienia eksperckie	Serwery DNS	Serwery DNS	
	Trasy przekazywania	Trasy przekazywania	

Cisco Any Connect		
Serwer	Serwer	
Tryb certyfikatu	Wyłączony	Wyłączony
	Automatyczny	Automatyczny
Ustawienia eksperckie	Serwery DNS	Serwery DNS
	Trasy przekazywania	Trasy przekazywania

VPN dla poszczególnych aplikacji

Klient VPN

Klient VPN AppTec360		
Konfiguracja bramy	Wybierz konfigurację Gateway VPN (patrz **Ustawienia ogólne > Universal Gateway > Ustawienia VPN**).	
Aplikacje VPN	Aplikacje VPN	
Always On VPN	Włącz blokadę natywną	Always On VPN
Włącz blokadę AppTec360	Włącz blokadę AppTec360	

Samsung / Strong Swan			
Typ połączenia	PPTP	Serwer	Serwer
		Aplikacje VPN	Aplikacje VPN
		Nazwa użytkownika	Nazwa użytkownika
		Hasło	Hasło
		Włącz szyfrowanie PPTP	Włącz szyfrowanie PPTP
	L2TP / IPSec PSK	Serwer	Serwer
		Aplikacje VPN	Aplikacje VPN
		Klucz wstępny IPSec	Klucz wstępny IPSec
		Nazwa użytkownika	Nazwa użytkownika
		Hasło	Hasło
		Włącz L2TP Secret	L2TP Secret
	IPSec XAuth PSK	Serwer	Serwer
		Aplikacje VPN	Aplikacje VPN
		Identyfikator IPSec	Identyfikator IPSec
		Klucz wstępny IPSec	Klucz wstępny IPSec
		Nazwa użytkownika	Nazwa użytkownika
		Hasło	Hasło
Ustawienia eksperckie	Serwery DNS	Serwery DNS	
	Trasy przekazywania	Trasy przekazywania	

Ograniczenia

Tutaj można ustawić ograniczenia związane z zarządzaniem połączeniami.

Zezwalaj na transmisję danych w roamingu	Zezwalaj na transmisję danych w roamingu
Wymuś roaming danych	W przypadku aktywacji roaming danych mobilnych jest włączony na stałe (niezalecane!). To ustawienie zastępuje ustawienie "Zezwalaj na transmisję danych w roamingu"!
Poniższe ustawienia są dostępne tylko w wersji SAFE 2.x lub nowszej	
Zezwalaj tylko na połączenia alarmowe	Zezwalaj tylko na połączenia alarmowe
Zezwalaj na WiFi	Zezwalaj na WiFi
Minimalny poziom bezpieczeństwa sieci Wi-Fi	Minimalny poziom bezpieczeństwa sieci WiFi Otwarte = wszystkie rodzaje WiFi są dozwolone
Zabronić użytkownikowi dodawania sieci WiFi	Użytkownik nie może samodzielnie dodać sieci Wi-Fi To ustawienie jest możliwe tylko wtedy, gdy profil WiFi został zdefiniowany w sekcji "Zarządzanie połączeniami".
Zezwalaj na wiadomości SMS i MMS	Wszystkie = cały ruch SMS i MMS jest dozwolony Tylko przychodzące wiadomości SMS = dozwolone są tylko przychodzące wiadomości SMS. Tylko wychodzące wiadomości SMS = dozwolone są tylko wychodzące wiadomości SMS. Brak = ruch SMS / MMS nie jest dozwolony
Zezwalaj na synchronizację w roamingu	Zezwalaj na synchronizację w roamingu Włączony = aktywowany Wyłączone = dezaktywowane Wybór użytkownika = wybór użytkownika
Zezwalaj na roaming głosowy	Zezwalaj na roaming głosowy Włączony = aktywowany Wyłączone = dezaktywowane Wybór użytkownika = wybór użytkownika
Użyj systemowego serwera proxy http	Korzystanie z serwera proxy HTTP, który jest dostępny w ustawieniach systemu, zależy od podłączonej sieci (WiFi lub APN)

Zarządzanie PIM

Gmail Exchange

Informacje: Ta konfiguracja zostanie zastosowana do aplikacji Gmail. Musisz więc zatwierdzić i zainstalować Gmaila.

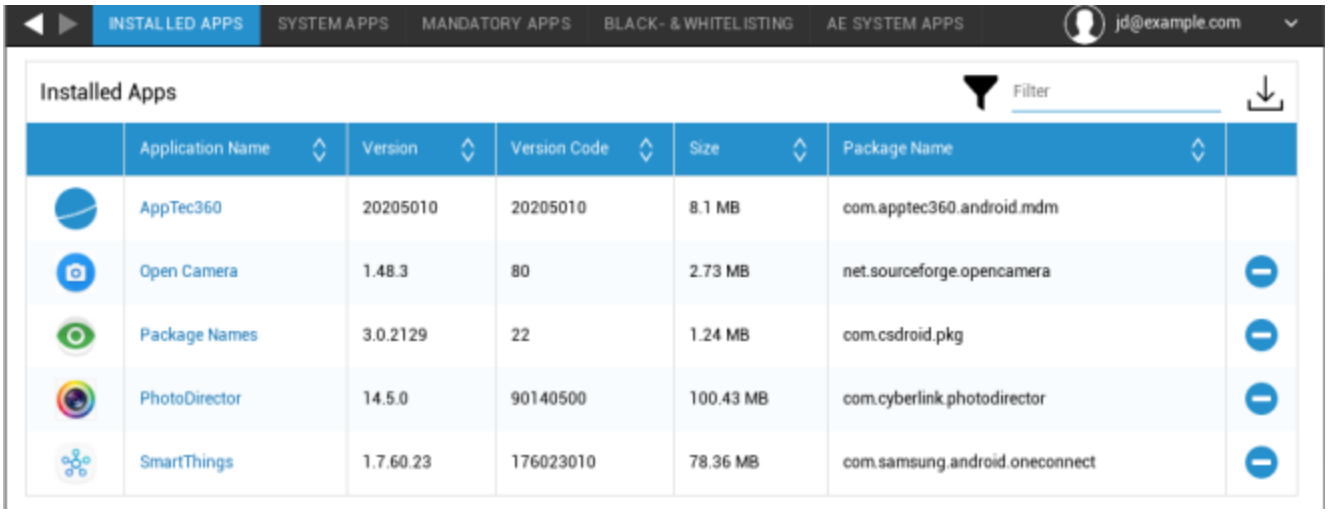
Adres e-mail	Podany adres e-mail użytkownika Zwróć uwagę na "symbole zastępcze", których możesz użyć do pracy z poświadczeniami i nie wprowadzaj zmian ręcznie na każdym urządzeniu. Wystarczy jedno kliknięcie, aby wyświetlić je dla siebie
Nazwa hosta serwera	Adres serwera serwerów Exchange
Nazwa logowania	Nazwa logowania dla danego urządzenia użytkownika końcowego, należy również zwrócić uwagę na "symbole zastępcze tutaj
Podpis	Można dołączyć podpis (wskazówka: niektóre urządzenia wymagają formatowania HTML dla podpisu).
Liczba poprzednich dni do synchronizacji	Liczba dni określająca, kiedy wiadomości e-mail są synchronizowane z powrotem
Identyfikator urządzenia	Łańcuch zawierający identyfikator urządzenia EAS. Jest to część protokołów EAS i jest dostępna w niektórych lokalizacjach
Używanie protokołu Secure Sockets Layer (SSL)	Użyj połączenia SSL
Akceptuj wszystkie certyfikaty	Akceptowane są wszystkie certyfikaty. Wybierz tę opcję, jeśli serwer Exchange korzysta z certyfikatu z podpisem własnym

Zarządzanie aplikacjami

Menedżer aplikacji dla przedsiębiorstw

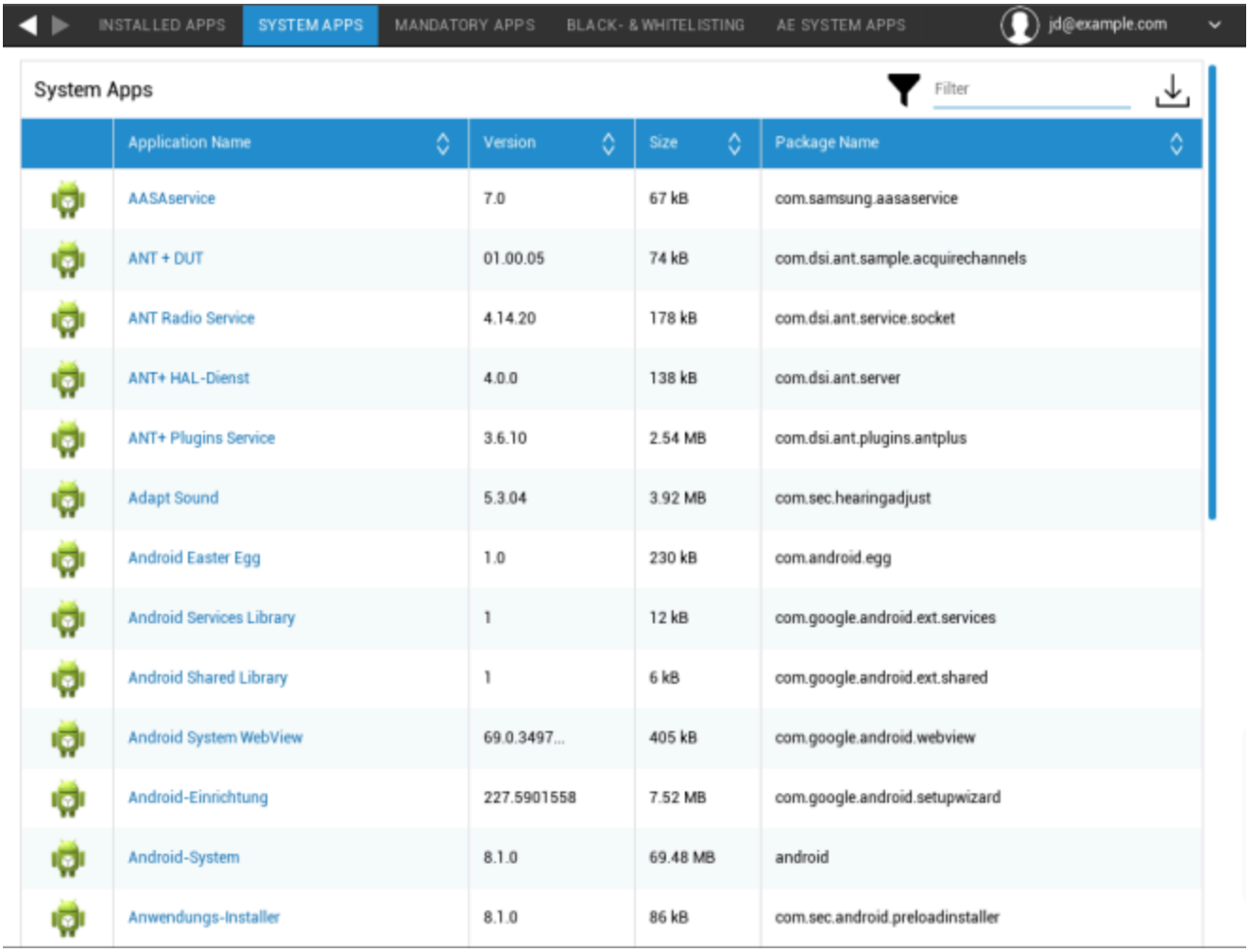
Zainstalowane aplikacje (tylko na poziomie urządzenia)

Tutaj zostaną wyświetlone wszystkie aplikacje, które są obecnie zainstalowane na urządzeniu użytkownika końcowego.



Aplikacje systemowe (tylko na poziomie urządzenia)

W sekcji "Aplikacje systemowe" wyświetlone zostaną wszystkie aplikacje i usługi, które zostały już zainstalowane na urządzeniu użytkownika końcowego przez producenta urządzenia.

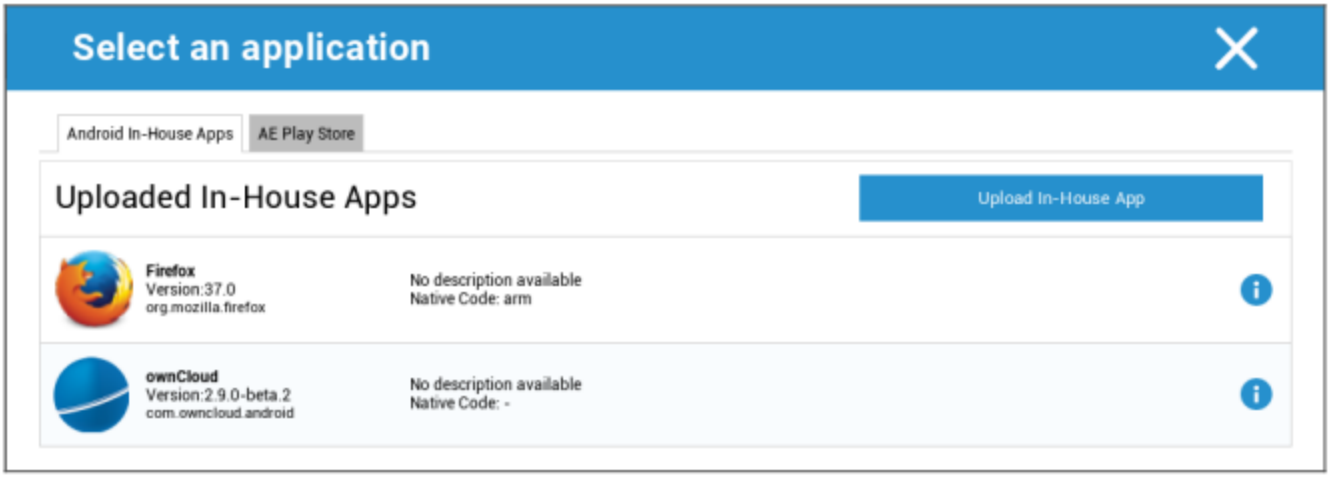


Aplikacje obowiązkowe

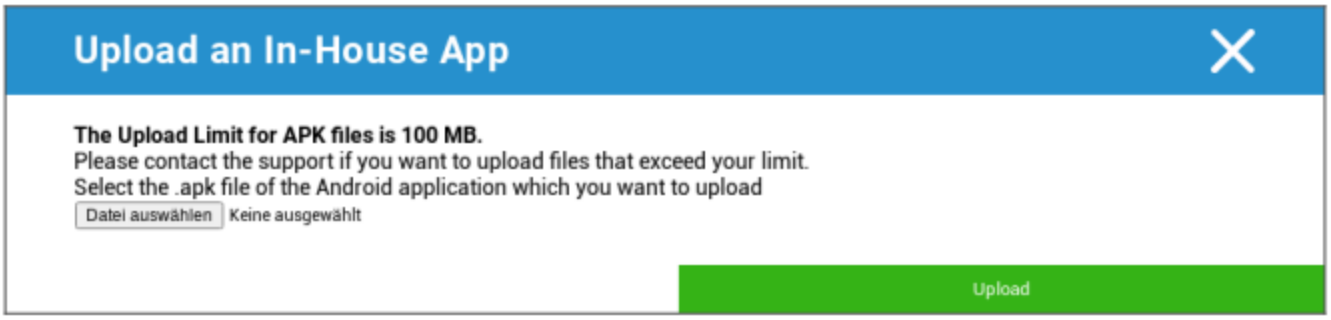
W sekcji Aplikacje obowiązkowe można ustanowić obowiązkowe wymagane aplikacje. Użytkownik będzie stale monitowany o zainstalowanie tej wyznaczonej aplikacji.

Za pomocą , można zdefiniować wymaganą aplikację.

Może to być aplikacja wewnętrzna z "Aplikacji wewnętrznych Android", którą przesłałeś w Ustawieniach ogólnych.

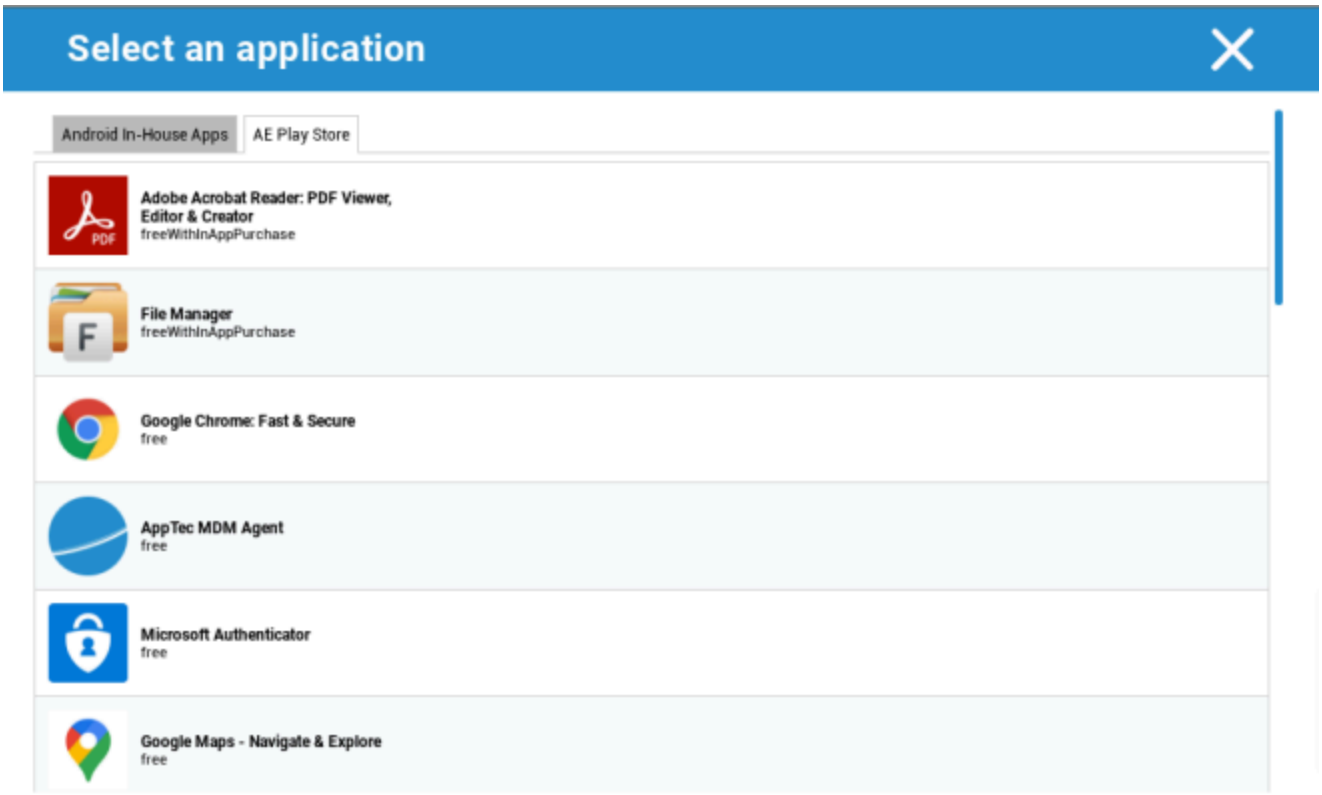


Możesz także bezpośrednio wybrać i przesłać plik apk za pomocą opcji "Prześlij aplikację wewnętrzną".



Jeśli instalujesz aplikację wewnętrzną, będziesz mieć możliwość aktywowania opcji "Aktualizuj". Jeśli ta opcja jest aktywna i zdefiniowano nowszą wersję w In-House App DB, aplikacja zostanie zaktualizowana na urządzeniu.

Może to być również aplikacja "AE Play Store" ze sklepu Google Work Play Store.



Tylko zatwierdzone "Aplikacje AE Play Store" będą wyświetlane w tej zakładce.

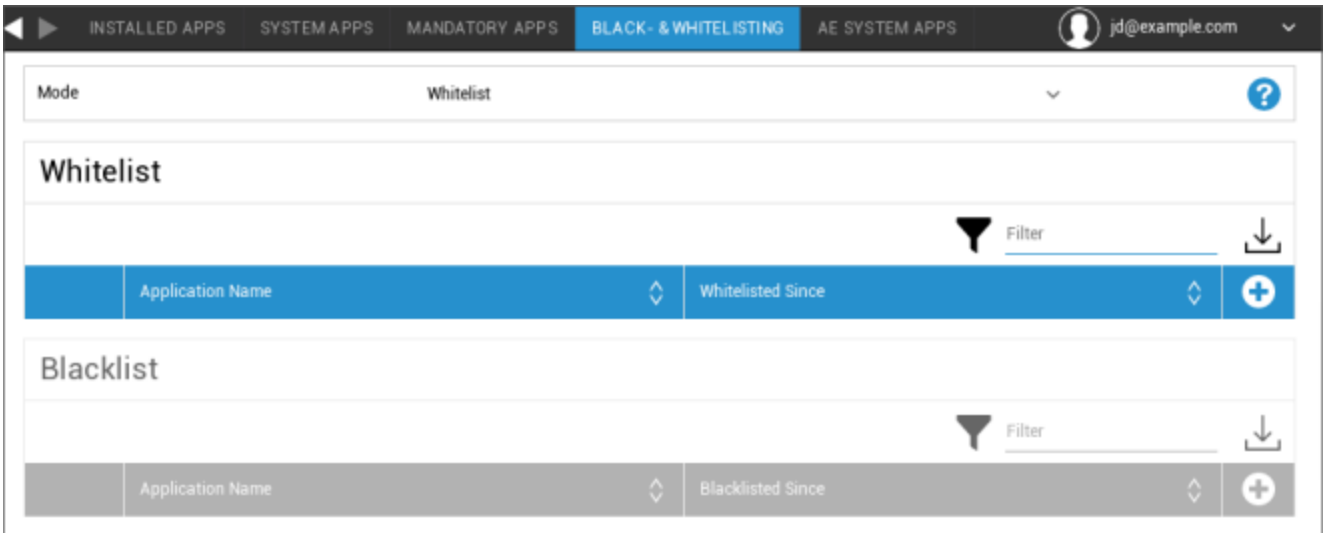
Aby zatwierdzić "Aplikację AE Play Store", przejdź do "Ustawienia ogólne" > "Zarządzanie aplikacjami" > "AE Play".

Store" i dodać aplikację za pomocą przycisku, który przekieruje Cię do zakładki "Play Store Apps" (lub możesz
bezpośrednio przejść do zakładki "Play Store Apps").

W zakładce "Play Store Apps" można wyszukiwać aplikacje. Po kliknięciu aplikacji otworzy się strona aplikacji
, na której można zatwierdzić aplikację, klikając przycisk "Zatwierdź".

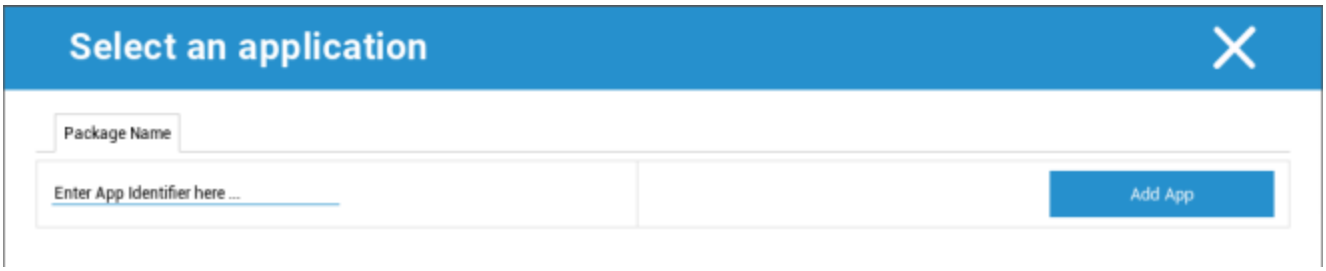
Czarna i biała lista

W sekcji "Czarna i biała lista" można wybrać między trybem "Biała lista" i trybem "Czarna lista".



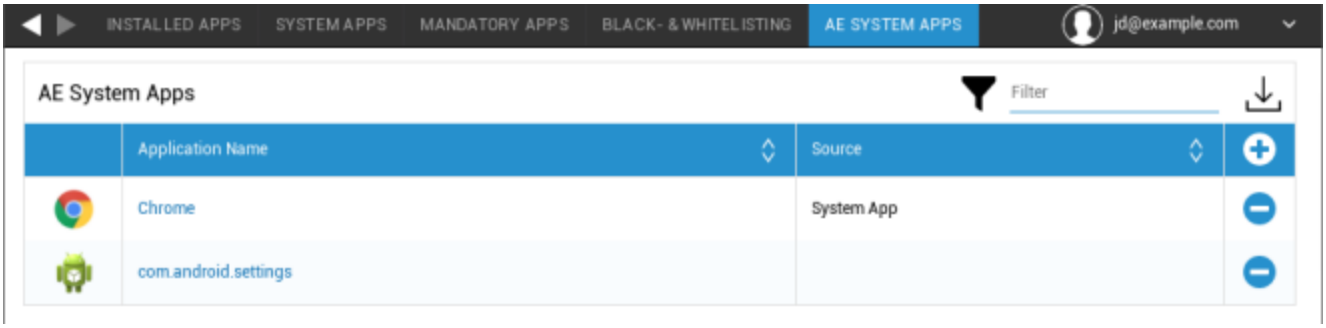
Biała lista	Tylko aplikacje i usługi dodane do listy mogą zostać zainstalowane na urządzeniu użytkownika końcowego. Jeśli są one już wstępnie zainstalowane na urządzeniu użytkownika końcowego, zostaną aktywowane i ustawione, aby użytkownik mógł je uruchomić.
	Wszystkie inne aplikacje, które nie zostały dodane do listy, nie mogą być instalowane na urządzeniu użytkownika końcowego. Jeśli są one już wstępnie zainstalowane na urządzeniu użytkownika końcowego, zostaną dezaktywowane i ustawione tak, aby użytkownik nie mógł ich uruchomić.
Czarna lista	Aplikacje i usługi dodane do listy nie mogą być instalowane na urządzeniu użytkownika końcowego. Jeśli są one już wstępnie zainstalowane na urządzeniu użytkownika końcowego, zostaną dezaktywowane i ustawione tak, aby użytkownik nie mógł ich uruchomić.
	Wszystkie inne aplikacje, które nie zostały dodane do listy, mogą zostać zainstalowane na urządzeniu użytkownika końcowego. Jeśli są one już wstępnie zainstalowane na urządzeniu użytkownika końcowego, zostaną aktywowane i ustawione, aby użytkownik mógł je uruchomić.

Za pomocą przycisku , można dodać dodatkowe aplikacje lub usługi do aktualnie używanej listy.
Za pomocą przycisku , można dodać dodatkowe aplikacje lub usługi do aktualnie nieaktywnej listy.
Można zdefiniować "Packagename":

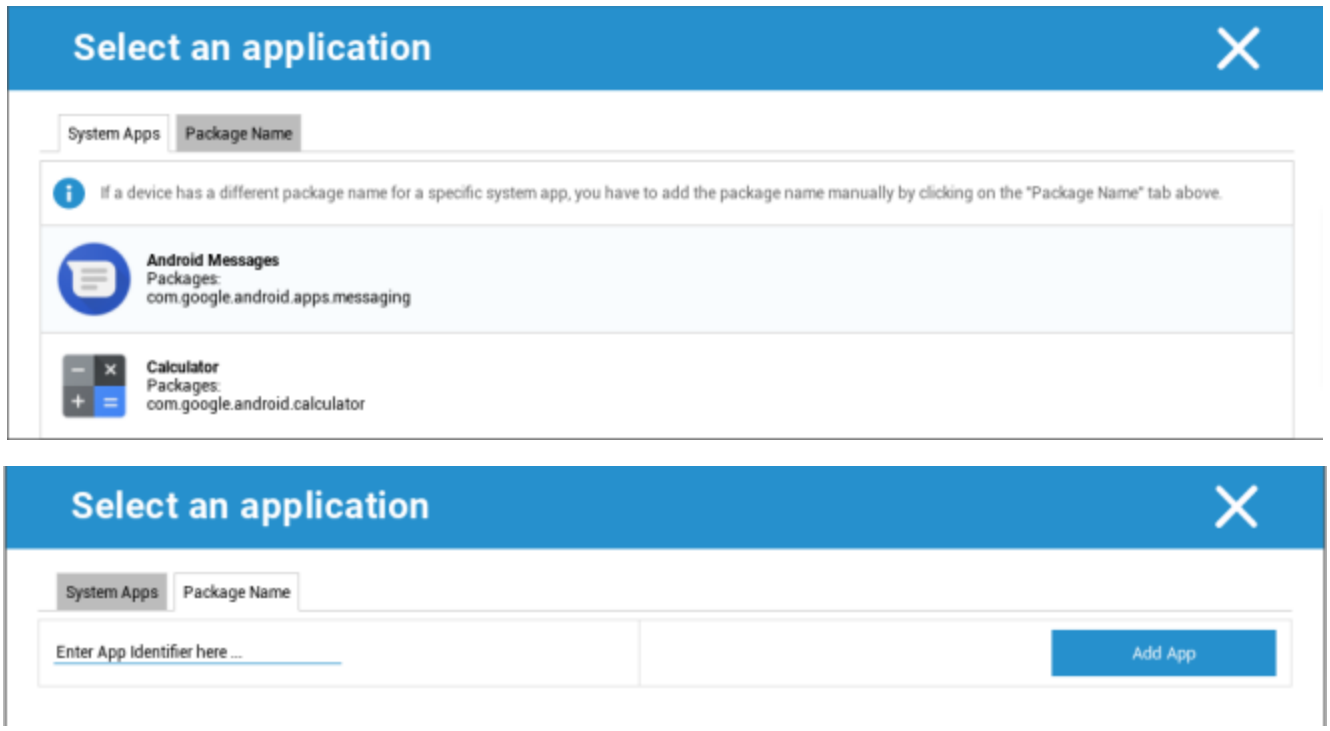

Select an application
Package Name
Enter App Identifier here ...
Add App

Aplikacje systemowe AE

W tym miejscu można zdefiniować listę zawierającą określone aplikacje systemowe, które powinny być aktywowane na urządzeniach.



Po kliknięciu przycisku można wybrać z listy możliwych aplikacji systemowych dostarczonych przez Google lub bezpośrednio wprowadzić nazwę pakietu aplikacji systemowej, która powinna zostać aktywowana.



Należy pamiętać, że aplikacje systemowe na liście dostarczonej przez Google to tylko aplikacje, które mogą być aplikacjami systemowymi, ale niekoniecznie muszą być aplikacjami systemowymi na urządzeniach.

Jednak ta lista dotyczy tylko aplikacji, które są już wstępnie zainstalowane.

Dodawanie aplikacji, które nie są wstępnie zainstalowane na urządzeniach, nie będzie miało wpływu na urządzenia, niezależnie od tego, czy aplikacja znajduje się na liście dostarczonej przez Google, czy nazwa pakietu aplikacji jest wprowadzana bezpośrednio.

Ograniczenia i ustawienia

Ustawienia zarządzania aplikacjami

W tym miejscu można skonfigurować zachowanie urządzenia w zakresie aktualizacji aplikacji.

Częstotliwość sprawdzania aktualizacji	Określa, w jakich odstępach czasu klient AppTec360 będzie wyszukiwał aktualizacje aplikacji. Wartość domyślna to 24 godziny.
Próg Wi-Fi	Aplikacje większe niż określony rozmiar będą pobierane przez sieć Wi-Fi. W przypadku wybrania opcji "Tylko Wi-Fi" wszystkie aplikacje będą pobierane przez sieć Wi-Fi.

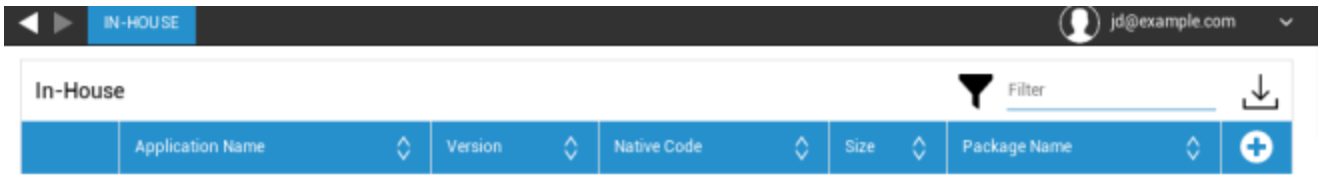
Sklep z aplikacjami dla przedsiębiorstw

Wewnątrz firmy

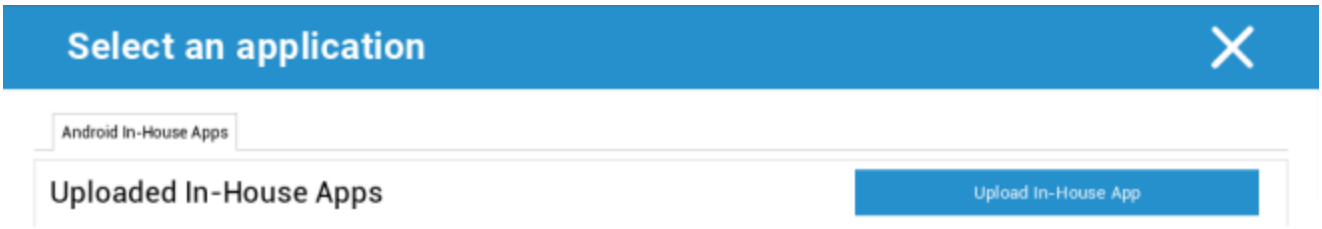
W punkcie "In-House" można przesyłać i rozpowszechniać aplikacje opracowane wewnętrznie.

Symbol ten umożliwia dystrybucję dodatkowych aplikacji wewnętrznych.

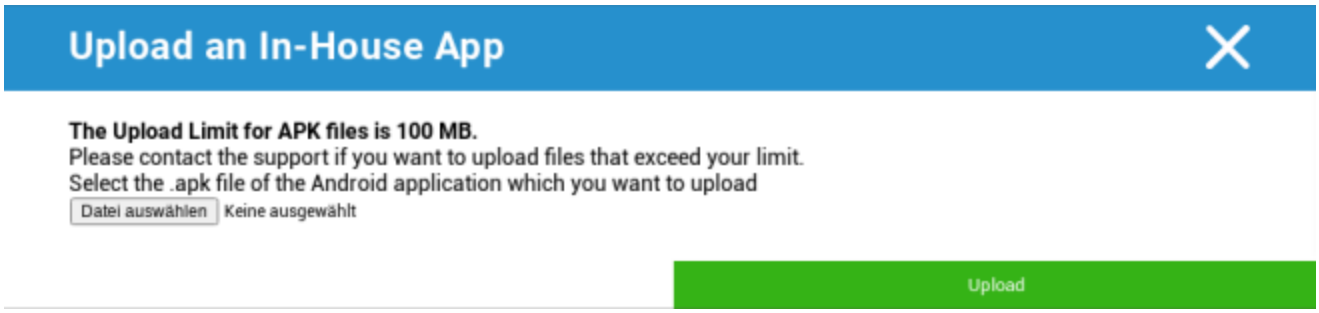
Jeśli instalujesz aplikację wewnętrzną, będziesz mieć możliwość aktywowania opcji "Aktualizuj". Jeśli opcja
jest aktywna i zdefiniowano nowszą wersję w In-House App DB, aplikacja zostanie zaktualizowana na urządzeniu.



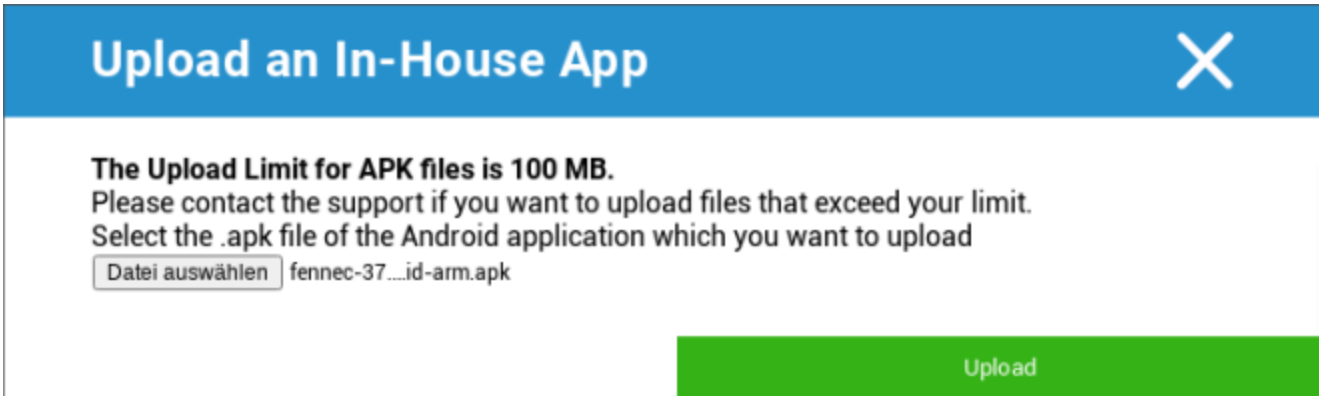
Jeśli nie rozpowszechniłeś aplikacji wewnętrznych, otrzymasz następujący przegląd:



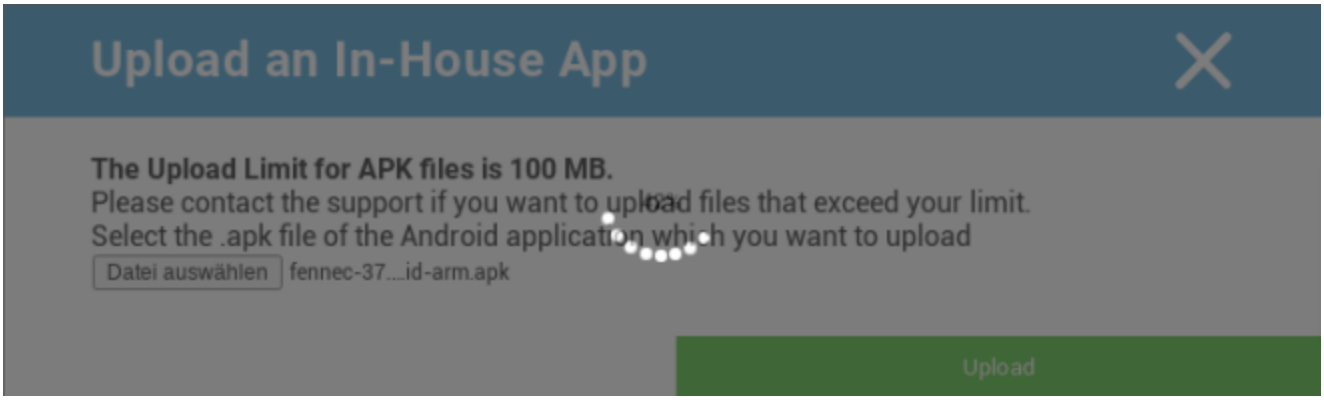
W tym celu kliknij "Prześlij aplikację wewnętrzną", a następnie otrzymasz następujący przegląd:



Teraz wybierz za pomocą "Wyszukaj..." plik .apk, a następnie kliknij "Prześlij".



Twoja aplikacja zostanie teraz przesłana, w środku okręgu zobaczysz wskaźnik procentowy, pokazujący, ile Twojej aplikacji zostało już przesłane.



W przypadku pomyślnego przesłania aplikacji wewnętrznej, można ją znaleźć pod adresem
w katalogu aplikacji.

Użytkownik ma teraz możliwość wyświetlenia i zainstalowania tej aplikacji w AppTec360 Store na urządzeniu użytkownika końcowego
, w kategorii "In-House".

Ze względu na fakt, że nie wiąże się to z aplikacją Google PlayStore, użytkownik nie potrzebuje zapisanego identyfikatora Google
ID na swoim urządzeniu końcowym.

Sklep Play dla przedsiębiorstw

Sklep AE Play

Tutaj można dodawać aplikacje do Android Enterprise Playstore. Należy pamiętać, że przed dodaniem aplikacji należy zatwierdzić aplikację
za pomocą konta administratora AE.

Aby zatwierdzić aplikację, zapoznaj się z instrukcjami w sekcji Aplikacje obowiązkowe.

Tryb kiosku i program uruchamiający

Tryb kiosku

Tryb kiosku umożliwia wstępne zdefiniowanie aplikacji lub adresu URL. Następnie możliwe będzie wyłącznie
uruchomienie/odwiedzenie tej aplikacji lub adresu URL.

Podobnie, różne przyciski sprzętowe można dezaktywować w zróżnicowanym trybie kiosku.

Automatyczny start	Automatycznie uruchamia tryb kiosku, gdy tylko profil dotrze do urządzenia użytkownika końcowego.
Zaplanowany tryb kiosku?	Możesz zaplanować czas dla trybu kiosku, który następnie rozpocznie się i zakończy automatycznie o ustawionej przez Ciebie godzinie
Godzina rozpoczęcia	Czas rozpoczęcia
Czas w minutach	Czas w minutach, po którym tryb kiosku powinien się ponownie zakończyć.

Typ aplikacji

Pojedyncza aplikacja	Jeśli chcesz uruchomić aplikację w trybie kiosku, wybierz "Pakiet" w sekcji "Typ aplikacji".
Aplikacja kiosku	Kliknij tutaj, aby wybrać aplikację, która ma zostać uruchomiona w trybie kiosku. Znajdziesz tu zwykły przegląd zarządzania aplikacjami Można wybrać pomiędzy "Google Play Store", "Android In-House Apps" i "Packagename".

Typ aplikacji

URL	Jeśli chcesz uruchomić adres URL w trybie kiosku, wybierz "URL" w sekcji "Typ aplikacji". Następnie zdefiniuj żądany adres URL
Wyczyść przeglądarkę po braku aktywności	W tym miejscu można zdefiniować przedział czasu w minutach, po którym tryb kiosku powinien zostać ponownie uruchomiony
Wyczyść pamięć podręczną i pliki cookie	Jeśli funkcja ta zostanie aktywowana, po ponownym uruchomieniu trybu kiosku pamięć podręczna sieci Web (pliki cookie i obrazy w pamięci podręcznej) zostanie usunięta.
Polityka tego samego pochodzenia	Jeśli ta funkcja jest aktywna, użytkownik może przeglądać tylko podstrony zdefiniowanego adresu URL Na przykład, zdefiniowano następujący adres URL: www.mypage.com Następnie użytkownik może surfować na stronie: www.mypage.com/subpage
Adresy URL na białej liście	Tutaj można prowadzić białą listę, wszystkie te adresy URL są dozwolone Maksymalnie 1 adres URL w wierszu Adres URL musi zaczynać się od http:/ lub https://.
Adresy URL na czarnej liście	Tutaj można utworzyć czarną listę, na której wszystkie te adresy URL są niedozwolone. Maksymalnie 1 adres URL w wierszu Adres URL musi zaczynać się od http:/ lub https://.
Orientacja ekranu	To ustawienie odnosi się do regulacji ekranu Automatyczny = automatyczny Portret = format pionowy Krajobraz = tryb krajobrazowy

Multi App	Jeśli wybierzesz tryb kiosku "Multi App", korzystanie z AppTec360 Launcher będzie wymuszone.
Aplikacje	Aplikacja: Wybierz Playstore lub aplikację wewnętrzną jako aplikację kiosku. Możliwe jest również wprowadzenie nazwy pakietu. Wybrana aplikacja Kiosk musi być zainstalowana na urządzeniu. Pamiętaj, aby ustawić aplikację Kiosk jako obowiązkową. Skrót na ekranie głównym: W przypadku ustawienia na "Wł." zostanie utworzony skrót na ekranie głównym. W przypadku ustawienia na "Wył." aplikacja będzie nadal widoczna na liście aplikacji.

Hasło wyjścia włączone	Po aktywowaniu tej funkcji użytkownik może zakończyć tryb kiosku za pomocą wstępnie zdefiniowanego hasła
Hasło wyjścia	Jest to hasło, które zostało wstępnie zdefiniowane przez użytkownika
Automatycznie zwijany pasek stanu	Jeśli ta opcja jest włączona, pasek stanu będzie automatycznie kolorowany. Dzięki tej opcji użytkownicy mogą zobaczyć informacje na pasku stanu, ale nie mają dostępu do jego funkcji
Wyłącz pasek stanu	Pasek stanu zawiera powiadomienia, skróty i informacje. Dostępne tylko dla urządzeń Samsung z systemem SAFE 4.0 lub nowszym.
Wyłącz klawisze głośności	Wyłącz klawisze głośności (dostępne tylko na urządzeniach Samsung z funkcją SAFE 3.0 lub nowszą)
Wyłącznik wł.	Wyłącz przełącznik On / Off (dostępny tylko na urządzeniach Samsung z SAFE 3.0 lub nowszym)
Wyłącz przycisk Home	Wyłącz przycisk Home. Jeśli ta funkcja została aktywowana, tryb kiosku można zakończyć tylko w konsoli AppTec360. (dostępne tylko na urządzeniach Samsung z funkcją SAFE 3.0 lub nowszą)
Wyłącz pasek nawigacji	W ten sposób można wyłączyć pasek nawigacji (Wstecz / Menu). Jeśli ta funkcja została aktywowana, tryb kiosku można zakończyć tylko w konsoli AppTec360. (dostępne tylko na urządzeniach Samsung z funkcją SAFE 3.0 lub nowszą)

AppTec360 Launcher

Włącz program uruchamiający AppTec360	Wł: Włącza AppTec360 Launcher. Użytkownik musi jednorazowo ustawić go jako domyślny program uruchamiający. Uwaga: Jeśli tryb kiosku jest włączony, a tryb kiosku jest ustawiony na "Multi App", korzystanie z programu uruchamiającego AppTec360 będzie wymuszone.
Duże ikony	Wł: Wyświetla większą wersję ikon aplikacji w programie uruchamiającym.
Ukryj ikonę aplikacji AppTec360	Wł: Całkowicie ukrywa aplikację AppTec360
Ukryj ikonę sklepu AppTec360	Wł: Całkowicie ukrywa AppStore AppTec360 Enterprise.

Ustawienia AppTec360

Włącz aplikację ustawień AppTec360	Aplikacja AppTec360 Settings zapewnia kontrolę nad połączeniami WiFi i Bluetooth
Włącz ustawienia w aplikacji Multi Tryb kiosku	Jeśli ta opcja jest włączona, użytkownicy mogą uzyskać dostęp do aplikacji ustawień AppTec360, gdy aktywny jest tryb kiosku z wieloma aplikacjami.

Pilot zdalnego sterowania

Splashtop

Aby rozpocząć sesję zdalnego sterowania urządzeniem, aplikacja "Splashtop Streamer" musi być zainstalowana na urządzeniu poprzez dodanie aplikacji do **App Management** → **Enterprise App Manager** → **Mandatory Apps**.

Następnie skonfiguruj następujące ustawienia dla Splashtop:

Włącz Splashtop	Jeśli jest włączona, AppTec360 skonfiguruje aplikację Splashtop, aby umożliwić zdalne sterowanie
Wdrażanie kodu	Przejdź na stronę https://my.splashtop.com i zaloguj się na swoje konto Splashtop. Kliknij "Dodaj komputer" i skopiuj 12-cyfrowy kod wdrożeniowy z wyświetlonej strony.
Ustawić niestandardową bramę wdrażania?	Wdrażanie bramy
Wdrożenie bramy domeny / hosta	Wdrażanie bramy
Weryfikacja certyfikatu	Weryfikacja certyfikatu

Następnie można użyć opcji Splashtop Remote Control w menu kontekstowym (koło zębate obok paska wyszukiwania, po wybraniu urządzenia lub kliknięciu prawym przyciskiem myszy urządzenia w drzewie), aby rozpocząć sesję zdalnego sterowania.

TeamViewer

Aby rozpocząć sesję zdalnego sterowania na urządzeniu, aplikacja "TeamViewer QuickSupport" musi być zainstalowana na urządzeniu poprzez dodanie aplikacji do **App Management** → **Enterprise App Manager** → **Mandatory Apps**.

Następnie możesz użyć opcji **TeamViewer Remote Control** w menu kontekstowym (koło zębate obok paska wyszukiwania, gdy urządzenie jest zaznaczone lub kliknij prawym przyciskiem myszy urządzenie w drzewie), aby rozpocząć sesję zdalnego sterowania.

Zarządzanie treścią

ContentBox

Tutaj można aktywować ContentBox.

Po przełączeniu opcji "Enable ContentBox" na "On", na urządzeniu użytkownika końcowego zostanie automatycznie zainstalowana oddzielna aplikacja ContentBox

.

Bezpieczna przeglądarka

W tym miejscu można skonfigurować ustawienia przeglądarki AppTec360 Secure Browser.

Po przełączeniu sekcji "Secure Browser" na "On", oddzielna aplikacja przeglądarki zostanie automatycznie zainstalowana na urządzeniu użytkownika końcowego.

Wymagaj hasła	Wymagaj od użytkownika skonfigurowania i używania hasła w celu uzyskania dostępu do przeglądarki.
Minimalna wymagana długość hasła	Ustaw wymaganą liczbę znaków dla hasła
Wymagana jakość hasła	Ustaw wymaganą jakość hasła
Ogranicz pobieranie / Otwórz w	
Ogranicz przesyłanie	
Prześlij na białą listę	Lista adresów URL, dla których przesyłanie będzie zawsze dozwolone.
Zezwalaj na kopiowanie	Zezwalaj na kopiowanie, wycinanie lub udostępnianie tekstu wewnątrz stron internetowych.
Zezwalaj na przechwytywanie ekranu	Zezwalaj na przechwytywanie zrzutów ekranu.
Częstotliwość czyszczenia danych	Wybierz, z jaką częstotliwością WSZYSTKIE dane użytkownika (historia, pamięć podręczna itp.) mają być automatycznie usuwane.
Zakładki firmowe	Zakładki pojawią się w folderze "Zakładki firmowe" w zakładkach przeglądarki. Nie są one edytowalne przez użytkownika.
Ukryj pasek adresu	
Biała lista w przeglądarce (bez Universal Gateway)	Włącza białą listę adresów URL po stronie klienta. • Zakładki firmowe są zawsze na białej liście • Obsługiwane tylko dla 100 adresów URL • Użyj Universal Gateway do nieograniczonej czarnej i białej listy.
Adresy URL na białej liście	Lista dozwolonych adresów URL.

Czarna i biała lista oparta na bramie	Czarna lista zawiera następujące wymagania: • Działająca bramka uniwersalna AppTec360 ("Ustawienia ogólne" → "Bramka uniwersalna"). • Działająca konfiguracja VPN z określonym serwerem DNS ("Ustawienia ogólne" → "Brama uniwersalna" → "Ustawienia VPN"). • Konfiguracja czarnej listy ("Ustawienia ogólne" → "Universal Gateway" → "Czarna lista domen"). • Prawidłowe połączenie VPN w profilu ("Zarządzanie połączeniami" → "VPN").

Dodatkowy interfejs API

Samsung KNOX

Ograniczenia

Zezwól na kartę SD	
Zezwalaj na zapis na karcie SD	
Zezwalaj na przechwytywanie ekranu	
Zezwalaj na schowek	
Tworzenie kopii zapasowych ustawień i danych aplikacji w Google Cloud	
Przywracanie ustawień z Google Cloud podczas ponownej instalacji aplikacji	
Zezwalaj na debugowanie USB	
Zezwól na Google Crash Report	
Zezwalaj na przywrócenie ustawień fabrycznych	
Zezwalaj na aktualizację OTA	
Zezwalaj na pamięć USB hosta	Jeśli ta opcja jest włączona, użytkownik może podłączyć dowolny pendrive (przenośna pamięć USB), zewnętrzny dysk HD lub czytnik kart Secure Digital (SD), który zostanie zamontowany w urządzeniu jako dysk pamięci masowej.
Zezwalaj na odtwarzacz multimedialny USB (MTP, PTP)	
Zezwól na mikrofon	Wyłącza mikrofon dla aplikacji innych firm
Zezwalaj na komunikację NFC (Near Field Communication)	
Zezwalaj na nieznane źródła (boczne ładowanie APK)	Jeśli opcja ta jest włączona, dozwolone jest pobieranie aplikacji (plików APK) z boku.

	Po wyłączeniu tego ustawienia użytkownik musi włączyć je ręcznie po ponownym zezwoleniu na instalację plików APK z nieznanych źródeł.
Zezwalaj na tworzenie użytkowników	Jeśli opcja ta jest włączona, użytkownik może tworzyć wiele kont na urządzeniu, np. konta gości.

E-mail

Adres e-mail	
Protokół serwera przychodzącego	
Adres serwera przychodzącego	
Port serwera przychodzącego	
Login/nazwa użytkownika serwera przychodzącego	
Hasło serwera przychodzącego	
Serwer przychodzący używa protokołu SSL	
Serwer przychodzący używa protokołu TLS	
Serwer przychodzący akceptuje wszystkie certyfikaty	
Protokół serwera wychodzącego	
Adres serwera wychodzącego	
Port serwera wychodzącego	
Serwer wychodzący używa dodatkowych poświadczeń	Jeśli jest wyłączona, system używa poświadczeń przychodzących również dla serwera wychodzącego.
Login/nazwa użytkownika serwera wychodzącego	
Hasło serwera wychodzącego	
Serwer wychodzący używa protokołu SSL	
Serwer wychodzący używa protokołu TLS	
Serwer wychodzący akceptuje wszystkie certyfikaty	
Podpis zestawu	
Podpis	Uwaga: W przypadku niektórych urządzeń podpis musi być określony w formacie HTML.

Powiadomienie użytkownika o otrzymaniu nowej wiadomości e-mail	

Wymiana

Adres e-mail	
Nazwa hosta serwera	Nazwa hosta serwera Exchange
Nazwa logowania	Nazwa użytkownika używana do logowania się do serwera Exchange.
Domena	Jeśli włączona jest konfiguracja ACL Gateway, a pole Domain nie jest puste, AppTec360 Universal Gateway uwierzytelni urządzenie za pomocą następującej nazwy "Domain\Login Name
Hasło	
Liczba poprzednich dni do synchronizacji	
Częstotliwość synchronizacji poczty e-mail	
Synchronizacja w roamingu	
Podpis zestawu	
Podpis	Uwaga: W przypadku niektórych urządzeń podpis musi być określony w formacie HTML.
Konto domyślne	
Używanie protokołu Secure Sockets Layer (SSL)	
Używanie protokołu TLS (Transport Layer Security)	
Akceptuj wszystkie certyfikaty	

APN

Wyświetlana nazwa APN	
Nazwa punktu dostępu	Nazwa APN
Protokół serwera wychodzącego	
MCC - kod kraju sieci komórkowej	Pozostaw puste, aby użyć mmc zainstalowanej karty SIM
MNC - kod sieci komórkowej	Pozostaw puste, aby użyć mnc zainstalowanej karty SIM
Adres serwera	
Numer portu serwera	
Adres serwera proxy	
Adres serwera MMS	Pozostaw puste dla wartości domyślnych
Numer portu MMS	Pozostaw puste dla wartości domyślnych
Adres proxy MMS	Pozostaw puste dla wartości domyślnych
Nazwa użytkownika	
Hasło	
Typ punktu dostępu	Akceptowane typy to "default", "mms", "supl".
	Jeśli przekazano wartość null lub pustą, domyślnie używane jest "default,supl,mms".
	Domyślnie pozostaw puste.
Preferowany APN	

Bluetooth

Zezwalaj na wykrywanie urządzeń przez Bluetooth	
Zezwalaj na parowanie Bluetooth	
Zezwalaj na korzystanie z zestawów słuchawkowych Bluetooth	
Zezwalaj na korzystanie z urządzeń głośnomówiących Bluetooth	
Zezwalaj na urządzenia Bluetooth A2DP	A2DP, Advanced Audio Distribution Profile umożliwia strumieniowe przesyłanie dźwięku między urządzeniami
Zezwalaj na połączenia wychodzące	
Zezwalaj na przesyłanie danych przez Bluetooth	
Zezwalaj na tethering Bluetooth	
Zezwalaj na połączenie z komputerem przez Bluetooth	

Połączenie

Zezwalaj tylko na połączenia alarmoweZezwalaj na Wi-Fi	
Minimalny poziom zabezpieczeń sieci Wi-Fi	
Zakaz dodawania sieci Wi-Fi przez użytkownika	Ograniczenie to można aktywować tylko wtedy, gdy co najmniej jeden aktywny profil Wi-Fi jest zdefiniowany w sekcji Zarządzanie połączeniami.
Zezwalaj na wiadomości SMS i MMS	
Zezwalaj na synchronizację w roamingu	
Zezwalaj na roaming głosowy	

Android Enterprise – w pełni zarządzane urządzenie z profilem pracy (COPE)

Ogólne wyjaśnienie COPE

COPE to skrót od **Corporate Owned Personally Enabled**.

Tryb COPE umożliwia zarejestrowanie urządzenia z systemem Android jako **Android Enterprise - Fully Managed Device** ze zintegrowanym profilem **Android Enterprise - Container**.

Może to być albo urządzenie z systemem Android, które jest już zarejestrowane jako **Android Enterprise - Fully Managed Device** i na którym dodatkowo skonfigurowany jest **Android Enterprise - Cont** ainer, albo nowo zarejestrowane urządzenie z systemem Android, które jest bezpośrednio zarejestrowane jako **Android Enterprise - Fully Man aged Device** wraz z **Android Enterprise - Container** na nim.

Tryb COPE jest dostępny tylko dla urządzeń z systemem Android 8, 9 i 10

Konfiguracja profili dla urządzeń COPE

Ponieważ nie ma profilu konfiguracji dla samego trybu COPE, konfiguracja **Android Enterprise - Fully Managed Device** i **Android Enterprise - Container** jest podzielona na dwa profile w ramach profilu COPE. Możliwe jest przełączanie się między tymi dwoma profilami w celu konfiguracji każdego z nich poprzez kliknięcie odpowiedniego przycisku po lewej stronie konsoli:

Oba profile można skonfigurować w sposób opisany dla każdego z nich:

Android Enterprise - w pełni zarządzane urządzenie

Android Enterprise - Kontener

Powrót do w pełni zarządzanego urządzenia AE

Profil **Android Enterprise - Container** można usunąć zgodnie z opisem w sekcji **Zarządzanie urządzeniami mobilnymi**.

Po usunięciu profilu Container profil COPE zostanie przekształcony w profil **Android Enterprise - Fully Managed Device**.

Android Enterprise – konfiguracja kontenera

W zależności od tego, czy aktualnie wybrano profil grupy, czy urządzenie, przegląd i jego podpunkty różnią się - należy to dokładnie rozważyć!

Ogólne

Przegląd profilu (tylko na poziomie profilu)

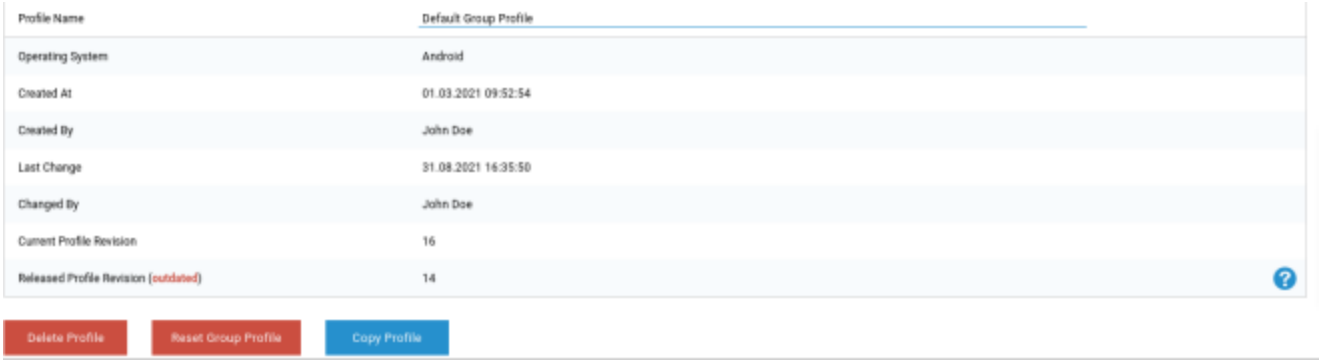
Jeśli jesteś w profilu, otrzymasz krótki przegląd profilu, w odniesieniu do nazwy, systemu operacyjnego, daty utworzenia, autora itp.

Nazwa profilu	Nazwa profilu - może być bezpośrednio zmieniona tutaj.
System operacyjny	Prawidłowy system operacyjny dla profilu
Utworzono w	Data utworzenia
Utworzony przez	Stworzony przez
Ostatnia zmiana	Data ostatniej zmiany
Zmienione przez	Użytkownik, który dokonał ostatnich zmian w tym profilu
Aktualna wersja profilu	Liczba aktualizacji profilu
Wydana wersja profilu	Liczba przypadków, w których profil został już zaktualizowany i przypisano do niego urządzenia.

Usuń profil	Usuń profil
Resetowanie profilu grupy	Resetowanie profilu grupy
Kopiuj profil	Kopiuj profil

Przegląd profilu grupy (tylko na poziomie grupy)

Po otwarciu profilu grupy wyświetlony zostanie szybki przegląd profilu.



Nazwa profilu	Nazwa profilu (można ją zmienić tutaj)
System operacyjny	System operacyjny, dla którego przeznaczony jest profil
Utworzono w	Czas stworzenia
Utworzony przez	Twórca profilu
Ostatnia zmiana	Czas ostatniej zmiany profilu
Zmienione przez	Konto, które wprowadziło ostatnie zmiany
Aktualna wersja profilu	Zmiana zapisanego stanu profilu
Wydana wersja profilu	Wersja przypisanego profilu ("Przypisz teraz"). Jeśli etykieta pokazuje "(nieaktualne)" za tekstem, oznacza to, że profil został zapisany, ale nie został jeszcze przypisany, więc urządzenia nadal będą otrzymywać starszą wersję.

Przegląd urządzeń (tylko na poziomie urządzenia)

Jeśli jesteś na urządzeniu, otrzymasz podsumowanie wybranego urządzenia, które zawiera następujące informacje:

Nazwa urządzenia	Nazwa urządzenia
Lokalizacja	Współrzędne lokalizacji
Numer telefonu	Numer telefonu
Przypisane aplikacje obowiązkowe	Liczba przypisanych aplikacji obowiązkowych
Wersja systemu operacyjnego	Wersja systemu operacyjnego urządzenia
System operacyjny	System operacyjny (Android Enterprise)
Numer seryjny	Numer seryjny urządzenia
Własność urządzenia	Urządzenie firmowe lub prywatne
Typ urządzenia	Urządzenie zarządzane AE Work
Zakorzeniony	Status, wskazujący, czy urządzenie zostało zrootowane.
Zgodność	Zgodność z wytycznymi
Adres IP	Adres IP urządzenia
Ostatnio widziany	Punkt w czasie, kiedy urządzenie ostatnio łączyło się z AppTec
Last Push	Punkt w czasie, w którym do urządzenia wysłano ostatnią wiadomość push.
Przypisanie użytkownika	Użytkownik lub grupa, do której przypisane jest urządzenie

Wersja konfiguracji

W tym miejscu można sprawdzić, który profil grupy jest przypisany do urządzenia.

Jeśli klikniesz profil grupy, uzyskasz bezpośredni dostęp do tego profilu i będziesz mógł dokonać ustawień.

Za pomocą tego symbolu można przywrócić rozproszone aplikacje do ustawień profilu grupy.

Za pomocą tego symbolu można przywrócić wszystkie używane aplikacje do ustawień profilu grupy.

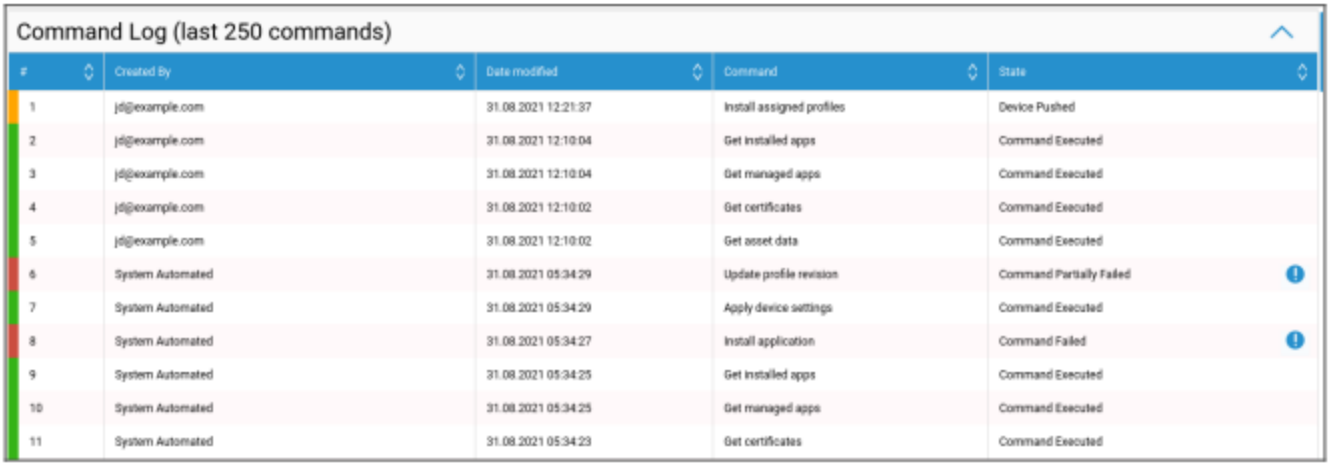
"Newer Revision available" oznacza, że profil grupy został zmieniony i zapisany, ale nie został przypisany. Profil grupy musi zostać przypisany za pomocą opcji "Przypisz teraz" na poziomie grupy, aby zastosować zmiany do urządzeń.

Dziennik urządzenia (tylko na poziomie urządzenia)

Tutaj dostępne są różne dzienniki urządzeń. W razie potrzeby można tutaj bezpośrednio znaleźć przyczynę błędu.

Dziennik poleceń

Tutaj można sprawdzić, które polecenia zostały wydane dla urządzenia i jaki jest ich status.



Możliwe statusy poleceń

Urządzenie wciśnięte	Żądanie push zostało wysłane do usługi push (np. APNS), aby poinformować urządzenie o konieczności połączenia się z serwerem EMM.
Utworzone polecenie	Polecenie zostało utworzone w systemie.
Wysłane polecenie	Polecenie zostało wysłane do urządzenia po nawiązaniu połączenia z serwerem.
Polecenie wykonane	Polecenie zostało pomyślnie wykonane.
Polecenie nie powiodło się	Polecenie nie powiodło się. *
Polecenie częściowo nieudane	W zależności od systemu operacyjnego urządzenia niektóre polecenia mogą zostać zgrupowane. W tym przypadku niektóre części tej grupy poleceń nie powiodły się. *
Polecenie wykonane, ostatecznie nieudane	Polecenie zostało wykonane, ale być może nie.
Przesunięcie polecenia	Polecenie zostało powtórzone przez użytkownika.
Odrzucony	Polecenie zostało odrzucone. Na przykład dlatego, że zostało zastąpione przez inne polecenie lub urządzenie zostało ponownie zarejestrowane, a stare polecenia zostały usunięte.

*Jeśli za wiadomością znajduje się wykrzyknik, możesz uzyskać więcej informacji, najeżdżając kursorem na ikonę.

Ustawienia urządzenia

Konfiguracja klienta

W tym miejscu można przeprowadzić następujące konfiguracje na urządzeniu z systemem Android:

Czas niezgodności	Limit czasu odpowiedzi użytkownika, po którym stosowana jest akcja wymuszania.
Działania egzekucyjne po przekroczeniu limitu czasu zgodności	Egzekwowanie działań, gdy użytkownik nie wykonuje czynności, które prowadzą do stanu zgodnego urządzenia.
Częstotliwość zbierania danych	Częstotliwość gromadzenia informacji o urządzeniu/GPS
Częstotliwość uderzeń serca urządzenia	Interwał, w którym urządzenie powinno kontaktować się z serwerem AppTec Min. 1 minuta Maks. 24 godziny
Włącz aktualizacje lokalizacji	W przypadku aktywacji urządzenie wysyła aktualizacje lokalizacji do serwera AppTec.
Czas aktualizacji lokalizacji	Określa, w jakich odstępach czasu urządzenie wysyła aktualizacje lokalizacji do AppTec.
Użyj dokładności lokalizacji Google do aktualizacji lokalizacji	Jeśli jest włączona, lokalizacja sieciowa będzie używana do aktualizacji lokalizacji (jeśli została wyłączona w sekcji "Ograniczenia", to ustawienie to nie będzie miało żadnego wpływu).
Używanie lokalizacji GPS do aktualizacji lokalizacji	Jeśli jest włączona, GPS będzie używany do aktualizacji lokalizacji
Zezwalaj na fałszywe lokalizacje	Umożliwia fałszowanie informacji o lokalizacji za pośrednictwem aplikacji innych firm.
Akcja Utracone połączenie	Jeśli opcja ta jest włączona, można określić działanie w przypadku, gdy urządzenie nie uzyska połączenia z serwerem MDM w interwale pulsu. Na przykład, jeśli urządzenie ma czas bicia serca wynoszący 5 minut, łączy się z serwerem o godzinie 10:35. Następnie urządzenie opuszcza zasięg Wi-Fi. Następne bicie serca o 10:40 nie powiedzie się i zostanie wykonana określona akcja.
Działanie	Działanie, które należy podjąć, gdy tylko urządzenie stanie się niezgodne.

	• Lock Urządzenie = urządzenie blokujące • Wipe Device = urządzenie zostanie przywrócone do ustawień fabrycznych. • Wipe Device & SD Card = urządzenie zostanie przywrócone do ustawień fabrycznych, a pamięć karty SD zostanie usunięta.
Próg	Można określić próg nieudanych uderzeń serca, które są niezbędne do wyzwolenia określonej akcji.

Tryb egzekwowania zasad	Domyślnie:	Użytkownicy będą okresowo monitowani o wykonanie zaległych działań
	Leniwe egzekwowanie zasad:	Użytkownicy nigdy nie będą proszeni o wykonanie zaległych akcji. Wszystkie otwarte akcje będą wyświetlane w AppTec Client
	Agresywne egzekwowanie zasad:	Użytkownicy będą nieustannie proszeni o wykonanie zaległych działań
Blokada wersji AppTec	Jeśli opcja ta jest włączona, można określić kod wersji aplikacji AppTec. Klient AppTec zaktualizuje się tylko do określonej wersji. Nowsze wersje będą ignorowane. Obniżenie wersji NIE jest możliwe.	
Kod wersji	Kod wersji aplikacji AppTec, która ma zostać zablokowana.	
Wyłączanie powiadomień AppTec	Jeśli opcja ta zostanie wyłączona, klient AppTec nie będzie wyświetlał powiadomienia na pasku powiadomień. W ten sposób użytkownicy mogą zamknąć klienta AppTec za pośrednictwem menedżera zadań. Jeśli klient AppTec jest zamknięty, kilka funkcji, w tym tryb kiosku i czarna/biała lista aplikacji, nie będzie działać poprawnie. Urządzenia Samsung oferują mechanizm ochrony dla AppTec Client. Powiadomienie jest domyślnie wyłączone na urządzeniach Samsung obsługujących interfejsy API KNOX. Powiadomienie nie powinno być wyłączone na urządzeniach z systemem Android 8.0 lub nowszym.	

Tapeta

Ustaw niestandardową tapetę	Włączanie/wyłączanie niestandardowej tapety
Tapeta	Ustawienie trybu tapety na użycie kodu koloru lub obrazu
Określ kolor	Określ kolor tła jako wartość szesnastkową, np. #000000 dla czarnego lub #fffff dla białego.
Ustaw obraz jako tapetę	Prześlij plik obrazu, którego chcesz użyć jako tapety.

Zarządzanie zasobami (tylko na poziomie urządzenia)

Informacje o urządzeniu

Model	Oznaczenie modelu urządzenia
System operacyjny	OS
Wersja systemu operacyjnego	Wersja systemu operacyjnego
Numer seryjny	Numer seryjny
Nazwa urządzenia	Nazwa urządzenia
Stan akumulatora	Stan akumulatora
Pamięć wolna / całkowita	Pamięć wolna / całkowita
Samsung Safe	Interfejs Samsung SAFE, wymagany dla różnych opcji ustawień
Dostępna karta SD	Dostępna karta SD
Emulowana karta SD	Emulowana karta SD
Wyjmowana karta SD	Wyjmowana karta SD
SD Free / Pamięć całkowita	Wolna pamięć SD / całkowita pamięć karty SD

Wi-Fi

Adres IP	Adres IP urządzenia
WiFi MAC	Adres MAC sieci Wi-Fi

Komórkowy

Status	Status (zainstalowana karta SIM)
Numer telefonu	Numer telefonu
Roaming (połączenia głosowe / transmisja danych)	Roaming dla połączeń głosowych / transmisji danych
Status roamingu	Bieżący status roamingu
Adres IP	Adres IP
Operator/Przewoźnik	Operator/Przewoźnik
Technologia komórkowa	Technologia komórkowa
IMEI	Numer IMEI
ICCID	Jest to identyfikator karty SIM, często również karty Smartcard lub Integrated Circuit Card (ICC).
IMSI	International Mobile Subscriber Identity (IMSI) zapewnia w sieciach GSM i UMTS jednoznaczną identyfikację użytkowników sieci. IMSI składa się z maksymalnie 15 cyfr i jest konfigurowany w następujący sposób: • Kod kraju sieci komórkowej (MCC), 3 cyfry • Kod sieci komórkowej (MNC), 2 lub 3 cyfry • Numer identyfikacyjny abonenta sieci komórkowej (MSIN), 1-10 cyfr
Obecny MCC/MNC	Patrz "SIM MCC/MNC"
SIM MCC/MNC	Kod kraju sieci komórkowej to ustalony identyfikator kraju, określony przez ITU zgodnie ze standardem E.212. Działa on w połączeniu z kodem sieci komórkowej (MNC) w celu identyfikacji sieci komórkowej. Oznacza kod kraju/sieci komórkowej karty SIM. Jeśli korzystasz z roamingu w innej sieci komórkowej, logicznie rzecz biorąc, "Bieżące MCC/MNC" i "SIM MCC/MNC" będą się różnić.

Bluetooth

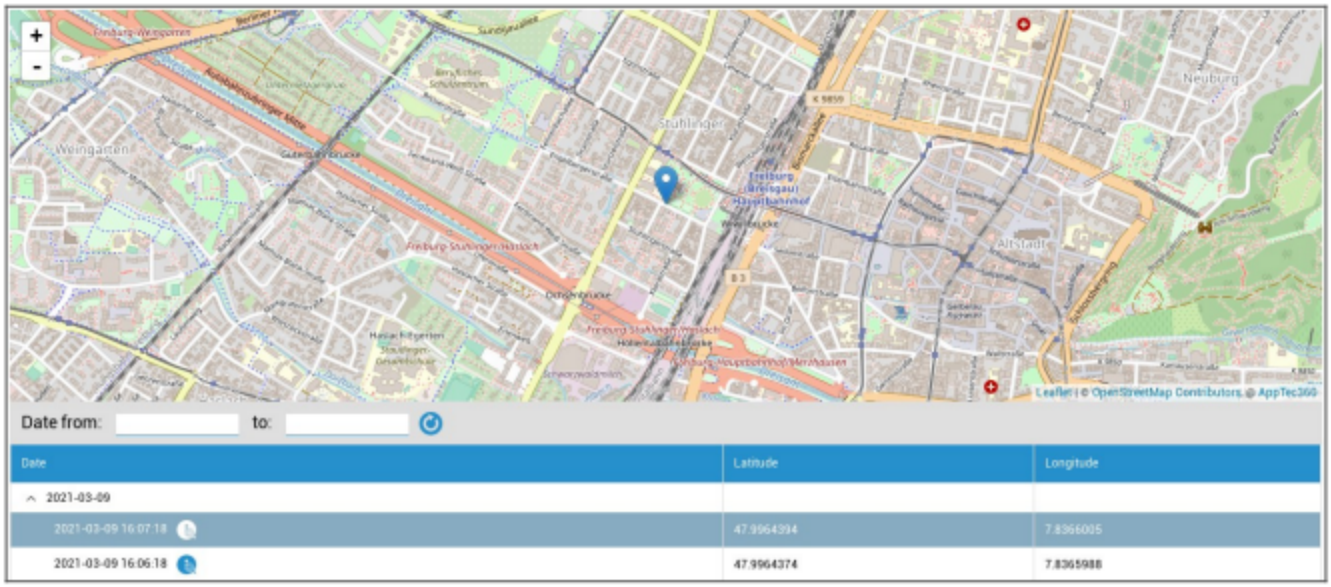
Bluetooth MAC	Adres MAC Bluetooth

Zarządzanie bezpieczeństwem

Ochrona przed kradzieżą (tylko na poziomie urządzenia)

Informacje GPS (tylko na poziomie urządzenia)

Tutaj można ustalić bieżącą/ostatnią lokalizację urządzenia. Lokalizacja może być chroniona jednym lub nawet dwoma hasłami - patrz: Ustawienia ogólne - Prywatność - Dostęp GPS



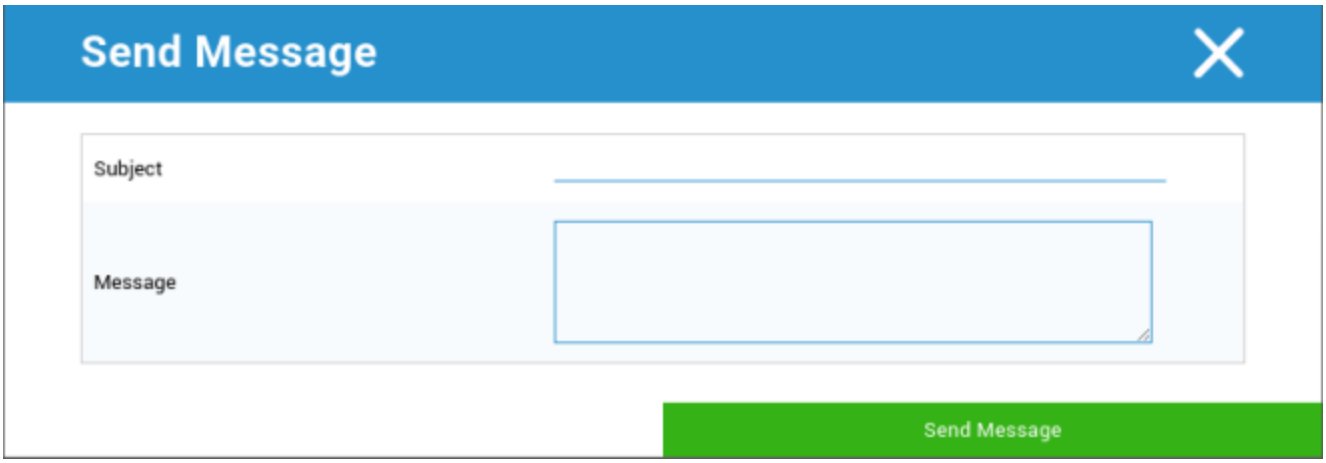
Wipe & Lock (tylko na poziomie urządzenia)

W sekcji "Wyczyść i zablokuj" można wykonać następujące trzy czynności:

Pełne wytarcie	Urządzenie jest przywracane do ustawień fabrycznych (dane firmowe i osobiste są usuwane). Działa tylko w przypadku Ulepszonego profilu pracy
Enterprise Wipe	Z urządzenia użytkownika końcowego usuwane są tylko dane firmowe (wszystkie aplikacje, dane itp. dostarczone przez AppTec).
Ekran blokady	Blokada ekranu jest aktywna, wystarczy odblokować urządzenie za pomocą hasła / kodu PIN urządzenia.

Wiadomość (tylko na poziomie urządzenia)

Tutaj można wpisać temat i wiadomość, a następnie wysłać ją do urządzenia użytkownika końcowego



Konfiguracja zabezpieczeń

Kod dostępu urządzenia

W sekcji "Kod dostępu" można ustawić hasło urządzenia, dostępne są następujące opcje ustawień

Minimalna długość hasła	Ustala minimalną liczbę symboli, które musi zawierać hasło	
Jakość hasła	Nieokreślony	Niniejsza polityka nie zawiera żadnych wymagań dotyczących hasła.
	Słabość biometryczna	Polityka ta zezwala na stosowanie technologii rozpoznawania biometrycznego o niskim poziomie bezpieczeństwa. Oznacza to technologie, które mogą rozpoznać tożsamość osoby do około 3-cyfrowego kodu PIN (fałszywe wykrycie jest mniejsze niż 1 na 1000).
	Coś	Ta polityka wymaga ustawienia pewnego rodzaju hasła lub wzorca, ale nie wymusza żadnych konkretnych reguł.
	Alfabetyczny	Użytkownik musi wprowadzić hasło zawierające co najmniej znaki alfabetu (lub inne symbole).
	Alfanumeryczne	Użytkownik musi wprowadzić hasło zawierające co najmniej znaki numeryczne i alfabetyczne (lub inne symbole).
	Kompleks	Domyślnie użytkownik musi wprowadzić hasło zawierające co najmniej literę, cyfrę i symbol specjalny. Dzięki tej jakości hasła można ograniczyć do różnych zestawów znaków, takich jak co najmniej wielka litera itp.
Minimalna długość hasła	Ustaw wymaganą liczbę znaków dla hasła. Można na przykład wymagać, aby kod PIN lub hasło miały co najmniej sześć znaków.	
Minimalne cyfry wymagane w haśle	Minimalne cyfry wymagane w haśle	
Minimalne małe litery wymagane w haśle	Minimalne małe litery wymagane w haśle	
Minimalne wielkie litery wymagane w haśle	Minimalne wielkie litery wymagane w haśle	

Minimalna liczba znaków nieliterowych wymaganych w haśle	Minimalna liczba znaków nieliterowych wymaganych w haśle
Minimalne symbole wymagane w haśle	Minimalne symbole wymagane w haśle

Maksymalna blokada czasu nieaktywności	Maksymalny czas nieaktywności użytkownika do blokady czasowej
Limit czasu wygaśnięcia hasła	Ustala, po jakim czasie hasło wygasa i musi zostać wydane nowe hasło.
Ograniczenie historii haseł	Liczba poprzednio używanych haseł, które nie są dozwolone
Maksymalna liczba nieudanych prób podania hasła	Ustala, jak często hasło może być wprowadzane niepoprawnie, zanim zostanie wykonane całkowite czyszczenie urządzenia.
Zezwalaj na uwierzytelnianie biometryczne	Umożliwia uwierzytelnianie za pomocą odcisku palca lub skanu tęczówki. Tylko dla Samsung KNOX 2.1 i nowszych wersji

Kod dostępu do kontenera

W sekcji "Passcode" można ustawić hasło do kontenera, dostępne są następujące opcje ustawień

Minimalna długość hasła	Ustala minimalną liczbę symboli, które musi zawierać hasło	
Jakość hasła	Nieokreślony	Niniejsza polityka nie zawiera żadnych wymagań dotyczących hasła.
	Słabość biometryczna	Polityka ta zezwala na stosowanie technologii rozpoznawania biometrycznego o niskim poziomie bezpieczeństwa. Oznacza to technologie, które mogą rozpoznać tożsamość osoby do około 3-cyfrowego kodu PIN (fałszywe wykrycie jest mniejsze niż 1 na 1000).
	Coś	Ta polityka wymaga ustawienia pewnego rodzaju hasła lub wzorca, ale nie wymusza żadnych konkretnych reguł.
	Alfabetyczny	Użytkownik musi wprowadzić hasło zawierające co najmniej znaki alfabetu (lub inne symbole).
	Alfanumeryczne	Użytkownik musi wprowadzić hasło zawierające co najmniej znaki numeryczne i alfabetyczne (lub inne symbole).
	Kompleks	Domyślnie użytkownik musi wprowadzić hasło zawierające co najmniej literę, cyfrę i symbol specjalny. Dzięki tej jakości hasła można ograniczyć do różnych zestawów znaków, takich jak co najmniej wielka litera itp.
Minimalna długość hasła	Ustaw wymaganą liczbę znaków dla hasła. Można na przykład wymagać, aby kod PIN lub hasło miały co najmniej sześć znaków.	
Minimalne cyfry wymagane w haśle	Minimalne cyfry wymagane w haśle	
Minimalne małe litery wymagane w haśle	Minimalne małe litery wymagane w haśle	
Minimalne wielkie litery wymagane w haśle	Minimalne wielkie litery wymagane w haśle	
Minimalna liczba znaków nieliterowych wymaganych w haśle	Minimalna liczba znaków nieliterowych wymaganych w haśle	

Minimalne symbole wymagane w haśle	Minimalne symbole wymagane w haśle

Maksymalna blokada czasu nieaktywności	Maksymalny czas nieaktywności użytkownika do blokady czasowej
Limit czasu wygaśnięcia hasła	Ustala, po jakim czasie hasło wygasa i musi zostać wydane nowe hasło.
Ograniczenie historii haseł	Liczba poprzednio używanych haseł, które nie są dozwolone
Maksymalna liczba nieudanych prób podania hasła	Ustala, jak często hasło może być wprowadzane niepoprawnie, zanim zostanie wykonane całkowite czyszczenie urządzenia.

Antywirus

Automatyczne skanowanie	Włącz okresowe automatyczne skanowanie
Interwał skanowania	Interwał badania (szybki / pełny)
Pełne automatyczne skanowanie	Włącz w pełni automatyczne skanowanie
Automatyczne aktualizacje	Włącz automatyczne aktualizacje
Interwał sprawdzania aktualizacji	Jak często aplikacja i jej baza danych powinny być aktualizowane (wirusy / uszkodzony kod)?
Ochrona aplikacji	Włącz automatyczne skanowanie aplikacji
Ochrona karty SD	Włącz automatyczne skanowanie karty SD
Aktualizacja tylko przez Wi-Fi	Po włączeniu tej opcji aktualizacje będą stosowane tylko wtedy, gdy urządzenie zostanie pomyślnie połączone z siecią Wi-Fi.

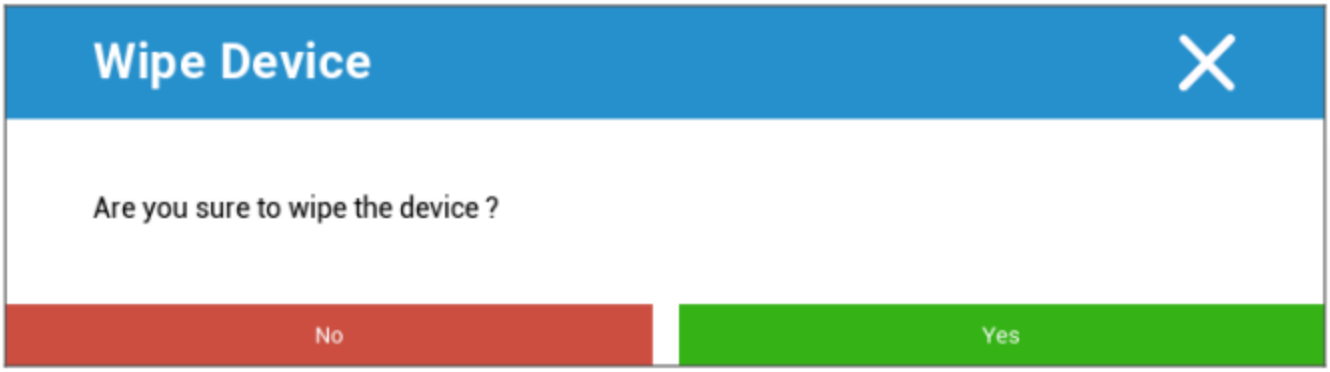
Koniec życia (tylko na poziomie urządzenia)

Wipe (tylko na poziomie urządzenia)

W sekcji "Wipe" można przywrócić ustawienia fabryczne urządzenia (tylko w przypadku profilu Enhanced Work Profile).

W tym przypadku dane firmowe i prywatne zostaną usunięte z urządzenia użytkownika końcowego.

Kliknięcie na "Symbol minus" spowoduje wyświetlenie następującego komunikatu:



Po wybraniu opcji "Tak" można wykonać czyszczenie.

W sekcji "Wipe Report" można wyświetlić następujące elementy

Wymazane przez	Historia tego, kto wykonał czyszczenie
Data	Data
Status	Status (np. czy czyszczenie zostało wykonane pomyślnie)

Ustawienia ograniczeń

Ograniczenia

Tutaj różne rzeczy mogą być ograniczane i blokowane.

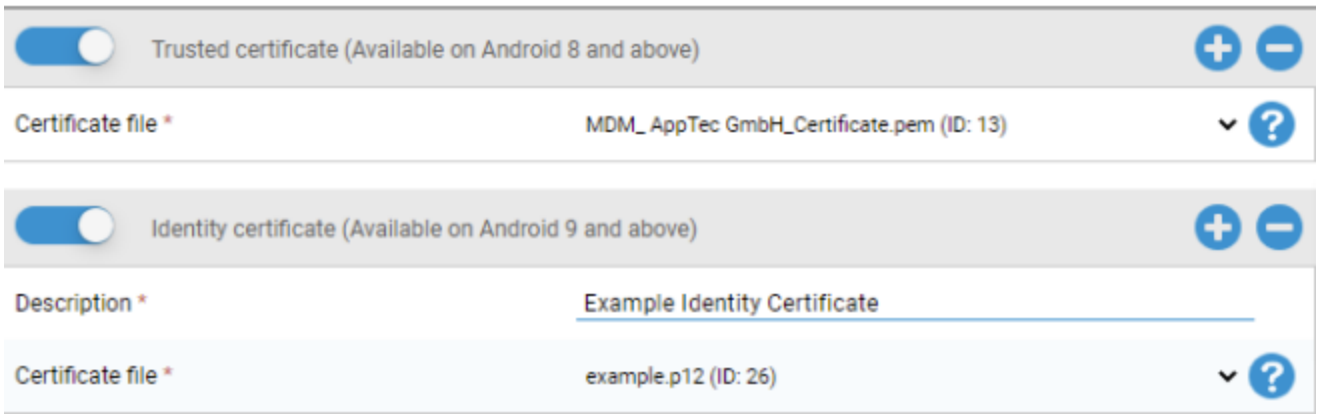
Egzekwowanie zgodności	Mode Prompt User - Użytkownik zostanie poproszony o wykonanie niezbędnych czynności. Tryb Lock-Down Container - Ukryj wszystkie aplikacje, dopóki nie zostaną spełnione wszystkie wymagania.
Polityka uprawnień środowiska uruchomieniowego	Monitowanie użytkownika o nowe żądania uprawnień Zawsze przyznawaj nowe żądania uprawnień Zawsze odrzucaj nowe żądania uprawnień Ostrzeżenie: Niektóre aplikacje mają problemy z rozpoznawaniem uprawnień, jeśli są one ustawione automatycznie. Jeśli zawsze udzielasz uprawnień i napotykasz problemy z aplikacjami informującymi o braku uprawnień, ustaw tę opcję na "monituj użytkownika" i ponownie zainstaluj aplikację
Zezwalaj na schowek wychodzący	Umożliwia kopiowanie i wklejanie z wnętrza kontenera na zewnątrz.
Zezwalaj na rozdzielczość ID dzwoniącego	Wyświetla nazwę połączenia przychodzącego na podstawie kontaktów w kontenerze.
Rozdzielczość wyszukiwania kontaktów	Umożliwia wyszukiwanie nazw w kontenerze kontaktów podczas wykonywania połączeń.
Zezwalaj na udostępnianie kontaktów Bluetooth	Umożliwia dostęp do kontenera kontaktowego w samochodzie
Nie zezwalaj na wychodzącą wiązkę NFC	Wyłącza NFC dla kontenera
Zezwalaj na nieznane źródła	Jeśli opcja ta jest włączona, użytkownicy mogą pobierać aplikacje poprzez instalację pliku .apk.
Zezwalaj na debugowanie USB	Jeśli opcja ta jest włączona, użytkownicy mogą włączyć debugowanie USB.
Nie zezwalaj na modyfikację konta	Zabrania tworzenia, usuwania i modyfikowania kont w kontenerze. Należy pamiętać, że niektóre aplikacje muszą utworzyć lub zmodyfikować konta, aby działały zgodnie z oczekiwaniami

Ograniczenia profilu roboczego. Dostępne tylko na urządzeniach z systemem Android 11 lub nowszym, z rozszerzonym profilem pracy.	
Nie zezwalaj na kamerę	Określa, czy kamera jest niedozwolona w profilu roboczym.
Wyłącz Bluetooth	Określa, czy bluetooth jest niedozwolony w profilu roboczym.
Włącz ochronę przed przywróceniem ustawień fabrycznych	Aktywuj tę opcję, aby zastąpić ochronę przed przywróceniem ustawień fabrycznych Androida kontem Google zdefiniowanym w "Ustawieniach ogólnych" → "Konfiguracja Androida" → "Android Enterprise" → "Ochrona przed przywróceniem ustawień fabrycznych" Jeśli ta opcja jest włączona i zresetujesz urządzenie, będziesz musiał podać skonfigurowane konto Google, aby ponownie skonfigurować urządzenie.
Kontrola aktualizacji systemu operacyjnego	Włącz tę opcję, aby ustawić zachowanie aktualizacji na automatyczne, okienkowe lub odroczone.
Polityka aktualizacji	Automatyczna: instaluje się automatycznie, gdy tylko dostępna jest aktualizacja. Windowed: Automatyczna instalacja w ramach codziennego okna konserwacji. Konfiguruje to również aplikacje Play do aktualizacji w oknie. Jest to zdecydowanie zalecane dla urządzeń kioskowych, ponieważ jest to jedyny sposób, w jaki aplikacje trwale przypięte do pierwszego planu mogą być aktualizowane przez Play. Odłóż: Odkłada automatyczną instalację na maksymalnie 30 dni.

Ograniczenia profilu osobistego. Dostępne tylko na urządzeniach z systemem Android 11 lub nowszym, z ulepszonym profilem roboczym.	
Nie zezwalaj na kamerę	Określa, czy kamera jest niedozwolona w profilu osobistym.
Wyłącz Bluetooth	Określa, czy bluetooth jest niedozwolony w profilu osobistym.
Zezwalaj na nieznane źródła	Jeśli opcja ta jest włączona, użytkownicy profilu roboczego mogą pobierać aplikacje poprzez instalację pliku .apk.

Zarządzanie certyfikatami

Tutaj możesz dystrybuować zaufane certyfikaty i certyfikaty tożsamości na swoje urządzenia. Do dystrybucji zaufanych certyfikatów wymagany jest system Android 8 lub nowszy, a do dystrybucji certyfikatów tożsamości wymagany jest system Android 9 lub nowszy.



Za pomocą "+" można dodać wiele certyfikatów.

Zaufane certyfikaty muszą być w formacie PEM.

Certyfikaty tożsamości muszą być w formacie PKCS12.

Zarządzanie połączeniami

Wifi

W przypadku tego ustawienia należy przeprowadzić wstępną konfigurację urządzeń użytkowników końcowych w celu uzyskania dostępu do wewnętrznych punktów dostępu

.

Identyfikator zestawu usług (SSID)	SSID dla sieci, która ma być połączona
Ukryta sieć	Aktywuj, jeśli punkt dostępowy nie rozgłasza identyfikatora SSID

Typ zabezpieczenia

Ustalenie typu zabezpieczeń punktu dostępowego

WEP

Hasło	Hasło do punktu dostępowego

WPA/WPA2

Hasło	Hasło do punktu dostępowego

802.1x EAP

Metoda EAP

PWD	Tożsamość	Tożsamość
	Hasło	Hasło

PEAP	Protokół uwierzytelniania fazy 2	brak	Brak dodatkowego protokołu
		MSCHAPV2	Protokół MSCHAPV2
		GTC	Protokół GTC
	Certyfikat CA	Certyfikat CA	
	Tożsamość	Tożsamość	
	Anonimowa tożsamość	Anonimowa tożsamość	
	Hasło	Hasło	

TTLS	Protokół uwierzytelniania fazy 2	brak	Brak dodatkowego protokołu
		PAP	Protokół PAP
		MSCHAP	Protokół MSCHAP
		MSCHAPV2	Protokół MSCHAPV2
		GTC	Protokół GTC
	Certyfikat CA	Certyfikat CA	
	Tożsamość	Tożsamość	
	Anonimowa tożsamość	Anonimowa tożsamość	
	Hasło	Hasło	

TLS	Certyfikat CA	Certyfikat CA
	Tożsamość	Tożsamość
	Hasło	Hasło

VPN

Nazwa połączenia	Nazwa połączenia VPN

Typ VPN

VPN

Klient VPN

AppTec VPN Client	
Konfiguracja bramy	Wybierz konfigurację Gateway VPN (patrz **Ustawienia ogólne > Universal Gateway > Ustawienia VPN**).
Always On VPN	Włącz blokadę natywną
Włącz blokadę AppTec	Włącz blokadę AppTec

Wbudowany (dostępny tylko w urządzeniach Samsung)			
Typ połączenia	PPTP	Serwer	Serwer
		Włącz szyfrowanie PPTP	Włącz szyfrowanie PPTP
	L2TP / IPSec PSK	Serwer	Serwer
		Klucz wstępny IPSec	Klucz wstępny IPSec
		Włącz L2TP Secret	Włącz L2TP Secret
		L2TP Secret	L2TP Secret
	IPSec XAuth PSK	Serwer	Serwer
		Identyfikator IPSec	Identyfikator IPSec
		Klucz wstępny IPSec	Klucz wstępny IPSec
Domeny wyszukiwania DNS	Domeny wyszukiwania DNS		
Ustawienia eksperckie	Serwery DNS	Serwery DNS	
	Trasy przekazywania	Trasy przekazywania	

Open VPN		
Serwer	Serwer	
Profil OpenVPN	Profil OpenVPN	
Aplikacja OpenVPN	OpenVPN dla systemu Android (zalecane)	
	OpenVPN Connect	
Ustawienia eksperckie	Serwery DNS	Serwery DNS
	Trasy przekazywania	Trasy przekazywania

Samsung / Strong Swan			
Typ połączenia	PPTP	Serwer	Serwer
		Nazwa użytkownika	Nazwa użytkownika
		Hasło	Hasło
		Włącz szyfrowanie PPTP	Włącz szyfrowanie PPTP
	L2TP / IPSec PSK	Serwer	Serwer
		Klucz wstępny IPSec	Klucz wstępny IPSec
		Nazwa użytkownika	Nazwa użytkownika
		Hasło	Hasło
		Włącz L2TP Secret	L2TP Secret
	IPSec XAuth PSK	Serwer	Serwer
		Identyfikator IPSec	Identyfikator IPSec
		Klucz wstępny IPSec	Klucz wstępny IPSec
		Nazwa użytkownika	Nazwa użytkownika
		Hasło	Hasło
Ustawienia eksperckie	Serwery DNS	Serwery DNS	
	Trasy przekazywania	Trasy przekazywania	

Cisco Any Connect		
Serwer	Serwer	
Tryb certyfikatu	Wyłączony	Wyłączony
	Automatyczny	Automatyczny
Ustawienia eksperckie	Serwery DNS	Serwery DNS
	Trasy przekazywania	Trasy przekazywania

VPN dla poszczególnych aplikacji

Klient VPN

AppTec VPN Client		
Konfiguracja bramy	Wybierz konfigurację Gateway VPN (patrz **Ustawienia ogólne > Universal Gateway > Ustawienia VPN**).	
Aplikacje VPN	Aplikacje VPN	
Always On VPN	Włącz blokadę natywną	Always On VPN
Włącz blokadę AppTec	Włącz blokadę AppTec	

Samsung / Strong Swan			
Typ połączenia	PPTP	Serwer	Serwer
		Aplikacje VPN	Aplikacje VPN
		Nazwa użytkownika	Nazwa użytkownika
		Hasło	Hasło
		Włącz szyfrowanie PPTP	Włącz szyfrowanie PPTP
	L2TP / IPSec PSK	Serwer	Serwer
		Aplikacje VPN	Aplikacje VPN
		Klucz wstępny IPSec	Klucz wstępny IPSec
		Nazwa użytkownika	Nazwa użytkownika
		Hasło	Hasło
		Włącz L2TP Secret	L2TP Secret
	IPSec XAuth PSK	Serwer	Serwer
		Aplikacje VPN	Aplikacje VPN
		Identyfikator IPSec	Identyfikator IPSec
		Klucz wstępny IPSec	Klucz wstępny IPSec
		Nazwa użytkownika	Nazwa użytkownika
		Hasło	Hasło
Ustawienia eksperckie	Serwery DNS	Serwery DNS	
	Trasy przekazywania	Trasy przekazywania	

Ograniczenia

Tutaj można ustawić ograniczenia związane z zarządzaniem połączeniami

Zezwalaj na transmisję danych w roamingu	Zezwalaj na transmisję danych w roamingu
Wymuś roaming danych	W przypadku aktywacji roaming danych mobilnych jest włączony na stałe (niezalecane!). To ustawienie zastępuje ustawienie "Zezwalaj na transmisję danych w roamingu"!
Użyj systemowego serwera proxy http	Korzystanie z serwera proxy HTTP, który jest dostępny w ustawieniach systemu, zależy od podłączonej sieci (WiFi lub APN)

Zarządzanie PIM

Gmail Exchange

Informacje: Ta konfiguracja zostanie zastosowana do aplikacji Gmail. Musisz więc zatwierdzić i zainstalować Gmaila.

Adres e-mail	Podany adres e-mail użytkownika Zwróć uwagę na "symbole zastępcze", których możesz użyć do pracy z poświadczeniami i nie wprowadzaj zmian ręcznie na każdym urządzeniu. Wystarczy jedno kliknięcie, aby wyświetlić je dla siebie
Nazwa hosta serwera	Adres serwera serwerów Exchange
Nazwa logowania	Nazwa logowania dla danego urządzenia użytkownika końcowego, należy również zwrócić uwagę na "symbole zastępcze tutaj
Podpis	Można dołączyć podpis (wskazówka: niektóre urządzenia wymagają formatowania HTML dla podpisu).
Liczba poprzednich dni do synchronizacji	Liczba dni określająca, kiedy wiadomości e-mail są synchronizowane z powrotem
Identyfikator urządzenia	Łańcuch zawierający identyfikator urządzenia EAS. Jest to część protokołów EAS i jest dostępna w niektórych lokalizacjach
Używanie protokołu Secure Sockets Layer (SSL)	Użyj połączenia SSL
Akceptuj wszystkie certyfikaty	Akceptowane są wszystkie certyfikaty. Wybierz tę opcję, jeśli serwer Exchange korzysta z certyfikatu z podpisem własnym
Zezwalaj na konta niezarządzane	Zezwalaj użytkownikom na dodawanie lub usuwanie dowolnego konta Exchange innego niż konto określone w tej konfiguracji zarządzanej. Jeśli to ustawienie jest włączone, nie można uniemożliwić użytkownikom dodawania innych kont Exchange do Gmaila. Nie można również kontrolować udostępniania danych między innymi aplikacjami a kontami Exchange dodanymi przez użytkowników. To ustawienie powinno być włączone tylko wtedy, gdy użytkownicy muszą utrzymywać więcej niż jedno służbowe konto Exchange w Gmailu.

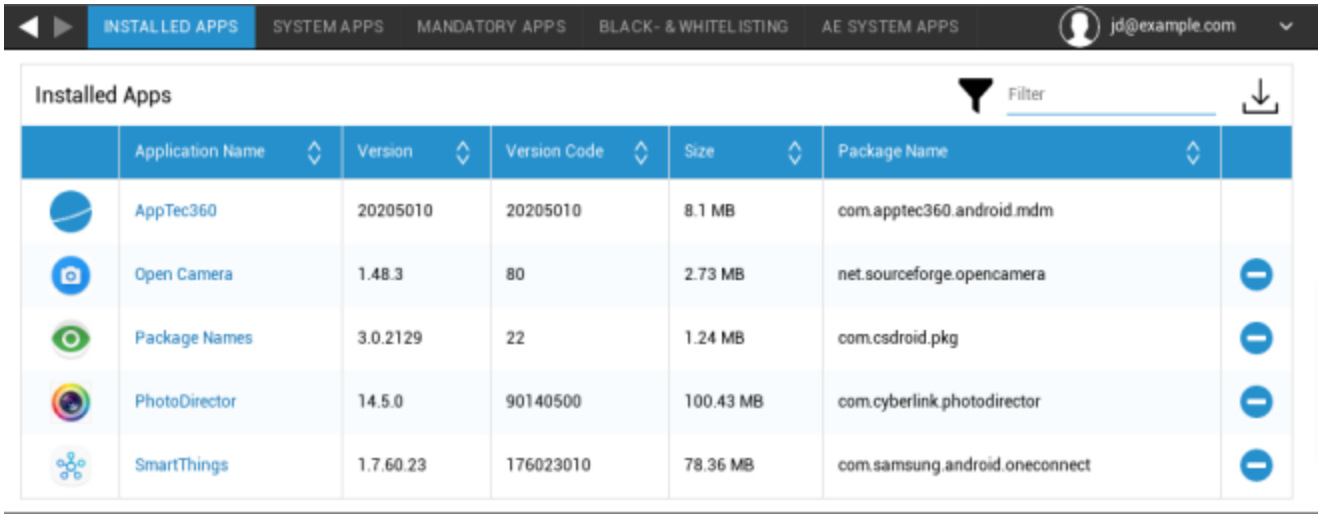
Certyfikat klienta	Certyfikat klienta. Wymagany tylko wtedy, gdy serwer pocztowy oczekuje jego obecności.

Zarządzanie aplikacjami

Menedżer aplikacji dla przedsiębiorstw

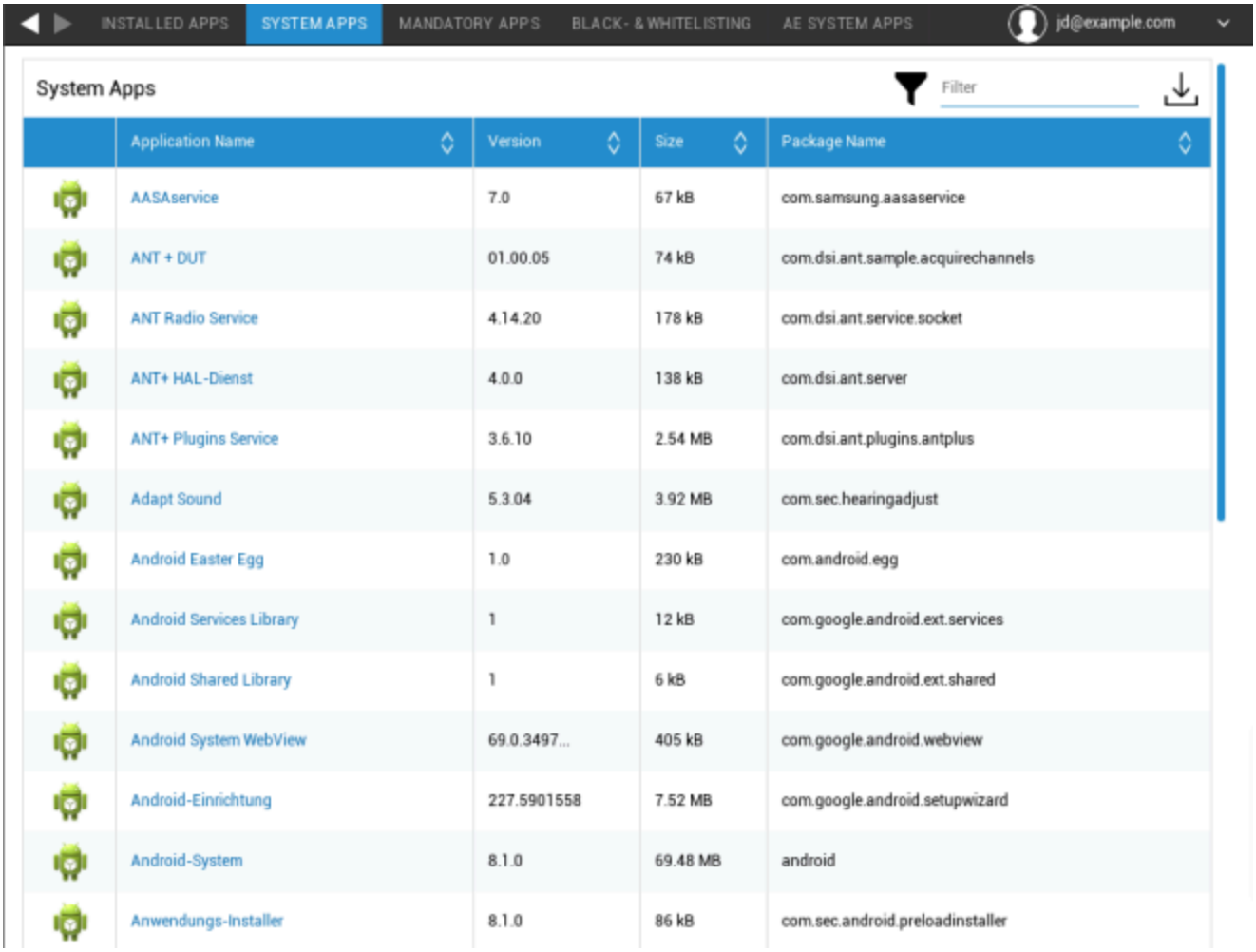
Zainstalowane aplikacje (tylko na poziomie urządzenia)

Tutaj zostaną wyświetlone wszystkie aplikacje, które są obecnie zainstalowane w kontenerze.



Aplikacje systemowe (tylko na poziomie urządzenia)

W sekcji "Aplikacje systemowe" wyświetlone zostaną wszystkie aplikacje i usługi, które zostały już zainstalowane na urządzeniu użytkownika końcowego przez producenta urządzenia.

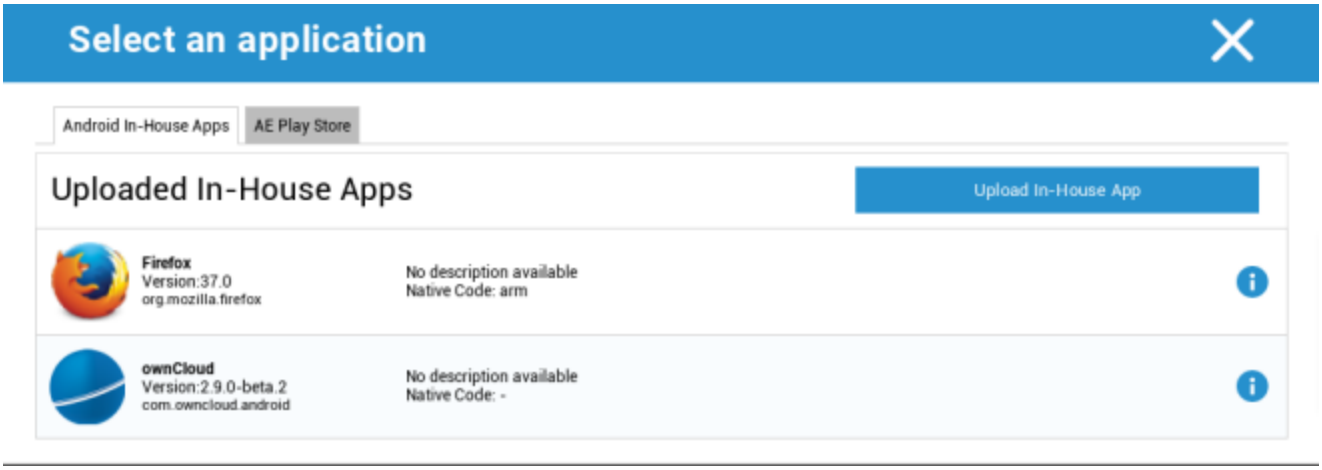


Aplikacje obowiązkowe

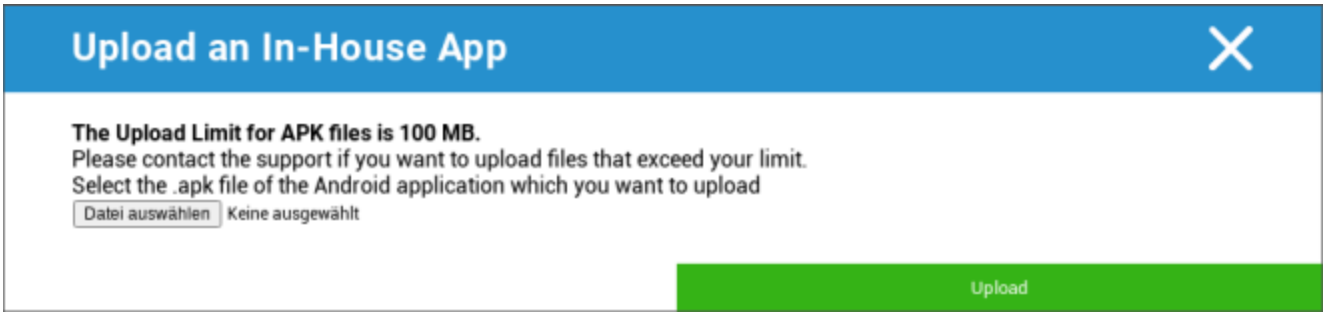
W sekcji Aplikacje obowiązkowe można ustanowić obowiązkowe wymagane aplikacje. Użytkownik będzie stale monitowany o zainstalowanie tej wyznaczonej aplikacji, jeśli jest to aplikacja wewnętrzna. Aplikacje ze Sklepu Play zostaną zainstalowane automatycznie.

Za pomocą , można zdefiniować wymaganą aplikację.

Może to być aplikacja wewnętrzna z "Aplikacji wewnętrznych Android", którą przesłałeś w Ustawieniach ogólnych.

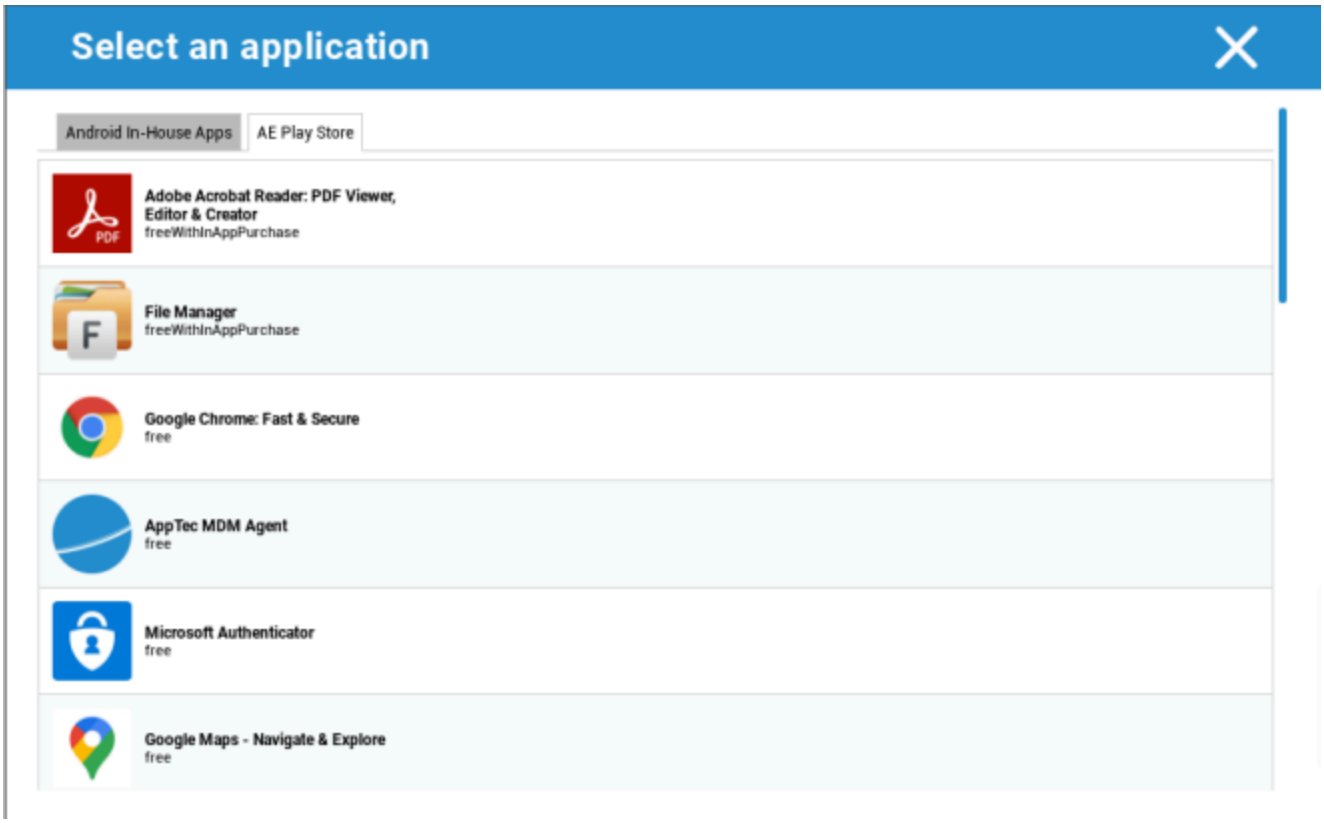


Możesz także bezpośrednio wybrać i przesłać plik apk za pomocą opcji "Prześlij aplikację wewnętrzną".



Jeśli instalujesz aplikację wewnętrzną, będziesz mieć możliwość aktywowania opcji "Aktualizuj". Jeśli ta opcja jest aktywna i zdefiniowano nowszą wersję w In-House App DB, aplikacja zostanie zaktualizowana na urządzeniu.

Może to być również aplikacja "AE Play Store" ze sklepu Google Work Play Store.



Tylko zatwierdzone "Aplikacje AE Play Store" będą wyświetlane w tej zakładce.

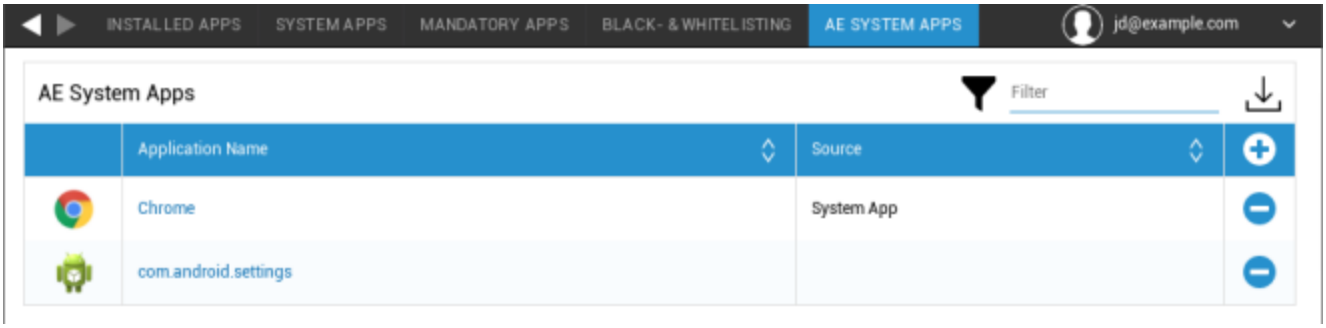
Aby zatwierdzić "Aplikację AE Play Store", przejdź do "Ustawienia ogólne" > "Zarządzanie aplikacjami" > "AE Play".

Store" i dodać aplikację za pomocą przycisku, który przekieruje Cię do zakładki "Play Store Apps" (lub możesz bezpośrednio przejść do zakładki "Play Store Apps").

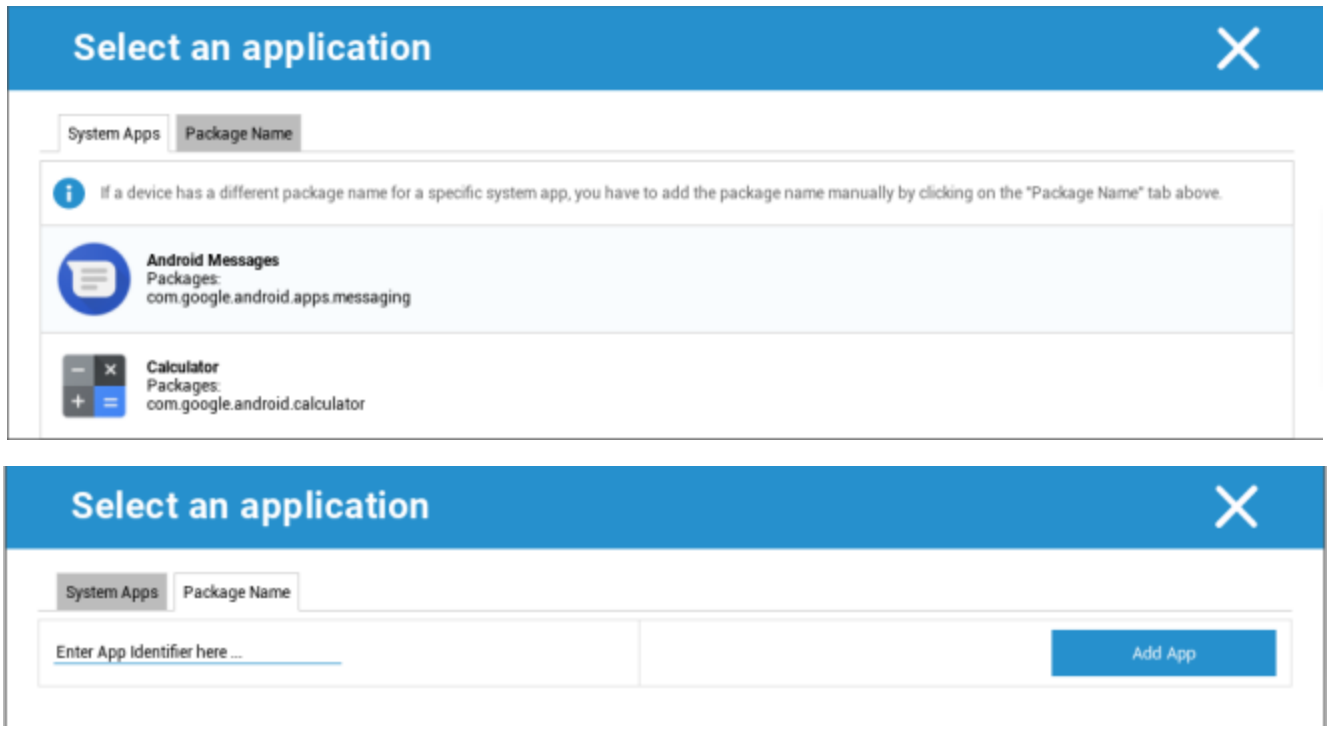
W zakładce "Play Store Apps" można wyszukiwać aplikacje. Po kliknięciu aplikacji otworzy się strona aplikacji, na której można zatwierdzić aplikację, klikając przycisk "Zatwierdź".

Aplikacje systemowe AE

W tym miejscu można zdefiniować listę zawierającą określone aplikacje systemowe, które powinny być aktywowane na urządzeniach.



Po kliknięciu przycisku można wybrać z listy możliwych aplikacji systemowych dostarczonych przez Google lub bezpośrednio wprowadzić nazwę pakietu aplikacji systemowej, która powinna zostać aktywowana.



Należy pamiętać, że aplikacje systemowe na liście dostarczonej przez Google to tylko aplikacje, które mogą być aplikacjami systemowymi, ale niekoniecznie muszą być aplikacjami systemowymi na urządzeniach.

Jednak ta lista dotyczy tylko aplikacji, które są już wstępnie zainstalowane.

Dodawanie aplikacji, które nie są wstępnie zainstalowane na urządzeniach, nie będzie miało wpływu na urządzenia, niezależnie od tego, czy aplikacja znajduje się na liście dostarczonej przez Google, czy nazwa pakietu aplikacji jest wprowadzana bezpośrednio.

Ograniczenia i ustawienia

Ustawienia zarządzania aplikacjami

W tym miejscu można skonfigurować zachowanie urządzenia w zakresie aktualizacji aplikacji.

Częstotliwość sprawdzania aktualizacji	Określa, w jakich odstępach czasu klient AppTec będzie wyszukiwał aktualizacje aplikacji. Wartość domyślna to 24 godziny.
Próg Wi-Fi	Aplikacje większe niż określony rozmiar będą pobierane przez sieć Wi-Fi. W przypadku wybrania opcji "Tylko Wi-Fi" wszystkie aplikacje będą pobierane przez sieć Wi-Fi.

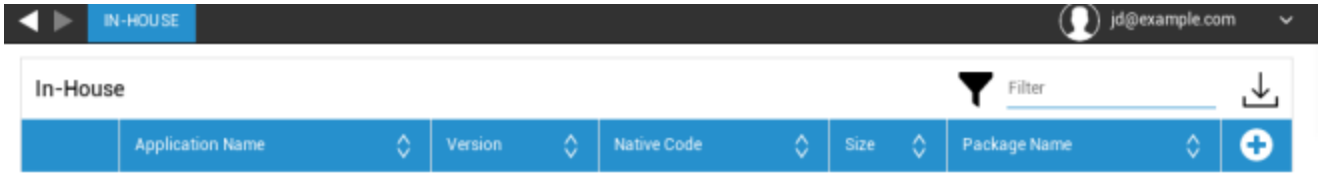
Sklep z aplikacjami dla przedsiębiorstw

Wewnątrz firmy

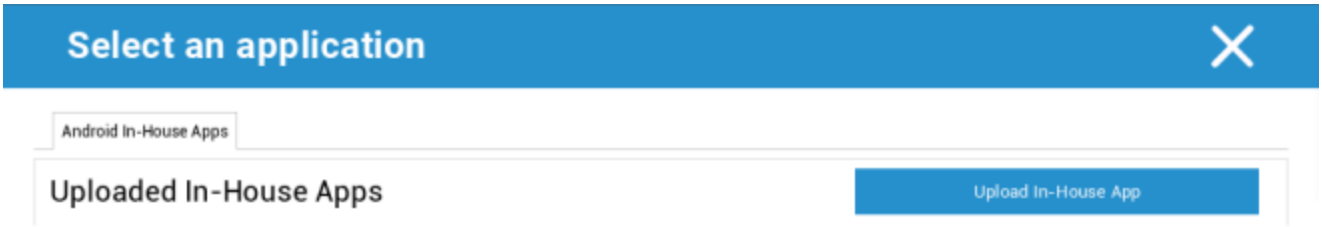
W punkcie "In-House" można przesyłać i rozpowszechniać aplikacje opracowane wewnętrznie.

Symbol ten umożliwia dystrybucję dodatkowych aplikacji wewnętrznych.

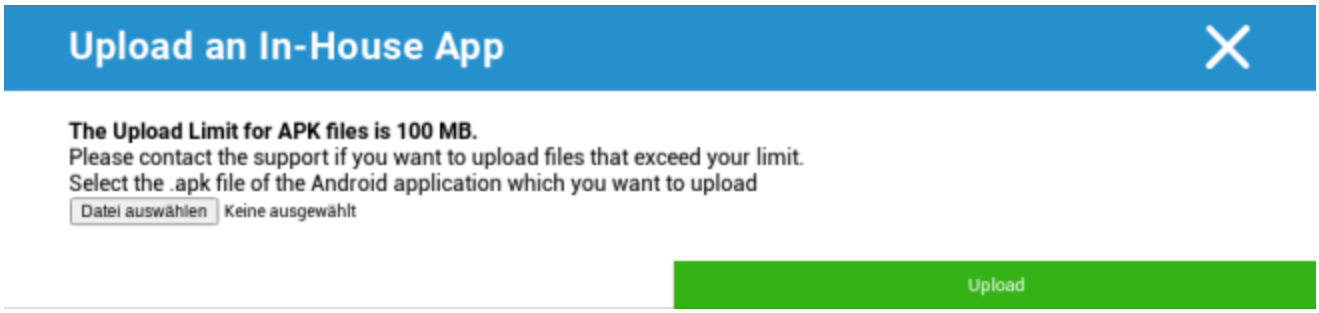
Jeśli instalujesz aplikację wewnętrzną, będziesz mieć możliwość aktywowania opcji "Aktualizuj". Jeśli ta opcja jest aktywna i zdefiniowano nowszą wersję w In-House App DB, aplikacja zostanie zaktualizowana na urządzeniu.



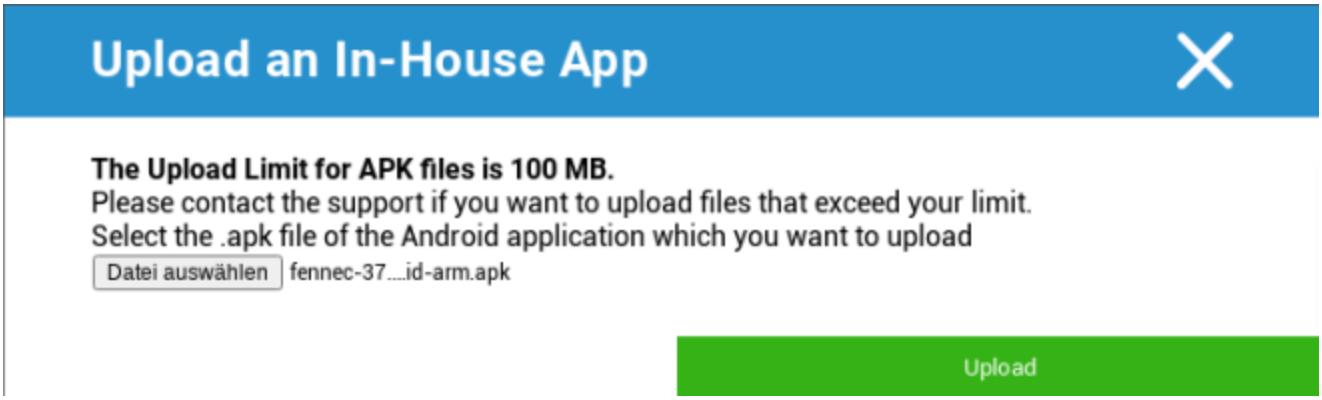
Jeśli nie rozpowszechniłeś aplikacji wewnętrznych, otrzymasz następujący przegląd:



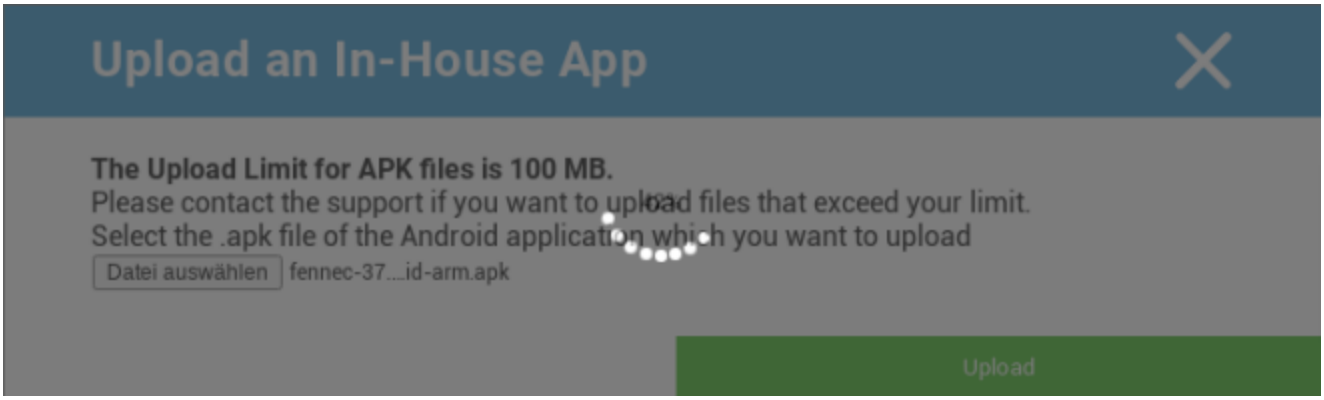
W tym celu kliknij "Prześlij aplikację wewnętrzną", a następnie otrzymasz następujący przegląd:



Teraz wybierz za pomocą "Wyszukaj..." plik .apk, a następnie kliknij "Prześlij".



Aplikacja zostanie teraz przesłana, a w środku okręgu pojawi się wskaźnik procentowy pokazujący, jaka część aplikacji została już przesłana.



Jeśli przesyłanie aplikacji wewnętrznej powiodło się, można ją znaleźć w katalogu aplikacji.

Użytkownik ma teraz możliwość wyświetlenia i zainstalowania tej aplikacji w AppTec Store na urządzeniu użytkownika końcowego, w kategorii "In-House".

Ze względu na fakt, że nie wiąże się to z aplikacją Google PlayStore, użytkownik nie potrzebuje zapisanego identyfikatora Google ID na swoim urządzeniu końcowym.

Sklep Play dla przedsiębiorstw

Sklep AE Play

Tutaj można dodawać aplikacje do Android Enterprise Playstore. Pamiętaj, że przed dodaniem aplikacji musisz je zatwierdzić za pomocą konta administratora AE.

Aby zatwierdzić aplikację, zapoznaj się z instrukcjami w sekcji Aplikacje obowiązkowe.

Zarządzanie treścią

ContentBox

Tutaj można aktywować ContentBox.

Po przełączeniu opcji "Enable ContentBox" na "On", oddzielna aplikacja ContentBox zostanie automatycznie zainstalowana na urządzeniu użytkownika końcowego.

Bezpieczna przeglądarka

W tym miejscu można skonfigurować ustawienia przeglądarki AppTec Secure Browser.

Po przełączeniu sekcji "Secure Browser" na "On", na urządzeniu użytkownika końcowego zostanie automatycznie zainstalowana oddzielna aplikacja przeglądarki.

Wymagaj hasła	Wymagaj od użytkownika skonfigurowania i używania hasła w celu uzyskania dostępu do przeglądarki.
Minimalna wymagana długość hasła	Ustaw wymaganą liczbę znaków dla hasła
Wymagana jakość hasła	Ustaw wymaganą jakość hasła
Ogranicz pobieranie / Otwórz w	
Ogranicz przesyłanie	
Prześlij na białą listę	Lista adresów URL, dla których przesyłanie będzie zawsze dozwolone.
Zezwalaj na kopiowanie	Zezwalaj na kopiowanie, wycinanie lub udostępnianie tekstu wewnątrz stron internetowych.
Zezwalaj na przechwytywanie ekranu	Zezwalaj na przechwytywanie zrzutów ekranu.
Częstotliwość czyszczenia danych	Wybierz, z jaką częstotliwością WSZYSTKIE dane użytkownika (historia, pamięć podręczna itp.) mają być automatycznie usuwane.
Zakładki firmowe	Zakładki pojawią się w folderze "Zakładki firmowe" w zakładkach przeglądarki. Nie są one edytowalne przez użytkownika.
Ukryj pasek adresu	
Biała lista w przeglądarce (bez Universal Gateway)	Włącza białą listę adresów URL po stronie klienta. • Zakładki firmowe są zawsze na białej liście • Obsługiwane tylko dla 100 adresów URL • Użyj Universal Gateway do nieograniczonej czarnej i białej listy.
Adresy URL na białej liście	Lista dozwolonych adresów URL.

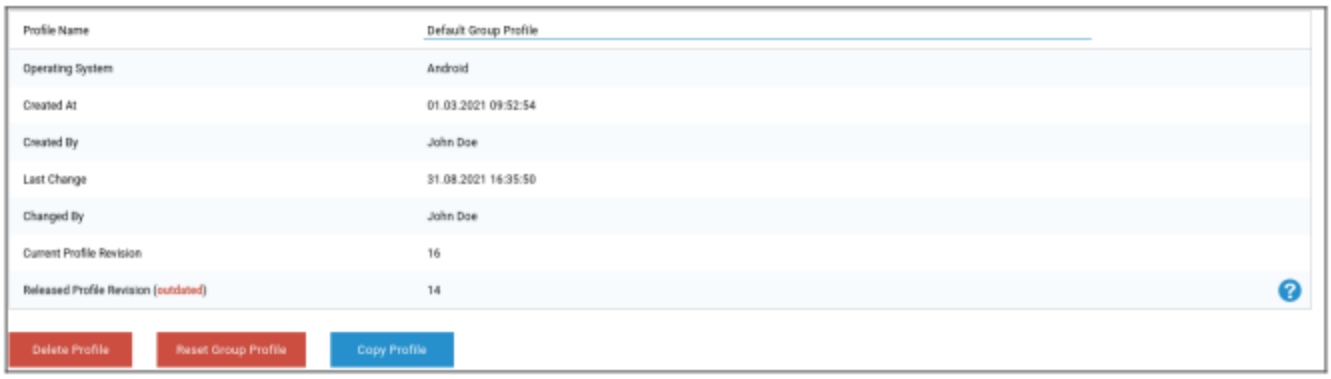
Czarna i biała lista oparta na bramie	Czarna lista zawiera następujące wymagania: • Działająca bramka uniwersalna AppTec ("Ustawienia ogólne" → "Bramka uniwersalna") • Działająca konfiguracja VPN z określonym serwerem DNS ("Ustawienia ogólne" → "Brama uniwersalna" → "Ustawienia VPN"). • Konfiguracja czarnej listy ("Ustawienia ogólne" → "Universal Gateway" → "Czarna lista domen"). • Prawidłowe połączenie VPN w profilu ("Zarządzanie połączeniami" → "VPN").

Konfiguracja systemu Android

Ogólne

Przegląd profilu grupy (tylko na poziomie grupy)

Po otwarciu profilu grupy wyświetlony zostanie szybki przegląd profilu.



Nazwa profilu	Nazwa profilu (można ją zmienić tutaj)
System operacyjny	System operacyjny, dla którego przeznaczony jest profil
Utworzono w	Czas stworzenia
Utworzony przez	Twórca profilu
Ostatnia zmiana	Czas ostatniej zmiany profilu
Zmienione przez	Konto, które wprowadziło ostatnie zmiany
Aktualna wersja profilu	Zmiana zapisanego stanu profilu
Wydana wersja profilu	Wersja przypisanego profilu ("Przypisz teraz"). Jeśli etykieta pokazuje "(nieaktualne)" za tekstem, oznacza to, że profil został zapisany, ale nie został jeszcze przypisany, więc urządzenia nadal będą otrzymywać starszą wersję.

Przegląd urządzeń (tylko na poziomie urządzenia)

Jeśli jesteś na urządzeniu, otrzymasz podsumowanie wybranego urządzenia, które zawiera następujące informacje:

Nazwa urządzenia	Nazwa urządzenia
Ostatnia znana lokalizacja	Ostatnie znane współrzędne GPS
Numer telefonu	Numer telefonu
Przypisane aplikacje obowiązkowe	Liczba przypisanych aplikacji obowiązkowych
Wersja systemu operacyjnego	Wersja systemu operacyjnego urządzenia
System operacyjny	System operacyjny (Android / iOS / Windows Phone)
Numer seryjny	Numer seryjny urządzenia
Własność urządzenia	Urządzenie firmowe lub prywatne
Typ urządzenia	Telefon lub tablet
Zakorzeniony	Status, wskazujący, czy urządzenie zostało zrootowane.
Zgodność	Zgodność z wytycznymi
Adres IP	Adres IP
Ostatnio widziany	Punkt w czasie, kiedy urządzenie ostatnio łączyło się z AppTec
Last Push	Punkt w czasie, gdy serwer wysłał wiadomość push do urządzenia
Przypisanie użytkownika	Lista rozwijana umożliwiająca przypisanie urządzenia do innego użytkownika

Wersja konfiguracji (tylko na poziomie urządzenia)

W tym miejscu wyświetlany jest przegląd profili grupowych przypisanych do urządzenia.

Jeśli klikniesz profil grupy, uzyskasz do niego bezpośredni dostęp i będziesz mógł dokonać ustawień.

Za pomocą symbolu można przywrócić przypisane aplikacje do ustawień profilu grupy.

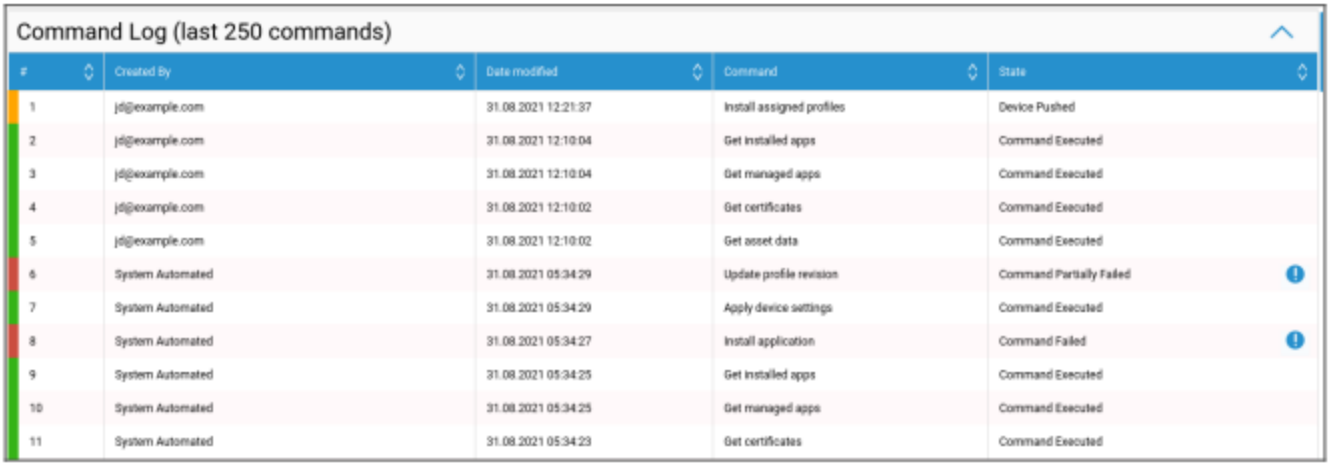
Za pomocą symbolu można zresetować profil urządzenia, aby nie miał żadnych ustawień.

"Newer Revision available" oznacza, że profil grupy został zmieniony i zapisany, ale nie został przypisany. Profil grupy musi zostać przypisany za pomocą opcji "Przypisz teraz" na poziomie grupy, aby zastosować zmiany do urządzeń.

Dziennik urządzenia (tylko na poziomie urządzenia)

Dziennik poleceń

Tutaj można sprawdzić, które polecenia zostały wydane dla urządzenia i jaki jest ich status.



Polecenia utworzone przez "System Automated" są automatycznie tworzone przez system.

Możliwe statusy poleceń

Urządzenie wciśnięte	Żądanie push zostało wysłane do usługi push (np. APNS), aby poinformować urządzenie o konieczności połączenia się z serwerem EMM.
Utworzone polecenie	Polecenie zostało utworzone w systemie.
Wysłane polecenie	Polecenie zostało wysłane do urządzenia po nawiązaniu połączenia z serwerem.
Polecenie wykonane	Polecenie zostało pomyślnie wykonane.
Polecenie nie powiodło się	Polecenie nie powiodło się. *
Polecenie częściowo nieudane	W zależności od systemu operacyjnego urządzenia niektóre polecenia mogą zostać zgrupowane. W tym przypadku niektóre części tej grupy poleceń nie powiodły się. *
Polecenie wykonane, ostatecznie nieudane	Polecenie zostało wykonane, ale być może nie.
Przesunięcie polecenia	Polecenie zostało powtórzone przez użytkownika.
Odrzucony	Polecenie zostało odrzucone. Na przykład dlatego, że zostało zastąpione przez inne polecenie lub urządzenie zostało ponownie zarejestrowane, a stare polecenia zostały usunięte.

*Jeśli za wiadomością znajduje się wykrzyknik, możesz uzyskać więcej informacji, najeżdżając kursorem na ikonę.

Ustawienia urządzenia

Konfiguracja klienta

W tym miejscu można przeprowadzić następujące konfiguracje na urządzeniu z systemem Android:

Komunikat ostrzegawczy po wyłączeniu zarządzania urządzeniami	Ustanowiony komunikat ostrzegawczy po wyłączeniu zarządzania urządzeniami
Czas niezgodności	Limit czasu, po którym zostanie wykonana "Akcja egzekwowania po zapewnieniu zgodności", jeśli urządzenie nie jest zgodne. Min. 1 minuta Maks. 24 godziny
Działania egzekucyjne po przekroczeniu limitu czasu zgodności	Działanie, które należy podjąć, gdy tylko urządzenie stanie się niezgodne. • nic nie robić = brak działania • Urządzenie blokujące = urządzenie blokujące • Wipe Device = urządzenie zostanie przywrócone do ustawień fabrycznych.
Częstotliwość zbierania danych	Częstotliwość gromadzenia informacji o urządzeniu/GPS
Częstotliwość uderzeń serca urządzenia	Interwał, w którym urządzenie powinno kontaktować się z serwerem AppTec360 Min. 1 minuta Maks. 24 godziny
Włącz aktualizacje lokalizacji	W przypadku aktywacji urządzenie wysyła aktualizacje lokalizacji do serwera AppTec360.
Czas aktualizacji lokalizacji	Określa, w jakich odstępach czasu urządzenie wysyła aktualizacje lokalizacji do AppTec.
Użyj dokładności lokalizacji Google do aktualizacji lokalizacji	Jeśli zostanie aktywowana, dokładność lokalizacji Google (wcześniej znana jako lokalizacja sieciowa) będzie używana do aktualizacji lokalizacji (jeśli została wyłączona w sekcji "Ograniczenia", to ustawienie to nie będzie miało żadnego wpływu).
Używanie lokalizacji GPS do aktualizacji lokalizacji	Jeśli jest włączona, GPS będzie używany do aktualizacji lokalizacji

Zezwalaj na fałszywe lokalizacje	Umożliwia fałszowanie informacji o lokalizacji za pośrednictwem aplikacji innych firm.
Akcja Utracone połączenie	Umożliwia ustawienie określonej akcji, która zostanie wykonana po określonej liczbie nieudanych uderzeń serca.
Tryb egzekwowania zasad	Określa, jak agresywnie klient AppTec360 prosi użytkownika o wykonanie pewnych czynności, które wymagają wprowadzenia danych przez użytkownika. Interval (Domyślnie) = pytaj w odstępach czasu, aby użytkownik mógł umieścić to w tle na jakiś czas. Brak alertu = brak wyskakującego okienka dla wymaganej interakcji. Musisz ręcznie otworzyć klienta AppTec360, aby sprawdzić, czy jest wymagane działanie Stały alert = użytkownik może wykonać tylko wymaganą akcję. Klient AppTec360 wymusi działanie na pierwszym planie, jeśli użytkownik będzie próbował tego uniknąć.
Blokada wersji AppTec360	Pozwala zdefiniować wersję klienta AppTec360, która jest maksymalną wersją, do której klient się aktualizuje.

Tapeta

Tutaj można zdefiniować niestandardową tapetę.

"Określ kolor" umożliwia zdefiniowanie koloru w formacie szesnastkowym (np. #000000). Dozwolone są tylko wartości szesnastkowe.

"Ustaw obraz jako tapetę" umożliwia przesłanie obrazu. Należy pamiętać, że różne urządzenia z różnymi programami uruchamiającymi i wersjami systemu operacyjnego działają inaczej. Nie ma ogólnych wytycznych dotyczących rozmiaru i proporcji, ponieważ zależy to od urządzenia.

Format pliku to JPG (lub JPEG) lub PNG.

Zarządzanie zasobami (tylko na poziomie urządzenia)

Zarządzanie aktywami

Informacje o urządzeniu

Model	Oznaczenie modelu urządzenia
System operacyjny	OS
Wersja systemu operacyjnego	Wersja systemu operacyjnego
Wsparcie AE	Wsparcie dla systemu Android Enterprise (kontener i pełne zarządzanie)
Numer seryjny	Numer seryjny
Nazwa urządzenia	Nazwa urządzenia
Stan akumulatora	Stan akumulatora
Pamięć wolna / całkowita	Pamięć wolna / całkowita
Samsung KNOX	Poziom API Samsung KNOX
Dostępna karta SD	Dostępna karta SD
Emulowana karta SD	Emulowana karta SD
Wyjmowana karta SD	Wyjmowana karta SD
SD Free / Pamięć całkowita	Wolna pamięć SD / całkowita pamięć karty SD

Wi-Fi

Adres IP	Adres IP urządzenia
WiFi MAC	Adres MAC sieci Wi-Fi

Komórkowy

Status	Status (zainstalowana karta SIM)
Numer telefonu	Numer telefonu
Roaming (połączenia głosowe / transmisja danych)	Roaming dla połączeń głosowych / transmisji danych
Status roamingu	Bieżący status roamingu
Adres IP	Adres IP
Operator/Przewoźnik	Operator/Przewoźnik
Technologia komórkowa	Technologia komórkowa
IMEI	Numer IMEI
ICCID	Jest to identyfikator karty SIM, często również karty Smartcard lub Integrated Circuit Card (ICC).
IMSI	International Mobile Subscriber Identity (IMSI) zapewnia w sieciach GSM i UMTS jednoznaczną identyfikację użytkowników sieci. IMSI składa się z maksymalnie 15 cyfr i jest konfigurowany w następujący sposób: • Kod kraju sieci komórkowej (MCC), 3 cyfry • Kod sieci komórkowej (MNC), 2 lub 3 cyfry • Numer identyfikacyjny abonenta sieci komórkowej (MSIN), 1-10 cyfr
Obecny MCC/MNC	Patrz "SIM MCC/MNC"
SIM MCC/MNC	Kod kraju sieci komórkowej to ustalony identyfikator kraju, określony przez ITU zgodnie ze standardem E.212. Działa on w połączeniu z kodem sieci komórkowej (MNC) w celu identyfikacji sieci komórkowej. Oznacza kod kraju/sieci komórkowej karty SIM. Jeśli korzystasz z roamingu w innej sieci komórkowej, logicznie rzecz biorąc, "Bieżące MCC/MNC" i "SIM MCC/MNC" będą się różnić.

Bluetooth

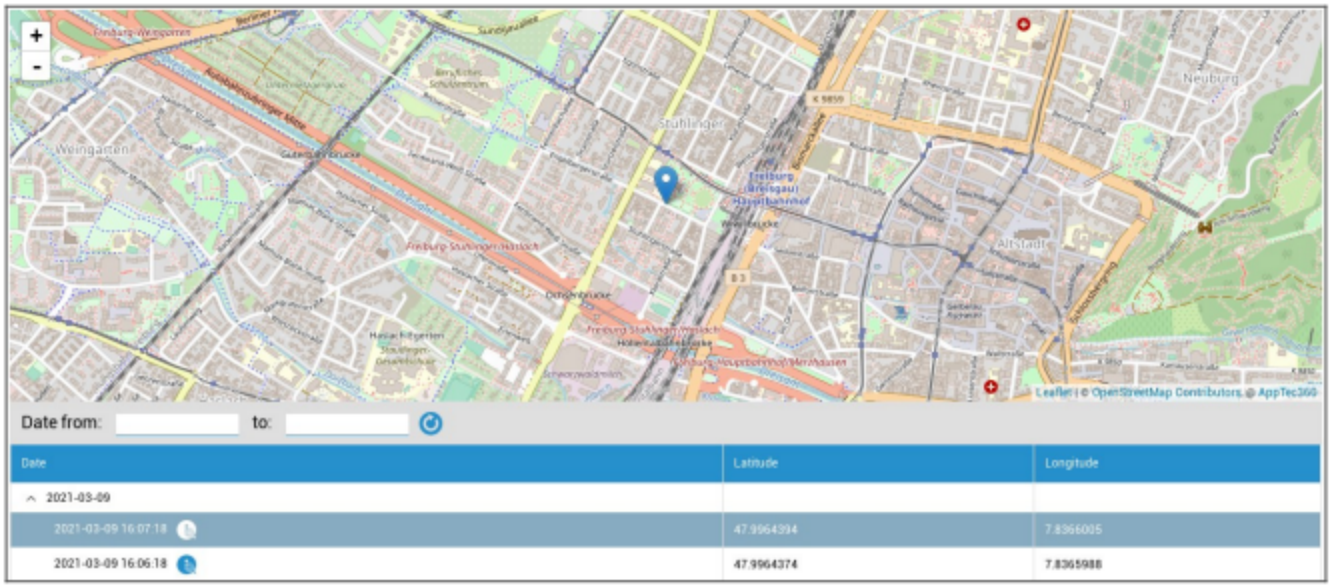
Bluetooth MAC	Adres MAC Bluetooth

Zarządzanie bezpieczeństwem

Ochrona przed kradzieżą (tylko na poziomie urządzenia)

Informacje GPS (tylko na poziomie urządzenia)

Tutaj można ustalić bieżącą/ostatnią lokalizację urządzenia. Lokalizacja może być chroniona jednym lub nawet dwoma hasłami - patrz: Ustawienia ogólne - Prywatność - Dostęp GPS



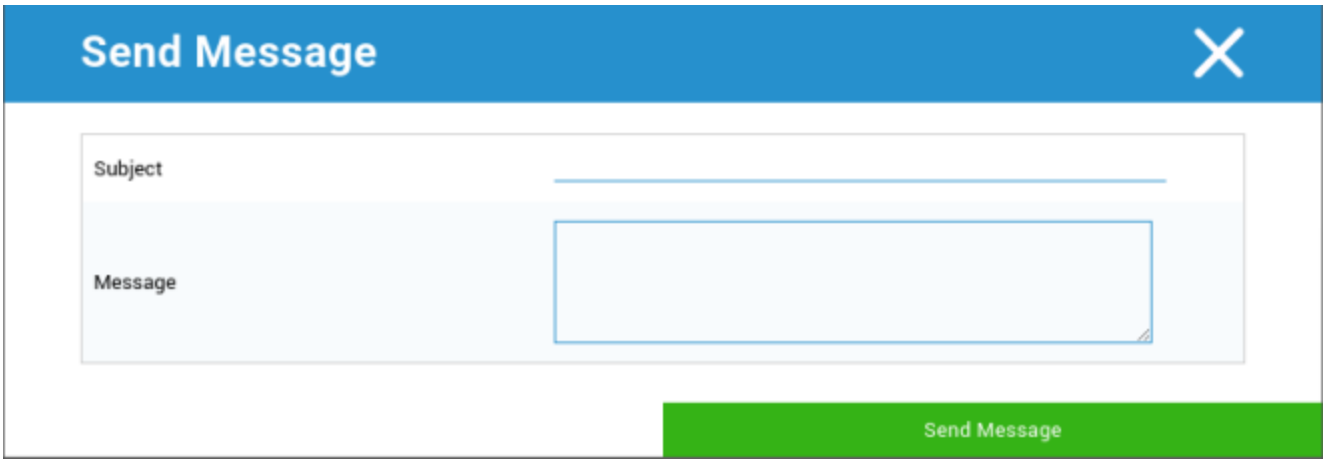
Wipe & Lock (tylko na poziomie urządzenia)

W sekcji "Wyczyść i zablokuj" można wykonać następujące trzy czynności:

Pełne wytarcie	Urządzenie jest przywracane do ustawień fabrycznych (dane firmowe i osobiste są usuwane).
Enterprise Wipe	Z urządzenia użytkownika końcowego usuwane są wyłącznie dane firmowe (wszystkie aplikacje, dane itp. dostarczone przez AppTec360).
Ekran blokady	Blokada ekranu jest aktywna, wystarczy odblokować urządzenie za pomocą hasła / kodu PIN urządzenia.

Wiadomość (tylko na poziomie urządzenia)

Możesz wpisać temat i wiadomość, a następnie wysłać ją do urządzenia użytkownika końcowego. Wiadomość ta zostanie wyświetlona w AppTec360 Client.



Konfiguracja zabezpieczeń

Kod dostępu

W sekcji "Kod dostępu" można ustawić hasło urządzenia, dostępne są następujące opcje ustawień

Minimalna długość hasła	Ustala minimalną liczbę symboli, które musi zawierać hasło
Jakość hasła	Siła hasła Nieokreślony = nieokreślony Każde hasło jest w porządku = każde hasło jest akceptowalne co najmniej znaki numeryczne = musi zawierać co najmniej znaki numeryczne co najmniej złożone znaki = musi zawierać co najmniej znaki specjalne co najmniej znaki alfanumeryczne = musi zawierać co najmniej znaki alfanumeryczne co najmniej znaki alfabetu = musi zawierać co najmniej znaki alfabetu
Maksymalna blokada czasu nieaktywności	Maksymalny limit czasu ekranu. Konfiguruje tylko maksymalną wartość, którą może wybrać użytkownik.
Minimalne małe litery wymagane w haśle	Minimalne małe litery wymagane w haśle
Minimalne wielkie litery wymagane w haśle	Minimalne wielkie litery wymagane w haśle
Minimalna liczba znaków nieliterowych wymaganych w haśle	Minimalna liczba znaków nieliterowych wymaganych w haśle
Minimalne cyfry wymagane w haśle	Minimalne cyfry wymagane w haśle
Minimalne symbole wymagane w haśle	Minimalne symbole wymagane w haśle
Limit czasu wygaśnięcia hasła	Ustala, po jakim czasie hasło wygasa i musi zostać wydane nowe hasło.
Ograniczenie historii haseł	Liczba poprzednio używanych haseł, które nie są dozwolone
Maksymalna liczba nieudanych prób podania hasła	Ustala, jak często hasło może być wprowadzane niepoprawnie, zanim zostanie wykonane całkowite czyszczenie urządzenia.

Szyfrowanie

W tym miejscu można zaszyfrować pamięć wewnętrzną urządzenia, a także pamięć karty SD.

Wymagaj szyfrowania pamięci masowej	Jeśli to ustawienie jest aktywne, pamięć urządzenia będzie szyfrowana, o ile urządzenie obsługuje tę funkcję. Po zaszyfrowaniu pamięci urządzenia po raz pierwszy nie jest już możliwe jej odszyfrowanie. Podobnie zasady dotyczące haseł zostaną automatycznie przełączone na 6 symboli alfanumerycznych
Wymagaj szyfrowania karty SD	To ustawienie dotyczy tylko urządzeń Samsung! Jeśli to ustawienie jest włączone, zewnętrzna karta SD może być zaszyfrowana i można ją ręcznie odszyfrować tylko na urządzeniu użytkownika końcowego. Podobnie zasady dotyczące haseł zostaną automatycznie przełączone na 6 symboli alfanumerycznych

Antywirus

Włączenie antywirusa spowoduje zainstalowanie aplikacji Ikarus na urządzeniach. Należy pamiętać, że wymaga to osobnej licencji, którą można wprowadzić w Ustawieniach ogólnych → Zarządzanie aplikacjami → Aplikacje innych firm.

Automatyczne skanowanie	Określa, czy Ikarus skanuje automatycznie i jak często to robi. Włączenie opcji "Pełne skanowanie automatyczne" spowoduje wykonanie pełnego skanowania. W przeciwnym razie zostanie przeprowadzone szybkie skanowanie
Automatyczne aktualizacje	Włącza automatyczne aktualizacje bazy danych wirusów i ustawia ich częstotliwość.
Ochrona aplikacji	Umożliwia skanowanie aplikacji oprócz zwykłego skanowania, które skanuje tylko pliki.
Ochrona karty SD	Włącza ochronę karty SD. Bez tej funkcji skanowanie jest ograniczone do lokalnej pamięci masowej
Aktualizacja tylko przez Wi-Fi	Ograniczenia aktualizacji do Wi-Fi

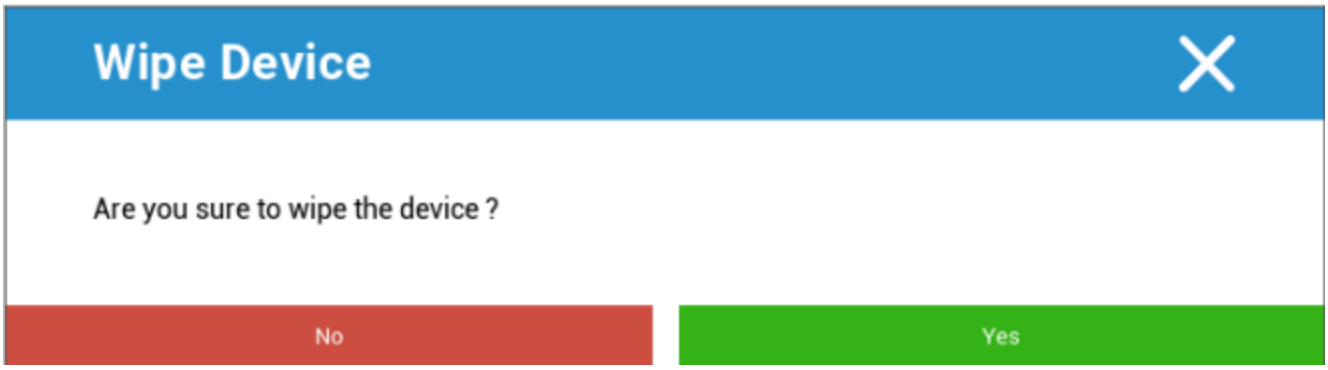
Koniec życia (tylko na poziomie urządzenia)

Wipe (tylko na poziomie urządzenia)

W sekcji "Wipe" można przywrócić urządzenie do ustawień fabrycznych. W tym przypadku dane firmowe i prywatne zostaną usunięte z urządzenia użytkownika końcowego.

Po kliknięciu na "Symbol minus" powinieneś otrzymać następujący komunikat

Wyczyścić również kartę SD?	Pamięć karty SD również zostanie usunięta



Po wybraniu opcji "Tak" można wykonać czyszczenie.

W sekcji "Wipe Report" można wyświetlić następujące elementy

Wymazane przez	Historia tego, kto wykonał czyszczenie
Data	Data
Status	Status (np. czy czyszczenie zostało wykonane pomyślnie)

Ustawienia ograniczeń

Ograniczenia

Tutaj różne rzeczy mogą być ograniczane i blokowane.

Włącz kamerę	Zezwalaj na korzystanie z kamery
Wymuś automatyczną synchronizację	Dotyczy interfejsu "Synchronizacja" On = synchronizacja jest włączona na stałe Off = synchronizacja jest trwale wyłączona Wybór użytkownika = wybrany przez użytkownika
Force Bluetooth	On = Bluetooth jest włączony na stałe Off = Bluetooth jest trwale wyłączony Wybór użytkownika = wybrany przez użytkownika
Force GPS	On = GPS jest włączony na stałe Off = GPS jest trwale wyłączony Wybór użytkownika = wybrany przez użytkownika
Wymuś dokładność lokalizacji Google	On = stała lokalizacja internetowa Wył = trwała dezaktywacja lokalizacji internetowej Wybór użytkownika = wybrany przez użytkownika

W przypadku urządzeń Samsung z interfejsem KNOX 1.0 lub nowszym dostępne są następujące opcje ustawień.

Zezwól na kartę SD	Zezwól na kartę SD
Zezwalaj na zapis na karcie SD	Zezwól na "zapis" na karcie SD
Zezwalaj na przechwytywanie ekranu	Zezwalaj na przechwytywanie ekranu
Zezwalaj na schowek	Zezwalaj na schowek
Tworzenie kopii zapasowych ustawień i danych aplikacji w Google Cloud	Wył. = dezaktywacja usługi Kopia zapasowa Google Włącz = aktywuj Kopię zapasową Google Wybór użytkownika = wybrany przez użytkownika
Zezwalaj na debugowanie USB	Zezwalaj na debugowanie USB (jest używane na przykład do tworzenia dzienników urządzeń (ADB)).
Zezwól na Google Crash Report	Zezwalaj na wysyłanie raportów Google Crash Report z aplikacji
Zezwalaj na przywrócenie ustawień fabrycznych	Umożliwia przywrócenie ustawień fabrycznych urządzenia.
Zezwalaj na aktualizację OTA	Zezwalaj na aktualizacje "Over-The-Air"
Zezwalaj na pamięć USB hosta	Po aktywacji można podłączyć pamięć USB w postaci dysku HD lub czytnika kart SD
Zezwalaj na odtwarzacz multimedialny USB (MTP, PTP)	Zezwalaj na odtwarzacz multimedialny USB (MTP, PTP)
Zezwól na mikrofon	On = zezwalaj na mikrofon dla aplikacji innych firm Off = blokuje mikrofon dla aplikacji innych firm Wybór użytkownika = użytkownicy mogą wybrać, czy aplikacja innej firmy ma dostęp do mikrofonu.
Zezwalaj na komunikację NFC (Near Field Communication)	Zezwalaj na NFC
Zezwalaj na nieznane źródła (boczne ładowanie APK)	Jeśli opcja ta jest włączona, dozwolone jest pobieranie aplikacji (plików APK) z boku. Po wyłączeniu tego ustawienia użytkownik musi włączyć je ręcznie po ponownym zezwoleniu na instalację plików APK z nieznanych źródeł.
Zezwalaj na tworzenie użytkowników	Umożliwia tworzenie wielu użytkowników

Właściciel urządzenia AE

(Urządzenie musi być w trybie właściciela urządzenia Android Enterprise) Zaleca się utworzenie urządzeń jako "Android Enterprise", a nie jako "Android".

Bezpieczeństwo	
Nie zezwalaj na udostępnianie lokalizacji	Określa, czy użytkownik nie może włączyć udostępniania lokalizacji.
Nie zezwalaj na bezpieczny rozruch	Określa, czy użytkownik nie może ponownie uruchomić urządzenia w trybie bezpiecznego rozruchu.
Nie zezwalaj na resetowanie sieci	Określa, czy użytkownik nie może resetować ustawień sieciowych w Ustawieniach.
Nie zezwalaj na przywracanie ustawień fabrycznych	Określa, czy użytkownik nie może resetować urządzenia.
Włącz ADB	Umożliwia połączenie z komputerem PC przez ADB
Wyłącz Keyguard	Wyłącza Keyguard
Właściciel urządzenia Informacje o ekranie blokady	Ustawia informacje o właścicielu urządzenia wyświetlane na ekranie blokady.
Egzekwowanie zgodności	Mode Prompt User - Użytkownik zostanie poproszony o wykonanie niezbędnych czynności. Tryb Lock-Down Container - Ukryj wszystkie aplikacje, dopóki nie zostaną spełnione wszystkie wymagania.

Zarządzanie aplikacjami	
Zezwalaj na łączenie aplikacji między profilami	Umożliwia aplikacjom w profilu nadrzędnym obsługę łączy internetowych z profilu zarządzanego.
Nie zezwalaj na kontrolę aplikacji	Określa, czy użytkownik nie może modyfikować aplikacji w ustawieniach lub programach uruchamiających.
Nie zezwalaj na instalację aplikacji	Określa, czy użytkownik nie może instalować aplikacji.
Nie zezwalaj na odinstalowywanie aplikacji	Określa, czy użytkownik nie może odinstalowywać aplikacji.
Polityka uprawnień środowiska uruchomieniowego	Określa sposób obsługi nowych żądań uprawnień od aplikacji.
Zezwalaj na nieznane źródła	Jeśli opcja ta jest włączona, użytkownicy mogą pobierać aplikacje poprzez instalację pliku .apk.

Łączność	
Nie zezwalaj na konfigurację sieci komórkowej	Określa, czy użytkownik nie może konfigurować sieci komórkowych.
Wyłącz konfigurację tetheringu	Określa, czy użytkownik nie może konfigurować tetheringu i przenośnych hotspotów.
Nie zezwalaj na konfigurację VPN	Określa, czy użytkownik nie może konfigurować sieci VPN.
Nie zezwalaj na konfigurację Wi-Fi	Określa, czy użytkownik nie może zmieniać punktów dostępu WiFi.
Nie zezwalaj na wychodzącą wiązkę NFC	Określa, czy użytkownik nie może używać NFC do przesyłania danych z aplikacji.
Zablokuj konfigurację WiFi	To ustawienie kontroluje, czy konfiguracje WiFi utworzone przez aplikację właściciela urządzenia powinny być zablokowane (tj. edytowalne lub usuwalne tylko przez aplikację właściciela urządzenia, nawet przez aplikację Ustawienia).
Włącz roaming danych	Aktywuje roaming danych

Bluetooth	
Wyłącz Bluetooth	Określa, czy bluetooth jest niedozwolony na urządzeniu. Wymaga systemu Android 8.0
Wyłącz udostępnianie Bluetooth	Określa, czy wychodzące udostępnianie Bluetooth jest niedozwolone na urządzeniu. Wymaga systemu Android 8.0
Wyłącz konfigurację Bluetooth	Określa, czy użytkownik nie może konfigurować bluetooth.

Zarządzanie kontem	
Nie zezwalaj na dodawanie profilu zarządzanego	Określa, czy użytkownik nie może dodawać zarządzanych profili. Wymaga systemu Android 8.0
Nie zezwalaj na dodawanie użytkowników	Określa, czy użytkownik nie może dodawać nowych użytkowników.
Nie zezwalaj na usuwanie profilu zarządzanego	Określa, czy zarządzane profile tego użytkownika mogą być usuwane w inny sposób niż przez właściciela profilu. Wymaga systemu Android 8.0
Nie zezwalaj na modyfikację konta	Określa, czy użytkownik nie może dodawać i usuwać kont, chyba że zostały one dodane programowo przez Authenticator.

Telefonia	
Nie zezwalaj na połączenia wychodzące	Określa, że użytkownik nie może wykonywać wychodzących połączeń telefonicznych.
Nie zezwalaj na SMS-y	Określa, że użytkownik nie może wysyłać ani odbierać wiadomości SMS.

System	
Nie zezwalaj na tworzenie okien	Określa, że okna poza oknami aplikacji nie powinny być tworzone.
Nie zezwalaj na ustawianie ikony użytkownika	Określa, czy użytkownik nie może zmienić swojej ikony.
Nie zezwalaj na ustawianie tapet	Ograniczenie użytkownika uniemożliwiające ustawienie tapety.
Wyłącz pasek stanu	Wyłączenie paska stanu blokuje powiadomienia, szybkie ustawienia i inne nakładki ekranowe, które umożliwiają ucieczkę z urządzenia jednorazowego użytku.
Włącz automatyczny czas	Automatycznie ustawia godzinę.
Włącz automatyczną strefę czasową	Automatycznie ustawia strefę czasową.
Pozostaje włączony po podłączeniu	Urządzenie pozostanie aktywne po podłączeniu do źródła zasilania.

Przechowywanie	
Nie zezwalaj na wyłączanie weryfikacji aplikacji	Określa, czy użytkownik nie może wyłączyć weryfikacji aplikacji.
Nie zezwalaj na montowanie nośników fizycznych	Określa, czy użytkownik nie może montować fizycznych nośników zewnętrznych.
Włącz usługę kopii zapasowej	Usługa kopii zapasowych zarządza wszystkimi mechanizmami tworzenia kopii zapasowych i przywracania danych na urządzeniu. Ustawienie tej opcji na wartość false uniemożliwi tworzenie kopii zapasowych lub przywracanie danych. Usługa kopii zapasowej jest domyślnie wyłączona. Wymaga systemu Android 8.0
Włączanie pamięci masowej USB	Umożliwia korzystanie z pamięci masowej USB.

Klawiatura	
Wyłącz autouzupełnianie	Określa, czy użytkownik nie może korzystać z usług autouzupełniania. Wymaga systemu Android 8.0
Nie zezwalaj na kopiowanie i wklejanie między profilami	Określa, czy zawartość skopiowana do schowka tego profilu może zostać wklejona do powiązanych profili.

Dźwięk	
Nie zezwalaj na korektę głośności	Określa, czy użytkownik nie może regulować głośności głównej.
Wyłącz wyciszenie mikrofonu	Określa, czy użytkownik nie może regulować głośności mikrofonu.
Urządzenie wyciszające	Urządzenie wyciszające.

Zasady aktualizacji systemu	
Kontrola aktualizacji systemu operacyjnego	Włącz tę opcję, aby ustawić zachowanie aktualizacji na automatyczne, okienkowe lub odroczone.

Kontener BYOD

Android Enterprise

Android Enterprise

Włącz system Android Enterprise	Włącz Android Enterprise (AE). AE jest obsługiwany od wersji Android 5.1 i nowszych.
Egzekwowanie zgodności	Mode Prompt User - Użytkownik zostanie poproszony o wykonanie niezbędnych czynności. Tryb Lock-Down Container - Ukryj wszystkie aplikacje, dopóki nie zostaną spełnione wszystkie wymagania.
Polityka uprawnień środowiska uruchomieniowego	Monitowanie użytkownika o nowe żądania uprawnień Zawsze przyznawaj nowe żądania uprawnień Zawsze odrzucaj nowe żądania uprawnień Ostrzeżenie: Niektóre aplikacje mają problemy z rozpoznawaniem uprawnień, jeśli są one ustawione automatycznie. Jeśli zawsze udzielasz uprawnień i napotykasz problemy z aplikacjami informującymi o braku uprawnień, ustaw tę opcję na "monituj użytkownika" i ponownie zainstaluj aplikację
Zezwalaj na schowek wychodzący	Umożliwia kopiowanie i wklejanie z wnętrza kontenera na zewnątrz.
Zezwalaj na rozdzielczość ID dzwoniącego	Wyświetla nazwę połączenia przychodzącego na podstawie kontaktów w kontenerze.
Rozdzielczość wyszukiwania kontaktów	Umożliwia wyszukiwanie nazw w kontenerze kontaktów podczas wykonywania połączeń.
Zezwalaj na udostępnianie kontaktów Bluetooth	Umożliwia dostęp do kontenera kontaktowego w samochodzie
Nie zezwalaj na wychodzącą wiązkę NFC	Wyłącza NFC dla kontenera
Zezwalaj na nieznane źródła	Jeśli opcja ta jest włączona, użytkownicy mogą pobierać aplikacje poprzez instalację pliku .apk.
Zezwalaj na debugowanie USB	Jeśli opcja ta jest włączona, użytkownicy mogą włączyć debugowanie USB.

Nie zezwalaj na modyfikację konta	Zabrania tworzenia, usuwania i modyfikowania kont w kontenerze. Należy pamiętać, że niektóre aplikacje muszą utworzyć lub zmodyfikować konta, aby działały zgodnie z oczekiwaniami

Gmail Exchange

Umożliwia skonfigurowanie Gmaila w kontenerze. Należy pamiętać, że włączenie tej konfiguracji nie powoduje automatycznej instalacji aplikacji. Nadal musisz dodać tę aplikację jako aplikację obowiązkową.

Adres e-mail	Adres e-mail
Nazwa hosta serwera	Nazwa hosta serwera
Nazwa logowania	Nazwa logowania
Podpis	Podpis
Liczba poprzednich dni do synchronizacji	Liczba poprzednich dni do synchronizacji.
Identyfikator urządzenia	Identyfikator EAS. Pozostaw to pole puste, jeśli środowisko tego nie wymaga
Używanie protokołu Secure Sockets Layer (SSL)	Włącza użycie protokołu SSL. Wyłączenie tej opcji może obniżyć poziom bezpieczeństwa
Akceptuj wszystkie certyfikaty	Akceptuje wszystkie certyfikaty. Włączenie tej opcji może obniżyć poziom bezpieczeństwa
Zezwalaj na konta niezarządzane	Umożliwia użytkownikowi dodanie dodatkowych kont
Certyfikat klienta	Prześlij certyfikat klienta, jeśli serwer Exchange tego wymaga.

Aplikacje systemowe AE

Tutaj można włączyć aplikacje systemowe dla Android Enterprise Container. Należy pamiętać, że określona aplikacja musi znajdować się w pamięci masowej systemu, w przeciwnym razie nic się nie stanie.

Kod dostępu do kontenera

Tylko dla systemu Android 7.0 lub nowszego

Umożliwia ustawienie określonego wymogu hasła dla kontenera.

Minimalna długość hasła	Ustala minimalną liczbę symboli, które musi zawierać hasło
Jakość hasła	Siła hasła Nieokreślony = nieokreślony Każde hasło jest w porządku = każde hasło jest akceptowalne co najmniej znaki numeryczne = musi zawierać co najmniej znaki numeryczne co najmniej złożone znaki = musi zawierać co najmniej znaki specjalne co najmniej znaki alfanumeryczne = musi zawierać co najmniej znaki alfanumeryczne co najmniej znaki alfabetu = musi zawierać co najmniej znaki alfabetu
Maksymalna blokada czasu nieaktywności	Maksymalny czas do zablokowania kontenera. Konfiguruje to tylko maksymalną wartość, którą może wybrać użytkownik
Minimalne małe litery wymagane w haśle	Minimalne małe litery wymagane w haśle
Minimalne wielkie litery wymagane w haśle	Minimalne wielkie litery wymagane w haśle
Minimalna liczba znaków nieliterowych wymaganych w haśle	Minimalna liczba znaków nieliterowych wymaganych w haśle
Minimalne cyfry wymagane w haśle	Minimalne cyfry wymagane w haśle
Minimalne symbole wymagane w haśle	Minimalne symbole wymagane w haśle
Limit czasu wygaśnięcia hasła	Ustala, po jakim czasie hasło wygasa i musi zostać wydane nowe hasło.
Ograniczenie historii haseł	Liczba poprzednio używanych haseł, które nie są dozwolone
Maksymalna liczba nieudanych prób podania hasła	Ustala, jak często hasło może być wprowadzane niepoprawnie, zanim kontener zostanie usunięty.

Samsung KNOX

Aktywacja

Tutaj można włączyć Samsung KNOX Container. Należy pamiętać, że nie jest on już obsługiwany przez firmę Samsung w systemie Android 10 lub nowszym. Korzystanie z kontenera Android Enterprise Container w systemie Android 10 lub nowszym

Kod dostępu Knox

Ustanowienie wytycznych dotyczących ustawień hasła urządzenia

Minimalna długość hasła	Ustala, ile symboli musi zawierać hasło
Jakość hasła	Siła hasła Każde hasło jest w porządku = Każde hasło jest w porządku Co najmniej znaki numeryczne = Minimalna liczba znaków numerycznych musi być obecna Co najmniej złożone znaki = Minimalna liczba znaków specjalnych. Co najmniej znaki alfanumeryczne = Minimalna liczba znaków alfanumerycznych musi być obecna. Co najmniej znaki alfabetu = Minimalna liczba znaków alfabetu musi być obecna.
Wymagane minimalne złożone znaki	Muszą być obecne co najmniej złożone znaki
Maksymalny czas bezczynności	Maksymalny czas bezczynności użytkownika przed zablokowaniem klawiatury
Zezwalaj na uwierzytelnianie odciskiem palca	Zezwalaj na uwierzytelnianie odciskiem palca
Zezwalaj na uwierzytelnianie Iris	Zezwalaj na uwierzytelnianie za pomocą rozpoznawania tęczówki
Maksymalny wiek hasła	Ustala, po jakim czasie hasło wygasa i musi zostać wydane nowe hasło.
Historia przechowywanych haseł	Liczba poprzednich haseł, które nie są dozwolone
Maksymalna liczba nieudanych prób podania hasła	Ustala, jak często hasło może być podawane nieprawidłowo, zanim nastąpi całkowite wyczyszczenie urządzenia.

Knox Security

Ograniczenie określonych funkcji urządzenia

Włącz kamerę	Zezwalaj na korzystanie z kamery
Zezwalaj na Samsung KNOX App Store	Zezwalanie na korzystanie z Samsung KNOX App Store
Zezwalaj na usługi Google Play	Zezwalaj na usługi Google Play

Zezwalaj przeglądarce	Zezwalaj na korzystanie z natywnej przeglądarki
Zezwalaj na zrzuty ekranu	Zezwalaj na tworzenie zrzutów ekranu
Zezwalaj na import kontaktów	W przypadku aktywacji, dostęp do kontaktów urządzenia z kontenera KNOX jest dozwolony
Zezwalaj na eksport kontaktów	W przypadku aktywacji, dostęp do kontaktów KNOX z urządzenia jest dozwolony
Zezwalaj na import kalendarza	W przypadku aktywacji, dostęp do kalendarza urządzenia z kontenera KNOX jest dozwolony
Zezwalaj na eksport kalendarza	W przypadku aktywacji, dostęp do kalendarza KNOX z urządzenia jest dozwolony
Zezwalaj na niezabezpieczoną klawiaturę	Zezwalaj na używanie niezabezpieczonej klawiatury
Włącz import plików	Włącz import plików do kontenera KNOX
Włącz eksport plików	Włącz eksport plików z kontenera KNOX

Knox Exchange

Tutaj można skonfigurować Exchange-Profile dla kontenera KNOX.

Adres e-mail	Podany adres e-mail użytkownika Zwróć uwagę na "symbole zastępcze", których możesz użyć do pracy z poświadczeniami i nie wprowadzaj zmian ręcznie na każdym urządzeniu. Po kliknięciu na **Pokaż symbole zastępcze** możesz je wyświetlić dla siebie
Nazwa hosta serwera	Adres serwera serwerów Exchange
Nazwa logowania	Nazwa logowania dla danego urządzenia użytkownika końcowego, należy również zwrócić uwagę na "symbole zastępcze".
Domena	Adres domeny
Hasło (tylko na poziomie urządzenia)	Opcjonalnie indywidualne urządzenie może otrzymać hasło, jeśli pozostanie ono puste, użytkownik zostanie poproszony o wprowadzenie hasła Exchange.
Liczba poprzednich dni do synchronizacji	Liczba dni określająca, kiedy wiadomości e-mail są synchronizowane z powrotem
Podpis	Można dołączyć podpis
Konto domyślne	Ustala, że to konto e-mail jest kontem standardowym
Używanie protokołu Secure Sockets Layer (SSL)	Użyj połączenia SSL
Używanie protokołu TLS (Transport Layer Security)	Użyj połączenia TLS
Akceptuj wszystkie certyfikaty	Akceptowane są wszystkie certyfikaty. Wybierz tę opcję, jeśli serwer Exchange korzysta z certyfikatu z podpisem własnym

Knox eMail

Adres e-mail	Podany adres e-mail użytkownika Zwróć uwagę na "symbole zastępcze", których możesz użyć do pracy z poświadczeniami i nie wprowadzaj zmian ręcznie na każdym urządzeniu. Po kliknięciu na **Pokaż symbole zastępcze** możesz je wyświetlić dla siebie
Protokół serwera przychodzącego	Protokół serwera przychodzącego IMAP lub POP
Adres serwera przychodzącego	Adres serwera przychodzącego
Port serwera przychodzącego	Port serwera przychodzącego
Login/nazwa użytkownika serwera przychodzącego	Login/nazwa użytkownika serwera przychodzącego
Hasło serwera przychodzącego	Hasło serwera przychodzącego
Serwer przychodzący używa protokołu SSL	Serwer przychodzący używa protokołu SSL
Serwer przychodzący używa protokołu TLS	Serwer przychodzący używa protokołu TLS
Serwer przychodzący akceptuje wszystkie certyfikaty	Serwer przychodzący akceptuje wszystkie typy certyfikatów
Protokół serwera wychodzącego	Protokół serwera wychodzącego SMTP
Port serwera wychodzącego	Port serwera wychodzącego
Serwer wychodzący używa dodatkowych poświadczeń	Dodatkowe poświadczenia dla serwera wychodzącego. Jeśli ta opcja jest ustawiona na "wył.", zostaną użyte ustawienia serwera przychodzącego.
Login/nazwa użytkownika serwera wychodzącego	Login/nazwa użytkownika serwera wychodzącego
Hasło serwera wychodzącego	Hasło serwera wychodzącego
Serwer wychodzący używa protokołu SSL	Serwer wychodzący używa protokołu SSL
Serwer wychodzący używa protokołu TLS	Serwer wychodzący używa protokołu TLS
Serwer wychodzący akceptuje wszystkie certyfikaty	Serwer wychodzący akceptuje wszystkie typy certyfikatów

Podpis	Tutaj można dołączyć podpis
Powiadomienie użytkownika o otrzymaniu nowej wiadomości e-mail	Powiadomienie użytkownika o otrzymaniu nowej wiadomości e-mail

Knox Apps

Utwórz tutaj aplikacje, które chcesz dystrybuować do urządzeń użytkowników końcowych. Będą one następnie dostępne w KNOX-Container. Aby dodać aplikację, postępuj tak samo jak w menu Aplikacje obowiązkowe

Nazwa aplikacji	Nazwa aplikacji
Obowiązkowe od	Punkt w czasie, kiedy aplikacja została dodana
Źródło	Źródło aplikacji (Sklep Play | Własne)

Kliknięcie symbolu umożliwia ponowne usunięcie danej aplikacji

Zarządzanie połączeniami

Wifi

W przypadku tego ustawienia należy przeprowadzić wstępną konfigurację urządzeń użytkownika końcowego w celu uzyskania dostępu do wewnętrznych punktów dostępowych

Identyfikator zestawu usług (SSID)	SSID dla sieci, która ma być połączona
Ukryta sieć	Aktywuj, jeśli punkt dostępowy nie rozgłasza identyfikatora SSID
Typ zabezpieczenia	Ustalenie typu zabezpieczeń punktu dostępowego

Typ zabezpieczenia

WEP

Hasło	Hasło do punktu dostępowego

WPA/WPA2

Hasło	Hasło do punktu dostępowego

802.1x EAP

Metoda EAP	

PWD	Tożsamość	Tożsamość
	Hasło	Hasło

PEAP	Protokół uwierzytelniania fazy 2	brak	Brak dodatkowego protokołu
		MSCHAPV2	Protokół MSCHAPV2
		GTC	Protokół GTC
	Certyfikat CA	Certyfikat CA	
	Tożsamość	Tożsamość	
	Anonimowa tożsamość	Anonimowa tożsamość	
	Hasło	Hasło	

Metoda EAP	

TTLS	Protokół uwierzytelniania fazy 2	brak	Brak dodatkowego protokołu
		PAP	Protokół PAP
		MSCHAP	Protokół MSCHAP
		MSCHAPV2	Protokół MSCHAPV2
		GTC	Protokół GTC
	Certyfikat CA	Certyfikat CA	
	Tożsamość	Tożsamość	
	Anonimowa tożsamość	Anonimowa tożsamość	
	Hasło	Hasło	

TLS	Certyfikat CA	Certyfikat CA
	Tożsamość	Tożsamość
	Hasło	Hasło

VPN

Typ połączenia	**Ustanowienie typu połączenia VPN**

Jeśli wybierzesz "Per-App VPN" jako typ VPN, dostępne klienty VPN ulegną zmianie. Per-App VPN ogranicza VPN do określonych aplikacji i uruchamia połączenie VPN automatycznie po uruchomieniu określonej aplikacji.

Klient VPN AppTec360	Wykorzystuje AppTec360 VPN Client w połączeniu z Universal Gateway.
Nazwa połączenia	Nazwa połączenia VPN
Konfiguracja bramy	Wybierz konfigurację VPN bramy uniwersalnej
Zawsze włączona sieć VPN	Wymusza, aby VPN był zawsze aktywny, więc cały ruch przechodzi przez VPN.
Włącz blokadę natywną	Blokuje wszystkie połączenia sieciowe, gdy urządzenie nie jest podłączone do sieci VPN. Należy używać tej opcji ostrożnie, ponieważ może ona spowodować całkowitą utratę połączenia, jeśli nie zostanie prawidłowo skonfigurowana. Tylko dla Android Enterprise z systemem Android 7 lub nowszym
Włącz blokadę AppTec360	Blokuje korzystanie ze wszystkich aplikacji do momentu uruchomienia połączenia VPN.

Cisco AnyConnect	
Nazwa połączenia	Nazwa połączenia VPN
Serwer	Adres serwera
Tryb certyfikatu	Wyłączony = dezaktywowany Automatyczny = automatyczny

L2TP (tylko KNOX)	Dostępne tylko na urządzeniach Samsung
Nazwa połączenia	Nazwa połączenia
Serwer	Adres serwera
Włącz L2TP Secret	
Domeny wyszukiwania DNS	Domeny wyszukiwania DNS

Typ połączenia	**Ustanowienie typu połączenia VPN**

PPTP (tylko KNOX)	Dostępne tylko na urządzeniach Samsung
Nazwa połączenia	Nazwa połączenia VPN
Serwer	Adres serwera
Włącz szyfrowanie	Włącz szyfrowanie
Domeny wyszukiwania DNS	Domeny wyszukiwania DNS

L2TP / IPSec PSK (tylko KNOX)	Dostępne tylko na urządzeniach Samsung
Nazwa połączenia	Nazwa połączenia VPN
Serwer	Adres serwera
Klucz wstępny IPSec	Wstępnie udostępniony klucz do uwierzytelniania
Włącz L2TP Secret	
L2TP Secret	
Domeny wyszukiwania DNS	Domeny wyszukiwania DNS

IPSec XAuth PSK (tylko KNOX)	Dostępne tylko na urządzeniach Samsung
Nazwa połączenia	Nazwa połączenia VPN
Serwer	Adres serwera
Identyfikator IPSec	Nazwa użytkownika dla połączenia
Klucz wstępny IPSec	Hasło do połączenia
Domeny wyszukiwania DNS	Domeny wyszukiwania DNS

OpenVPN	

Nazwa połączenia	Nazwa połączenia
Profil OpenVPN	Tutaj zostanie skopiowana zawartość pliku .ovpn
Aplikacja OpenVPN	Istnieją dwie różne aplikacje do korzystania z OpenVPN Polecamy aplikację "OpenVPN for Android". Alternatywnie można jednak użyć aplikacji "OpenVPN Connect"

Ograniczenia

Tutaj można ustawić ograniczenia związane z zarządzaniem połączeniami.

Zezwalaj na transmisję danych w roamingu	Zezwalaj na transmisję danych w roamingu
Wymuś roaming danych	W przypadku aktywacji roaming danych mobilnych jest włączony na stałe (niezalecane!). To ustawienie zastępuje ustawienie "Zezwalaj na transmisję danych w roamingu"!
Następujące ustawienia są dostępne tylko w Samsung KNOX 2.0 lub nowszym	
Zezwalaj tylko na połączenia alarmowe	Zezwalaj tylko na połączenia alarmowe
Zezwalaj na WiFi	Zezwalaj na WiFi
Minimalny poziom bezpieczeństwa sieci Wi-Fi	Minimalny poziom bezpieczeństwa sieci WiFi Otwarte = wszystkie rodzaje WiFi są dozwolone
Zabronić użytkownikowi dodawania sieci WiFi	Użytkownik nie może samodzielnie dodać sieci Wi-Fi To ustawienie jest możliwe tylko wtedy, gdy profil WiFi został zdefiniowany w sekcji "Zarządzanie połączeniami".
Zezwalaj na wiadomości SMS i MMS	Wszystkie = cały ruch SMS i MMS jest dozwolony Tylko przychodzące wiadomości SMS = dozwolone są tylko przychodzące wiadomości SMS. Tylko wychodzące wiadomości SMS = dozwolone są tylko wychodzące wiadomości SMS. Brak = ruch SMS / MMS nie jest dozwolony
Zezwalaj na synchronizację w roamingu	Zezwalaj na synchronizację w roamingu Włączony = aktywowany Wyłączone = dezaktywowane Wybór użytkownika = wybór użytkownika
Zezwalaj na roaming głosowy	Zezwalaj na roaming głosowy Włączony = aktywowany Wyłączone = dezaktywowane Wybór użytkownika = wybór użytkownika
Użyj systemowego serwera proxy http	Korzystanie z serwera proxy HTTP, który jest dostępny w ustawieniach systemu, zależy od podłączonej sieci (WiFi lub APN)

APN

Poniższe ustawienia są dostępne tylko w Samsung SAFE 2.0 lub nowszym!

Wyświetlana nazwa APN	Wyświetlana nazwa APN	
Nazwa punktu dostępu	Nazwa APN	
Protokół serwera wychodzącego	Nie ustawiono	
	Brak	
	PAP	Protokół PAP
	CHAP	Protokół CHAP
	PAP lub CHAP	Protokół PAP lub CHAP
MCC - kod kraju sieci komórkowej	W tym miejscu wprowadzany jest MCC, pozostaw to pole puste, jeśli ma być używany MCC włożonej karty SIM.	
MNC - kod sieci komórkowej	W tym miejscu wprowadzany jest MNC, pozostaw to pole puste, jeśli ma być używany MCC włożonej karty SIM	
Adres serwera	Adres serwera	
Numer portu serwera	Numer portu serwera	
Adres serwera proxy	Adres serwera proxy	
Adres serwera MMS	Adres serwera MMS, w przypadku wersji Standard pozostaw puste miejsce	
Numer portu MMS	Numer portu MMS	
Adres proxy MMS	Adres proxy MMS	
Nazwa użytkownika	Nazwa użytkownika	
Hasło	Hasło	
Typ punktu dostępu	Dozwolone typy to: "default", "mms", "supl" Jeśli to pole pozostanie puste, użyty zostanie typ "default,supl,mms".	
Preferowany APN	APN jest preferowany	

Bluetooth

W tym miejscu można dokonać różnych ustawień Bluetooth.

Poniższe ustawienia są dostępne tylko w Samsung KNOX 1.0 lub nowszym!

Zezwalaj na wykrywanie urządzeń przez Bluetooth	Zezwalaj na wykrywanie urządzeń przez Bluetooth
Zezwalaj na parowanie Bluetooth	Zezwalaj na parowanie Bluetooth
Zezwalaj na korzystanie z zestawów słuchawkowych Bluetooth	Zezwalaj na korzystanie z zestawów słuchawkowych Bluetooth
Zezwalaj na korzystanie z urządzeń głośnomówiących Bluetooth	Zezwalaj na korzystanie z urządzeń głośnomówiących Bluetooth
Zezwalaj na urządzenia Bluetooth A2DP	Zezwalaj na strumieniowe przesyłanie dźwięku Bluetooth A2DP między urządzeniami
Zezwalaj na połączenia wychodzące	Zezwalaj na połączenia wychodzące przez BT
Zezwalaj na przesyłanie danych przez Bluetooth	Zezwalaj na przesyłanie danych przez Bluetooth
Zezwalaj na tethering Bluetooth	Umożliwia korzystanie z urządzenia jako modemu (połączenie internetowe Bluetooth).
Zezwalaj na połączenie z komputerem przez Bluetooth	Zezwalaj na połączenie z komputerem przez Bluetooth

Zarządzanie PIM

Wymiana

Dostępne tylko dla Samsung KNOX w wersji 1.0 lub wyższej!

Adres e-mail	Podany adres e-mail użytkownika Zwróć uwagę na "symbole zastępcze", których możesz użyć do pracy z poświadczeniami i nie wprowadzaj zmian ręcznie na każdym urządzeniu. Kliknięcie przycisku **Pokaż symbole zastępcze** pozwala wyświetlić je dla siebie
Nazwa hosta serwera	Adres serwera serwerów Exchange
Nazwa logowania	Nazwa logowania dla danego urządzenia użytkownika końcowego, należy również zwrócić uwagę na "symbole zastępcze tutaj
Domena	Adres domeny
Hasło (tylko na poziomie urządzenia)	Opcjonalnie, indywidualne urządzenie może otrzymać hasło, jeśli pozostanie ono puste, użytkownik zostanie poproszony o wprowadzenie swojego hasła Exchange.
Liczba poprzednich dni do synchronizacji	Liczba dni określająca, kiedy wiadomości e-mail są synchronizowane z powrotem
Podpis	Można dołączyć podpis (wskazówka: niektóre urządzenia wymagają formatowania HTML dla podpisu).
Konto domyślne	Ustala, że to konto pocztowe jest kontem standardowym
Używanie protokołu Secure Sockets Layer (SSL)	Użyj połączenia SSL
Używanie protokołu TLS (Transport Layer Security)	Użyj połączenia TLS
Akceptuj wszystkie certyfikaty	Akceptowane są wszystkie certyfikaty. Wybierz tę opcję, jeśli serwer Exchange korzysta z certyfikatu z podpisem własnym

eMail

Tutaj można dystrybuować konta IMAP i POP do odpowiednich urządzeń użytkowników końcowych.

Poniższe ustawienia są dostępne tylko w Samsung KNOX 1.0 lub nowszym!		
Adres e-mail	Podany adres e-mail użytkownika Zwróć uwagę na "symbole zastępcze", których możesz użyć do pracy z poświadczeniami i nie wprowadzaj zmian ręcznie na każdym urządzeniu. Po kliknięciu na **Pokaż symbole zastępcze** możesz je wyświetlić dla siebie	
Protokół serwera przychodzącego	Protokół serwera przychodzącego	IMAP lub POP
Adres serwera przychodzącego	Adres serwera przychodzącego	
Port serwera przychodzącego	Port serwera przychodzącego	
Login/nazwa użytkownika serwera przychodzącego	Login/nazwa użytkownika serwera przychodzącego	
Hasło serwera przychodzącego (tylko na poziomie urządzenia)	Hasło serwera przychodzącego (tylko na poziomie urządzenia)	
Serwer przychodzący używa protokołu SSL	Serwer przychodzący używa protokołu SSL	
Serwer przychodzący używa protokołu TLS	Serwer przychodzący używa protokołu TLS	
Serwer przychodzący akceptuje wszystkie certyfikaty	Serwer przychodzący akceptuje wszystkie typy certyfikatów	
Protokół serwera wychodzącego	Protokół serwera wychodzącego	SMTP
Port serwera wychodzącego	Port serwera wychodzącego	
Serwer wychodzący używa dodatkowych poświadczeń	Dodatkowe poświadczenia dla serwera wychodzącego. Jeśli ta opcja jest ustawiona na "wył.", zostaną użyte ustawienia serwera przychodzącego.	
Login/nazwa użytkownika serwera wychodzącego	Login/nazwa użytkownika serwera wychodzącego	
Hasło serwera wychodzącego (tylko na poziomie urządzenia)	Hasło serwera wychodzącego	
Serwer wychodzący używa protokołu SSL	Serwer wychodzący używa protokołu SSL	

Serwer wychodzący używa protokołu TLS	Serwer wychodzący używa protokołu TLS
Serwer wychodzący akceptuje wszystkie certyfikaty	Serwer wychodzący akceptuje wszystkie typy certyfikatów
Podpis	Podpis można załączyć tutaj (Wskazówka: niektóre urządzenia wymagają formatowania HTML dla podpisu).
Powiadomienie użytkownika o otrzymaniu nowej wiadomości e-mail	Powiadamia użytkownika o otrzymaniu nowej wiadomości e-mail

AE Gmail Exchange

Informacje: Ta konfiguracja zostanie zastosowana do aplikacji Gmail. Musisz więc zatwierdzić i zainstalować Gmaila.

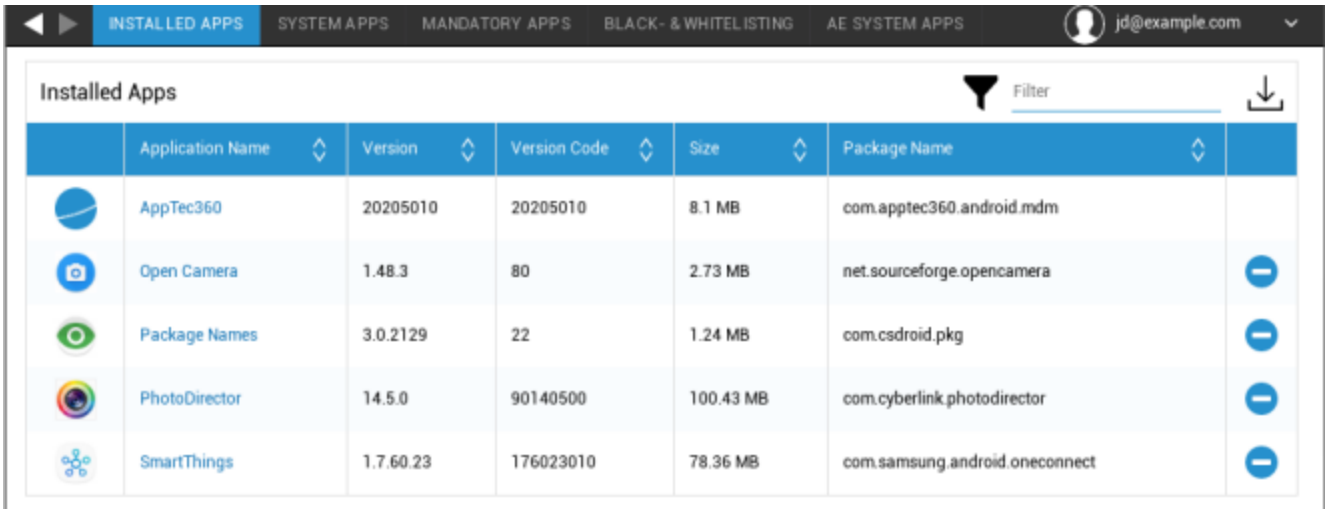
Adres e-mail	Podany adres e-mail użytkownika Zwróć uwagę na "symbole zastępcze", których możesz użyć do pracy z poświadczeniami i nie wprowadzaj zmian ręcznie na każdym urządzeniu. Po kliknięciu na Pokaż symbole zastępcze możesz je wyświetlić dla siebie
Nazwa hosta serwera	Adres serwera serwerów Exchange
Nazwa logowania	Nazwa logowania dla danego urządzenia użytkownika końcowego, należy również zwrócić uwagę na "symbole zastępcze tutaj
Podpis	Można dołączyć podpis (wskazówka: niektóre urządzenia wymagają formatowania HTML dla podpisu).
Liczba poprzednich dni do synchronizacji	Liczba dni określająca, kiedy wiadomości e-mail są synchronizowane z powrotem
Identyfikator urządzenia	Identyfikator EAS. Pozostaw to pole puste, jeśli środowisko tego nie wymaga
Używanie protokołu Secure Sockets Layer (SSL)	Użyj połączenia SSL
Akceptuj wszystkie certyfikaty	Akceptowane są wszystkie certyfikaty. Wybierz tę opcję, jeśli serwer Exchange korzysta z certyfikatu z podpisem własnym
Zezwalaj na konta niezarządzane	Umożliwia użytkownikowi dodanie dodatkowych kont
Certyfikat klienta	Prześlij certyfikat klienta, jeśli serwer Exchange tego wymaga.

Zarządzanie aplikacjami

Menedżer aplikacji dla przedsiębiorstw

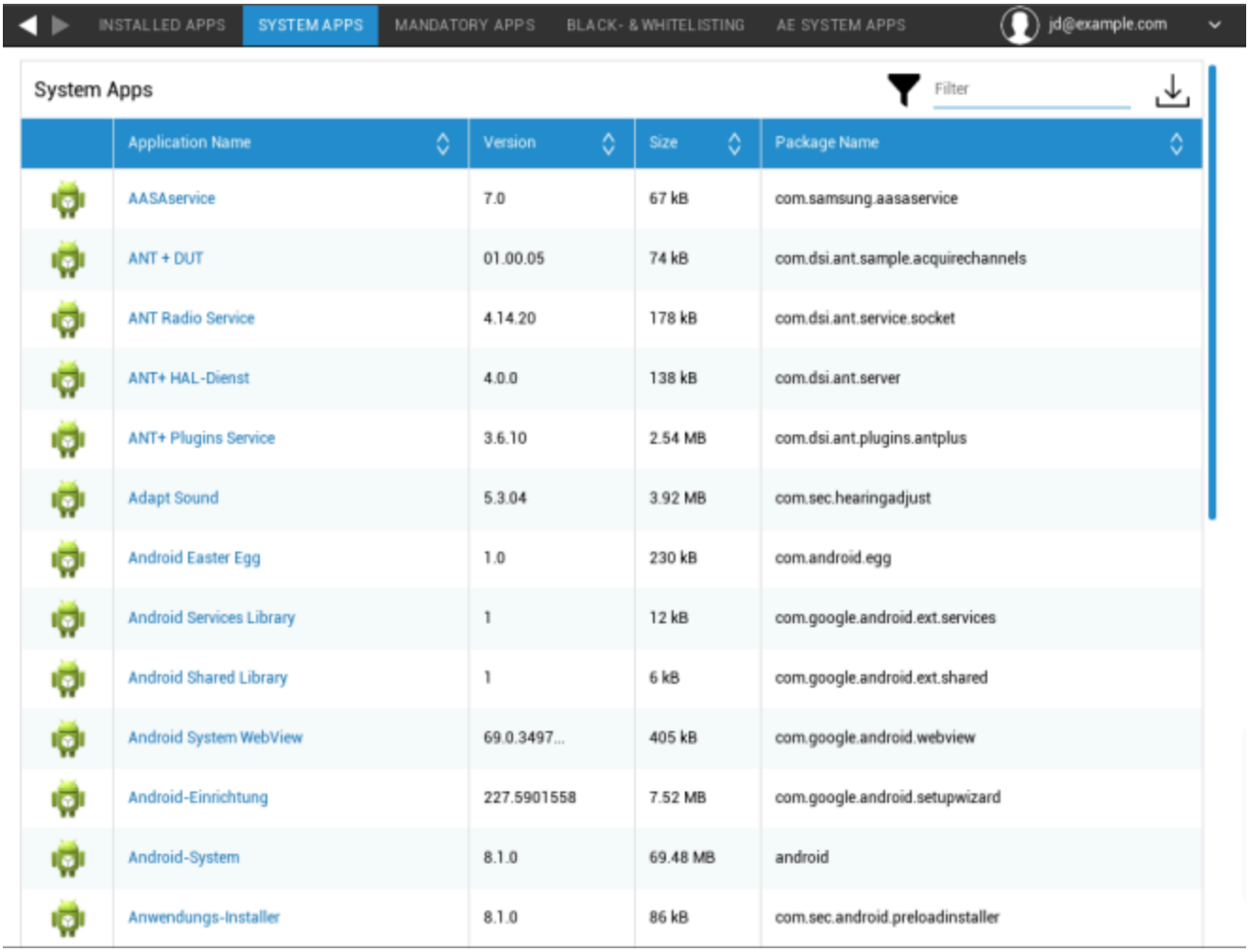
Zainstalowane aplikacje (tylko na poziomie urządzenia)

Tutaj zostaną wyświetlone wszystkie aplikacje, które są obecnie zainstalowane na urządzeniu użytkownika końcowego.


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

Aplikacje systemowe (tylko na poziomie urządzenia)

W sekcji "Aplikacje systemowe" wszystkie preinstalowane aplikacje systemowe zostaną wyświetlone wraz z nazwą i wersją pakietu.



Aplikacje obowiązkowe

W sekcji Aplikacje obowiązkowe można określić, które aplikacje muszą być zainstalowane na urządzeniu. W zależności od konfiguracji i urządzenia aplikacja zostanie zainstalowana automatycznie lub użytkownik zostanie poproszony o jej zainstalowanie.

Należy pamiętać, że zaleca się korzystanie z Android Enterprise w celu łatwego zarządzania aplikacjami.

Scenariusze są wymienione poniżej:

Zwykłe aplikacje ze Sklepu Play

Instalacje aplikacji w sklepie Playstore zawsze wymagają interakcji użytkownika. Dodatkowo na urządzeniu musi być skonfigurowane konto Google.

Wewnętrzna instalacja aplikacji

Na urządzeniach Samsung aplikacje te zostaną zainstalowane po cichu. Jedynym wyjątkiem jest kontener, w którym użytkownik musi potwierdzić instalację.

W każdym innym przypadku użytkownik musi potwierdzić instalację aplikacji.

Aplikacje Android Enterprise Play Store

Aplikacje te będą zawsze instalowane po cichu, bez interakcji użytkownika.

Aby dodać obowiązkową aplikację, kliknij "+" i wybierz żądaną aplikację z listy. Należy pamiętać, że nie można instalować aplikacji z karty "Sklep Google Play", jeśli urządzenie jest skonfigurowane z systemem Android Enterprise jako w pełni zarządzane lub jako kontener.

Jeśli korzystasz z systemu Android Enterprise, wybierz aplikacje z sekcji "AE Play Store". Aby udostępnić aplikacje tutaj, potwierdź je w sklepie Google Enterprise Play, przechodząc do Ustawienia ogólne → AE Play Store → Play Store Apps.

Po usunięciu obowiązkowej aplikacji zostanie ona również odinstalowana z urządzenia.

Możesz kliknąć nazwę aplikacji na liście aplikacji obowiązkowych i przejść do zakładki "konfiguracja", aby skonfigurować aplikację. Wymaga to korzystania z Android Enterprise, a aplikacja musi to obsługiwać. Dlatego dostępne opcje zależą od wybranej aplikacji.

Aplikacje systemowe AE

Tutaj można włączyć aplikacje systemowe dla urządzeń Android Enterprise. Należy pamiętać, że określona aplikacja musi znajdować się w pamięci masowej systemu, w przeciwnym razie nic się nie

stanie. 296

Ograniczenia i ustawienia

Czarna i biała lista

Tutaj można zdefiniować czarną lub białą listę. Wszystkie aplikacje na czarnej liście zostaną zablokowane. Wszystkie aplikacje, które nie znajdują się na białej liście, zostaną zablokowane. Pusta czarna lista nie blokuje niczego, a pusta biała lista blokuje wszystko*.

**Wszystkie obowiązkowe aplikacje i aplikacje z Enterprise App Store zostaną automatycznie umieszczone na białej liście. Nie trzeba dodawać ich ręcznie*

Klikając na "+" możesz wyszukać aplikację, którą chcesz dodać do czarnej lub białej listy lub ręcznie wprowadzić nazwę pakietu.

Ograniczenia aplikacji systemowych

W sekcji "Sys App Restrictions" można między innymi zablokować preinstalowane aplikacje i usługi.

Wyłącz przeglądarkę	Wyłącz standardową przeglądarkę
Wyłączanie kalendarza	Wyłącz natywny kalendarz
Wyłącz kalkulator	Wyłączanie kalkulatora
Wyłączanie przeglądarki Chrome	Wyłącz przeglądarkę Chrome
Wyłącz zegar	Wyłącz zegar
Wyłącz kontakty	Wyłącz kontakty
Wyłącz Dialer	Wyłącz natywny dialer
Wyłącz eMail	Wyłączanie poczty e-mail
Wyłączanie Exchange	Wyłączanie kont Exchange
Wyłączanie Facebooka	Wyłącz aplikację Facebook
Wyłącz galerię	Wyłącz natywną aplikację galerii
Wyłączanie Gmaila	Wyłączanie Gmaila
Wyłącz Google Books	Wyłącz Google Books
Wyłączanie Kiosku Google Play	Wyłączanie Kiosku Google Play
Wyłącz Mapy Google	Wyłącz Mapy Google
Wyłącz Google Music	Wyłącz Google Music
Wyłącz Filmy Google	Wyłącz filmy Google
Wyłącz Sklep Google Play	Wyłącz Google Play Store (publiczny App Store)
Wyłącz Google Plus	Wyłącz Google Plus
Wyłączanie wyszukiwarki Google	Wyłączanie wyszukiwarki Google
Wyłącz Google Talk / Google Hangouts	Wyłącz Google Talk / Google Hangouts
Wyłączanie odtwarzacza muzyki	Wyłącz natywną aplikację odtwarzacza muzyki
Wyłącz ustawienia	Wyłączanie ustawień urządzenia
Wyłącz Sim Toolkit	Wyłączanie usług Sim Toolkit
Wyłącz SMS / MMS	Wyłącz SMS / MMS
Wyłącz Street View	Wyłączanie usług Street View
Wyłącz Youtube	Wyłącz Youtube

Samsung Apps

W sekcji "Samsung Apps" można zdefiniować dodatkowe ustawienia i/lub ograniczenia dla urządzeń Samsung.

Wyłącz AllShare Play / Samsung Link	Wyłącz AllShare Play / Samsung Link
Wyłącz ChatON	Wyłącz ChatON
Wyłącz Game Hub	Wyłącz Game Hub
Wyłącz grę grupową	Wyłącz grę grupową
Wyłącz pomoc	Wyłącz Samsung Help
Wyłącz KNOX	Wyłączanie kontenera Samsung KNOX
Wyłączanie notatki	Wyłączanie notatki głosowej
Wyłącz Moje pliki	Wyłącz Moje pliki
Wyłączanie czytnika optycznego	Wyłączanie czytnika optycznego
Wyłączanie Polaris Office	Wyłączanie Polaris Office
Wyłącz Readers Hub / Samsung Books	Wyłącz Readers Hub / Samsung Books
Wyłączanie S Memo	Wyłączanie aplikacji Samsung Memo
Wyłącz S Translator	Wyłącz aplikację Tłumacz Samsung
Wyłączanie funkcji S Voice	Wyłączanie asystenta głosowego S
Wyłączanie aplikacji Samsung	Wyłącz Samsung App Store
Wyłącz Samsung Hub	Wyłącz Samsung Entertainment Stores
Wyłącz odtwarzacz wideo	Wyłącz odtwarzacz wideo
Wyłączanie dyktafonu	Wyłączanie dyktafonu
Wyłącz WatchON	Wyłącz WatchON (symuluje zdalne sterowanie)

Aplikacje Huawei

W sekcji "Aplikacje Huawei" można zdefiniować dodatkowe ustawienia i/lub ograniczenia na urządzeniu Huawei.

Wyłączanie DLNA	Wyłączanie DLNA
Wyłącz instalator aplikacji	Wyłącz instalator aplikacji
Wyłączanie Menedżera plików	Wyłączanie Menedżera plików
Wyłączanie Menedżera kopii zapasowych	Wyłączanie Menedżera kopii zapasowych
Wyłącz aktualizator systemu	Wyłącz aktualizator systemu
Wyłącz skrzynkę narzędziową	Wyłącz skrzynkę narzędziową
Wyłącz pogodę	Wyłącz pogodę
Wyłączanie radia FM	Wyłączanie radia FM

Ustawienia zarządzania aplikacjami

W tym miejscu można zdefiniować sposób aktualizacji aplikacji InHouse Apps.

Częstotliwość sprawdzania aktualizacji określa, jak często aplikacja AppTec360 szuka aktualizacji dla aplikacji InHouse. Po wykryciu nowej wersji zostanie ona pobrana i zainstalowana.

Próg Wi-Fi określa, czy pobieranie powinno być ograniczone do połączeń Wi-Fi, jeśli aplikacja jest większa niż skonfigurowany próg. Jeśli próg jest mniejszy lub nie zostanie zdefiniowany, aplikacja będzie pobierana przez Wi-Fi i sieć komórkową.

Sklep z aplikacjami dla przedsiębiorstw

Należy pamiętać, że aplikacje dodane tutaj (Enterprise App Store) NIE spowodują ich automatycznej instalacji na urządzeniach. Użytkownik musi otworzyć Enterprise App Store na urządzeniu i zainstalować aplikację ręcznie.

Jeśli chcesz automatycznie instalować aplikacje na urządzeniu, przejdź do "App Management" → "Enterprise App Manager" → "Mandatory Apps" i dodaj tam żądane aplikacje.

W tym miejscu możesz dystrybuować opcjonalne aplikacje do swoich użytkowników.

Sklep Play

Kliknij "+", aby dodać aplikację do sklepu Play Store. Jeśli korzystasz z systemu Android Enterprise, przejdź do "App Management Enterprise Play Store". Należy również pamiętać, że konto Google musi być skonfigurowane na → urządzeniu, aby zainstalować aplikacje zdefiniowane tutaj.

Wewnątrz firmy

W punkcie "In-House" można przesyłać i rozpowszechniać aplikacje opracowane wewnętrznie.

Kliknij "+", aby dodać aplikację InHouse do sklepu z aplikacjami dla przedsiębiorstw, którą następnie może zainstalować użytkownik. W tym oknie dialogowym można również przesłać nową aplikację InHouse.

Sklep Play dla przedsiębiorstw

Należy pamiętać, że aplikacje dodane tutaj (Enterprise Play Store) NIE spowodują ich automatycznej instalacji na urządzeniach. Użytkownik musi otworzyć Sklep Play na urządzeniu i zainstalować aplikację ręcznie.

Jeśli chcesz automatycznie instalować aplikacje na urządzeniu, przejdź do "App Management" → "Enterprise App Manager" → "Mandatory Apps" i dodaj tam żądane aplikacje.

W tym miejscu możesz dystrybuować opcjonalne aplikacje do swoich użytkowników.

Tutaj można dodawać aplikacje do sklepu Android Enterprise Playstore. Pamiętaj, że musisz zatwierdzić aplikacje w Ustawieniach ogólnych → AE Play Store → Play Store Apps. Aplikacje te zostaną dodane do normalnego Sklepu Google Play.

Należy również pamiętać, że najpierw trzeba zdefiniować układ z aplikacjami w Ustawieniach ogólnych → Zarządzanie aplikacjami → AE Play Store → Układ sklepu.

Aplikacje muszą znajdować się w układzie, zanim będzie można je dodać do sklepu.

Tryb kiosku i program uruchamiający

Tryb kiosku

Tryb kiosku umożliwia wstępne zdefiniowanie aplikacji lub adresu URL. Wówczas możliwe będzie wyłącznie uruchamianie/odwiedzanie tej aplikacji lub adresu URL.

Podobnie, różne przyciski sprzętowe można dezaktywować w zróżnicowanym trybie kiosku.

Automatyczny start	Automatycznie uruchamia tryb kiosku, gdy tylko profil dotrze do urządzenia użytkownika końcowego.
Zaplanowany tryb kiosku?	Możesz zaplanować czas dla trybu kiosku, który następnie rozpocznie się i zakończy automatycznie o ustawionej przez Ciebie godzinie
Godzina rozpoczęcia	Czas rozpoczęcia
Czas w minutach	Czas w minutach, po którym tryb kiosku powinien się ponownie zakończyć.

Typ aplikacji

Pojedyncza aplikacja	Jeśli chcesz uruchomić aplikację w trybie kiosku, wybierz "Pakiet" w sekcji "Typ aplikacji".
Aplikacja kiosku	Kliknij tutaj, aby wybrać aplikację, która ma zostać uruchomiona w trybie kiosku. Znajdziesz tu zwykły przegląd zarządzania aplikacjami Można wybrać pomiędzy "Google Play Store", "Android In-House Apps" i "Packagename".

Typ aplikacji

URL	Jeśli chcesz uruchomić adres URL w trybie kiosku, wybierz "URL" w sekcji "Typ aplikacji". Następnie zdefiniuj żądany adres URL
Wyczyść przeglądarkę po braku aktywności	W tym miejscu można zdefiniować przedział czasu w minutach, po którym tryb kiosku powinien zostać ponownie uruchomiony
Wyczyść pamięć podręczną i pliki cookie	Jeśli funkcja ta zostanie aktywowana, po ponownym uruchomieniu trybu kiosku pamięć podręczna sieci Web (pliki cookie i obrazy w pamięci podręcznej) zostanie usunięta.
Polityka tego samego pochodzenia	Jeśli ta funkcja jest aktywna, użytkownik może przeglądać tylko podstrony zdefiniowanego adresu URL Na przykład, zdefiniowano następujący adres URL: www.mypage.com Następnie użytkownik może surfować na stronie: www.mypage.com/subpage
Adresy URL na białej liście	Tutaj można prowadzić białą listę, wszystkie te adresy URL są dozwolone Maksymalnie 1 adres URL w wierszu Adres URL musi zaczynać się od http:/ lub https://.
Adresy URL na czarnej liście	Tutaj można utworzyć czarną listę, na której wszystkie te adresy URL są niedozwolone. Maksymalnie 1 adres URL w wierszu Adres URL musi zaczynać się od http:/ lub https://.
Orientacja ekranu	To ustawienie odnosi się do regulacji ekranu Automatyczny = automatyczny Portret = format pionowy Krajobraz = tryb krajobrazowy

Multi App	Jeśli wybierzesz tryb kiosku "Multi App", korzystanie z AppTec360 Launcher będzie wymuszone.
Aplikacje	Aplikacja: Wybierz Playstore lub aplikację wewnętrzną jako aplikację kiosku. Możliwe jest również wprowadzenie nazwy pakietu. Wybrana aplikacja Kiosk musi być zainstalowana na urządzeniu. Pamiętaj, aby ustawić aplikację Kiosk jako obowiązkową. Skrót na ekranie głównym: W przypadku ustawienia na "Wł." zostanie utworzony skrót na ekranie głównym. W przypadku ustawienia na "Wył." aplikacja będzie nadal widoczna na liście aplikacji.

Hasło wyjścia włączone	Po aktywowaniu tej funkcji użytkownik może zakończyć tryb kiosku za pomocą wstępnie zdefiniowanego hasła
Hasło wyjścia	Jest to hasło, które zostało wstępnie zdefiniowane przez użytkownika
Automatycznie zwijany pasek stanu	Jeśli ta opcja jest włączona, pasek stanu będzie automatycznie kolorowany. Dzięki tej opcji użytkownicy mogą zobaczyć informacje na pasku stanu, ale nie mają dostępu do jego funkcji
Wyłącz pasek stanu	Pasek stanu zawiera powiadomienia, skróty i informacje. Dostępne tylko dla urządzeń Samsung z KNOX 1.0 lub nowszym.
Wyłącz klawisze głośności	Wyłącz klawisze głośności (dostępne tylko na urządzeniach Samsung z KNOX 1.0 lub nowszym)
Wyłącznik wł.	Wyłącz przełącznik On / Off (dostępny tylko na urządzeniach Samsung z KNOX 1.0 lub nowszym)
Wyłącz przycisk Home	Wyłącz przycisk Home. Jeśli ta funkcja została aktywowana, tryb kiosku można zakończyć tylko w konsoli AppTec360. (dostępne tylko na urządzeniach Samsung z KNOX 1.0 lub nowszym)
Wyłącz pasek nawigacji	W ten sposób można wyłączyć pasek nawigacji (Wstecz / Menu). Jeśli ta funkcja została aktywowana, tryb kiosku można zakończyć tylko w konsoli AppTec360. (dostępne tylko na urządzeniach Samsung z KNOX 1.0 lub nowszym)

Ustawienia aktualizacji aplikacji	
Zezwalaj na aktualizacje aplikacji	Użytkownicy będą proszeni o wykonanie aktualizacji aplikacji, nawet gdy aktywny jest tryb kiosku. Na urządzeniach z Samsung KNOX aplikacje będą aktualizowane po cichu.
Okno aktualizacji	Ustaw interwał, w którym użytkownicy będą proszeni o zainstalowanie aktualizacji aplikacji.

TeamViewer	
Włącz dostęp nienadzorowany	Jeśli jest włączona, administratorzy mogą zdalnie sterować urządzeniem bez interakcji z użytkownikiem. Aplikacja TeamViewer Host musi być zainstalowana na urządzeniu.

AppTec360 Launcher

Włącz program uruchamiający AppTec360	Wł: Włącza AppTec360 Launcher. Użytkownik musi jednorazowo ustawić go jako domyślny program uruchamiający. Uwaga: Jeśli tryb kiosku jest włączony, a tryb kiosku jest ustawiony na "Multi App", korzystanie z programu uruchamiającego AppTec360 będzie wymuszone.
Duże ikony	Wł: Wyświetla większą wersję ikon aplikacji w programie uruchamiającym.
Ukryj ikonę aplikacji AppTec360	Wł: Całkowicie ukrywa aplikację AppTec360
Ukryj ikonę sklepu AppTec360	Wł: Całkowicie ukrywa AppStore AppTec360 Enterprise.

Ustawienia AppTec360

Włącz aplikację ustawień AppTec360	Aplikacja AppTec360 Settings zapewnia kontrolę nad połączeniami WiFi i Bluetooth
Włącz ustawienia w aplikacji Multi Tryb kiosku	Jeśli ta opcja jest włączona, użytkownicy mogą uzyskać dostęp do aplikacji ustawień AppTec360, gdy aktywny jest tryb kiosku z wieloma aplikacjami.

Pilot zdalnego sterowania

Splashtop

Pokazuje aktualny stan konfiguracji Splashtop. Tutaj zobaczysz kroki, które musisz wykonać, aby uzyskać zdalny dostęp do urządzenia za pośrednictwem Splashtop. W tym miejscu należy również wprowadzić kod wdrożenia, który można uzyskać ze strony internetowej Splashtop. Kod wdrożenia jest wymagany do połączenia się z urządzeniem.

Teamviewer

Pokazuje aktualny stan konfiguracji Teamviewer. W tym miejscu wyświetlane są kroki, które należy wykonać, aby uzyskać zdalny dostęp do urządzenia za pośrednictwem Teamviewer.

Zarządzanie treścią

Contentbox

Tutaj można włączyć Contentbox dla tego urządzenia. Po aktywacji aplikacja Contentbox zostanie zainstalowana na urządzeniu.

Bezpieczna przeglądarka

Tutaj możesz włączyć Bezpieczną przeglądarkę dla tego urządzenia. Po aktywacji na urządzeniu zostanie zainstalowana aplikacja Secure Browser. Przeglądarkę tę można skonfigurować tak, aby oferowała przeglądarkę internetową na urządzeniu, która jest ograniczona do potrzeb użytkownika.

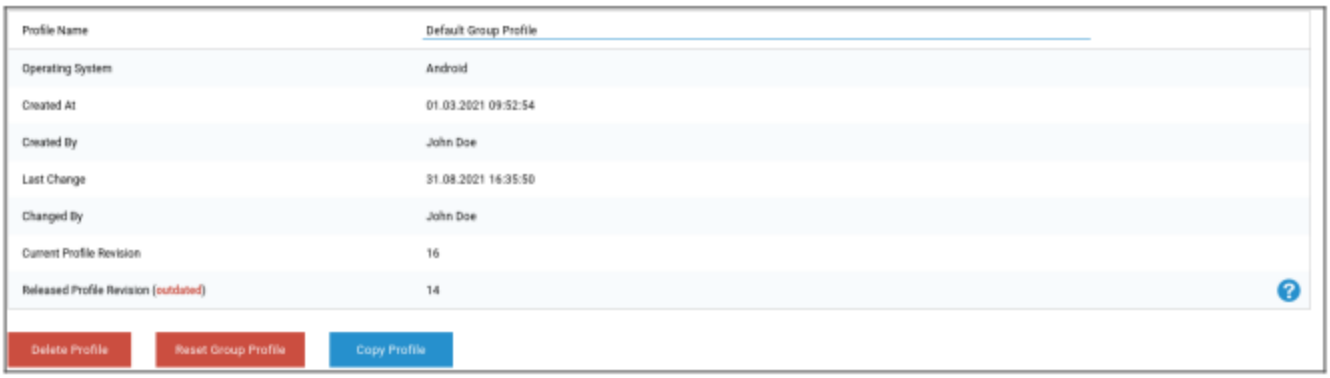
Wymagaj hasła	Wymagaj od użytkownika skonfigurowania i używania hasła w celu uzyskania dostępu do przeglądarki.
Ogranicz pobieranie / Otwórz w	Blokuje pobieranie plików z witryn internetowych
Ogranicz przesyłanie	Ogranicza przesyłanie do określonych adresów URL. Nie podawaj adresu URL, aby całkowicie zablokować przesyłanie
Zezwalaj na kopiowanie	Zezwalaj na kopiowanie, wycinanie lub udostępnianie tekstu wewnątrz stron internetowych.
Zezwalaj na przechwytywanie ekranu	Zezwalaj na przechwytywanie zrzutów ekranu.
Częstotliwość czyszczenia danych	Wybierz, z jaką częstotliwością WSZYSTKIE dane użytkownika (historia, pamięć podręczna itp.) mają być automatycznie usuwane.
Zakładki firmowe	Zakładki pojawią się w folderze "Zakładki firmowe" w zakładkach przeglądarki. Użytkownik nie może ich edytować.
Ukryj pasek adresu	Ukrywa pasek adresu, aby użytkownik nie widział odwiedzanego adresu URL.
Biała lista w przeglądarce (bez Universal Gateway)	Włącza białą listę adresów URL po stronie klienta. - Zakładki firmowe są zawsze umieszczane na białej liście - Obsługiwane tylko dla 100 adresów URL - Użyj Universal Gateway, aby uzyskać nieograniczoną czarną i białą listę.
Czarna i biała lista oparta na bramie	Czarna lista ma następujące wymagania: - Działająca brama uniwersalna AppTec360 ("Ustawienia ogólne" → "Brama uniwersalna") - Działająca konfiguracja VPN z określonym serwerem DNS ("Ustawienia ogólne" → "Brama uniwersalna" → "Ustawienia VPN") - Konfiguracja czarnej listy ("Ustawienia ogólne" → "Brama uniwersalna" → "Czarna lista domen") - Ważne połączenie VPN w profilu ("Zarządzanie połączeniami" → "VPN")

Konfiguracja komputera z systemem Windows 10

Ogólne

Przegląd profilu grupy (tylko na poziomie grupy)

Po otwarciu profilu grupy wyświetlony zostanie szybki przegląd profilu.



Nazwa profilu	Nazwa profilu (można ją zmienić tutaj)
System operacyjny	System operacyjny, dla którego przeznaczony jest profil
Utworzono w	Czas stworzenia
Utworzony przez	Twórca profilu
Ostatnia zmiana	Czas ostatniej zmiany profilu
Zmienione przez	Konto, które wprowadziło ostatnie zmiany
Aktualna wersja profilu	Zmiana zapisanego stanu profilu
Wydana wersja profilu	Wersja przypisanego profilu ("Przypisz teraz"). Jeśli etykieta pokazuje "(nieaktualne)" za tekstem, oznacza to, że profil został zapisany, ale nie został jeszcze przypisany, więc urządzenia nadal będą otrzymywać starszą wersję.

Przegląd urządzeń (tylko na poziomie urządzenia)

Podsumowanie urządzenia, które zawiera następujące informacje:

Nazwa komputera	Nazwa komputera
Klient	Urządzenia typu Windows
Ostatnia znana lokalizacja	Szerokość i długość geograficzna ostatniej znanej lokalizacji urządzenia
Przypisane aplikacje obowiązkowe	Liczba aplikacji obowiązkowych przypisanych do urządzenia
PC UID	UID komputera
OS Edition	Pokazuje wersję systemu Windows
Wersja systemu operacyjnego	Aktualnie zainstalowana wersja systemu Windows
Kompilacja systemu operacyjnego	Aktualna wersja systemu Windows
System operacyjny	Aktualnie zainstalowany system operacyjny
Numer seryjny	Numer seryjny urządzenia
Własność urządzenia	Skonfigurowany typ własności
Typ urządzenia	Typ urządzenia
Zakorzeniony	Pokazuje, czy urządzenie jest zrootowane
Zgodność	Pokazuje, czy urządzenie jest zgodne
Ostatnio widziany	Data i godzina wprowadzenia zmian w profilu.
Przypisanie użytkownika	Wyświetla użytkownika lub grupę, do której aktualnie przypisane jest urządzenie. Urządzenie można przenieść, wybierając innego użytkownika lub grupę z listy rozwijanej.

Ustawienia

Zezwalaj na automatyczną aktualizację	Zezwalaj lub nie zezwalaj na automatyczne aktualizacje systemu operacyjnego.

Wersja konfiguracji (tylko na poziomie urządzenia)

W tym miejscu wyświetlany jest przegląd profili grupowych przypisanych do urządzenia.

Jeśli klikniesz profil grupy, uzyskasz do niego bezpośredni dostęp i będziesz mógł dokonać ustawień.

Za pomocą symbolu można przywrócić przypisane aplikacje do ustawień profilu grupy.

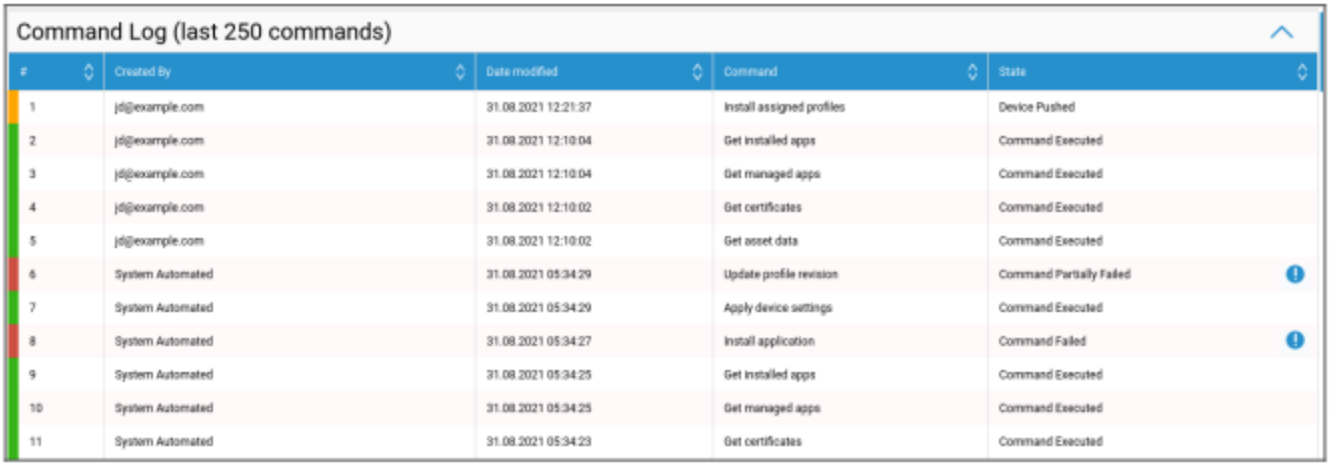
Za pomocą symbolu można zresetować profil urządzenia, aby nie miał żadnych ustawień.

"Newer Revision available" oznacza, że profil grupy został zmieniony i zapisany, ale nie został przypisany. Profil grupy musi zostać przypisany za pomocą opcji "Przypisz teraz" na poziomie grupy, aby zastosować zmiany do urządzeń.

Dziennik urządzenia (tylko na poziomie urządzenia)

Dziennik poleceń

Tutaj można sprawdzić, które polecenia zostały wydane dla urządzenia i jaki jest ich status.



Polecenia utworzone przez "System Automated" są automatycznie tworzone przez system.

Możliwe statusy poleceń

Urządzenie wciśnięte	Żądanie push zostało wysłane do usługi push (np. APNS), aby poinformować urządzenie o konieczności połączenia się z serwerem EMM.
Utworzone polecenie	Polecenie zostało utworzone w systemie.
Wysłane polecenie	Polecenie zostało wysłane do urządzenia po nawiązaniu połączenia z serwerem.
Polecenie wykonane	Polecenie zostało pomyślnie wykonane.
Polecenie nie powiodło się	Polecenie nie powiodło się. *
Polecenie częściowo nieudane	W zależności od systemu operacyjnego urządzenia niektóre polecenia mogą zostać zgrupowane. W tym przypadku niektóre części tej grupy poleceń nie powiodły się. *
Polecenie wykonane, ostatecznie nieudane	Polecenie zostało wykonane, ale być może nie.
Przesunięcie polecenia	Polecenie zostało powtórzone przez użytkownika.
Odrzucony	Polecenie zostało odrzucone. Na przykład dlatego, że zostało zastąpione przez inne polecenie lub urządzenie zostało ponownie zarejestrowane, a stare polecenia zostały usunięte.

*Jeśli za wiadomością znajduje się wykrzyknik, możesz uzyskać więcej informacji, najeżdżając kursorem na ikonę.

Zarządzanie zasobami (tylko na poziomie urządzenia)

Informacje o urządzeniu

Producent	Producent urządzenia
Model	Model urządzenia
Numer modelu	Numer modelu
System operacyjny	System operacyjny
Wersja systemu operacyjnego	Wersja systemu operacyjnego
Numer seryjny	Numer seryjny
ExchangeID	ExchangeID
Całkowita pamięć RAM	Całkowita pamięć RAM
Rozdzielczość wyświetlacza	Rozdzielczość wyświetlacza
Język telefonu	Język urządzenia
Wersja oprogramowania sprzętowego	Wersja oprogramowania sprzętowego
Wersja klienta DM	Wersja klienta zarządzania urządzeniami
Wersja sprzętowa	Wersja sprzętowa urządzenia
Architektura procesora	Architektura procesora (typ procesora)

Komórkowy

SIM Sieć operatora	Sieć operatora
Numer telefonu	Numer telefonu
Status roamingu	Status roamingu
IMEI	IMEI
IMSI	IMSI
Oprogramowanie sprzętowe modemu	Oprogramowanie sprzętowe modemu

Informacje o synchronizacji

Natychmiastowe połączenie DM	Urządzenie powinno natychmiast nawiązać połączenie z AppTec
Początkowy czas ponawiania próby	Początkowy czas ponawiania dla tego pierwszego połączenia
Próby połączenia	Liczba ponownych prób nawiązania połączenia po rozłączeniu przez Menedżera połączeń lub błędzie na poziomie WinInet.
Maksymalny czas uśpienia	Maksymalny czas uśpienia po błędzie wysyłania pakietu
Pierwsze próby synchronizacji	Czas na pierwszy etap po rejestracji
Interwał pierwszej próby	Czas na pierwszy etap po rejestracji
Druga próba synchronizacji	Czas na drugi etap po rejestracji
Drugi interwał ponawiania próby	Czas na drugi etap po rejestracji
Regularne próby synchronizacji	Czas na dodatkowe etapy po rejestracji
Regularny interwał ponawiania prób	Czas na dodatkowe etapy po rejestracji

Zarządzanie bezpieczeństwem

Ochrona przed kradzieżą (tylko na poziomie urządzenia)

Informacje GPS (tylko na poziomie urządzenia)

Tutaj można ustalić bieżącą/ostatnią lokalizację urządzenia. Lokalizacja może być chroniona jednym lub nawet dwoma hasłami - patrz: "Ustawienia ogólne" > "Prywatność" > "Dostęp GPS"

Ustawienia GPS

Włącz śledzenie GPS	Włączenie regularnej synchronizacji informacji GPS.
Interwał śledzenia	Ustawienie interwału synchronizacji informacji GPS.

Konfiguracja zabezpieczeń

Kod dostępu

Minimalna długość hasła	Minimalna długość hasła	
Skład hasła	Określa liczbę określonych znaków, które musi zawierać hasło. Składają się one z wielkich liter, małych liter, cyfr i symboli specjalnych	
Jakość hasła	Tutaj można ustawić jakość hasła	
	Alfanumeryczne	Tylko cyfry i litery
	Numeryczny	Tylko liczby
	Numeryczne lub alfanumeryczne	Liczby lub liczby i litery
Blokada maksymalnego czasu nieaktywności	Liczba minut bezczynności użytkownika na urządzeniu, po której urządzenie zostanie zablokowane. Użytkownik musi odblokować urządzenie po upływie tego czasu, wprowadzając hasło urządzenia.	
Wygaśnięcie hasła	Ustawienie czasu do ustawienia nowego hasła	
Ograniczenie historii haseł	Liczba wcześniej używanych haseł, które są niedozwolone	
Maksymalna liczba nieudanych prób wpisania hasła	Liczba powtórzeń nieprawidłowego wprowadzenia hasła przed całkowitym wyczyszczeniem urządzenia.	

Antywirus

Ustawienia antywirusa - konfiguracja skanowania	
Typ skanowania	Umożliwia wybór szybkiego lub pełnego skanowania.
Ustawienie rozpoczęcia skanowania	Wybiera porę dnia, w której program Windows Defender rozpocznie skanowanie.
Częstotliwość skanowania	Wybiera dzień, w którym ma zostać uruchomione skanowanie Windows Defender
Częstotliwość aktualizacji podpisu	Określa interwał w godzinach, który będzie używany do sprawdzania podpisów

Konfiguracja typu plików do skanowania	
Zezwalaj na skanowanie plików archiwalnych	Zezwalaj lub nie zezwalaj na skanowanie archiwów (takich jak .zip) podczas uzyskiwania do nich dostępu.
Zezwalaj na skanowanie skryptów	Włącza lub wyłącza funkcję skanowania skryptów w usłudze Windows Defender.
Zezwalaj na skanowanie wiadomości e-mail	Zezwalaj lub nie zezwalaj na skanowanie wiadomości e-mail.
Zezwalaj na skanowanie plików sieciowych	Zezwalaj lub zabraniaj skanowania plików sieciowych.
Umożliwienie pełnego skanowania zmapowanych dysków sieciowych	Zezwól lub nie zezwalaj na skanowanie zmapowanych dysków sieciowych (włączone tylko wtedy, gdy włączone jest pełne skanowanie).
Kontrola skanowania dwukierunkowego	Kontroluje, które zestawy plików powinny być monitorowane.
Zezwalaj na pełne skanowanie dysków wymiennych	Zezwól lub nie zezwalaj na pełne skanowanie dysków wymiennych. Tylko podczas pełnego skanowania.

Typ plików, które mają zostać wykluczone ze skanowania	
Ignorowanie typów plików do skanowania	Zdefiniuj zestaw typów rozszerzeń plików. Każde rozszerzenie pliku dla każdego pola.
Ignorowanie ścieżek katalogów	Zdefiniuj zestaw ścieżek katalogów, aby ich nie skanować. Jedna ścieżka na pole. Przykłady: "C:\Example", "C:\Windows" lub "C:\Users".
Wyklucz procesy ze skanowania	Wyklucz pliki, które zostały otwarte przez określone procesy ze skanowania antywirusowego Microsoft Defender. . Jedna ścieżka na pole. Przykłady: "C:\myFile.exe", "C:\Windows\myProcess.exe", "C:\myScript.bat".

Ustawienia dodatkowe	
Zezwalaj na monitorowanie w czasie rzeczywistym	Zezwalaj lub zabraniaj funkcji monitorowania w czasie rzeczywistym w usłudze Windows Defender.
Zezwalaj na monitorowanie zachowania	Zezwalaj lub zabraniaj funkcji monitorowania zachowania systemu Windows.
Zezwalaj na ochronę w chmurze	Zezwól lub nie zezwalaj usłudze Windows Defender na wysyłanie do firmy Microsoft informacji o wykrytych problemach. Microsoft przeanalizuje te informacje, dowie się więcej o problemie wpływającym na urządzenie i zaoferuje ulepszone rozwiązania
	Zachowanie podczas wysyłania próbek
Zezwalaj na ochronę IOAV w usłudze Windows Defender	Zezwalaj lub nie zezwalaj na ochronę IOAV w usłudze Windows Defender
Zezwól na dostęp do interfejsu użytkownika Defenders "On Access protection".	
Średni współczynnik obciążenia procesora	Przedstawia średni współczynnik obciążenia procesora dla skanowania Windows Defender (w procentach).

Obsługa złośliwego oprogramowania	
Niska dotkliwość	Dla każdego poziomu ważności można zdefiniować sposób obsługi złośliwego oprogramowania przez urządzenie. Dostępne opcje to: • Czystość • Kwarantanna • Usunąć • Zezwalaj • Zdefiniowane przez użytkownika • Blok
Umiarkowane nasilenie	
Wysoka dotkliwość	
Poważne nasilenie	
Dni na zachowanie wyczyszczonego złośliwego oprogramowania	Okres czasu w dniach, w którym pliki/elementy kwarantanny będą przechowywane w systemie. Domyślną wartością jest 0, która

	utrzymuje elementy w kwarantannie i nie usuwa ich automatycznie. Maksymalna wartość to 90.

Centrum bezpieczeństwa

Centrum zabezpieczeń systemu Windows - ustawienia zabezpieczeń systemu Windows	
Wyłącz interfejs użytkownika ochrony przed wirusami i zagrożeniami	
Ukryj interfejs odzyskiwania danych Ransomware	
Wyłącz interfejs użytkownika ochrony konta	
Wyłącz zaporę sieciową i interfejs ochrony sieci	
Wyłączenie interfejsu sterowania aplikacji i przeglądarki	
Nie zezwalaj na zmiany w ochronie przed exploitami	Nie zezwalaj użytkownikowi na wprowadzanie zmian w ustawieniach ochrony przed exploitami
Wyłącz interfejs zabezpieczeń urządzenia	
Ukryj rozwiązywanie problemów z TPM	Ukryj ustawienia rozwiązywania problemów TPM
Wyłącz przycisk Wyczyść TPM	
Wyłączenie interfejsu użytkownika wydajności i kondycji urządzenia	
Wyłączenie interfejsu użytkownika opcji rodziny	

Dostosuj toasty	
Włącz niestandardowe informacje pomocy technicznej	Włącz wyświetlanie niestandardowych informacji kontaktowych pomocy technicznej dla Twojej firmy w prawym dolnym rogu aplikacji Security Center.
Adres e-mail	Ustaw firmowy adres e-mail
Nazwa firmy	Ustaw nazwę firmy
Telefon służbowy	Ustaw telefon firmowy
Pomoc URL	Ustaw adres URL pomocy firmy

Ustawienia dodatkowe	
Wyłącz powiadomienia	Wyłącz wyświetlanie powiadomień Centrum zabezpieczeń Windows Defender.
Ukryj zalecenia dotyczące aktualizacji oprogramowania układowego TPM	Ukryj zalecenie aktualizacji oprogramowania układowego TPM po wykryciu podatnego oprogramowania układowego.
Wyświetlanie nazwy firmy i opcji kontaktu	Wyświetlaj nazwę firmy i opcje kontaktu na wysuwanej karcie kontaktu w Centrum zabezpieczeń programu Windows Defender.
Ukryj bezpieczny rozruch	Ukryj obszar rozruchu zabezpieczeń.
Ukryj kontrolę obszaru powiadomień zabezpieczeń	Ukryj kontrolkę obszaru powiadomień zabezpieczeń systemu Windows.

Konfiguracja zapory sieciowej

Konfiguracja zapory sieciowej - ustawienia globalne	
Ignorowanie zestawu uwierzytelniania	Zignoruj cały zestaw uwierzytelniania, jeśli nie obsługuje on wszystkich zestawów uwierzytelniania określonych w zestawie.
Typ kolejkowania pakietów	Określa, w jaki sposób skalowanie oprogramowania po stronie odbiorczej jest włączone zarówno dla szyfrowanego odbioru, jak i wyczyszczenia ścieżki przekazywania dla scenariusza bramy tunelu IPsec.
Wyłącz wykonywanie stanowego filtrowania FTP	Jeśli jest wyłączona, nie będzie wykonywać filtrowania stanowego protokołu transferu plików (FTP), aby zezwolić na połączenia dodatkowe
Czas bezczynności skojarzenia zabezpieczeń	To pole konfiguruje czas bezczynności skojarzenia zabezpieczeń w sekundach. Skojarzenia zabezpieczeń są usuwane, gdy ruch sieciowy nie jest widoczny przez określony czas.
Kodowanie klucza wstępnego	Ustawienie kodowania klucza wstępnego
Wyjątki IPSec	Konfiguracja wyjątków protokołu internetowego
Sprawdzanie listy odwołania certyfikatów	

Profile zapory (profil domeny / profil prywatny / profil publiczny)	
Włącz zaporę dla tego profilu	
Wyłącz powiadomienia	Wyłączenie wyświetlania powiadomień dla użytkownika, gdy aplikacja jest zablokowana przed nasłuchem na porcie.
Blokowanie odpowiedzi unicast na transmisje multicast	
Wymuszanie reguł zapory dla autoryzowanych aplikacji	Jeśli nie jest wymuszana, autoryzowane reguły zapory aplikacji w lokalnym magazynie są ignorowane i nie są wymuszane
Wymuszanie globalnych reguł zapory portów	Jeśli nie jest wymuszane, globalne reguły zapory portów w magazynie lokalnym są ignorowane i nie są wymuszane. Ustawienie ma znaczenie tylko wtedy, gdy jest ustawione lub wyliczone w magazynie zasad grupy lub jeśli jest wyliczone z GroupPolicyRSoPStore
Wymuszanie reguł zapory sieciowej	Jeśli nie jest wymuszana, reguły zapory z lokalnego magazynu są ignorowane i nie są wymuszane
Wymuszanie reguł bezpieczeństwa połączeń	Jeśli nie jest egzekwowana, reguły zabezpieczeń połączeń z lokalnego sklepu są ignorowane i nie są egzekwowane
Domyślne działanie wychodzące	Działanie, które firewall domyślnie wykonuje na połączeniach wychodzących
Domyślne działanie przychodzące	Działanie, które firewall domyślnie wykonuje na połączeniach przychodzących
Wyłącz tryb niewidzialności	Tryb ukrycia to mechanizm Zapory systemu Windows, który pomaga zapobiegać wykrywaniu przez złośliwych użytkowników informacji o komputerach w sieci i uruchomionych przez nie usługach.
Wyłączenie zapobiegania odpowiadaniu na niechciany ruch	Jeśli jest wyłączona, reguły trybu ukrycia zapory nie mogą uniemożliwiać komputerowi hosta odpowiadania na niechciany ruch sieciowy, jeśli ruch ten jest zabezpieczony przez IPsec

Reguły zapory sieciowej

Reguły zapory sieciowej	
Nazwa	Nazwa reguły
Opis	Opis zasady
Działanie	Określ, czy ta reguła ma blokować ruch, czy na niego zezwalać. Należy pamiętać, że opcja Blokuj może również blokować ruch (w zależności od reszty konfiguracji) między serwerem MDM a urządzeniem.
Kierunek	
Enable Edge traversal (dostępne tylko wtedy, gdy **Direction** jest ustawione na **ruch przychodzący**)	Wskazuje, że określony ruch przychodzący jest dozwolony do tunelowania przez NAT i inne urządzenia brzegowe przy użyciu technologii tunelowania Teredo.

Programy i usługi	
Definiowanie aplikacji, wszystkie inne	Jeśli nie jest włączona, będzie brać pod uwagę wszystkie aplikacje
Nazwa rodziny pakietów	Nazwa rodziny pakietów, do której będzie stosowana reguła.
Ścieżka pliku aplikacji	Pełna aplikacja, taka jak C:\Windows\System\Notepad.exe, do której zostanie zastosowana reguła
W pełni kwalifikowana nazwa binarna	W pełni kwalifikowana nazwa binarna, której będzie dotyczyć reguła. FQBN to ciąg znaków w następującej postaci: {Publisher\Product\Filename,Version}
Nazwa usługi	Wprowadź nazwę usługi (np. "EventLog"). Listę nazw usług można uzyskać w Powershell, uruchamiając polecenie "Get-Service".

Protokoły i porty				
Protokół	Protokół używany przez regułę.			
	Dostępne wartości: - Dowolny - Niestandardowe - HOPORT - ICMPv4 - IGMP - TCP - UDP - IPv6 - Trasa IPv6 - IPv6-Frag - GRE - ICMPv6 - IPv6-NoNxt - IPv6-Opts - VRRP - PGM - L2TP	Po ustawieniu na Niestandardowe	Wstaw numer protokołu z przedziału od 0 do 255	Numer protokołu
		Po ustawieniu na TCP lub UDP	Określ porty lokalne, w przeciwnym razie użyte zostaną wszystkie.	Porty lokalne, z których będzie korzystać reguła, dozwolone są również porty zakresowe.
			Port lokalny	Pojedynczy port lub zakres portów. Np. 100-120,200,300-320.
			Określ porty zdalne, w przeciwnym razie użyte zostaną wszystkie.	Zdalne porty, które będą używane przez regułę, dozwolone są również porty zakresu.
			Port zdalny	Pojedynczy port lub zakres portów. Np. 100-120,200,300-320.

Zakres	
Określ lokalny adres IP, w przeciwnym razie dowolny adres IP	Zestaw lokalnych adresów IP, może to być również zakres adresów IP oddzielonych znakiem -.
Lokalny adres IP	Zestaw pojedynczych adresów IP lub zakres adresów IP oddzielonych znakiem -
Określ zdalne adresy IP, w przeciwnym razie dowolny zdalny adres IP	Określa zestaw zdalnych adresów IP, może to być również zakres adresów IP oddzielonych znakiem "-".
Zdalny adres IP	Określ pojedynczy adres IP lub zakres adresów IP
Żetony	Tokeny, które można ustawić wraz z adresami zdalnymi. Tokeny Intranet, RmtIntranet i Ply2Renders są obsługiwane w systemie Windows 10, wersja 1809 i nowszych.

Ustawienia zaawansowane	
Określ profile, w przeciwnym razie zostaną użyte wszystkie.	Jeśli wyłączone, używane będą wszystkie profile
Domena	Profil domeny
Prywatny	Profil prywatny
Publiczny	Profil publiczny
Określ interfejsy, w przeciwnym razie użyte zostaną wszystkie.	Jeśli wyłączone, używane będą wszystkie interfejsy
Sieć lokalna	Interfejs sieci lokalnej
Zdalny dostęp	Interfejs zdalnego dostępu
Bezprzewodowy	Interfejs bezprzewodowy

Lokalni dyrektorzy	
Dodawanie autoryzowanych użytkowników lokalnych	Zezwól na dodanie listy użytkowników lokalnych, którzy będą korzystać z tej reguły.
Autoryzowani użytkownicy	Lista autoryzowanych użytkowników lokalnych dla tej reguły. Użytkownik musi być w formacie Security Description Definition language (SDDL), np. PC_NAME\USERNAME. To pole nie może być wypełnione, jeśli nazwa usługi jest ustawiona na używanie tej reguły

Ustawienia ograniczeń

Funkcjonalność urządzenia

Zezwól na kartę SD	Zezwalaj na korzystanie z karty SD
Zezwól na kamerę	Zezwalaj na korzystanie z kamery
Zezwalaj na usługę lokalizacji	Zezwalaj na usługę lokalizacji urządzenia
Zezwalaj na boczne ładowanie aplikacji	Zezwalaj na instalację aplikacji z nieznanych źródeł
Zezwalaj na tryb programisty	Zezwala na tryb deweloperski
Zezwalaj na transmisję danych w roamingu	Zezwalaj na transmisję danych w roamingu
Zezwól Cortanie	Zezwól asystentowi głosowemu Cortana
Zezwalaj wyszukiwarce na korzystanie z lokalizacji	Zezwalaj wyszukiwaniu na korzystanie z lokalizacji
Zezwalaj na dodawanie kont e-mail innych niż Microsoft	Określa, czy użytkownik może dodawać konta e-mail spoza MSA.
Zezwalaj na połączenie z kontem Microsoft	Określa, czy zezwolić na używanie konta MSA do uwierzytelniania połączeń i usług niezwiązanych z pocztą e-mail.
Zezwalaj na synchronizację moich ustawień	Umożliwia synchronizację ustawień na całym urządzeniu.
Nazwy domen chronione dla przedsiębiorstw	Określa nazwy domen przedsiębiorstwa oddzielone znakiem ";".
Umożliwienie użytkownikowi wyłączenia	Umożliwia użytkownikowi wyłączenie Przywracania systemu. **OSTRZEŻENIE!**

Przywracania systemu	Ta funkcja powinna być używana tylko na urządzeniach, które są własnością lub są dostarczane przez firmę lub organizację korporacyjną lub na urządzeniu należącym do użytkownika, gdy użytkownik zezwala, aby urządzenie było w pełni zarządzane przez firmę korporacyjną. Jeśli wyłączysz to ustawienie zasad, Przywracanie systemu zostanie wyłączone i nie będzie można uzyskać dostępu do Kreatora przywracania systemu. Opcja konfiguracji Przywracania systemu lub tworzenia punktu przywracania za pomocą Ochrony systemu jest również wyłączona.
Zezwalaj na wyrejestrowanie użytkownika	Umożliwia użytkownikowi usunięcie części korporacyjnej z urządzenia, a tym samym odłączenie się od serwerów AppTec360. Jeśli tak się stanie, zarządzanie urządzeniem nie będzie już możliwe. **OSTRZEŻENIE!** Ta funkcja powinna być używana tylko na urządzeniach, które są własnością lub są dostarczane przez firmę lub organizację korporacyjną lub na urządzeniach należących do użytkownika, w przypadku gdy użytkownik zezwala, aby urządzenie było w pełni zarządzane przez firmę korporacyjną. Jeśli to ustawienie zasad zostanie wyłączone, użytkownicy nie będą mogli usuwać rejestracji MDM. Określ, czy użytkownik może usunąć konto w miejscu pracy za pośrednictwem panelu sterowania w miejscu pracy. Serwer MDM zawsze może zdalnie usunąć konto.

BitLocker

Konfiguracja funkcji BitLocker

Ustawienia ogólne	
Wymóg szyfrowania urządzeń	W zależności od wersji systemu Windows i konfiguracji systemu, użytkownicy mogą zostać poproszeni o włączenie szyfrowania urządzenia: - Aby potwierdzić, że szyfrowanie od innego dostawcy nie jest włączone. - Aby wyłączyć szyfrowanie dysków funkcją BitLocker, a następnie włączyć ją ponownie.
Metody szyfrowania	
Metoda szyfrowania dysków systemu operacyjnego	
Metoda szyfrowania dla stacjonarnych dysków danych	
Metoda szyfrowania dysków wymiennych	
Wyłączenie ostrzeżenia o szyfrowaniu dysku przez firmę trzecią	Wyłączenie monitu ostrzegawczego o usłudze szyfrowania dysków innej firmy używanej na urządzeniu. Począwszy od Windows 10, wersja 1803, to ustawienie jest obsługiwane tylko dla urządzeń połączonych z Azure Active Directory.
Zezwalaj na uruchomienie szyfrowania, gdy zalogowany jest użytkownik niebędący administratorem	Obsługiwane tylko dla urządzeń połączonych z Azure Active Directory

Rozszerzenia AppTec360		
Ciche szyfrowanie		Jeśli zostanie wybrana wraz z opcją "Wymagaj szyfrowania urządzenia", usługa zarządzania AppTec360 uruchomi automatyczne ciche szyfrowanie dysków urządzenia.
	Automatyczne generowanie poświadczeń użytkownika	Zaszyfrowany dysk systemu operacyjnego będzie chroniony automatycznie wygenerowanymi poświadczeniami użytkownika. PIN TPM, jeśli moduł TPM jest dostępny, lub 6-cyfrowe hasło tekstowe. Wygenerowane dane uwierzytelniające są wysyłane na adres e-mail zarejestrowany dla danego urządzenia. Jeśli ta opcja jest wyłączona, jedynym możliwym zabezpieczeniem dla cichego szyfrowania jest użycie TPM. W takim przypadku, w przypadku urządzeń bez modułu TPM, ciche szyfrowanie nie powiedzie się.
	Szyfrowanie dysków stałych	Wszelkie dostępne stałe dyski danych zostaną również zaszyfrowane i zabezpieczone za pomocą funkcji "Automatyczne odblokowanie" przy użyciu klucza przechowywanego na dysku systemu operacyjnego.

Ustawienia dysku systemu operacyjnego

Wymagaj dodatkowego uwierzytelniania podczas uruchamiania		To ustawienie pozwala skonfigurować, czy funkcja BitLocker wymaga uwierzytelnienia przy każdym uruchomieniu komputera. To ustawienie jest stosowane podczas konfiguracji funkcji BitLocker. Po włączeniu tego ustawienia użytkownicy mogą skonfigurować zaawansowane opcje uruchamiania w kreatorze konfiguracji funkcji BitLocker.
	Blokowanie funkcji BitLocker bez kompatybilnego modułu TPM	
	Tylko TPM	
	TPM i PIN	
	TPM i klucz	
	TPM, klucz i PIN	Jeśli chcesz wymagać użycia kodu PIN i pamięci flash USB (klucza), użytkownik musi skonfigurować funkcję BitLocker za pomocą narzędzia wiersza poleceń "manage-bde" zamiast kreatora konfiguracji szyfrowania dysków BitLocker.

Wymagana minimalna długość kodu PIN

	Minimalna liczba znaków

Konfiguracja komunikatu i adresu URL odzyskiwania przed uruchomieniem komputera	Skonfiguruj cały komunikat odzyskiwania lub zastąp istniejący adres URL, który jest wyświetlany na ekranie odzyskiwania klucza przed uruchomieniem, gdy dysk systemu operacyjnego jest zablokowany. Uwaga: Nie wszystkie znaki i języki są obsługiwane w trybie pre-boot. Zdecydowanie zaleca się sprawdzenie, czy używane znaki są prawidłowo wyświetlane na ekranie odzyskiwania przed uruchomieniem systemu.
	Opcja komunikatu odzyskiwania przed uruchomieniem komputera
	Niestandardowy komunikat odzyskiwania
	Niestandardowy adres URL odzyskiwania

Opcje odzyskiwania systemu operacyjnego		To ustawienie pozwala kontrolować sposób odzyskiwania dysków systemu operacyjnego chronionych funkcją BitLocker w przypadku braku wymaganych poświadczeń. To ustawienie jest stosowane podczas konfiguracji funkcji BitLocker. Domyślnie dozwolony jest agent odzyskiwania danych oparty na certyfikatach, opcje odzyskiwania mogą być określone przez użytkownika, w tym hasło odzyskiwania i klucz odzyskiwania, a informacje o odzyskiwaniu nie są archiwizowane w usługach AD DS.
	Agent odzyskiwania danych oparty na certyfikacie blokowym	Określenie, czy agent odzyskiwania danych może być używany z dyskami systemu operacyjnego chronionymi funkcją BitLocker. Przed użyciem agenta odzyskiwania danych należy go dodać z pozycji Zasady klucza publicznego w Konsoli zarządzania zasadami grupy lub Edytorze lokalnych zasad grupy. Więcej informacji na temat dodawania agentów odzyskiwania danych można znaleźć w Przewodniku wdrażania szyfrowania dysków funkcją BitLocker w witrynie Microsoft TechNet.
	Ustawienia hasła odzyskiwania funkcji BitLocker	
	Ustawienia klucza odzyskiwania BitLocker	
	Zapisywanie informacji o odzyskiwaniu funkcji BitLocker w Usługach domenowych w usłudze Active Directory	
	Konfiguracja magazynu odzyskiwania AD DS BitLocker	Przechowywanie pakietu kluczy wspomaga odzyskiwanie danych z dysku, który został fizycznie uszkodzony.
	Wymóg przechowywania danych odzyskiwania w usługach AD DS	Uniemożliwienie użytkownikom włączenia funkcji BitLocker, chyba że komputer jest podłączony do domeny i

Stałe ustawienia napędu	
Opcje odzyskiwania danych z dysków stałych	To ustawienie pozwala kontrolować sposób odzyskiwania dysków stałych chronionych funkcją BitLocker w przypadku braku wymaganych poświadczeń. To ustawienie jest stosowane podczas konfiguracji funkcji BitLocker. Domyślnie dozwolony jest agent odzyskiwania danych oparty na certyfikatach, opcje odzyskiwania mogą być określone przez użytkownika, w tym hasło odzyskiwania i klucz odzyskiwania, a informacje o odzyskiwaniu nie są archiwizowane w usługach AD DS.
Agent odzyskiwania danych oparty na certyfikacie blokowym	
Ustawienia hasła odzyskiwania funkcji BitLocker	
Ustawienia klucza odzyskiwania BitLocker	
Zapisywanie informacji o odzyskiwaniu funkcji BitLocker w Usługach domenowych w usłudze Active Directory	
Konfiguracja magazynu odzyskiwania AD DS BitLocker	Przechowywanie pakietu kluczy wspomaga odzyskiwanie danych z dysku, który został fizycznie uszkodzony.
Wymóg przechowywania danych odzyskiwania w usługach AD DS	Zapobieganie włączaniu funkcji BitLocker przez użytkowników, chyba że komputer jest podłączony do domeny, a kopia zapasowa informacji odzyskiwania funkcji BitLocker w usługach AD DS powiedzie się. Uwaga: Hasło odzyskiwania jest generowane automatycznie.
Odmowa dostępu do zapisu na niezabezpieczonych dyskach stałych	

Ustawienia dysku wymiennego	
Odmowa dostępu do zapisu na niezabezpieczonych dyskach wymiennych	Odmowa dostępu do zapisu na wymiennych dyskach danych, które nie są chronione przez Bitlocker. Uwaga: Jeśli opcja "Dyski wymienne: Odmów dostępu do zapisu" jest włączona w zasadach grupy, to ustawienie zasad zostanie zignorowane.
Odmowa dostępu do zapisu na urządzeniach skonfigurowanych w innej organizacji	Tylko dyski z polami identyfikacyjnymi pasującymi do pól identyfikacyjnych komputera otrzymają dostęp do zapisu. Pola te są definiowane przez ustawienie zasad grupy "Podaj unikatowe identyfikatory dla organizacji".

Stan funkcji BitLocker

Tutaj możesz zobaczyć aktualny stan dysków zaszyfrowanych funkcją BitLocker

C [OS Drive]
Status szyfrowania
Zaszyfrowane (%)
Status ochrony
Metoda szyfrowania
Ochraniacze na klucze
Hasło odzyskiwania

Kliknięcie przycisku "Obróć hasło odzyskiwania" umożliwia obrócenie hasła odzyskiwania BitLocker.

Zarządzanie certyfikatami

Lista certyfikatów

Tutaj znajduje się lista certyfikatów zainstalowanych na wyświetlanym urządzeniu.

Konfiguracja certyfikatu

W tym miejscu można skonfigurować certyfikaty i sposób ich instalacji na urządzeniu.

Zaufany certyfikat	
Opis	Opis certyfikatu
Zakres	Zakres wdrożenia certyfikatu: Bieżący użytkownik vs Urządzenie
Magazyn certyfikatów	"Niezaufane certyfikaty" są dostępne tylko w systemie Windows 10 w wersji 1803.
Plik certyfikatu	Prześlij plik PKCS#1

Certyfikat tożsamości			
Opis	Opis certyfikatu		
Zakres	Zakres wdrożenia certyfikatu: Bieżący użytkownik vs Urządzenie		
Kluczowa lokalizacja	Dostawca magazynu kluczy do zainstalowania klucza prywatnego.		
		TPM. Niepowodzenie w przypadku braku modułu TPM	
	TPM. Jeśli nie ma TPM, następuje powrót do Software KSP		
	Dostawca oprogramowania do przechowywania kluczy	Oznacz klucz prywatny jako eksportowalny	
	Windows Hello dla firm	Nazwa pojemnika	Określa nazwę kontenera Windows Hello for Business (wcześniej znanego jako Microsoft Passport for Work).
		Tekst monitu o kod PIN	Określa niestandardowy tekst wyświetlany w monicie PIN usługi Windows Hello dla Firm podczas rejestracji certyfikatu.
Poświadczenie	Prześlij plik PKCS#12		

SCEP

Opis	Opis serwera SCEP		
Zakres wdrożenia	Zakres wdrożenia certyfikatu: Bieżące urządzenie vs Użytkownik		
Adresy URL serwerów SCEP	Jeden lub więcej serwerów wystawiających certyfikaty za pośrednictwem SCEP		
Przedmiot	Reprezentacja nazwy X.500. Np. "C=US, O=Microsoft Corporation, CN=foo, 1.2.5.3=bar".		
Alternatywne nazwy przedmiotów	Typ	Adres e-mail	
		DNS	
		URI	
		Główna nazwa użytkownika (UPN)	
Odcisk palca CA	Odcisk palca SHA1 certyfikatu urzędu certyfikacji. E.g. 31:8F:1E:78:5C:D5:12:9F:7E:3B:AD:F3:1C:C0:19:03:96:43:A9:E5		
Jednostki okresu ważności	Dni, miesiące lub lata		
Okres ważności			
Wyzwanie	Używany jako wstępnie udostępniony klucz tajny do automatycznej rejestracji.		
Próby	Liczba prób ponawianych przez urządzenie, jeśli serwer wyśle odpowiedź PENDING. Domyślna wartość to 5. Maksymalna wartość to 30.		
Opóźnienie ponowienia próby	Liczba minut oczekiwania przed ponowieniem próby. Wartość domyślna to 5. Wartość minimalna to 1.		
Rozmiar klucza	Rozmiar klucza w bitach		
Algorytm Hash	Rodzina algorytmów Hash		
Kluczowe zastosowanie	Rozszerzenie użycia klucza określa cel (np. szyfrowanie, podpis) klucza zawartego w certyfikacie. Należy wybrać co najmniej jedną z opcji "Podpis cyfrowy" lub "Szyfrowanie klucza".		
Rozszerzone użycie klucza	Określa rozszerzone użycie klucza. Podlega konfiguracji serwera SCEP. Określa listę odpowiednich identyfikatorów OID, np. 1.3.6.1.5.5.7.3.2 (uwierzytelnianie klienta).		

Kluczowa lokalizacja	Dostawca magazynu kluczy do zainstalowania klucza prywatnego.		
		TPM. Niepowodzenie w przypadku braku modułu TPM	
	TPM. Jeśli nie ma TPM, następuje powrót do Software KSP		
	Dostawca oprogramowania do przechowywania kluczy		
	Windows Hello dla firm	Nazwa pojemnika	Określa nazwę kontenera Windows Hello for Business (wcześniej znanego jako Microsoft Passport for Work).
		Tekst monitu o kod PIN	Określa niestandardowy tekst wyświetlany w monicie PIN usługi Windows Hello dla Firm podczas rejestracji certyfikatu.

Zarządzanie połączeniami

Wifi

Przy tym ustawieniu należy przeprowadzić wstępną konfigurację urządzeń użytkowników końcowych w celu uzyskania dostępu do wewnętrznych punktów dostępowych

Identyfikator zestawu usług (SSID)	SSID sieci, z którą zostanie nawiązane połączenie
Automatyczne dołączanie	Aktywacja automatycznego dołączania do sieci
Ukryta sieć	Aktywuj, jeśli punkt dostępowy nie rozgłasza identyfikatora SSID

Typ zabezpieczenia

Ustalenie typu zabezpieczeń punktu dostępowego

Otwarty system WEP	
Hasło	Hasło do punktu dostępowego

WPA PSK	
Hasło	Hasło do punktu dostępowego

WPA EAP	
Typ uwierzytelniania	Typ uwierzytelniania, możliwy tylko z "PEAP-MSCAHPv2"
Szybkie ponowne połączenie	Urządzenia mogą przełączać się między punktami dostępowymi bez konieczności ponownego uwierzytelniania.
Dostęp dla gości	Użytkownik nie posiada konta i powinien zarejestrować się jako gość.
Kontrole kwarantanny	Klient musi przeprowadzać kontrole NAP (Network Access Protection) i udostępniać wyniki systemowi, który następnie decyduje, czy klient może się połączyć.
Wymagaj powiązania kryptograficznego	Uwierzytelnianie jest możliwe tylko poprzez Crypto Binding
Weryfikacja serwera	Klient sprawdza, czy certyfikat serwera jest ważny. Jeśli tak, połączenie zostanie nawiązane
Monit o certyfikaty	Umożliwia użytkownikowi akceptowanie niezaufanych certyfikatów.
Nazwy serwerów	Oferuje opcję wyświetlenia nazwy serwera RADIUS, który oferuje uwierzytelnianie i autoryzację sieci.

WPA2-PSK	
Hasło	Hasło AP

WPA2 EAP	
Typ uwierzytelniania	Typ uwierzytelniania, możliwy tylko z "PEAP-MSCAHPv2"
Szybkie ponowne połączenie	
Dostęp dla gości	
Kontrole kwarantanny	Aktywuje ochronę dostępu do sieci NAP
Wymagaj powiązania kryptograficznego	Uwierzytelnianie jest możliwe tylko poprzez Crypto Binding
Weryfikacja serwera	
Monit o certyfikaty	Monity o podanie zweryfikowanego certyfikatu serwera, nazwy lub uwierzytelnienia certyfikatu głównego (CA).
Nazwy serwerów	Lista serwerów, które powinny być zaufane przez urządzenia
Brak	Brak ustalonych zabezpieczeń
Użyj serwera proxy	Korzystanie z serwera proxy
Adres serwera	Adres serwera proxy
Port serwera	Port serwera serwera proxy

Użyj serwera proxy

Włącz korzystanie z serwera proxy.

Adres serwera	Adres serwera proxy używanego w tej sieci.
Port serwera	Port serwera proxy używany przez tę sieć.

Ograniczenia Wi-Fi

Tutaj można zdefiniować różne ograniczenia Wi-Fi.

Zezwalaj na WiFi	Zezwalaj/odmawiaj WiFi
Zezwalaj na udostępnianie Internetu	Zezwalaj na korzystanie z hotspotu
Zezwalaj na automatyczne łączenie z hotspotami WiFi Sense	Zezwalaj na automatyczne łączenie z hotspotami WiFi Sense
Zezwalaj na ręczną konfigurację Wi-Fi	Zezwalanie użytkownikowi na łączenie się z sieciami WiFi, które nie zostały zdefiniowane przez AppTec.
Częstotliwość skanowania WLAN	Ustala interwał skanowania sieci WLAN. Wyższa wartość zwiększa zdolność rozpoznawania sieci WIFI.

VPN

W tym miejscu należy wprowadzić odpowiednie ustawienia, aby skonfigurować połączenia VPN

Nazwa połączenia	Wskazana nazwa połączenia		
Typ VPN	Połączenie Per-App VPN służy do zabezpieczenia ruchu niektórych aplikacji.		
	VPN	Zawsze włączony	Spowoduje to automatyczne połączenie VPN podczas logowania i pozostanie połączone do momentu ręcznego rozłączenia przez użytkownika.
	VPN dla poszczególnych aplikacji	Aplikacje VPN	Definiowanie aplikacji korzystających z tego połączenia VPN
		Blokada aplikacji	Per-App Lockdown sprawia, że wybrane aplikacje mogą łączyć się tylko za pośrednictwem tego połączenia VPN. Ta funkcja zależy od Zapory systemu Windows Defender.
	Profil WIP	Domena WIP dla tego połączenia	Identyfikator Enterprise ID, który jest wymagany do połączenia tego profilu VPN z zasadami Windows Information Protection (WIP).

Typ połączenia

AppTec360 VPN	
Dla "AppTec360 VPN" wymagane jest, aby sideloading aplikacji był dozwolony. Włącz opcję "Allow App Sideloading" w "Security Management" → "Restriction Settings" → "Device Functionality".	
Konfiguracja bramy	Aby skonfigurować połączenie VPN z czarną listą, należy wybrać konfigurację VPN z określonym serwerem DNS. Konfigurację VPN można skonfigurować w sekcji "Ustawienia ogólne" → "Brama uniwersalna" → "Ustawienia VPN".

IKEv2		
Serwery	Lista serwerów VPN	
Tunel urządzenia	Włącz połączenie przed zalogowaniem użytkownika.	
Metoda uwierzytelniania	EAP	EAP XML
	Certyfikaty maszyn	
Algorytm szyfrowania		
Algorytm sprawdzania integralności		
Grupa Diffiego-Hellmana		
Algorytm transformacji szyfru		
Algorytm transformacji uwierzytelniania		
Grupa PFS (Perfect Forward Secrecy)		

PPTP		
Serwery	Lista serwerów VPN	
Metoda uwierzytelniania	EAP	EAP XML

L2TP		
Serwery	Lista serwerów VPN	
Metoda uwierzytelniania	EAP	EAP XML
Algorytm szyfrowania		
Algorytm sprawdzania integralności		
Grupa Diffiego-Hellmana		
Algorytm transformacji szyfru		
Algorytm transformacji uwierzytelniania		
Grupa PFS (Perfect Forward Secrecy)		

Automatyczny		
Serwery	Lista serwerów VPN	
Metoda uwierzytelniania	EAP	EAP XML

Ogólne konfiguracje VPN

Zapamiętywanie poświadczeń przy każdym logowaniu	
Rejestrowanie adresów IP w wewnętrznym systemie DNS	
Reguły filtrowania ruchu sieciowego	Ograniczenie połączenia VPN do zdefiniowanego zestawu reguł.
Lista wyszukiwania sufiksów DNS	Sufiksy DNS do dodania do listy wyszukiwania DNS dla routingu nazw skróconych.
Reguły tabeli zasad rozpoznawania nazw (NRPT)	Reguły tabeli zasad rozpoznawania nazw (NRPT) definiują sposób, w jaki DNS rozpoznaje nazwy po połączeniu z VPN.
Wykrywanie zaufanej sieci	Lista sufiksów DNS do identyfikacji zaufanej sieci.
Dzielone tunelowanie	Dzielone tunelowanie oznacza, że ruch może przechodzić przez dowolny interfejs określony przez stos sieciowy.
Podzielone trasy tunelowania	Lista tras, które mają zostać dodane do tablicy routingu dla interfejsu VPN.
Konfiguracja proxy	Konfiguruje serwer proxy używany w tej sieci
Adres pełnomocnika	Adres serwera proxy jako w pełni kwalifikowana nazwa hosta lub adres IP.
Port	Port serwera proxy.
Adres URL autokonfiguracji serwera proxy	URL, aby automatycznie pobrać ustawienia proxy.

Ograniczenia VPN

Tutaj można zdefiniować różne ograniczenia VPN.

Zezwalaj na ustawienia VPN	Niniejsze wytyczne umożliwiają/zabraniają użytkownikowi dezaktywację i zmianę ustawień VPN
Zezwalaj na VPN przez sieć komórkową	Zezwala/zabrania urządzeniu na ustanowienie połączenia VPN, jeśli urządzenie korzysta z danych mobilnych.
Zezwalaj na roaming VPN przez sieć komórkową	Zezwala/zabrania urządzeniu na ustanowienie połączenia VPN, jeśli urządzenie jest w roamingu.

Bluetooth

Tutaj można ustalić, czy Bluetooth powinien być dozwolony/zabroniony.

Zezwalaj na Bluetooth	Aktywacja/dezaktywacja Bluetooth

Zarządzanie PIM

Exchange Active Sync

Konfiguracja konta ActiveSync na urządzeniu użytkownika końcowego

Nazwa konta	Nazwa konta e-mail
Nazwa hosta serwera	Adres serwera/FQDN
Nazwa domeny	Domena serwera
Adres e-mail	Adres e-mail
Nazwa użytkownika	Nazwa użytkownika
Hasło użytkownika	Opcjonalnie można już tutaj dołączyć hasło do użytkownika
Używanie protokołu SSL	Użyj połączenia SSL
Interwał synchronizacji	Tutaj można ustalić interwał synchronizacji Synchronizacja ręczna = użytkownik musi pobrać swoje wiadomości e-mail i przeprowadzić ręczną synchronizację.
Filtr wieku poczty	Czas, po którym wiadomości e-mail powinny zostać zsynchronizowane Brak filtra = nieograniczony
Poziom dziennika	Ustanowienie poziomów rejestrowania dla ruchu ActiveSync
Synchronizacja poczty e-mail	Aktywowany = wiadomości e-mail są synchronizowane
Synchronizacja kontaktów	Aktywowane = kontakty są zsynchronizowane
Synchronizacja kalendarza	Aktywowany = kalendarz jest zsynchronizowany
Synchronizacja zadań	Aktywowany = zadania są zsynchronizowane

eMail

Utworzenie kont POP3/IMAP4 na urządzeniu użytkownika końcowego.

Opis konta	Nazwa konta e-mail
Nazwa nadawcy	Wyświetlana nazwa nadawcy
Nazwa domeny	Nazwa domeny dla konta e-mail
Adres e-mail	Adres e-mail użytkownika
Nazwa użytkownika	Nazwa użytkownika
Hasło użytkownika	Opcjonalnie można już tutaj dołączyć hasło do użytkownika
Alternatywne poświadczenia serwera wychodzącego	W tym miejscu można zdefiniować, czy wymagane są inne dane uwierzytelniające dla serwera wychodzącego
Nazwa domeny wychodzącej	Nazwa domeny wychodzącej
Nazwa użytkownika serwera wychodzącego	Nazwa użytkownika serwera wychodzącego
Hasło serwera wychodzącego	Hasło serwera wychodzącego
Protokół e-mail	POP3 lub IMAP4, może być używany jako protokół
Nazwa hosta serwera poczty przychodzącej	Nazwa hosta serwera poczty przychodzącej
Używanie protokołu SSL dla poczty przychodzącej	Używanie protokołu SSL dla przychodzących wiadomości e-mail
Nazwa hosta serwera poczty wychodzącej	Nazwa hosta serwera poczty wychodzącej
Używanie protokołu SSL dla poczty wychodzącej	Używanie protokołu SSL dla wychodzących wiadomości e-mail
Uwierzytelnianie serwera wychodzącego	Wymagane jest uwierzytelnienie serwera wychodzącego
Interwał synchronizacji	Tutaj można ustalić interwał synchronizacji Synchronizacja ręczna = użytkownik musi pobrać swoje wiadomości e-mail i przeprowadzić ręczną synchronizację.
Filtr wieku poczty	Czas, po którym wiadomości e-mail powinny zostać zsynchronizowane Brak filtra = nieograniczony

Zarządzanie aplikacjami

Menedżer aplikacji dla przedsiębiorstw

Zainstalowane aplikacje

Oto lista aplikacji, które są obecnie zainstalowane na wyświetlanym urządzeniu.

Aplikacje obowiązkowe

Tutaj można skonfigurować listę aplikacji, które są obowiązkowe na urządzeniu.

Lista ta będzie sprawdzana za każdym razem, gdy urządzenie połączy się z MDM i zainstaluje wszystkie aplikacje z tej listy, które nie są zainstalowane na urządzeniu, niezależnie od tego, czy aplikacja została odinstalowana, czy nigdy wcześniej nie była zainstalowana.

Możesz przesłać aplikacje wewnętrzne Windows 10, a następnie dodać je do tej listy lub dodać konfiguracje Microsoft Office, które należy wcześniej skonfigurować w "Ustawieniach ogólnych" > "Zarządzaniu aplikacjami" > "Microsoft Office".

Ograniczenia aplikacji systemowych

Aplikacje Inbox
Zezwalaj na alarmy i zegar
Kalkulator zezwoleń
Zezwól na kamerę
Zezwól na kontakt z pomocą techniczną
Zezwól Cortanie
Zezwalaj na Eksploratora plików
Zezwól na rozpoczęcie
Allow Groove Music
Zezwalaj na mapy
Zezwalaj na przesyłanie wiadomości
Zezwól Microsoft Edge
Dozwolone filmy i telewizja
Pozwól na pieniądze
Zezwalaj na wiadomości
Zezwalaj na OneDrive
Zezwól OneNote
Zezwalaj na kalendarz i pocztę programu Outlook
Pozwól ludziom
Zezwól na telefon
Zezwalaj na zdjęcia
Zezwalaj na Powerpoint
Zezwalaj na ustawienia
Zezwól Skype
Pozwól na sport
Allow Store
Zezwalaj na nagrywanie głosu
Zezwalaj na portfel
Zezwalaj na pogodę

Zezwalaj na usługę Windows Feedback Hub
Allow Word
Zezwól Xbox

Strony ustawień
Zezwalaj na konta w miejscu pracy
Zezwalaj na zaawansowane informacje
Kącik dozwolonych aplikacji
Zezwalaj na blokowanie i filtrowanie
Zezwalaj na profil kolorów
Zezwalaj na tryb jazdy
Zezwalaj na pocztę e-mail i konta
Zezwalaj na korektor
Zezwalaj na klawiaturę
Zezwalaj na pasek nawigacji
Zezwalaj na tryb samolotowy sieci
Zezwalaj na udostępnianie Internetu w sieci
Zezwalaj na usługi sieciowe
Zezwalaj na sieć Wi-Fi
Zezwól systemowi PC na Bluetooth
Zezwalaj na ocenianie urządzenia
Zezwalaj na przywrócenie aktualizacji
Zezwalaj na udostępnianie
Zezwalaj na start
Dozwolony czas Język
Dozwolony czas Region
Zezwalaj na domyślny ekran blokady systemu Windows
Zezwól na pracę lub konto szkolne

Czarna i biała lista

W sekcji "Czarna i biała lista" można wybrać między trybem "Biała lista" i trybem "Czarna lista".

Biała lista	Tylko aplikacje i usługi dodane do listy mogą zostać zainstalowane na urządzeniu użytkownika końcowego. Jeśli są one już wstępnie zainstalowane na urządzeniu użytkownika końcowego, zostaną aktywowane i ustawione, aby użytkownik mógł je uruchomić.
	Wszystkie inne aplikacje, które nie zostały dodane do listy, nie mogą być instalowane na urządzeniu użytkownika końcowego. Jeśli są one już wstępnie zainstalowane na urządzeniu użytkownika końcowego, zostaną dezaktywowane i ustawione tak, aby użytkownik nie mógł ich uruchomić.
Czarna lista	Aplikacje i usługi dodane do listy nie mogą być instalowane na urządzeniu użytkownika końcowego. Jeśli są one już wstępnie zainstalowane na urządzeniu użytkownika końcowego, zostaną dezaktywowane i ustawione tak, aby użytkownik nie mógł ich uruchomić.
	Wszystkie inne aplikacje, które nie zostały dodane do listy, mogą zostać zainstalowane na urządzeniu użytkownika końcowego. Jeśli są one już wstępnie zainstalowane na urządzeniu użytkownika końcowego, zostaną aktywowane i ustawione, aby użytkownik mógł je uruchomić.

Za pomocą przycisku można dodać dodatkowe aplikacje lub usługi do aktualnie używanej listy.

Za pomocą przycisku można dodać dodatkowe aplikacje lub usługi do aktualnie nieaktywnej listy.

Możesz dodać aplikację z "Windows App Store" lub bezpośrednio wprowadzić "Identyfikator aplikacji", aby dodać ją do czarnej lub białej listy.

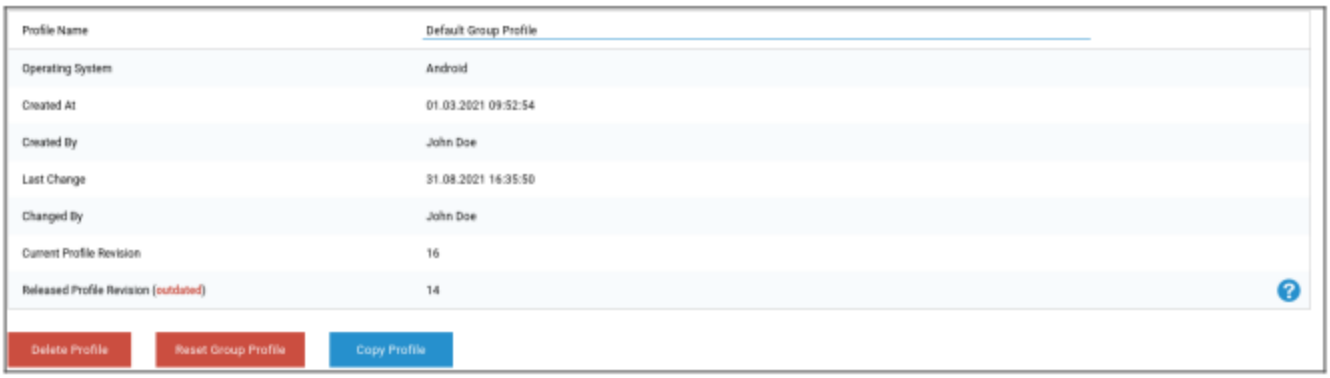
Konfiguracja macOS

W zależności od tego, czy wybrano profil, czy urządzenie, wyświetlanie i jego podpunkty różnią się - należy zwrócić na to szczególną uwagę!

Ogólne

Przegląd profilu grupy (tylko na poziomie grupy)

Po otwarciu profilu grupy wyświetlony zostanie szybki przegląd profilu.



Nazwa profilu	Nazwa profilu (można ją zmienić tutaj)
System operacyjny	System operacyjny, dla którego przeznaczony jest profil
Utworzono w	Czas stworzenia
Utworzony przez	Twórca profilu
Ostatnia zmiana	Czas ostatniej zmiany profilu
Zmienione przez	Konto, które wprowadziło ostatnie zmiany
Aktualna wersja profilu	Zmiana zapisanego stanu profilu
Wydana wersja profilu	Wersja przypisanego profilu ("Przypisz teraz"). Jeśli etykieta pokazuje "(nieaktualne)" za tekstem, oznacza to, że profil został zapisany, ale nie został jeszcze przypisany, więc urządzenia nadal będą otrzymywać starszą wersję.

Przegląd urządzeń (tylko na poziomie urządzenia)

Podsumowanie urządzenia.

Nazwa urządzenia	Nazwa urządzenia
Model	Model
System operacyjny	System operacyjny
Numer seryjny	Numer seryjny urządzenia
Własność urządzenia	Skonfigurowany typ własności
Typ urządzenia	Typ urządzenia
Zgodność	Pokazuje, czy urządzenie jest zgodne
Adres IP	Adres IP, z którego urządzenie łączy się z serwerem
Ostatnio widziany	Czas ostatniego połączenia z urządzenia
Last Push	Czas ostatniego naciśnięcia wysłanego do urządzenia
Przydział	W tym miejscu można przenieść urządzenie do innego użytkownika lub grupy.

Wersja konfiguracji (tylko na poziomie urządzenia)

W tym miejscu wyświetlany jest przegląd profili grupowych przypisanych do urządzenia.

Jeśli klikniesz profil grupy, uzyskasz do niego bezpośredni dostęp i będziesz mógł dokonać ustawień.

Za pomocą symbolu można przywrócić przypisane aplikacje do ustawień profilu grupy.

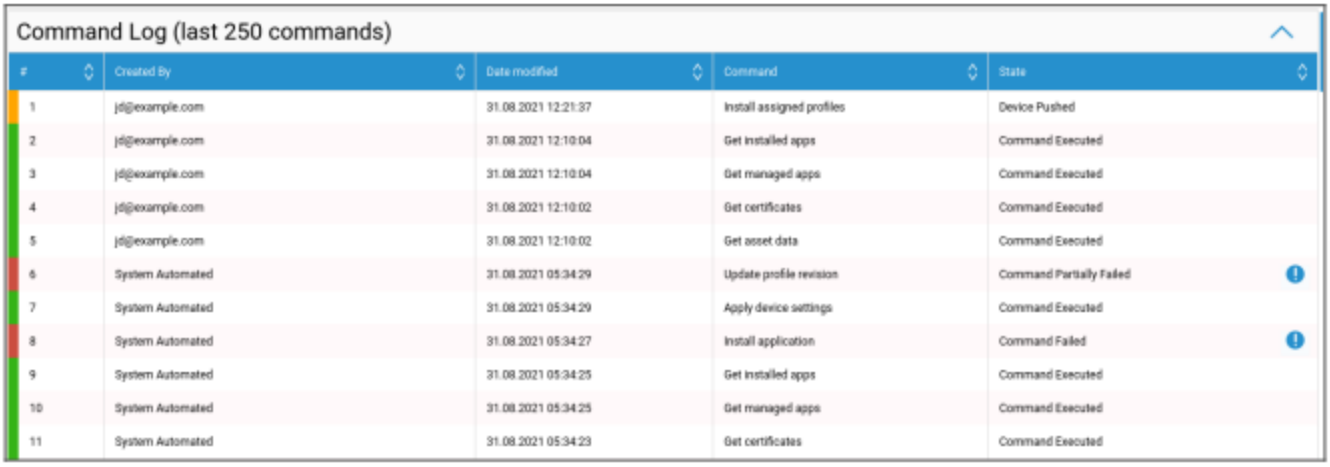
Za pomocą symbolu można zresetować profil urządzenia, aby nie miał żadnych ustawień.

"Newer Revision available" oznacza, że profil grupy został zmieniony i zapisany, ale nie został przypisany. Profil grupy musi zostać przypisany za pomocą opcji "Przypisz teraz" na poziomie grupy, aby zastosować zmiany do urządzeń.

Dziennik urządzenia (tylko na poziomie urządzenia)

Dziennik poleceń

Tutaj można sprawdzić, które polecenia zostały wydane dla urządzenia i jaki jest ich status.



Polecenia utworzone przez "System Automated" są automatycznie tworzone przez system.

Możliwe statusy poleceń

Urządzenie wciśnięte	Żądanie push zostało wysłane do usługi push (np. APNS), aby poinformować urządzenie o konieczności połączenia się z serwerem EMM.
Utworzone polecenie	Polecenie zostało utworzone w systemie.
Wysłane polecenie	Polecenie zostało wysłane do urządzenia po nawiązaniu połączenia z serwerem.
Polecenie wykonane	Polecenie zostało pomyślnie wykonane.
Polecenie nie powiodło się	Polecenie nie powiodło się. *
Polecenie częściowo nieudane	W zależności od systemu operacyjnego urządzenia niektóre polecenia mogą zostać zgrupowane. W tym przypadku niektóre części tej grupy poleceń nie powiodły się. *
Polecenie wykonane, ostatecznie nieudane	Polecenie zostało wykonane, ale być może nie.
Przesunięcie polecenia	Polecenie zostało powtórzone przez użytkownika.
Odrzucony	Polecenie zostało odrzucone. Na przykład dlatego, że zostało zastąpione przez inne polecenie lub urządzenie zostało ponownie zarejestrowane, a stare polecenia zostały usunięte.

*Jeśli za wiadomością znajduje się wykrzyknik, możesz uzyskać więcej informacji, najeżdżając kursorem na ikonę.

Zarządzanie zasobami (tylko na poziomie urządzenia)

Informacje o urządzeniu

Numer modelu	Numer modelu
Nazwa hosta	Nazwa hosta
Lokalna nazwa hosta	Lokalna nazwa hosta
System operacyjny	System operacyjny
Wersja systemu operacyjnego	Wersja systemu operacyjnego
UDID	UDID
Pamięć wolna / całkowita	Pamięć wolna / całkowita

WiFi

Adres IP	Adres IP
WiFi MAC	WiFi MAC

Komórkowy

Numer telefonu	Numer telefonu
Status roamingu	Status roamingu
Roaming (połączenia głosowe / transmisja danych)	Roaming (połączenia głosowe / transmisja danych)
Adres IP	Adres IP
Operator/Przewoźnik	Operator/Przewoźnik
SIM Sieć operatora	Sieć operatora
Wersja dla przewoźników	Wersja dla przewoźników
ICCID	ICCID
Obecny MCC/MNC	Obecny MCC/MNC
SIM MCC/MNC	SIM MCC/MNC

Bluetooth

Bluetooth MAC	Bluetooth MAC

Zarządzanie aktualizacjami (tylko na poziomie urządzenia)

Informacje o aktualizacji

Na tej karcie wyświetlane są informacje o ustawieniach aktualizacji systemu na urządzeniu.

Autokontrola włączona	Jeśli system automatycznie sprawdza dostępność aktualizacji.
Automatyczna aktualizacja aplikacji włączona	Jeśli system będzie automatycznie instalował aktualizacje aplikacji.
Włączone automatyczne aktualizacje systemu operacyjnego	Jeśli system będzie automatycznie instalował aktualizacje systemu operacyjnego.
Automatyczne aktualizacje zabezpieczeń włączone	Jeśli system będzie automatycznie instalował aktualizacje zabezpieczeń.
Włączona funkcja pobierania w tle aktualizacji aplikacji	Jeśli system będzie pobierał aktualizacje aplikacji w tle.
Adres URL katalogu	Adres URL katalogu aktualizacji oprogramowania używanego przez klienta.
Jest domyślnym katalogiem	Jeśli "tak", katalog jest katalogiem domyślnym.
Przeprowadzanie okresowych kontroli	Jeśli "tak", rozpocznij nowe skanowanie.
Data poprzedniego skanowania	Data ostatniego skanowania aktualizacji oprogramowania.
Wynik poprzedniego skanowania	Kod wyniku ostatniego skanowania aktualizacji oprogramowania.

Zarządzanie bezpieczeństwem

Ochrona przed kradzieżą

Wipe & Lock

Pełne wytarcie	Wysłanie polecenia przywrócenia ustawień fabrycznych urządzenia
Enterprise Wipe	Usunąć MDM z urządzenia i usunąć wszystkie dane MDM (np. konta, aplikacje).
Ekran blokady	Powrót urządzenia do ekranu blokady

Konfiguracja zabezpieczeń

Kod dostępu

Dozwolona dezaktywacja kodu	Określa, czy użytkownik jest zmuszony do ustawienia kodu PIN. Samo ustawienie tej wartości (a nie innych) wymusza na użytkowniku wprowadzenie kodu dostępu, bez narzucania długości lub jakości.
Zezwalaj na prostą wartość	Zezwalanie użytkownikowi na używanie tych samych, rosnących i malejących ciągów numerów (np. 1234, 1111).
Wymagana wartość alfanumeryczna	Hasła muszą zawierać co najmniej jedną literę
Minimalna długość kodu dostępu	Minimalna długość hasła
Minimalna liczba złożonych znaków	Minimalna liczba symboli alfanumerycznych w haśle
Maksymalny wiek kodu dostępu	Liczba dni, po których hasło musi zostać zmienione
Maksymalna automatyczna blokada	Maksymalny czas, po którym urządzenie zostanie zablokowane
Maksymalny okres karencji dla blokady urządzenia	Czas, przez jaki urządzenie może być zablokowane bez konieczności podawania hasła przy odblokowywaniu.
Maksymalny wiek kodu dostępu (1-730 dni lub brak)	Dni, po których należy zmienić hasło
Historia kodów dostępu (1-50 kodów lub brak)	Liczba unikalnych kodów przed ponownym użyciem

Certyfikat

PKCS#1	
Opis	Wprowadź opis certyfikatu
Poświadczenie	Prześlij plik pkcs1

PKCS#12	
Opis	Wprowadź opis certyfikatu
Poświadczenie	Prześlij plik pkcs12

Ustawienia ograniczeń

Funkcjonalność urządzenia

Zezwól na kamerę	Zezwalaj na korzystanie z kamery
Zezwól na Game Center	Gdy wartość ta jest fałszywa, Game Center jest wyłączone, a jego ikona jest usuwana z ekranu głównego.
Umożliwienie gry wieloosobowej	Gdy fałsz, zabrania gry wieloosobowej.
Zezwalaj na dodawanie znajomych z Game Center	Gdy wartość jest fałszywa, zabrania dodawania znajomych do Game Center.
Zezwalanie na korzystanie z biblioteki zdjęć iCloud	Ustawienie wartości false powoduje wyłączenie Biblioteki zdjęć iCloud. Wszystkie zdjęcia, które nie zostały w pełni pobrane z Biblioteki zdjęć iCloud na urządzenie, zostaną usunięte z pamięci lokalnej.
Zezwalaj na Touch ID	Jeśli fałsz, uniemożliwia Touch ID odblokowanie urządzenia.

iCloud

Blokowanie niektórych funkcji podczas parowania iCloud

Zezwalaj na synchronizację dokumentów	Zezwalaj na synchronizację dokumentów
Zezwalanie na synchronizację pęku kluczy iCloud	Zezwalanie na synchronizację pęku kluczy iCloud
Zezwalanie na Notatki iCloud	Gdy wartość jest fałszywa, wyłącza usługi MacOS iCloud Notes.
Zezwalanie na BTMM iCloud	Gdy wartość ta jest fałszywa, wyłącza usługę MacOS Back to My Mac iCloud.
Zezwalaj na FMM iCloud	Gdy wartość ta jest fałszywa, wyłącza usługę iCloud Znajdź mój Mac w systemie MacOS.
Zezwalaj na zakładki iCloud	Gdy wartość ta jest fałszywa, wyłącza synchronizację zakładek iCloud w systemie MacOS.
Zezwalanie na korzystanie z aplikacji iCloud Mail	Fałsz powoduje wyłączenie usług iCloud w aplikacji MacOS Mail.

Zezwalanie na Kalendarz iCloud	Gdy wartość ta jest fałszywa, wyłącza usługi iCloud w chmurze systemu MacOS.
Zezwalanie na przypomnienia iCloud	Gdy wartość ta jest fałszywa, wyłącza usługi Przypomnienia iCloud.
Zezwalanie na korzystanie z książki adresowej iCloud	Gdy wartość ta jest fałszywa, wyłącza usługi książki adresowej iCloud systemu MacOS.

Zarządzanie mediami

Wysuwanie przy wylogowaniu	Wysuwanie wszystkich nośników wymiennych przy wylogowywaniu
Zezwalaj na sieć	Zezwalaj na dostęp do nośników sieciowych
Zezwalaj na dysk wewnętrzny	Zezwól na dostęp do dysku wewnętrznego.
Wymagaj uwierzytelnienia	Wymagaj uwierzytelnienia do korzystania z tego nośnika
Tylko do odczytu	Użytkownik może jedynie odczytywać dane z nośnika
Zezwalaj na dysk zewnętrzny	Zezwól na dostęp do dysku zewnętrznego.
Wymagaj uwierzytelnienia	Wymagaj uwierzytelnienia do korzystania z tego nośnika
Tylko do odczytu	Użytkownik może jedynie odczytywać dane z nośnika
Zezwalaj na korzystanie z obrazów dysków	Zezwalaj na dostęp do obrazów.
Wymagaj uwierzytelnienia	Wymagaj uwierzytelnienia do korzystania z tego nośnika
Tylko do odczytu	Użytkownik może jedynie odczytywać dane z nośnika
Zezwalaj na korzystanie z dysków DVD-RAM	Zezwól na dostęp do dysku DVD-RAM.
Wymagaj uwierzytelnienia	Wymagaj uwierzytelnienia do korzystania z tego nośnika
Tylko do odczytu	Użytkownik może jedynie odczytywać dane z nośnika
Zezwalaj na korzystanie z płyt DVD	Zezwól na dostęp do dysku DVD.
Wymagaj uwierzytelnienia	Wymagaj uwierzytelnienia do korzystania z tego nośnika
Zezwalaj na korzystanie z płyt CD	Zezwól na dostęp do dysku CD.
Wymagaj uwierzytelnienia	Wymagaj uwierzytelnienia do korzystania z tego nośnika

Zarządzanie połączeniami

Wi-Fi

Tutaj można dodawać i konfigurować połączenia Wi-Fi

Identyfikator zestawu usług (SSID)	SSID sieci, z którą zostanie nawiązane połączenie
Automatyczne dołączanie	Włącz automatyczne dołączanie do sieci
Ukryta sieć	Włącz, jeśli punkt dostępowy nie rozgłasza identyfikatora SSID.
Konfiguracja proxy	Konfiguracja serwera proxy dla każdego punktu dostępowego
Brak	Nie używaj serwera proxy
Podręcznik	Ustanowienie ręcznego pełnomocnika
Adres URL serwera proxy	Adres dostępu do ustawień serwera proxy
Port	Ustalenie portu dla serwera proxy
Uwierzytelnianie	Nazwa użytkownika do uwierzytelniania na serwerze proxy
Hasło	Hasło do uwierzytelniania na serwerze proxy
Automatyczny	Automatyczne ustanowienie serwera proxy
Adres URL serwera proxy	Adres URL pliku ustawień serwera proxy
Typ zabezpieczenia	Ustalenie typu zabezpieczeń dla punktu dostępowego
WEP	
Hasło	Hasło do punktu dostępowego
WPA/WPA2	
Hasło	Hasło do punktu dostępowego
WEP Enterprise - WPA / WPA2 Enterprise / Dowolne przedsiębiorstwo	Zobacz błąd tabeli: Nie znaleziono źródła poniżej
Brak	Brak zabezpieczeń

Wyłączanie randomizacji adresów MAC	Wyłącza randomizację adresów MAC dla tej sieci Wi-Fi podczas powiązania z siecią. Powoduje to również wyświetlenie ostrzeżenia o prywatności w Ustawieniach, wskazującego, że sieć ma ograniczoną ochronę prywatności.

Konfiguracja sieci Wi-Fi w przedsiębiorstwie

Uwaga: Dostępne tylko wtedy, gdy "Typ zabezpieczeń" jest ustawiony na typ Enterprise.

Protokoły	Protokół uwierzytelniania obsługiwany w sieci docelowej
TLS	Włączanie / wyłączanie użycia
TTLS	Włączanie / wyłączanie użycia
Uwierzytelnianie wewnętrzne	Protokół uwierzytelniania, który powinien być używany: PAP, CHAP, MSCHAP, MSCHAPv2
LEAP	Włączanie / wyłączanie użycia
PEAP	Włączanie / wyłączanie użycia
EAP-FAST	Włączanie / wyłączanie użycia
EAP-SIM	Włączanie / wyłączanie użycia
Korzystanie z PAC	Korzystanie z PAC (chronionej kontroli dostępu)
Przepis PAC	Konfiguracja Provision PAC
Udostępnianie PAC anonimowo	Anonimowe dostarczanie PAC
Uwierzytelnianie	
Nazwa użytkownika	Nazwa użytkownika uwierzytelniania
Nie używaj Na połączenie Hasło	Nie używaj hasła na połączenie
Hasło	Hasło do użycia
Certyfikat tożsamości	Prześlij/wybierz certyfikat uwierzytelniania
Tożsamość zewnętrzna	Tożsamość widoczna na zewnątrz
Zaufanie	
Zaufany certyfikat 1	Prześlij pierwszy zaufany certyfikat
Zaufany certyfikat 2	Prześlij drugi zaufany certyfikat
Zaufany certyfikat 3	Prześlij trzeci zaufany certyfikat

Zaufany serwer Nazwy certyfikatów	Nazwy oczekiwanych certyfikatów serwera (na liście oddzielonej przecinkami)

VPN

W zależności od wybranego typu połączenia mogą być widoczne różne pola.

Nazwa połączenia	Nazwa profilu VPN
Typ VPN	
VPN	Cały ruch sieciowy urządzenia będzie kierowany przez połączenie VPN.
Typ połączenia	Ustanowienie typu połączenia VPN
IPsec (cisco)	Protokół IPsec firmy cisco
L2TP	Protokół L2TP
Niestandardowy SSL	Połączenie przez niestandardowy protokół SSL
IKEv2	Protokół IKEv2
Konfiguracja proxy	Konfiguracja serwera proxy dla połączenia VPN
Brak	Ustanowienie braku proxy
Podręcznik	Ręczne ustanowienie serwera proxy
Adres URL serwera proxy	Adres dostępu do ustawień proxy
Port	Ustalenie portu dla serwera proxy
Uwierzytelnianie	Nazwa użytkownika do uwierzytelniania na serwerze proxy
Hasło	Hasło do uwierzytelniania na serwerze proxy
Automatyczny	Automatyczne ustanowienie serwera proxy
Adres URL serwera proxy	Adres URL umożliwiający dostęp do ustawień serwera proxy

Serwer proxy HTTP

Typ proxy	
Podręcznik	Ręczne ustanowienie serwera proxy
Adres URL serwera proxy	Adres dostępu do ustawień serwera proxy
Port	Ustanowienie portu proxy
Uwierzytelnianie	Nazwa użytkownika do uwierzytelniania na serwerze proxy
Hasło	Hasło do uwierzytelniania na serwerze proxy
Automatyczny	Automatyczne ustanowienie serwera proxy
Adres URL serwera proxy PAC	Adres URL serwera proxy PAC
Zezwalaj na bezpośrednie połączenie, jeśli PAC jest nieosiągalny	Zezwalaj na bezpośrednie połączenie (bez VPN), jeśli PAC jest nieosiągalny.
Zezwalanie na omijanie proxy w celu uzyskania dostępu do sieci wewnętrznych	Zezwalanie na omijanie proxy w celu uzyskania dostępu do wewnętrznych sieci captive

AirPrint

Adres IP	Adres IP drukarki
Ścieżka zasobów	Określona ścieżka do urządzenia AirPrint

AirPlay

Nazwa urządzenia	Nazwa urządzenia
Hasło	Hasło parowania
Biała lista	Zdefiniuj listę urządzeń, z którymi urządzenie może się sparować na wyłączność.

Zarządzanie PIM

Exchange Active Sync

Nazwa konta	Nazwa konta.
Adres e-mail	Adres konta (np. max@company.com)
Nazwa hosta serwera	Wewnętrzna nazwa hosta
Nazwa logowania	"Domena" i "Nazwa logowania" muszą być puste, aby urządzenie wyświetliło monit o użytkownika.
Domena	"Domena" i "Nazwa logowania" muszą być puste, aby urządzenie wyświetliło monit o użytkownika. Jeśli włączona jest konfiguracja bramy ACL, a pole Domain nie jest puste, AppTec360 Universal Gateway uwierzytelni urządzenie przy użyciu następującej nazwy "Domain\Login Name".
Hasło	Hasło do konta (np. secretUserPassword)
Poprzednie dni Mail to Sync	Liczba ostatnich dni poczty do zsynchronizowania
Używanie protokołu SSL	Używanie protokołu SSL dla wewnętrznego hosta Exchange
Opcja zaawansowana	Pokaż opcje zaawansowane
Port serwera	Port wewnętrzny
Ścieżka serwera	Ścieżka wewnętrzna
Zewnętrzna nazwa hosta	Host zewnętrzny
Port zewnętrzny	Port zewnętrzny
Ścieżka zewnętrzna	Ścieżka zewnętrzna
Używanie protokołu SSL dla urządzeń zewnętrznych Host wymiany	Użyj SSL dla zewnętrznego hosta Exchange

eMail

Konfiguracja kont POP3 / IMAP na urządzeniu użytkownika końcowego

Opis konta	Nazwa konta e-mail
Typ konta	
IMAP	
Prefiks ścieżki	Prefiks ścieżki dla folderów specjalnych
POP	
Wyświetlana nazwa użytkownika	Wyświetlana nazwa użytkownika
Adres e-mail	Adres e-mail użytkownika

Poczta przychodząca	Ustawienia serwera przychodzącego
Adres serwera pocztowego	Adres serwera pocztowego
Port serwera poczty	Port serwera poczty
Nazwa użytkownika	Odpowiednia nazwa użytkownika
Typ uwierzytelniania	Typ uwierzytelniania
Brak	Brak typu uwierzytelniania
Hasło (tylko na poziomie urządzenia)	Monit o hasło
Wyzwanie - odpowiedź MDM	
NTLM	Uwierzytelnianie NTLM
HTTP MD5 Digest	
Używanie protokołu SSL	W razie potrzeby użyj protokołu SSL

Poczta wychodząca	Ustawienia serwera wychodzącego
Adres serwera pocztowego	Adres serwera pocztowego
Port serwera poczty	Port serwera poczty
Nazwa użytkownika	Odpowiednia nazwa użytkownika
Typ uwierzytelniania	
Brak	Brak metody uwierzytelniania
Hasło (tylko na poziomie urządzenia)	Monit o hasło
Wyzwanie - odpowiedź MDM	
NTLM	Uwierzytelnianie NTLM
HTTP MD5 Digest	
Używanie protokołu SSL	W razie potrzeby użyj protokołu SSL
Hasło wychodzące takie samo jak przychodzące	Hasło wychodzące takie samo jak przychodzące
Używać tylko w korespondencji	Aktywuj, jeśli wszystkie wychodzące wiadomości e-mail mają być wysyłane za pośrednictwem aplikacji Mail.

CalDav

Konfiguracja konfiguracji i dystrybucji konta CalDav

Opis konta	Wyświetlana nazwa konta
Nazwa hosta	Nazwa hosta i/lub adres IP
Port	Port konta CalDav
Główny adres URL	Główny adres URL konta
Nazwa użytkownika	Odpowiednia nazwa użytkownika CalDav
Hasło (tylko na poziomie urządzenia)	Odpowiednie hasło CalDav
Używanie protokołu SSL	W razie potrzeby użyj protokołu SSL

CardDav

Konfiguracja konfiguracji i dystrybucji konta CardDav

Opis konta	Wyświetlana nazwa konta
Nazwa hosta	Nazwa hosta i/lub adres IP
Port	Port konta CardDav
Główny adres URL	Główny adres URL konta
Nazwa użytkownika	Odpowiednia nazwa użytkownika CardDav
Hasło (tylko na poziomie urządzenia)	Odpowiednie hasło CardDav
Używanie protokołu SSL	W razie potrzeby użyj protokołu SSL

LDAP

W tym obszarze należy skonfigurować połączenie LDAP, aby umożliwić dynamiczną wymianę certyfikatów między urządzeniem użytkownika końcowego a usługą Active Directory.

Należy pamiętać, że wybrany użytkownik wymaga odpowiednich uprawnień do odczytu.

Opis konta	Opis konta
Nazwa użytkownika konta	Użytkownik dla dostępu LDAP
Hasło do konta	Hasło dostępu do protokołu LDAP
Nazwa hosta konta	Nazwa hosta/adres IP serwera LDAP
Używanie protokołu SSL	W razie potrzeby użyj protokołu SSL

W drugiej części można zdefiniować indywidualne filtry do wyszukiwania w rejestrze LDAP.

Opis	Zakres	Baza wyszukiwania
Opis filtra	Poziom wyszukiwania w rejestrze LDAP	Zdefiniuj filtr indywidualny

Pulpit nawigacyjny i raportowanie

Ustawienia pulpitu nawigacyjnego

Tutaj możesz zobaczyć, które pulpity nawigacyjne istnieją, edytować je lub tworzyć nowe. Każdy pulpit nawigacyjny ma własny zestaw danych do wyświetlenia i konfigurację wykresu.

Kontrola ustawień pulpitu nawigacyjnego

Publiczny	Ustawia pulpit nawigacyjny jako publiczny, aby inni użytkownicy mogli go zobaczyć. Użytkownicy muszą oczywiście mieć możliwość zalogowania się i przeglądania pulpitów nawigacyjnych. Jeśli opcja "Publiczny" nie jest aktywna, tylko twórca może go zobaczyć.
Domyślny	Ustawia pulpit nawigacyjny jako domyślny, aby automatycznie otwierał się przy następnym dostępie do widoku pulpitu nawigacyjnego.
	Wyświetlanie pulpitu nawigacyjnego i jego wykresów
	Usuwanie pulpitu nawigacyjnego
	Edycja nazwy i ustawień pulpitu nawigacyjnego
	Utwórz kopię pulpitu nawigacyjnego
	Dodaj zupełnie nowy pulpit nawigacyjny

Widok pulpitu nawigacyjnego

Wyświetla dane i wykresy wybranego pulpitu nawigacyjnego, a także umożliwia ich zmianę.

Kontrola pulpitu nawigacyjnego

	Pozwala określić, które dane mają być wyświetlane na pulpicie nawigacyjnym, ilość danych do wyświetlenia i rozmiar tych danych.
	Powoduje powrót do przeglądu pulpitu nawigacyjnego
	Przywraca domyślne ustawienia aktualnie otwartego pulpitu nawigacyjnego.
	Zapisuje wszystkie zmiany wprowadzone w aktualnie otwartym pulpicie nawigacyjnym (np. które dane mają być wyświetlane).
	Zmiana typu wykresu na wykres słupkowy
	Zmiana typu wykresu na wykres kołowy
	Zmiana typu wykresu na wykres pączkowy
	Zmiana typu wykresu na wykres obszaru biegunowego
	Zmiana kolejności sortowania

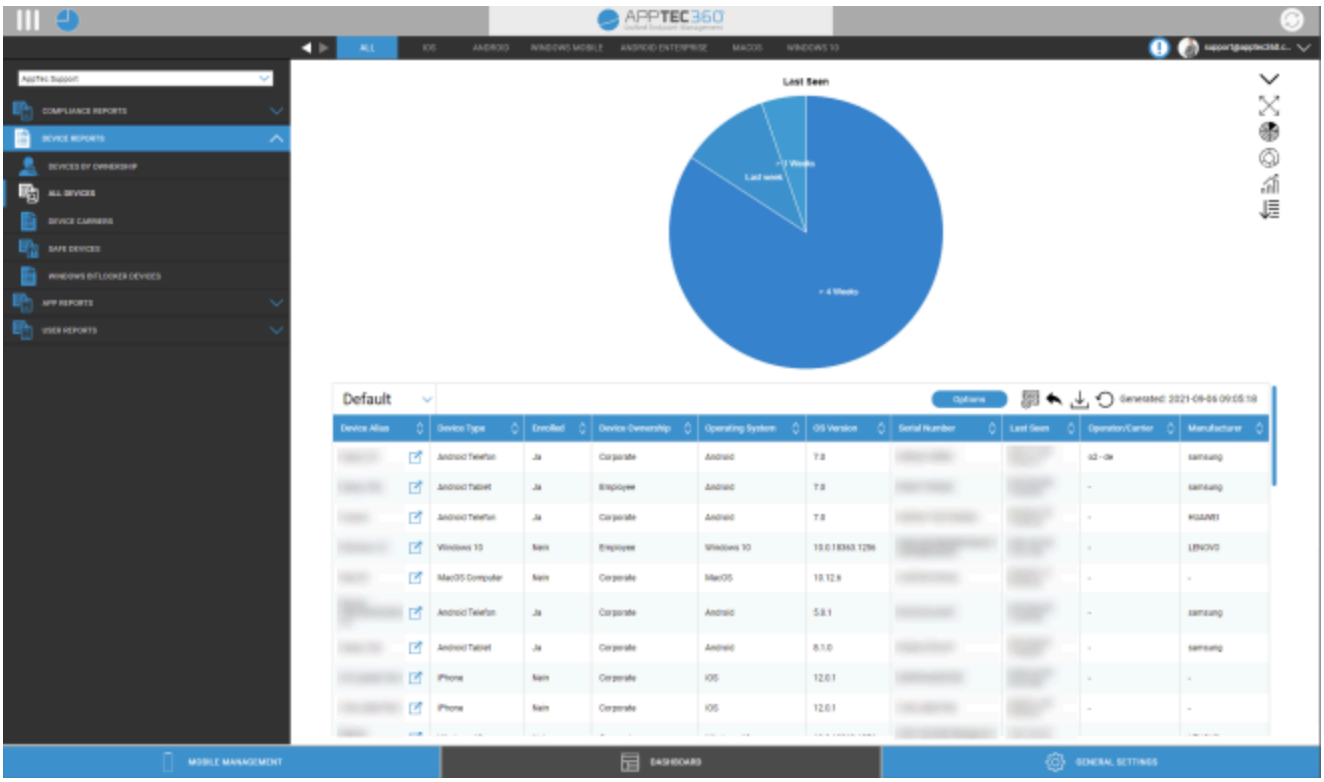
Rozszerzone raportowanie

"Rozszerzone raportowanie" oferuje szczegółowe przeglądy i wykresy dotyczące informacji o urządzeniach i użytkownikach.

Istnieje kilka domyślnych raportów, ale wszystkie z nich można ręcznie zmienić, aby dodać lub usunąć dane do wyświetlenia.

Należy pamiętać, że ręcznie można zmienić tylko te dane, które są wyświetlane. Wybrana kategoria raportu definiuje dane, na których jest on oparty. Np. nigdy nie będzie można zobaczyć urządzeń z systemem Android w raporcie iOS w kategorii Device Reports All Devices iOS.

W lewym górnym rogu można ograniczyć dane raportowania do określonej grupy (i wszystkich jej podgrup). Domyślnie jest to ustawione na węzeł główny, więc uwzględnia WSZYSTKIE urządzenia i użytkowników.



Rozszerzona kontrola raportowania

W każdym przeglądzie można użyć następujących funkcji, aby zmienić raport w dowolny sposób:

	Ukryj wykres (jeśli wykres jest wyświetlany)
	Pokaż wykres (jeśli wykres jest ukryty)
	Rozwiń wykres (jeśli wykres jest zwinięty)
	Zwiń wykres (jeśli wykres jest rozwinięty)
	Zmiana typu wykresu na wykres słupkowy
	Zmiana typu wykresu na wykres kołowy
	Zmiana typu wykresu na wykres pączkowy
	Zmiana typu wykresu na wykres obszaru biegunowego
	Zmiana kolejności sortowania
	Zmodyfikuj następujące elementy wyświetlanego przeglądu: • Dodawanie/usuwanie kolumn • Określ kolejność wyświetlania kolumn • Pokaż/ukryj wykres nad tabelą • Wybierz kolumnę używaną dla wykresu • Filtrowanie danych tabeli
	Otwórz menedżera konfiguracji, aby zapisywać i wczytywać różne raporty
	Resetuje aktualnie otwarty raport do ustawień domyślnych
	Eksport bieżącego raportu do pliku .csv
	Regeneracja danych i ponowne wczytanie bieżącego raportu

Lista wszystkich domyślnych raportów znajduje się na następnych stronach.

Raporty zgodności

Zrootowane urządzenia

Przegląd urządzeń, które zostały zrootowane/jailbreakowane.

Domyślne kolumny tego raportu:

Alias urządzenia
Właściciel urządzenia
E-mail
System operacyjny
Numer telefonu
Ostatnio widziany
Producent

Urządzenia w roamingu

Przegląd wszystkich urządzeń w roamingu

Domyślne kolumny tego raportu:

Alias urządzenia
Właściciel urządzenia
E-mail
Typ urządzenia
System operacyjny
Numer telefonu
Ostatnio widziany

Urządzenia z włączonym roamingiem

Przegląd wszystkich urządzeń, które aktywowały roaming, ale niekoniecznie aktualnie korzystają z roamingu.

Domyślne kolumny tego raportu:

Alias urządzenia
Właściciel urządzenia
E-mail
Typ urządzenia
System operacyjny
Numer telefonu
Ostatnio widziany

Nadzorowane urządzenia

Przegląd wszystkich nadzorowanych urządzeń w trybie nadzorowanym (tylko iOS)

Domyślne kolumny tego raportu:

Alias urządzenia
Właściciel urządzenia
E-mail
Typ urządzenia
Ostatnio widziany

Nieaktywne urządzenia

Przegląd wszystkich urządzeń, które nie łączyły się z serwerem w ciągu ostatnich 7 dni.

Domyślne kolumny tego raportu:

Alias urządzenia
Właściciel urządzenia
E-mail
Typ urządzenia
System operacyjny
Ostatnio widziany

Raporty o urządzeniach

Urządzenia według własności

Tutaj możesz zobaczyć, ile urządzeń zostało obecnie wdrożonych jako urządzenia firmowe (urządzenia firmowe) i urządzenia pracowników (urządzenia prywatne).

Domyślne kolumny tego raportu:

Alias urządzenia
Właściciel urządzenia
Typ urządzenia
Własność urządzenia
System operacyjny

Wszystkie urządzenia

Tutaj można zobaczyć przegląd wszystkich urządzeń wraz z najważniejszymi informacjami.

Domyślne kolumny tego raportu:

Alias urządzenia
Typ urządzenia
Zarejestrowany
Własność urządzenia
System operacyjny
Wersja systemu operacyjnego
Numer seryjny
Ostatnio widziany
Operator/Przewoźnik
Producent

Nośniki urządzeń

Tutaj możesz zobaczyć przegląd dotyczący operatora (operatora komórkowego).

Domyślne kolumny tego raportu:

Alias urządzenia
Właściciel urządzenia
E-mail
System operacyjny
Wersja systemu operacyjnego
Operator/Przewoźnik

Bezpieczne urządzenia

Tutaj można zobaczyć przegląd urządzeń korzystających z wersji SAFE.

Ponieważ przegląd i / lub SAFE są dostępne tylko dla urządzeń Samsung, w tym punkcie nie zobaczysz zwykłych zakładek.

Domyślne kolumny tego raportu:

Alias urządzenia
Właściciel urządzenia
E-mail
Typ urządzenia
Ostatnio widziany
Wersja SAFE

Urządzenia Windows BitLocker

Tutaj można zobaczyć przegląd urządzeń z systemem Windows, które korzystają z funkcji BitLocker.

Domyślne kolumny tego raportu:

Alias urządzenia
Właściciel urządzenia
E-mail

Stan funkcji BitLocker

Raporty aplikacji

Tutaj dostępne są różne przeglądy dotyczące aplikacji. We wszystkich tych raportach można kliknąć wpis, aby sprawdzić, które wersje są zainstalowane na urządzeniach i jak często. W tym widoku można ponownie kliknąć określoną wersję, aby zobaczyć, na których urządzeniach jest ona zainstalowana.

Uwaga: Może upłynąć trochę czasu, zanim system otrzyma aktualne informacje z urządzenia. Ponadto raporty nie są aktualizowane co minutę. Być może będziesz musiał uzbroić się w cierpliwość, aby zobaczyć aktualny status, jeśli właśnie przypisałeś nową aplikację lub wersję. Ręczne przeładowanie raportu wymusi wyświetlenie najbardziej aktualnych dostępnych danych

Zainstalowane aplikacje

Tutaj znajduje się przegląd wszystkich zainstalowanych aplikacji.

Domyślne kolumny tego raportu:

Nazwa	Nazwa odpowiedniej aplikacji i/lub usługi
Identyfikator	Określony identyfikator aplikacji/usługi
Łączna liczba	Jak często ta aplikacja / usługa była instalowana na urządzeniach użytkowników końcowych?

Najczęściej instalowane aplikacje

Tutaj można uzyskać przegląd najczęściej instalowanych aplikacji.

Domyślne kolumny tego raportu:

Nazwa	Nazwa odpowiedniej aplikacji i/lub usługi
Identyfikator	Określony identyfikator aplikacji/usługi
Łączna liczba	Jak często ta aplikacja / usługa była instalowana na urządzeniach użytkowników końcowych?

Aplikacje obowiązkowe

W tym miejscu znajduje się przegląd obowiązkowych aplikacji.

Domyślne kolumny tego raportu:

Nazwa	Nazwa odpowiedniej aplikacji i/lub usługi
Identyfikator	Określony identyfikator aplikacji/usługi
Źródło aplikacji	Który AppStore jest zaangażowany: • Sklep Google Play (Android) • iTunes AppStore (iOS)
OS	System operacyjny

Aplikacje na czarnej liście

Tutaj znajduje się przegląd wszystkich zdefiniowanych aplikacji z czarnej listy.

Domyślne kolumny tego raportu:

Nazwa	Nazwa odpowiedniej aplikacji i/lub usługi
Identyfikator	Określony identyfikator aplikacji/usługi
Źródło aplikacji	Który AppStore jest zaangażowany: • Sklep Google Play (Android) • iTunes AppStore (iOS)
OS	System operacyjny

Raporty użytkowników

Taryfa

Tutaj można uzyskać przegląd taryf telefonicznych i kart SIM użytkowników.

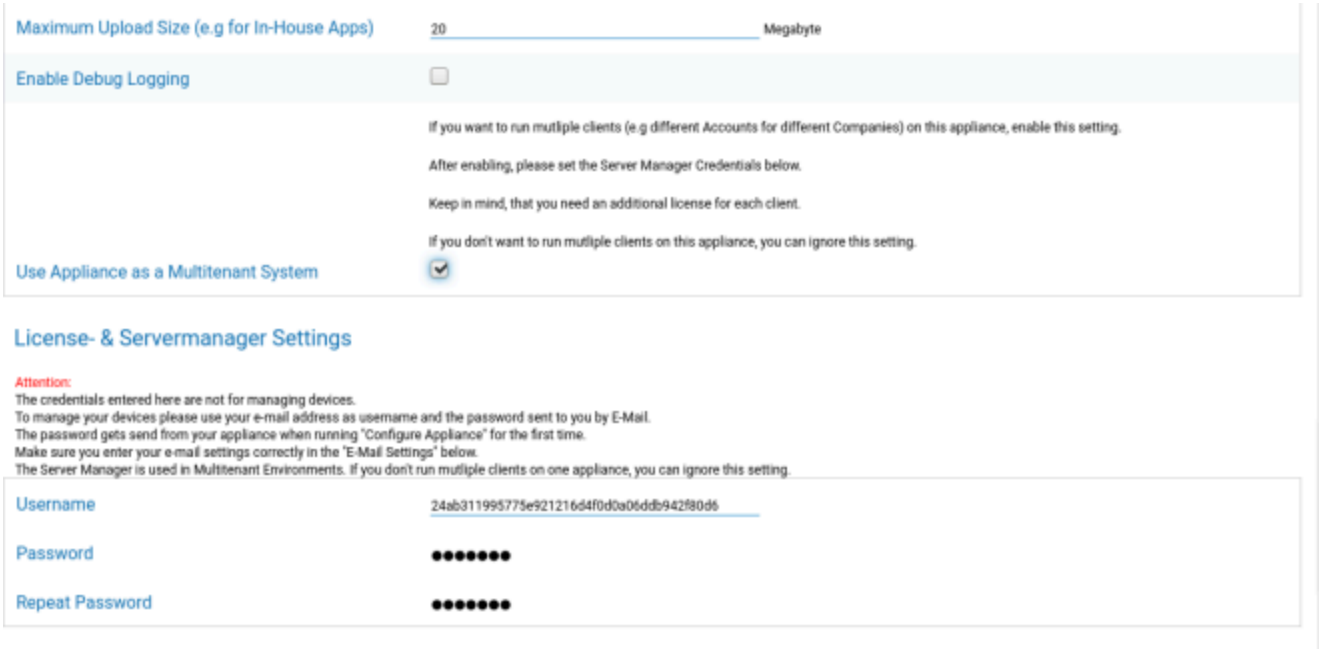
Domyślne kolumny tego raportu:

E-mail
Nazwa
phoneNumber
przewoźnik
taryfa
opcja
cena
contractCancelled
contractStart
duringTime
mobileAndData
dataVolume
multiSIM
typ
simCardSerial1
simCardSerial2
simCardSerial3
pin1
pin2
puk1
puk2
uwaga

Zarządzanie wieloma dzierżawcami

AppTec360 EMM może obsługiwać wiele oddzielnych dzierżawców, z których każdy ma własnych użytkowników i grupy, uprawnienia i ustawienia globalne.

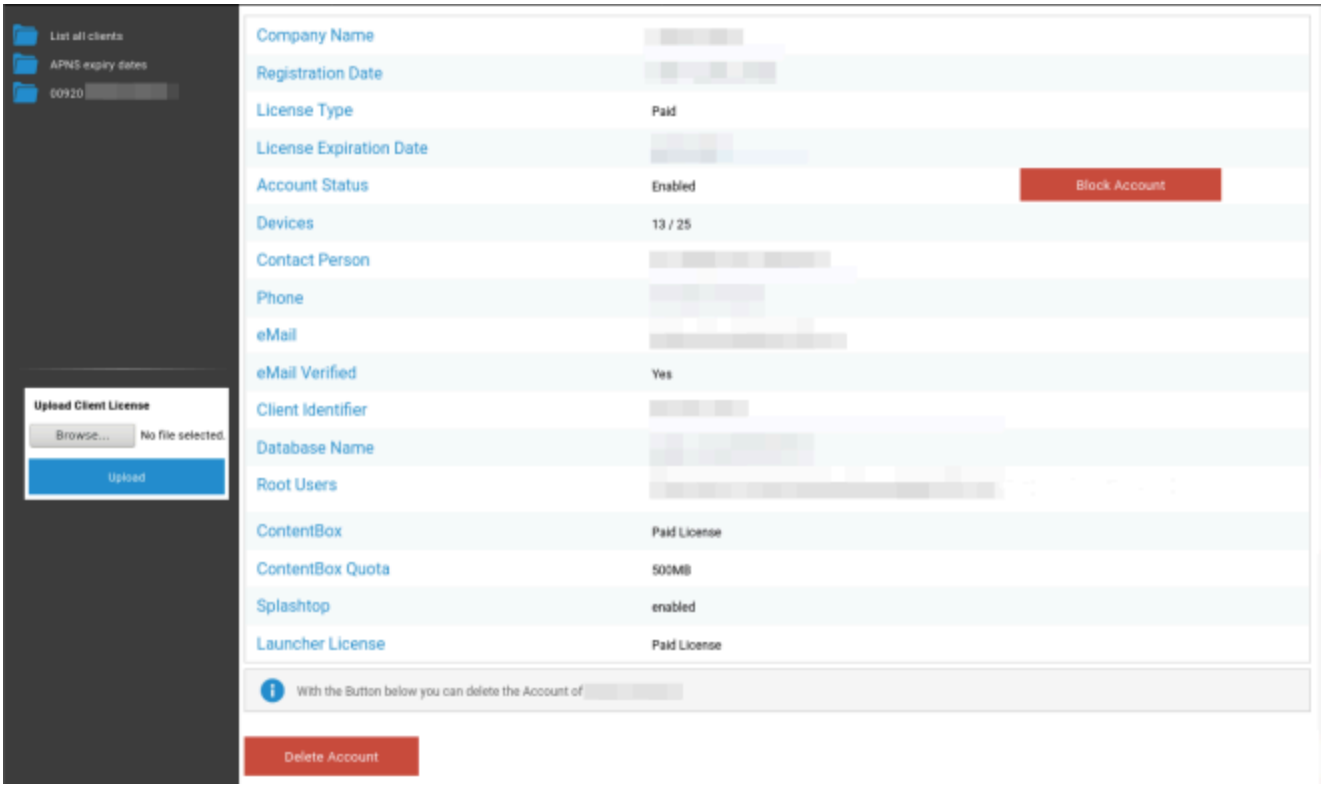
Aby włączyć funkcje Multitenant, należy włączyć je w interfejsie konfiguracyjnym urządzenia w "Kroku trzecim - Ustawienia serwera".



W nowym menu ustaw nazwę użytkownika i hasło dla Servermanager. Zapisz ustawienia i uruchom "Configure Appliance" w "Step Five - License Agreement", aby zastosować ustawienia.

Po zakończeniu konfiguracji można zalogować się przy użyciu ustawionych poświadczeń za pośrednictwem normalnego interfejsu Mobile Management.

Po zalogowaniu można zobaczyć następujący widok.



Po lewej stronie możesz zobaczyć wszystkich najemców (w tym przypadku tylko jednego o identyfikatorze 920), a po prawej informacje o tym kliencie. Masz również możliwość zablokowania dostępu do konta, a także usunięcia klienta (UWAGA: Spowoduje to usunięcie wszystkich danych związanych z tym klientem).

Po lewej stronie można przesłać nową licencję klienta, która może być aktualizacją licencji dla istniejącego klienta lub nową licencją, która automatycznie tworzy nowego klienta. Po utworzeniu nowego klienta wiadomość e-mail zawierająca hasło logowania jest automatycznie wysyłana na adres e-mail, na który została wydana licencja.

Aby uzyskać nową lub zaktualizowaną licencję klienta (np. w przypadku zapotrzebowania na większą liczbę licencji na urządzenia), należy skontaktować się z przedstawicielem handlowym.

Dodatkowe widoki

Lista wszystkich klientów

Wyświetla przegląd wszystkich klientów w systemie.

Identyfikator klienta	Identyfikator klienta
Identyfikator	Identyfikator klienta
Baza danych	Baza danych
Nazwa firmy	Nazwa firmy
eMail	Osoba kontaktowa eMail
Zweryfikowano	Czy wiadomość e-mail osoby kontaktowej jest zweryfikowana, czy nie
Kraj	Kraj
Urządzenia	Liczba zarejestrowanych urządzeń
Data rejestracji	Punkt w czasie przypisania licencji
Ostatnie logowanie	Ostatni login do konta administratora
Licencja	Wyświetlanie typu licencji (Bezpłatna|Płatna)
Licencja CB	Typ licencji ContentBox (Free|Paid)
Status	Aktualny status AppTec-Client
Wygasł	Wyświetla, jeśli licencja wygasła
iOS	Liczba urządzeń z systemem iOS
Android	Liczba urządzeń z systemem Android
Windows Mobile	Liczba urządzeń z systemem Windows Mobile
macOS	Liczba urządzeń z systemem macOS
Windows 10	Liczba urządzeń z systemem Windows 10
Android Enterprise	Liczba urządzeń Android dla przedsiębiorstw
IOS BYOD (rejestracja użytkowników)	Liczba urządzeń IOS BYOD (rejestracja użytkowników)
IoT	Liczba urządzeń IoT

Daty wygaśnięcia APNS

Wyświetla przegląd wszystkich dat wygaśnięcia certyfikatów APNS wszystkich klientów.

Identyfikator klienta	Identyfikator klienta
Nazwa firmy	Nazwa firmy
Data wygaśnięcia	Data wygaśnięcia certyfikatu Apple APNS
Info	Informacje o wygaśnięciu

Kontakt

Dodatkowe pytania? Skontaktuj się z nami pod adresem:

Ogólne pytania techniczne

support@apptec360.com

+41 61 511 3210

W przypadku pytań związanych z instalacją urządzenia wirtualnego

consulting@apptec360.com

+41 61 511 3214

Zastrzeżenie