AppTec360 Enterprise Mobile Manager & ContentBox

Panduan Administrasi | Versi 5.0 (202110)

Daftar Isi

Gambaran Umum

Pengantar ke AppTec360

Sistem Operasi Perangkat yang Didukung

Direktori LDAP yang didukung

Penjelasan tentang “Mode Terawasi” pada Perangkat Apple

- Tersedia dalam Mode Terawasi
- Mengaktifkan mode yang diawasi
- Menambahkan perangkat ke DEP

Penjelasan tentang Android Enterprise

- Apa yang dimaksud dengan Android Enterprise?
- Apa saja persyaratan untuk menggunakan Android Enterprise?.
- Apa saja mode yang tersedia dengan Android Enterprise?
- Bagaimana cara menetapkan aplikasi ke perangkat Android Enterprise?

Unggah Aplikasi Anda sendiri ke Google Play Store

Persyaratan dan Instalasi

Persyaratan

- Persyaratan sistem
- Kunci lisensi
- Alamat IP dan Resolusi DNS
- Sertifikat SSL
- Server SMTP
- Aturan Firewall

Pembaruan Keamanan

- Kata Sandi Default Alat Virtual

Konfigurasi Perangkat Virtual

- Persiapan
  - Mengkonfigurasi dari host eksternal
- Langkah Pertama – Lisensi Alat
- Langkah Kedua – Sertifikat SSL
  - Otomatis

- Kustom
- Langkah Ketiga – Pengaturan Server
- Langkah Keempat – Pengaturan MySQL
- Langkah Kelima – Perjanjian Lisensi
- Pemecahan masalah
- Rekomendasi Keamanan

Pengaturan Umum

Ikhtisar Akun

- Informasi Akun
  - Ikhtisar
  - Laporan Bug
  - Permintaan Fitur

Konfigurasi Global

- Pengaturan eMail
- Templat eMail
- Pendaftaran SMS

Privasi

- Akses GPS

Akses Berbasis Peran

- Manajemen Peran
- Penugasan Peran
  - Penugasan peran
- Akses API
  - Mengakses API REST AppTec360
  - Aturan Umum
  - Contoh permintaan
  - Pertanyaan
  - Contoh Kode dalam Python3

Konfigurasi Apple

- Sertifikat APNS
  - Langkah 1
  - Langkah 2
  - Langkah 3
- Akses Terkelola

- Pendaftaran Pengguna
- iPad bersama
- DEP
- Konfigurator & URL
  - URL Pendaftaran Kolam Renang
  - Profil MDM – Konfigurator Apple

Konfigurasi Android

- Konfigurasi Android
- Pendaftaran Otomatis
- Perusahaan Android
  - Metode Pertama: Akun Perusahaan Android (Akun Google)
  - Metode Kedua: Akun G-Suite
  - Perlindungan Reset Pabrik
- Pendaftaran AE
  - Metode 1: Pendaftaran Kode QR
  - Metode 2: Pendaftaran NFC
  - Metode 3: Akun Google
- Pendaftaran KNOX
- Zero-Touch

Konfigurasi Windows

- Konfigurasi Windows

Kotak Konten

- Konfigurasi

Konfigurasi LDAP

- Ikhtisar LDAP

Manajemen Aplikasi

- DB Aplikasi In-House
  - Android
  - iOS
  - MacOS
  - Windows 10
- Pengaturan Aplikasi
  - Pengaturan Aplikasi iOS
  - Pengaturan Aplikasi Android

- Aplikasi Pihak Ketiga
  - Android
  - iOS
- VPP / KNOX Premium
  - Lisensi VPP
  - Token VPP
  - Kunci Premium KNOX
- Pengaturan App Store
  - Wilayah & Bahasa
- AE Play Store
  - Aplikasi yang Disetujui
  - Aplikasi Play Store
  - Aplikasi Pribadi
  - Aplikasi Web
  - Tata Letak Toko
- Bundel Aplikasi

Kontrol Jarak Jauh

- Penampil Tim
  - Konektor TeamViewer
  - Instal TeamViewer QuickSupport
  - Kontrol jarak jauh perangkat Anda
  - Akses Tanpa Pengawasan
- Splashtop

Manajemen Kartu Sim

- Impor Massal CSV
- Operator & Tarif

Manajemen Langganan

- Manajemen Langganan

Catatan Audit Umum

- Log Audit
- Pengaturan Log Audit

Manajemen Sertifikat

Manajemen Seluler

Layar Manajemen Seluler

- Filter perangkat
- Jendela pencarian
- Perlengkapan pilihan
- Panah navigasi

Pengaturan akun administrasi

- Informasi Pengguna
- Pengaturan Konsol
- Log Masuk

Administrasi perusahaan (Root-Node) dalam Manajemen Seluler

- Membuat Subkelompok
- Ganti nama Root Node
- Pendaftaran Massal
- Penugasan Massal
- Administrasi Aplikasi Cepat
- Impor Pengguna CSV

Manajemen Grup dalam Manajemen Seluler

- Membuat Subkelompok
- Mengedit Grup yang dipilih
- Menghapus Grup yang dipilih
- Membuat Pengguna
  - Membuat Pengguna Admin baru

Manajemen Pengguna dalam Manajemen Seluler

- Menambah dan mendaftarkan Perangkat

Manajemen Profil dalam Manajemen Seluler

- Membuat profil
- Edit Profil
- Salin Profil
- Menghapus Profil
- Mewarisi Profil

Manajemen Perangkat dalam Manajemen Seluler

- IOS
  - Edit Perangkat
  - Hapus Kode Sandi
  - Perangkat Kunci

- Mematikan Perangkat
- Mulai Ulang Perangkat
- Alarm & Mode Hilang | Nonaktifkan Mode Hilang
- Menghapus Perangkat
- Bersihkan Perangkat
- Penghapusan Perusahaan | Hapus MDM
- Kirim Pesan
- Kontrol Jarak Jauh TeamViewer
- Kirim Permintaan Pendaftaran

Android

- Edit Perangkat
- Hapus Kode Sandi
- Perangkat Kunci
- Menghapus Perangkat
- Bersihkan Perangkat
- Hapus MDM
- Kirim Pesan
- Mengubah ke Mode COPE
- Kirim Permintaan Pendaftaran
- Memigrasi Perangkat Lama

Windows

- Edit Perangkat
- Menghapus Perangkat
- Penghapusan Perusahaan | Hapus MDM
- Kontrol Jarak Jauh TeamViewer
- Kirim Permintaan Pendaftaran

Manajemen Konten

- File Grup
- Penjelajah File
- Jejak Audit
- Sampah
- Penyimpanan Eksternal

Log Audit

Konfigurasi iOS

- Umum
  - Ikhtisar profil grup (hanya pada tingkat grup)
  - Informasi Umum
  - Pengaturan
  - Revisi Konfigurasi
  - Log Perangkat (hanya pada tingkat perangkat)
    - Log Perintah
    - Kemungkinan status perintah
- Manajemen Aset (hanya pada tingkat perangkat)
  - Manajemen Aset (hanya pada tingkat perangkat)
    - Info Perangkat
    - Wi-Fi
    - Seluler
    - Bluetooth
- Manajemen Keamanan
  - Anti Pencurian (hanya pada tingkat perangkat)
    - Informasi GPS (hanya pada tingkat perangkat)
    - Hapus & Kunci (hanya pada tingkat perangkat)
    - Pesan (hanya pada tingkat perangkat)
  - Konfigurasi Keamanan
    - Kode Sandi
    - Sertifikat (hanya pada tingkat perangkat)
    - Enkripsi
    - Sistem Masuk Tunggal
  - Akhir Masa Pakai (hanya pada tingkat perangkat)
    - Menghapus (hanya pada tingkat perangkat)
  - Pengaturan Pembatasan
    - Fungsionalitas Perangkat
    - iCloud
    - Keamanan dan Privasi
- BYOD
  - Keamanan iOS bawaan (Wadah)
    - Aktivasi
    - Kata Sandi SecurePIM

- Keamanan SecurePIM
- Browser SecurePIM
- Pertukaran

Manajemen Koneksi

- Wi-Fi
  - Pengaturan Proxy
  - Jenis Keamanan
- VPN
  - Jenis VPN
    - VPN
    - VPN Per-Aplikasi
  - Pengaturan Proxy
- APN
- Seluler
- Proksi HTTP
- AirPrint
- AirPlay

Manajemen PIM

- Sinkronisasi Aktif Pertukaran
- eMail
  - Surat Masuk
  - Surat Keluar
- CalDav
- Kalender Berlangganan
- LDAP

Manajemen Web

- Klip web
- Filter Konten Web

Manajemen Aplikasi

- Manajer Aplikasi Perusahaan
  - Aplikasi Terinstal (hanya pada tingkat perangkat)
  - Aplikasi Wajib
    - Opsi pemasangan
  - Aplikasi Web

- Pembatasan & Pengaturan
  - Aplikasi yang Masuk Daftar Hitam/Daftar Putih
  - Pembatasan SysApp
  - Aplikasi-VPN
  - Pengaturan Aplikasi
- Toko Aplikasi Perusahaan
  - Aplikasi iTunes
  - In-House
- Mode Kios
  - Jenis Aplikasi
    - Paket
    - URL
  - Pengaturan Mode Kios

Android Enterprise – Konfigurasi Perangkat yang Dikelola Sepenuhnya

Umum

- Ikhtisar profil grup (hanya pada tingkat grup)
- Ikhtisar Perangkat (hanya pada tingkat perangkat)
- Revisi Konfigurasi (hanya pada tingkat perangkat)
- Log Perangkat (hanya pada tingkat perangkat)
  - Log Perintah
  - Kemungkinan status perintah
- Pengaturan Perangkat
  - Konfigurasi Klien
  - Wallpaper

Manajemen Aset (hanya pada tingkat perangkat)

- Info Perangkat
  - Wi-Fi
- Seluler
- Bluetooth

Manajemen Keamanan

- Anti Pencurian (hanya pada tingkat perangkat)
  - Informasi GPS (hanya pada tingkat perangkat)
  - Hapus & Kunci (hanya pada tingkat perangkat)

- Pesan (hanya pada tingkat perangkat)
- Konfigurasi Keamanan
  - Kode Sandi Perangkat
  - Anti Virus
- Akhir Masa Pakai (hanya pada tingkat perangkat)
  - Menghapus (hanya pada tingkat perangkat)
- Pengaturan Pembatasan
  - Pembatasan
- Manajemen Sertifikat

Manajemen Koneksi

- Wifi
  - Jenis Keamanan
    - WEP
    - WPA/WPA2
    - 802.1x EAP
- VPN
  - Jenis VPN
    - VPN
    - VPN Per-Aplikasi
- Pembatasan

Manajemen PIM

- Pertukaran Gmail

Manajemen Aplikasi

- Manajer Aplikasi Perusahaan
  - Aplikasi Terinstal (hanya pada tingkat perangkat)
  - Aplikasi Sistem (hanya pada tingkat perangkat)
  - Aplikasi Wajib
  - Daftar Hitam & Putih
  - Aplikasi Sistem AE
- Pembatasan & Pengaturan
  - Pengaturan Manajemen Aplikasi
- Toko Aplikasi Perusahaan
  - In-House
- Perusahaan Play Store
  - AE Play Store

- Mode Kios & Peluncur
  - Mode Kios
  - Peluncur AppTec360
  - Pengaturan AppTec360
- Kontrol Jarak Jauh
  - Splashtop
  - Penampil Tim
- Manajemen Konten
  - Kotak Konten
  - Peramban yang Aman
- API tambahan
  - Samsung KNOX
    - Pembatasan
    - Email
    - Pertukaran
    - APN
    - Bluetooth
    - Koneksi

Android Enterprise – Perangkat yang Dikelola Sepenuhnya dengan Profil Kerja (COPE)

- Penjelasan Umum tentang COPE
- Konfigurasi Profil untuk Perangkat COPE
- Mengembalikan ke Perangkat yang Dikelola Sepenuhnya AE

Android Enterprise – Konfigurasi Kontainer

- Umum
  - Ikhtisar Profil (hanya pada tingkat profil)
  - Ikhtisar profil grup (hanya pada tingkat grup)
  - Ikhtisar Perangkat (hanya pada tingkat perangkat)
  - Revisi Konfigurasi
  - Log Perangkat (hanya pada tingkat perangkat)
    - Log Perintah
    - Kemungkinan status perintah
  - Pengaturan Perangkat

- Konfigurasi Klien
- Wallpaper

Manajemen Aset (hanya pada tingkat perangkat)

- Info Perangkat
  - Wi-Fi
- Seluler
- Bluetooth

Manajemen Keamanan

- Anti Pencurian (hanya pada tingkat perangkat)
  - Informasi GPS (hanya pada tingkat perangkat)
  - Hapus & Kunci (hanya pada tingkat perangkat)
  - Pesan (hanya pada tingkat perangkat)
- Konfigurasi Keamanan
  - Kode Sandi Perangkat
  - Kode Sandi Kontainer
  - Anti Virus
- Akhir Masa Pakai (hanya pada tingkat perangkat)
  - Menghapus (hanya pada tingkat perangkat)
- Pengaturan Pembatasan
  - Pembatasan
- Manajemen Sertifikat

Manajemen Koneksi

- Wifi
  - Jenis Keamanan
    - WEP
    - WPA/WPA2
    - 802.1x EAP
- VPN
  - Jenis VPN
    - VPN
    - VPN Per-Aplikasi
- Pembatasan

Manajemen PIM

- Pertukaran Gmail

Manajemen Aplikasi

- Manajer Aplikasi Perusahaan
  - Aplikasi Terinstal (hanya pada tingkat perangkat)
  - Aplikasi Sistem (hanya pada tingkat perangkat)
  - Aplikasi Wajib
  - Aplikasi Sistem AE
- Pembatasan & Pengaturan
  - Pengaturan Manajemen Aplikasi
- Toko Aplikasi Perusahaan
  - In-House
- Perusahaan Play Store
  - AE Play Store

Manajemen Konten

- Kotak Konten
- Peramban yang Aman

Konfigurasi Android

Umum

- Ikhtisar profil grup (hanya pada tingkat grup)
  - Ikhtisar Perangkat (hanya pada tingkat perangkat)
- Revisi Konfigurasi (hanya pada tingkat perangkat)
- Log Perangkat (hanya pada tingkat perangkat)
  - Log Perintah
  - Kemungkinan status perintah
- Pengaturan Perangkat
  - Konfigurasi Klien
  - Wallpaper

Manajemen Aset (hanya pada tingkat perangkat)

- Manajemen Aset
  - Info Perangkat
  - Wi-Fi
  - Seluler
  - Bluetooth

Manajemen Keamanan

- Anti Pencurian (hanya pada tingkat perangkat)
  - Informasi GPS (hanya pada tingkat perangkat)

- Hapus & Kunci (hanya pada tingkat perangkat)
- Pesan (hanya pada tingkat perangkat)
- Konfigurasi Keamanan
  - Kode Sandi
  - Enkripsi
  - Anti Virus
- Akhir Masa Pakai (hanya pada tingkat perangkat)
  - Menghapus (hanya pada tingkat perangkat)
- Pengaturan Pembatasan
  - Pembatasan
  - Pemilik Perangkat AE

Wadah BYOD

- Perusahaan Android
  - Perusahaan Android
  - Pertukaran Gmail
  - Aplikasi Sistem AE
  - Kode Sandi Kontainer
- Samsung KNOX
  - Aktivasi
  - Kode Sandi Knox
  - Keamanan Knox
  - Pertukaran Knox
  - Knox eMail
  - Aplikasi Knox

Manajemen Koneksi

- Wifi
  - Jenis Keamanan
    - WEP
    - WPA/WPA2
    - 802.1x EAP
- VPN
- Pembatasan
- APN
- Bluetooth

Manajemen PIM

- Pertukaran
- eMail
- Pertukaran AE Gmail

Manajemen Aplikasi

- Manajer Aplikasi Perusahaan
  - Aplikasi Terinstal (hanya pada tingkat perangkat)
  - Aplikasi Sistem (hanya pada tingkat perangkat)
  - Aplikasi Wajib
  - Aplikasi Sistem AE
- Pembatasan & Pengaturan
  - Daftar Hitam & Putih
  - Pembatasan Aplikasi Sys
    - Aplikasi Samsung
    - Aplikasi Huawei
  - Pengaturan Manajemen Aplikasi
- Toko Aplikasi Perusahaan
  - Playstore
  - In-House
- Perusahaan Play Store
- Mode Kios & Peluncur
  - Mode Kios
  - Peluncur AppTec360
  - Pengaturan AppTec360

Kontrol Jarak Jauh

- Splashtop
- Peninjau tim

Manajemen Konten

- Kotak konten
- Peramban yang Aman

Konfigurasi PC Windows 10

Umum

- Ikhtisar profil grup (hanya pada tingkat grup)
- Ikhtisar Perangkat (hanya pada tingkat perangkat)
- Pengaturan

- Revisi Konfigurasi (hanya pada tingkat perangkat)
- Log Perangkat (hanya pada tingkat perangkat)
  - Log Perintah
  - Kemungkinan status perintah
- Manajemen Aset (hanya pada tingkat perangkat)
  - Info Perangkat
  - Seluler
  - Info Sinkronisasi
- Manajemen Keamanan
  - Anti Pencurian (hanya pada tingkat perangkat)
    - Informasi GPS (hanya pada tingkat perangkat)
    - Pengaturan GPS
  - Konfigurasi Keamanan
    - Kode Sandi
    - Antivirus
    - Pusat Keamanan
    - Konfigurasi Firewall
    - Aturan Firewall
  - Pengaturan Pembatasan
    - Fungsionalitas Perangkat
  - BitLocker
    - Konfigurasi BitLocker
    - Status BitLocker
  - Manajemen Sertifikat
    - Daftar Sertifikat
    - Konfigurasi Sertifikat
    - SCEP
- Manajemen Koneksi
  - Wifi
    - Jenis Keamanan
    - Gunakan Server Proxy
  - Pembatasan Wifi
  - VPN
    - Jenis koneksi
    - Konfigurasi VPN Umum
  - Pembatasan VPN
  - Bluetooth

- Manajemen PIM
  - Sinkronisasi Aktif Pertukaran
  - eMail
- Manajemen Aplikasi
  - Manajer Aplikasi Perusahaan
    - Aplikasi Terinstal
    - Aplikasi Wajib
    - Pembatasan Aplikasi Sys
    - Daftar Hitam & Putih

Konfigurasi MacOS

Umum

- Ikhtisar profil grup (hanya pada tingkat grup)
- Ikhtisar Perangkat (hanya pada tingkat perangkat)
- Revisi Konfigurasi (hanya pada tingkat perangkat)
- Log Perangkat (hanya pada tingkat perangkat)
  - Log Perintah
  - Kemungkinan status perintah

Manajemen Aset (hanya pada tingkat perangkat)

- Info Perangkat
- WiFi
- Seluler
- Bluetooth

Manajemen Pembaruan (hanya pada tingkat perangkat)

- Perbarui Info

Manajemen Keamanan

- Anti Pencurian
  - Bersihkan & Kunci
- Konfigurasi Keamanan
  - Kode Sandi
  - Sertifikat
- Pengaturan Pembatasan
  - Fungsionalitas Perangkat
  - iCloud
  - Manajemen Media

- Manajemen Koneksi
  - Wi-Fi
    - Konfigurasi Wi-Fi Perusahaan
  - VPN
  - Proksi HTTP
  - AirPrint
  - AirPlay
- Manajemen PIM
  - Sinkronisasi Aktif Pertukaran
  - eMail
  - CalDav
  - CardDav
  - LDAP

Dasbor & Pelaporan

- Pengaturan Dasbor
- Tampilan Dasbor
- Pelaporan yang Diperpanjang
  - Laporan Kepatuhan
    - Perangkat yang di-root
    - Perangkat Roaming
    - Perangkat yang Diaktifkan Roaming
    - Perangkat yang Diawasi
    - Perangkat Tidak Aktif
  - Laporan Perangkat
    - Perangkat berdasarkan Kepemilikan
    - Semua Perangkat
    - Pembawa Perangkat
    - Perangkat AMAN
    - Perangkat BitLocker Windows
  - Laporan Aplikasi
    - Aplikasi Terinstal
    - Aplikasi yang Paling Banyak Diinstal
    - Aplikasi Wajib
    - Aplikasi dalam Daftar Hitam

- Laporan Pengguna
  - Tarif
- Manajemen Multitenant
  - Tampilan tambahan
    - Daftar semua klien
    - Tanggal kedaluwarsa APNS
- Kontak
  - Untuk pertanyaan teknis umum
  - Untuk pertanyaan yang terkait dengan pemasangan alat virtual
- Penafian

Gambaran Umum

Pengantar ke AppTec360

Solusi Manajemen-Perusahaan-Mobile dari AppTec menawarkan opsi untuk mengelola dan mengonfigurasi semua perangkat seluler dengan konsol manajemennya yang intuitif. Dalam skenario ini, server EMM bisa berjalan di lingkungan Anda sendiri atau Anda bisa memanfaatkan solusi berbasis cloud kami.

Bahkan pada topik instalasi pusat aplikasi perusahaan ke smartphone, Anda datang ke tempat yang tepat. Dengan Enterprise Mobile Manager, Anda dapat mendistribusikan aplikasi dan dokumen perusahaan ke perangkat dalam hitungan detik atau memblokir aplikasi yang tidak diinginkan dengan daftar putih/hitam.

Penggunaan perangkat pribadi di perusahaan menimbulkan tantangan baru untuk mengamankan smartphone dan tablet. Karena karyawan ingin menggunakan ponsel pintar mereka semakin banyak, administrator TI harus melindungi sejumlah besar jenis perangkat yang berbeda. Kami akan membantu Anda mengamankan semua perangkat dan data sensitif yang tersimpan di dalamnya serta mengelolanya dari konsol yang intuitif.

Sistem Operasi Perangkat yang Didukung

AppTec360 menawarkan dukungan untuk perangkat iOS, Android dan Windows. Harap diperhatikan, bahwa kapasitas fungsi platform yang disebutkan di atas dapat berbeda dari satu OS ke OS lainnya.

- Apple iOS 11.0 atau lebih tinggi*.
- Apple macOS 10.11 atau lebih tinggi
- Google Android 4.4 atau lebih tinggi** pada Versi Cloud
- Google Android 4.1 atau lebih tinggi** pada Versi OnPrem
- MS Windows 10 atau lebih tinggi*** (Desktop-Komputer, Notebook, dan Tablet)

**Harap diperhatikan bahwa perangkat dengan iOS 10 atau yang lebih lama tidak dapat didaftarkan karena perubahan drastis yang dilakukan oleh Apple dalam proses pendaftaran.*

***Perangkat dapat disambungkan dan dikonfigurasi meskipun menggunakan versi yang tidak lagi didukung oleh produsen. Harap diperhatikan bahwa mungkin ada fitur yang memerlukan Versi Android tertentu. Dalam kasus dukungan, kami mengikuti dukungan resmi dari produsen. Jika terjadi masalah atau bug yang disebabkan oleh versi usang yang tidak lagi didukung oleh produsen, kami berhak menawarkan dukungan terbatas.*

**** Versi Windows tidak didukung karena keterbatasan Sistem Operasi. Kami sangat menyarankan untuk menggunakan versi OS yang masih didukung oleh produsen. Tidak hanya untuk kompatibilitas, tetapi juga untuk alasan keamanan. Oleh karena itu, kami merekomendasikan iOS 12 atau lebih tinggi dan Android 9 atau lebih tinggi.*

Direktori LDAP yang didukung

- Direktori Aktif Microsoft
- Buka LDAP

Informasi terkini tentang "Sistem Operasi Perangkat yang Didukung" dan "Direktori LDAP yang Didukung" dapat ditemukan di sini:

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

Penjelasan tentang “Mode Terawasi” pada Perangkat Apple

Supervised-Mode mewakili antarmuka yang diperluas untuk perangkat iOS.

Pada masing-masing perangkat yang dikonfigurasi, batasan tambahan, karena berkaitan dengan fungsionalitas perangkat pengguna akhir, dapat diterapkan. Hal ini juga tercantum dalam buku panduan administrasi dan ditandai dengan spanduk.

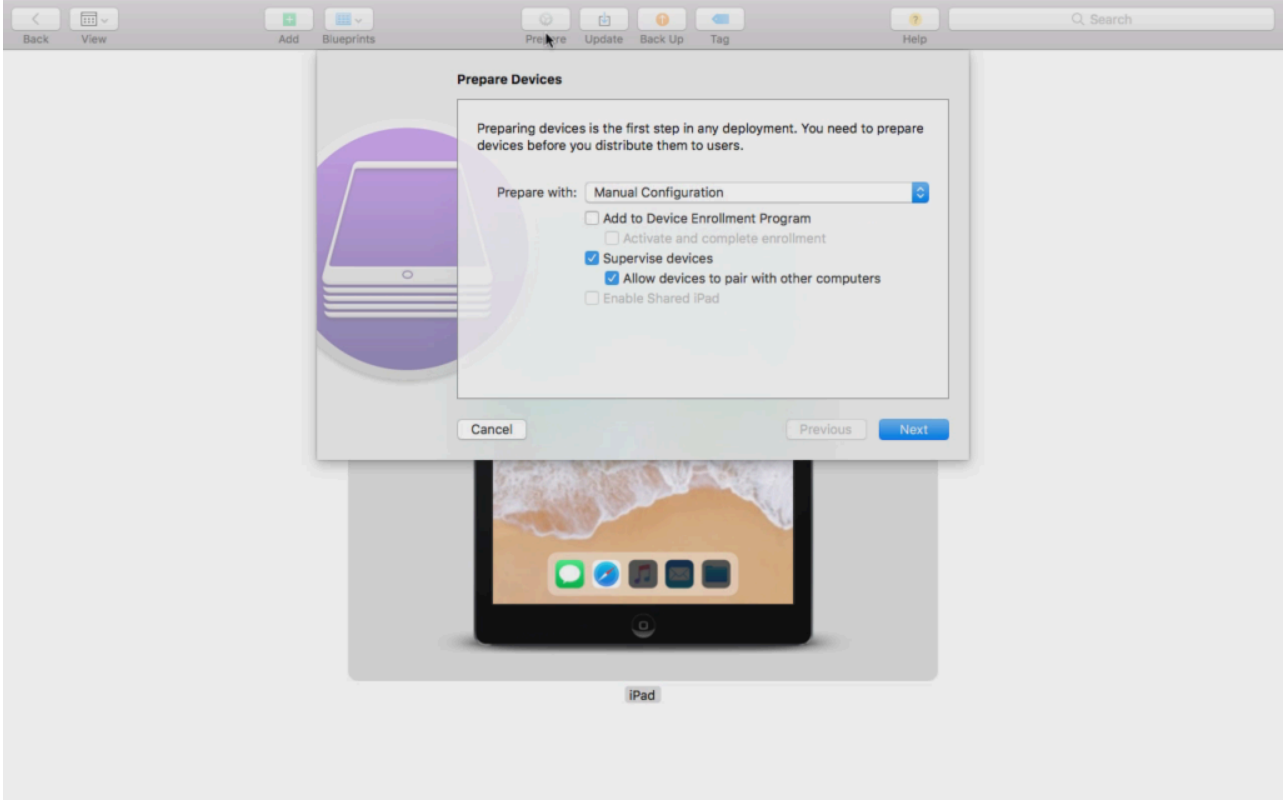
Tersedia dalam Mode Terawasi

"Mode Terawasi" dapat diaktifkan dengan program "Apple Configurator". Apple Configurator dapat mengatur pengaturan default pada perangkat iOS baru sebagai alat konfigurasi (melalui antarmuka USB).

Alat ini tidak hanya dapat menginstal profil konfigurasi, tetapi juga aplikasi. Aplikasi ini gratis, tetapi membutuhkan komputer Mac.

Mengaktifkan mode yang diawasi

1. Buka Konfigurator Apple



2. Klik pada perangkat dan pilih "Siapkan"
3. Pilih "Konfigurasi Manual" dan "Awasi perangkat"
4. Klik "Berikutnya"
5. (Opsional) Sekarang Anda dapat menambahkan Server MDM di mana perangkat akan didaftarkan. Tautan untuk ini dapat ditemukan di "Pengaturan Umum - Konfigurasi iOS - Konfigurator & URL" Pilih Organisasi Anda atau buat yang baru
6. Pilih Organisasi Anda atau buat yang baru
7. Pilih langkah mana yang harus dilewati pada pengaturan awal dan klik "Berikutnya" (PERHATIAN: Melanjutkan akan menghapus perangkat Anda!)

Sekarang perangkat Anda akan dimasukkan ke dalam mode yang diawasi. Hal ini bisa memakan waktu beberapa menit. Setelah selesai, perangkat akan melakukan boot ulang.

Sekarang perangkat Anda diawasi!

Menambahkan perangkat ke DEP

Anda juga dapat menambahkan perangkat ke DEP (Device Enrollment Programm) menggunakan Apple Configurator, jika perangkat Anda menggunakan iOS 11 atau lebih tinggi.

Informasi lebih lanjut tentang DEP: https://www.apple.com/business/dep/

Ikuti langkah yang sama seperti Anda mengawasi perangkat dan juga centang "Tambahkan ke Program Pendaftaran Perangkat". Anda akan dimintai data login DEP jika Anda belum pernah login ke DEP dengan Apple Configurator.

Setelah Proses selesai, perangkat dapat ditemukan di Server DEP "Perangkat yang Ditambahkan oleh Apple Configurator 2". Anda sekarang dapat menggunakan Server ini dan menghubungkannya ke konsol manajemen atau mentransfer perangkat ke server yang sudah ada.

Anda sekarang telah berhasil menambahkan perangkat ke DEP!

Penjelasan tentang Android Enterprise

Apa yang dimaksud dengan Android Enterprise?

Android Enterprise menawarkan kontrol yang lebih baik terhadap perangkat kerja yang dikelola dengan MDM. Hal ini memungkinkan administrator untuk memiliki kontrol penuh atas perangkat Android mereka atau memisahkan data perusahaan dari data pribadi pada perangkat kontainer. Selain itu, Android Enterprise memungkinkan pendaftaran perangkat yang lebih mudah dan distribusi aplikasi yang mudah.

Apa saja persyaratan untuk menggunakan Android Enterprise?.

Android Enterprise dapat digunakan secara gratis oleh semua orang. Anda hanya perlu menghubungkan akun google ke MDM untuk mengaktifkan semua fitur Android Enterprise. Lebih lanjut tentang hal ini dapat ditemukan di bagian Android Enterprise.

Android Enterprise dapat digunakan pada perangkat dengan Android 5.1 atau lebih tinggi, dengan pengecualian pada Profil Kerja yang Disempurnakan (lihat di bawah). Kami merekomendasikan setidaknya Android 7 atau lebih tinggi untuk pendaftaran yang lebih mudah atau Android 11 untuk memanfaatkan semua fitur yang tersedia.

Apa saja mode yang tersedia dengan Android Enterprise?

Ada 3 mode berbeda yang dapat digunakan saat menggunakan Android Enterprise.

AE Perangkat yang Dikelola Sepenuhnya (Dikelola Kerja): Perangkat yang dikelola sepenuhnya yang hanya digunakan untuk bekerja. Hal ini memungkinkan administrator memiliki kontrol penuh atas perangkat. Hal ini tidak memungkinkan penggunaan perangkat secara pribadi. Untuk mendaftarkan perangkat dalam mode ini, perangkat harus diatur ulang dan didaftarkan dengan Kode QR (lihat Pendaftaran AE) atau didaftarkan melalui Pendaftaran Knox atau Zero Touch.

Wadah AE BYOD: Wadah BYOD (bawa perangkat Anda sendiri) memungkinkan pengguna untuk mengakses data perusahaan di ponsel pribadi mereka dalam wadah terpisah. Dalam mode ini, aplikasi pribadi tidak dapat melihat data dan aplikasi perusahaan dan sebaliknya. Untuk mendaftarkan perangkat dalam mode ini, aplikasi AppTec harus diunduh dan QR Code dapat dipindai. Buat perangkat di konsol dan pilih "AE Container (BYOD & Enahnced Work Profile)" sebagai jenis perangkat. Klik QR Code pada perangkat yang baru dibuat untuk mendapatkan QR Code dan atur sakelar pertama ke "Legacy & BYOD".

AE Enhanced Work Profile: (membutuhkan Android 11 atau lebih tinggi) Sementara BYOD Container yang disebutkan di atas membawa data perusahaan ke perangkat pribadi, Enhanced Work Profile melakukan hal yang sama tetapi untuk perangkat milik perusahaan. Ini menciptakan kontainer yang

sama, tetapi memberikan administrator sedikit lebih banyak kontrol atas perangkat, sehingga pengguna tidak bisa begitu saja menghapus MDM dari perangkat. Buat perangkat di konsol dan pilih "AE Container (BYOD & Enahnced Work Profile)" sebagai jenis perangkat. Klik QR Code pada perangkat yang baru dibuat untuk mendapatkan QR Code dan atur sakelar pertama ke "Enhanced Work Profile". Kode QR ini dapat dipindai setelah mengatur ulang perangkat dan mengetuk 6 kali pada layar seperti yang dijelaskan pada Metode 1 di Pendaftaran AE.

Bagaimana cara menetapkan aplikasi ke perangkat Android Enterprise?

Pertama, Anda harus menyetujui Aplikasi yang ingin Anda gunakan di Pengaturan Umum → Manajemen Aplikasi → AE Play Store → Aplikasi Play Store. Setelah menyetujui aplikasi, Anda bisa menetapkannya ke daftar aplikasi wajib → profil Anda dengan mengeklik "+" dan memilih aplikasi dari tab "AE Play Store". Ini akan mengunduh dan menginstal aplikasi secara otomatis. Tidak diperlukan akun Google pada perangkat dan pengguna tidak perlu mengonfirmasi atau mengizinkannya.

Unggah Aplikasi Anda sendiri ke Google Play Store

Anda dapat mengunggah Aplikasi Inhouse Anda ke Google Play Store. Dengan cara ini Anda bisa mendapatkan keuntungan dari berbagai keuntungan seperti mekanisme pembaruan Play Store.

Untuk melakukannya, Anda memerlukan Akun Pengembang Google. Masuk menggunakan Konsol Google Play(https://play.google.com/apps/publish)

Klik "Buat Aplikasi". Pilih bahasa default dan judul aplikasi.

Create application

Default language *

English (United Kingdom) – en-GB ▾

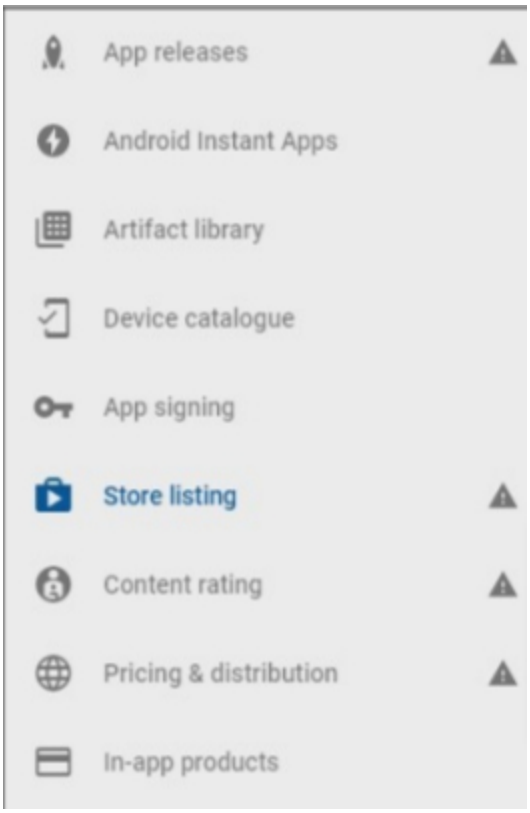
Title *

AppTec Demo App

15/50

CANCEL CREATE

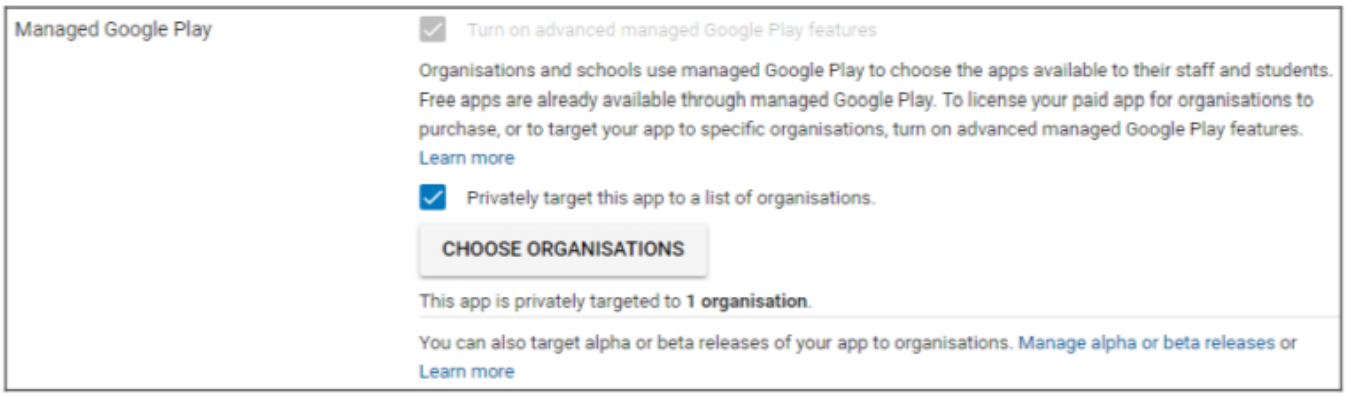
Pada halaman berikut, Anda akan diminta untuk memasukkan berbagai detail tentang aplikasi Anda.



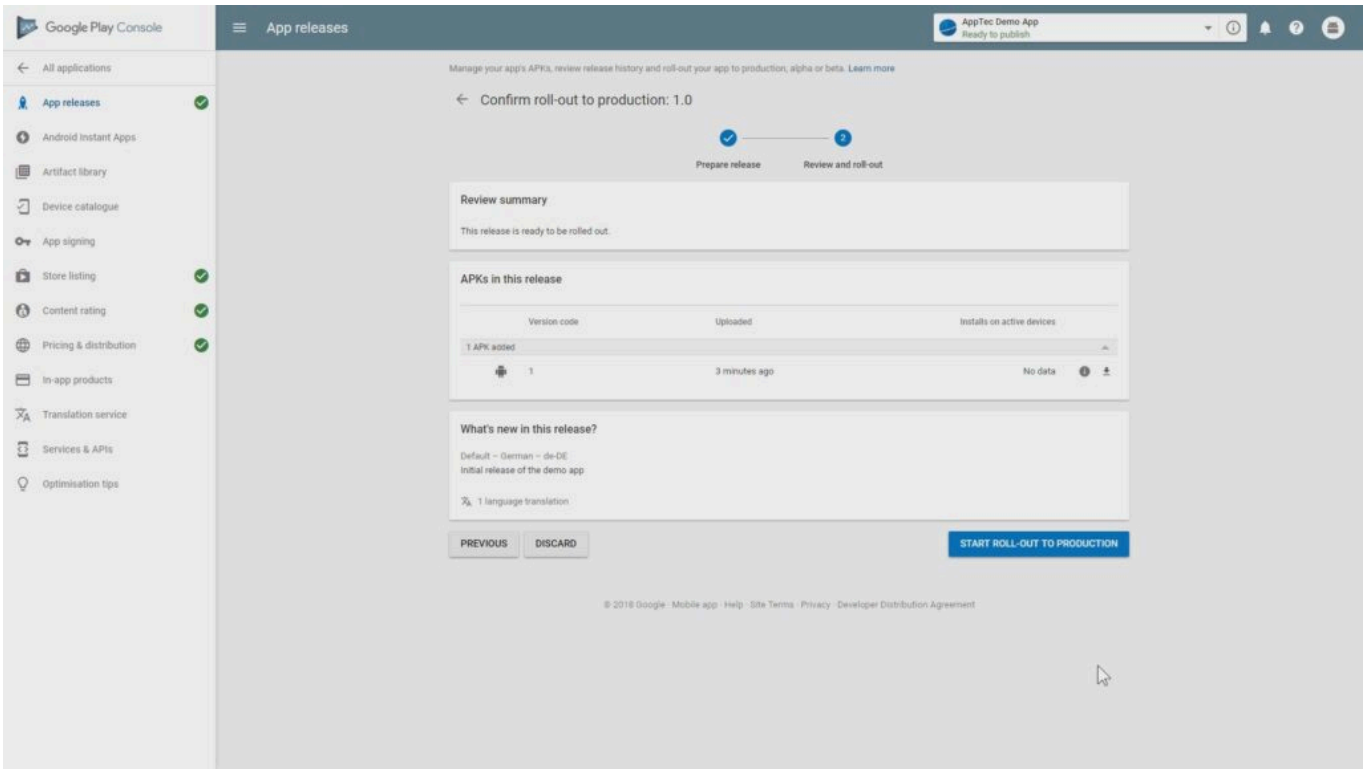
Setelah Anda memasukkan semua detail, Anda akan melihat berbagai simbol petunjuk di sisi kiri.

Arahkan kursor ke atas untuk melihat langkah mana yang tersisa dan ikuti langkah-langkah ini dalam urutan apa pun yang Anda inginkan.

Catatan: Pastikan untuk mencentang dua kotak centang di "Google Play yang dikelola" di bawah "Harga & Distribusi". Jika tidak, aplikasi akan menjadi publik dan dapat diakses oleh semua orang. Pastikan juga untuk memilih negara untuk distribusi.



Setelah Anda menyelesaikan setiap langkah, Anda bisa masuk ke "Rilis aplikasi". Klik "Tinjau" dan "Mulai Luncurkan ke Produksi" untuk menyelesaikan draf Anda dan mempublikasikan aplikasi.



Diperlukan waktu hingga aplikasi tersedia di Play Store. Setelah proses selesai, Anda dapat mencari aplikasi Anda di toko Play for Work dan menyetujuinya. Setelah itu, Anda dapat dengan mudah menetapkan aplikasi ke perangkat menggunakan konsol EMM seperti yang Anda lakukan pada aplikasi lain.

Persyaratan dan Instalasi

Persyaratan

Persyaratan sistem

Alat virtual tersedia dalam Format Virtualisasi Terbuka (VMWare, VirtualBox, Citrix Xen Server) dan sebagai file .vhdx (Hyper-V) yang dikompresi*.

*Catatan: Mesin harus dibuat dengan Generasi 1 saat menggunakan Hyper-V.

Disk virtual memiliki ukuran target 20GB dan mesin membutuhkan RAM 4 GB.

Alat ini berbasis Debian 9 64bit

Tingkatkan mesin yang diimpor ke kompatibilitas terbaru (misalnya di VMWare) dan pastikan jenis OS mesin diatur dengan benar di hypervisor Anda.

Kunci lisensi

Agar berhasil mengaktifkan dan menginstal server, Anda memerlukan file lisensi yang valid. Anda bisa mendapatkannya dari AppTec360 secara langsung dan/atau dari reseller Anda.

Alamat IP dan Resolusi DNS

Alat AppTec360 harus dapat dijangkau oleh perangkat dengan menggunakan nama host yang digunakan untuk mengeluarkan lisensi.

Untuk mendaftarkan perangkat Windows 10, Anda juga perlu menyiapkan subdomain tambahan dalam bentuk "enterpriseenrollment.", yang menunjuk ke alat.

Sertifikat SSL

Karena semua koneksi ke dan dari perangkat harus diamankan menggunakan SSL, Anda memerlukan sertifikat yang valid untuk nama host yang dikeluarkan oleh Otoritas Sertifikat yang dipercaya oleh perangkat. Kunci pribadi untuk sertifikat harus diunggah tanpa perlindungan kata sandi. Dalam banyak kasus, sertifikat perantara untuk CA diperlukan agar perangkat dapat mengenali sertifikat server.

Perangkat Windows 10 akan memerlukan sertifikat khusus untuk subdomain pendaftaran perusahaan Anda.

Mulai dari versi alat 202104 Anda juga bisa menggunakan sertifikat Let's Encrypt, yang dibuat secara otomatis (dijelaskan di Langkah Kedua - Sertifikat SSL).

Server SMTP

Server email dan/atau relai email diperlukan untuk memungkinkan EMM AppTec360 mengirim email (misalnya untuk registrasi perangkat dan validasi akun).

Aturan Firewall

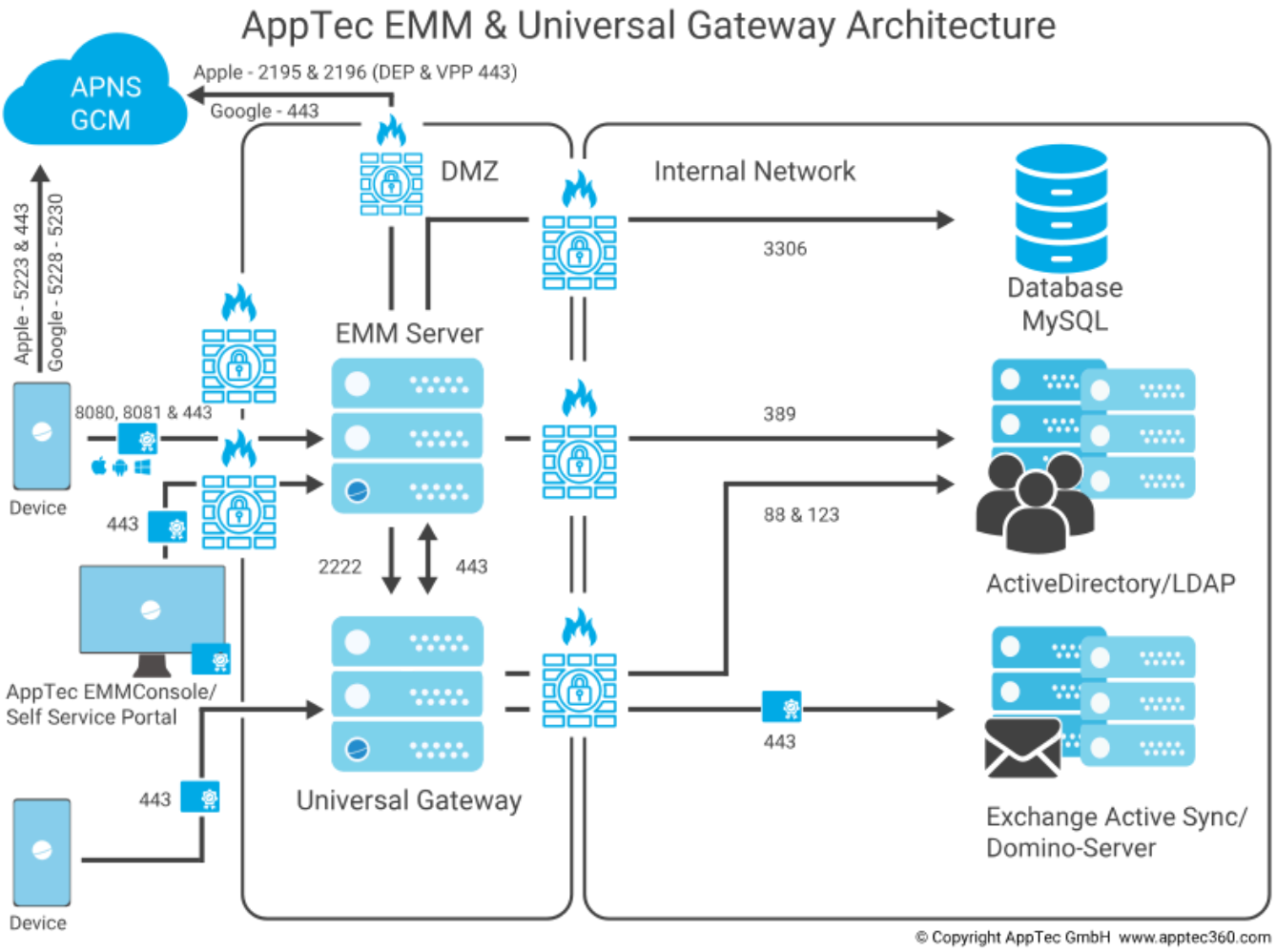


Diagram ini menunjukkan koneksi mana yang diperlukan tergantung pada layanan apa yang ingin Anda gunakan.

Untuk penjelasan yang lebih rinci, lihat tabel di halaman berikutnya.

Apa saja (eksternal/Perangkat)	→	**Alat AppTec360 / emmconsole.com**
Pelabuhan	443	Manajemen, AppStore Perusahaan & Komunikasi Windows Phone
	8080	Komunikasi Android & iOS
	80	Penyiapan Let's Encrypt untuk pertama kalinya. Menggunakan 443 setelahnya.
Apa saja (Perangkat)	→	**Apa saja (eksternal)**
Pelabuhan	5223, 443	Layanan Push Apple, harus dapat dijangkau tanpa proxy, 443 sebagai Fallback, lihat https://support.apple.com/en-us/HT203609
	5228-5230	Layanan Push Android (FCM), harus dapat dijangkau tanpa proxy
Peralatan AppTec360	→	**Pengontrol Domain**
Pelabuhan	389, (LDAPS 636)	Sinkronisasi pengguna dengan LDAP
Peralatan AppTec360	→	**Apa saja**
Pelabuhan	443	Digunakan untuk Layanan Push Android (GCM) Pencarian AppStore / Play Store
Peralatan AppTec360	→	**emmconsole.com**
Pelabuhan	443	Pembaruan Peralatan AppTec360, pembuatan sertifikat APNS
Peralatan AppTec360	→	**Jaringan Apple (17.0.0.0/8)**
Pelabuhan	2195, 2196	Layanan Push Apple & Layanan Umpan Balik
	443	DEP & VPP

Pembaruan Keamanan

Sistem operasi Debian harus diperbarui secara teratur untuk mendapatkan perbaikan keamanan terbaru. Namun, pastikan Anda tidak meng-upgrade ke versi utama Debian yang lebih baru secara manual. Ketika AppTec360 EMM kompatibel dengan versi utama yang lebih baru, kami akan menambahkan cara untuk meng-upgrade dalam pembaruan alat.

Kata Sandi Default Alat Virtual

Login Pengguna (Login root dinonaktifkan. Gunakan "sudo" untuk tugas-tugas administrasi)

apptec

Kata Sandi Masuk

apptec

Pengguna Root MySQL

root

Kata Sandi Root MySQL

apptec

Pengguna Default MySQL

AppTec

Kata Sandi Pengguna Default MySQL

AppTec

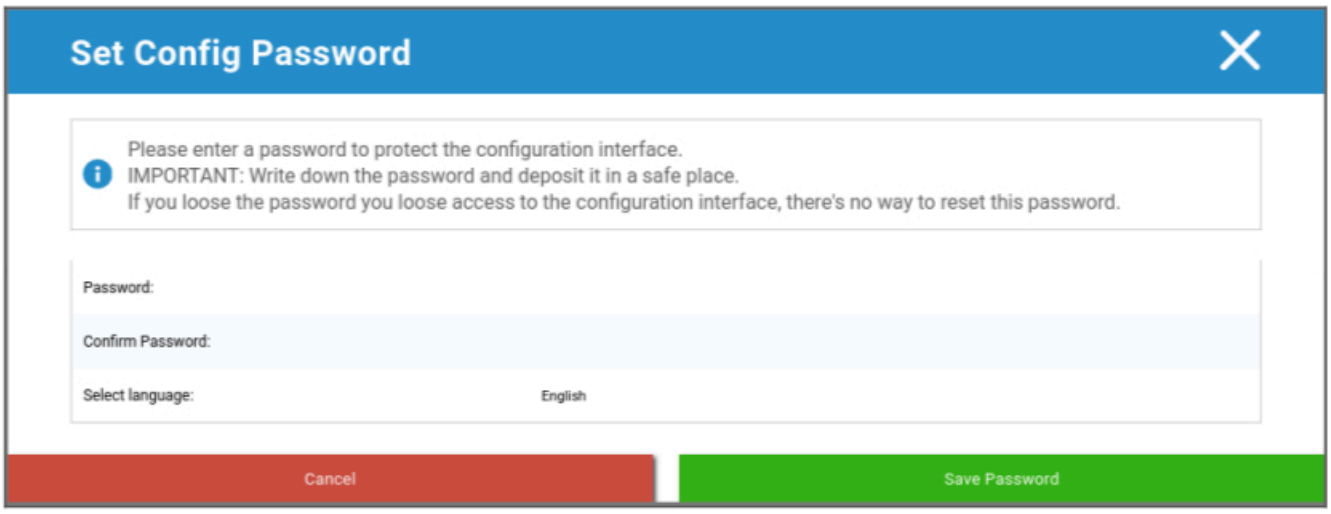
Konfigurasi Perangkat Virtual

Penting: Sebelum Anda memulai dengan konfigurasi Alat Virtual, resolusi layar harus ditetapkan ke setidaknya 1280 x 800 piksel.

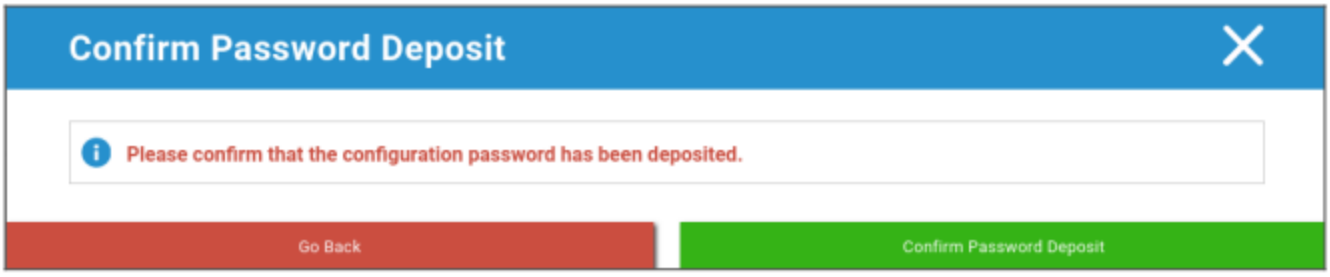
Setelah masuk ke Appliance, Firefox akan secara otomatis memulai dan menampilkan antarmuka konfigurasi.

Persiapan

Pertama, Anda perlu memberikan kata sandi untuk antarmuka konfigurasi. Kata sandi ini digunakan untuk mengenkripsi semua informasi dan file yang dimasukkan dalam antarmuka konfigurasi. Di sini Anda juga dapat mengatur bahasa antarmuka yang akan ditampilkan (dapat diubah nanti).

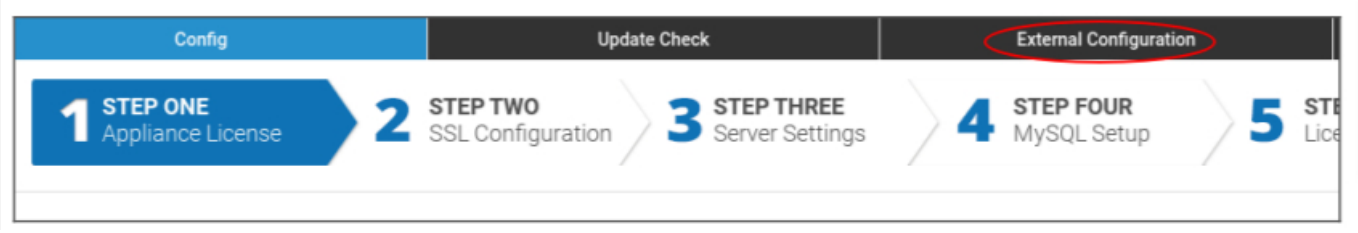


Kata sandi hanya dapat diatur ulang oleh Dukungan AppTec360, jadi pastikan Anda menyimpannya di tempat yang aman dan mengonfirmasi popup yang akan datang.



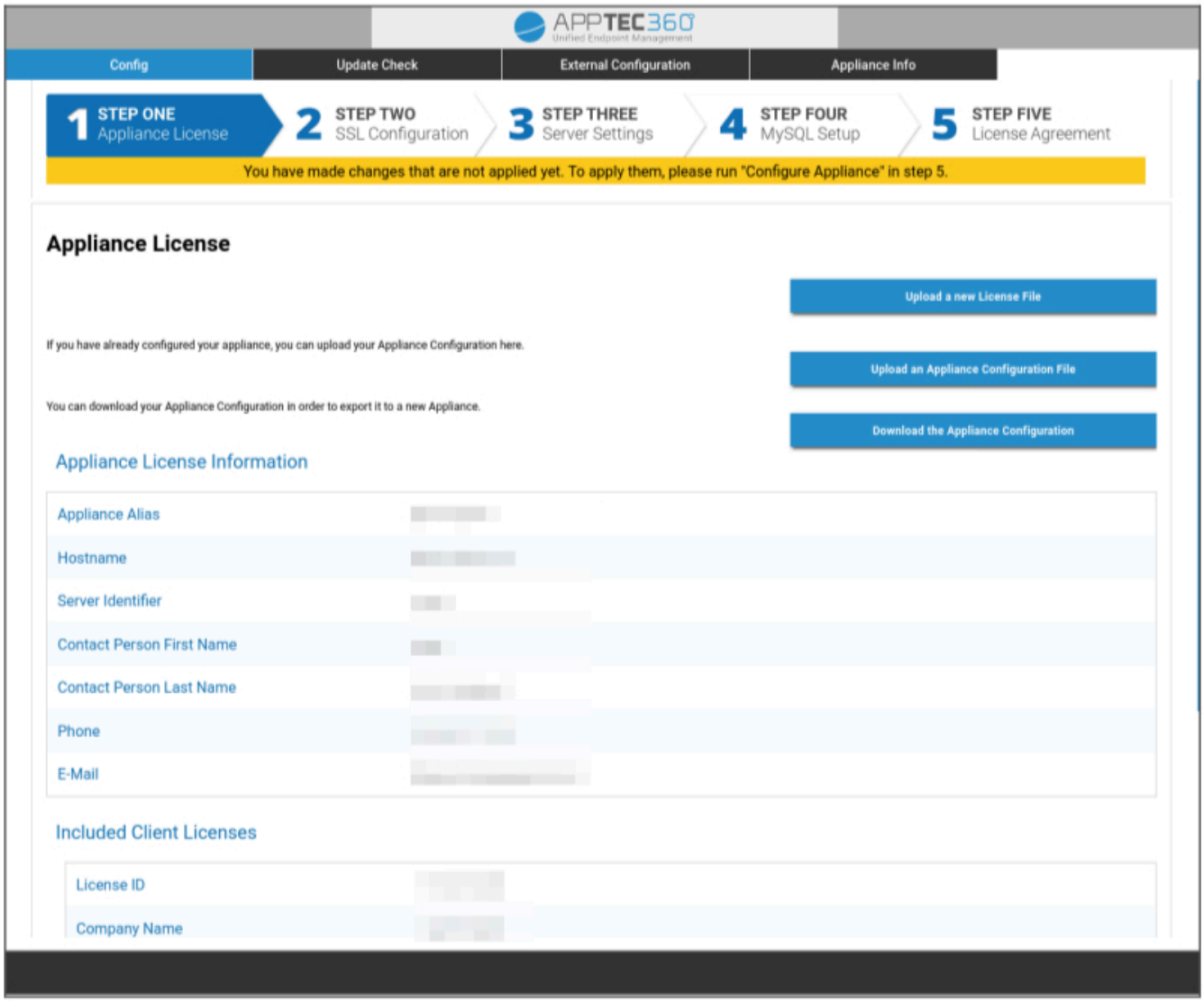
Mengkonfigurasi dari host eksternal

Untuk memudahkan proses penyiapan, Anda dapat membuat halaman konfigurasi dapat diakses dari jarak jauh. Untuk melakukannya, ikuti langkah-langkah dalam "Konfigurasi dari host eksternal".



Langkah Pertama – Lisensi Alat

1. Silakan unggah file lisensi yang telah Anda terima dari AppTec.
2. Jika file lisensi telah berhasil diunggah, Anda dapat melihat informasi lisensi alat seperti pada gambar di bawah ini.



Langkah Kedua – Sertifikat SSL

Anda bisa menggunakan penyiapan sertifikat otomatis menggunakan Let's Encrypt atau menyediakan sertifikat sendiri (lihat SSL-Certificate untuk informasi lebih lanjut).

Otomatis

Sertifikat akan dibuat secara otomatis menggunakan layanan Let's Encrypt.

AppTec360 EMM menggunakan tantangan HTTP-01 untuk validasi domain yang berarti bahwa port HTTP harus terbuka dari internet untuk permintaan sertifikat pertama. Permintaan perpanjangan selanjutnya dapat divalidasi melalui HTTPS.

Alihkan tombol radio ke "Otomatis (Mari Enkripsi)" dan tekan "SIMPAN NILAI". Sertifikat akan secara otomatis diminta ketika menerapkan konfigurasi pada Langkah Kelima - Perjanjian Lisensi. Sertifikat akan diperpanjang secara otomatis jika diperlukan dan Anda akan menerima email jika sertifikat akan kedaluwarsa (yang mengimplikasikan bahwa perpanjangan mungkin gagal).

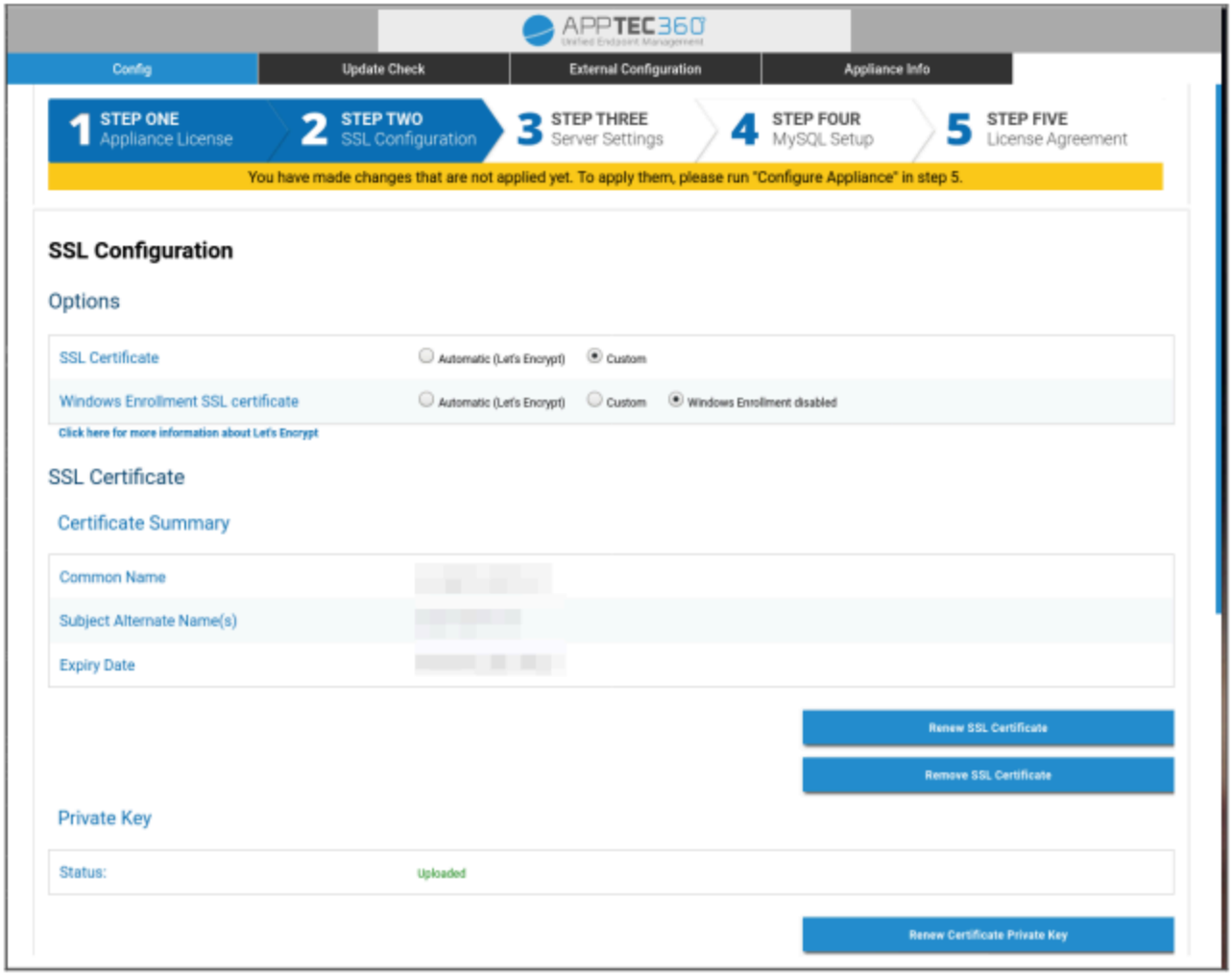
Kustom

1. Unggah Sertifikat SSL untuk nama host berlisensi Anda. Anda dapat melihat nama host di Langkah Pertama - Lisensi Perangkat.

2. Unggah juga kunci privat untuk sertifikat dan jika perlu, sertifikat perantara.

Penting: Kunci tidak boleh dilindungi kata sandi. Jika ya, hapus kata sandi sebelum mengunggah.

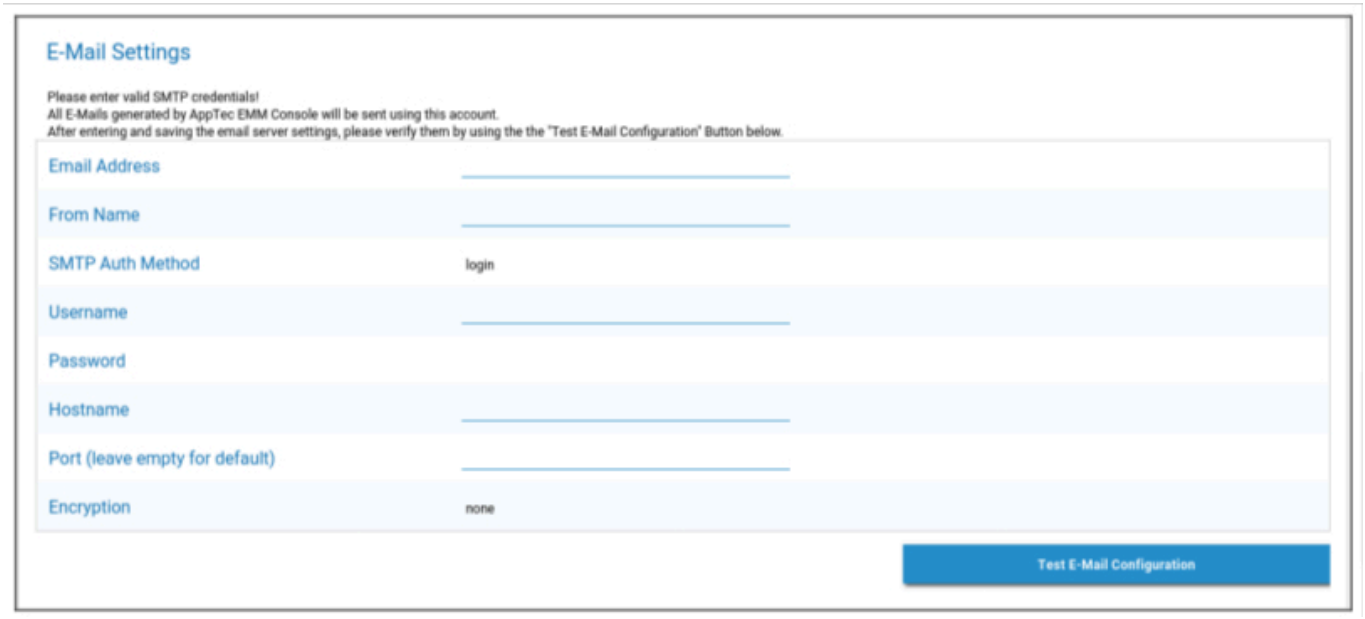
Petunjuk: Jika Anda juga ingin menggunakan perangkat Windows 10, Anda harus mengaktifkan "Sertifikat SSL Pendaftaran Windows" dan mengunggah sertifikat, kunci privat, dan sertifikat perantara untuk subdomain Anda (dijelaskan di Alamat IP dan Resolusi DNS) yang diunggah di bagian bawah halaman.



Langkah Ketiga – Pengaturan Server

1. Masukkan alamat email dukungan global. Alamat ini akan digunakan dalam email kepada pengguna Anda sehingga mereka tahu siapa yang harus dihubungi jika terjadi masalah apa pun terkait perangkat mereka.

2. Menyediakan Pengaturan E-Mail yang akan digunakan oleh sistem untuk mengirim e-mail. Pengaturan ini akan digunakan untuk mengirim e-mail kepada pengguna dan juga untuk mengirim Laporan Bug dan Permintaan Fitur ke"support@apptec360.com". Setelah menyimpan pengaturan email Anda, Anda perlu memverifikasinya dengan mengklik "Test E-Mail Configuration" dan mengikuti petunjuknya.



Langkah Keempat – Pengaturan MySQL

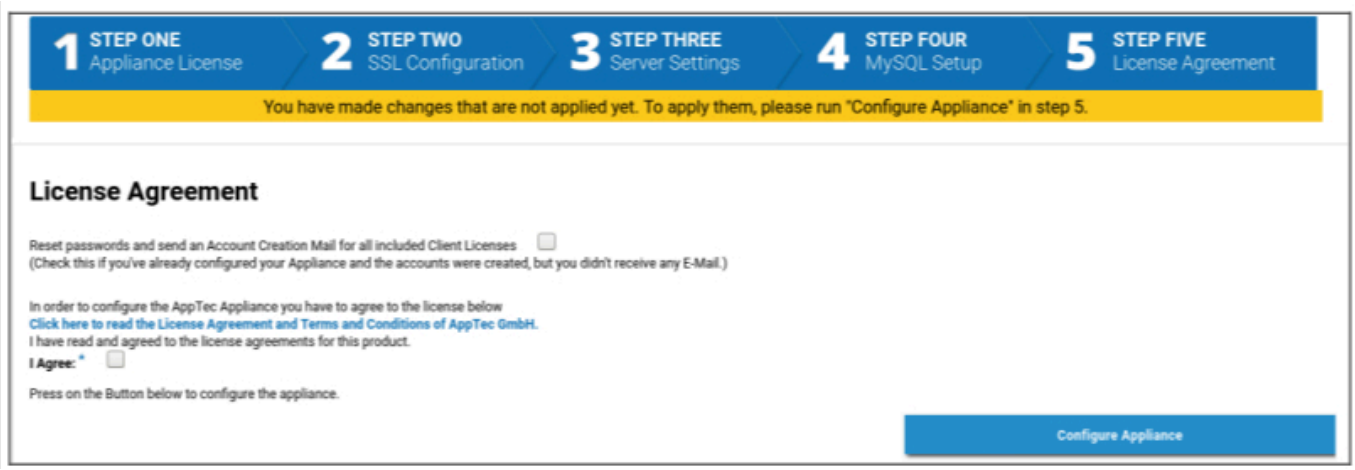
1. Jika Anda ingin menggunakan basis data internal, Anda dapat melewati langkah ini. Jika tidak, Anda dapat memasukkan informasi koneksi untuk server database eksternal Anda.


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)

Langkah Kelima – Perjanjian Lisensi

1. Mohon untuk membaca perjanjian lisensi.
2. Centang "Saya Setuju" dan tekan tombol "Konfigurasi Alat", untuk menerapkan pengaturan.

Petunjuk: Anda harus menjalankan "Configure Appliance" setiap kali Anda mengubah pengaturan dalam 5 langkah untuk menerapkan pengaturan.



Selamat!

Anda telah menyelesaikan konfigurasi alat virtual.

Sebuah email termasuk kata sandi Anda dikirim ke alamat yang Anda berikan untuk lisensi (dapat dilihat di "Lisensi Klien yang Disertakan" di Langkah Pertama - Lisensi Alat).

Anda sekarang dapat masuk ke konsol menggunakan kata sandi ini dan alamat email yang Anda terima.

Untuk masuk ke konsol, masukkan nama host konsol ke dalam bilah alamat browser Anda.

Anda dapat menemukan nama host alat Anda di Langkah Pertama - Lisensi Alat.

Pemecahan masalah

1. 1. Anda tidak menerima email saat mengonfigurasi alat di Langkah Lima - Perjanjian Lisensi:

Pastikan pengaturan email Anda di Langkah Ketiga - Pengaturan Server sudah benar. Untuk mengirim ulang kata sandi, periksa "Atur ulang kata sandi dan kirimkan Email Pembuatan Akun untuk semua Lisensi Klien yang disertakan" pada Langkah Kelima - Perjanjian Lisensi sebelum menjalankan "Konfigurasikan Alat" lagi.

2. Anda telah menerima kesalahan terkait Let's Encrypt selama konfigurasi di Langkah Lima - Perjanjian Lisensi:

Pastikan alat ini dapat dijangkau oleh nama domainnya pada port 80. Let's Encrypt juga menulis log ke "/var/log/letsencrypt" yang dapat membantu pemecahan masalah lebih lanjut.

Rekomendasi Keamanan

Disarankan untuk melakukan langkah-langkah berikut ini untuk mengamankan alat AppTec360 Anda.

Ini bukan seperangkat instruksi lengkap, ini hanya rekomendasi untuk konfigurasi dasar.

- Mengubah kata sandi untuk pengguna AppTec360
- Ubah kata sandi untuk pengguna MySQL "root" dan "AppTec" dan perbarui Langkah Keempat - Penyiapan MySQL yang sesuai
- Mengubah port server SSH default
- Blokir port 80 pada konsol Anda dan larang lalu lintas HTTP yang masuk, hanya gunakan HTTPS. Setelah dikonfigurasi, konfigurasi eksternal melalui HTTPS juga dapat dilakukan.
- Batasi akses ke antarmuka manajemen hanya untuk Ips tertentu di bagian bawah Langkah Ketiga - Pengaturan Server
- Mengkonfigurasi firewall

Pengaturan Umum

Ikhtisar Akun

Informasi Akun

Ikhtisar

Di sini, Anda dapat melihat ikhtisar akun AppTec360 Anda.

Nama Perusahaan	Nama perusahaan Anda
Tanggal Pembuatan	Tanggal pembuatan akun Anda
Jenis Lisensi	Berbayar = lisensi berbayar Gratis = lisensi tidak berbayar Catatan: Akun pada Perangkat OnPremise akan selalu ditampilkan sebagai berbayar karena alasan teknis
Pengenal Klien	Pengenal akun Anda (Ini BUKAN nomor pelanggan Anda)
Tanggal Berakhirnya Lisensi	Tanggal kedaluwarsa lisensi AppTec360 Anda
Lisensi ContentBox	Gratis = lisensi gratis untuk 25 perangkat Berbayar = lisensi berbayar untuk x perangkat
Peluncur	Menunjukkan apakah Anda dapat menggunakan peluncur khusus untuk Android atau tidak
Perangkat	Jumlah lisensi yang saat ini digunakan / total lisensi
Kontak Person	Narahubung yang disediakan
Telepon	Nomor telepon yang disediakan
eMail*	Alamat email yang diberikan
Pengguna Root	Pengguna Root yang dapat masuk
Versi Perangkat Lunak	Versi Perangkat Lunak Saat Ini

**Catatan: Alamat email yang ditampilkan di sini adalah alamat email yang Anda masukkan untuk mendaftarkan Akun. Berdasarkan hal ini, pengguna akan dibuat di pohon pengguna/perangkat dan dapat dimodifikasi. Mengedit pengguna ini akan mengubah alamat email yang akan Anda gunakan untuk masuk, tetapi tidak mengubah informasi dalam ikhtisar akun. .*

Laporan Bug

Laporan bug dapat dikirim langsung ke bagian dukungan untuk melaporkan masalah atau bug dan menyertakan informasi dan log tentang akun dan pengaturan Anda.

Subjek	Subjek laporan bug. Sertakan nomor tiket jika Anda ingin menambahkannya ke tiket dukungan yang sudah ada.
Perilaku yang Diharapkan	Jelaskan secara rinci apa yang Anda lakukan dan apa yang Anda harapkan terjadi
Perilaku Aktual	Jelaskan secara rinci apa yang sebenarnya terjadi. Harap kutip pesan kesalahan dengan TEPAT. Akan sangat membantu jika Anda menambahkan tangkapan layar ke lampiran.
Pada jam berapa Anda mengalami masalah tersebut?	Berikan waktu yang tepat ketika Anda mendapatkan pesan kesalahan/masalah tertentu. Dalam kasus terbaik, sertakan juga detik, misalnya 18:55:27
Dapatkah masalah ini direplikasi? Jika ya, bagaimana caranya (secara rinci)?	Jelaskan bagaimana Anda dapat mereproduksi masalah tersebut secara rinci.
Apakah fitur ini sebelumnya berfungsi seperti yang Anda harapkan? Jika ya, sampai kapan?	Biarkan kosong jika Anda tidak tahu.
Apakah ada perubahan khusus yang dilakukan pada sistem sebelum masalah ini muncul? Jika ya, perubahan apa yang dilakukan (secara rinci)?	Selalu sebutkan perubahan atau tindakan terakhir yang Anda lakukan sebelum masalah tersebut muncul, meskipun menurut Anda hal tersebut tidak relevan.
Jika Berlaku: Model perangkat dan versi OS mana yang terpengaruh?	Harap selalu sebutkan Versi OS yang tepat (misalnya iOS 14.7.1 atau Android 11)
Jika Berlaku: Apa alamat IP publik dan/atau nomor seri Perangkat?	Sebutkan setidaknya satu, meskipun semua perangkat terpengaruh.
Menyertakan file log	Centang ini untuk mengirim file log dengan laporan bug. Hal ini disarankan untuk dilakukan.
Mengambil status VPP saat ini dari Apple dan menyertakan ke laporan bug	Termasuk informasi tentang Penugasan Lisensi VPP. Hanya aktifkan ini jika Anda diminta oleh bagian dukungan atau jika masalah Anda terkait dengan VPP.

Lampiran	Lampirkan file apa pun yang mungkin berguna (misalnya, tangkapan layar dari pesan kesalahan)

Permintaan Fitur

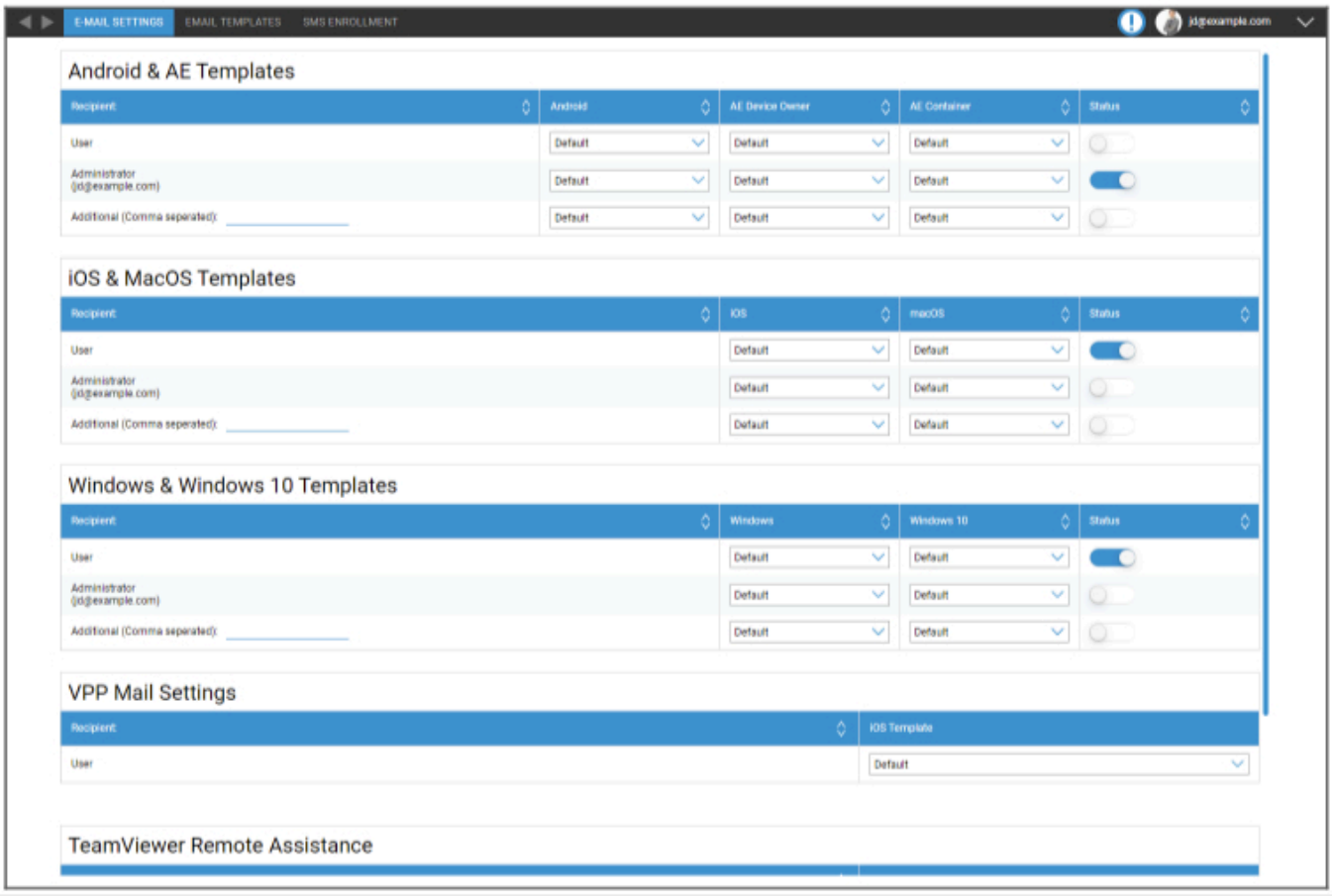
Permintaan fitur dapat dikirim langsung ke bagian dukungan. Ini dapat berisi permintaan untuk fitur tertentu atau perbaikan untuk

Ringkasan	Sinopsis singkat tentang masalah Anda
Deskripsi	Penjelasan rinci tentang masalah Anda, harap sespesifik mungkin
Lampiran	Melampirkan file ke laporan bug

Konfigurasi Global

Pengaturan eMail

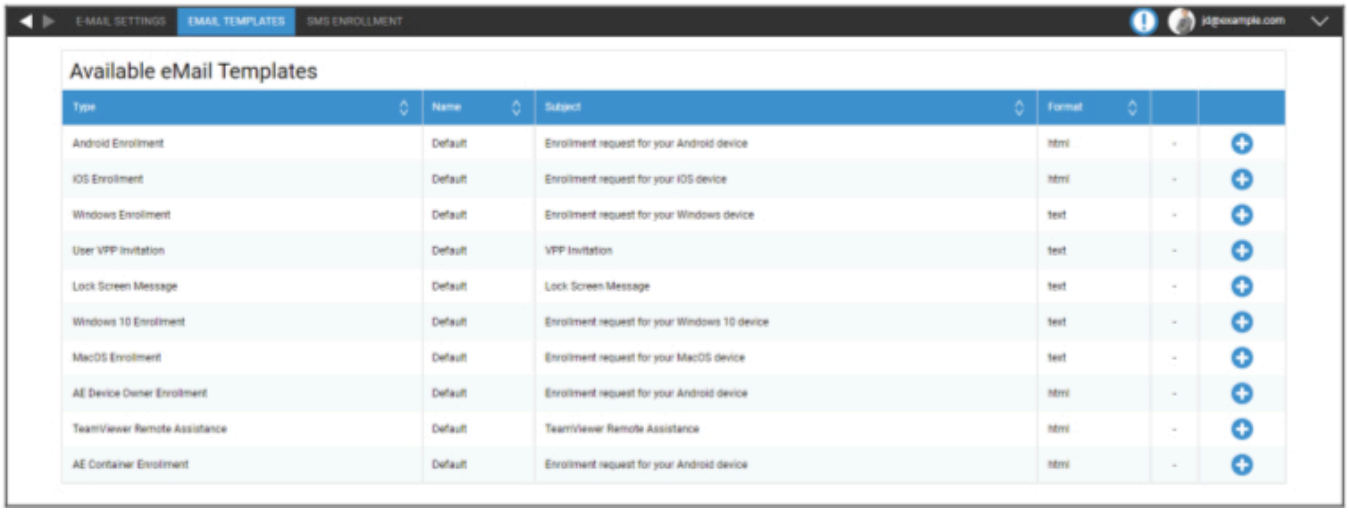
Di sini Anda dapat menentukan siapa yang mendapatkan email ketika permintaan pendaftaran dibuat dan template teks mana yang digunakan untuk email tersebut.



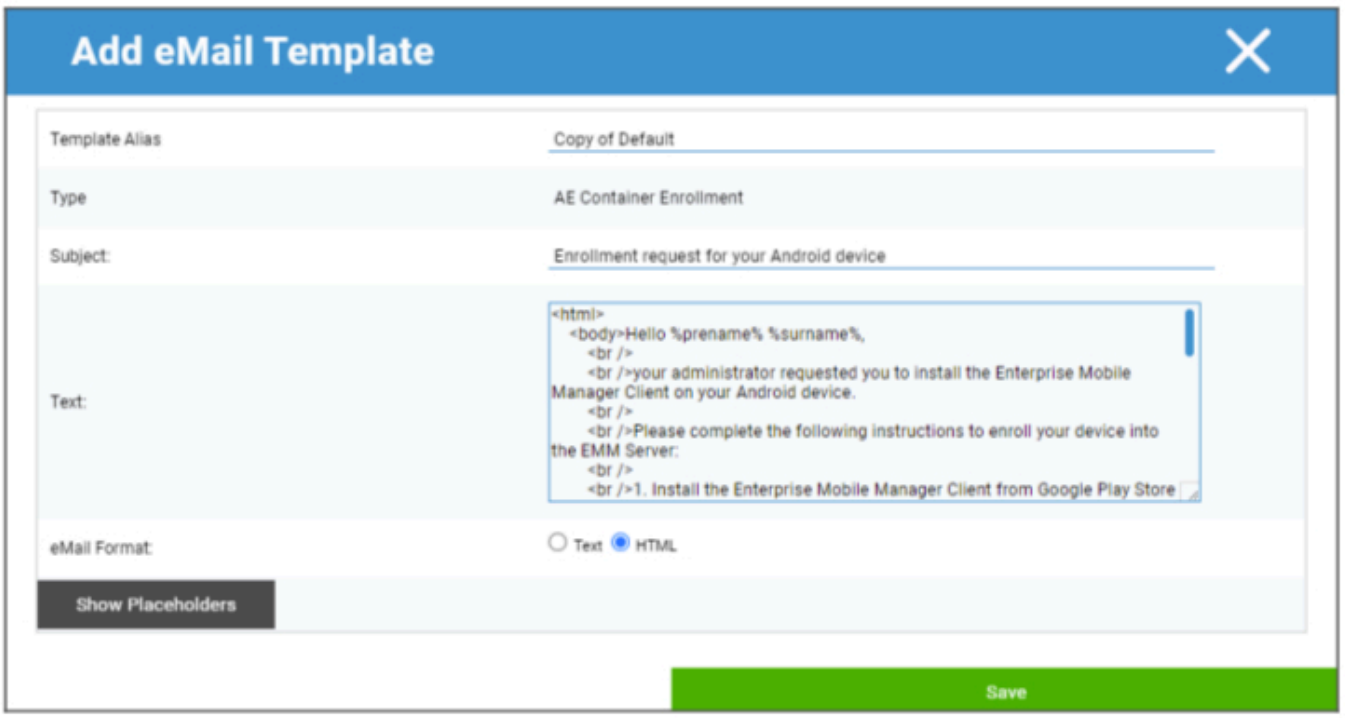
Templat eMail

Di sini Anda bisa membuat dan mengedit templat Anda untuk berbagai skenario. Ini bisa dalam bentuk teks biasa atau HTML. Dengan HTML, Anda dapat mengontrol pemformatan teks dengan lebih baik.

Templat default tidak dapat diedit atau dihapus.



Anda juga dapat menggunakan Placeholder sebagai variabel yang akan diganti secara otomatis. Klik "Tampilkan Placeholder" saat mengedit untuk melihat Placeholder yang tersedia. Kategori yang berbeda memiliki Placeholder yang berbeda.



Pendaftaran SMS

Di sini Anda dapat menonaktifkan/mengaktifkan proses Pendaftaran SMS.

(Default: dinonaktifkan)

Anda juga akan melihat tampilan yang menunjukkan jumlah Kredit SMS yang masih tersedia.

Kredit SMS harus dibeli secara terpisah.

Privasi

Akses GPS

Di sini Anda dapat melindungi Tampilan GPS untuk setiap perangkat dengan 1 atau 2 kata sandi (prinsip empat mata). Anda akan diminta untuk memasukkan kata sandi setiap kali Anda mencoba mengakses lokasi perangkat.

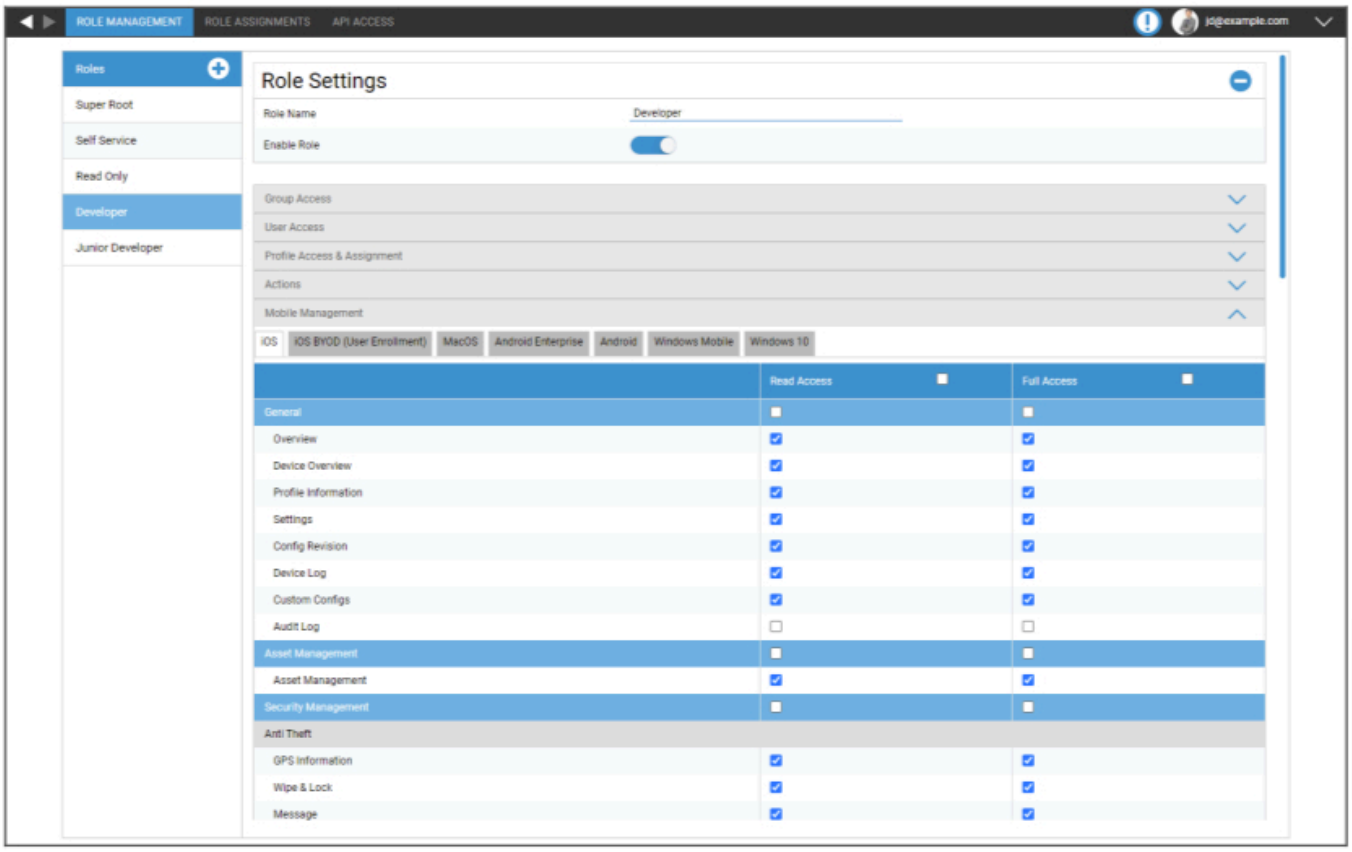
Membatasi akses ke Pengaturan GPS	Mati = fungsi dimatikan dan tidak diperlukan kata sandi untuk melokalisasi
	On = fungsi diaktifkan dan kata sandi diperlukan untuk melokalisasi
Metode Perlindungan	Gunakan satu kata sandi = gunakan satu kata sandi untuk pelokalan
	Gunakan dua kata sandi = gunakan dua kata sandi untuk pelokalan
Masukkan Kata Sandi (1)	Masukkan kata sandi yang dipilih
Ulangi Kata Sandi (1)	Masukkan kembali kata sandi yang dipilih
opsional: Masukkan Kata Sandi 2	Masukkan kata sandi kedua yang dipilih
opsional: Ulangi Kata Sandi 2	Masukkan kembali kata sandi kedua yang dipilih

Catatan: Setelah mengatur kode sandi, Anda harus memasukkannya sekali lagi sebelum benar-benar diaktifkan.

Akses Berbasis Peran

Manajemen Peran

Peran mendefinisikan apa yang dapat dilihat dan dilakukan oleh pengguna ketika ia masuk ke konsol manajemen. Hal ini memungkinkan Anda untuk membuat pengguna yang dapat masuk namun memiliki fungsionalitas terbatas.



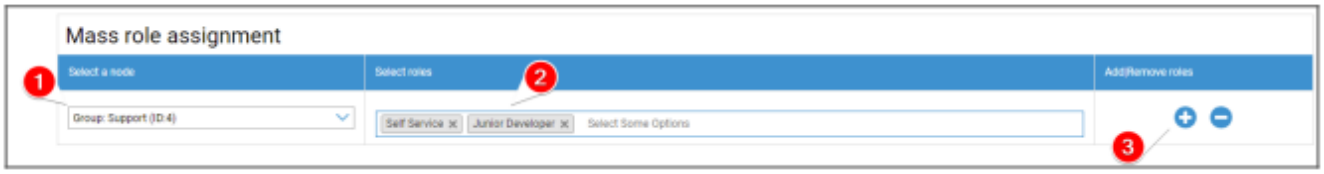
Peran Super Root adalah Peran default yang selalu dapat melihat dan mengubah segalanya. Peran ini tidak dapat diubah atau dihapus. Peran Layanan Mandiri hanya dapat melihat pengguna dan perangkatnya sendiri. Anda dapat menggabungkan Layanan Mandiri dan peran khusus untuk, misalnya, mengizinkan pengguna masuk dan mendaftarkan perangkat sendiri dan hanya untuk pengguna mereka.

Peran Khusus dapat diaktifkan atau dinonaktifkan secara manual. Peran Baru dinonaktifkan secara default. Pengguna dengan peran yang dinonaktifkan bekerja seperti mereka tidak memiliki peran tersebut. Hal ini memungkinkan Anda, misalnya, untuk sementara membatasi peran tertentu dari tindakan mereka.

Semua Izin dibagi antara "Akses Baca" dan "Akses Penuh". Memberikan Akses Baca kepada Role memungkinkan mereka untuk melihat bagian tertentu dari konsol. Memberi mereka Akses Penuh memungkinkan Peran untuk melihat dan mengubah bagian tertentu dari konsol.

Penugasan Peran

Di sini Anda mendapatkan gambaran umum semua pengguna yang memiliki peran dan melihat peran yang mereka miliki. Anda juga dapat menetapkan peran untuk pengguna atau seluruh grup di sini:

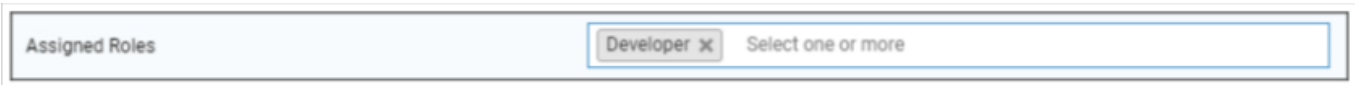


1. Pilih grup atau pengguna mana yang ingin Anda tambahkan atau hapus perannya. Anda dapat memilih satu pengguna atau memilih grup. Ketika memilih grup, perubahan Anda akan memengaruhi semua pengguna di dalam grup tersebut dan semua pengguna sub-grup di dalam grup yang dipilih.
2. Pilih peran mana yang ingin Anda tambahkan atau hapus. Anda dapat memilih satu atau beberapa peran.
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. Simpan untuk menyelesaikan proses. Pengguna yang sebelumnya tidak memiliki peran dan "Dapat Masuk" dinonaktifkan akan secara otomatis menerima email dengan tautan untuk mengatur kata sandi.

Di bawah Penetapan peran massal, Anda dapat menemukan ikhtisar atas peran yang ditetapkan. Anda juga dapat mengubah peran secara manual di sana untuk pengguna tertentu.

Penugasan peran

Untuk menetapkan peran ke pengguna, Anda harus masuk ke Manajemen Seluler, di mana Anda dapat menemukan pohon grup, pengguna, dan perangkat Anda. Edit pengguna untuk menetapkan peran. Atau, Anda dapat menggunakan metode yang disebutkan di atas hanya untuk satu pengguna saja.



Akses API

Mengakses API REST AppTec360

AppTec360 REST API memerlukan token otentikasi (kunci API) dan kunci privat yang harus dibuat di Konsol Manajemen.

Untuk melakukannya, masuk ke AppTec360 EMM dan buka

Pengaturan Umum → Akses Berbasis Peran → Akses API dan tambahkan Kunci baru.

Anda harus memilih pengguna yang izinnya akan berlaku untuk kunci API.

Kunci pribadi hanya dapat diunduh satu kali. Setelah pengunduhan dimulai, kunci akan dihapus, dan tombol "Unduh" akan menghilang.

Jika Anda kehilangan kunci pribadi, Anda harus membuat kunci API yang baru.

Aturan Umum

- API REST tersedia di bawah URL dasar:

/public/external/api

- Semua permintaan harus dikirim melalui POST.
- API REST hanya mendukung permintaan melalui HTTPS.
- Permintaan harus berisi Header berikut ini:

Nama Header	Nilai Header	Deskripsi
Jenis konten	application/json	tetap
auth	123... xyz	Kunci API dari Tab "Akses API"
tanda tangan	Tanda tangan yang dikodekan dengan Base64	Tanda tangan dari muatan yang dihasilkan dengan Kunci pribadi dari Tab "Akses API"

- Badan permintaan harus berupa objek yang dikodekan dengan json yang harus berisi nilai-nilai berikut:

Bidang	Nilai Contoh Bidang	Deskripsi
api	v2/perangkat/daftarperangkat	Nama API
waktu	1529662725	Stempel Waktu Unix (UTC) dari mesin klien. Perbedaan waktu maksimum yang diizinkan antara klien dan server adalah 30 menit.

- Jika berhasil, API akan mengembalikan data yang diminta (lihat Query di bawah ini) dan kode status HTTP 200.
- Jika terjadi kesalahan, kode status HTTP akan berada di antara 4xx dan 5xx, tergantung pada kesalahan, dan objek respons akan berisi sebuah larik dengan kunci "kesalahan", yang berisi daftar pesan kesalahan yang dapat dibaca oleh manusia.
- Jika tidak ada data yang cocok untuk perangkat, array kosong akan dikembalikan.
- Jika Id perangkat tidak ada, maka data yang dikembalikan akan menjadi nol.

Contoh permintaan

```
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]}}
```

Pertanyaan

Membuat daftar semua perangkat

Fungsi: Mengembalikan daftar semua perangkat yang berisi ID Perangkat, IMEI, dan Serial
API URI: v2/device/listdevices
Parameter Wajib: tidak ada
Parameter Opsional: tidak ada

Contoh Badan Permintaan


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


Contoh Badan Tanggapan


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

Dapatkan daftar posisi (GPS)

Fungsi: Mengembalikan daftar semua entri log posisi yang tersimpan untuk id perangkat
API URI: v2/device/listposition
Parameter Wajib: "ids" - Larik ID Perangkat
Parameter Opsional: tidak ada

Contoh Badan Permintaan


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


Contoh Badan Tanggapan


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

Dapatkan peta aset

Fungsionalitas:
Mengembalikan daftar semua aset yang tersimpan yang memungkinkan untuk diminta menggunakan Dapatkan data aset apa pun.
Anda dapat menggunakan formulir yang dapat dibaca manusia atau tag aset untuk meminta data.
API URI: v2/device/getassetmap
Parameter Wajib: tidak ada
Parameter Opsional: tidak ada

Contoh Badan Permintaan

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

Contoh Badan Tanggapan

Tanggapan ini dipersingkat agar mudah dibaca.

{
"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": []
}

Dapatkan data aset apa pun

Fungsi: Mengembalikan daftar data aset yang diminta untuk id perangkat
API URI: v2/device/getassetdata
Parameter Wajib: "ids" - Array ID Perangkat
Parameter Opsional:
"assetkeys" - Kunci data aset yang akan dikembalikan. Jika tidak ditentukan, semua data aset yang tersedia akan dikembalikan ke
. Anda bisa mendapatkan daftar kunci aset menggunakan Dapatkan peta aset.

Contoh Badan Permintaan

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

Contoh Badan Tanggapan

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

Contoh Kode dalam 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)
```

Konfigurasi Apple

Sertifikat APNS

Di sini Anda dapat mengunggah Sertifikat APNS. Ini diperlukan untuk mengelola perangkat iOS dan MacOS.

Catatan: Sertifikat APNS hanya berlaku selama satu tahun. Sertifikat ini harus diperbarui sebelum masa berlakunya habis. Proses perpanjangannya sama dengan pembuatan (lihat di bawah) dan hanya memerlukan waktu beberapa menit saja.

Jika Anda lupa memperbarui ini tepat waktu, Anda tidak dapat membuat perubahan pada perangkat yang sudah terdaftar **dan Anda harus mendaftarkan semua perangkat lagi**.

Langkah 1

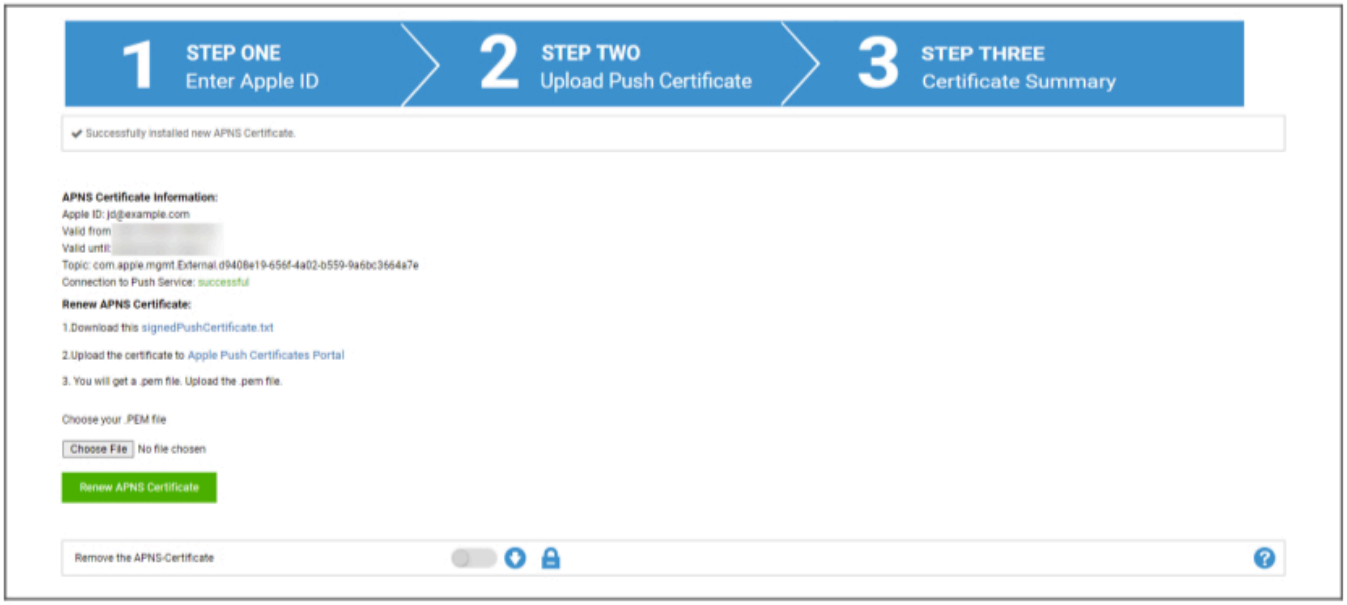
- Pertama, masukkan ID Apple yang ingin Anda gunakan untuk membuat Sertifikat APNS.

Catatan: ID Apple ini hanya digunakan untuk pembuatan Sertifikat APNS. ID Apple ini tidak ada hubungannya dengan perangkat dan perangkat tidak akan tahu tentang ID Apple ini. Selain itu, Anda juga memerlukan akses ke ID Apple ini untuk memperbarui Sertifikat APNS. Oleh karena itu, disarankan untuk menggunakan beberapa ID Apple umum dan mendokumentasikan data login. Pengingat akan dikirimkan ke alamat email yang digunakan untuk ID Apple sebelum Sertifikat APNS berakhir.

- Klik "Langkah Berikutnya" untuk melanjutkan.
- (opsional) Anda juga dapat memulihkan Sertifikat APNS yang sebelumnya terhapus jika Anda menghapusnya secara tidak sengaja

Langkah 2

- Unduh file signedPushCertificate.txt
- Buka https://identity.apple.com/pushcert/ dan masuk dengan ID Apple dari Langkah 1
- Klik "Buat Sertifikat"
- (opsional) masukkan Catatan. Ini dapat membantu jika Anda mengelola beberapa penyewa untuk mengidentifikasi mereka dengan mudah.
- Klik "Pilih File" untuk memilih file signedPushCertificate.txt yang telah diunduh sebelumnya
- Klik "Unggah".
- Sekarang Anda akan melihat konfirmasi bahwa Anda telah membuat Sertifikat APNS.
- Klik "Unduh" dan simpan.
- Kembali ke konsol manajemen.
- Klik "Pilih File" dan pilih Sertifikat APNS yang ingin Anda unggah.
- Klik "Unggah"



Langkah 3

Anda sekarang telah berhasil menyiapkan Sertifikat APNS dan dapat mengelola perangkat iOS dan MacOS.

Pada Langkah 3, Anda akan melihat ikhtisar Sertifikat APNS yang sedang Anda gunakan.

Anda juga memiliki Opsi untuk memperbarui Sertifikat APNS dengan mengikuti langkah-langkah yang ditampilkan di layar. Ingatlah untuk memperbaruinya sebelum masa berlakunya habis.

Saat memperbarui Sertifikat APNS, ingatlah untuk masuk dengan ID Apple yang ditunjukkan pada Langkah 3 dan juga untuk memperbarui sertifikat yang sebelumnya digunakan dan BUKAN membuat yang baru. Anda akan melihat "topik" Sertifikat APNS di Langkah 3 dan ketika mengklik "i" di Portal Sertifikat Push Apple. Ini adalah ID unik yang mengidentifikasi Sertifikat. Ini akan membantu Anda mengidentifikasi yang benar dan memperbarui yang benar.

Ketika Anda mendapatkan "Kesalahan: Sertifikat Push memiliki topik yang berbeda!" saat memperbarui, ini berarti Anda telah memperbarui Sertifikat lain atau membuat yang baru.

Jika Anda ingin mengunggah Sertifikat baru, misalnya jika Anda tidak dapat mengakses ID Apple yang digunakan sebelumnya, Anda harus terlebih dahulu menghapus Sertifikat yang sedang diunggah.

Bagaimanapun juga, menghapus Sertifikat APNS berarti Anda tidak bisa lagi membuat perubahan untuk perangkat yang saat ini terdaftar sampai Anda mendaftarkannya lagi. Jadi, pastikan Anda siap untuk hal ini dan hanya hapus Sertifikat jika tidak ada cara lain.

Akses Terkelola

Di sini Anda dapat mengaktifkan Pendaftaran Pengguna untuk Perangkat iOS dan iPad Bersama untuk Perangkat iOS.

Pendaftaran Pengguna

'Pendaftaran Pengguna' memungkinkan mode khusus untuk perangkat BYOD.

Untuk setiap pengguna, Apple-ID yang dikelola harus dibuat di Apple Business Portal.

Selama proses pendaftaran, pengguna akan diminta kredensial Apple-ID mereka.

'Pendaftaran Pengguna' menjamin keamanan maksimum bagi pengguna karena hanya mengizinkan serangkaian pengaturan dan pembatasan terbatas untuk dikonfigurasi oleh MDM.

Domain Terkelola:

Domain yang digunakan untuk memetakan alamat email pengguna ke Apple-ID yang dikelola (harus dalam format: '@appleid.company.com'), misalnya john.doe@example.com akan dipetakan ke john.doe@appleid.company.com

Periksa Manajer Bisnis Apple untuk melihat Domain Terkelola Anda

iPad bersama

iPad bersama adalah perangkat DEP yang dikonfigurasikan dengan Profil DEP khusus.

Hal ini memungkinkan beberapa pengguna untuk masuk ke perangkat menggunakan Apple-ID yang dikelola.

Apple-ID yang dikelola harus dibuat di Portal Bisnis Apple atau Manajer Sekolah Apple.

Pengguna yang masuk ke iPad bersama akan diminta kredensial Apple-ID yang dikelola.

Domain Terkelola:

Domain yang digunakan untuk memetakan alamat email pengguna ke Apple-ID yang dikelola (harus dalam format: '@appleid.company.com'), misalnya john.doe@example.com akan dipetakan ke john.doe@appleid.company.com

Periksa Manajer Bisnis Apple untuk melihat Domain Terkelola Anda

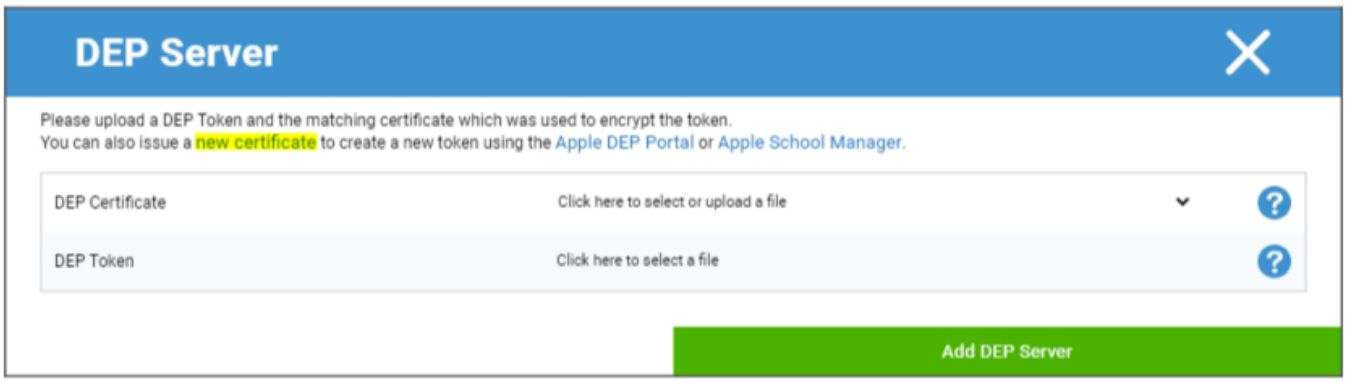
DEP

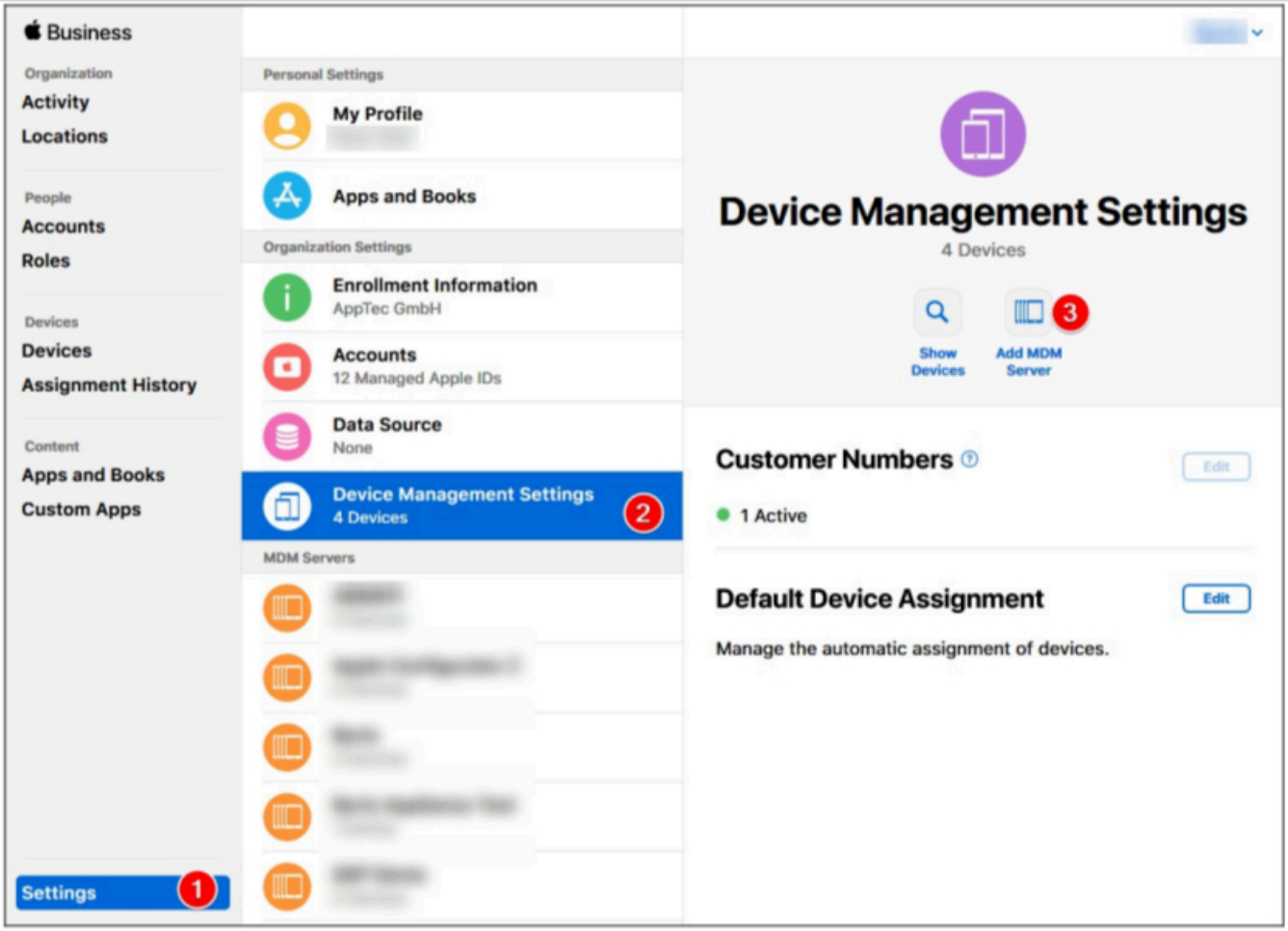
DEP (Device Enrollment Program) memungkinkan Anda mendaftarkan perangkat dengan mudah ke dalam MDM. Ketika menggunakan DEP, perangkat akan secara otomatis terhubung ke MDM ketika mengatur perangkat. Anda juga dapat melewatkan hampir semua langkah penyiapan yang biasanya wajib dilakukan pada iOS.

Perlu diingat bahwa Anda harus membeli perangkat dari reseller yang mendukung DEP. Untuk informasi lebih lanjut, hubungi reseller Anda atau Apple.

Informasi lebih lanjut tentang DEP: https://www.apple.com/business/dep/

Klik tanda "+" untuk menambahkan DEP Token. Pada Popup, klik "sertifikat baru" pada teks (ditandai dengan warna kuning pada gambar di bawah). Ini akan menghasilkan dan mengunduh sertifikat DEP. Setelah itu, buka Apple Business Manager(https://business.apple.com/) atau Apple School Manager(https://school.apple.com/).

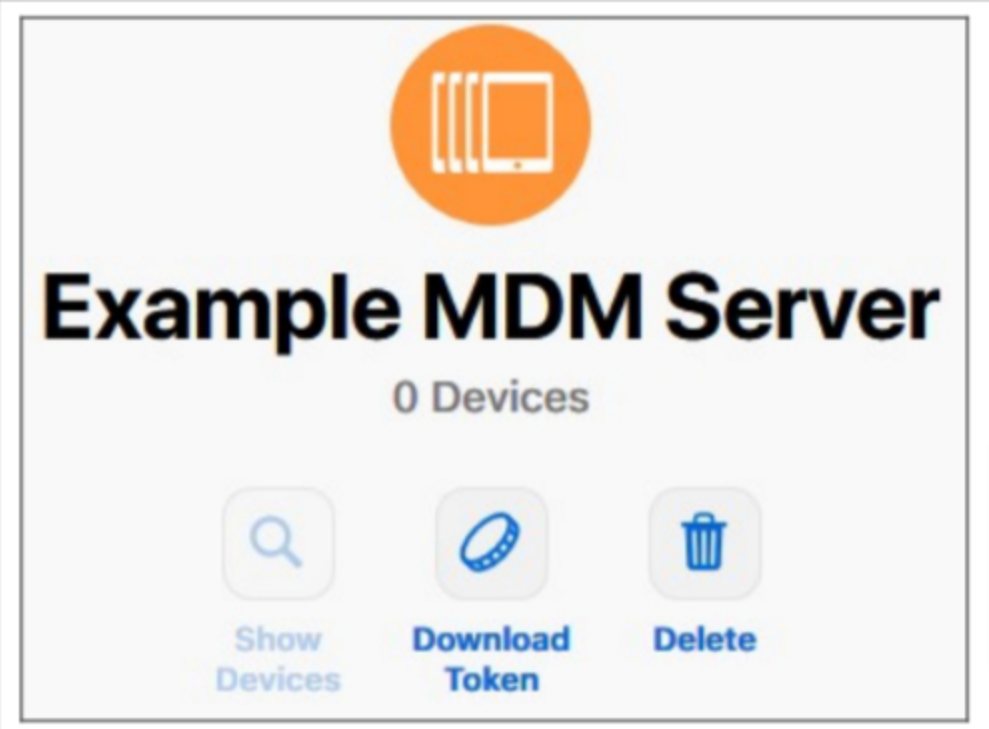




Di Apple Business Manager, ikuti langkah-langkah seperti yang ditunjukkan pada gambar di atas. Pengaturan → Pengaturan Manajemen Perangkat → Tambahkan Server MDM.

Berikan nama Server apa pun yang Anda inginkan dan unggah Sertifikat DEP yang telah diunduh sebelumnya di bawah Pengaturan Server MDM → Unggah Kunci Publik dan klik "Simpan".

Anda sekarang akan memiliki opsi "Unduh Token". Klik ini dan simpan. Token hanya berlaku selama 1 tahun. Tetapi hanya dengan mengklik "Unduh Token" lagi, Anda akan mendapatkan token yang baru, yang membuat pembaruan token menjadi sangat mudah.



Anda sekarang dapat kembali ke MDM, tempat Anda sebelumnya mengunduh Sertifikat DEP. Jika Anda tidak menutup tab, popup untuk menambahkan DEP Server seharusnya masih terbuka dan Sertifikat DEP seharusnya sudah dipilih. Anda sekarang dapat mengunggah Token Anda di bidang "DEP Token" dan klik DEP Server.

Pada kolom "**Perangkat**" Anda akan melihat jumlah perangkat yang ditugaskan ke Server DEP ini. Perangkat yang ditambahkan ke server DEP ini akan secara otomatis dibuat di DEP Pool di Manajemen Seluler.

Anda dapat mengklik nomor ini untuk mendapatkan gambaran umum mengenai semua perangkat DEP Anda dan statusnya.

Catatan: Tergantung pada alur kerja atau konfigurasi Anda di Manajer Bisnis, mungkin Anda harus menetapkan perangkat ini secara manual ke DEP Server. Anda juga dapat mengatur DEP Server default di Apple Business Manager untuk perangkat baru.

Pada kolom "**Profil**", Anda dapat melihat jumlah Profil DEP yang Anda miliki. Anda juga dapat mengklik nomor ini untuk melihat detail mengenai Profil DEP Anda dan Anda dapat menghapus profil lama/tidak terpakai di sini. Saat ini tidak memungkinkan untuk mengubahnya. Jika Anda ingin melakukan perubahan, Anda harus membuat yang baru.

Pada kolom "**Sinkronisasi Terakhir**", Anda dapat menyinkronkan Server DEP secara manual (misalnya jika Anda baru saja menambahkan perangkat baru ke DEP) dan melihat tanggal sinkronisasi terakhir yang berhasil.

Pada kolom "**Profil Otomatis**" Anda dapat menetapkan profil DEP sebagai default otomatis. Profil ini akan ditetapkan secara otomatis ke perangkat baru. Jika Anda tidak menetapkan Profil Otomatis, Anda harus menetapkan profil secara manual ke perangkat baru setiap kali.

Pada kolom "**Tambah Profil**" Anda dapat menambahkan profil DEP baru. Perangkat akan menerima ini pada awal penyiapan perangkat. Profil DEP mendefinisikan bagaimana perangkat diatur dan langkah pengaturan mana yang akan dilewati.

Catatan: setelah perangkat didaftarkan, pengaturan ini hanya dapat diubah dengan melakukan pengaturan ulang pabrik dan mendaftarkan perangkat dengan profil baru. Hal ini terutama relevan untuk "**Removable**" dan "**Izinkan pemasangan**". Untuk "Izinkan**pemasangan**", disarankan untuk mengaktifkannya, karena ini dapat dinonaktifkan melalui pembatasan MDM, tetapi tidak dapat diaktifkan lagi jika dinonaktifkan di profil DEP.

Pada kolom "**Edit**" Anda dapat mengunggah token baru, misalnya saat memperbarui Token.

Konfigurator & URL

URL Pendaftaran Kolam Renang

Di sini Anda dapat membuat URL pendaftaran dan Kode QR pendaftaran yang berlaku untuk jumlah pendaftaran tertentu dan hingga tanggal tertentu. Hal ini memungkinkan Anda untuk mendaftarkan beberapa perangkat yang hanya memiliki satu tautan atau kode QR.

Perangkat yang terdaftar dengan URL atau QR Code ini akan berada di Pool di Manajemen Seluler dan Anda harus menetapkannya secara manual ke grup atau pengguna setelahnya.

Catatan: ini hanya untuk pendaftaran manual. Jangan gunakan URL ini jika Anda mendaftarkan perangkat melalui Apple Configurator

Profil MDM – Konfigurator Apple

Di sini Anda bisa mendapatkan URL yang Anda perlukan saat mendaftarkan perangkat melalui Apple Configurator. Saat menyiapkan perangkat dengan Apple Configurator, Anda dapat menambahkan perangkat ke MDM dalam proses yang sama. Apple Configurator memerlukan URL ini untuk melakukan hal ini.

Perangkat yang ditambahkan melalui Apple Configurator akan berada di Pool di Manajemen Seluler dan Anda harus menetapkannya secara manual ke grup atau pengguna setelahnya.

Anda juga akan menemukan file .mobileconfig di sini yang dapat digunakan untuk mendaftarkan perangkat melalui Apple Configurator. Bagaimanapun, penggunaan URL ini direkomendasikan.

Konfigurasi Android

Konfigurasi Android

Copot Pemasangan Perlindungan	Jika fungsi ini diaktifkan, pengguna tidak dapat menonaktifkan administrator perangkat, tanpa memasukkan kata sandi yang ditetapkan oleh Administrator MDM. Kata sandi ditetapkan selama pendaftaran, sehingga perangkat harus didaftarkan ulang untuk memperbarui kata sandi. Ada dua opsi untuk menghapus administrator perangkat: 1. Secara manual pada perangkat ◦ Buka Aplikasi EMM pada perangkat ◦ Beralih ke tab Status ◦ Ketuk "Copot Pemasangan Proteksi" ◦ Masukkan kata sandi Anda dapat menggunakan Revisi untuk mendapatkan kata sandi yang benar dari "Riwayat Kata Sandi" di konsol. ◦ Gulir ke bawah dan ketuk titik yang baru ditambahkan, "Ketuk untuk menghapus Aplikasi MDM AppTec360" (Anda memiliki waktu 20 detik untuk melakukan tugas ini) ◦ Konfirmasikan dialog "Copot pemasangan Aplikasi MDM AppTec360" dengan "ok". Ini akan membatalkan pendaftaran perangkat dari konsol. ◦ Untuk menghapus Aplikasi dari perangkat, konfirmasikan dialog "AppTec360 MDM akan dihapus instalasinya" dengan "UNINSTALL" 2. otomatis (Konsol) ◦ Pilih Perangkat di konsol ◦ Klik ikon roda gigi biru dan pilih "Enterprise Wipe" Catatan: Hanya tersedia dengan Android 4.x dan versi yang lebih rendah atau pada perangkat dengan API KNOX (perangkat Samsung)

Copot Pemasangan Kata Sandi (Revisi x)	Kata sandi yang ditetapkan, yang dapat digunakan pengguna untuk menghapus administrator perangkat Revisi x = penghitung, seberapa sering kata sandi telah diubah Penting untuk mengetahui kata sandi mana yang dibutuhkan pengguna, karena ada kemungkinan perangkat belum berkomunikasi dengan Server AppTec360 dan oleh karena itu kata sandi terbaru belum dikirimkan
Riwayat Kata Sandi	Ketika Anda mengklik tombol biru ("Tampilkan Riwayat"), Anda dapat melihat kata sandi yang telah dibuat sebelumnya
Perlindungan Penghapusan Instalasi yang Diperpanjang	Opsi ini menawarkan perlindungan terhadap perangkat yang tidak AMAN Selama pengaturan ini diaktifkan, tidak mungkin menonaktifkan administrator perangkat dengan mudah
Meminta pengguna untuk menghapus Aplikasi yang diblokir?	Jika memungkinkan, Aplikasi yang diblokir tidak hanya akan diblokir tetapi juga dihapus secara otomatis. Pengguna akan diminta untuk menghapus Aplikasi yang diblokir jika tidak ada penghapusan otomatis yang dapat dilakukan.
Pemblokiran Aplikasi Sistem Cerdas	Jika Daftar Putih diaktifkan, Klien MDM Android akan memblokir semua Aplikasi yang diinstal pengguna. Aktifkan pengaturan ini untuk memblokir semua Aplikasi Sistem yang dapat diluncurkan dalam mode Daftar Putih.

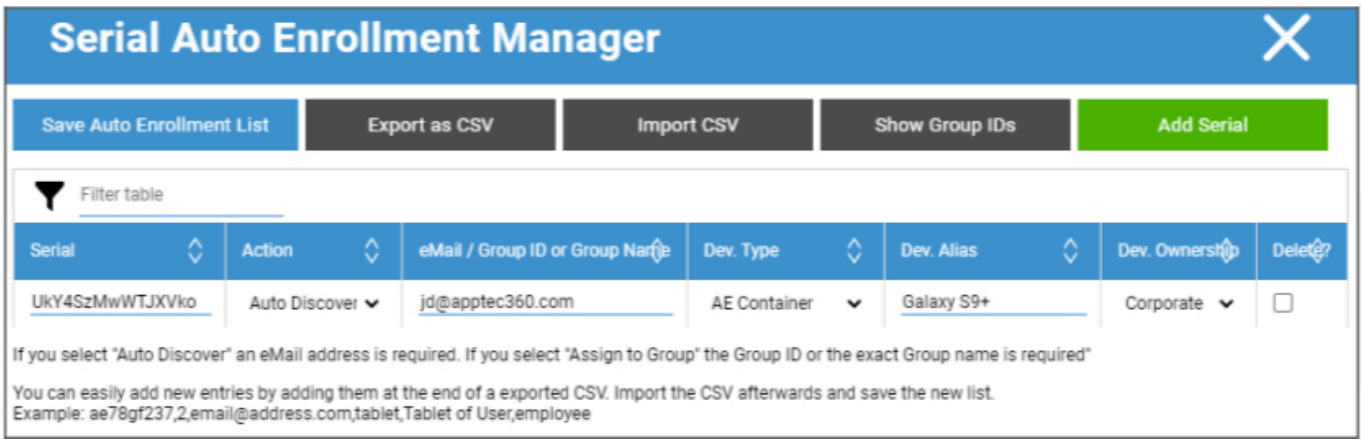
Pendaftaran Otomatis

Di sini Anda dapat mengaktifkan fitur Pendaftaran Otomatis untuk mendaftarkan perangkat Anda secara otomatis ketika AppTec360 MDM Client dibuka pada perangkat.

Penting: Metode pendaftaran ini sudah tidak digunakan lagi dan tidak lagi berfungsi pada Android 10 atau lebih tinggi. Bagaimanapun, saat menggunakan Android 7 atau lebih tinggi, Anda harus mendaftarkan perangkat sebagai Android Enterprise yang dikelola sepenuhnya. Jika Anda ingin menggunakan wadah Android Enterprise BYOD dan Anda menggunakan Android 10 atau lebih tinggi, Anda harus mendaftarkan perangkat secara manual melalui kredensial, Kode QR atau SMS. Bagaimanapun, Daftar Pendaftaran Otomatis masih digunakan untuk mengotomatiskan proses pendaftaran, misalnya Pendaftaran AE, Pendaftaran Knox, dll.

Bagaimanapun, Daftar Pendaftaran Otomatis masih digunakan untuk mengotomatiskan proses pendaftaran, misalnya Pendaftaran AE, Pendaftaran Knox, dll.

Dengan mengklik "Serial Manager" atau "IMEI Manager", Anda dapat menambahkan Serial atau IMEI perangkat Anda masing-masing. Anda tidak perlu melakukan keduanya untuk perangkat Anda, cukup satu saja.



Tindakan menentukan apakah perangkat akan didaftarkan ke dalam pool, pengguna atau grup.

Anda juga dapat mengekspor dan mengimpor file .csv dan memfilter entri Anda dengan kata kunci.

Perusahaan Android

Di sini Anda dapat menyiapkan Android Enterprise. Hal ini diperlukan untuk menggunakan semua fitur Android Enterprise.

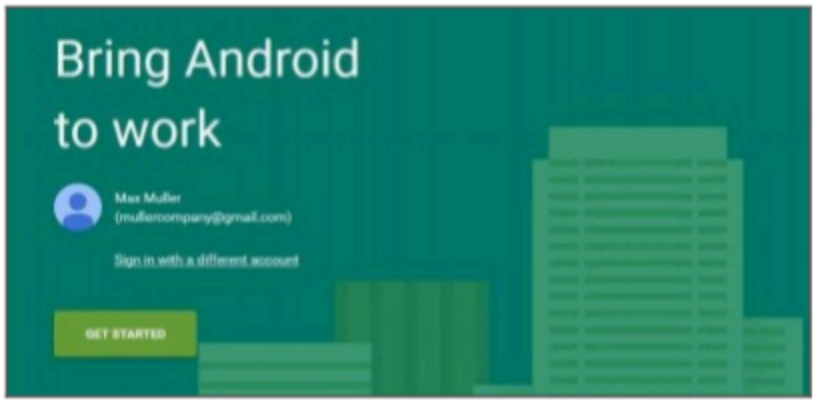
Metode Pertama: Akun Perusahaan Android (Akun Google)

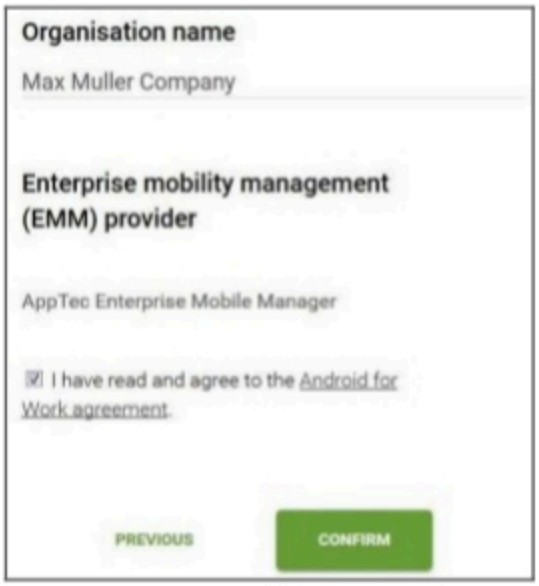
Pertama-tama tekan "Siapkan Penyiapan", kemudian setelah beberapa saat akan muncul tombol "Mulai Penyiapan".

Ini akan membawa Anda ke Halaman Pengaturan Perusahaan Android Google.

Masuk dengan Akun Google yang ingin Anda gunakan, jika Anda belum masuk dan tekan "Mulai".

Sekarang Anda dapat memasukkan nama perusahaan Anda. Setelah melakukannya, centang kotak centang dan tekan "Konfirmasi"





Pada langkah terakhir, Anda dapat menyelesaikan pendaftaran Anda dan kembali ke konsol. Jika semuanya berhasil, tampilannya akan seperti ini:

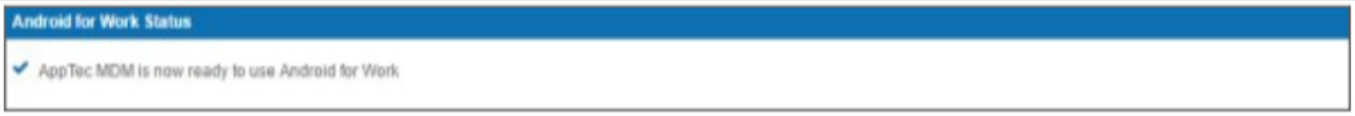
Sekarang Anda bisa mulai mengonfigurasi Android Enterprise Container.

Metode Kedua: Akun G-Suite

Tekan "Gunakan G-Suite" dan masuk ke Akun Admin Google Anda. Di sana Anda akan masuk ke "Keamanan" -> "Tampilkan lebih banyak" -> "Kelola penyedia EMM untuk Android" dan buatlah Token. Catatan: Jika Anda tidak melihat Pengaturan Perusahaan Android di Akun G-Suite Anda, Anda harus membuka "Dapatkan lebih banyak aplikasi dan layanan" dan menambahkan manajemen perangkat Android. Sekarang masukkan Token dan Domain utama Anda di konsol kami dan klik "Simpan Perubahan". Setelah selesai, klik "Gunakan Akun Perusahaan Android".

Sekarang Anda akan melihat Tombol "Buat Akun Layanan". Klik di atasnya. Proses ini bisa memakan waktu beberapa saat.

Jika semuanya berhasil, seharusnya terlihat seperti ini:



Sekarang Anda bisa mulai mengonfigurasi Android Enterprise Container.

Perlindungan Reset Pabrik

Dengan Perlindungan Pengaturan Ulang Pabrik, Anda dapat mengikat perangkat Anda ke akun google pilihan Anda, yang juga mengesampingkan pengikatan yang sudah ada ke akun google. Untuk menggunakan Perlindungan Pengaturan Ulang Pabrik, Anda harus mengaturnya di sini terlebih dahulu dan mengaktifkannya di profil Anda setelahnya.

Untuk mengatur Perlindungan Reset Pabrik, klik "Pengaturan FRP" dan ikuti petunjuk pada layar.

CATATAN: Baca dan lakukan langkah-langkahnya dengan cermat. Kami sarankan untuk melakukan hal ini di jendela browser penyamaran baru untuk menghindari masuk secara otomatis ke Akun Google yang salah. Anda dapat mengunci diri Anda sepenuhnya dari perangkat, jika Anda memasukkan ID yang salah atau kehilangan akses ke Akun Google yang digunakan!

Pendaftaran AE

Di sini Anda dapat mengaktifkan Android Enterprise Ernollment. Menggunakan Metode ini akan mendaftarkan Perangkat Anda ke dalam Mode Pemilik Perangkat Android Enterprise. Dalam mode ini, Anda akan memiliki kontrol penuh atas perangkat.

Mengaktifkan Pendaftaran AE	Mengaktifkan Peringatan Pendaftaran AE: Jika Anda menonaktifkan Pendaftaran AE, Kode QR yang ada dan perangkat pemrogram NFC yang sudah dikonfigurasi akan berhenti berfungsi. Jika Anda mengaktifkan lagi Pendaftaran AE, Anda harus mengirim ulang konfigurasi push NFC/menghasilkan kode QR baru.
Aktifkan Temukan Otomatis	Ketika perangkat mendaftarkan dirinya sendiri melalui "Pendaftaran AE", sistem akan mencoba menetapkannya ke pengguna berdasarkan informasi yang ditetapkan dalam Daftar Putih Serial / IMEI ("Pengaturan Umum" > "Konfigurasi Android" > "Pendaftaran Otomatis").
Blokir Perangkat Tidak Dikenal	Hanya perangkat yang telah masuk dalam daftar putih di Daftar Putih Serial / IMEI ("Pengaturan Umum" > "Konfigurasi Android" > "Pendaftaran Otomatis") yang diizinkan untuk mendaftar.

Catatan tentang Metode 1 & 2: "Layar Selamat Datang" mengacu pada layar pertama yang Anda lihat setelah pengaturan ulang pabrik. Tampilannya bisa berbeda tergantung pada versi Android dan/atau model perangkat yang Anda gunakan.

Metode 1: Pendaftaran Kode QR

(memerlukan Android 7.0 atau lebih tinggi) Kami merekomendasikan untuk selalu menggunakan metode ini jika Anda menjalankan Android 7 atau lebih tinggi.

1. Menyetel ulang perangkat ke pengaturan pabrik
2. Buat Kode QR untuk Pendaftaran menggunakan salah satu dari dua metode berikut:
    - Klik di "Pengaturan Umum -> Konfigurasi Android -> Pendaftaran AE" pada "Hasilkan Kode QR". Pilih apakah Anda ingin melewatkan enkripsi penyimpanan dan/atau semua aplikasi sistem harus dihapus.
    - (alternatif) Pilih Perangkat yang sudah ada. Pada "Ikhtisar Perangkat", klik Kode QR yang ditampilkan di sana. Pilih apakah Anda ingin melewatkan enkripsi penyimpanan dan/atau semua aplikasi sistem harus dihapus.
3. Sekarang ketuk 6 kali pada Layar Selamat Datang perangkat Anda. Ini akan memulai Mode Pendaftaran QR.
4. Sekarang sambungkan ke jaringan nirkabel dan tunggu beberapa saat hingga pembaca kode QR terinstal
5. Sekarang pindai kode QR
6. Selesai. Perangkat Anda sekarang terdaftar dalam Mode Perangkat Perusahaan Android.

- a. Jika Anda menggunakan Kode QR di "Pengaturan Umum", Anda dapat menemukan perangkat Anda di "Pool -> Perangkat Pemilik Perangkat AE". (Petunjuk: Ada kemungkinan Anda harus memuat ulang situs untuk melihat perangkat). Jika Anda mencentang "Aktifkan Auto Discover", Anda akan menemukannya di dalam pengguna Auto Discover.
- Jika Anda menggunakan kode QR dari profil perangkat yang sudah ada, perangkat akan didaftarkan ke dalam profil ini.

Metode 2: Pendaftaran NFC

(memerlukan NFC dan Android 6.0 atau lebih tinggi)

Persiapan: Masukkan informasi WiFi Anda dalam "Pengaturan Umum -> Konfigurasi Android -> Pendaftaran AE -> Data untuk penyediaan NFC". Sekarang, gunakan "NFC Device" untuk mencari perangkat yang akan menjadi programmer. Perangkat ini akan digunakan untuk mengirim informasi pendaftaran ke perangkat lain melalui NFC.

1. Setel Ulang Pabrik perangkat Anda
2. Buka aplikasi pemasangan NFC dari AppTec360 pada programmer Anda
3. Pilih jika Anda ingin melewatkan enkripsi penyimpanan dan/atau semua aplikasi sistem harus dihapus.
4. Pegang kedua perangkat saling membelakangi
5. Sekarang Pendaftaran Perusahaan Android harus mencolok
6. Anda sekarang menemukan perangkat Anda di konsol
    - a. Di kolam renang, jika Anda belum mengonfigurasi Auto Discover
    - b. Di dalam pengguna, Anda mengonfigurasi untuk Temukan Otomatis
    - c. Petunjuk: Ada kemungkinan Anda harus memuat ulang situs untuk melihat perangkat

Metode 3: Akun Google

(membutuhkan Android 5.1 atau lebih tinggi)

(Catatan: Jika Anda menggunakan metode ini, perangkat tidak akan terdaftar secara otomatis. Sebaliknya, Anda harus mendaftarkannya secara manual atau mengotomatiskan prosesnya dengan menggunakan Auto Enrollment).

1. Setel Ulang Pabrik perangkat Anda
2. Lakukan langkah-langkah penyiapan hingga Anda dapat masuk dengan akun Google
3. Masukkan "afw#apptec" sebagai Nama Pengguna/Mail
4. Ketuk "Berikutnya"
5. Perangkat Anda sekarang menjadi Perangkat Perusahaan Android

Pendaftaran KNOX

Di sini Anda dapat mengaktifkan Pendaftaran KNOX dan menemukan informasi yang Anda perlukan untuk membuat Profil Pendaftaran KNOX di Portal Penerapan KNOX. Anda memerlukan Akun di KNOX Deployment Portal untuk mengonfigurasi dan menggunakan ini.

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

Aktifkan Pendaftaran KNOX	Mengaktifkan Pendaftaran KNOX. Perhatian: Jika Anda menonaktifkan Pendaftaran KNOX, profil MDM yang sudah ada akan berhenti berfungsi. Jika Anda mengaktifkan kembali Pendaftaran KNOX, Anda harus memperbarui bidang "Data JSON Khusus" pada Profil MDM Anda
Aktifkan Temukan Otomatis	Ketika perangkat mendaftarkan dirinya sendiri melalui "Pendaftaran KNOX", sistem akan mencoba menetapkannya ke pengguna berdasarkan informasi yang ditetapkan dalam Daftar Putih Serial / IMEI ("Pengaturan Umum" > "Konfigurasi Android" > "Pendaftaran Otomatis").

1. Masuk ke Portal Pendaftaran Seluler Samsung KNOX https://eukme.samsungknox.com/itadmin
2. Buka "Profil MDM"
3. Klik pada "Tambah"
4. Pilih "Server URI tidak diperlukan untuk MDM saya" dan klik "Berikutnya"
5. Sekarang buat profil dengan informasi yang ditampilkan di konsol manajemen

Sekarang Profil Pendaftaran KNOX ini dapat langsung diinstal pada perangkat oleh Samsung jika Anda memperoleh perangkat dari Samsung secara langsung.

Atau Anda dapat mengunduh Aplikasi Penyebaran KNOX, masuk dengan Akun Penyebaran KNOX Anda dan mengirim Profil Pendaftaran KNOX melalui NFC ke perangkat lain.

Jika perangkat memiliki Profil Pendaftaran KNOX yang diinstal, perangkat akan mengunduh Aplikasi kami dan mendaftarkan perangkat, jika perangkat memiliki koneksi internet yang berfungsi.

Pendaftaran perangkat melalui KNOX Enrollment dapat ditemukan di "Pool -> KNOX Enrollment", atau dalam pengguna yang Anda tentukan di Auto Discover.

Zero-Touch

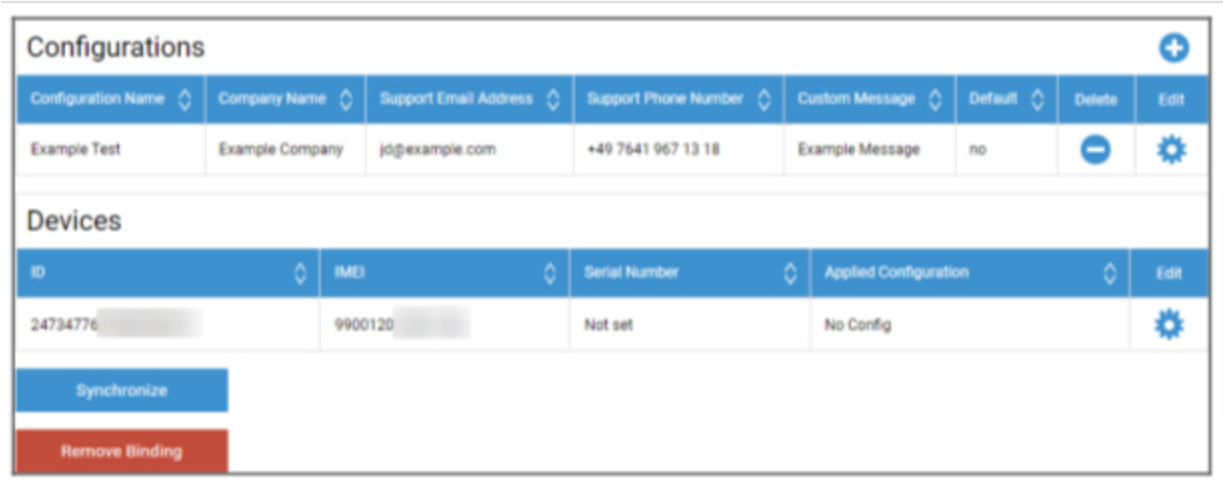
Dengan Zero-Touch, Anda dapat dengan mudah mendaftarkan perangkat Anda tanpa perlu menyentuhnya atau mengonfigurasi apa pun pada perangkat itu sendiri. Anda hanya perlu menyalakannya, melanjutkan konfigurasi seperti biasa dan perangkat akan menerima semua informasi tentang cara mengatur dan terhubung ke MDM secara otomatis.

Untuk menggunakan Zero-Touch, Anda harus membeli perangkat dari Reseller yang mendukung Zero-Touch. Reseller yang sama juga akan membuatkan Akun untuk Anda di Zero-Touch Portal. Hubungi Reseller Anda untuk mendapatkan info lebih lanjut tentang prosedur atau jika Anda mengalami masalah saat mengakses Zero-Touch Portal.

Klik "Mulai Penyiapan" untuk memulai penyiapan. Anda akan diarahkan ke halaman login di mana Anda harus memilih Akun Google yang memiliki akses ke Zero-Touch Portal.

CATATAN: Anda dapat memilih Akun APAPUN. Jadi, pastikan untuk memilih Akun yang benar pada langkah ini. Jika Anda tidak melihat perangkat/konfigurasi Anda, kemungkinan besar Anda menggunakan Akun yang salah.

Setelah menyelesaikan login, akan terlihat seperti ini:



Klik "+" untuk menambahkan Konfigurasi dan isi bidang seperti yang ditampilkan di layar. Jika Anda mengaktifkan Konfigurasi sebagai Konfigurasi default, konfigurasi tersebut akan ditetapkan ke perangkat baru secara otomatis. Membuat atau menetapkan konfigurasi default tidak akan menetapkannya ke perangkat yang sudah ada.

Jika perangkat tidak memiliki Konfigurasi yang ditetapkan, perangkat akan diatur sebagai perangkat normal dan tidak akan tersambung ke MDM. Oleh karena itu, pastikan perangkat Anda memiliki Konfigurasi yang ditetapkan.

Setelah Anda menghubungkan Akun Anda, perangkat Anda terlihat dan Anda memiliki Konfigurasi yang ditetapkan untuk perangkat tersebut, Anda dapat mulai mengatur perangkat.

Anda dapat menambahkan perangkat ke Daftar Pendaftaran Otomatis agar perangkat tersebut dapat didaftarkan ke grup atau pengguna tertentu secara otomatis. Jika Anda tidak mengonfigurasi apa pun di daftar Auto Enrollment, perangkat akan didaftarkan ke dalam Pool.

Konfigurasi Windows

Konfigurasi Windows

Di sini Anda memiliki opsi untuk mengaktifkan konfigurasi berikut pada PC Windows 10 Anda:

Koneksi DM Instan	
Waktu Coba Ulang Awal	Menetapkan upaya koneksi pertama ke perangkat, nilai ini meningkat secara eksponensial
Mencoba Ulang Koneksi	Menunjukkan berapa banyak upaya koneksi yang harus dilakukan oleh klien DM, selama terjadi kesalahan koneksi
Waktu Tidur Maksimum	Menunjukkan waktu tidur maksimum setelah terjadi kesalahan koneksi
Mencoba Ulang Sinkronisasi Pertama	Interval, di mana perangkat akan berkomunikasi dengan server, setelah koneksi pertama
Interval Percobaan Ulang Pertama	Terkait dengan "Sinkronisasi Ulang Pertama" Di sini waktu dicantumkan dalam menit Misalnya di bawah "Sinkronisasi Ulang Pertama" tercantum nilai "2" dan di bawah "Interval Coba Ulang Pertama" tercantum nilai "4 Menit", dengan cara ini perangkat berkomunikasi 2 kali setiap 4 menit, setelah koneksi pertama
Mencoba Ulang Sinkronisasi Kedua	Interval, di mana perangkat harus berkomunikasi dengan server, setelah menyelesaikan "Sinkronisasi Ulang Pertama"
Interval Coba Ulang Kedua	Prinsip yang sama seperti untuk "Interval Coba Ulang Pertama" - hanya saja di sini, prinsip ini berlaku untuk "Sinkronisasi Ulang Kedua"
Mencoba Ulang Sinkronisasi Reguler	Interval, seberapa sering perangkat harus berkomunikasi dengan server di masa mendatang Default: "Tak Terbatas" Kami sarankan untuk tidak mengubah nilai ini, karena jika Anda memasukkan "10", perangkat akan berkomunikasi dengan server 10x dan kemudian berhenti Oleh karena itu, komunikasi dengan server AppTec360 terputus!
Interval Coba Ulang Reguler	Prinsip yang sama seperti "First/Second Retry Interval" - hanya saja di sini, ini menerapkan pengaturan untuk masa mendatang
Interval Coba Ulang Reguler	Prinsip yang sama seperti "First/Second Retry Interval" - hanya saja di sini, ini menerapkan pengaturan untuk masa mendatang

Kotak Konten

Konfigurasi

Di sini Anda dapat mengonfigurasi ContentBox. Anda dapat menempatkan file untuk grup di ContentBox yang dapat diakses dengan Aplikasi ContentBox pada perangkat.

Aktifkan Kotak Konten	Aktifkan ContentBox. Menonaktifkan ini jika Anda tidak menggunakan ContentBox, dapat menghemat sumber daya pada mesin OnPremise.
Gunakan penginstalan ContentBox eksternal	ContentBox juga dapat dioperasikan dengan Nextcloud Anda sendiri.
URL	URL lengkap dari entitas Nextcloud
Pengguna Root	Pengguna Root dari Akun Nextcloud
Kata Sandi Root	Kata sandi root dari Akun Nextcloud
Izin folder grup default	Izin folder grup default, dapat dimodifikasi satu per satu berdasarkan grup (di Manajemen Seluler)
Berbagi folder grup dengan subgrup	Jika aktif, setiap subgrup dapat membaca semua folder grup utama, juga dapat dikonfigurasikan secara individual untuk setiap grup (Manajemen Seluler)
Izin untuk subkelompok	Izin untuk subkelompok dapat dikonfigurasi secara individual untuk setiap grup (Manajemen Seluler)
Izinkan berbagi	Memungkinkan pengguna untuk berbagi konten melalui Tautan, dapat dikonfigurasi secara individual untuk setiap grup
Ukuran Unggah File Maksimum dalam MB	Ukuran maksimum file Standar: 512 MB Konfigurasi maksimum: 2048
Kredensial WebDAV	
URL WebDAV	Anda juga dapat membuka ContentBox dengan WebDAV. Jangan hapus folder berikut ini, dalam keadaan apa pun: /apptecgroups /apptecgroups/AppTecGroup-X
Pengguna Root	Nama Pengguna Root
Kata sandi	Kata Sandi Pengguna Root

Sinkronisasi dengan ContentBox terjadi secara otomatis. Namun, Anda dapat melakukan sinkronisasi manual dengan "Sinkronisasi ContentBox".

Selain itu, di sini Anda dapat mengaktifkan/menonaktifkan ContentBox pada masing-masing perangkat.

Ini hanya relevan, jika Anda belum melisensikan ContentBox, maka Anda masih memiliki akses ke 25 perangkat yang dapat digunakan untuk menguji ContentBox - di sini Anda dapat mengaktifkannya untuk masing-masing perangkat.

Konfigurasi LDAP

Ikhtisar LDAP

Di sini Anda dapat membuat koneksi ke Direktori Aktif Anda melalui LDAP untuk mengimpor pengguna dan grup secara massal. Sinkronisasi harus dilakukan secara manual. Anda dapat mengonfigurasi beberapa koneksi LDAP ke sistem yang berbeda atau dengan konfigurasi/filter yang berbeda.

Nama Server	Tampilan Nama Server
Jenis	Saat ini hanya Direktori Aktif yang mendukung LDAP yang didukung
Domain LDAP	Domain LDAP utama (misalnya example.com)
Host LDAP	Hanya diperlukan jika host LDAP tidak dapat dijangkau di bawah Domain LDAP yang diberikan.
Pelabuhan	Biarkan kosong untuk menggunakan Port Standar (389 atau 636 untuk SSL)
Nama pengguna	Contoh: CN = John, OU = Pengguna, DC = CONTOH, DC = COM Catatan: Sebagian besar sistem mengharuskan nama pengguna dalam format ini dan tidak menerima "John" sebagai Nama Pengguna
Kata sandi	
Konfirmasi Kata Sandi	
Keamanan Koneksi	Catatan: saat menggunakan SSL atau TLS, sertifikat Direktori Aktif akan diperiksa. Jika ini ditandatangani sendiri, Anda harus menambahkan root CA ke penyimpanan kepercayaan Mesin OnPremise. Jika Anda menggunakan Cloud, Direktori Aktif harus menyediakan sertifikat tepercaya atau koneksi hanya akan berfungsi tanpa Enkripsi
Sinkronisasi Otomatis.	Mengaktifkan sinkronisasi otomatis direktori LDAP dalam interval waktu yang ditentukan dalam pengaturan umum LDAP.
Basis DN	Jika Anda tidak ingin menyinkronkan seluruh direktori, Anda dapat menentukan OU di sini, misalnya OU = AndroidUsers, OU = Users, DC = EXAMPLE, DC = COM
Anggota	Semua pengguna yang diimpor akan ditambahkan ke grup yang dipilih
Hanya pengguna yang diaktifkan?	Ketika diaktifkan, atribut userAccountControl akan dipertimbangkan, pengguna tanpa atribut tersebut tidak akan diimpor.
Filter LDAP	Anda dapat menggunakan Filter LDAP untuk memfilter Pengguna mana yang akan diimpor

Filter Regex	Anda dapat menggunakan Filter Regex untuk memfilter Pengguna mana yang akan diimpor
Uji Koneksi	Menguji koneksi saat menyimpan konfigurasi
Atur ulang struktur direktori saat sinkronisasi?	Jika benar, semua entri LDAP akan dipindahkan kembali ke lokasi aslinya di pohon LDAP. Disarankan untuk diaktifkan.
Mengimpor ulang pengguna dan grup yang dihapus?	Bila diaktifkan, pengguna dan grup yang telah dihapus akan dibuat ulang. Disarankan untuk diaktifkan.
Penghapusan sinkronisasi?	Bila diaktifkan, grup dan pengguna akan dihapus bila dihapus di server LDAP. Perangkat pengguna yang dihapus juga akan dihapus.

Di bawah daftar Konfigurasi LDAP, Anda dapat menentukan periode sinkronisasi sistem secara otomatis. Hanya menggunakan Konfigurasi LDAP untuk sinkronisasi otomatis yang memiliki opsi yang sesuai yang diaktifkan.

Manajemen Aplikasi

DB Aplikasi In-House

Android

Di sini Anda dapat mengunggah Aplikasi Android yang telah dikembangkan perusahaan Anda dan mendistribusikannya nanti di Manajemen Seluler di profil perangkat atau grup.

Perlu diketahui bahwa kami menyarankan untuk hanya mendistribusikan Aplikasi dengan cara ini, yang tidak tersedia di Google Play Store.

Klik "+" untuk mengunggah APK dari Aplikasi yang ingin Anda unggah. Hanya format APK yang saat ini didukung.

Batas unggahan pada Peralatan OnPremise dapat ditingkatkan di Langkah 3 Konfigurasi Peralatan. Jika Anda ingin meningkatkan Batas Unggah di Cloud, silakan hubungi bagian dukungan untuk informasi lebih lanjut.

Perlu diketahui bahwa biasanya APK berukuran sedikit lebih kecil daripada kontennya. Ada kemungkinan pengunggahan gagal karena hal ini, karena APK dibongkar dalam prosesnya. Misalnya, ada kemungkinan APK berukuran 95MB gagal dengan batas unggahan 100MB. Dalam kasus ini, tingkatkan batas unggahan seperti yang disebutkan di atas.

Kami juga menyarankan untuk terlebih dahulu memindahkan APK secara manual ke satu perangkat uji (misalnya melalui USB) dan mencoba menginstalnya secara manual dengan aplikasi Files pada perangkat. Jika cara ini tidak berhasil karena alasan apa pun, maka proses instalasi melalui MDM juga akan gagal.

Perbarui Target

Dengan fitur "Update Target" Anda dapat memilih versi aplikasi yang harus diinstal atau ke versi mana aplikasi harus diperbarui jika Anda mengaktifkan "Keep up to date" untuk sebuah aplikasi.

Jika Anda belum memilih Target Pembaruan, versi tertinggi akan digunakan.

Ingatlah bahwa Android tidak dapat menurunkan versi aplikasi. Perlu diketahui juga bahwa "Kode Versi" menentukan apakah suatu versi lebih tinggi, lebih rendah, atau sama. Jadi, pastikan untuk meningkatkan versi ini dengan benar di aplikasi Anda saat membuat pembaruan.

iOS

Di sini Anda dapat mengunggah Aplikasi iOS yang Anda kembangkan dan mendistribusikannya nanti di Manajemen Seluler di profil perangkat atau grup Anda.

Klik "+" untuk mengunggah IPA dari Aplikasi yang ingin Anda unggah. Hanya format IPA yang didukung untuk saat ini.

Batas unggahan pada Peralatan OnPremise dapat ditingkatkan di Langkah 3 Konfigurasi Peralatan. Jika Anda ingin meningkatkan Batas Unggah di Cloud, silakan hubungi bagian dukungan untuk informasi lebih lanjut.

Perbarui Target

Dengan fitur "Update Target" Anda dapat memilih versi aplikasi yang harus diinstal atau ke versi mana aplikasi harus diperbarui jika Anda mengaktifkan "Keep up to date" untuk sebuah aplikasi.

Jika Anda belum memilih Target Pembaruan, versi tertinggi akan digunakan.

MacOS

Di sini Anda dapat mengunggah Aplikasi MacOS yang Anda kembangkan dan mendistribusikannya nanti di Manajemen Seluler di profil perangkat atau grup.

Klik "+" untuk mengunggah PKG dari Aplikasi yang ingin Anda unggah. Hanya format PKG yang didukung untuk saat ini.

Batas unggahan pada Peralatan OnPremise dapat ditingkatkan di Langkah 3 Konfigurasi Peralatan. Jika Anda ingin meningkatkan Batas Unggah di Cloud, silakan hubungi bagian dukungan untuk informasi lebih lanjut.

Perbarui Target

Dengan fungsi "Perbarui Target", Anda dapat memilih versi aplikasi mana yang harus diinstal atau ke versi mana aplikasi harus diperbarui jika Anda mengaktifkan "Selalu perbarui" untuk suatu aplikasi.

Jika Anda belum memilih Target Pembaruan, versi tertinggi akan digunakan.

Windows 10

Di sini Anda dapat mengunggah Aplikasi Windows 10 dan mendistribusikannya nanti di Manajemen Seluler di profil perangkat atau grup Anda.

Klik "+" untuk mengunggah APPX, APPXBUNDLE atau MSI dari Aplikasi yang ingin Anda unggah. Hanya format APPX, APPXBUNDLE atau MSI yang didukung untuk saat ini.

Anda juga dapat mengunggah dan menentukan Ketergantungan untuk Aplikasi, yang akan secara otomatis didistribusikan dan diinstal sebelum menginstal Aplikasi yang diinginkan.

Batas unggahan pada Peralatan OnPremise dapat ditingkatkan di Langkah 3 Konfigurasi Peralatan. Jika Anda ingin meningkatkan Batas Unggah di Cloud, silakan hubungi bagian dukungan untuk informasi lebih lanjut.

Perbarui Target

Dengan fungsi "Perbarui Target", Anda dapat memilih versi aplikasi mana yang harus diinstal atau ke versi mana aplikasi harus diperbarui jika Anda mengaktifkan "Selalu perbarui" untuk suatu aplikasi.

Jika Anda belum memilih Target Pembaruan, versi tertinggi akan digunakan.

Paket Win32 (.exe)

Anda juga dapat mendistribusikan file/penginstal .exe ke perangkat Anda.

Nama paket	Nama yang akan ditampilkan di MDM
Deskripsi	Deskripsi yang ditampilkan dalam MDM
File paket	Hanya file .zip yang diperbolehkan. Tempatkan file yang ingin Anda gunakan dalam file zip ini.
Konteks penerapan	**Sistem**: Perintah install berjalan dengan hak akses sistem yang lebih tinggi dari "User". Juga ketika menggunakan "System", prosesnya tidak memiliki UI, sehingga akan diam dan profil pengguna, misalnya variabel lingkungan seperti %AppDat%, tidak dapat diakses. **User**: Perintah install memiliki akses ke profil pengguna dan dapat menampilkan UI jika diperlukan. Catatan: Beberapa proses mungkin hanya bekerja dalam satu konteks. Misalnya, jika perangkat lunak menginstal dirinya sendiri ke dalam AppData, ia hanya akan bekerja ketika memilih "User"
Instal perintah	Perintah yang digunakan untuk menginstal program. Sebagai contoh perintah install untuk file zip yang berisi "setup.exe" di root-nya, yang mendukung parameter "/s" untuk instalasi tanpa suara, perintah Install adalah "setup.exe /s". Perlu diketahui bahwa perangkat lunak yang berbeda mungkin memiliki parameter yang berbeda.
Copot pemasangan perintah	Perintah yang harus dijalankan untuk menghapus perangkat lunak melalui MDM. Biasanya ini mengarah ke pencopot pemasangan. Misalnya "C:\Program Files\ExampleSoftware\uninstall.exe".
Persyaratan	
Catatan: Semua persyaratan yang ditetapkan harus dipenuhi agar perangkat lunak dapat diinstal. Jika tidak, perangkat lunak tidak akan diinstal. Beberapa bidang mungkin wajib diisi. Jika tidak ada nilai yang ditetapkan untuk suatu persyaratan, persyaratan tersebut akan diabaikan.	
Arsitektur OS	Arsitektur OS
Versi OS Min	Versi OS Min
Ruang disk kosong minimum (MB)	Ruang disk kosong minimum (MB)
Memori fisik minimum (MB)	Memori fisik minimum (MB)
Jumlah minimum prosesor logis	Jumlah minimum prosesor logis

Kecepatan CPU minimum (MHz)	Kecepatan CPU minimum (MHz)
Persyaratan Tambahan	Anda juga dapat menentukan aturan secara manual atau mengunggah skrip di sini untuk melakukan pemeriksaan persyaratan tambahan jika Anda mau.
Aturan Deteksi	
Metode deteksi	Di sini Anda dapat menentukan cara mendeteksi apakah aplikasi telah diinstal pada perangkat. Perintah instal hanya akan dijalankan ketika aturan ini mendeteksi bahwa aplikasi TIDAK diinstal. Perintah hapus instalan hanya akan dijalankan jika aturan ini mendeteksi bahwa aplikasi tidak terinstal. **Menentukan aturan secara manual**: Memungkinkan Anda menentukan satu atau beberapa aturan secara manual untuk memeriksa, misalnya, apakah file, folder, MSI, atau kunci registri tertentu ada. Jika semua aturan deteksi yang diberikan benar, aplikasi akan dianggap ada. **Gunakan skrip**: Unggah skrip Anda sendiri dengan pemeriksaan Anda sendiri. Jika skrip mengembalikan "$TRUE", aplikasi akan dianggap ada.
Aturan deteksi	

Pengaturan Aplikasi

Pengaturan Aplikasi iOS

Di sini Anda dapat menentukan pengaturan default untuk menambahkan aplikasi ke aplikasi wajib atau toko aplikasi perusahaan.

Catatan: Ini hanya mengatur apa yang dipilih secara default saat menambahkan aplikasi. Ini TIDAK mengubah pengaturan yang sudah ada untuk aplikasi yang sudah ditambahkan di aplikasi wajib atau toko aplikasi perusahaan.

Tetap up to date	Secara otomatis memperbarui aplikasi. Perlu diketahui bahwa diperlukan waktu hingga 7 hari setelah pembaruan dirilis hingga aplikasi diperbarui.
Menyalip ketika tidak dikelola	Jika Aplikasi sudah diinstal sebagai tidak dikelola (oleh pengguna), aplikasi akan diambil alih dan dikelola oleh MDM.
Menghapus aplikasi saat profil MDM dihapus	Menghapus instalan Aplikasi saat MDM dihapus.
Mencegah pencadangan data aplikasi	Mencegah pencadangan data aplikasi.

Pengaturan Aplikasi Android

Di sini Anda dapat menentukan pengaturan default untuk menambahkan aplikasi ke aplikasi wajib atau toko aplikasi perusahaan.

Catatan: Ini hanya mengatur apa yang dipilih secara default saat menambahkan. Ini TIDAK mengubah pengaturan untuk aplikasi yang sudah ditambahkan di aplikasi wajib atau toko aplikasi perusahaan.

Tetap up to date	Secara otomatis memperbarui aplikasi. Hanya tersedia untuk Aplikasi InHouse.
Pembaruan Klien EMM AppTec360 yang Terkendali	Jika diaktifkan, Admin dapat menentukan target pembaruan untuk Klien EMM AppTec360. Daftar semua versi yang tersedia dari AppTec360 EMM Client akan ditampilkan di "Pengaturan Umum" → "Manajemen Aplikasi" → "DB Aplikasi Internal" → "Android".

Aplikasi Pihak Ketiga

Android

Di sini Anda dapat mengatur Kode Aktivasi untuk Ikarus.

Atur ke "Gunakan Kode Aktivasi" dan masukkan Kode Aktivasi Anda di sini.

Catatan: Setelah memasukkan Kode dan menyimpannya, Kode belum ditambahkan ke profil yang akan dikirim ke perangkat. Anda harus melakukan perubahan apa pun di profil Anda agar kode dapat ditambahkan ke profil. Misalnya, ubah Sakelar apa pun di Profil dari mati → hidup → mati - Simpan → Tetapkan sekarang.

iOS

Di sini Anda dapat memasukkan Lisensi SecurePIM Anda. Setelah memasukkan lisensi, tekan "Simpan Perubahan" dan Anda dapat menggunakan opsi SecurePIM.

VPP / KNOX Premium

Program Pembelian Volume Apple (VPP) memungkinkan Anda mendistribusikan Aplikasi berbayar dan gratis dengan mudah ke perangkat Anda. Hal ini sangat disarankan karena Anda tidak memerlukan ID Apple pada perangkat, pengguna tidak perlu mengonfirmasi penginstalan (diawasi), pengguna tidak perlu memasukkan kata sandi ID Apple, dan Anda dapat dengan mudah mendistribusikan Aplikasi berbayar tanpa harus membelinya lagi di setiap Perangkat.

Untuk menggunakan VPP, Anda harus mendaftar di Apple Business Manager.

Lisensi VPP

Di sini Anda bisa mendapatkan gambaran umum tentang Aplikasi VPP Anda, berapa banyak Lisensi yang digunakan dan berapa banyak yang tersedia.

Dengan mengeklik Roda, Anda dapat melihat perangkat mana saja yang memiliki Lisensi yang ditetapkan dan apa status Penetapan ini.

Mengklik pada akan menyegarkan Cache VPP yang membandingkan Lisensi yang ditetapkan di MDM dengan Lisensi yang ditetapkan di sisi Apel. Hal ini dapat mengatasi Masalah Lisensi dalam beberapa kasus.

Token VPP

Di sini Anda bisa mengunggah Token VPP Anda, yang bisa ditemukan di Manajer Bisnis Apple di Pengaturan → Aplikasi & Buku. Anda dapat mengunggah beberapa Token VPP.

Anda dapat memperbarui Token hanya dengan mengunduh yang baru di Apple Business Manager, klik Roda "Edit" dan unggah yang baru.

"Mode VPP" memutuskan bagaimana Penugasan Lisensi ditangani. Tergantung pada skenario Anda, Anda harus menggunakan mode yang berbeda:

"Berbasis perangkat" harus digunakan saat mendaftarkan perangkat melalui QR Code, Link, Apple Configurator, atau DEP.

"Berbasis pengguna" diperlukan jika Perangkat didaftarkan dengan Pendaftaran Pengguna atau sebagai iPad Bersama.

Jika Anda mengaktifkan "Manajemen Lisensi Otomatis", pengguna yang dipindahkan dari satu grup ke grup lainnya akan secara otomatis diberikan lisensi Apple VPP berdasarkan profil grup tempat mereka dipindahkan.

Lisensi VPP Apple yang sudah ada dari grup tempat mereka pindah tidak akan dicabut.

Pengguna baru yang ditambahkan ke grup akan secara otomatis diberikan Lisensi Apple VPP berdasarkan profil grup masing-masing.

Kunci Premium KNOX

Di sini Anda dapat memasukkan Kunci Premium KNOX Anda untuk menggunakan Samsung KNOX Container.

Perlu diketahui bahwa ini tidak lagi didukung sejak Android 10. Sebagai gantinya, gunakan Android Enterprise Container.

Pengaturan App Store

Wilayah & Bahasa

Di sini Anda dapat mengatur Bahasa dan Wilayah default untuk Pencarian Aplikasi di Manajemen Aplikasi.

Perlu diketahui bahwa pengaturan untuk iTunes juga menentukan bagaimana sistem mengambil informasi tentang aplikasi tertentu. Jika Anda menemukan Aplikasi dalam daftar Anda yang ditampilkan dengan cara yang aneh (mis. Ikon yang hilang), Anda mungkin telah mengatur wilayah di mana Aplikasi tertentu tidak tersedia.

AE Play Store

Di sini Anda dapat menemukan semua Opsi untuk Play Store untuk Perangkat Perusahaan Android untuk menyetujui Aplikasi, mengunggah Aplikasi sendiri ke Play Store, atau membuat Aplikasi Web Anda sendiri.

Aplikasi yang Disetujui

Di sini Anda bisa mendapatkan Ikhtisar atas semua Aplikasi yang telah Anda setujui.

Aplikasi Play Store

Ini akan memuat iFrame yang menampilkan Play Store. Cari Aplikasi yang Anda inginkan, klik dan setujui. Saat menyetujui Aplikasi, Anda juga dapat menentukan bahwa persetujuan akan dicabut jika izin yang diperlukan berubah. Kami sarankan untuk membiarkan pengaturan ini default saat menyetujui Aplikasi.

Setelah Aplikasi disetujui, Anda dapat menambahkannya ke profil Anda.

Tombol "Setujui" akan berubah menjadi "Cabut persetujuan" setelah menyetujuinya, sehingga Anda selalu dapat menghapus Aplikasi jika Anda tidak memerlukannya lagi.

Aplikasi Pribadi

Di sini Anda dapat mengunggah Aplikasi Anda sendiri sebagai Aplikasi pribadi ke Google Play Store. Hal ini memungkinkan Anda untuk mendistribusikan Aplikasi melalui Layanan Google dan memperbaruinya melalui layanan tersebut. Hal ini juga memiliki manfaat bahwa Aplikasi Anda dapat diinstal tanpa konfirmasi pengguna yang biasanya diperlukan.

Aplikasi Web

Di sini Anda dapat membuat Aplikasi Web, yang merupakan tautan ke Halaman Web tertentu yang dapat ditetapkan seperti Aplikasi.

Anda juga dapat memberikan Ikon khusus dan menentukan lebih lanjut bagaimana tepatnya Ikon tersebut ditampilkan.

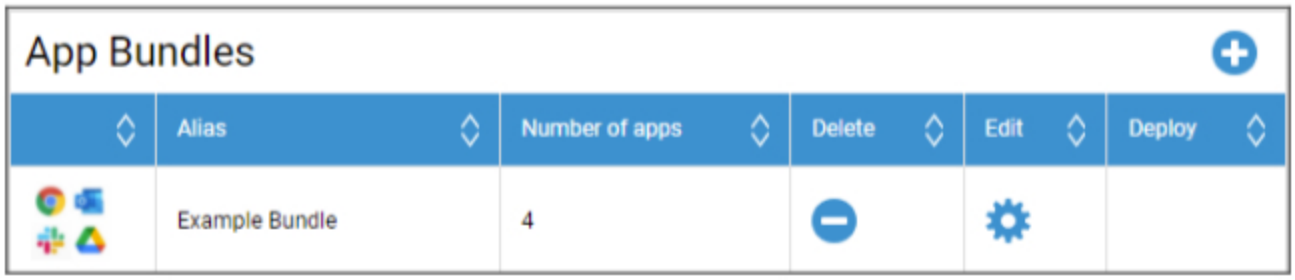
Tata Letak Toko

Tata Letak Toko menentukan bagaimana Aplikasi ditampilkan di Play Store atau apakah Aplikasi tersebut ditampilkan sama sekali.

Perlu diingat, jika Anda ingin menampilkan Aplikasi di Play Store agar pengguna dapat menginstal secara manual, ini harus ditambahkan di sini di Layout **DAN** di profil ke Play Store Perusahaan. Jika Anda menambahkan Aplikasi hanya pada salah satunya, maka Aplikasi tersebut tidak akan ditampilkan.

Bundel Aplikasi

Dengan App Bundle, Anda dapat menentukan grup aplikasi yang dapat ditetapkan ke profil perangkat atau grup dengan satu klik.



Klik "+" untuk membuat Bundel Aplikasi baru. Setelah membuat Bundel Aplikasi, Anda dapat mengeklik "Edit" untuk menambahkan aplikasi dari berbagai Sumber ke Bundel.

Bundel dapat ditambahkan ke profil seperti halnya Aplikasi lainnya. Saat menambahkan aplikasi, Anda akan memiliki Tab tambahan bernama "Bundel Aplikasi" di mana Anda memiliki Bundel Anda.

Jika Anda membuat perubahan apa pun pada Bundel Aplikasi, sebuah tombol di kolom "Deploy" akan muncul. Ini akan memungkinkan Anda untuk mendorong perubahan ini ke semua profil yang berisi Bundel ini. Jadi, perlu diingat bahwa Anda harus melakukan ini secara manual setelah menambahkan atau menghapus aplikasi dalam Bundel.

Kontrol Jarak Jauh

Penampil Tim

Konektor TeamViewer

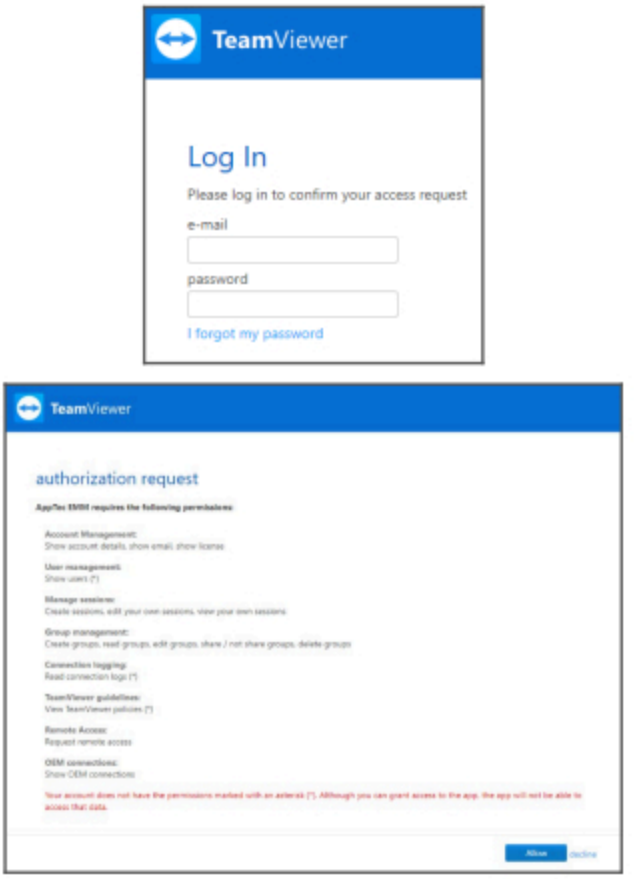
Catatan: Dalam uji coba gratis pada versi cloud kami, Anda tidak dapat menghubungkan akun TeamViewer Anda. Sebagai gantinya, Anda akan mendapatkan akun demo gratis yang ditautkan secara otomatis.

Buka Pengaturan Umum -> Remote Control -> TeamViewer. Di sini Anda dapat menautkan Akun TeamViewer dengan konsol atau melihat informasi tentang akun yang sedang terhubung. Anda juga dapat melihat semua sesi yang sedang aktif jika Anda membuka "Sesi Aktif".

Untuk menautkan akun Anda, klik "Mulai Pengaturan".

Dengan melakukan hal tersebut, Anda akan diarahkan ke halaman baru di mana Anda harus masuk dengan akun TeamViewer.

Setelah masuk, Anda telah mengesahkan AppTec360 MDM untuk menggunakan akun ini. Setelah mengonfirmasi hal ini, Anda harus menunggu beberapa detik dan Akun akan terhubung.


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

Instal TeamViewer QuickSupport

Tambahkan aplikasi "TeamViewer QuickSupport" ke aplikasi wajib di profil perangkat atau profil grup Anda dan klik "Tetapkan Sekarang". Tunggu hingga Aplikasi terinstal pada perangkat.

Jika Anda mencoba mengakses perangkat yang belum menginstal aplikasi, aplikasi akan diinstal atau diminta untuk menginstalnya, tergantung konfigurasi perangkat.

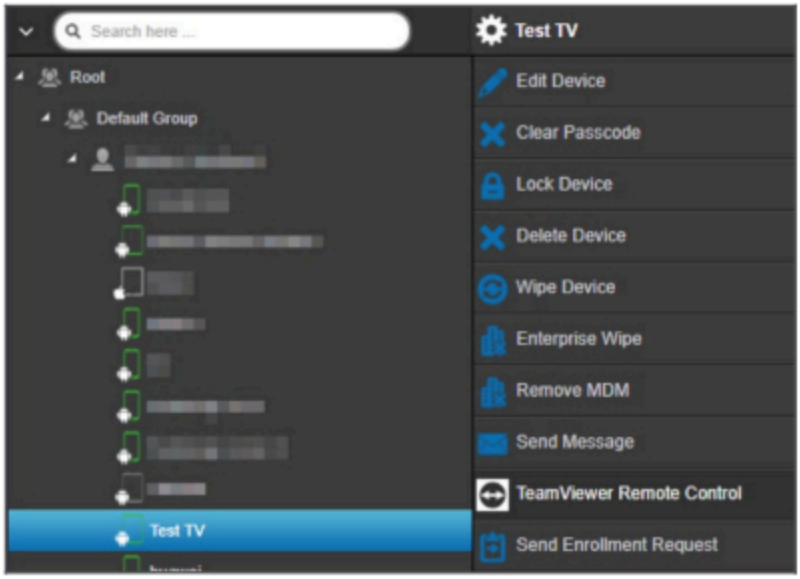
Kontrol jarak jauh perangkat Anda

Untuk mengontrol perangkat Anda dari jarak jauh, pilih perangkat, klik pada roda dan pilih "Kontrol Jarak Jauh TeamViewer"

Jika sudah ada sesi yang aktif, Anda dapat menggunakan sesi lama atau membuat sesi baru.

Konfirmasikan bahwa Anda ingin membuat Sesi TeamViewer baru.

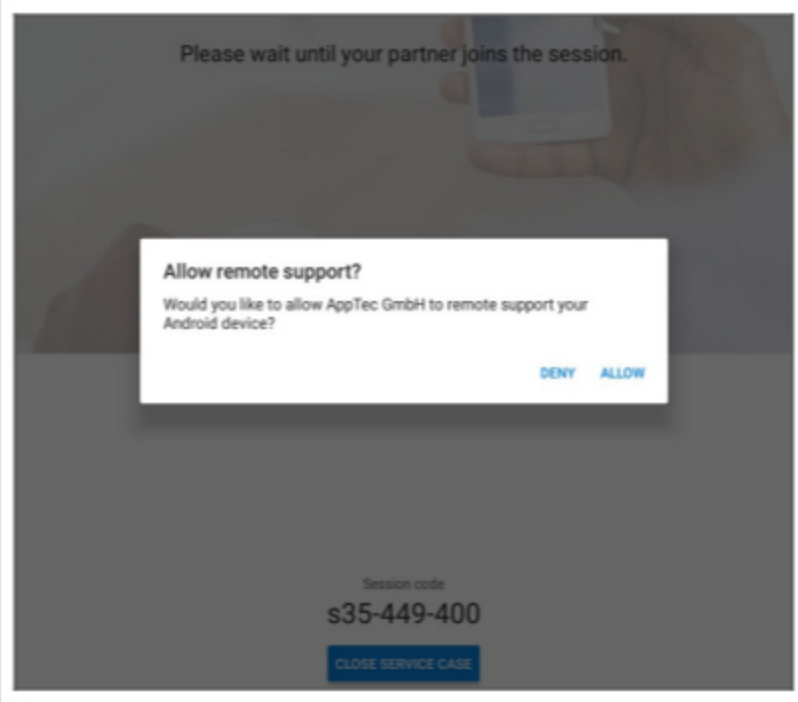
Setelah beberapa detik, Anda akan mendapatkan tautan untuk Sesi TeamViewer Anda. Anda dapat mengklik "Mulai" untuk membuka tautan ini di jendela baru.


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

Tautan ini akan membuka TeamViewer yang terinstal dan menghubungkan Anda ke perangkat.

Sekarang, Anda harus mengonfirmasi koneksi pada perangkat itu sendiri untuk mengendalikannya dari jarak jauh.



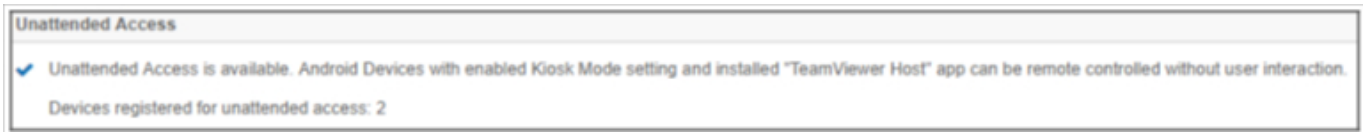
Jika Anda menggunakan iOS, Anda akan mendapatkan pesan di Klien MDM AppTec360. Dengan tautan tersebut, perangkat akan bergabung dengan sesi remote. Tergantung pada pengaturan

notifikasi perangkat, ada kemungkinan Anda tidak akan menerima notifikasi dan harus membuka AppTec360 MDM Client secara manual.

Pada sebagian perangkat Android (misalnya Samsung), Anda perlu menginstal aplikasi tambahan sebagai addon. Aplikasi TeamViewer pada perangkat akan memberi tahu Anda tentang hal itu, jika diperlukan pada perangkat Anda.

Akses Tanpa Pengawasan

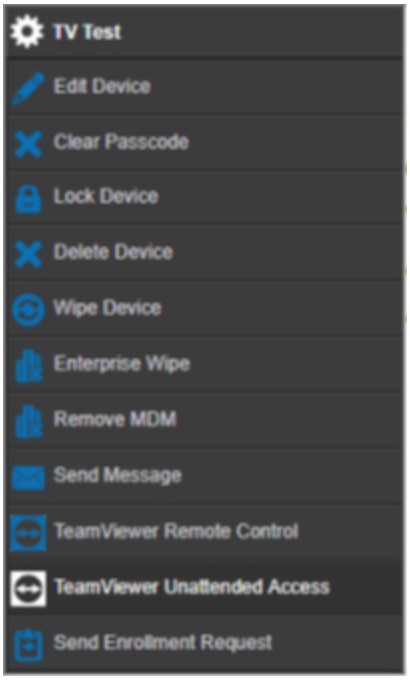
Catatan: Akses Tanpa Pengawasan hanya dapat dilakukan pada perangkat Android.



Anda hanya dapat menyambung ke perangkat Anda, tanpa menerima sambungan pada perangkat, jika Akun TeamViewer Anda menggunakan Lisensi "Tensor" atau "Perusahaan".

Anda dapat memeriksanya, setelah menautkan akun Anda, di "Pengaturan Umum"

Untuk menggunakan akses tanpa pengawasan, Anda harus menginstal aplikasi "TeamViewer Host" dan mengaktifkan "Aktifkan Akses Tanpa Pengawasan" di bawah "Mode Kios & Peluncur" di profil Anda. Perlu diketahui bahwa ini hanya dapat dilakukan jika Anda menggunakan Mode Kios.



Sekarang Anda dapat memilih akses tanpa pengawasan jika Anda memilih perangkat Anda dan mengklik roda. Ini akan menghubungkan Anda ke perangkat Anda tanpa perlu konfirmasi pada perangkat itu sendiri. Perlu diketahui bahwa diperlukan waktu beberapa saat sampai Anda mendapatkan Tautan untuk mengakses perangkat Anda.

Splashtop

Jika Anda mengaktifkan opsi Splashtop, Anda akan melihat opsi konfigurasi Splashtop di profil Anda.

Untuk menggunakan Splashtop, Anda harus mengatur Splashtop Streamer (com.splashtop.streamer.csrs) sebagai aplikasi wajib di profil Anda. Setelah itu Anda dapat mengaktifkan Konfigurasi Splashtop di profil Anda di "Remote Control". Mengaktifkan ini akan mengkonfigurasi aplikasi Splashtop Streamer. Jika Anda menggunakan Splashtop Streamer tetapi tidak dikombinasikan dengan MDM, Anda harus membiarkannya tidak aktif.

Pada profil Anda di bawah "Remote Control" Anda juga harus mengatur kode penyebaran. Buka https://my.splashtop.com dan masuk ke akun Splashtop Anda. Klik "Tambah Komputer" dan salin 12 digit kode deploy dari halaman yang muncul.

Tanpa Deploy Code, remote control TIDAK dapat dilakukan.

Setelah melakukannya, Anda dapat mengklik kanan perangkat Anda dan memulai Sesi jarak jauh dengan mengklik "Kontrol Jarak Jauh Splashtop"

Manajemen Kartu Sim

Impor Massal CSV

Ini menunjukkan ikhtisar atas Kartu Sim yang Anda tetapkan dan semua informasi tentangnya. Hal ini membantu Anda memiliki semua informasi, tidak hanya tentang perangkat Anda tetapi juga tentang Kartu Sim Anda dalam satu sistem.

CATATAN: Ini adalah manajemen/dokumentasi manual. Data ini tidak dapat diperoleh secara otomatis dari perangkat karena mekanisme privasi/keamanan sistem operasi.

Anda juga dapat mengeluarkan dan mengimpor daftar ini sebagai CSV.

Operator & Tarif

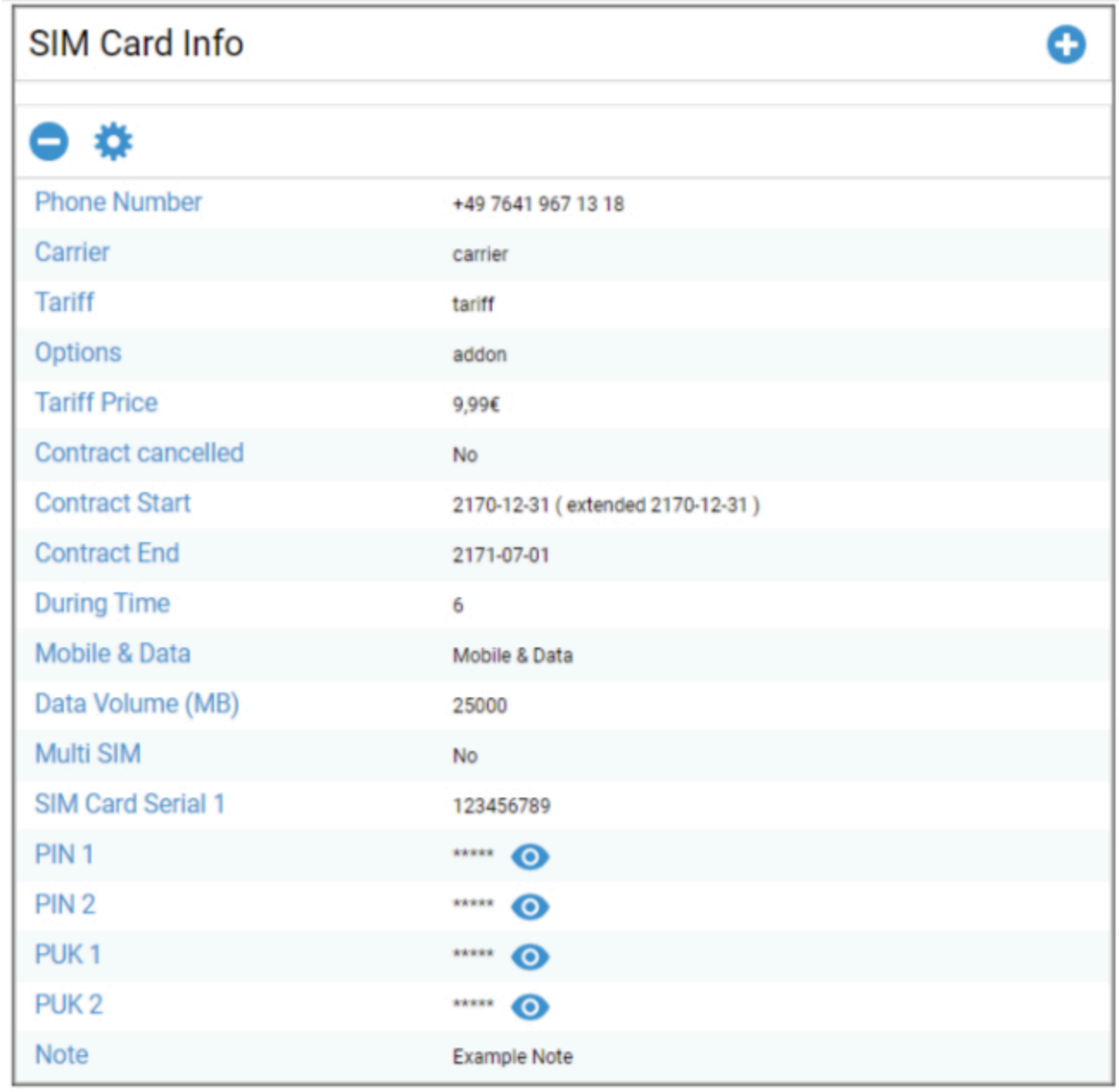
Untuk menambahkan kartu Sim, pertama-tama klik Tombol untuk menambahkan satu atau beberapa operator.

Setelah itu klik "+" pada "Informasi Tarif" untuk menambahkan tarif ke operator.

Secara opsional, Anda dapat menambahkan Add-On opsional di bawah ini jika Anda memiliki sesuatu seperti ini.

Ini menyiapkan semua yang Anda butuhkan untuk menambahkan Kartu Sim yang sebenarnya. Kartu Sim saat ini ditetapkan ke Pengguna. Oleh karena itu, buka Manajemen Seluler, pilih Pengguna dan buka "Ikhtisar Kartu Sim.

Di sini Anda melihat Kartu Sim pengguna ini. Jika ada, Anda dapat mengedit atau menghapusnya. Pengguna dapat memiliki beberapa Kartu Sim.

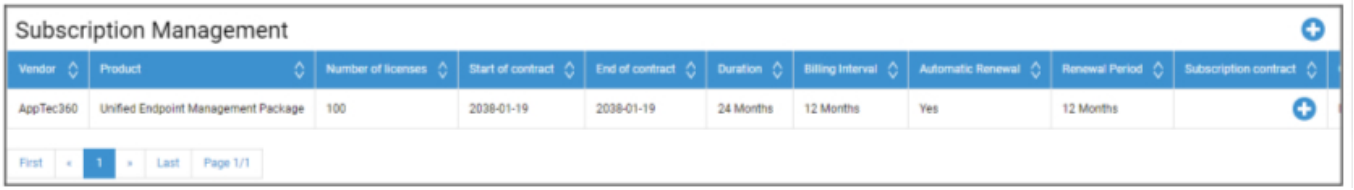


Klik pada "+" untuk menambahkan Kartu Sim dan tambahkan semua Info yang Anda butuhkan. Kartu Sim ini juga akan tercantum dalam daftar semua Kartu Sim Anda di Pengaturan Umum → Manajemen Kartu Sim.

Manajemen Langganan

Manajemen Langganan

Di sini Anda dapat mendokumentasikan langganan yang sedang berjalan, detailnya, dan juga menyimpan file yang berbeda, misalnya kontrak yang telah ditandatangani, Surat penghentian, dll. Anda juga dapat mengatur pengingat yang mengingatkan Anda per surat sebelum langganan berakhir dan mungkin diperpanjang secara otomatis.



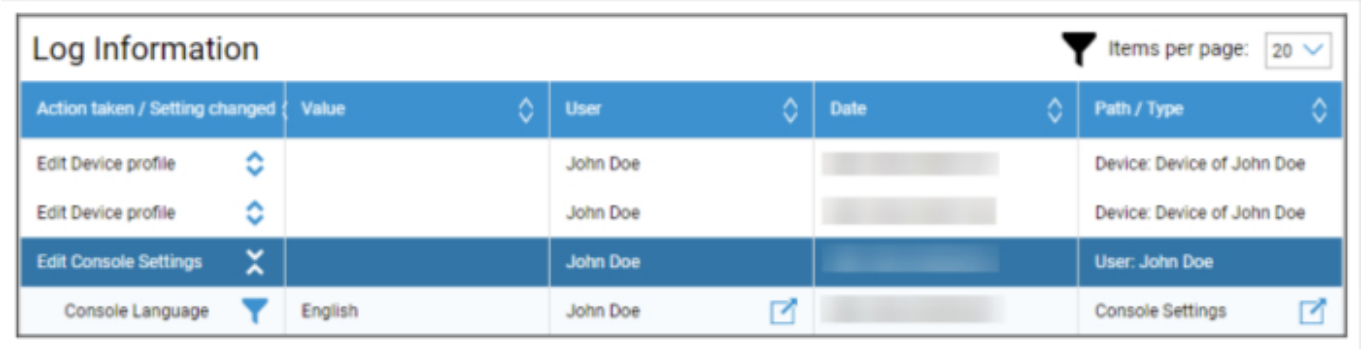
Klik "+" di bagian atas untuk menambahkan langganan. Anda dapat menambahkan langganan sebanyak yang Anda inginkan.

Klik "+" pada bidang yang berbeda untuk mengunggah file terkait Langganan ini. Secara teknis, Anda dapat mengunggah jenis file apa pun, namun perlu diketahui bahwa tidak semua jenis file dapat dipratinjau di browser.

Catatan Audit Umum

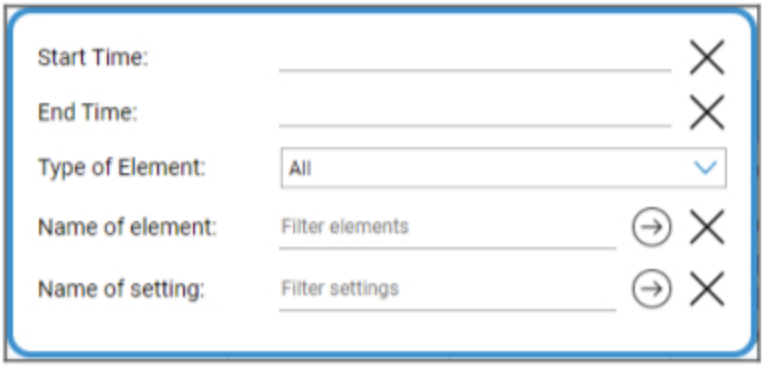
Log Audit

Di sini Anda memiliki Log Audit umum yang menunjukkan semua perubahan yang dibuat. Sementara Audit Log pada pengguna atau grup hanya menunjukkan perubahan menurut pengguna atau grup ini, ini menunjukkan SETIAP perubahan yang dibuat di mana saja di konsol.



Anda dapat melihat apa yang telah diubah, oleh siapa, kapan dan di mana. Dalam beberapa kasus, Anda juga dapat memperluas Entri untuk melihat detail lebih lanjut.

Anda dapat mengklik pengguna atau entri di "Path / Type" untuk menuju ke lokasi di mana perubahan telah dibuat.



Di kanan atas, Anda juga dapat menentukan filter yang dapat membantu menemukan perubahan tertentu dalam lingkungan di mana banyak perubahan yang terjadi.

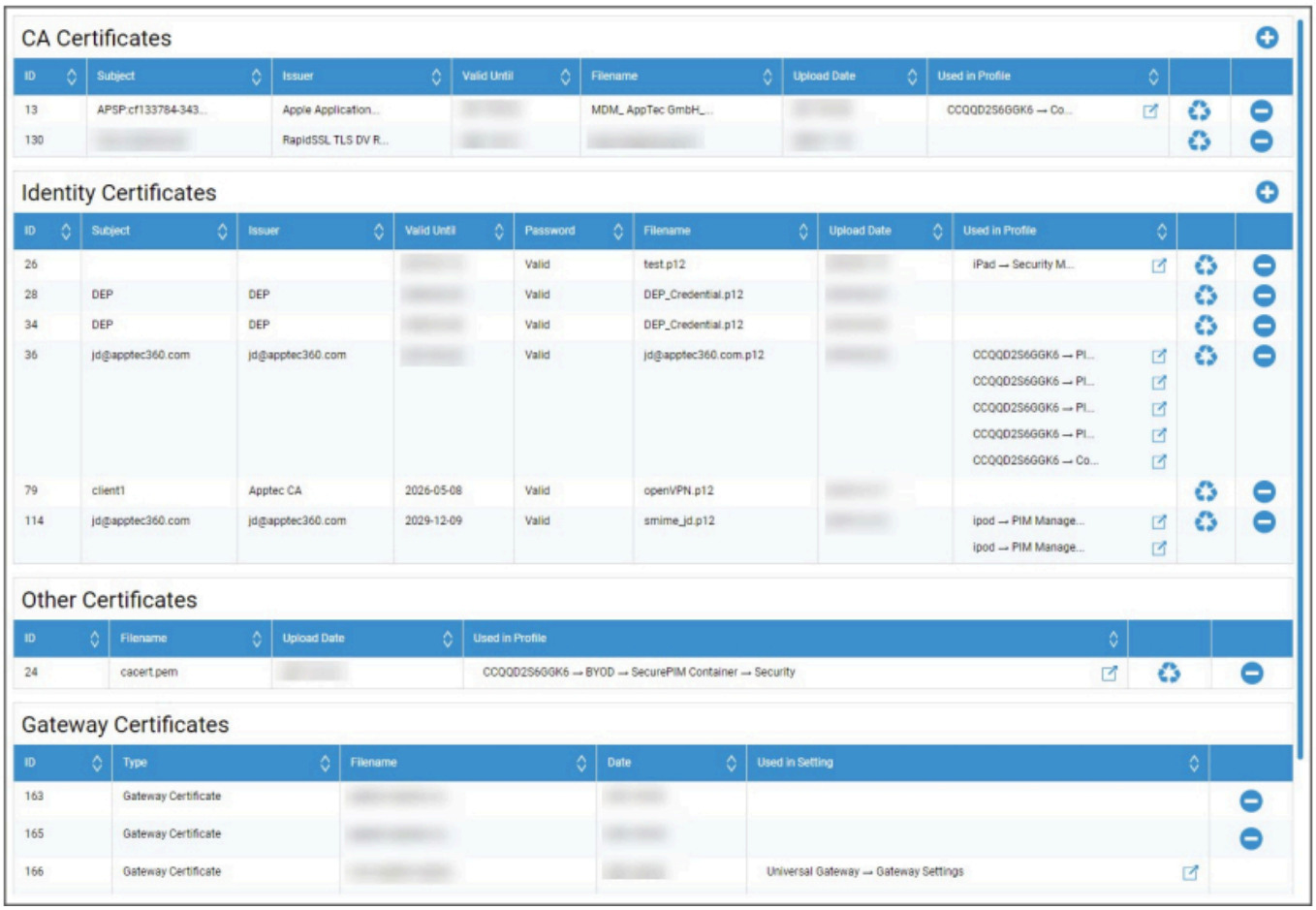
Pengaturan Log Audit

"Periode Penyimpanan Log Audit" mendefinisikan berapa lama Log Audit harus disimpan sebelum dihapus.

Manajemen Sertifikat

Di sini Anda akan mendapatkan gambaran umum tentang semua sertifikat yang diunggah dan digunakan di Konsol. Ini hanya gambaran umum. Konfigurasi aktual untuk, misalnya, sertifikat Wi-Fi masih dilakukan di profil di lokasi yang sesuai.

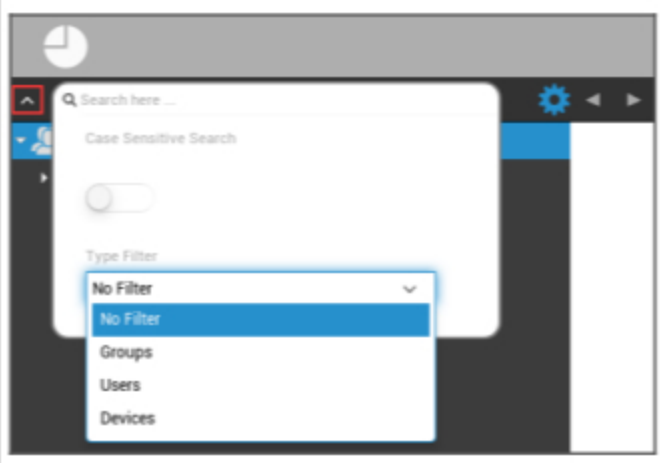
Di sini Anda juga dapat menghapus atau memperbarui sertifikat, yang secara otomatis akan tercermin dalam profil yang terpengaruh. Klik pada info di "Digunakan di Profil" untuk melihat di mana tepatnya sertifikat yang masih ditetapkan.



Manajemen Seluler

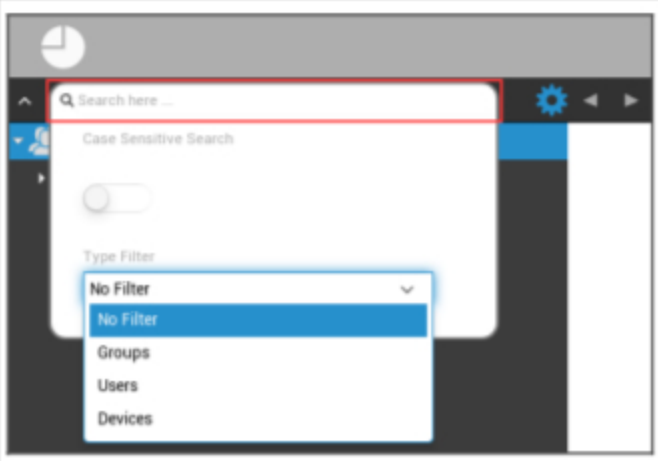
Layar Manajemen Seluler

Filter perangkat



Dengan satu klik di sudut kiri atas layar, Anda bisa menemukan beragam filter untuk tampilan perangkat.

Jendela pencarian



Jendela pencarian memungkinkan Anda mencari semua perangkat dan/atau pengguna dengan kata kunci tertentu.

Perlengkapan pilihan

Setelah mengeklik masing-masing simbol, daftar opsi yang tersedia bagi Anda, akan ditampilkan.

Hal ini berubah pada setiap jendela saat ini dan dijelaskan dalam masing-masing bab.

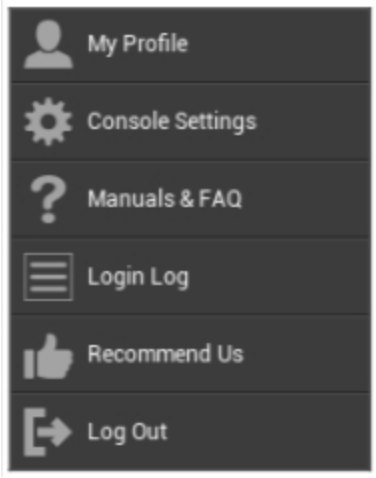
Panah navigasi

Dengan mengklik panah kiri, Anda akan dibawa ke halaman sebelumnya.

Setelah itu, dengan klik pada panah kanan, Anda akan dibawa ke halaman yang baru saja Anda tinggalkan.

Pengaturan akun administrasi

Mengklik alamat email seperti yang terlihat di atas akan menampilkan menu berikut:



Profil Saya	Mengedit detail akun admin
Pengaturan Konsol	Mengonfigurasi pengaturan konsol untuk akun Admin
Panduan & Tanya Jawab	Lihat halaman "Panduan & Tanya Jawab" di "Pengaturan Umum"
Log Masuk	Mengakses "Log Masuk"
Rekomendasikan Kami	Lihat halaman "Rekomendasikan Kami" di "Pengaturan Umum"
Log Out	Keluar dari konsol MDM

Informasi Pengguna

Di sini Anda dapat mengedit detail akun dari admin yang sedang login.

Nama pengguna	Nama pengguna dan/atau alamat email akun
Nama	Nama depan administrator
Nama belakang	Nama belakang administrator
Nama Login	Nama login administrator
Alamat email	Alamat email administrator
Alamat email alternatif	Alamat email alternatif administrator
Gambar	Gambar profil
Nomor Telepon	Nomor telepon administrator
Nomor ponsel	Nomor ponsel administrator
Perpanjangan Telepon	Perpanjangan telepon
Lokasi	Lokasi
Posisi	Posisi di perusahaan
Kelompok pengguna	Pilih grup pengguna yang ingin Anda tetapkan akun admin
Komentar	Masukkan komentar
Masukkan kata sandi baru	Masukkan kata sandi untuk perubahan kata sandi
Ulangi kata sandi baru	Ulangi kata sandi baru untuk mengonfirmasi

Harap diperhatikan, bahwa akses administrasi juga dapat diajukan sebagai akun pengguna lokal dalam struktur hirarki. Tanpa penetapan administrator tambahan, yang satu ini tidak boleh dihapus!

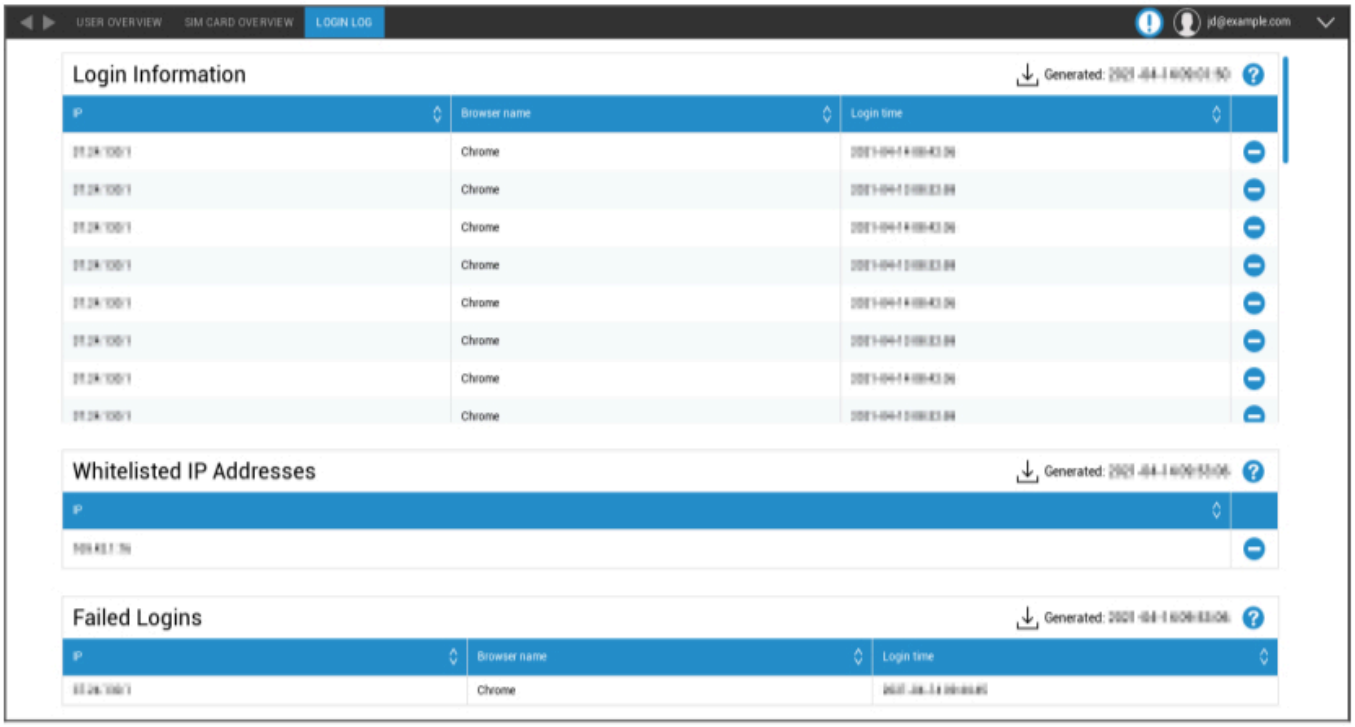
Pengaturan Konsol

Di sini Anda dapat mengonfigurasi pengaturan konsol berikut untuk akun Admin:

Opsi Tampilan Pengguna Direktori	Tentukan bagaimana pengguna harus diberi label di pohon
Opsi Tampilan Perangkat Direktori	Tentukan bagaimana perangkat harus diberi label di pohon
Batas Waktu Sesi	Jika pengguna tidak melakukan apa pun dalam waktu yang ditentukan, pengguna akan keluar. Nilai default adalah 60 menit. Harap keluar dan masuk lagi setelah mengubah pengaturan ini.
Zona waktu	Pilih zona waktu yang digunakan
Format Waktu	Memilih bagaimana stempel waktu akan ditampilkan
Bahasa Konsol	Pilih bahasa yang akan digunakan untuk menampilkan konsol. Tersedia bahasa Inggris dan Jerman.
Warna utama	Anda dapat menetapkan warna yang akan digunakan sebagai dasar untuk skema warna konsol. Anda bisa menggunakan pemilih warna, atau memasukkan warna dalam notasi HTML HEX. Formator RGB seperti 'merah muda', 'kuning' juga bisa digunakan.
Simpan Perintah	Kombinasi tombol untuk memicu penyimpanan tanpa menekan tombol "Save".
Gunakan Autentikasi Dua Faktor	Aktifkan penggunaan autentikasi dua faktor saat masuk. Anda akan menerima email saat login dengan kode yang harus Anda masukkan untuk masuk.
Batas Waktu Otentikasi Dua Faktor	Tetapkan periode waktu di mana Anda tidak akan diminta autentikasi dua faktor setelah autentikasi yang sudah berhasil.
Kirim Kode Verifikasi melalui	Kode verifikasi akan dikirim ke opsi yang dipilih. Pesan perangkat akan ditampilkan di AppTec360 MDM App di semua perangkat Android dan iOS milik Anda.
Kirim pesan masuk setelah masuk	Jika diaktifkan, email akan dikirim untuk setiap login dari alamat ip yang tidak masuk daftar putih. Email berisi informasi tentang login (mis. IP, Browser).

Log Masuk

Di sini Anda dapat melihat informasi mengenai login dari akun admin yang sedang login.



Informasi Login	Daftar yang berisi login dari akun admin yang saat ini masuk yang direkam oleh konsol. Daftar ini menunjukkan semua login Anda yang berhasil dalam 30 hari terakhir.
Alamat IP yang Masuk Daftar Putih	Ini adalah daftar semua alamat IP Anda yang masuk daftar putih. Jika Anda masuk dari IP yang tercantum di sini, Anda tidak akan mendapatkan pesan masuk. Anda dapat menambahkan alamat IP ke daftar ini dengan mengeklik tombol di samping entri dalam daftar "Informasi Login" di atas. Anda dapat menghapus alamat IP dari daftar ini dengan mengeklik tombol di samping entri dalam daftar ini atau dalam daftar "Informasi Masuk" di atas.
Gagal Masuk	Ini adalah daftar semua upaya login yang gagal dalam 30 hari terakhir. Jika Anda gagal memasukkan kata sandi yang benar setidaknya 3 kali dalam 20 menit, sebuah entri akan muncul dalam daftar ini. Anda juga akan diberi tahu tentang upaya login yang gagal melalui email.

Administrasi perusahaan (Root-Node) dalam Manajemen Seluler

Ketika Anda telah mencapai Root-Node (grup pertama), Anda dapat melakukan berbagai pengaturan untuk perusahaan Anda, dalam hal Manajemen Seluler.

Membuat Subkelompok	Membuat subkelompok
Ganti nama Root Node	Mengganti nama Root-Node (mis. nama perusahaan Anda)
Pendaftaran Massal	Mendaftarkan beberapa perangkat/pengguna secara bersamaan
Penugasan Massal	Menetapkan profil untuk masing-masing grup, dengan satu tampilan
Administrasi Aplikasi Cepat	Kirim (Batalkan) Permintaan pemasangan untuk aplikasi ke grup masing-masing perangkat
Impor Pengguna CSV	Impor Pengguna dari CSV ke dalam grup masing-masing

Membuat Subkelompok

Dengan "Buat Subgrup", Anda dapat membuat subgrup tambahan.

Anda dapat menetapkan di bawah grup mana subgrup harus ditetapkan.

(Secara default, grup baru dibuat yang ditetapkan sebagai subgrup di simpul akar)

Ganti nama Root Node

Di sini Anda dapat mengganti nama root Anda. Biasanya nama perusahaan digunakan dalam hal ini.

Pendaftaran Massal

Dengan "Pendaftaran Massal", Anda dapat mendaftarkan beberapa perangkat dan pengguna.

Anda dapat memilih secara langsung dengan cara apa pengguna akan menerima pendaftaran (eMail; eMail alternatif; SMS)

Tergantung pada perangkat mana yang akan diterima pengguna (iOS, Android, Windows Phone), Anda bisa langsung menandainya di sini.

Perbedaan apakah itu Smartphone atau Tablet, juga dapat dikonfigurasikan di sini, yang harus Anda pilih dengan benar, dengan tanda centang.

Sebagai langkah terakhir, Anda bisa menentukan apakah perangkat yang bersangkutan merupakan perangkat perusahaan atau pribadi (BYOD).

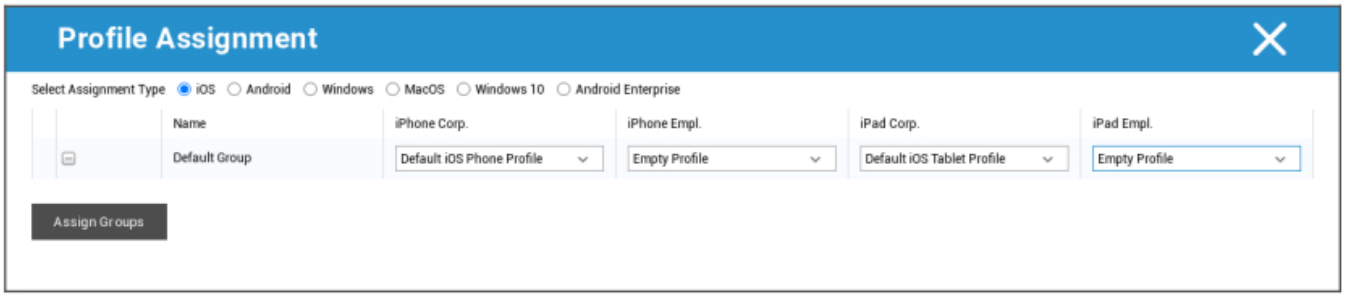
Dengan "Ekspor sebagai CSV", Anda dapat mengekspor Informasi sebagai file data CSV. Sebagai gantinya, Anda juga dapat mengimpor file data CSV dengan "Impor CSV", file akan terlihat seperti

contoh di bawah ini:

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

Penugasan Massal

Di bawah Penugasan Massal, Anda dapat menetapkan profil ke semua grup, yang dibagi menjadi iOS - Android - Windows - MacOS - Windows 10 - Android Enterprise

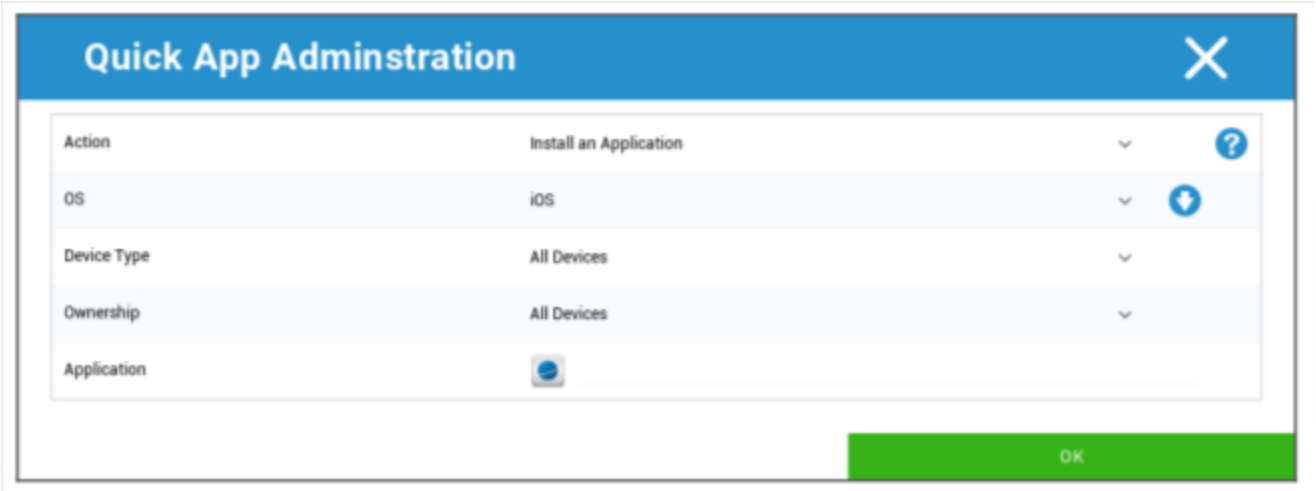


Windows - MacOS - Windows 10 - Android Enterprise

Administrasi Aplikasi Cepat

Di bawah Administrasi Aplikasi Cepat, Anda dapat mengirim permintaan Instalasi atau Penghapusan Instalasi untuk aplikasi tertentu ke OS pilihan Anda.

Anda juga dapat menentukan apakah permintaan akan dikirim ke semua jenis perangkat dari OS yang dipilih atau hanya ke jenis perangkat tertentu.



Impor Pengguna CSV

Impor Pengguna dari CSV ke dalam grup masing-masing.

Dengan "Unduh Template CSV", Anda dapat mengekspor file template CSV, yang dapat diisi (atau dapat digunakan sebagai referensi).

Anda juga dapat menggunakan opsi "Tampilkan Id Peran" dan "Tampilkan Id Grup" sebagai referensi untuk membuat file CSV Anda sendiri.

File CSV dapat diunggah ke MDM dengan "Unggah CSV".

Sebagai langkah terakhir, Anda dapat memulai Impor dengan mengklik "Mulai Impor".

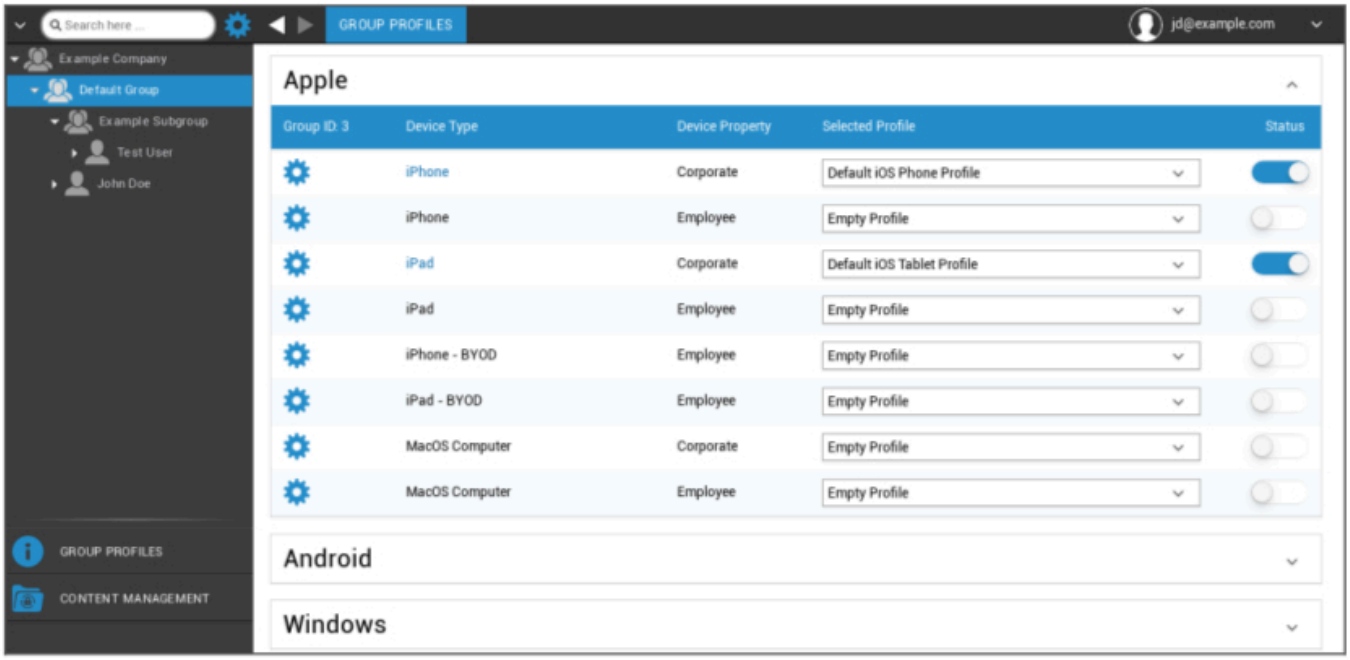
Manajemen Grup dalam Manajemen Seluler

Satu klik pada ikhtisar menampilkan profil konfigurasi yang berbeda untuk masing-masing platform.

Satu profil berisi semua opsi pengaturan yang dapat dibuat dengan AppTec360 terlebih dahulu pada perangkat pengguna akhir. Pada setiap platform, Anda dapat membuat profil untuk perangkat perusahaan (Korporat) atau perangkat Bawa-Perangkat-Anda-Sendiri (Karyawan).

Untuk membedakan konfigurasi grup perangkat, misalnya berdasarkan lokasi atau fungsi, disarankan untuk membuat beberapa subgrup.

Harap perhatikan Manajemen Profil di Manajemen Seluler



Dengan menu gear, Anda dapat menyiapkan beragam pengaturan untuk masing-masing (sub)grup.

Membuat Subkelompok	Membuat subkelompok untuk masing-masing (sub) grup
Mengedit Grup yang dipilih	Mengedit grup yang dipilih
Menghapus Grup yang dipilih	Menghapus grup yang dipilih
Pendaftaran massal	Mendaftarkan banyak perangkat/pengguna sekaligus untuk profil yang dipilih
Penugasan Massal	Menetapkan profil ke grup yang saat ini dipilih
Membuat Subkelompok	Membuat subkelompok untuk masing-masing (sub) grup

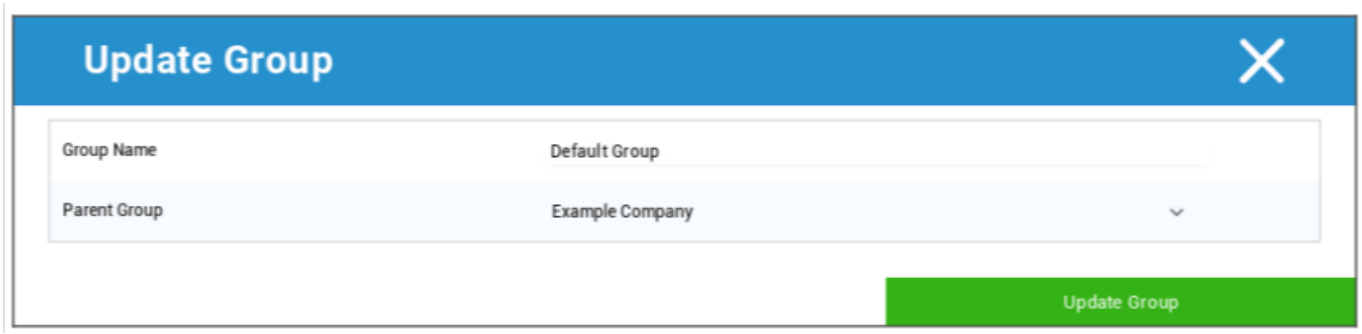
Membuat Pengguna	Membuat pengguna untuk masing-masing (sub) grup

Membuat Subkelompok

Dengan "Create a Subgroup", Anda dapat membuat subgrup tambahan.

Anda dapat menetapkan di bawah grup mana subgrup akan ditetapkan (sebagai default, subgrup ditetapkan ke grup yang saat ini dipilih).

Mengedit Grup yang dipilih



Di sini Anda dapat mengedit profil - di sini, pengaturan berikut ini dapat dilakukan:

- Nama grup dapat diubah
- Grup induk dapat diubah

Menghapus Grup yang dipilih

Di bawah "hapus Grup yang dipilih", semua pengguna dan perangkat terdaftar untuk Anda yang ada di grup yang bersangkutan. Di sini, Anda memiliki opsi untuk menghapusnya.

Untuk satu pengguna, Anda dapat melakukan perintah hapus berikut ini:

Menghapus Pengguna	Pengguna dihapus
Pindahkan Pengguna ke Grup:	Anda dapat memindahkan pengguna ke grup lain (kolom berikutnya, mis. "Admin")

Untuk satu perangkat, Anda dapat melakukan perintah hapus berikut ini:

Menghapus & Menghapus	Menghapus dan menghapus perangkat
Menghapus dari Sistem	Hapus perangkat hanya dari AppTec

Referensi Pendaftaran Massal

Referensi Penugasan Massal

Membuat Pengguna

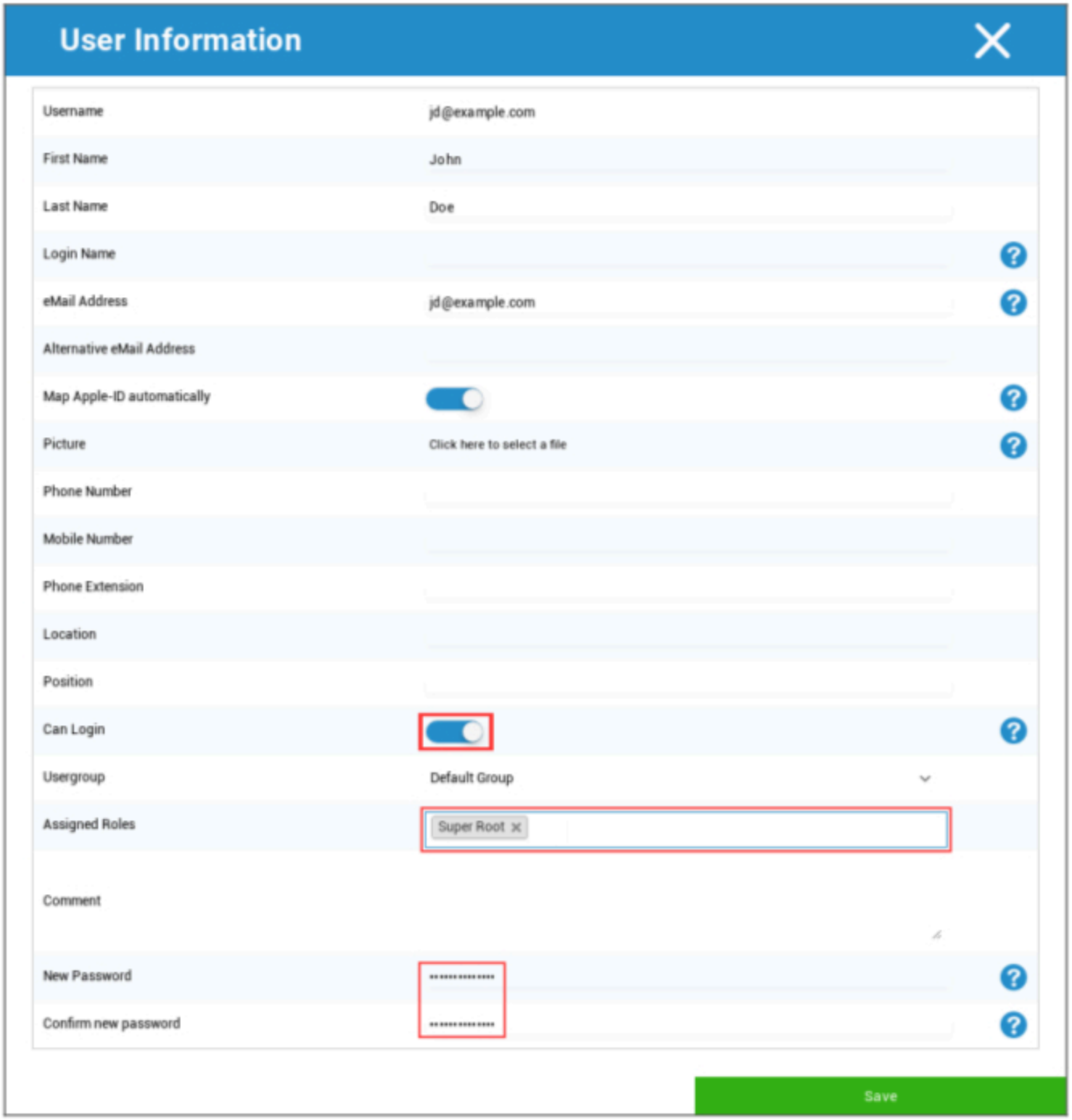
Dengan "Buat Pengguna", Anda dapat menambahkan pengguna baru.

Membuat Pengguna Admin baru

Anda dapat mengatur Pengguna sebagai Admin-Pengguna. Dengan demikian, ia akan mendapatkan izin untuk masuk ke konsol dan juga mengubah pengguna/grup/perangkat.

Buat Pengguna biasa atau gunakan Pengguna yang sudah ada. Pilih Pengguna yang ingin Anda beri izin admin, klik roda dan pilih "Edit Pengguna":

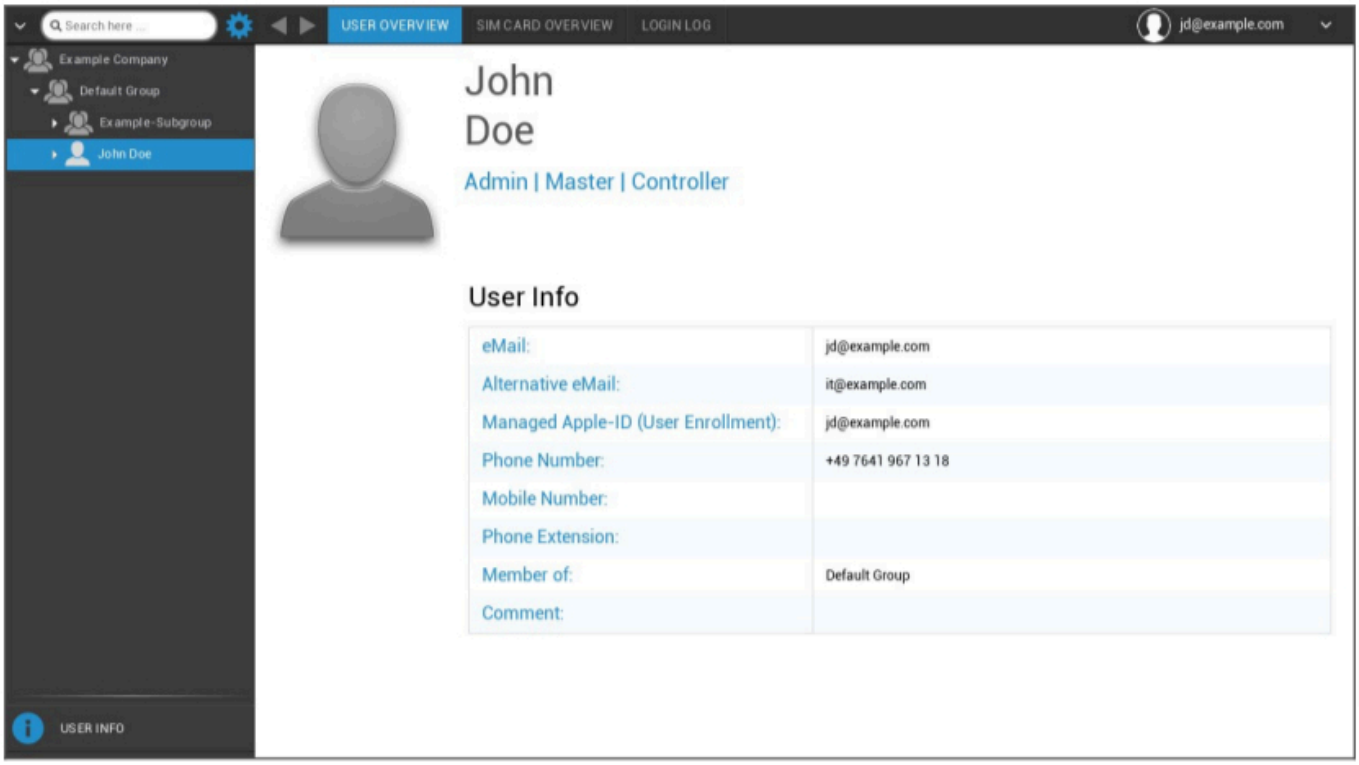
Aktifkan sakelar untuk "Dapat Masuk", tetapkan peran "Super-Root" ke pengguna dan tetapkan kata sandi.



Simpan ini dan pengguna sekarang dapat masuk dengan nama pengguna dan kata sandi.

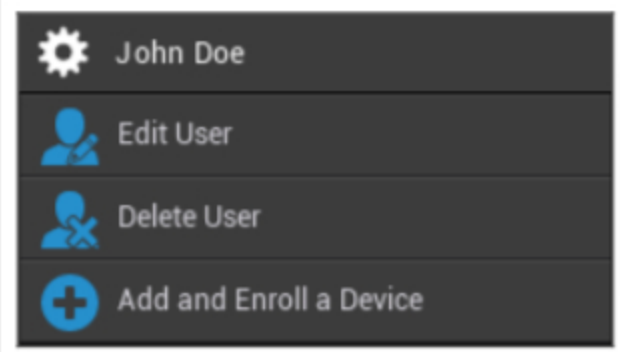
Manajemen Pengguna dalam Manajemen Seluler

Apabila Anda memilih pengguna tertentu, Anda akan melihat ikhtisar berikut ini:



Anda akan menerima ikhtisar semua informasi yang Anda masukkan sebelumnya di "Buat Pengguna".

Dengan perlengkapan yang dipasang di bagian atas, Anda dapat melakukan konfigurasi berikut ini:



Nama Pengguna	Nama Pengguna dari Pengguna yang dipilih
Edit Pengguna	Mengedit informasi pengguna
Menghapus pengguna	Menghapus pengguna • Hapus dari Sistem = Perangkat akan dihapus dari AppTec

	• Wipe & Delete = Perangkat akan dikembalikan ke pengaturan pabrik dan dihapus dari AppTec
Menambah dan mendaftarkan Perangkat	Mendaftarkan perangkat untuk pengguna yang dipilih

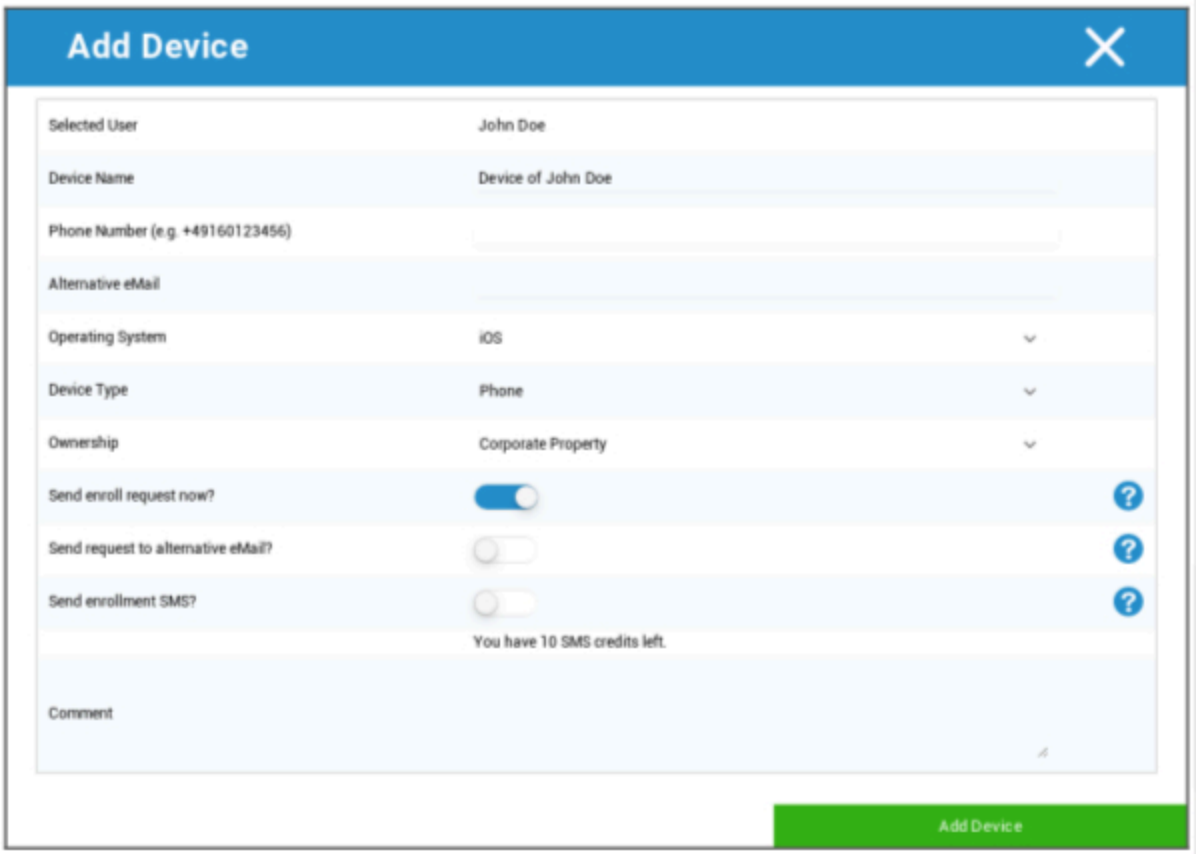
Harap diperhatikan, bahwa akses administrasi juga dapat diajukan sebagai akun pengguna lokal dalam struktur hirarki. Tanpa penetapan administrator tambahan, yang satu ini tidak boleh dihapus!

Menambah dan mendaftarkan Perangkat

Di sini Anda dapat memilih perangkat untuk penggunaan yang dipilih.

Atau, Anda dapat mendaftarkan perangkat ke dalam grup secara langsung. Untuk melakukannya, klik pada grup, klik pada roda dan pilih "Tambah dan daftarkan Perangkat".

Anda dapat melihat gambaran umum berikut ini:



Tergantung pada jenis perangkat yang ingin Anda daftarkan, Anda harus melakukan konfigurasi berikut:

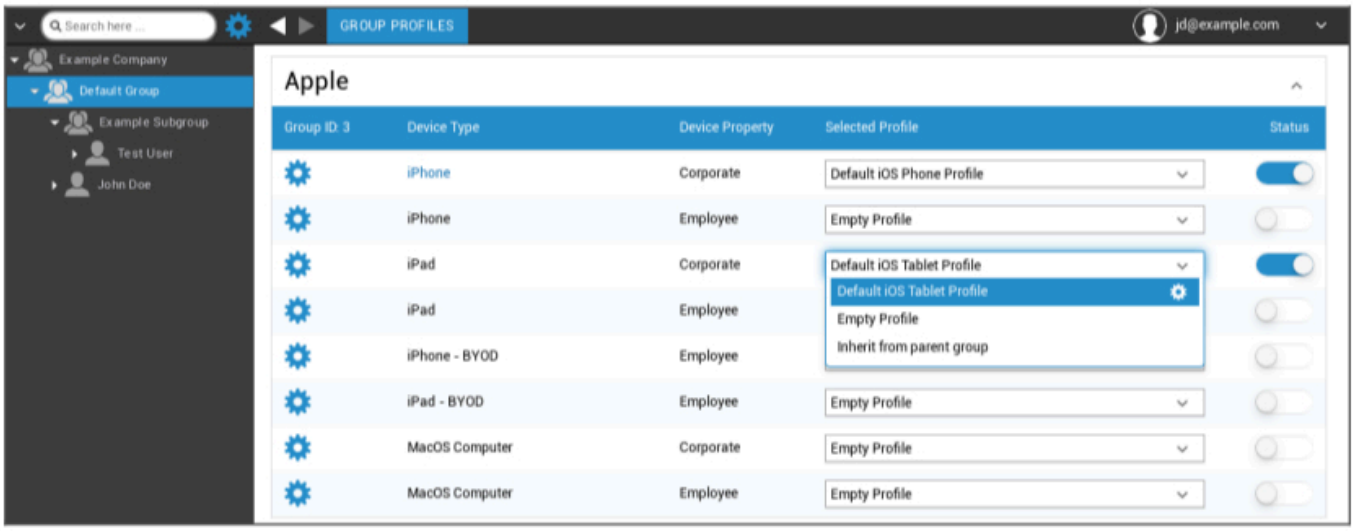
Pengguna yang Dipilih	Pengguna yang dipilih (akan terisi secara otomatis)
Nama Perangkat	Akan terisi secara otomatis (perangkat untuk "nama pengguna") - namun dapat diubah
Nomor Telepon	Nomor telepon, akan terisi secara otomatis (selama disediakan oleh pengguna) - di sini, nomor telepon dapat ditambahkan atau diubah
Email alternatif	Email alternatif, akan terisi secara otomatis (selama disediakan oleh pengguna) - di sini, bagaimanapun, dapat ditambahkan atau diubah
Pemilik Perangkat	Properti Perusahaan = perangkat perusahaan Properti Karyawan = Perangkat BYOD
Pilih Sistem Operasi	Di sini, Anda dapat memilih di antara sistem operasi berikut ini: • iOS • iOS BYOD (Pendaftaran Pengguna) • MacOS • Perusahaan Android • Android • Windows Mobile • Windows 10
Kirim permintaan pendaftaran?	Email segera dikirim ke alamat email utama dan pengguna diminta untuk menghubungkan perangkat mereka
Kirim permintaan ke email alternatif?	Kirim email tambahan atau secara eksklusif (jika "Kirim permintaan pendaftaran?" dinonaktifkan) ke alamat email alternatif (email berbeda dengan email Permintaan Pendaftaran "normal")
Kirim SMS pendaftaran?	Kirim permintaan pendaftaran melalui SMS ("Nomor Telepon" harus dimasukkan)

Setelah Permintaan Pendaftaran dikirimkan, perangkat akan langsung ditampilkan (ditandai dengan warna merah).

Segera setelah perangkat berhasil terhubung, perangkat akan ditandai dengan warna hijau setelahnya dan dengan demikian siap untuk menerima pembatasan, aplikasi, dll.

Manajemen Profil dalam Manajemen Seluler

Setelah mengeklik grup, Anda akan menerima ikhtisar semua platform perangkat yang akan dikonfigurasi dan masing-masing profil yang ditetapkan.



	Lakukan konfigurasi untuk profil yang dipilih
Jenis Perangkat	Jenis dan/atau model perangkat
Properti Perangkat	Pemilik perangkat (Perusahaan = milik perusahaan, Karyawan = perangkat pribadi karyawan)
Profil yang Dipilih	Profil yang dipilih (roda gigi membuka dialog konfigurasi profil)
Status	Hidup/Mati (profil diaktifkan/dinonaktifkan)

Apabila Anda memilih roda gigi, Anda akan menerima opsi berikut ini:

Membuat profil

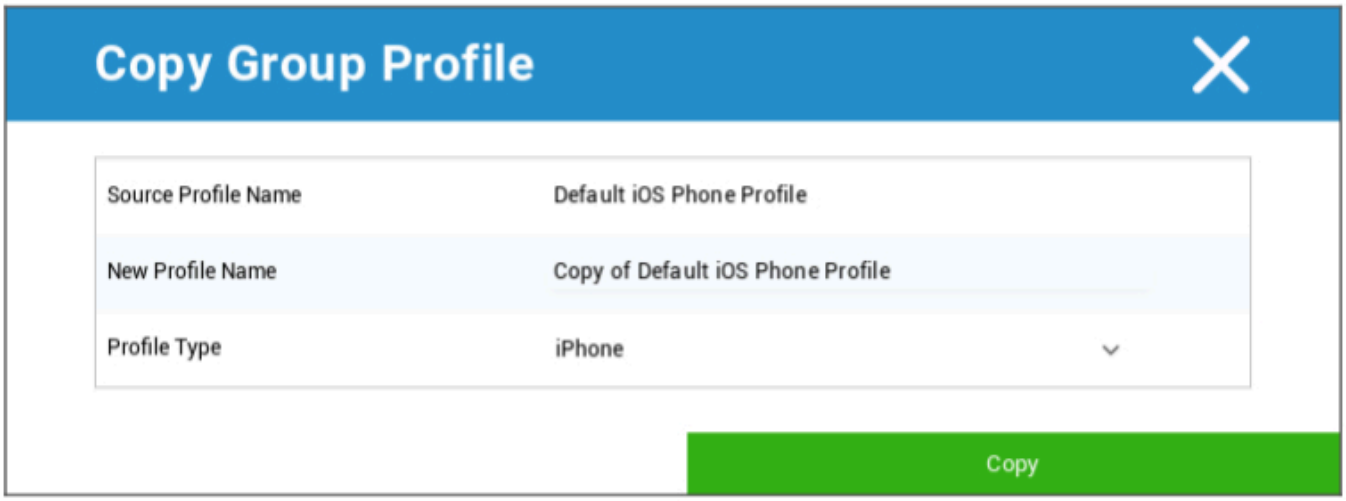
Anda dapat membuat dan mengonfigurasi profil baru untuk setiap entri dan/atau platform. Setelah mengklik sub poin ini, profil akan segera dibuat dan Anda dapat langsung memulai dengan konfigurasi iOS, Android dan Windows Phone.

Edit Profil

Setelah mengklik "Edit Profil", Anda akan mencapai tampilan konfigurasi untuk masing-masing profil, di mana Anda dapat mengatur konfigurasinya.

Salin Profil

Dengan bantuan fungsi "Copy Profile", Anda dapat menyalin pengaturan/konfigurasi dari profil yang sudah ada dan menambahkannya ke profil baru.

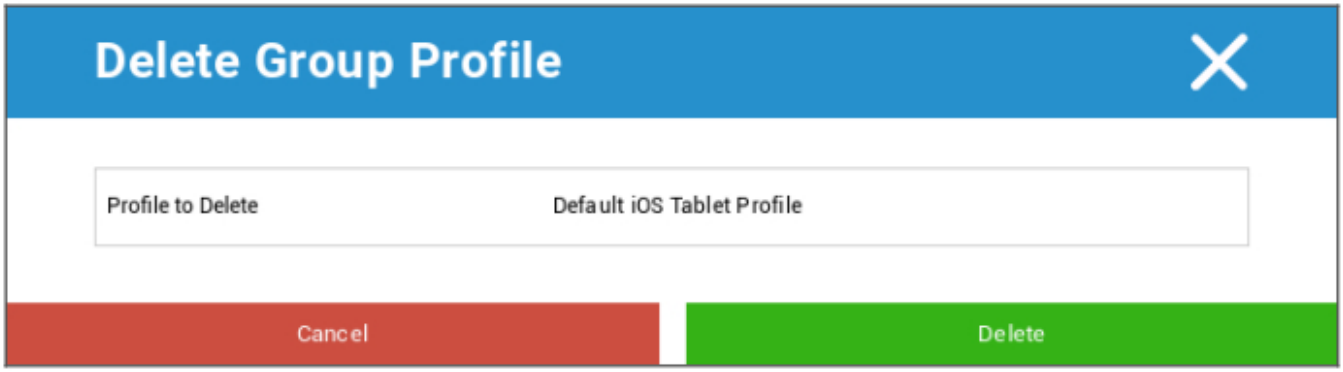


Nama Profil Sumber	Nama profil yang akan disalin
Nama Profil Baru	Nama profil baru
Jenis Profil	Jenis profil (Ponsel/Tablet)

Setelah Anda mengklik "Salin", profil akan dibuat dan sekarang dapat ditugaskan ke grup

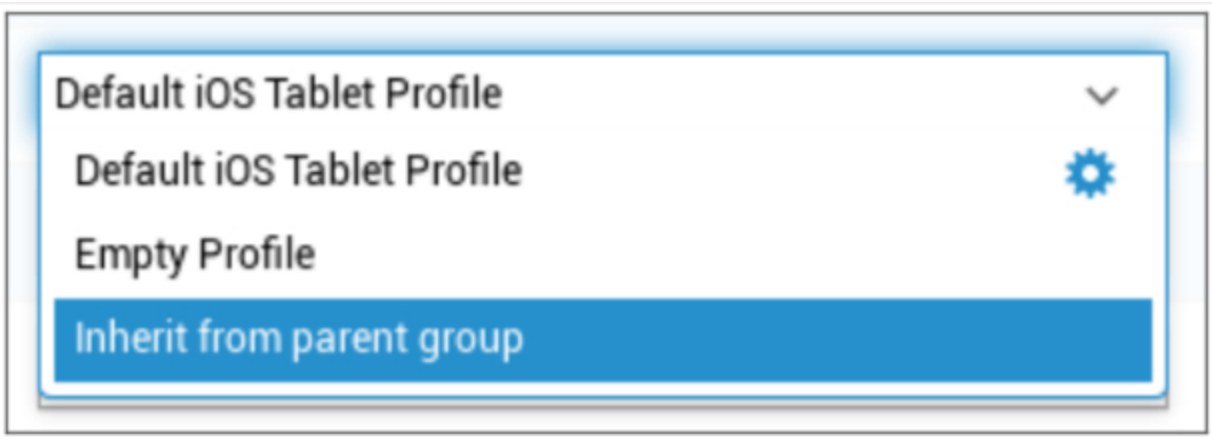
Menghapus Profil

Di sini Anda dapat menghapus profil secara permanen. Harap diperhatikan, bahwa selama proses penghapusan dan proses "Tetapkan Sekarang" berikut untuk profil, konfigurasi akan hilang pada masing-masing perangkat dari grup yang terpengaruh dan tidak dapat dipulihkan!


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

Mewarisi Profil

Selama pemilihan profil, opsi "Mewarisi dari grup induk" tersedia.



Apabila profil diaktifkan, maka profil grup induk akan digunakan untuk masing-masing perangkat yang dipilih (dan masing-masing jenis perangkat). Harap diperhatikan juga, bahwa perubahan pada profil ini mungkin dapat memengaruhi banyak grup.

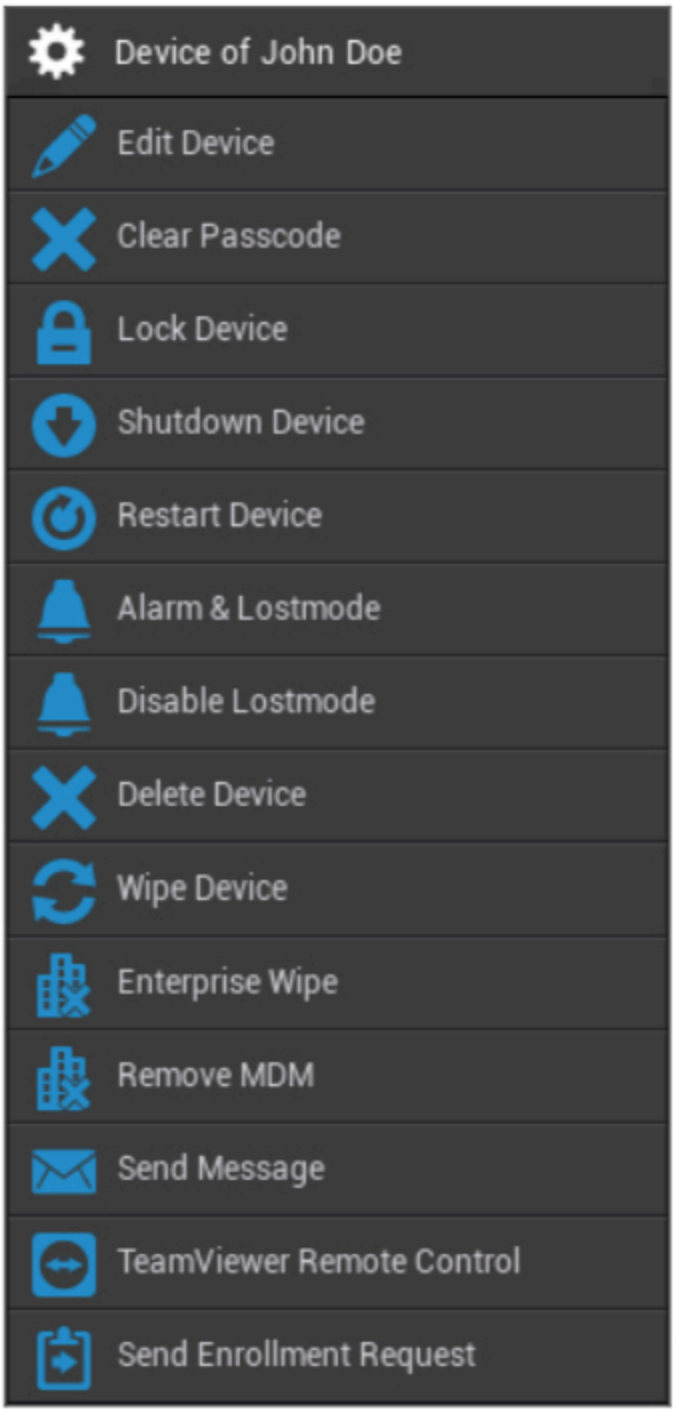
Konfigurasi ini ditetapkan sebagai nilai default, ketika subgrup baru dibuat.

Konfigurasi "Empty Profile" juga tersedia, yang sesuai dengan profil kosong, yang berarti bahwa pada akhirnya tidak ada konfigurasi baru yang akan dilakukan pada perangkat pengguna akhir.

Manajemen Perangkat dalam Manajemen Seluler

Apabila Anda memilih perangkat, Anda dapat melakukan berbagai tugas melalui "gear". Hal ini berbeda, tergantung pada platform OS (iOS, Android Enterprise, Android, Windows Mobile, Windows 10).

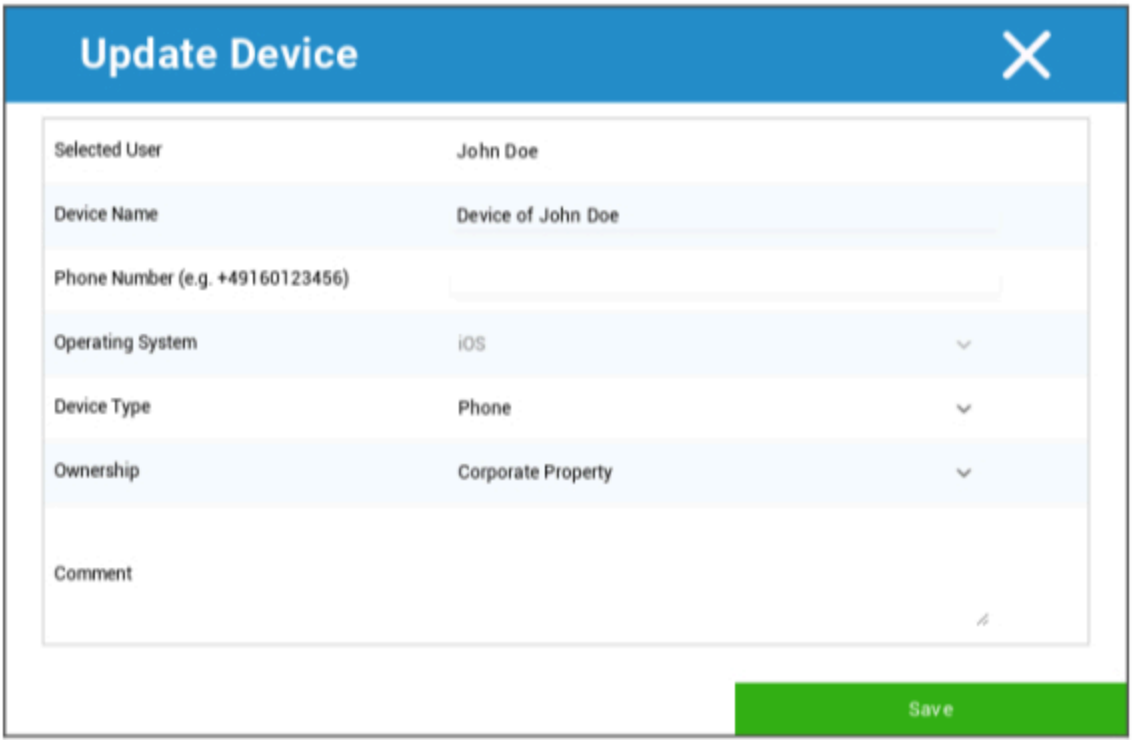
IOS



Edit Perangkat	Edit perangkat
Hapus Kode Sandi	Kode sandi perangkat terhapus
Perangkat Kunci	Mengunci perangkat (layar kunci)
Mematikan Perangkat	Mematikan perangkat

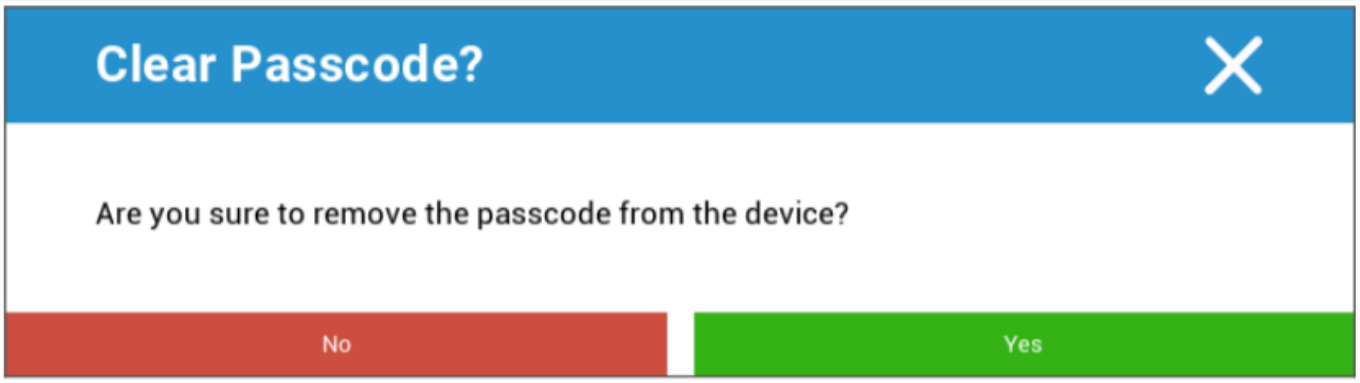
Mulai Ulang Perangkat	Mulai ulang perangkat
Alarm & Mode Hilang	Mulai Alarm & Mode Hilang
Nonaktifkan Mode Hilang	Nonaktifkan Mode Hilang
Menghapus Perangkat	Menghapus perangkat dari AppTec
Bersihkan Perangkat	Mengembalikan perangkat ke pengaturan pabrik
Penghapusan Perusahaan	Informasi, aplikasi, dan profil yang disediakan oleh AppTec360 akan dihapus (perangkat dipisahkan dari MDM)
Hapus MDM	
Kirim Pesan	Mengirim Pemberitahuan Push ke perangkat Pesan akan ditampilkan di Aplikasi AppTec360 (Tab Pesan)
Kontrol Jarak Jauh TeamViewer	Memulai Sesi Kontrol Jarak Jauh menggunakan TeamViewer
Kirim Permintaan Pendaftaran	Kirim (berulang) Permintaan pendaftaran

Edit Perangkat



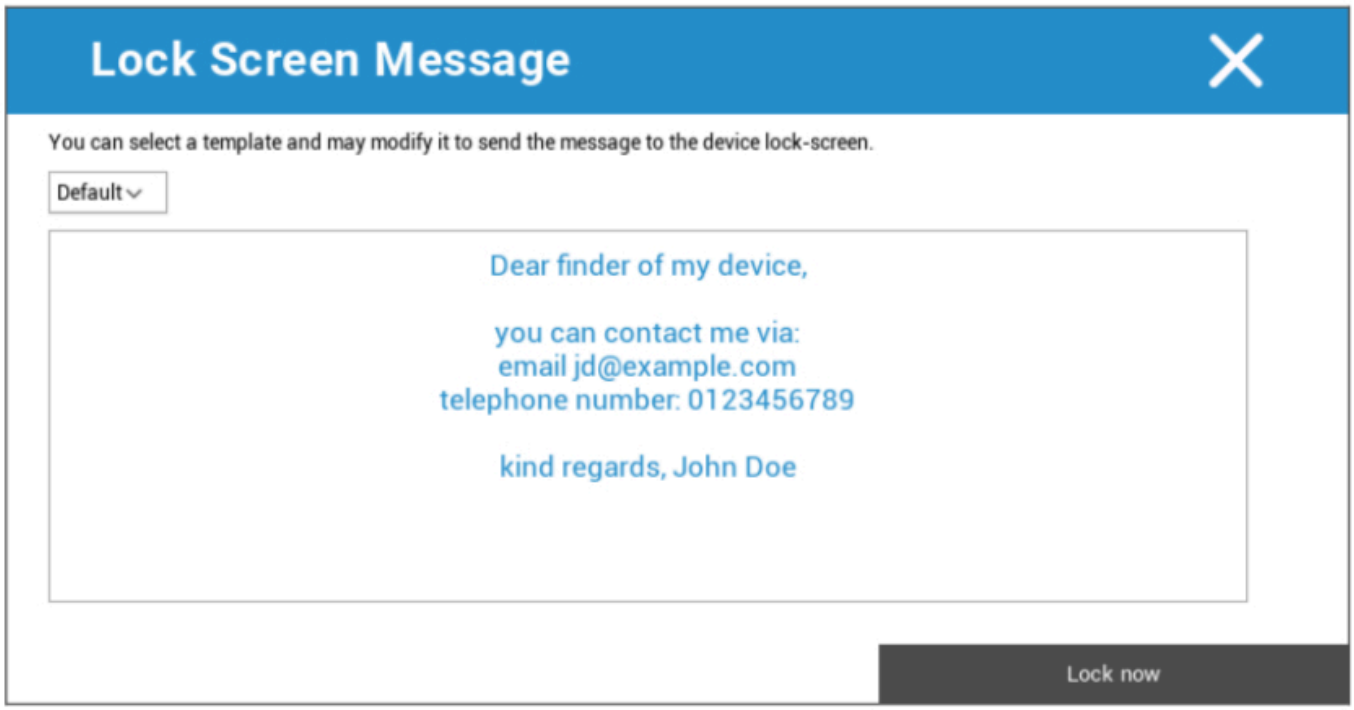
Di sini Anda dapat memperbarui berbagai informasi pada perangkat.

Hapus Kode Sandi



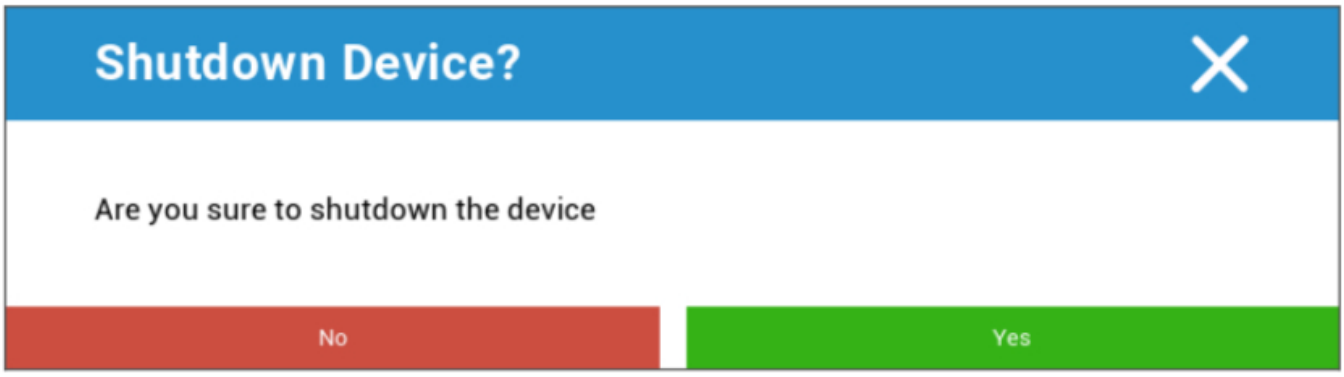
Di bawah "Hapus Kode Sandi", Anda dapat menghapus kode sandi dari perangkat dari jarak jauh. Selanjutnya, pengguna akan diminta untuk membuat kata sandi baru (tergantung pada panduan Kode Sandi).

Perangkat Kunci



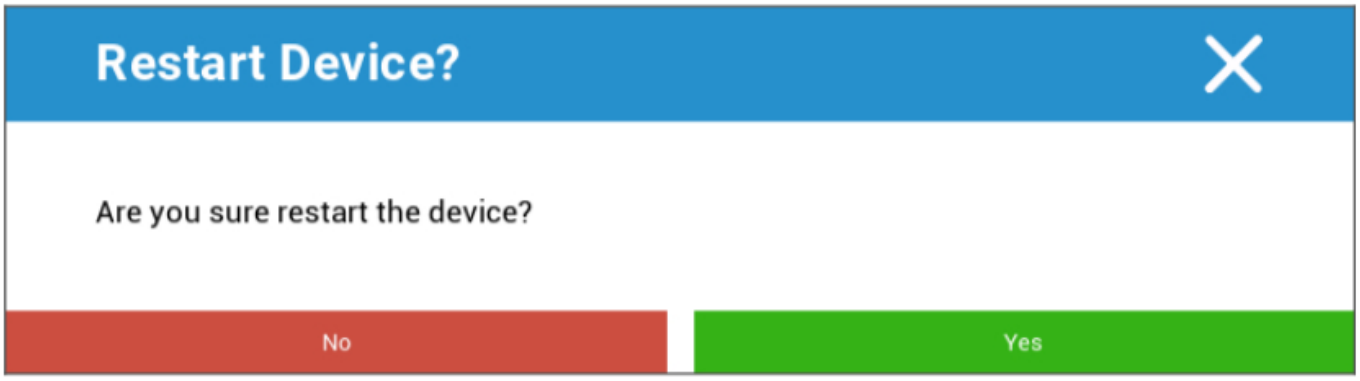
Di sini, perintah penguncian dikirim ke perangkat pengguna akhir (layar kunci).

Mematikan Perangkat



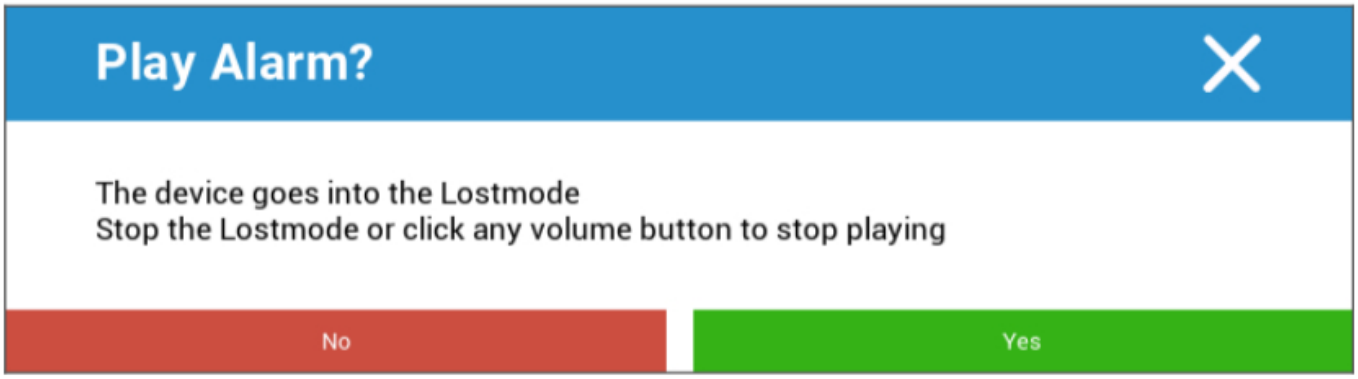
Di sini, perintah mematikan dikirim ke perangkat pengguna akhir.

Mulai Ulang Perangkat

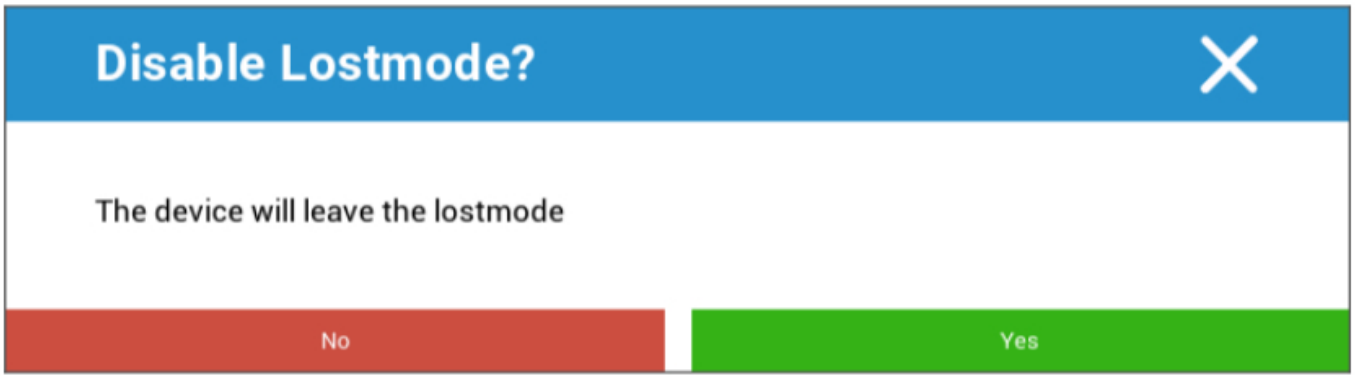


Di sini, perintah restart dikirim ke perangkat pengguna akhir.

Alarm & Mode Hilang | Nonaktifkan Mode Hilang



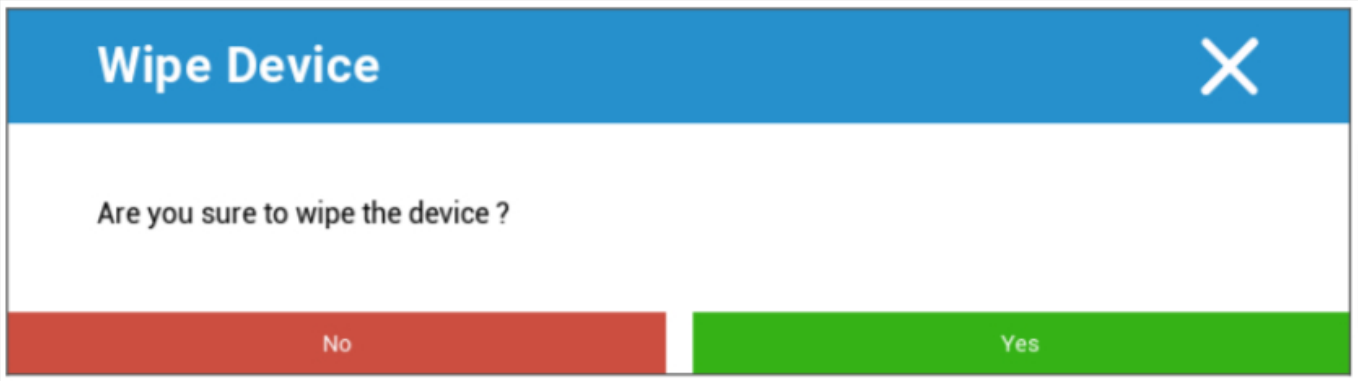
Di sini, perangkat dapat diatur ke dalam Lostmode, yang mengatur perangkat untuk terus-menerus memainkan suara Alarm. Lostmode dapat dihentikan dengan menekan tombol volume apa pun pada perangkat atau dari jarak jauh dengan mengeklik "Nonaktifkan Lostmode":



Menghapus Perangkat

Di sini perintah hapus dapat dilakukan. Anda dapat sekali lagi memutuskan, apakah perangkat hanya akan dihapus dari AppTec360 ("Hapus dari Sistem") atau, jika perangkat harus dihapus dari AppTec360 dan juga dikembalikan ke pengaturan pabrik ("Wipe & Delete).

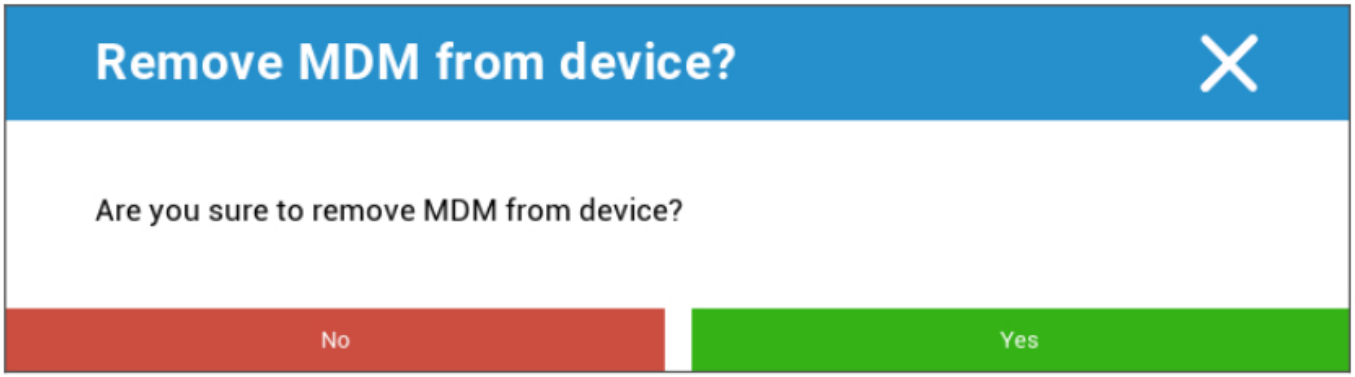
Bersihkan Perangkat



Di bawah "Wipe Device (Hapus Perangkat)", Anda dapat melakukan penghapusan perangkat secara menyeluruh. Perangkat akan dikembalikan ke pengaturan pabrik.

Penghapusan Perusahaan | Hapus MDM

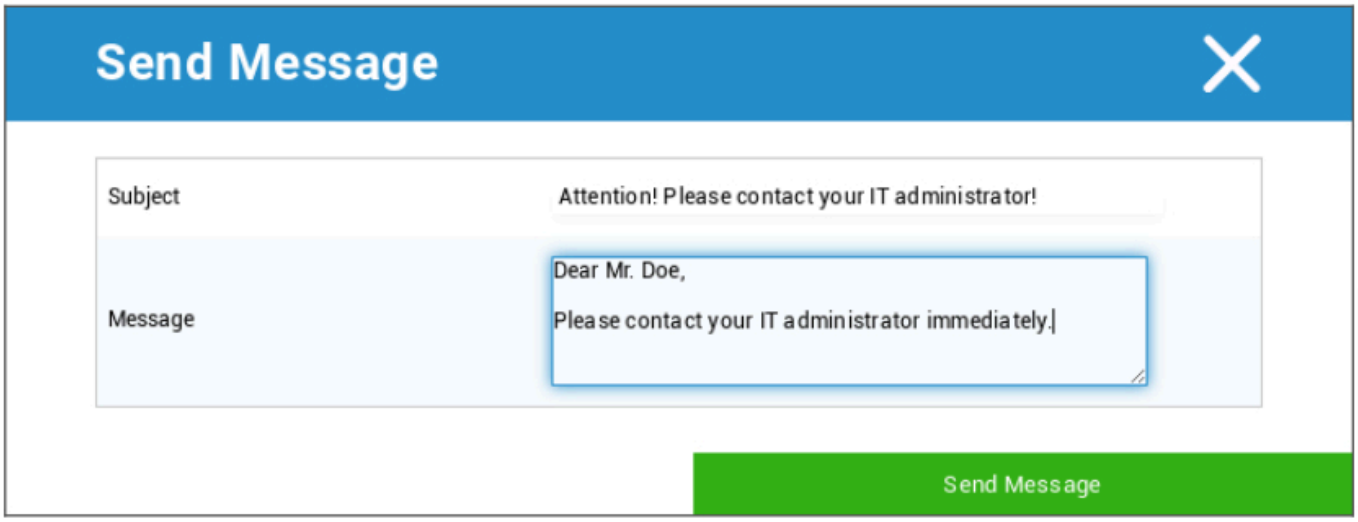
Hanya informasi, aplikasi, dan profil yang disediakan oleh AppTec360 yang dihapus. Dengan cara ini, data perusahaan tidak lagi tersedia di perangkat pengguna akhir. Area pribadi tidak terpengaruh dan tetap ada di perangkat pengguna akhir.



Dengan "Hapus MDM" Anda dapat menghapus profil MDM pada perangkat pengguna akhir dan semua item lain yang disediakan oleh AppTec.

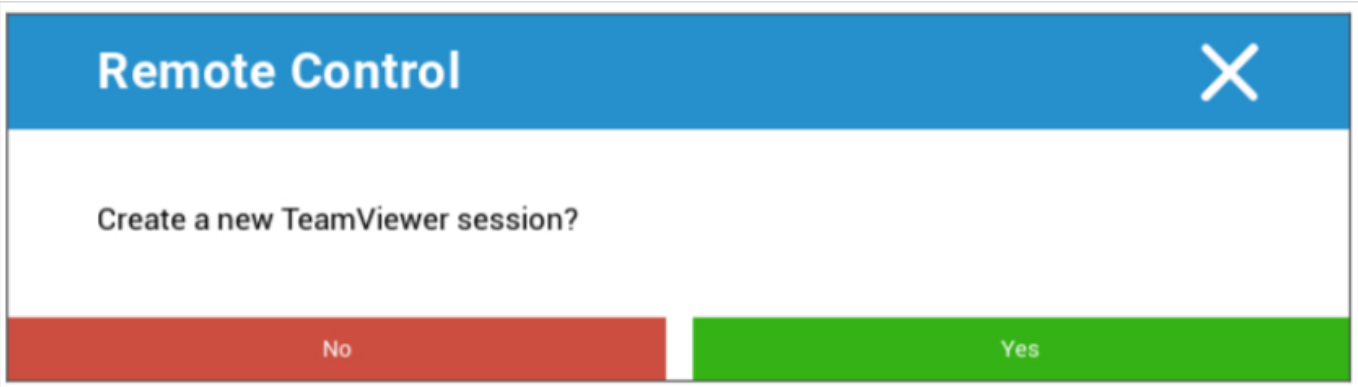
Perintah ini melakukan tindakan yang sama dengan "Enterprise Wipe".

Kirim Pesan



Di sini Anda dapat mengirim Pemberitahuan Push ke perangkat masing-masing.

Kontrol Jarak Jauh TeamViewer



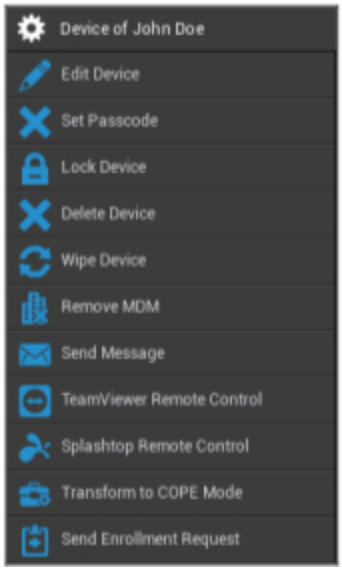
Di sini, sesi Remote Control Teamviewer dapat dimulai.

Kirim Permintaan Pendaftaran

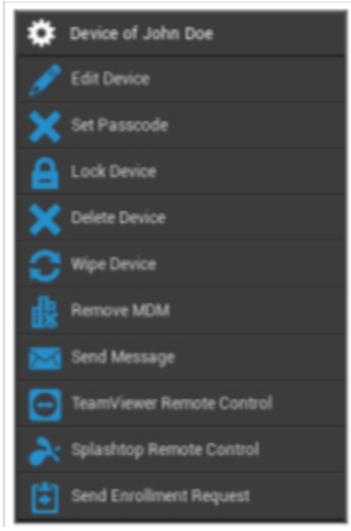
Dengan "Kirim Permintaan Pendaftaran", Anda dapat mengirimkan Permintaan Pendaftaran (lagi), kepada pengguna yang bersangkutan.

Android

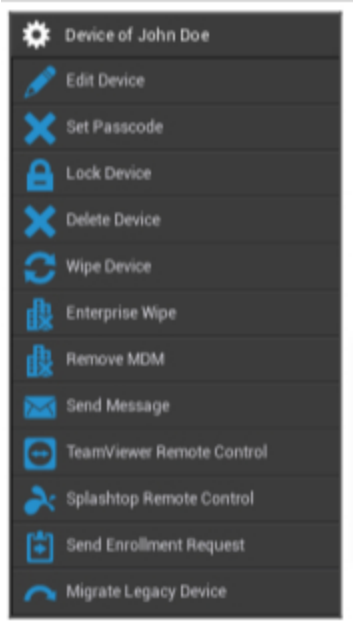
AE Perangkat yang Dikelola Sepenuhnya (Work Managed)



Profil Kerja AE (Kontainer)



Ponsel Android | Tablet

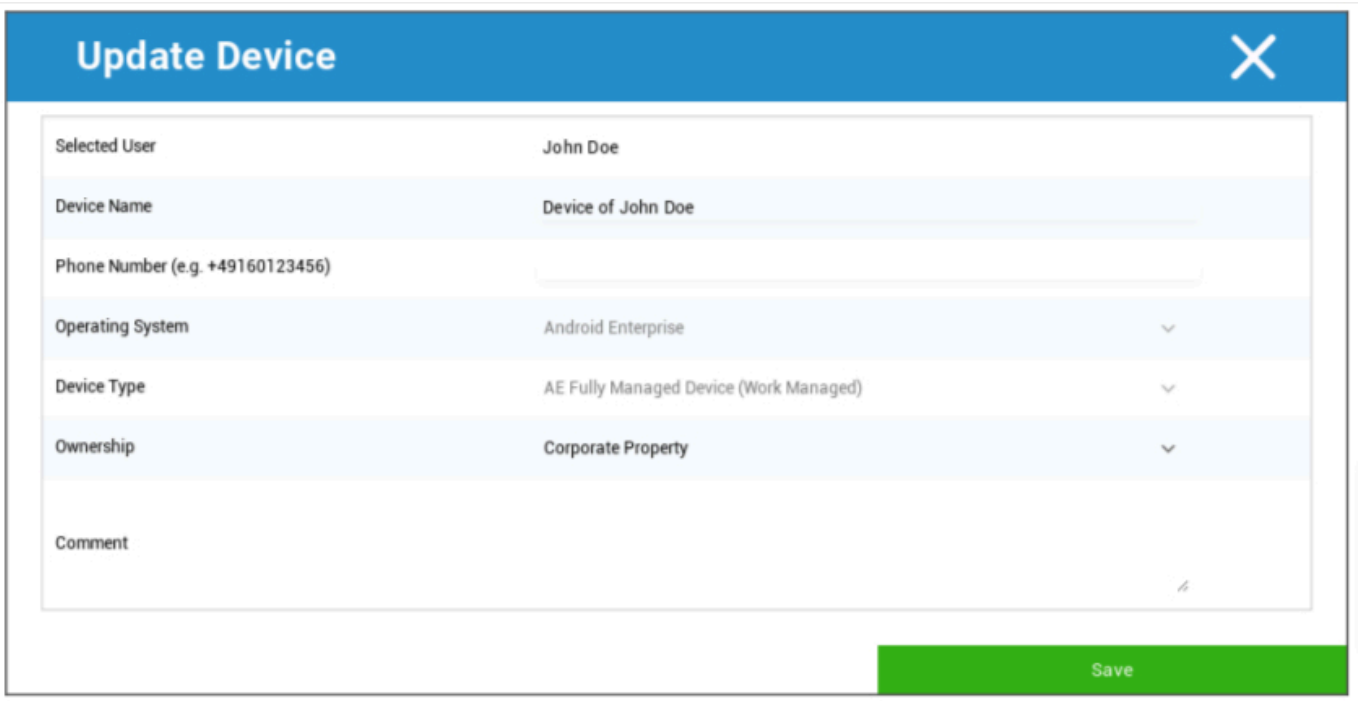


Edit Perangkat	Mengedit informasi perangkat
Atur Kode Sandi	Mengatur kode sandi perangkat
Perangkat Kunci	Mengunci perangkat (layar kunci)
Menghapus Perangkat	Menghapus perangkat dari AppTec
Bersihkan Perangkat	Mengembalikan perangkat ke pengaturan pabrik
Penghapusan Perusahaan	Informasi, Aplikasi, Profil yang disediakan oleh AppTec360 akan dihapus (perangkat akan dipisahkan dari MDM)
Hapus MDM	
Kirim Pesan	Mengirim notifikasi Push ke perangkat Pesan akan ditampilkan di Aplikasi AppTec360 (Tab Pesan)
Kontrol Jarak Jauh TeamViewer	Memulai sesi Remote Control untuk perangkat ini menggunakan TeamViewer
Kontrol Jarak Jauh Splashtop	Memulai sesi Remote Control untuk perangkat ini menggunakan Splashtop
Mengubah ke Mode COPE (hanya pada Perangkat yang Dikelola Sepenuhnya AE (Work Managed))	Membuat Profil Kerja pada Perangkat yang Dikelola Sepenuhnya (Work Managed) AE ini
Kirim Permintaan Pendaftaran	Kirim permintaan pendaftaran (berulang)
Migrasi Perangkat Lama (hanya pada Ponsel / Tablet Android saat terdaftar menggunakan	Migrasi Profil Ponsel / Tablet Android ke Profil Perangkat yang Dikelola Sepenuhnya (Dikelola

Penyediaan Mode Pemilik Perangkat)	Pekerjaan) AE

Edit Perangkat

Di sini Anda dapat memperbarui berbagai informasi perangkat.



Pengguna yang Dipilih	Pengguna perangkat
Nama Perangkat	Nama perangkat
Nomor Telepon	Nomor telepon perangkat
Sistem Operasi	Perusahaan Android Android
Jenis Perangkat	Android Enterprise: • AE Perangkat yang Dikelola Sepenuhnya (Work Managed) • Mode Profil Kerja AE (Khusus kontainer) • Perangkat yang Dikelola Sepenuhnya AE dengan Profil Kerja (COPE) Android: • Telepon • Tablet
Kepemilikan	Korporat = properti perusahaan

	Karyawan = milik karyawan
Komentar	Deskripsi tambahan untuk perangkat

Hapus Kode Sandi

Di sini Anda dapat menghapus kode sandi perangkat pada perangkat yang dipilih. Secara default pada Android, kode sandi akan diatur ke "123456" - ini dapat dan harus diubah oleh pengguna setelahnya.

Perangkat Kunci

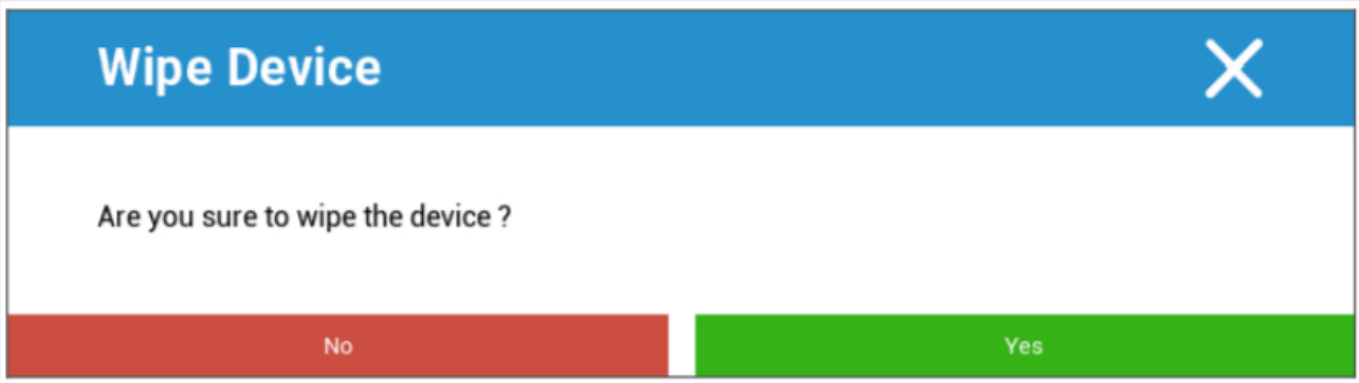
Di sini perintah mengunci perangkat akan dikirim ke perangkat (layar kunci).

Menghapus Perangkat

Di sini perintah hapus dapat dilakukan. Anda dapat sekali lagi memutuskan, apakah perangkat hanya akan dihapus dari AppTec360 ("Hapus dari Sistem") atau jika perangkat harus dihapus dari AppTec360 dan juga dikembalikan ke pengaturan pabrik ("Wipe & Delete).

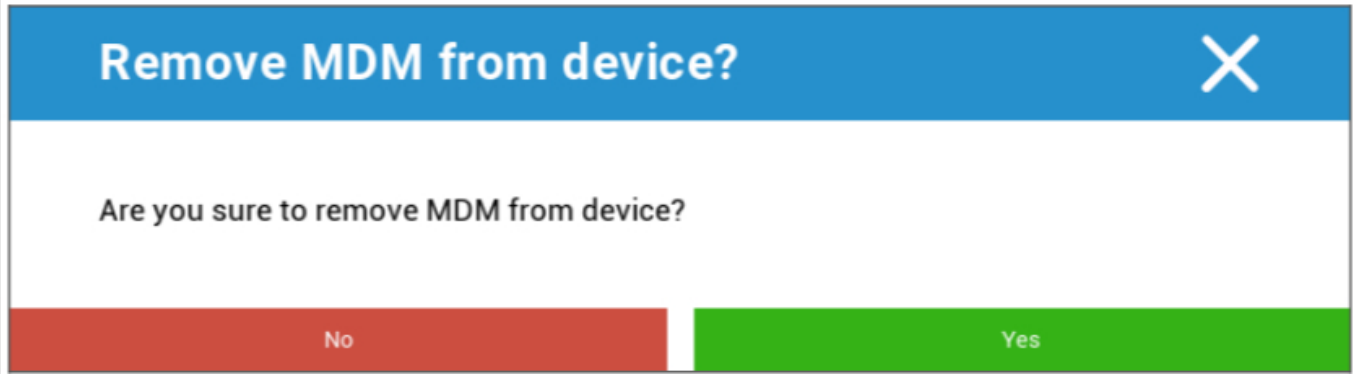
Bersihkan Perangkat

Di bawah "Wipe Device (Hapus Perangkat)", Anda dapat melakukan penghapusan perangkat secara menyeluruh. Perangkat kemudian akan dikembalikan ke pengaturan pabrik.



Selain itu, jika perangkat berisi kartu SD, Anda dapat menghapus kartu SD. Anda dapat melakukannya dengan mengatur "Wipe SD Card too? " ke "Aktif".

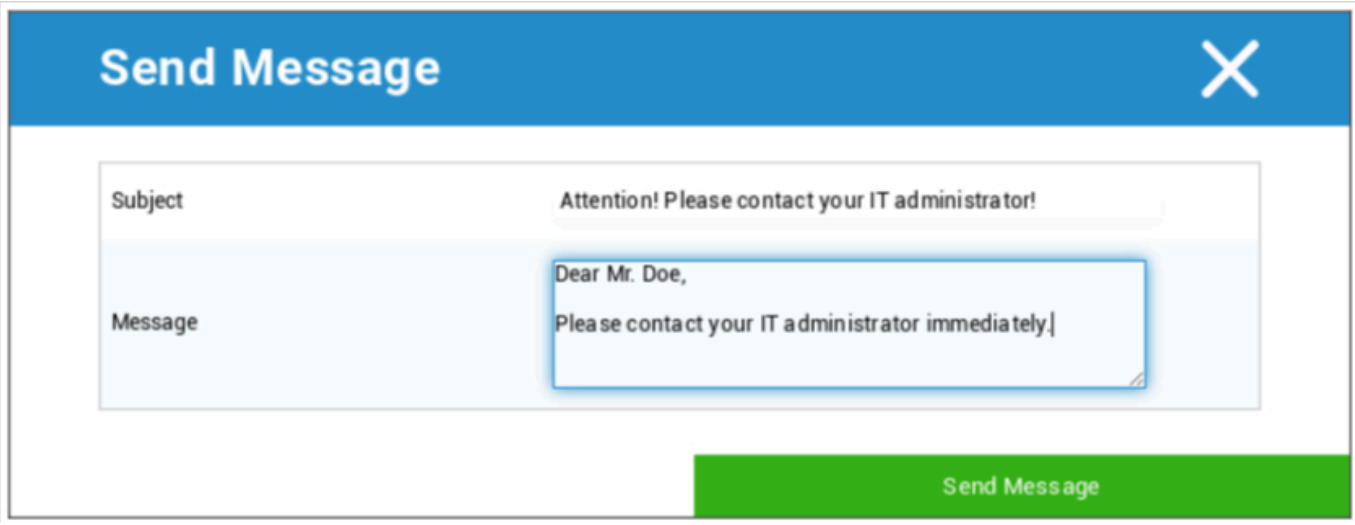
Hapus MDM



Ini adalah metode yang direkomendasikan, untuk membuat pemisahan dari MDM.

Hanya informasi, aplikasi, dan profil yang disediakan oleh AppTec360 yang dihapus, yang berarti bahwa semua data perusahaan tidak lagi tersedia di perangkat pengguna akhir. Namun, ruang pribadi tidak terpengaruh dan tetap ada di perangkat pengguna akhir.

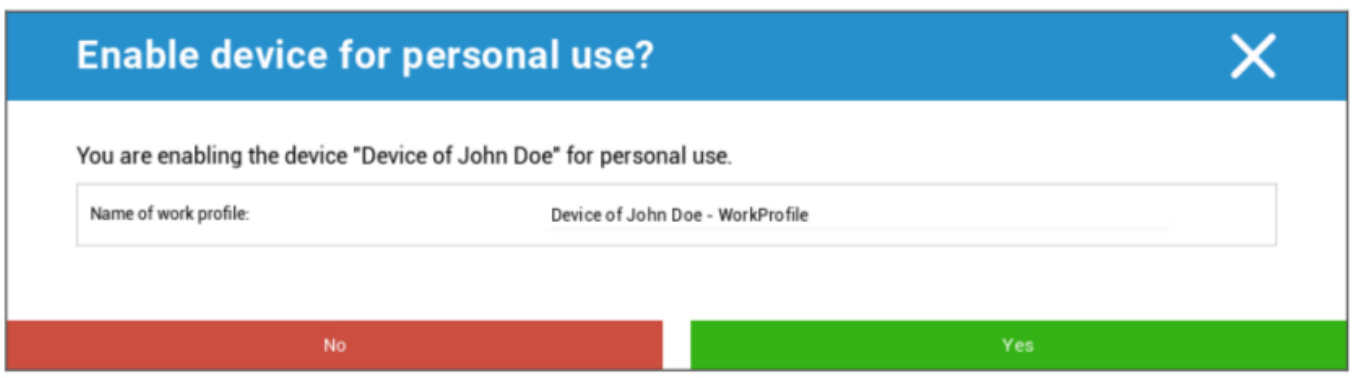
Kirim Pesan



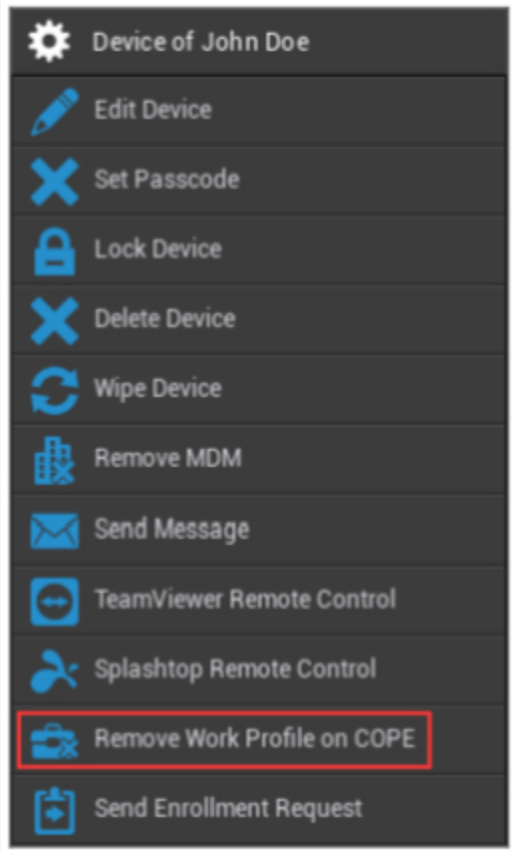
Di sini Anda dapat mengirim Notifikasi Push ke perangkat pengguna akhir yang bersangkutan.

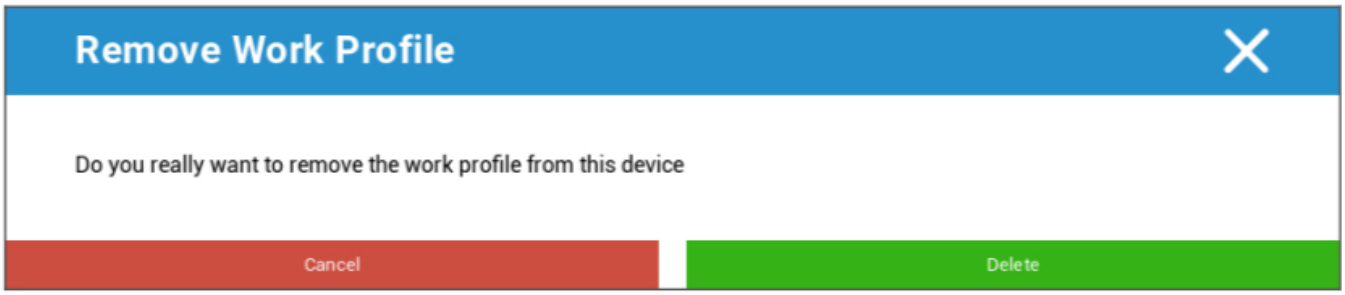
Mengubah ke Mode COPE

Membuat Profil Kerja pada Perangkat yang Dikelola Sepenuhnya (Work Managed) AE ini



Setelah mengubah perangkat ke Mode COPE, Anda dapat menghapus Profil Kerja dengan mengeklik opsi roda gigi **Hapus Profil Kerja pada COPE**:




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

Kirim Permintaan Pendaftaran

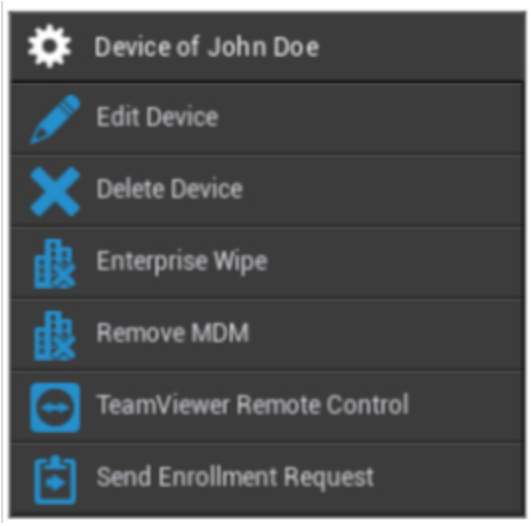
Dengan "Kirim Permintaan Pendaftaran", Anda dapat mengirimkan Permintaan Pendaftaran (lagi), kepada pengguna yang bersangkutan.

Harap diperhatikan, bahwa hanya Pendaftaran - Permintaan terbaru yang valid.

Memigrasi Perangkat Lama

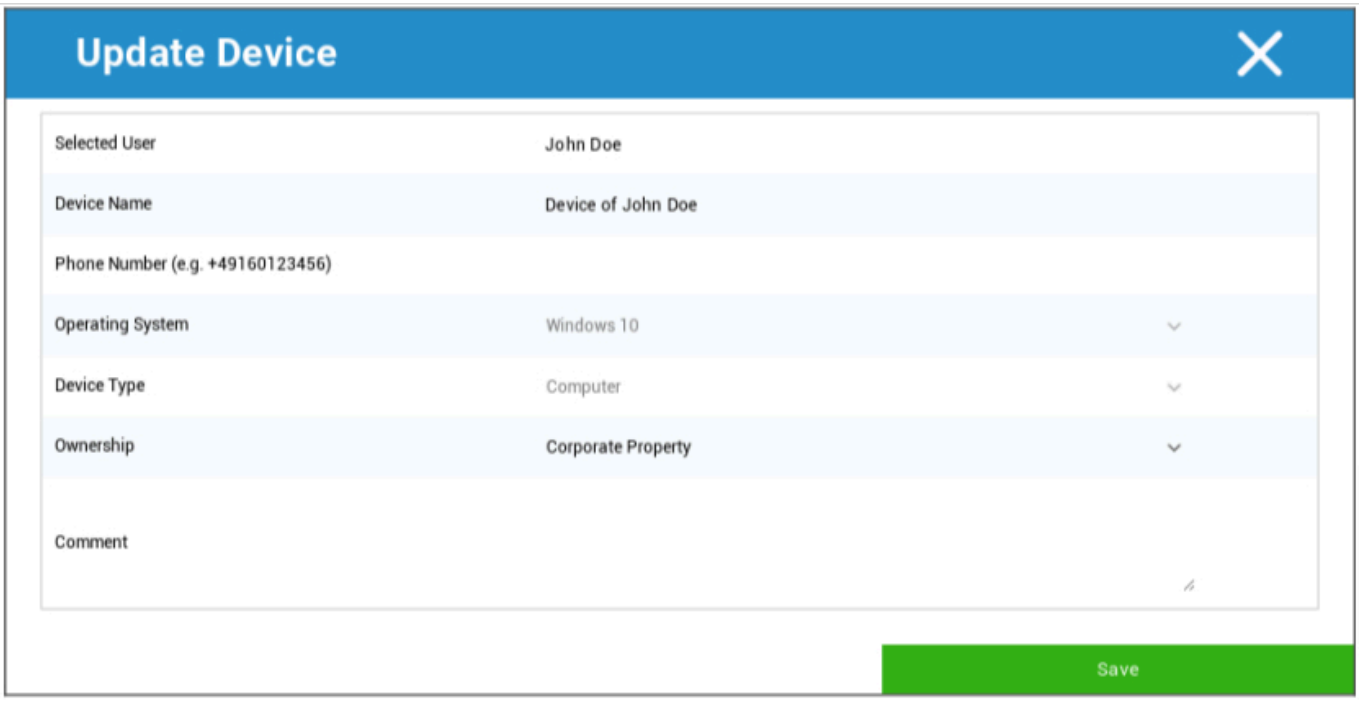
Migrasi Profil Ponsel / Tablet Android ke Profil Perangkat yang Dikelola Sepenuhnya (Dikelola Pekerjaan) AE

Windows



Nama Perangkat	Nama perangkat yang dipilih
Edit Perangkat	Edit perangkat
Menghapus Perangkat	Menghapus perangkat dari AppTec
Penghapusan Perusahaan	Informasi, aplikasi, dan profil yang disediakan oleh AppTec360 dihapus
Hapus MDM	
Kontrol Jarak Jauh TeamViewer	Mengendalikan perangkat dari jarak jauh dengan TeamViewer
Kirim Permintaan Pendaftaran	Kirim permintaan pendaftaran (lagi)

Edit Perangkat

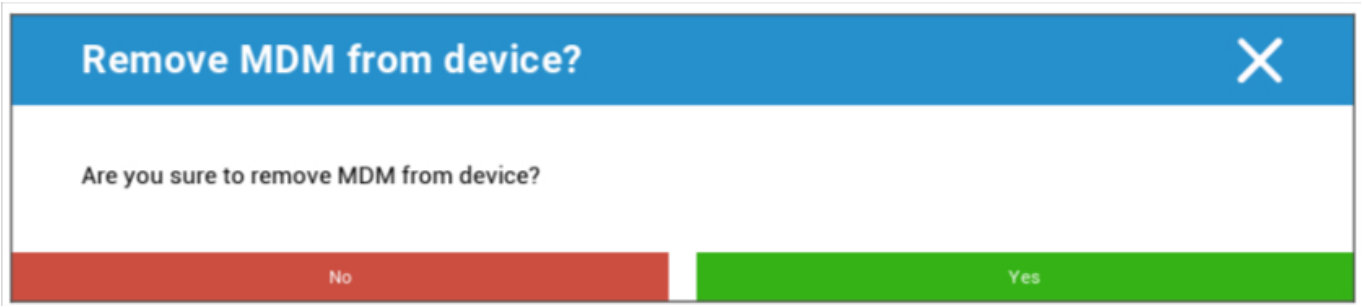


Di sini Anda dapat memperbarui berbagai informasi pada perangkat.

Menghapus Perangkat

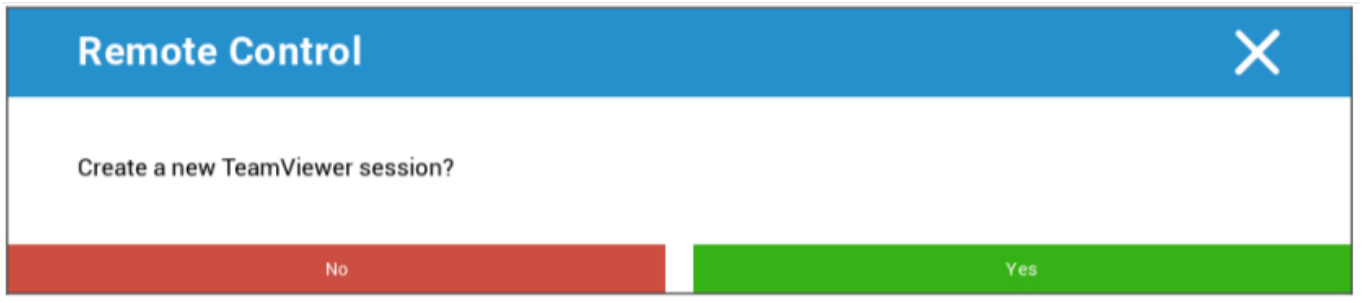
Di sini perintah hapus yang hanya menghapus perangkat dari AppTec360 dapat dilakukan.

Penghapusan Perusahaan | Hapus MDM



Hanya informasi, aplikasi, dan profil yang disediakan oleh AppTec360 yang dihapus. Dengan cara ini, data perusahaan tidak lagi tersedia di perangkat pengguna akhir. Area pribadi tidak terpengaruh dan tetap ada di perangkat pengguna akhir.

Kontrol Jarak Jauh TeamViewer



Di sini Anda dapat memulai sesi Remote Control TeamViewer untuk perangkat ini.

Kirim Permintaan Pendaftaran

Dengan "Kirim Permintaan Pendaftaran", Anda dapat mengirimkan Permintaan Pendaftaran (lagi), kepada pengguna yang bersangkutan.

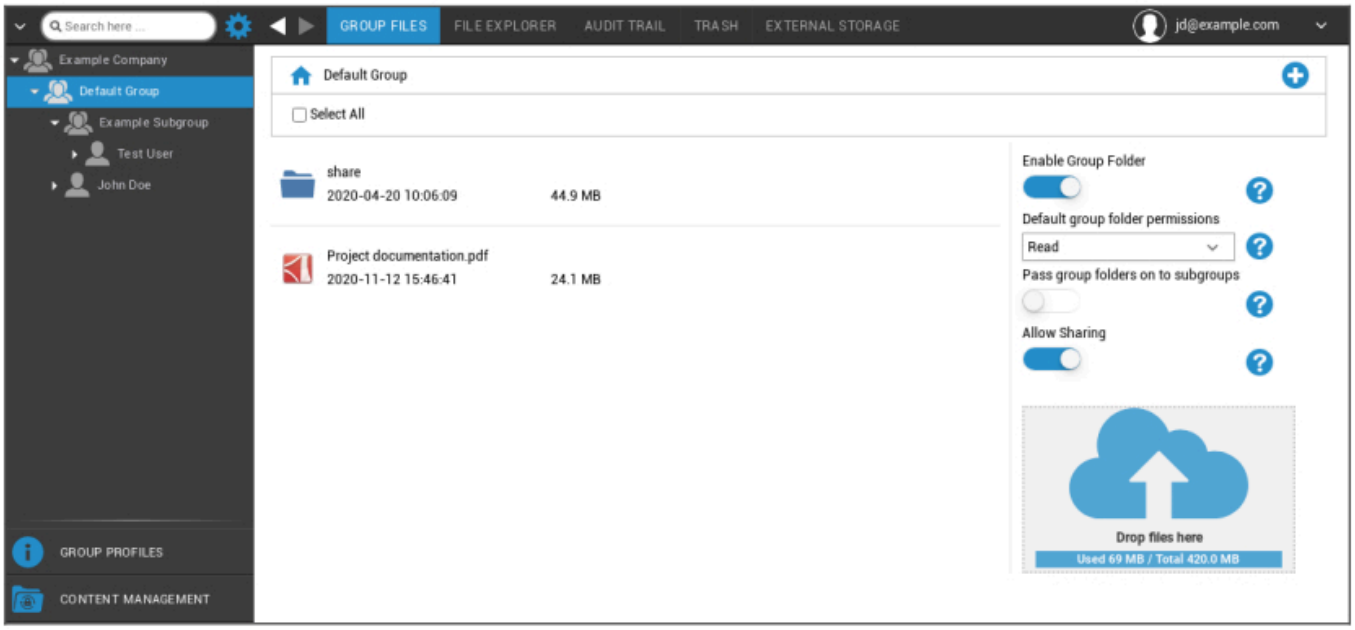
Manajemen Konten

Saat Anda berada dalam grup, Anda dapat mengelola ContentBox AppTec dengan "Manajemen Konten".

Dengan Content Box, Anda dapat mendistribusikan dokumen dan data perusahaan lainnya dengan aman ke perangkat pengguna akhir.

File Grup

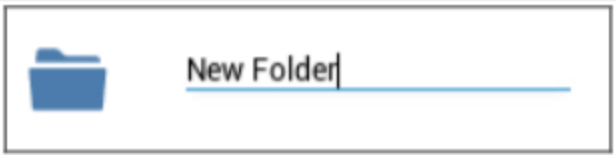
"File Grup" merupakan bagian fundamental ContentBox. Di sini Anda menetapkan pengaturan, mengunggah dokumen, membuat folder baru, dll.



Dengan simbol di sudut kanan atas, Anda dapat membuat folder baru yang ditujukan ke grup masing-masing dengan "Add Folder".

Dengan simbol di sudut kanan atas, Anda bisa membuat folder baru melalui "Add Folder", yang akan ditugaskan ke grup yang bersangkutan.

Anda dapat menamai folder dengan nama apa pun yang Anda inginkan.



Melalui "Upload File", Anda dapat mengunggah data. Di sini Standard-Explorer Anda akan dibuka. Tentu saja, Anda dapat melakukan kedua tindakan ini di setiap (sub) folder.

Dengan simbol di sudut kiri atas, Anda dapat kembali ke menu utama.

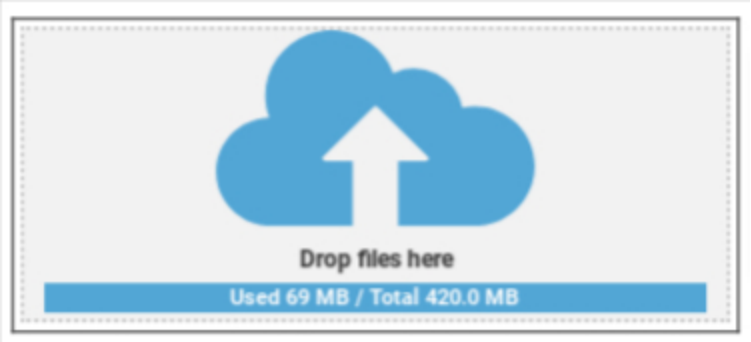
Anda dapat memilih beberapa folder dan file dan mengunduhnya dengan "Unduh" atau Anda dapat menghapusnya dengan mengeklik "Hapus".

Anda juga dapat memilih semua file dan folder dengan dan melakukan perintah "Unduh" dan "Hapus".

Apabila Anda menggerakkan mouse ke atas folder atau file, maka Anda akan melihat ikhtisar berikut ini:

- Dengan "Ubah Nama", Anda dapat mengganti nama folder/file
- Dengan "Unduh", Anda dapat mengunduh folder/file
- Dengan "Hapus", Anda dapat menghapus folder/file

Mengaktifkan Folder Grup	Jika diaktifkan, semua anggota grup memiliki akses ke folder masing-masing
Izin folder grup default	Izin pengguna dalam grup yang dipilih: Baca = izin hanya baca Pembaruan = izin pembaruan Buat = membuat izin Menghapus = menghapus izin
Meneruskan folder grup ke subgrup	Jika diaktifkan, masing-masing subkelompok dapat memiliki akses ke file data induk
Izin untuk subkelompok	Izin pengguna dalam subkelompok yang dipilih: Baca = izin hanya baca Pembaruan = izin pembaruan Buat = membuat izin Menghapus = menghapus izin
Izinkan Berbagi	Jika diaktifkan, pengguna dapat berbagi file melalui tautan



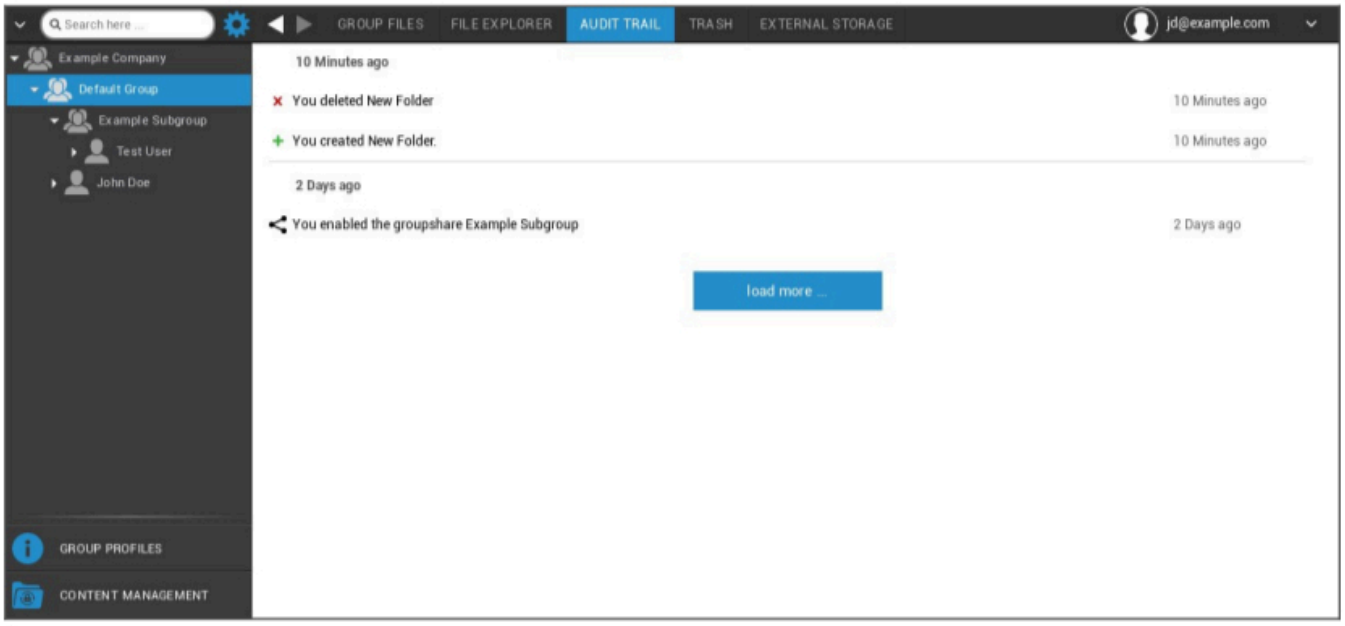
Untuk mengunggah file, Anda dapat menggunakan bidang ini, dengan menarik file melalui Drag & Drop ke jendela ini. Anda juga dapat mengklik bidang ini, untuk memilih dan mengunggah file dengan bantuan Internet Explorer.

Penjelajah File

Dengan "File Explorer", Anda dapat mengelola semua folder dan file - terlepas dari grup tempat file tersebut disimpan.

Anda juga akan menemukan pengaturan dan tombol yang sudah Anda pelajari di "Group Files".

Jejak Audit



Dalam "Audit Trail", Anda dapat melihat dari riwayat, pengguna mana yang membuat, menghapus, atau membagikan apa. Dengan cara ini, Anda bisa mengetahui kapan saja, apa yang telah dilakukan dengan data perusahaan.

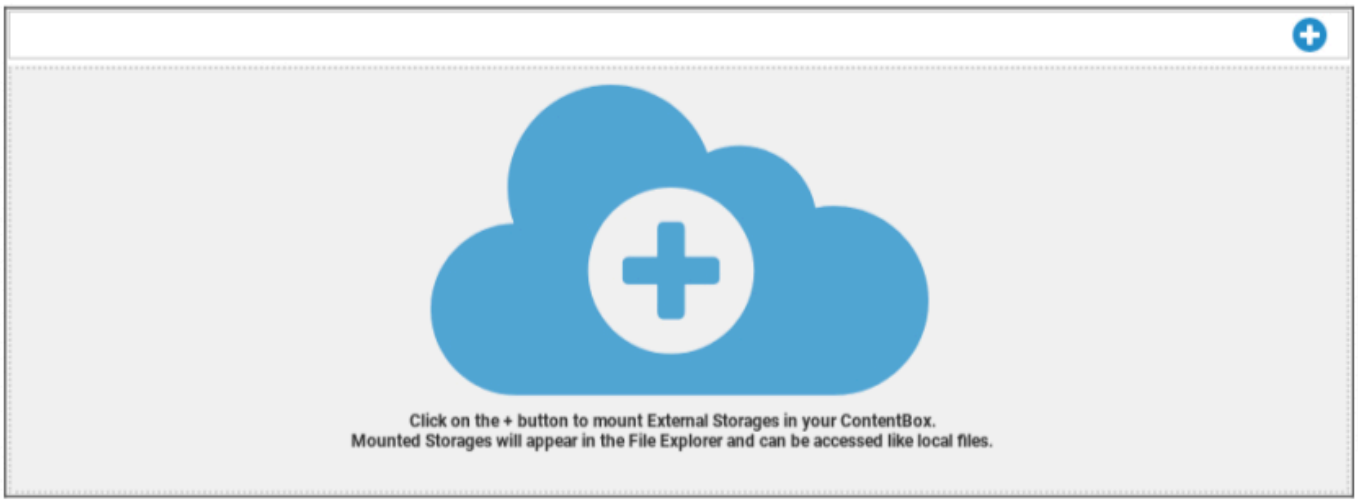
Sampah

Apabila Anda telah menghapus sesuatu (secara tidak sengaja), Anda dapat melihat folder dan file di bawah "Sampah" dan memulihkannya, sesuai dengan keinginan Anda.

- Dengan "Undelete", Anda dapat memulihkan data/folder.
- Dengan "Hapus", Anda dapat menghapus data/folder secara permanen - Anda harus mengonfirmasi perintah dele sekali lagi.

Harap diperhatikan, bahwa kapasitas penyimpanan yang digunakan di tempat sampah, mengurangi "Total Ruang" yang tersedia - ini adalah persyaratan ownCloud.

Penyimpanan Eksternal



Di bawah judul "Penyimpanan Eksternal", Anda dapat menghubungkan penyimpanan eksternal.

Dengan simbol tersebut, penyimpanan (tambahan) dapat ditambahkan.

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

Amazon S3	
Nama Tampilan	Nama tampilan
Kunci Akses	Kunci akses
Kunci Rahasia	Kunci keamanan
Ember	Identitas pasti dari subfolder yang telah ditetapkan untuk Anda
Nama host (opsional)	Nama host (opsional)
Port (opsional)	Port (opsional)
Wilayah	Wilayah (opsional)
Aktifkan SSL	Aktifkan SSL
Mengaktifkan Gaya Jalur	Hapus Alamat Jalur yang telah ditetapkan untuk Anda

FTP	
Nama Tampilan	Nama tampilan
Tuan rumah	Host-Alamat
Nama pengguna	Nama pengguna
Kata sandi	Kata sandi
Akar	Menu utama
Mengamankan ftps://	

SFTP	
Nama Tampilan	Nama tampilan
Tuan rumah	Host-Alamat
Nama pengguna	Nama pengguna
Kata sandi	Kata sandi
Akar	Menu utama

ownCloud	
Nama Tampilan	Nama tampilan
URL	URL ownCloud
Nama pengguna	Nama pengguna
Kata sandi	Kata sandi
Subfolder Jarak Jauh	Folder standar
Aman https://	

WebDAV	
Nama Tampilan	Nama tampilan
URL	URL WebDAV
Nama pengguna	Nama pengguna
Kata sandi	Kata sandi
Akar	Menu utama
Aman https://	
Berbagi Windows	Dukungan untuk Windows Share akan segera tersedia
SharePoint	Dukungan untuk Microsoft SharePoint akan segera tersedia

Log Audit

Di sini Anda dapat menemukan log yang mencatat informasi tentang tindakan yang dilakukan di konsol MDM.

Dengan ikon filter, Anda dapat menerapkan filter ke daftar yang ditampilkan.

Dengan menu tarik-turun **Item per halaman**: Anda dapat memilih jumlah item yang akan ditampilkan dalam satu halaman daftar.

Tindakan yang diambil / Pengaturan diubah	Tindakan yang diambil / Pengaturan yang diubah
Nilai	Nilai tindakan yang diambil / pengaturan yang diubah
Pengguna	Nama pengguna yang telah mengambil tindakan / telah mengubah pengaturan
Tanggal	Cap waktu kapan tindakan ini diambil / pengaturan ini diubah
Jalur / Jenis	Jalur ke tempat tindakan ini diambil / pengaturan ini diubah

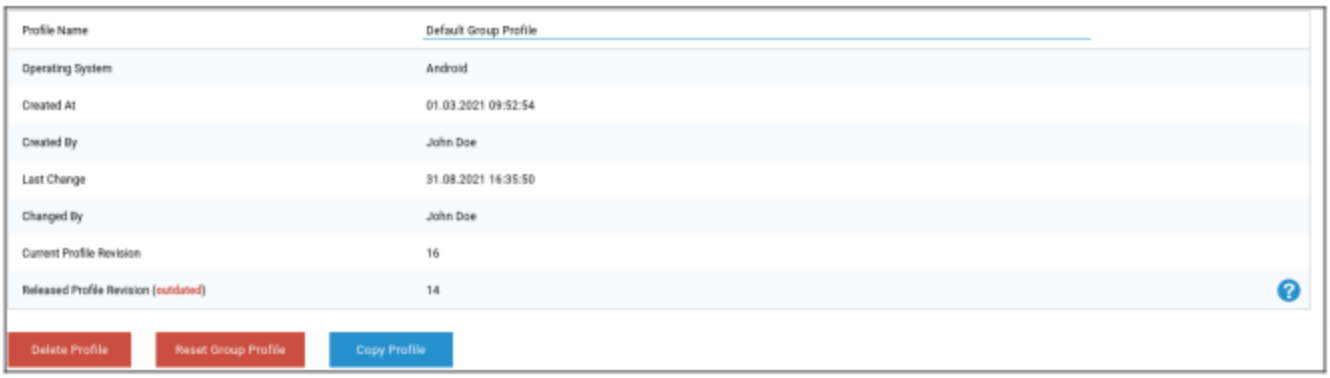
Konfigurasi iOS

Umum

Tergantung pada apakah Anda saat ini telah memilih grup atau perangkat, tampilan dan sub-poinnya akan berbeda - harap perhatikan dengan saksama hal ini!

Ikhtisar profil grup (hanya pada tingkat grup)

Saat membuka profil grup, Anda akan mendapatkan gambaran umum singkat tentang profil tersebut



Nama Profil	Nama profil (dapat diubah di sini)
Sistem Operasi	Sistem Operasi profil ini untuk
Dibuat di	Waktu pembuatan
Dibuat oleh	Pembuat profil
Perubahan Terakhir	Waktu perubahan terakhir pada profil
Diubah oleh	Akun yang melakukan perubahan terakhir
Revisi Profil Saat Ini	Revisi status profil yang disimpan
Revisi Profil yang Dirilis	Menetapkan revisi profil ("Tetapkan sekarang"). Jika label menunjukkan "(usang)" di belakang teks, itu berarti Anda telah menyimpan profil tetapi belum menetapkannya, sehingga perangkat masih akan mendapatkan versi yang lebih lama.

Informasi Umum

Jika Anda langsung menggunakan perangkat, Anda akan menerima ikhtisar singkat tentang perangkat yang Anda pilih.

Nama Perangkat	Nama perangkat
Nomor Telepon	Nomor telepon perangkat
Model	Nomor model
Sistem Operasi	OS
Nomor Seri	Nomor seri perangkat
Kepemilikan Perangkat	Perangkat perusahaan atau pribadi Korporat = perangkat perusahaan Karyawan = perangkat pribadi
Jenis Perangkat	Jenis perangkat (Tablet atau Ponsel)
Jailbroken	Jika ada Jailbreak pada perangkat
Diawasi	Menunjukkan apakah ini adalah perangkat yang diawasi
Sesuai	Jika ada pedoman yang dilanggar
Terakhir terlihat	Status kapan perangkat terakhir kali berkomunikasi dengan Server AppTec360

Pengaturan

Pengaturan ini berisi nama perangkat dan latar belakang yang sudah ditentukan sebelumnya.

Memberi nama perangkat ke nama sistem	Nama yang akan dikeluarkan di Konsol AppTec360 (di struktur hierarki sebelah kiri), akan sama dengan nama yang ada di perangkat pengguna akhir (dapat dilihat di pengaturan perangkat)
Gunakan wallpaper khusus (hanya untuk perangkat yang diawasi)	Di sini Anda dapat menentukan latar belakang yang akan ditampilkan pada perangkat pengguna akhir (mis. untuk jenis branding perusahaan untuk perangkat) Hanya tersedia dalam Mode Terawasi!
Pembaruan OS otomatis	Memaksa pembaruan OS jika tersedia. Hanya untuk perangkat DEP dalam mode yang diawasi.
Font Khusus	Di sini Anda dapat menambahkan font khusus.
Nama	Opsional. Nama yang dapat dilihat pengguna untuk font. Bidang ini diganti dengan nama font yang sebenarnya setelah instalasi.
Font	Unggah file font (.otf atau .ttf).

Revisi Konfigurasi

Di sini Anda akan menerima ikhtisar profil grup mana yang ditetapkan ke perangkat.

Jika Anda mengklik profil grup, Anda akan mengakses profil secara langsung dan dapat melakukan pengaturan.

Dengan simbol ini, Anda dapat mengembalikan aplikasi yang ditetapkan ke pengaturan profil grup.

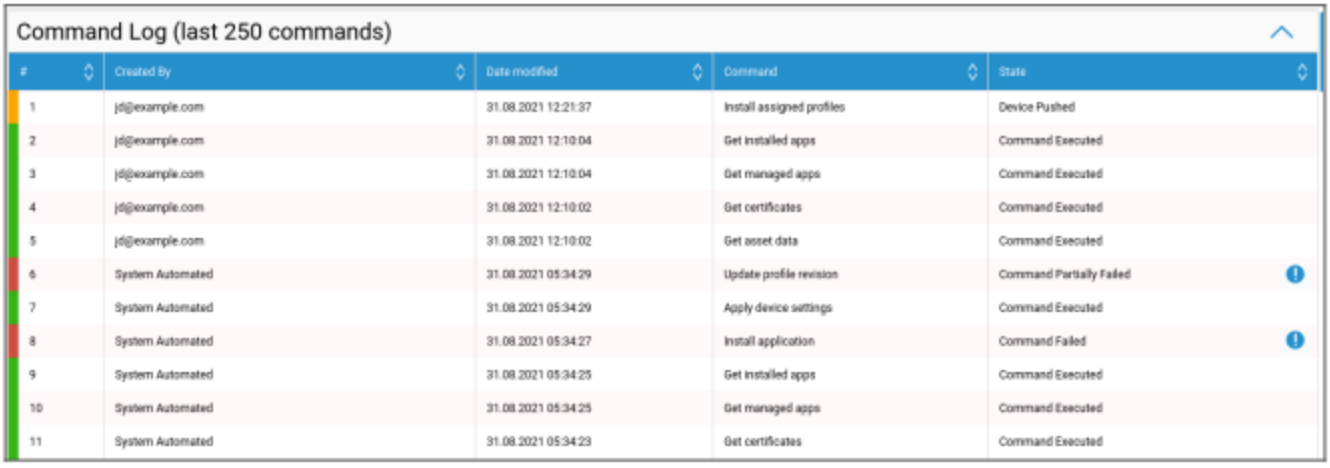
Dengan simbol tersebut, Anda dapat mengatur ulang profil perangkat agar tidak memiliki pengaturan sama sekali.

"Revisi terbaru tersedia" menunjukkan bahwa profil grup telah diubah dan disimpan namun belum ditetapkan. Profil grup harus ditetapkan dengan "Tetapkan sekarang" pada tingkat grup untuk menerapkan perubahan ke perangkat.

Log Perangkat (hanya pada tingkat perangkat)

Log Perintah

Di sini Anda dapat melihat perintah mana yang dikeluarkan untuk perangkat dan bagaimana statusnya.



Perintah yang dibuat oleh "System Automated" secara otomatis dibuat oleh sistem.

Kemungkinan status perintah

Perangkat Didorong	Permintaan push telah dikirim ke layanan push (misalnya APNS) untuk memberi tahu perangkat agar terhubung kembali ke server EMM.
Perintah Dibuat	Perintah ini dibuat dalam sistem.
Perintah Terkirim	Perintah dikirim ke perangkat setelah perangkat terhubung ke server.
Perintah Dieksekusi	Perintah berhasil dijalankan.
Perintah Gagal	Perintah gagal. *
Perintah Gagal Sebagian	Tergantung pada OS perangkat, beberapa perintah mungkin akan dikelompokkan bersama. Dalam hal ini, beberapa bagian dari grup perintah ini gagal. *
Perintah Dieksekusi, akhirnya Gagal	Perintah itu dijalankan tetapi mungkin tidak.
Perintah Ditolak	Perintah tersebut ditolak oleh pengguna.
Dibuang	Perintah telah dibuang. Misalnya karena digantikan oleh perintah lain atau perangkat didaftarkan ulang dan perintah lama dihapus

Jika ada tanda seru di belakang pesan, Anda dapat memperoleh informasi lebih lanjut dengan mengarahkan kursor ke ikon tersebut.

Manajemen Aset (hanya pada tingkat perangkat)

Manajemen Aset (hanya pada tingkat perangkat)

Info Perangkat

Model	Nomor model perangkat
Sistem Operasi	OS
Versi OS	Versi OS
Nomor Seri	Nomor seri
UDID	UDID perangkat
Nama Perangkat	Nama perangkat
Diawasi	Menampilkan jika perangkat diawasi
Status Baterai	Status baterai

Wi-Fi

Alamat IP	Alamat IP Perangkat
MAC WiFi	Alamat MAC WiFi

Seluler

Status	Status (ada kartu SIM)
Nomor Telepon	Nomor telepon
Status Roaming	Status roaming saat ini
Roaming (Suara/Data)	Status roaming untuk suara/data
Alamat IP	Alamat IP
IMEI	Nomor IMEI
Operator/Pengangkut	Penyedia layanan seluler
Jaringan Operator SIM	Jaringan operator SIM
Versi Operator	Versi operator
Firmware Modem	Firmware modem
PKS/MNC saat ini	Lihat "SIM MCC/MNC"
SIM PKS / MNC	Kode Negara Seluler adalah identifikasi negara yang ditetapkan oleh ITU sesuai dengan Standar E.212, yang, bersama dengan Kode Jaringan Seluler (MNC), digunakan untuk mengidentifikasi jaringan seluler (=kode negara) Ketika Anda masuk ke jaringan seluler lain, "MCC/MNC saat ini" dan "MCC/MNC SIM" akan berbeda.

Bluetooth

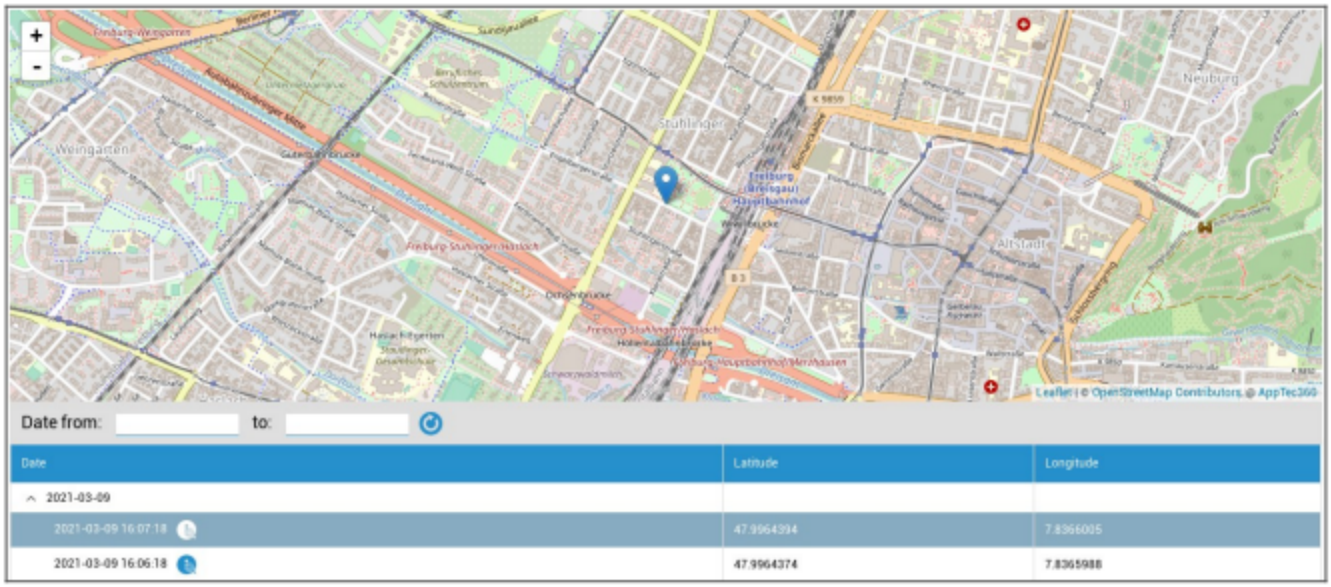
Bluetooth MAC	Alamat MAC Bluetooth

Manajemen Keamanan

Anti Pencurian (hanya pada tingkat perangkat)

Informasi GPS (hanya pada tingkat perangkat)

Di sini Anda dapat menilai lokasi perangkat saat ini/terakhir. Pelokalan dapat dilindungi dengan satu atau bahkan dua kata sandi - Lihat: Pengaturan Umum - Privasi - Akses GPS



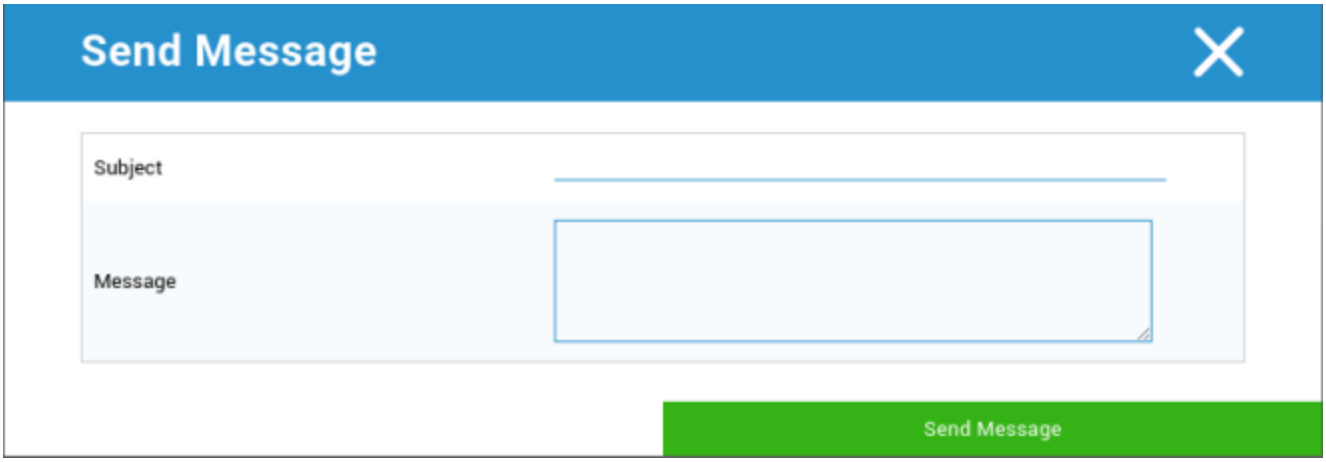
Hapus & Kunci (hanya pada tingkat perangkat)

Di bawah "Wipe & Lock", Anda dapat melakukan tiga tindakan berikut ini:

Penghapusan Penuh	Perangkat dipulihkan kembali ke pengaturan pabrik (data perusahaan dan data pribadi dihapus)
Penghapusan Perusahaan	Hanya data perusahaan yang dihapus dari perangkat pengguna akhir (semua aplikasi, data, dll. yang disediakan oleh AppTec)
Layar Kunci	Kunci layar diaktifkan, cukup untuk membuka kunci perangkat dengan kata sandi/PIN perangkat
Penguncian Forensik (hanya Perangkat yang Diawasi)	Jika fungsi ini diaktifkan dengan simbol  , perangkat akan terkunci, dengan menampilkan pesan yang tidak dapat ditutup. Karyawan juga tidak dapat membuka kunci perangkat. Hanya administrator yang dapat membuka kunci perangkat di konsol dengan simbol buka kunci  .
Izinkan Penguncian Aktivasi (Hanya Perangkat yang Diawasi)	Jika fungsi ini diaktifkan, perangkat akan terkunci, segera setelah "Temukan iPhone saya" diaktifkan di pengaturan iCloud

Pesan (hanya pada tingkat perangkat)

Dengan jendela berikut ini, Anda dapat mengisi subjek dan pesan, lalu mengirimkannya ke perangkat pengguna akhir:



Konfigurasi Keamanan

Kode Sandi

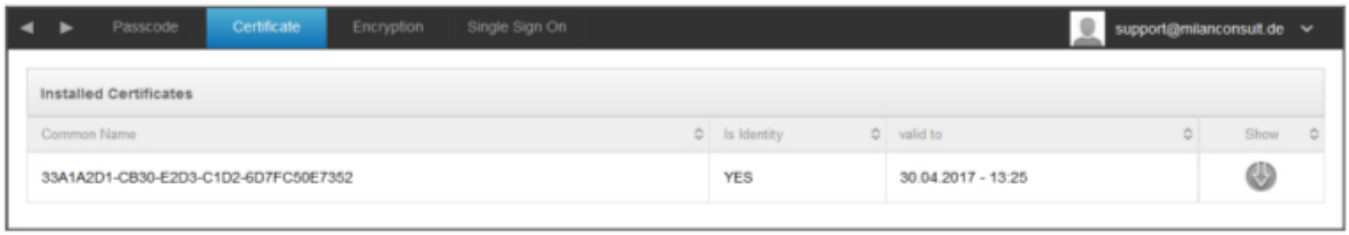
Di sini Anda menetapkan pengaturan untuk kata sandi perangkat

Penonaktifan kode diperbolehkan	Apabila pengaturan ini diaktifkan, tidak ada perintah untuk memasukkan kata sandi Setelah kata sandi dibuat, kata sandi tidak dapat dinonaktifkan
Izinkan nilai sederhana	Izinkan pengguna untuk menggunakan string angka yang sama, meningkat dan menurun (mis. 1234, 1111)
Memerlukan nilai alfanumerik	Kata sandi harus terdiri dari setidaknya satu huruf
Panjang kode sandi minimum	Panjang kata sandi minimal
Jumlah minimum karakter kompleks	Jumlah minimal simbol alfanumerik dalam kata sandi
Usia kode sandi maksimum	Jumlah hari, setelah itu kata sandi harus diubah
Kunci Otomatis Maksimum	Waktu maksimum, setelah itu perangkat terkunci
Masa tenggang maksimum untuk penguncian perangkat	Waktu, setelah itu perangkat memasuki mode Siaga yang terkunci
Jumlah maksimum percobaan yang gagal	Menetapkan, seberapa sering kata sandi dapat dimasukkan secara tidak benar, sebelum penghapusan perangkat secara menyeluruh akan dilakukan
Usia kode sandi maksimum (1-730 hari)	Usia kata sandi maksimum
Riwayat kode sandi (1-50 kode sandi)	Penggunaan kata sandi lama diperbolehkan setelah nomor ini

Klik pada tempat sampah, membuka Dialog Pengaturan Ulang Kata Sandi, yang dapat digunakan untuk menghapus kata sandi perangkat yang terlupa.

Sertifikat (hanya pada tingkat perangkat)

Menampilkan sertifikat yang tersedia pada perangkat


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

Enkripsi

Memerlukan enkripsi penyimpanan	Mengaktifkan fungsi enkripsi perangkat yang diinstal

Sistem Masuk Tunggal

Di bawah poin "Sistem Masuk Tunggal", Anda dapat mengonfigurasi autentikasi Kerberos.

Di sini, Anda menetapkan kredensial akses dan masing-masing URL/Aplikasi yang diizinkan untuk menggunakan Token Kerberos.

Tersedia dalam Mode Terawasi	
Nama Akun	Nama Akun
Nama Kepala Sekolah	Identitas unik yang dapat digunakan untuk mendistribusikan Tiket Kerberos
Realm	Realm Kerberos Anda, yang akan digunakan (mis. Domain Anda)

Dengan Simbol, Anda dapat membuat URL tambahan.

Pola URL yang digunakan untuk membatasi akun ini	URL yang akan ditentukan, di mana Tiket Kerberos dapat didistribusikan

Dengan Simbol, Anda dapat membuat Aplikasi tambahan.

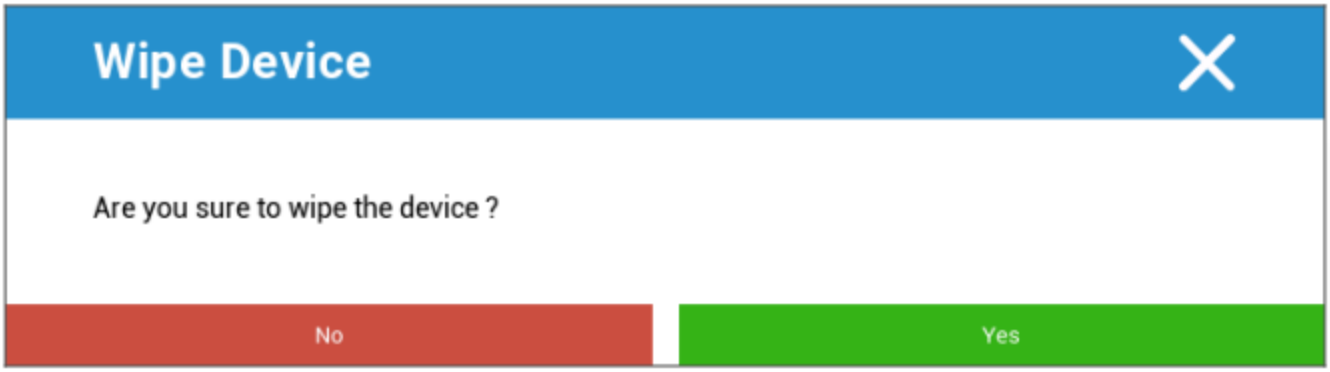
Aplikasi untuk membatasi akun ini	Aplikasi yang akan ditentukan, di mana Tiket Kerberos dapat didistribusikan

Akhir Masa Pakai (hanya pada tingkat perangkat)

Menghapus (hanya pada tingkat perangkat)

Di bawah "Hapus", Anda dapat memulihkan perangkat ke pengaturan pabrik. Di sini, data perusahaan dan data pribadi akan dihapus pada perangkat pengguna akhir.

Dengan mengklik "Simbol Minus", Anda akan menerima pesan berikut



Dengan "Ya", Anda dapat melakukan penghapusan.

Di bawah "Hapus Laporan", item berikut ini dapat ditampilkan

Dihapus oleh	Riwayat siapa yang melakukan penghapusan
Tanggal	Tanggal
Status	Status (mis. jika Penghapusan berhasil dilakukan)

Pengaturan Pembatasan

Fungsionalitas Perangkat

Di sini Anda dapat memblokir fungsi perangkat pengguna akhir secara individual

Mengizinkan penginstalan aplikasi	Mengizinkan penginstalan aplikasi
Izinkan kamera	Izinkan penggunaan kamera
Mengizinkan FaceTime	Mengizinkan FaceTime
Izinkan pengambilan layar	Izinkan pengambilan layar
Mengizinkan sinkronisasi otomatis saat roaming	Mengizinkan sinkronisasi otomatis saat roaming
Izinkan Siri	Izinkan Siri
Mengizinkan panggilan suara	Mengizinkan panggilan suara
Mengizinkan pembelian dalam aplikasi	Mengizinkan pembelian dalam aplikasi
Memerlukan kata sandi iTunes Store untuk semua pembelian	Memerlukan kata sandi iTunes Store untuk semua pembelian
Mengizinkan permainan multipemain	Mengizinkan permainan multipemain
Izinkan menambahkan teman Game Center	Izinkan menambahkan teman Game Center
Izinkan buka dari terkelola ke tidak terkelola	Izinkan membuka konten di aplikasi terkelola di aplikasi yang tidak terkelola
Izinkan buka dari tidak dikelola ke dikelola	Izinkan membuka konten di aplikasi yang tidak dikelola di aplikasi yang dikelola
Izinkan tampilan hari ini di layar kunci	Apabila pengaturan ini aktif, tampilan "Hari Ini" akan ditampilkan di Pusat Pemberitahuan pada layar kunci
Mengizinkan pusat kontrol di layar kunci	Mengizinkan Pusat Kontrol pada layar kunci
Izinkan TouchID	Izinkan TouchID
Mengizinkan pembaruan PKI melalui udara	Mengizinkan pembaruan PKI melalui udara

Izinkan buku tabungan saat terkunci	Izinkan buku tabungan saat perangkat terkunci
Batasi Pelacakan Iklan	Fungsi ini menonaktifkan Pelacakan Iklan (mis. pengiklan tidak dapat menggunakan Pelacakan Iklan untuk mendistribusikan iklan yang dipersonalisasi)
Izinkan Handoff	Izinkan Handoff
Memungkinkan hasil internet menjadi sorotan	Izinkan hasil internet menjadi sorotan (mis. Bing atau Wikipedia)
Memerlukan kode sandi pada pemasangan AirPlay pertama	Memerlukan kode sandi pada pemasangan AirPlay pertama
Pelindung Pergelangan Tangan Force Watch	Jika diaktifkan, Apple Watch dipaksa menggunakan "Perlindungan Pergelangan Tangan" (pengenalan pergelangan tangan)
Mengizinkan Perpustakaan Foto iCloud	Mengizinkan Perpustakaan Foto iCloud. Jika tidak diizinkan, maka semua gambar yang tidak diunduh sepenuhnya dari iCloud, akan dihapus di penyimpanan lokal
Tersedia dalam Mode Terawasi	
Izinkan Modifikasi Akun	Izinkan modifikasi "surat, kontak, kalender"
Izinkan AirDrop	Izinkan AirDrop
Izinkan Modifikasi Seluler Aplikasi	Pengaturan ini memblokir pengaturan aplikasi mana yang diizinkan untuk menggunakan data seluler Pengaturan ini dapat, misalnya, diatur secara manual pada perangkat pengguna akhir dan kemudian pembatasan ini dapat diaktifkan
Mengizinkan Siri meminta konten buatan pengguna dari web	Pencarian web di situs web tertentu diblokir, mis. Wikipedia, karena setiap orang dapat membuat perubahan sesuka mereka
Mengaktifkan filter kata-kata kotor Siri	Kata-kata kotor yang ditujukan kepada Siri akan disensor
Izinkan iBook Store	Izinkan iBook Store
Izinkan iBook Store Erotika	Izinkan iBook Store Erotika
Izinkan memodifikasi pengaturan Temukan Teman Saya	Izinkan memodifikasi pengaturan Temukan Teman Saya
Izinkan Game Center	Izinkan Game Center

Izinkan Pemasangan Host	Kontrol pemasangan komputer
Izinkan menginstal profil konfigurasi	Memungkinkan pemasangan profil konfigurasi
Izinkan Hapus Aplikasi	Kontrol penghapusan aplikasi
Izinkan iMessage	Izinkan iMessage
Izinkan hapus semua konten dan pengaturan	Memungkinkan penghapusan semua konten dan pengaturan
Izinkan pembatasan konfigurasi	Izinkan pembatasan konfigurasi
Izinkan Podcast	Izinkan Podcast
Izinkan Pencarian Definisi	Izinkan pencarian definisi
Izinkan Papan Ketik Prediktif	Izinkan keyboard prediktif
Izinkan Koreksi Otomatis	Izinkan koreksi otomatis
Izinkan Instalasi Aplikasi UI	Jika dinonaktifkan, tidak ada aplikasi yang dapat diinstal dari AppStore publik (ikon tidak lagi ditampilkan). Namun, aplikasi masih dapat diinstal melalui iTunes dan Konfigurator
Mengizinkan Pintasan Keyboard	Mengizinkan pintasan keyboard, jika perangkat terpasang ke keyboard fisik
Mengizinkan pemasangan Apple Watch	Melarang pemasangan antara perangkat dan Apple Watch, sambungan yang ada akan dihentikan
Izinkan modifikasi Kode Sandi	Jika tidak diizinkan, kata sandi perangkat tidak dapat ditambahkan, diubah, atau dihapus
Izinkan modifikasi nama perangkat	Panduan menentukan apakah nama perangkat dapat diubah
Izinkan modifikasi wallpaper	Pedoman menentukan apakah wallpaper dapat diubah
Mengizinkan pengunduhan aplikasi secara otomatis	Jika dinonaktifkan, aplikasi yang dibeli tidak akan diinstal secara otomatis di perangkat lain. Tidak berlaku untuk pembaruan untuk aplikasi yang sudah ada
Izinkan Berita	Mengizinkan Berita di perangkat iOS
Izinkan kepercayaan aplikasi Perusahaan	Jika diatur ke false, mencegah mempercayai aplikasi perusahaan

iCloud

Memblokir fungsi tertentu selama pemasangan iCloud

Izinkan pencadangan	Izinkan pencadangan
Mengizinkan sinkronisasi dokumen	Mengizinkan sinkronisasi dokumen
Izinkan Aliran Foto	Izinkan Aliran Foto
Izinkan Aliran Foto Bersama	Izinkan Aliran Foto Bersama
Izinkan Sinkronisasi Gantungan Kunci Cloud	Izinkan Sinkronisasi Gantungan Kunci Cloud
Izinkan aplikasi yang dikelola untuk menyimpan data	Izinkan aplikasi yang dikelola untuk menyimpan data
Memungkinkan sinkronisasi catatan dan sorotan untuk buku perusahaan	Izinkan sinkronisasi catatan & sorotan untuk buku perusahaan
Memungkinkan pencadangan buku perusahaan	Memungkinkan pencadangan buku perusahaan

Keamanan dan Privasi

Memblokir fungsi-fungsi yang terkait dengan data diagnostik

Mengizinkan data diagnostik dikirim ke Apple	Mengizinkan data diagnostik dikirim ke Apple
Izinkan pengguna untuk menerima sertifikat TLS yang tidak tepercaya	Izinkan pengguna, untuk menerima sertifikat TLS yang tidak terpercaya
Memaksakan pencadangan terenkripsi	Memaksakan pencadangan terenkripsi

BYOD

Keamanan iOS bawaan (Wadah)

iOS selalu dapat membuat perbedaan antara yang dikelola (bisnis) dan yang tidak dikelola (pribadi). Semua yang berasal dari Sistem MDM akan diperlakukan sebagai terkelola. Sebagai contoh, jika Anda menginstal Aplikasi melalui MDM atau mengonfigurasi Akun Exchange, ini akan diperlakukan sebagai dikelola oleh iOS.

Semua hal lain yang dikonfigurasi/dipasang secara manual di perangkat akan dianggap sebagai tidak terkelola. Misalnya jika Pengguna menginstal WhatsApp sendiri atau jika menambahkan Akun Exchange. Namun pemisahan ini tidak pernah mempengaruhi kontak. Namun sejak iOS 11.3 (dan yang lebih tinggi), hal ini juga ditambahkan untuk kontak.

Karena ini adalah fungsi dasar dari sistem operasi, Anda tidak perlu menginstal sesuatu atau menyiapkan wadah khusus.

Aktifkan Fungsi Bawaan untuk memisahkan aplikasi/informasi/file pribadi dan bisnis. Pengaturan ini juga akan menonaktifkan beberapa fungsi lain, yang jika tidak, dapat menonaktifkan bagian dari pemisahan ini secara tidak sengaja.

Aktivasi

Mengaktifkan Solusi Kontainer yang didukung oleh AppTec360

Aktifkan Wadah Pembagi Google	Aktifkan Wadah Pembagi Google
Mengaktifkan Kontainer SecurePIM	Mengaktifkan Kontainer SecurePIM

Jika Anda telah mengaktifkan SecurePIM Container, Anda juga akan menemukan poin berikut di bawah "Aktivasi". Selain itu, empat tab lainnya akan segera terbuka, yang dijelaskan di bawah ini.

Alamat Email Dukungan	Alamat email dukungan tempat pengguna dapat meminta bantuan jika ada masalah

Kata Sandi SecurePIM

Di bawah "Kata Sandi SecurePIM", Anda dapat menetapkan panduan untuk kekuatan keamanan kata sandi.

Batas Waktu Sesi	Di sini Anda bisa menentukan setelah berapa menit kata sandi baru harus dimasukkan lagi, setelah SecurePIM berjalan di latar belakang
Panjang Kata Sandi	Panjang kata sandi untuk akses ke Kontainer SecurePIM
Karakter Huruf Besar	Karakter huruf besar minimum
Karakter Huruf Kecil	Karakter huruf kecil minimum
Karakter Khusus	Karakter khusus minimum
Digit	Digit minimum
Hapus Aplikasi	Berapa kali kata sandi salah dimasukkan, sebelum konten SecurePIM dihapus (Namun demikian, Aplikasi masih tetap ada di perangkat pengguna akhir)

Keamanan SecurePIM

Di bawah "Keamanan SecurePIM", Anda dapat menetapkan berbagai pengaturan keamanan.

Mendeteksi Perangkat yang Dibobol Jailbreak	Jika pengaturan ini diaktifkan, akses ke SecurePIM Container akan diblokir, segera setelah perangkat terdeteksi telah di-jailbreak
Mengamankan Bidang Teks	Konten bidang pengiriman akan dienkripsi, tidak ada informasi yang sampai ke OS (iOS) Catatan: Selama pengaturan ini aktif, koreksi otomatis tidak lagi tersedia
Mengekspor Data Kontak ke Perangkat	Jika pengaturan ini diaktifkan, maka pengguna diizinkan untuk mengekspor Kontak Exchange ke perangkat lokal mereka Catatan: Hanya nama dan nomor telepon yang diekspor
Tampilkan Lokasi Acara	Jika pengaturan ini diaktifkan, lokasi acara yang akan datang akan ditampilkan di bilah notifikasi
Tampilkan Judul Acara	Apabila pengaturan ini diaktifkan, lokasi judul acara yang akan datang akan ditampilkan di bilah notifikasi

Browser SecurePIM

Di sini Anda dapat mengonfigurasi peramban SecurePIM.

Dengan simbol tersebut, Anda dapat menentukan URL baru.

Dengan simbol tersebut, Anda dapat menghapus URL yang telah ditentukan lagi.

"URL yang masuk daftar putih" adalah URL yang dapat dimuat.

"URL yang masuk daftar hitam" adalah URL yang tidak dapat dimuat dan karenanya diblokir.

Harap diperhatikan, bahwa entri Daftar Putih memiliki prioritas yang lebih tinggi daripada entri Daftar Hitam. Di bawah "Judul Penanda", Anda dapat memberikan judul. Dengan "URL Bookmark", Anda dapat mengaitkan alamat URL dengan judul bookmark - dengan cara ini Anda dapat mendistribusikan bookmark individual ke masing-masing pengguna.

Pertukaran

Di bawah "Exchange" Anda dapat mengonfigurasi akun Exchange.

Alamat Email ActiveSync	Tukar alamat email (perhatikan "Placeholder")
Login Pertukaran ActiveSync	Bertukar nama pengguna (perhatikan "Placeholder")
ActiveSync Exchange Server	Alamat Server Exchange (FQDN)
Domain Pertukaran ActiveSync	Tukar alamat Domain
Sertifikat Pengguna	Sertifikat pengguna
Otentikasi berbasis sertifikat	Pengguna mengautentikasi diri mereka sendiri dengan sertifikat
Izinkan Enkripsi S/MIME	Memungkinkan pengguna untuk mengenkripsi email mereka
Izinkan Penandatanganan S/MIME	Memungkinkan pengguna untuk menandatangani email mereka
Pemeriksaan CRL	Jika aktif, sertifikat pribadi akan dibandingkan dengan CRL (Daftar Pencabutan Sertifikat)

Manajemen Koneksi

Wi-Fi

Pengidentifikasi Set Layanan (SSID)	SSID jaringan yang akan disambungkan
Gabung Otomatis	Aktifkan penggabungan otomatis saat bergabung dengan jaringan
Jaringan Tersembunyi	Aktifkan, jika AP tidak menyiarkan SSID

Pengaturan Proxy

Mengkonfigurasi Proxy untuk setiap Titik Akses

Tidak ada		Tidak menetapkan Proxy
Manual		Membuat Proxy manual
	URL Server Proxy	Alamat untuk mengakses Pengaturan Proxy
	Pelabuhan	Menetapkan port untuk Proxy
	Otentikasi	Nama pengguna untuk autentikasi pada Proxy
	Kata sandi	Kata sandi untuk autentikasi pada Proxy
Otomatis		Membuat Proxy secara otomatis
URL Server Proxy		URL untuk akses ke pengaturan Proxy

Jenis Keamanan

Menetapkan Jenis Keamanan untuk AP

WEP	
Kata sandi	Kata sandi untuk AP

WPA/WPA2	
Kata sandi	Kata sandi untuk AP

Perusahaan WEP - Perusahaan WPA / WPA2 - Perusahaan Apa Saja			
	Protokol		
	TLS	Mengaktifkan/Menonaktifkan	
	TTLS	Mengaktifkan/Menonaktifkan	
	LEAP	Mengaktifkan/Menonaktifkan	
	PEAP	Mengaktifkan/Menonaktifkan	
	EAP-FAST	Mengaktifkan/Menonaktifkan	
	EAP-SIM	Mengaktifkan/Menonaktifkan	
	Gunakan PAC		Penggunaan PAC (Protected Access Controll)
	PAC Penyediaan	Konfigurasi PAC Penyediaan	
	PAC Penyediaan Secara Anonim	Anonim Penyediaan PAC	
	Otentikasi Bagian Dalam	Protokol autentikasi yang harus digunakan: PAP, CHAP, MSCHAP, MSCHAPv2	
	Nama pengguna	Nama pengguna otentikasi	
	Jangan gunakan Kata Sandi Per-Koneksi	Jangan gunakan Kata Sandi Per-Koneksi	
	Sertifikat Identitas	Unggah/pilih sertifikat autentikasi	
	Identitas Luar	Identitas yang dapat dilihat secara eksternal	
	Kepercayaan		
	Sertifikat Terpercaya 1	Unggah sertifikat tepercaya pertama	
	Sertifikat Terpercaya 2	Unggah sertifikat tepercaya kedua	
	Sertifikat Terpercaya 3	Unggah sertifikat tepercaya ketiga	
	Nama Sertifikat Server Tepercaya	Nama-nama sertifikat server yang diharapkan (dalam daftar yang dipisahkan koma)	

Tidak ada	Tidak menetapkan keamanan

VPN

Nama Koneksi	Nama Profil VPN

Jenis VPN

VPN

Semua lalu lintas jaringan perangkat akan dialihkan melalui koneksi VPN.

Jenis Koneksi	Menetapkan jenis koneksi VPN
IPsec (cisco)	Protokol IPsec oleh cisco
PPTP	Protokol PPTP
L2TP	Protokol L2TP
Cisco AnyConnect	Protokol AnyConnect
Juniper SSL	Protokol SSL Juniper
F5 SSL	Protokol SSL F5
SonicWall mConnect	SonicWall mobile Connect
Aruba VIA	Protokol Aruba VIA
SSL khusus	Koneksi melalui SSL Khusus
OpenVPN	Protokol OpenVPN

VPN Per-Aplikasi

Saat membuka aplikasi tertentu, koneksi VPN akan dibuat

Memulai koneksi VPN Per-Aplikasi secara otomatis		Memulai koneksi VPN Per-Aplikasi secara otomatis
Jenis Koneksi		Menetapkan jenis koneksi VPN
	Cisco AnyConnect	Protokol AnyConnect
	Juniper SSL	Protokol SSL Juniper
	F5 SSL	Protokol SSL F5
	SonicWall mConnect	SonicWall mobile Connect
	Aruba VIA	Protokol Aruba VIA
	SSL khusus	Koneksi melalui SSL Khusus
	OpenVPN	Protokol OpenVPN

Pengaturan Proxy

Mengkonfigurasi Proxy untuk koneksi VPN

Tidak ada	Tidak menetapkan Proxy
Manual	Membuat Proxy secara manual
URL Server Proxy	Alamat untuk akses ke Pengaturan Proxy
Pelabuhan	Menetapkan port untuk Proxy
Otentikasi	Nama pengguna untuk autentikasi di Proxy
Kata sandi	Kata sandi untuk autentikasi di Proxy
Otomatis	Membuat Proxy secara otomatis
URL Server Proxy	URL untuk akses ke pengaturan Proxy

Tampilkan Placeholder	Menampilkan semua variabel pengguna yang tersedia, yang dapat digunakan AppTec360

APN

Nama Titik Akses	Nama Titik Akses
Nama Pengguna Titik Akses	Nama pengguna Titik Akses
Kata Sandi Titik Akses	Kata sandi Titik Akses
Server Proxy	Alamat Server Proxy
Pelabuhan	Port Proxy yang bersangkutan

Seluler

Mengaktifkan Roaming Data	Mengaktifkan Roaming Data
Mengaktifkan Roaming Suara	Mengaktifkan Roaming Suara
Mengaktifkan Hotspot	Mengaktifkan Hotspot

Proksi HTTP

Jenis Proxy	
Manual	Membuat Proxy secara manual
URL Server Proxy	Alamat untuk akses ke Pengaturan Proxy
Pelabuhan	Menetapkan port Proxy
Otentikasi	Nama pengguna untuk autentikasi di Proxy
Kata sandi	Kata sandi untuk autentikasi di Proxy
Otomatis	Membuat Proxy secara otomatis
URL PAC Proksi	URL PAC Proksi
Izinkan koneksi langsung jika PAC tidak dapat dijangkau	Izinkan koneksi langsung (tanpa VPN), jika PAC tidak dapat dijangkau
Izinkan melewati proxy untuk mengakses jaringan captive	Izinkan melewati proxy untuk mengakses jaringan internal captive

AirPrint

Alamat IP	Alamat IP printer
Jalur Sumber Daya	Jalur yang pasti ke perangkat AirPrint

AirPlay

Nama Perangkat	Nama perangkat
Kata sandi	Memasangkan kata sandi
Daftar putih	Tentukan daftar perangkat yang dapat dipasangkan secara eksklusif dengan perangkat tersebut

Manajemen PIM

Sinkronisasi Aktif Pertukaran

Nama Akun	Nama akun email
Pertukaran Host ActiveSync	Alamat/FQDN server
Izinkan Pindah	Memungkinkan pemindahan email
Gunakan Hanya di Mail	Interaksi hanya dapat terjadi pada Aplikasi Mail asli
Gunakan SSL	Gunakan enkripsi SSL
Domain	Domain server
Pengguna	Nama pengguna
Alamat email	alamat email (hanya pada tingkat perangkat)
Kata sandi (hanya pada tingkat perangkat)	Kata sandi pengguna
Sertifikat Identitas	Pilih sertifikat masing-masing untuk autentikasi di server
Hari-hari Terakhir Mail untuk Disinkronkan	Jumlah hari, hingga email disinkronkan kembali. Tanpa Batas = tidak terbatas
Mengaktifkan S/MIME	Mengaktifkan enkripsi S/MIME
Menandatangani Sertifikat	Unggah Sertifikat Penandatanganan masing-masing
Sertifikat Enkripsi	Unggah Sertifikat Enkripsi masing-masing

eMail

Pengaturan akun POP3 / IMAP pada perangkat pengguna akhir

Deskripsi Akun	Nama des Akun Email		
Jenis Akun	IMAP	Awalan Jalur	Awalan Jalur untuk folder khusus
	POP		
Nama Tampilan Pengguna	Nama tampilan pengguna		
Alamat email	Alamat email pengguna		
Izinkan Pindah	Memungkinkan pemindahan email		
Mengaktifkan S/MIME	Mengaktifkan enkripsi S/MIME		
Menandatangani Sertifikat	Unggah Sertifikat Penandatanganan masing-masing		
Sertifikat Enkripsi	Unggah Sertifikat Enkripsi masing-masing		

Surat Masuk

Pengaturan server yang masuk

Alamat Server Surat	Alamat Server Surat
Port Server Surat	Port Server Surat
Nama Pengguna	Nama pengguna masing-masing
Jenis Otentikasi	Jenis Otentikasi
Tidak ada	Tidak Ada Jenis Otentikasi
Kata sandi (hanya pada tingkat perangkat)	Permintaan kata sandi
Tantangan-Tanggapan MDM	
NTLM	Otentikasi NTLM
HTTP MD5 Digest	
Gunakan SSL	Gunakan SSL, jika diperlukan

Surat Keluar

Pengaturan server keluar

Alamat Server Surat	Alamat Server Surat
Port Server Surat	Port Server Surat
Nama Pengguna	Nama Pengguna masing-masing
Jenis Otentikasi	
Tidak ada	Tidak ada metode otentikasi
Kata sandi (hanya pada tingkat perangkat)	Permintaan kata sandi
Tantangan-Tanggapan MDM	
NTLM	Otentikasi NTLM
HTTP MD5 Digest	
Gunakan SSL	Gunakan SSL, jika diperlukan
Kata sandi keluar sama dengan kata sandi masuk	Kata sandi keluar sama dengan kata sandi masuk
Gunakan hanya dalam surat	Aktifkan, jika semua email keluar akan dikirim melalui Aplikasi Mail

CalDav

Mengonfigurasi pengaturan dan distribusi Akun CalDav

Deskripsi Akun	Menampilkan nama akun
Nama host	Nama host dan/atau alamat IP
Pelabuhan	Pelabuhan Akun CalDav
URL utama	URL Utama Akun
Nama pengguna	Nama pengguna CalDav masing-masing
Kata sandi (hanya pada tingkat perangkat)	Kata sandi CalDav masing-masing
Gunakan SSL	Gunakan SSL, jika diperlukan

Kalender Berlangganan

Menyiapkan dan mendistribusikan Kalender Berlangganan

Deskripsi	Menampilkan nama akun
URL	URL basis data kalender
Nama pengguna	Nama pengguna langganan kalender
Kata sandi (hanya pada tingkat perangkat)	Kata sandi langganan kalender
Gunakan SSL	Gunakan SSL, jika diperlukan

LDAP

Di area ini, siapkan koneksi LDAP, untuk memungkinkan pertukaran sertifikat dinamis, antara perangkat pengguna akhir dan Direktori Aktif.

Harap diperhatikan bahwa pengguna yang dipilih memerlukan izin baca masing-masing.

Deskripsi Akun	Deskripsi Akun
Nama Pengguna Akun	Pengguna untuk akses LDAP
Kata Sandi Akun	Kata sandi untuk akses LDAP
Nama Host Akun	Nama host/alamat IP Server LDAP
Gunakan SSL	Gunakan SSL, jika diperlukan

Pada bagian kedua, Anda dapat menentukan filter individual untuk pencarian di registri LDAP.

Deskripsi	Cakupan	Basis Pencarian
Deskripsi filter	Tingkat pencarian di registri LDAP	Menentukan filter individual

Manajemen Web

Klip web

Di lokasi ini tentukan bookmark, dengan tautan ke halaman web, portal intranet, dan lain-lain, yang akan terlihat sebagai aplikasi pada perangkat pengguna akhir.

Label	Nama koneksi pada perangkat pengguna akhir
URL	Tautan ke situs web masing-masing
Dapat dilepas	Jika diaktifkan, pengguna dapat menghapus webclip
Ikon	Melalui dialog ini, unggah logo untuk koneksi: Dimensi 180x180, format png
Ikon yang Telah Disusun Sebelumnya	Jika diaktifkan, tidak ada efek tambahan (bayangan, pantulan) yang akan ditampilkan pada ikon
Layar Penuh	Saat membuka klip web, browser terbuka dalam mode layar penuh

Filter Konten Web

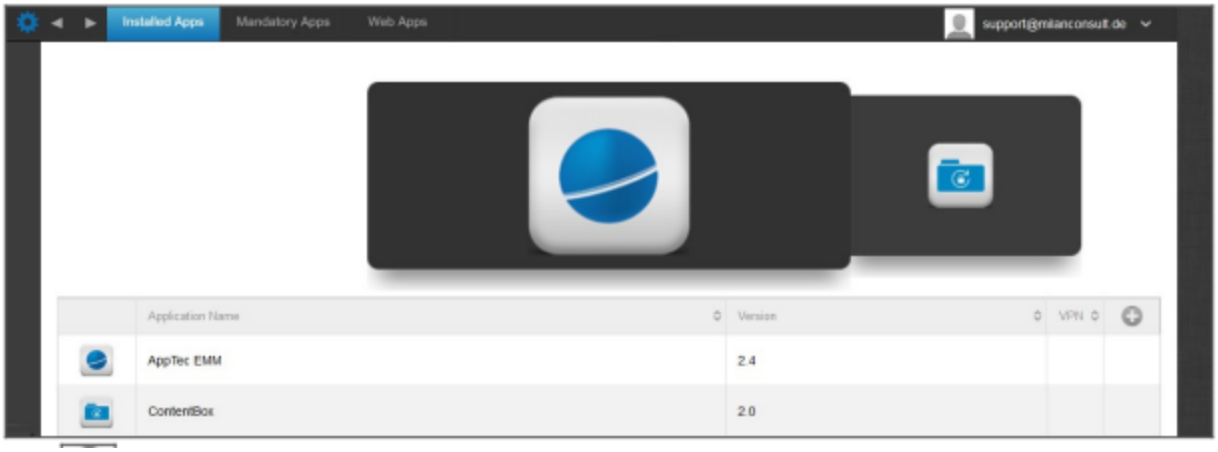
Filter Konten Web memungkinkan untuk membatasi akses ke halaman internet tertentu.

Situs Web yang Diizinkan	
Batasi Konten Dewasa	Filter web secara otomatis diterapkan untuk konten dewasa
URL yang diizinkan	Dengan simbol + tambahkan halaman yang diizinkan
URL yang masuk daftar hitam	Dengan simbol + tambahkan halaman yang diblokir
Hanya Situs Web Tertentu	Hanya konten tertentu yang dapat ditampilkan, yang dapat Anda tambahkan dengan simbol +.

Manajemen Aplikasi

Manajer Aplikasi Perusahaan

Aplikasi Terinstal (hanya pada tingkat perangkat)



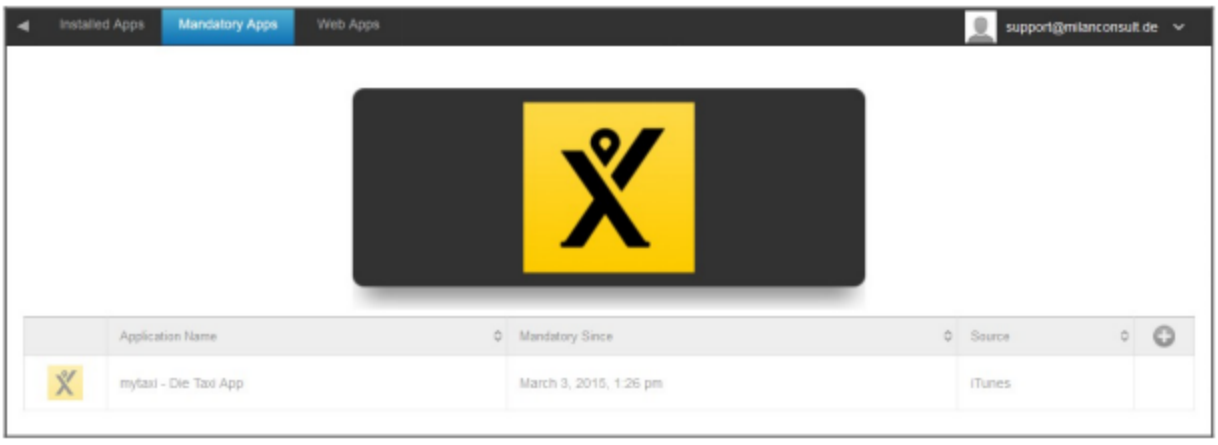
Di sini Anda dapat melihat Aplikasi yang saat ini terinstal pada perangkat.

Aplikasi Wajib

Di bawah Aplikasi Wajib, Anda dapat memandatkan Aplikasi yang diperlukan.

Pengguna akan terus diingatkan untuk menginstal Aplikasi yang disebutkan di atas.

Melalui , Aplikasi yang diamanatkan dapat ditentukan.



Ini dapat berupa Aplikasi Apple App Store, tetapi juga Aplikasi In-House.

Jika ini melibatkan perangkat yang diawasi, maka aplikasi akan diinstal secara otomatis.

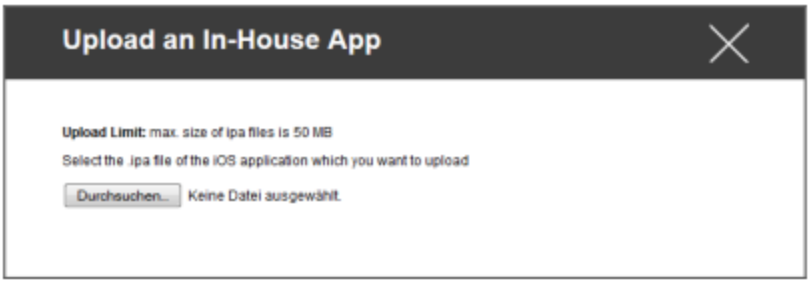
Anda dapat mendorong Aplikasi "Apple AppStore" dari AppStore publik ke perangkat, serta Aplikasi In-House yang dikembangkan secara internal.

Atau Anda dapat memilih dari kategori "Aplikasi In-House iOS" dan memilih Aplikasi In-House, yang telah Anda unggah di Pengaturan Umum.

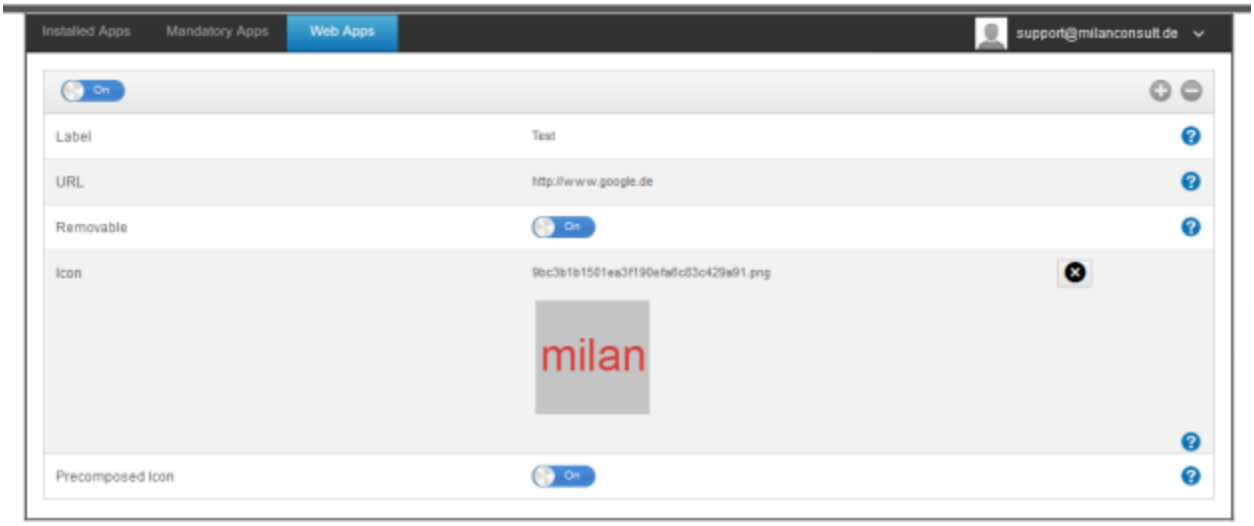
Opsi pemasangan

Tetap up to date (hanya didukung untuk VPP per perangkat)	Seminggu sekali, akan ditentukan, apakah ada pembaruan untuk aplikasi. Jika ya, pembaruan ini akan diinstal Untuk Aplikasi In-House, Target Pembaruan yang Anda konfigurasikan di Pengaturan Umum akan digunakan untuk proses pembaruan.
Menyalip ketika tidak dikelola	Jika aplikasi sudah terpasang, MDM akan mengambil alih aplikasi dan mengelolanya
Menghapus aplikasi saat profil MDM dihapus	Dalam kasus penghapusan manajemen perangkat, Aplikasi akan dihapus instalasinya
Mencegah pencadangan data aplikasi	Cadangan data khusus aplikasi tidak akan dibuat
Pengaturan Aplikasi	Di bawah "Pengaturan Aplikasi", Anda dapat menetapkan nilai tertentu ke dalam latar depan aplikasi (selama aplikasi mendukungnya, jika perlu tanyakan kepada pengembang aplikasi).

Anda juga dapat secara langsung memilih dan mengunggah file ipa, melalui "Unggah Aplikasi In-House".



Aplikasi Web



Di bawah poin "Aplikasi Web", Anda dapat, serupa dengan "Klip Web", mendorong halaman internet atau portal intranet sebagai aplikasi ke perangkat pengguna akhir, di area Manajemen Web. Sebagai default, Aplikasi Web akan ditampilkan dalam mode layar penuh, yang dapat dikonfigurasikan di bawah Klip Web.

Label	Nama koneksi pada perangkat pengguna akhir
URL	Tautan ke Situs Web masing-masing
Dapat dilepas	Jika diaktifkan, pengguna dapat menghapus Webclip
Ikon	Melalui dialog ini, unggah logo untuk koneksi: Dimensi 180x180, format png
Ikon yang Telah Disusun Sebelumnya	Jika diaktifkan, tidak ada efek tambahan (bayangan, pantulan) yang akan ditampilkan pada ikon

Pembatasan & Pengaturan

Aplikasi yang Masuk Daftar Hitam/Daftar Putih

Di sini Anda dapat mengatur aplikasi yang diblokir (atau diizinkan) tergantung pada pengaturan Anda di "Pengaturan Umum". Klik akan memunculkan pencarian aplikasi yang dikenal. Di sana Anda dapat mencari aplikasi yang ingin Anda tambahkan.

Perhatikan bahwa perangkat yang diawasi diperlukan untuk fungsi ini

Pembatasan SysApp

Memblokir aplikasi atau fungsi tertentu dari perangkat Anda

Mengizinkan penggunaan YouTube	Mengizinkan penggunaan YouTube
Mengizinkan penggunaan iTunes Store	Mengizinkan penggunaan iTunes Store
Mengizinkan penggunaan Safari	Mengizinkan penggunaan Safari
Mengaktifkan pengisian otomatis	Memungkinkan pengisian otomatis
Memaksa peringatan penipuan	Memaksakan peringatan penipuan
Mengaktifkan JavScript	Mengaktifkan penggunaan JavaScript
Blokir pop-up	Memblokir semua jenis pup-up
Izinkan Cookie	Memilih kapan Safari akan menerima cookie

Aplikasi-VPN

Melalui simbol ini, Anda dapat menentukan aplikasi yang secara otomatis akan meluncurkan koneksi VPN yang dipilih pada saat memulai.

Pengaturan Aplikasi

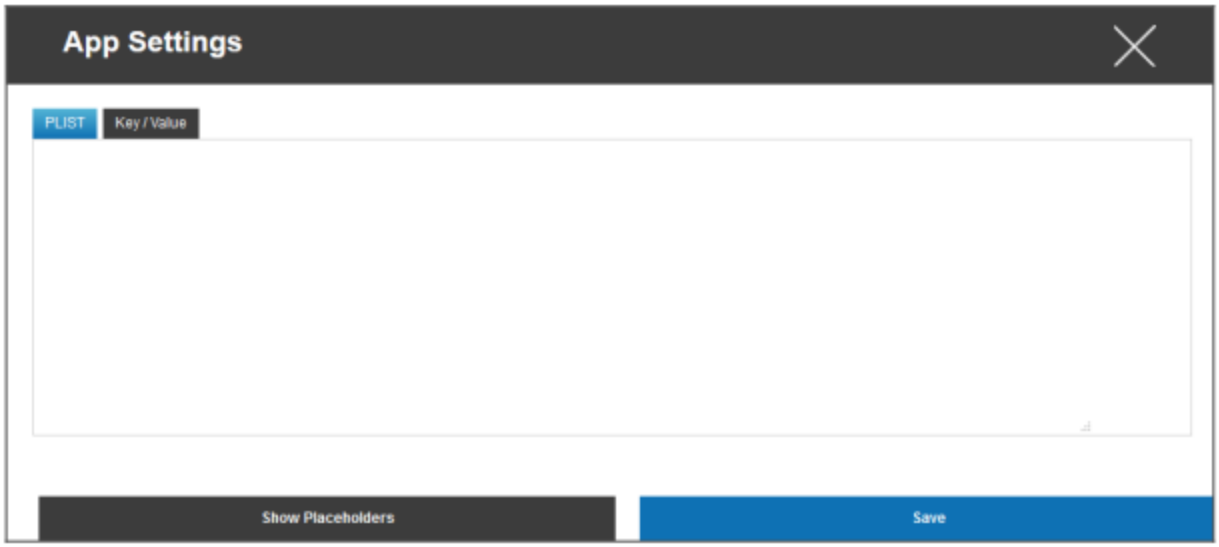
Di bawah "Pengaturan Aplikasi", Anda dapat menetapkan nilai tertentu ke dalam latar depan aplikasi (selama aplikasi mendukungnya, jika perlu tanyakan kepada pengembang aplikasi).

Melalui simbol tersebut, Anda menambahkan aplikasi (tambahan). Sekali lagi, Anda akan menemukan representasi AppTec360 yang sudah dikenal sebagai App-Import.

Cari di sini Aplikasi yang ingin Anda konfigurasikan dan pilih. Pengaturan hanya akan berlaku untuk aplikasi yang dikelola.

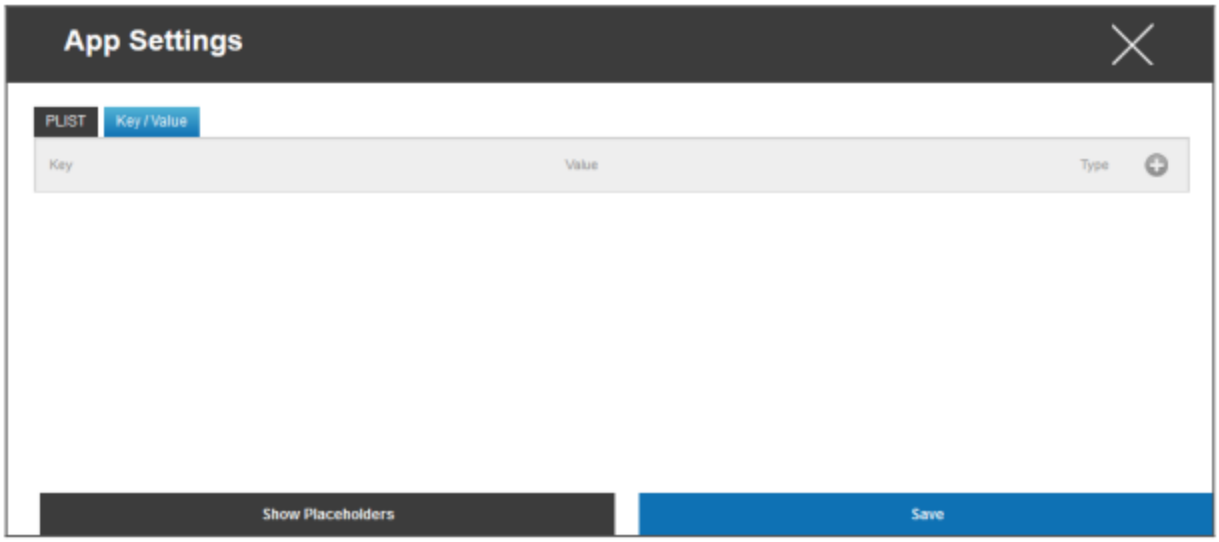
Jika impor telah berhasil, Anda akan melihat tampilan berikut ini:

Sekarang, dengan sekali klik pada , Anda dapat melakukan berbagai macam konfigurasi. Anda kemudian akan menerima ikhtisar berikut ini:

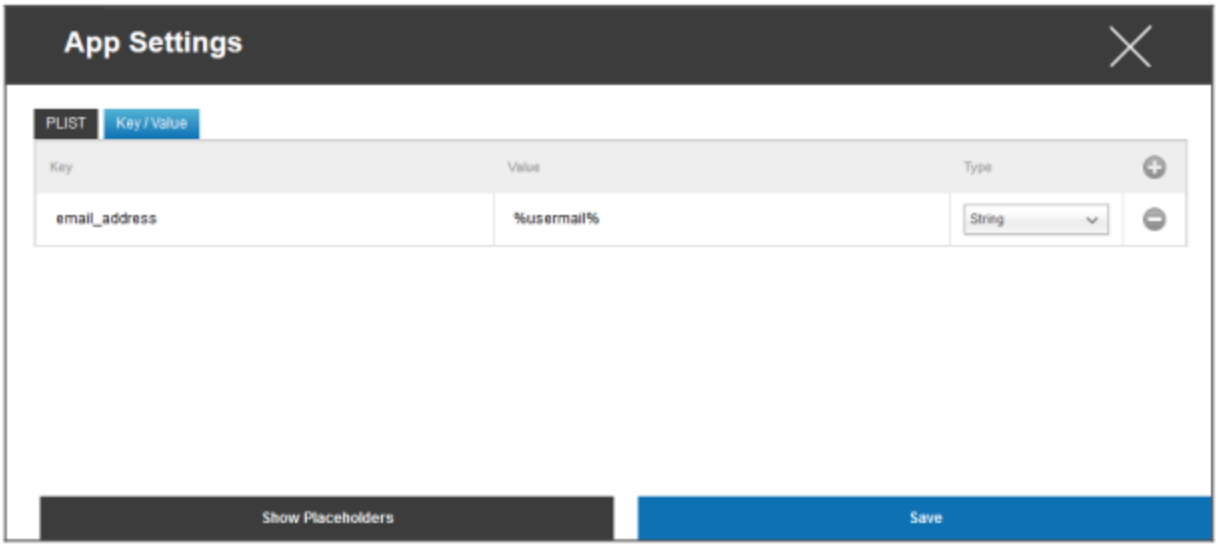


Jika Anda sudah memiliki PLIST (teks sumber konfigurasi), Anda dapat menambahkannya di sini dan menyimpannya dengan "Save".

Di bawah "Kunci / Nilai", Anda dapat melampirkan konfigurasi spesifik ke Aplikasi



Di sini, Anda dapat membuat kunci baru dan nilainya dengan simbol.



Tentu saja, semua placeholder AppTec siap membantu Anda

Penjelasan "Jenis":

String	Teks
Boolean	Benar/Salah
Nomor	Nomor

Dengan simbol tersebut, Anda dapat menghapus aplikasi lagi.

Toko Aplikasi Perusahaan

Aplikasi iTunes

Di bawah poin ini, Anda dapat mendistribusikan Aplikasi opsional untuk Pengguna Anda.

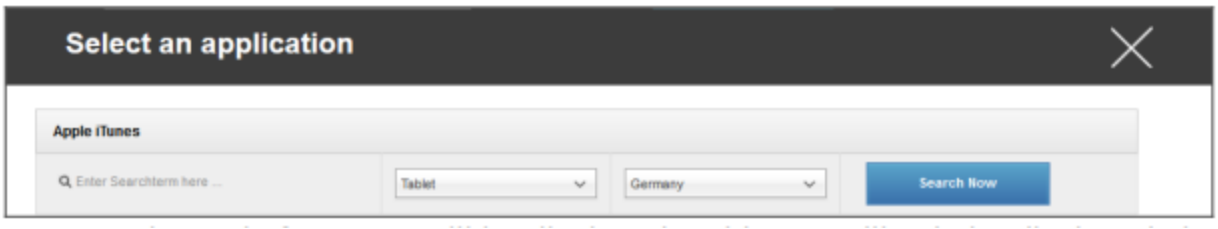
Jika ada Aplikasi di sini, maka akan diinstal secara otomatis pada perangkat pengguna akhir AppTec360 Store.

Ini hanyalah tautan ke Apple App Store resmi. Karena alasan ini, setiap perangkat pengguna akhir harus dilengkapi dengan ID Apple.

Pada titik ini, kami menyarankan agar setiap pengguna memiliki ID Apple sendiri.

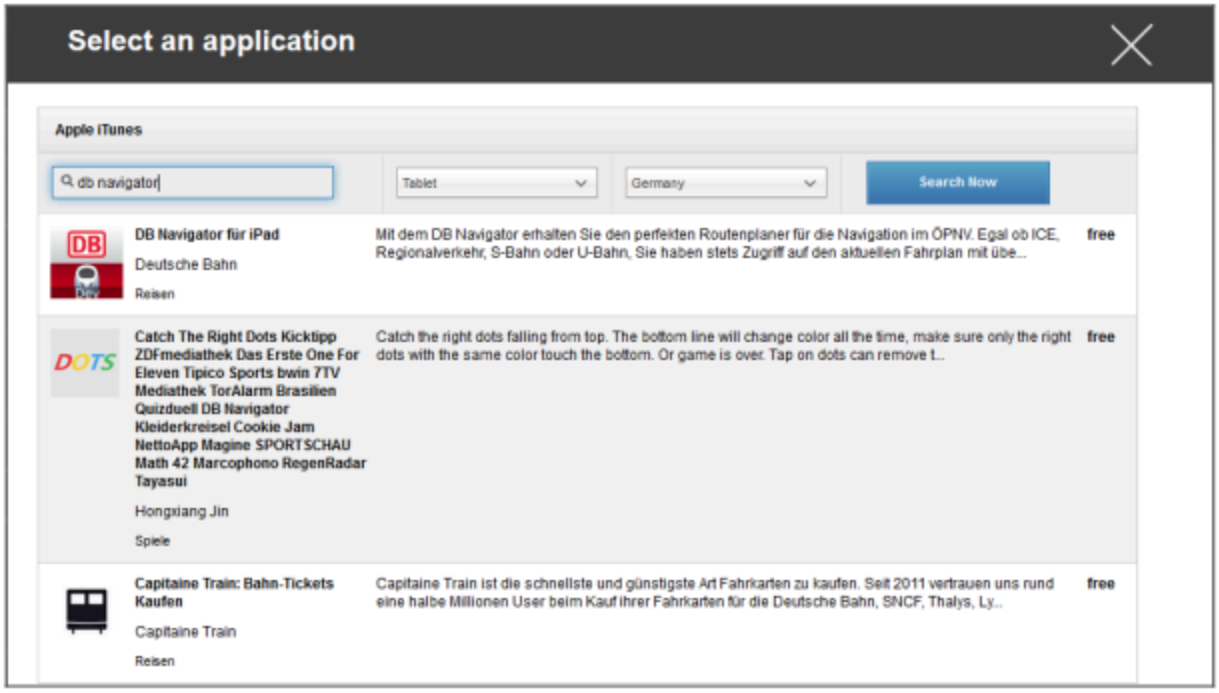
Dengan simbol tersebut, Anda dapat menambahkan Aplikasi tambahan.

Setelah itu, jendela dengan ikhtisar berikut ini akan terbuka.



Harap dicatat, bahwa hanya aplikasi gratis yang akan ditampilkan, aplikasi berbayar hanya akan ditampilkan melalui VPN.

Di bawah "Masukkan Istilah Pencarian di sini...", Anda dapat mencari aplikasi yang ada di Apple App Store.



Setelah Anda mengklik Ikon atau nama aplikasi, Anda akan diminta lagi untuk melakukan konfigurasi tambahan.

Tetap up to date	Seminggu sekali, akan ditentukan, apakah ada pembaruan untuk aplikasi. Jika ya, pembaruan ini akan diinstal
Menghapus aplikasi saat profil MDM dihapus	Dalam kasus penghapusan manajemen perangkat, Aplikasi akan dihapus instalasinya
Mencegah pencadangan data aplikasi	Cadangan data khusus aplikasi tidak akan dibuat
Aplikasi-VPN	Pilih koneksi VPN, yang akan diluncurkan saat membuka Aplikasi

Setelah klik pada "Instal", aplikasi akan ditambahkan ke Enterprise App Store dan kemudian dapat diinstal pada perangkat pengguna akhir, melalui AppTec360 AppStore.

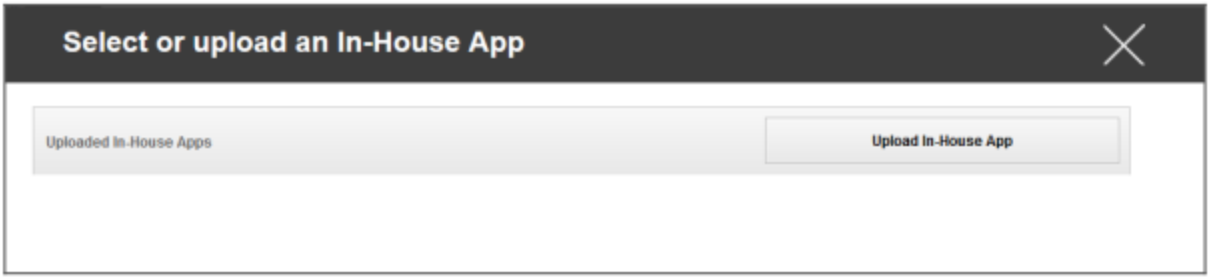
Jika Impor App-Store telah berhasil, Anda akan menerima ikhtisar berikut ini:

In-House

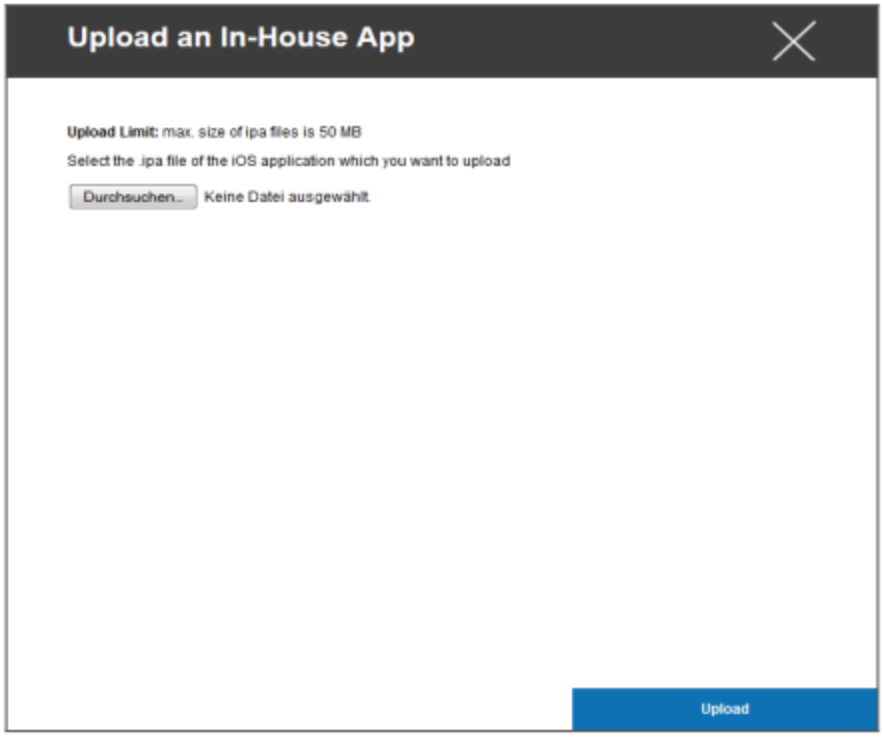
Di bawah poin "In-House", Anda dapat mengunggah Aplikasi yang dikembangkan secara internal dan mendistribusikannya.

Dengan simbol tersebut, Anda dapat mendistribusikan Aplikasi In-House tambahan.

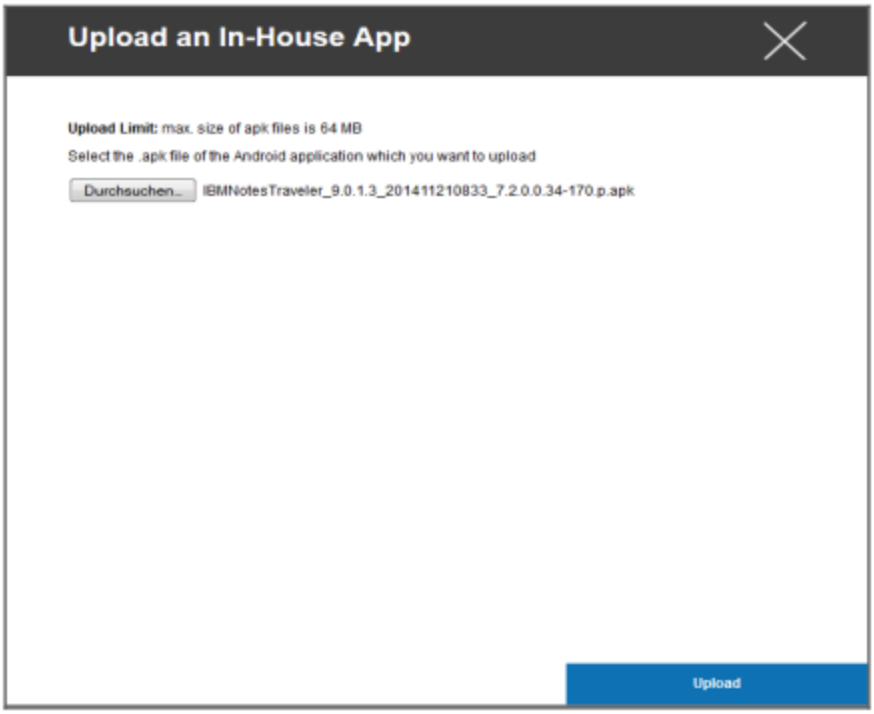
Jika Anda belum pernah mendistribusikan Aplikasi In-House, Anda akan menerima gambaran umum berikut ini:



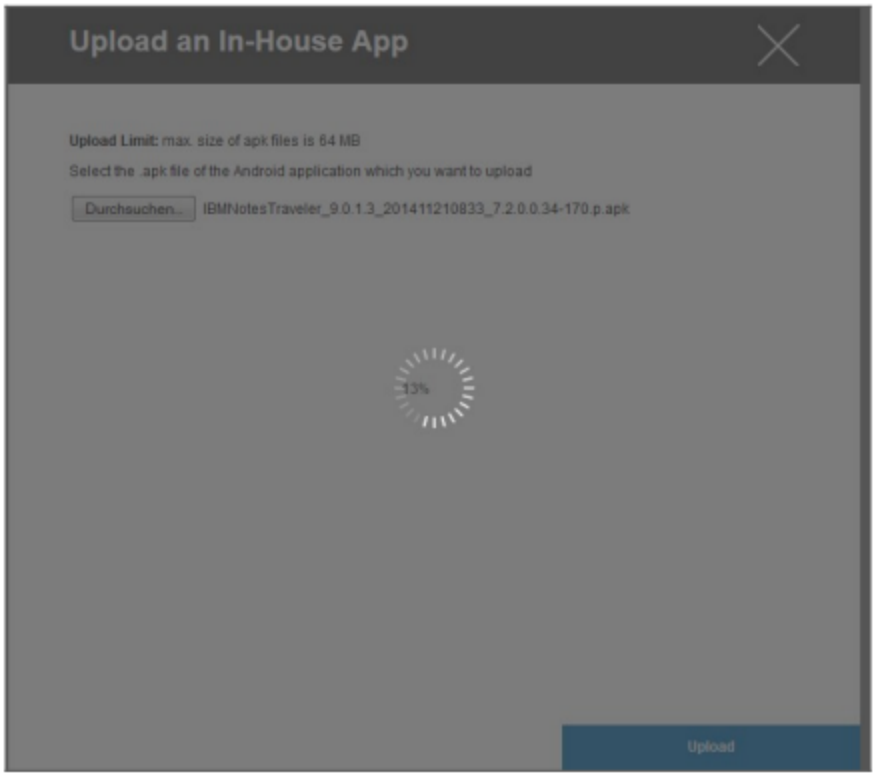
Untuk melakukan ini, klik "Unggah Aplikasi In-House", Anda kemudian akan menerima gambaran umum berikut:



Sekarang, pilih dengan "Cari..." file .ipa dan kemudian klik "Unggah"



Aplikasi Anda sekarang akan diunggah. Di tengah lingkaran, Anda bisa melihat persentase berapa banyak Aplikasi Anda yang telah diunggah.



Jika pengunggahan Aplikasi In-House berhasil dilakukan, Anda akan melihat aplikasi yang baru diunggah di Katalog Aplikasi Anda.

Pengguna sekarang memiliki opsi untuk melihat dan menginstal aplikasi ini di AppTec360 Store di perangkat pengguna akhir, di bawah kategori "In-House".

Karena ini tidak melibatkan Aplikasi Apple AppStore publik, pengguna tidak memerlukan ID Apple yang tersimpan di perangkat pengguna akhir.

Mode Kios

Mode Kios iOS hanya Tersedia dalam Mode Terawasi

Mode Kios memungkinkan Anda untuk menentukan terlebih dahulu Aplikasi atau URL, sehingga memungkinkan untuk menjalankan/mengunjungi Aplikasi/URL ini secara eksklusif.

Selain itu, Anda dapat menonaktifkan berbagai tombol perangkat keras dalam Kiosk Mode.

Jenis Aplikasi

Paket

Jika Anda ingin meluncurkan aplikasi dalam Mode Kios, pilih "Paket" di bawah "Jenis Aplikasi"

Aplikasi Kios	Klik di sini, untuk memilih aplikasi yang akan diluncurkan dalam Mode Kios Anda akan menemukan gambaran umum Manajemen Aplikasi saat ini Anda dapat memilih antara "Aplikasi Apple iTunes" dan "Aplikasi In-House iOS"

URL

Jika Anda ingin meluncurkan URL dalam Mode Kios, pilih "URL" di bawah "Jenis Aplikasi"

URL	Sekarang, tentukan alamat URL yang diinginkan
Kebijakan Asal yang Sama	Jika fungsi ini aktif, pengguna hanya dapat menjelajahi subhalaman dari URL yang telah ditentukan sebelumnya Misalnya, jika Anda telah menentukan URL berikut: www.mypage.com, maka pengguna dapat berselancar di www.mypage.com/subpage
URL yang masuk daftar putih	Di sini Anda dapat mengelola Daftar Putih, semua URL ini diizinkan Maksimum 1 URL per baris URL harus dimulai dengan http:/ atau https://
URL yang masuk daftar hitam	Di sini Anda dapat mengelola Daftar Hitam, semua URL ini dilarang Maksimum 1 URL per baris URL harus dimulai dengan http:/ atau https://
Menghapus browser setelah tidak aktif	Setelah tidak aktif, Cache Browser akan dikosongkan
Kata Sandi Keluar Diaktifkan	Jika Anda mengaktifkan fungsi ini, pengguna memiliki opsi untuk mengakhiri Mode Kios dengan kata sandi, yang telah Anda tentukan sebelumnya
Keluar dari Kata Sandi	Ini adalah kata sandi yang telah Anda tentukan sebelumnya

Pengaturan Mode Kios

Mode Kios Terjadwal	Berdasarkan waktu, Anda dapat mengatur Mode Kios, sehingga mode tersebut dimulai dan diakhiri secara otomatis pada waktu yang telah ditentukan sebelumnya
Waktu Mulai	Waktu mulai
Waktu dalam menit	Waktu dalam menit, setelah itu Mode Kios harus diakhiri lagi
Nonaktifkan Sentuhan	Jika diaktifkan, layar sentuh dinonaktifkan
Menonaktifkan Rotasi Perangkat	Jika diaktifkan, adaptasi layar otomatis dinonaktifkan
Menonaktifkan Tombol Dering	Jika diaktifkan, sakelar dering akan dinonaktifkan. Sejak saat itu, perilaku tergantung pada fungsi yang ditetapkan sebelumnya
Menonaktifkan tombol volume	Jika diaktifkan, tombol volume akan dinonaktifkan
Menonaktifkan Tombol Tidur Bangun	Jika diaktifkan, sakelar hidup/mati akan dinonaktifkan
Menonaktifkan Kunci Otomatis	Jika diaktifkan, perangkat tidak akan dialihkan ke mode siaga
Mengaktifkan Voice Over	Jika diaktifkan, Voice Over Assistant akan diaktifkan
Aktifkan Zoom	Jika diaktifkan, zoom akan diaktifkan
Aktifkan Balikkan Warna	Jika diaktifkan, mode tampilan terbalik akan diaktifkan
Mengaktifkan Sentuhan Bantuan	Jika diaktifkan, AssistiveTouch akan diaktifkan
Mengaktifkan Pilihan Bicara	Jika diaktifkan, pilihan bicara akan diaktifkan
Mengaktifkan Audio Mono	Jika diaktifkan, Audio Mono akan diaktifkan
Sulih Suara	Jika diaktifkan, pengguna dapat mengaktifkan VoiceOver
Memperbesar	Jika diaktifkan, pengguna dapat mengaktifkan Zoom
Membalikkan Warna	Jika diaktifkan, pengguna dapat mengaktifkan warna terbalik
Sentuhan Bantuan	Jika diaktifkan, pengguna dapat mengaktifkan sentuhan bantuan

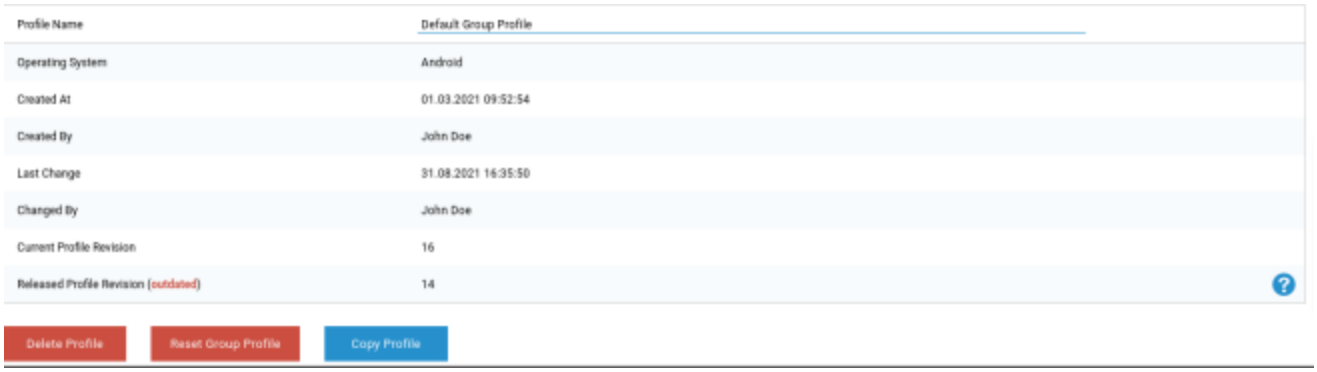
Android Enterprise – Konfigurasi Perangkat yang Dikelola Sepenuhnya

Tergantung pada apakah Anda saat ini telah memilih profil grup atau perangkat, ikhtisar dan sub-poinnya akan berbeda - harap pertimbangkan hal ini dengan saksama!

Umum

Ikhtisar profil grup (hanya pada tingkat grup)

Ketika membuka profil grup, Anda akan mendapatkan ikhtisar singkat profil.



Nama Profil	Nama profil (dapat diubah di sini)
Sistem Operasi	Sistem Operasi profil ini untuk
Dibuat di	Waktu pembuatan
Dibuat oleh	Pembuat profil
Perubahan Terakhir	Waktu perubahan terakhir pada profil
Diubah oleh	Akun yang melakukan perubahan terakhir
Revisi Profil Saat Ini	Revisi status profil yang disimpan
Revisi Profil yang Dirilis	Menetapkan revisi profil ("Tetapkan sekarang"). Jika label menunjukkan "(usang)" di belakang teks, itu berarti Anda telah menyimpan profil tetapi belum menetapkannya, sehingga perangkat masih akan mendapatkan versi yang lebih lama.

Ikhtisar Perangkat (hanya pada tingkat perangkat)

Jika Anda menggunakan perangkat, Anda akan menerima rekap ikhtisar perangkat yang dipilih, berikut ini yang terdapat di sini:

Nama Perangkat	Nama perangkat
Lokasi	Koordinat lokasi
Nomor Telepon	Nomor telepon
Aplikasi Wajib yang Ditetapkan	Jumlah Aplikasi Wajib yang ditetapkan
Versi OS	Versi OS perangkat
Sistem Operasi	Sistem Operasi (Android Enterprise)
Nomor Seri	Nomor seri perangkat
Kepemilikan Perangkat	Perangkat perusahaan atau pribadi
Jenis Perangkat	Perangkat yang Dikelola Pekerjaan AE
Berakar	Status, menunjukkan apakah perangkat telah di-root
Sesuai	Sesuai dengan pedoman
Alamat IP	Alamat IP perangkat
Terakhir terlihat	Titik waktu, ketika perangkat terakhir kali terhubung ke AppTec
Dorongan Terakhir	Titik waktu, ketika dorongan terakhir dikirim ke perangkat
Mode Pemilik Perangkat AE	Ya.
Penugasan Pengguna	Pengguna atau grup yang ditetapkan untuk perangkat ini

Revisi Konfigurasi (hanya pada tingkat perangkat)

Di sini Anda menerima ikhtisar profil grup mana yang ditetapkan ke perangkat.

Jika Anda mengklik profil grup, Anda akan mendapatkan akses langsung ke profil ini dan Anda dapat melakukan pengaturan.

Dengan simbol ini, Anda dapat mengembalikan aplikasi yang didistribusikan ke pengaturan profil grup.

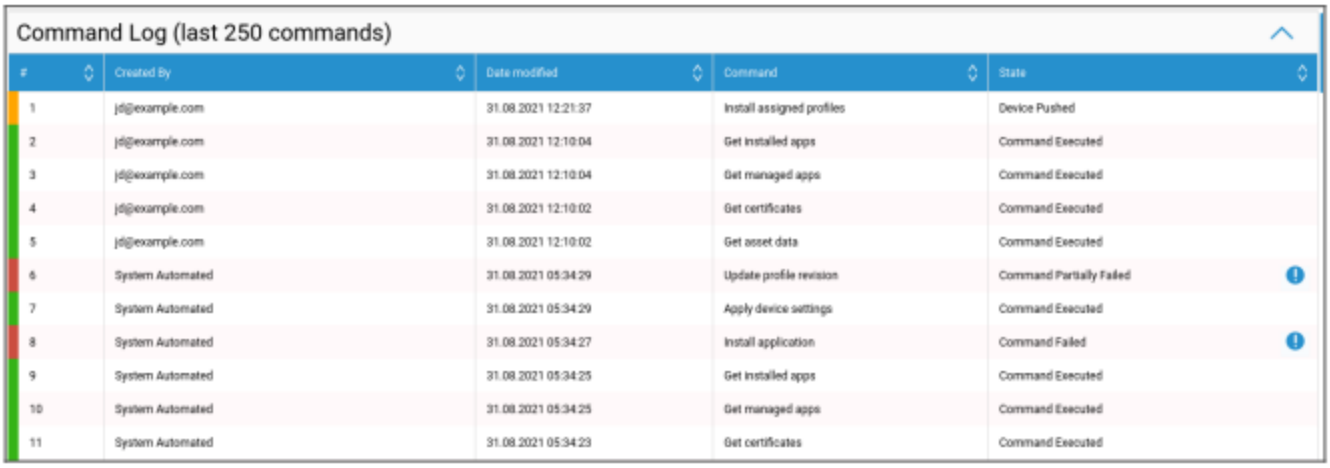
Dengan simbol ini, Anda dapat mengembalikan semua aplikasi yang digunakan ke pengaturan profil grup.

"Revisi terbaru tersedia" menunjukkan bahwa profil grup telah diubah dan disimpan namun belum ditetapkan. Profil grup harus ditetapkan dengan "Tetapkan sekarang" pada tingkat grup untuk menerapkan perubahan ke perangkat.

Log Perangkat (hanya pada tingkat perangkat)

Log Perintah

Di sini Anda dapat melihat perintah mana yang dikeluarkan untuk perangkat dan bagaimana statusnya.



Perintah yang dibuat oleh "System Automated" secara otomatis dibuat oleh sistem.

Kemungkinan status perintah

Perangkat Didorong	Permintaan push telah dikirim ke layanan push (misalnya APNS) untuk memberi tahu perangkat agar terhubung kembali ke server EMM.
Perintah Dibuat	Perintah ini dibuat dalam sistem.
Perintah Terkirim	Perintah dikirim ke perangkat setelah perangkat terhubung ke server.
Perintah Dieksekusi	Perintah berhasil dijalankan.
Perintah Gagal	Perintah gagal. *
Perintah Gagal Sebagian	Tergantung pada OS perangkat, beberapa perintah mungkin akan dikelompokkan bersama. Dalam hal ini, beberapa bagian dari grup perintah ini gagal. *
Perintah Dieksekusi, akhirnya Gagal	Perintah itu dijalankan tetapi mungkin tidak.
Perintah Ditolak	Perintah tersebut ditolak oleh pengguna.
Dibuang	Perintah telah dibuang. Misalnya karena digantikan oleh perintah lain atau perangkat didaftarkan ulang dan perintah lama dihapus

Jika ada tanda seru di belakang pesan, Anda dapat memperoleh informasi lebih lanjut dengan mengarahkan kursor ke ikon tersebut.

Pengaturan Perangkat

Konfigurasi Klien

Di sini Anda dapat melakukan konfigurasi berikut ini pada perangkat Android Anda:

Di luar Waktu Kepatuhan	Batas waktu respons pengguna setelah tindakan penegakan diterapkan.
Tindakan penegakan setelah batas waktu kepatuhan	Tindakan penegakan ketika pengguna tidak melakukan tindakan yang mengarah ke status perangkat yang sesuai
Frekuensi Pengumpulan Data	Frekuensi pengumpulan informasi perangkat/GPS yang akan dikumpulkan
Frekuensi Detak Jantung Perangkat	Interval di mana perangkat harus menghubungi Server AppTec360 Min. 1 menit Max. 24 jam
Mengaktifkan Pembaruan Lokasi	Jika diaktifkan, perangkat akan mengirimkan pembaruan lokasi ke Server AppTec360
Waktu Pembaruan Lokasi	Menentukan dalam interval waktu berapa perangkat mengirimkan pembaruan lokasi ke AppTec360
Gunakan Akurasi Lokasi Google untuk Pembaruan Lokasi	Jika diaktifkan, lokasi jaringan akan digunakan untuk pembaruan lokasi (jika ini dinonaktifkan pada "Pembatasan", maka pengaturan ini tidak akan memengaruhi apa pun)
Gunakan Lokasi GPS untuk Pembaruan Lokasi	Jika diaktifkan, GPS akan digunakan untuk pembaruan lokasi
Izinkan Lokasi Tiruan (Palsu)	Memungkinkan pemalsuan informasi lokasi melalui aplikasi pihak ketiga
Tindakan Kehilangan Koneksi	Jika diaktifkan, Anda dapat menentukan tindakan jika perangkat tidak mendapatkan koneksi ke server MDM dalam interval detak jantung. Misalnya, jika perangkat memiliki waktu detak jantung 5 menit, perangkat akan tersambung ke server pada pukul 10:35 pagi. Setelah itu perangkat meninggalkan jangkauan Wi-Fi. Detak jantung berikutnya pada pukul 10:40 pagi akan gagal, dan tindakan yang ditentukan akan dieksekusi.
Tindakan	Tindakan yang harus diambil, segera setelah perangkat menjadi tidak sesuai.

	• Perangkat Kunci = perangkat kunci • Wipe Device (Hapus Perangkat) = perangkat akan dikembalikan ke pengaturan pabrik • Wipe Device & SD Card = perangkat akan dikembalikan ke pengaturan pabrik dan penyimpanan SD Card akan dihapus
Ambang batas	Anda dapat menentukan ambang batas Detak Jantung yang gagal yang diperlukan untuk memicu tindakan yang ditentukan.

Mode Penegakan Kebijakan	Default:	Pengguna akan diminta secara berkala untuk melakukan tindakan yang belum diselesaikan
	Penegakan Kebijakan yang Malas:	Pengguna tidak akan pernah diminta untuk menjalankan tindakan yang belum selesai. Semua tindakan terbuka akan ditampilkan di Klien AppTec360
	Penegakan Kebijakan yang Agresif:	Pengguna akan diminta tanpa henti untuk melakukan tindakan yang luar biasa
Kunci Versi AppTec360	Jika diaktifkan, kode versi untuk Klien MDM AppTec360 dapat ditentukan. Klien AppTec360 hanya akan memperbarui ke versi yang ditentukan. Versi yang lebih baru akan diabaikan. Penurunan versi TIDAK dimungkinkan.	
Kode Versi	Kode versi untuk Klien MDM AppTec360 yang akan dikunci.	
Nonaktifkan Pemberitahuan AppTec360	Jika dinonaktifkan, Klien AppTec360 tidak akan menampilkan Pemberitahuan di Bilah Pemberitahuan. Dengan demikian pengguna dapat menutup klien AppTec360 melalui task manager. Jika klien AppTec360 ditutup, beberapa fitur termasuk Mode Kios dan Daftar Hitam/Putih Aplikasi tidak akan berfungsi dengan baik. Perangkat Samsung menawarkan mekanisme perlindungan untuk Klien AppTec360. Notifikasi dinonaktifkan secara default pada perangkat Samsung yang mendukung API KNOX. Pemberitahuan tidak boleh dinonaktifkan pada perangkat dengan Android 8.0 atau lebih tinggi.	

Wallpaper

Mengatur Wallpaper khusus	Mengaktifkan/menonaktifkan wallpaper khusus
Wallpaper	Mengatur mode wallpaper untuk menggunakan kode warna atau gambar
Tentukan Warna	Tentukan warna latar belakang sebagai nilai heksa, misalnya #000000 untuk hitam atau #ffffff sebagai putih
Mengatur Gambar sebagai Wallpaper	Unggah file gambar yang ingin Anda gunakan sebagai wallpaper

Manajemen Aset (hanya pada tingkat perangkat)

Info Perangkat

Model	Penunjukan model perangkat
Sistem Operasi	OS
Versi OS	Versi OS
Nomor Seri	Nomor seri
Nama Perangkat	Nama perangkat
Status Baterai	Status baterai
Memori Bebas / Total	Memori bebas / Total memori
Samsung Aman	Antarmuka Samsung SAFE, diperlukan untuk berbagai opsi pengaturan
Tersedia Kartu SD	Tersedia Kartu SD
Kartu SD Ditiru	Kartu SD ditiru
Kartu SD Dapat Dilepas	Kartu SD dapat dilepas
Memori Bebas SD / Total Memori	Memori SD Bebas / Total Kartu SD

Wi-Fi

Alamat IP	Alamat IP perangkat
MAC WiFi	Alamat MAC WiFi

Seluler

Status	Status (kartu SIM terpasang)
Nomor Telepon	Nomor Telepon
Roaming (Suara / Data)	Roaming untuk suara / data
Status Roaming	Status roaming saat ini
Alamat IP	Alamat IP
Operator/Pengangkut	Operator/Pengangkut
Teknologi Seluler	Teknologi Seluler
IMEI	Nomor IMEI
ICCID	Ini adalah ID untuk kartu SIM, yang sering kali juga merupakan Smartcard atau Kartu Sirkuit Terpadu (ICC)
IMSI	Identitas Pelanggan Seluler Internasional (IMSI) menyediakan identifikasi yang pasti bagi pengguna jaringan seluler GSM dan UMTS IMSI terdiri dari maksimum 15 digit dan dikonfigurasikan dengan cara berikut: • Kode Negara Seluler (Mobile Country Code (MCC)), 3 digit • Kode Jaringan Seluler (MNC), 2 atau 3 digit • Nomor Identifikasi Pelanggan Seluler (MSIN), 1-10 digit
PKS/MNC saat ini	Lihat "SIM MCC/MNC"
SIM PKS / MNC	Kode Negara Seluler adalah pengidentifikasi negara yang ditetapkan oleh ITU sesuai Standar E.212. Kode ini berfungsi bersama dengan Kode Jaringan Seluler (Mobile Network Code/MNC) untuk identifikasi jaringan seluler. Berarti negara/Kode Jaringan Seluler kartu SIM. Jika Anda roaming ke jaringan seluler lain, maka secara logika, "MCC/MNC saat ini" dan "MCC/MNC SIM", akan berbeda.

Bluetooth

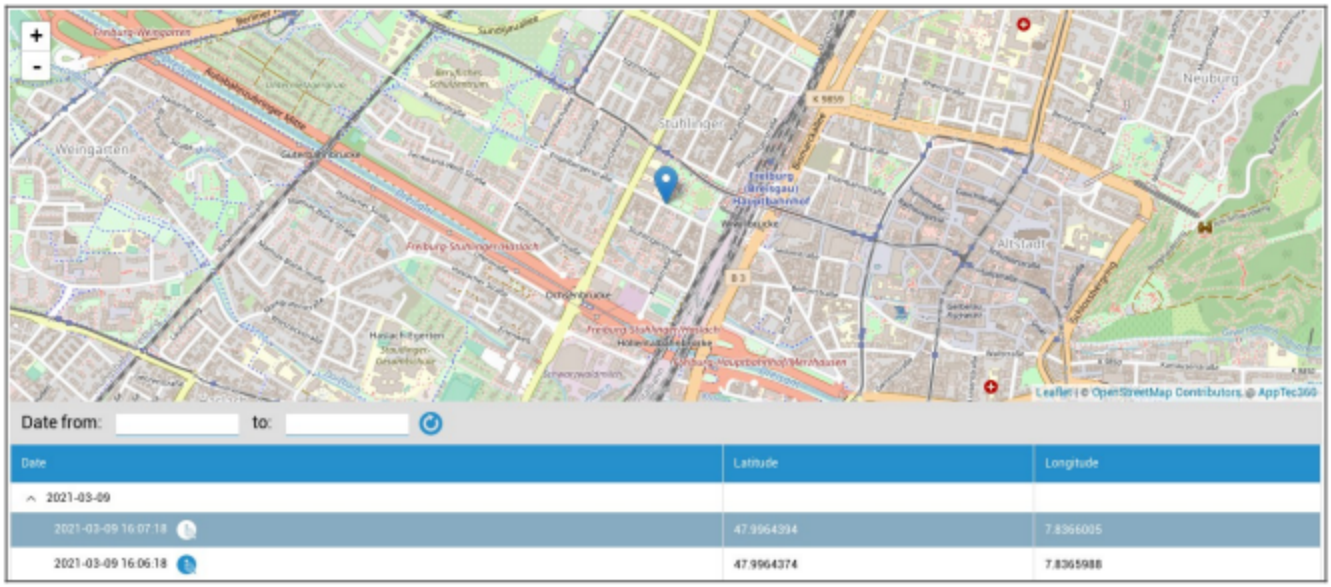
Bluetooth MAC	Alamat MAC Bluetooth

Manajemen Keamanan

Anti Pencurian (hanya pada tingkat perangkat)

Informasi GPS (hanya pada tingkat perangkat)

Di sini Anda dapat menetapkan lokasi perangkat saat ini/terakhir. Pelokalan dapat dilindungi dengan satu atau bahkan dua kata sandi - Lihat: Pengaturan Umum - Privasi - Akses GPS



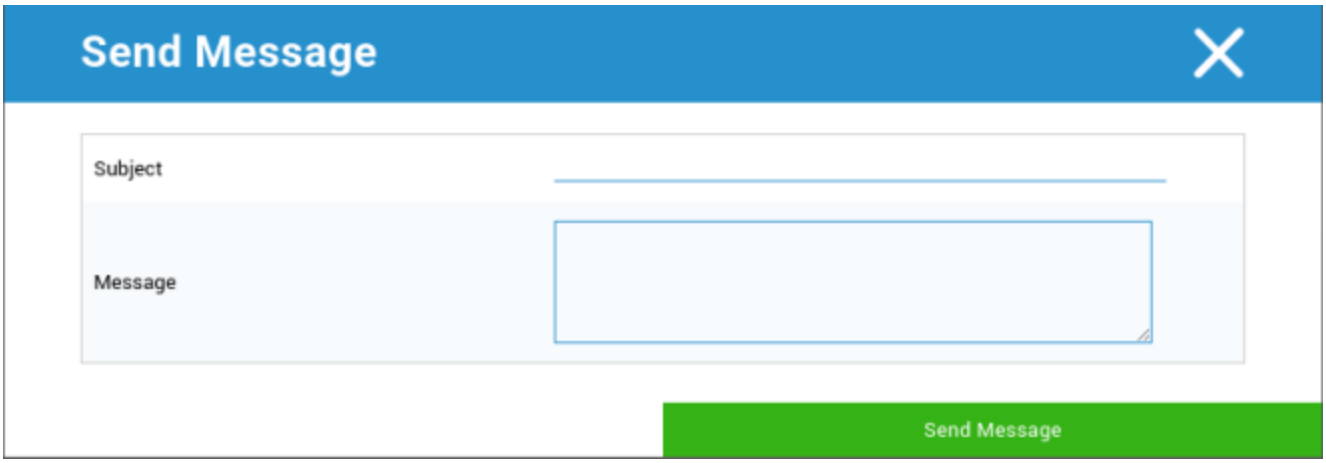
Hapus & Kunci (hanya pada tingkat perangkat)

Di bawah "Wipe & Lock", Anda dapat melakukan tiga tindakan berikut ini:

Penghapusan Penuh	Perangkat dipulihkan kembali ke pengaturan pabrik (data perusahaan dan data pribadi dihapus)
Penghapusan Perusahaan	Hanya data perusahaan yang dihapus dari perangkat pengguna akhir (semua aplikasi, data, dll. yang disediakan oleh AppTec360)
Layar Kunci	Kunci layar diaktifkan, cukup untuk membuka kunci perangkat dengan kata sandi/PIN perangkat

Pesan (hanya pada tingkat perangkat)

Di sini Anda dapat mengisi subjek dan pesan, lalu mengirimkannya ke perangkat pengguna akhir.



Konfigurasi Keamanan

Kode Sandi Perangkat

Di bawah "Kode Sandi" Anda dapat mengamanatkan kata sandi perangkat, opsi pengaturan berikut tersedia untuk Anda

Panjang kata sandi minimum	Menetapkan, jumlah minimum simbol yang harus dimiliki kata sandi	
Kualitas kata sandi	Tidak ditentukan	Kebijakan ini tidak memiliki persyaratan untuk kata sandi.
	Biometrik Lemah	Kebijakan ini memungkinkan teknologi pengenalan biometrik dengan keamanan rendah. Hal ini menyiratkan teknologi yang dapat mengenali identitas seseorang hingga sekitar 3 digit PIN (deteksi palsu kurang dari 1 dari 1.000).
	Sesuatu.	Kebijakan ini membutuhkan semacam kata sandi atau pola yang harus ditetapkan, tetapi tidak memberlakukan aturan tertentu.
	Abjad	Pengguna harus memasukkan kata sandi yang mengandung setidaknya karakter alfabet (atau simbol lainnya).
	Alfanumerik	Pengguna harus memasukkan kata sandi yang mengandung setidaknya kedua karakter tersebut, yaitu karakter numerik dan abjad (atau simbol lainnya).
	Kompleks	Pengguna harus memasukkan kata sandi yang setidaknya terdiri dari sebuah huruf, angka dan simbol khusus, secara default. Dengan kualitas kata sandi ini, kata sandi dapat dibatasi untuk mengandung berbagai rangkaian karakter, seperti setidaknya huruf besar, dll.
Panjang kata sandi minimum	Tetapkan jumlah karakter yang diperlukan untuk kata sandi. Misalnya, Anda dapat mewajibkan PIN atau kata sandi memiliki setidaknya enam karakter.	
Digit numerik minimum yang diperlukan dalam kata sandi	Digit numerik minimum yang diperlukan dalam kata sandi	
Huruf kecil minimum yang diperlukan dalam kata sandi	Huruf kecil minimum yang diperlukan dalam kata sandi	

Huruf besar minimum yang diperlukan dalam kata sandi	Huruf besar minimum yang diperlukan dalam kata sandi
Karakter non-huruf minimum yang diperlukan dalam kata sandi	Karakter non-huruf minimum yang diperlukan dalam kata sandi
Simbol minimum yang diperlukan dalam kata sandi	Simbol minimum yang diperlukan dalam kata sandi

Kunci waktu tidak aktif maksimum	Ketidakaktifan pengguna maksimum hingga kunci waktu
Batas waktu kedaluwarsa kata sandi	Menetapkan, setelah interval waktu mana kata sandi kedaluwarsa dan kata sandi baru harus dikeluarkan
Pembatasan riwayat kata sandi	Jumlah kata sandi yang pernah digunakan sebelumnya yang tidak diizinkan
Percobaan kata sandi maksimum yang gagal	Menetapkan, seberapa sering kata sandi dapat dimasukkan secara tidak benar, sebelum penghapusan perangkat secara menyeluruh akan dilakukan
Izinkan Otentikasi Biometrik	Memungkinkan autentikasi melalui sidik jari atau pemindaian iris mata. Hanya untuk Samsung KNOX 2.1 dan yang lebih tinggi

Anti Virus

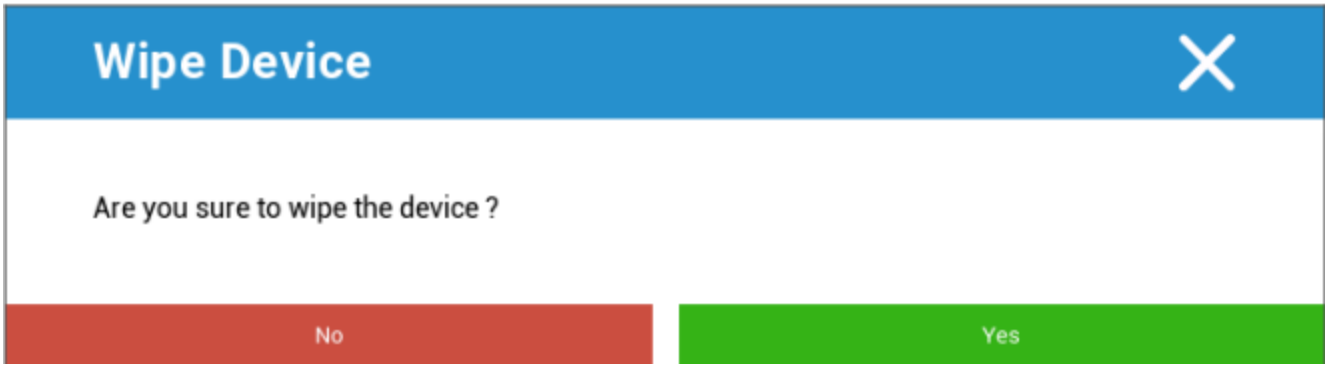
Pemindaian Otomatis	Mengaktifkan pemindaian otomatis secara berkala
Interval Pemindaian	Interval untuk pemeriksaan (Cepat / Penuh)
Pemindaian Otomatis Penuh	Mengaktifkan pemindaian otomatis penuh
Pembaruan Otomatis	Mengaktifkan pembaruan otomatis
Perbarui Interval Pemeriksaan	Seberapa sering aplikasi dan basis datanya harus diperbarui (virus/kode yang rusak)
Perlindungan Aplikasi	Mengaktifkan pemindaian aplikasi otomatis
Perlindungan Kartu SD	Mengaktifkan pemindaian Kartu SD otomatis
Pembaruan Khusus Wi-Fi	Ketika diaktifkan, pembaruan hanya akan diterapkan ketika perangkat berhasil tersambung ke jaringan Wi-Fi

Akhir Masa Pakai (hanya pada tingkat perangkat)

Menghapus (hanya pada tingkat perangkat)

Di bawah "Hapus", Anda dapat memulihkan perangkat ke pengaturan pabrik. Di sini, data perusahaan dan data pribadi akan dihapus pada perangkat pengguna akhir.

Dengan klik pada "Simbol Minus", Anda akan menerima pesan berikut ini:



Dengan "Ya", Anda dapat melakukan penghapusan.

Di bawah "Hapus Laporan", item berikut ini dapat ditampilkan

Dihapus oleh	Riwayat siapa yang melakukan penghapusan
Tanggal	Tanggal
Status	Status (mis. jika Penghapusan berhasil dilakukan)

Pengaturan Pembatasan

Pembatasan

Di sini, berbagai hal dapat dibatasi dan diblokir.

Aktifkan Kamera	Izinkan penggunaan kamera	
Paksa Sinkronisasi Otomatis	Pada	Sinkronisasi diaktifkan secara permanen
	Mati	Sinkronisasi dinonaktifkan secara permanen
	Pilihan pengguna	Dipilih oleh pengguna
Paksa Bluetooth	Pada	Bluetooth diaktifkan secara permanen
	Mati	Bluetooth dinonaktifkan secara permanen
	Pilihan pengguna	Dipilih oleh pengguna
Paksa GPS	Pada	GPS diaktifkan secara permanen
	Mati	GPS dinonaktifkan secara permanen
	Pilihan pengguna	Dipilih oleh pengguna
Lokasi Jaringan Kekuatan	Pada	Pelokalan internet permanen
	Mati	Penonaktifan permanen pelokalan internet
	Pilihan pengguna	Dipilih oleh pengguna

Keamanan		
Membatalkan Lokasi Berbagi	Menentukan apakah pengguna dilarang mengaktifkan berbagi lokasi.	
Tidak Mengizinkan Boot Aman	Menentukan apakah pengguna tidak diizinkan untuk mem-boot ulang perangkat ke mode boot aman.	
Tidak Mengizinkan Pengaturan Ulang Jaringan	Menentukan apakah pengguna dilarang mengatur ulang pengaturan jaringan dari Pengaturan.	
Membatalkan pengaturan ulang pabrik	Menentukan apakah pengguna dilarang mengatur ulang perangkat.	
Mengaktifkan ADB	Memungkinkan Koneksi ke PC melalui ADB	
Nonaktifkan Pelindung Kunci	Menonaktifkan Pelindung Kunci	
Info Layar Kunci Pemilik Perangkat	Mengatur informasi pemilik perangkat yang akan ditampilkan pada layar kunci.	
Penegakan Kepatuhan	Mode Permintaan Pengguna	Pengguna akan diminta untuk melakukan tindakan yang diperlukan.
	Wadah Penguncian Mode	Sembunyikan semua aplikasi sampai semua persyaratan terpenuhi

Manajemen Aplikasi	
Izinkan Tautan Aplikasi Lintas Profil	Memungkinkan aplikasi di profil induk menangani tautan web dari profil yang dikelola.
Membatalkan Kontrol Aplikasi	Menentukan apakah pengguna dilarang memodifikasi aplikasi di Pengaturan atau peluncur.
Melarang Pemasangan Aplikasi	Menentukan apakah pengguna dilarang menginstal aplikasi.
Larang Menghapus Instalasi Aplikasi	Menentukan apakah pengguna dilarang menghapus instalasi aplikasi.
Kebijakan Izin Runtime	Menentukan bagaimana permintaan izin baru dari aplikasi akan ditangani.
Izinkan Sumber Tidak Dikenal	Jika diaktifkan, pengguna dapat memuat Aplikasi secara terpisah dengan menginstal file .apk.

Konektivitas	
Membatalkan Konfigurasi Jaringan Seluler	Menentukan apakah pengguna dilarang mengkonfigurasi jaringan seluler.
Tidak Mengizinkan Konfigurasi Penambatan	Menentukan apakah pengguna dilarang mengkonfigurasi Tethering & hotspot portabel.
Membatalkan Konfigurasi VPN	Menentukan apakah pengguna dilarang mengkonfigurasi VPN.
Nonaktifkan Konfigurasi Wifi	Menentukan apakah pengguna dilarang mengubah titik akses WiFi.
Memblokir Sinar NFC Keluar	Menentukan apakah pengguna tidak diizinkan menggunakan NFC untuk memancarkan data dari aplikasi.
Mengunci Konfigurasi WiFi	Pengaturan ini mengontrol apakah konfigurasi WiFi yang dibuat oleh aplikasi Pemilik Perangkat harus dikunci (yaitu, hanya dapat diedit atau dihapus oleh Aplikasi Pemilik Perangkat, bukan oleh aplikasi Pengaturan).
Mengaktifkan Roaming Data	Mengaktifkan Roaming Data

Bluetooth	
Nonaktifkan Bluetooth	Menentukan apakah bluetooth dilarang pada perangkat. Memerlukan Android 8.0
Melarang Berbagi Bluetooth	Menentukan apakah berbagi bluetooth keluar dilarang pada perangkat. Memerlukan Android 8.0
Nonaktifkan Konfigurasi Bluetooth	Menentukan apakah pengguna dilarang mengkonfigurasi bluetooth.

Manajemen Akun	
Melarang penambahan profil terkelola	Menentukan apakah pengguna dilarang menambahkan profil terkelola. Memerlukan Android 8.0
Melarang menambahkan Pengguna	Menentukan apakah pengguna dilarang menambahkan pengguna baru.
Tidak mengizinkan Hapus Profil Terkelola	Menentukan apakah profil terkelola dari pengguna ini dapat dihapus, selain oleh pemilik profil. Memerlukan Android 8.0
Melarang Modifikasi Akun	Menentukan apakah pengguna dilarang menambah dan menghapus akun, kecuali jika akun tersebut ditambahkan secara terprogram oleh Authenticator.

Telepon	
Melarang Panggilan Keluar	Menentukan bahwa pengguna tidak diizinkan melakukan panggilan telepon keluar.
Melarang SMS	Menentukan bahwa pengguna tidak diizinkan mengirim atau menerima pesan SMS.

Sistem	
Melarang Pembuatan Jendela	Menentukan bahwa jendela selain jendela aplikasi tidak boleh dibuat.
Membatalkan setelan Ikon Pengguna	Menentukan apakah pengguna tidak diizinkan untuk mengubah ikon mereka.
Membatalkan Pengaturan Wallpaper	Pembatasan pengguna untuk tidak dapat menetapkan wallpaper.
Nonaktifkan Bilah Status	Menonaktifkan bilah status akan memblokir notifikasi, pengaturan cepat, dan hamparan layar lainnya yang memungkinkan keluar dari perangkat sekali pakai.
Mengaktifkan Waktu Otomatis	Mengatur waktu secara otomatis.
Mengaktifkan Zona Waktu Otomatis	Mengatur zona waktu secara otomatis.
Tetap menyala saat dicolokkan	Perangkat akan tetap aktif selama terhubung ke sumber daya.

Penyimpanan	
Nonaktifkan nonaktifkan Verifikasi Aplikasi	Menentukan apakah pengguna dilarang menonaktifkan verifikasi aplikasi.
Melarang Memasang Media Fisik	Menentukan apakah pengguna dilarang memasang media eksternal fisik.
Mengaktifkan Layanan Cadangan	Layanan pencadangan mengelola semua mekanisme pencadangan dan pemulihan pada perangkat. Mengatur ini ke false (tidak benar) akan mencegah data dicadangkan atau dipulihkan. Layanan pencadangan dinonaktifkan secara default. Memerlukan Android 8.0
Mengaktifkan Penyimpanan Massal USB	Mengaktifkan penggunaan Penyimpanan Massal USB.

Keyboard	
Larang Pengisian Otomatis	Menentukan apakah pengguna tidak diizinkan menggunakan Layanan IsiOtomatis. Memerlukan Android 8.0
Larang Salin & Tempel antar Profil	Menentukan apakah yang disalin di papan klip profil ini dapat ditempelkan di profil terkait.

Suara	
Tidak Mengizinkan Penyesuaian Volume	Menentukan apakah pengguna dilarang menyesuaikan volume master.
Membolehkan Membunyikan Mikrofon	Menentukan apakah pengguna dilarang menyesuaikan volume mikrofon.
Membisukan Perangkat	Bisukan perangkat.

Manajemen Sertifikat

Di sini Anda dapat mendistribusikan Sertifikat Tepercaya dan Sertifikat Identitas ke perangkat Anda.

Android 8 atau lebih tinggi diperlukan untuk mendistribusikan Sertifikat Tepercaya dan Android 9 atau lebih tinggi diperlukan untuk mendistribusikan Sertifikat Identitas.

Dengan tanda "+", Anda dapat menambahkan beberapa sertifikat.

Sertifikat Tepercaya harus dalam format PEM.

Sertifikat Identitas harus dalam format PKCS12

Manajemen Koneksi

Wifi

Untuk pengaturan ini, lakukan pra-konfigurasi perangkat pengguna akhir, untuk akses ke Access internal
Points

Pengidentifikasi Set Layanan (SSID)	SSID untuk jaringan yang akan disambungkan
Jaringan Tersembunyi	Aktifkan, jika AP tidak menyiarkan SSID

Jenis Keamanan

Menetapkan jenis keamanan AP

WEP

Kata sandi	Kata sandi untuk AP

WPA/WPA2

Kata sandi	Kata sandi untuk AP

802.1x EAP

Metode EAP

PENYANDANG DISABILITAS	Identitas	Identitas
	Kata sandi	Kata sandi

PEAP	Protokol Otentikasi Fase 2	tidak ada	Tidak ada protokol tambahan
		MSCHAPV2	Protokol MSCHAPV2
		GTC	Protokol GTC
	Sertifikat CA	Sertifikat CA	
	Identitas	Identitas	
	Identitas Anonim	Identitas anonim	
	Kata sandi	Kata sandi	

TTLS	Protokol Otentikasi Fase 2	tidak ada	Tidak ada protokol tambahan
		PAP	Protokol PAP
		MSCHAP	Protokol MSCHAP
		MSCHAPV2	Protokol MSCHAPV2
		GTC	Protokol GTC
	Sertifikat CA	Sertifikat CA	
	Identitas	Identitas	
	Identitas Anonim	Identitas Anonim	
	Kata sandi	Kata sandi	

TLS	Sertifikat CA	Sertifikat CA
	Identitas	Identitas
	Kata sandi	Kata sandi

VPN

Nama Koneksi	Nama Koneksi VPN

Jenis VPN

VPN

Klien VPN

Klien VPN AppTec360	
Konfigurasi Gateway	Pilih Konfigurasi VPN Gateway (Lihat **Pengaturan Umum > Gateway Universal > Pengaturan VPN**)
VPN yang selalu aktif	Mengaktifkan Penguncian Asli
Aktifkan Penguncian AppTec360	Aktifkan Penguncian AppTec360

Bawaan (Hanya tersedia pada perangkat Samsung)			
Jenis Koneksi	PPTP	Server	Server
		Mengaktifkan Enkripsi PPTP	Mengaktifkan Enkripsi PPTP
	L2TP / IPSec PSK	Server	Server
		Kunci Pra-Berbagi IPSec	Kunci Pra-Berbagi IPSec
		Aktifkan Rahasia L2TP	Aktifkan Rahasia L2TP
		Rahasia L2TP	Rahasia L2TP
	IPSec XAuth PSK	Server	Server
		Pengidentifikasi IPSec	Pengidentifikasi IPSec
		Kunci Pra-Berbagi IPSec	Kunci Pra-Berbagi IPSec
Domain Pencarian DNS	Domain Pencarian DNS		
Pengaturan Pakar	Server DNS	Server DNS	
	Rute Penerusan	Rute Penerusan	

Buka VPN		
Server	Server	
Profil OpenVPN	Profil OpenVPN	
Aplikasi OpenVPN	OpenVPN untuk Android (disarankan)	
	OpenVPN Connect	
Pengaturan Pakar	Server DNS	Server DNS
	Rute Penerusan	Rute Penerusan

Samsung / Strong Swan			
Jenis Koneksi	PPTP	Server	Server
		Nama pengguna	Nama pengguna
		Kata sandi	Kata sandi
		Mengaktifkan Enkripsi PPTP	Mengaktifkan Enkripsi PPTP
	L2TP / IPSec PSK	Server	Server
		Kunci Pra-Berbagi IPSec	Kunci Pra-Berbagi IPSec
		Nama pengguna	Nama pengguna
		Kata sandi	Kata sandi
		Aktifkan Rahasia L2TP	Rahasia L2TP
	IPSec XAuth PSK	Server	Server
		Pengidentifikasi IPSec	Pengidentifikasi IPSec
		Kunci Pra-Berbagi IPSec	Kunci Pra-Berbagi IPSec
		Nama pengguna	Nama pengguna
		Kata sandi	Kata sandi
Pengaturan Pakar	Server DNS	Server DNS	
	Rute Penerusan	Rute Penerusan	

Cisco Any Connect		
Server	Server	
Mode Sertifikat	Dinonaktifkan	Dinonaktifkan
	Otomatis	Otomatis
Pengaturan Pakar	Server DNS	Server DNS
	Rute Penerusan	Rute Penerusan

VPN Per-Aplikasi

Klien VPN

Klien VPN AppTec360		
Konfigurasi Gateway	Pilih Konfigurasi VPN Gateway (Lihat **Pengaturan Umum > Gateway Universal > Pengaturan VPN**)	
Aplikasi VPN	Aplikasi VPN	
VPN yang selalu aktif	Mengaktifkan Penguncian Asli	VPN yang selalu aktif
Aktifkan Penguncian AppTec360	Aktifkan Penguncian AppTec360	

Samsung / Strong Swan			
Jenis Koneksi	PPTP	Server	Server
		Aplikasi VPN	Aplikasi VPN
		Nama pengguna	Nama pengguna
		Kata sandi	Kata sandi
		Mengaktifkan Enkripsi PPTP	Mengaktifkan Enkripsi PPTP
	L2TP / IPSec PSK	Server	Server
		Aplikasi VPN	Aplikasi VPN
		Kunci Pra-Berbagi IPSec	Kunci Pra-Berbagi IPSec
		Nama pengguna	Nama pengguna
		Kata sandi	Kata sandi
		Aktifkan Rahasia L2TP	Rahasia L2TP
	IPSec XAuth PSK	Server	Server
		Aplikasi VPN	Aplikasi VPN
		Pengidentifikasi IPSec	Pengidentifikasi IPSec
		Kunci Pra-Berbagi IPSec	Kunci Pra-Berbagi IPSec
		Nama pengguna	Nama pengguna
		Kata sandi	Kata sandi
Pengaturan Pakar	Server DNS	Server DNS	
	Rute Penerusan	Rute Penerusan	

Pembatasan

Di sini Anda dapat menetapkan pembatasan, sehubungan dengan manajemen koneksi.

Izinkan Roaming Data	Izinkan data seluler saat roaming
Paksa Roaming Data	Jika diaktifkan, roaming untuk data seluler akan diaktifkan secara permanen (tidak disarankan!) Pengaturan ini menimpa pengaturan "Izinkan Data Roaming"!
Pengaturan berikut ini hanya tersedia pada SAFE 2.x atau yang lebih tinggi	
Izinkan Panggilan Darurat Saja	Izinkan Panggilan Darurat Saja
Izinkan WiFi	Izinkan WiFi
Tingkat Keamanan Minimum Jaringan WiFi	Tingkat keamanan minimum jaringan WiFi Terbuka = semua jenis WiFi diizinkan
Melarang pengguna untuk menambahkan jaringan WiFi	Pengguna tidak boleh menambahkan jaringan WiFi sendiri Pengaturan ini hanya dapat dilakukan, jika profil WiFi ditentukan di bawah "Manajemen Koneksi"
Izinkan SMS & MMS	Semua = Semua lalu lintas SMS & MMS diperbolehkan Hanya SMS Masuk = Hanya pesan SMS masuk yang diperbolehkan Hanya SMS Keluar = Hanya pesan SMS keluar yang diperbolehkan Tidak ada = Tidak ada lalu lintas SMS / MMS yang diizinkan
Izinkan Sinkronisasi selama Roaming	Izinkan Sinkronisasi selama Roaming Aktif = diaktifkan Mati = dinonaktifkan Pilihan pengguna = pilihan pengguna
Izinkan Roaming Suara	Izinkan Roaming Suara Aktif = diaktifkan Mati = dinonaktifkan Pilihan Pengguna = pilihan pengguna
Gunakan Sistem http Server Proxy	Penggunaan server proxy HTTP, yang disediakan oleh pengaturan sistem dalam pengaturan, bergantung pada jaringan yang terhubung (WiFi atau APN)

Manajemen PIM

Pertukaran Gmail

Info: Konfigurasi ini akan diterapkan pada aplikasi Gmail. Jadi, Anda harus menyetujui dan menginstal Gmail.

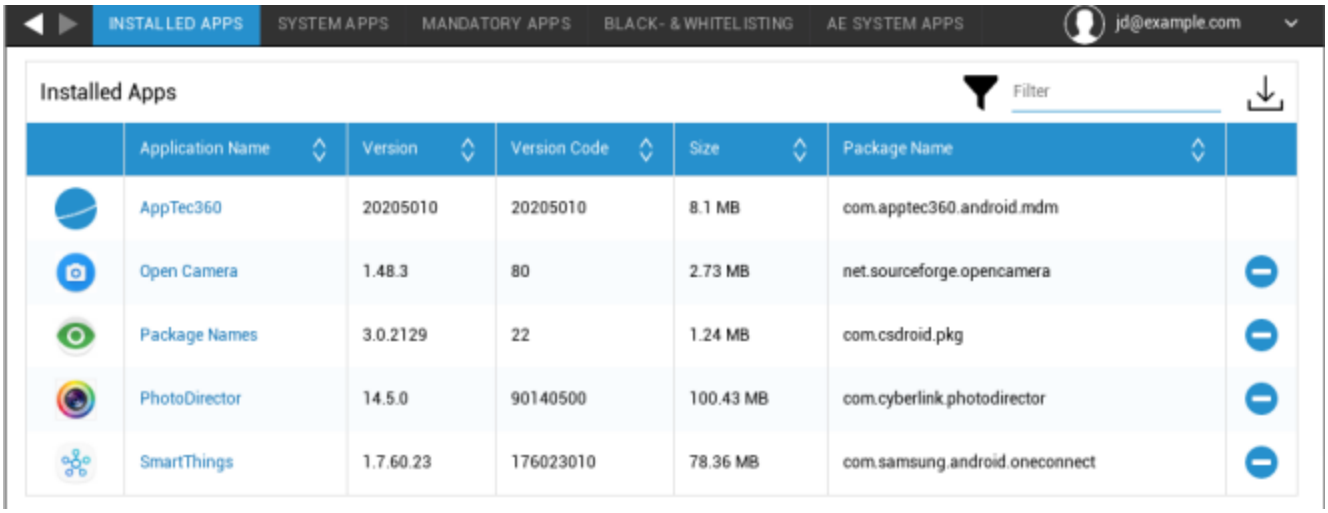
Alamat email	Alamat email pengguna yang diberikan Harap perhatikan "Placeholder", yang dapat Anda gunakan untuk bekerja dengan kredensial dan Anda tidak melakukan perubahan secara manual pada setiap perangkat Dengan sekali klik, Anda dapat menampilkannya sendiri
Nama Host Server	Alamat server dari Server Exchange Anda
Nama login	Nama Login untuk masing-masing perangkat pengguna akhir, harap perhatikan juga "Placeholder di sini
Tanda tangan	Tanda tangan dapat dilampirkan (Petunjuk: Beberapa perangkat memerlukan format HTML untuk tanda tangan)
Jumlah hari sebelumnya untuk disinkronkan	Jumlah hari, menentukan kapan email disinkronkan kembali
Pengenal Perangkat	Sebuah string yang berisi EAS DeviceID. Ini adalah bagian dari Protokol EAS dan akan digunakan dalam beberapa aplikasi
Gunakan Lapisan Soket Aman (SSL)	Gunakan koneksi SSL
Menerima semua sertifikat	Semua sertifikat diterima. Pilih opsi ini, jika Exchange Server Anda menggunakan sertifikat yang ditandatangani sendiri

Manajemen Aplikasi

Manajer Aplikasi Perusahaan

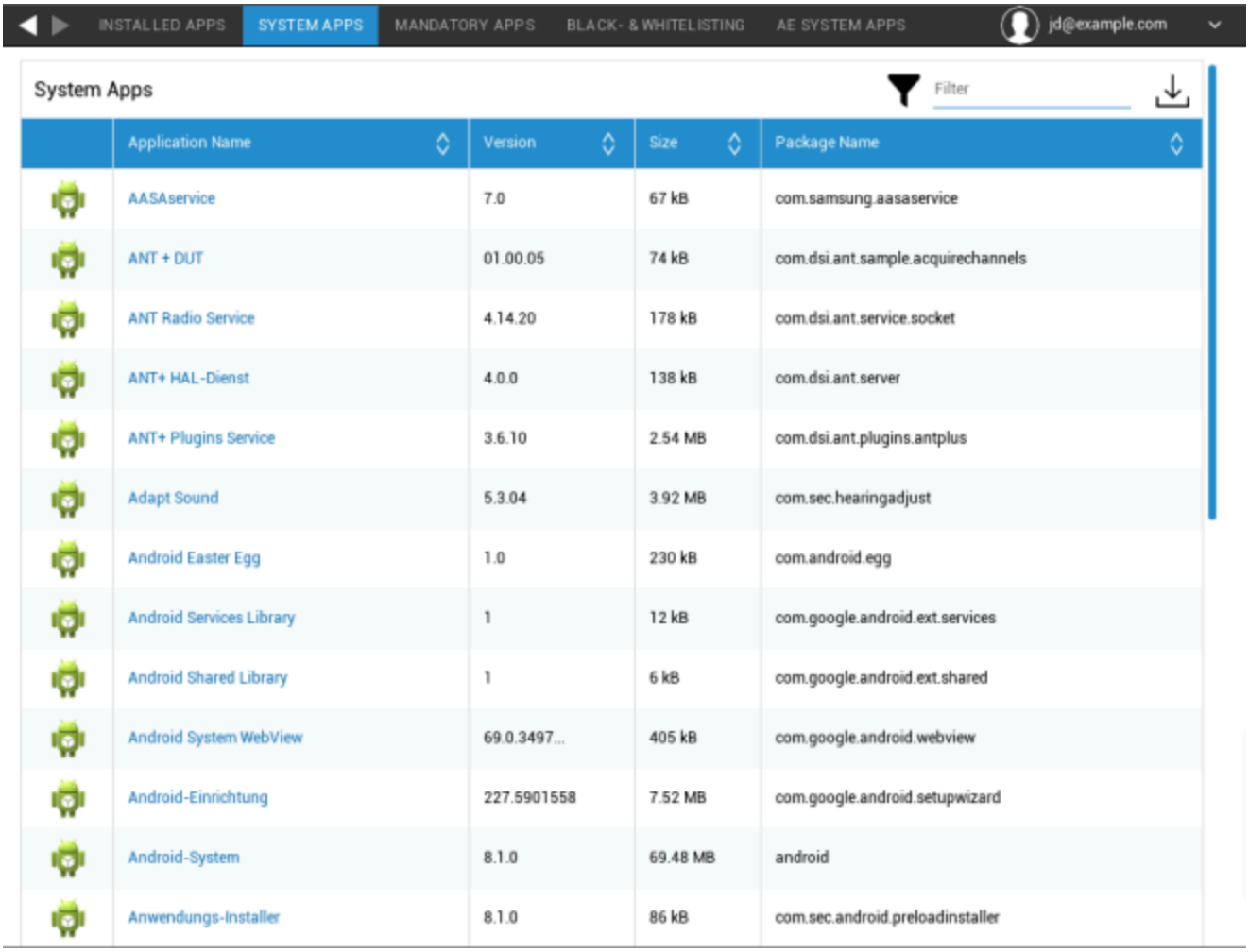
Aplikasi Terinstal (hanya pada tingkat perangkat)

Di sini semua Aplikasi yang saat ini terinstal pada perangkat pengguna akhir akan ditampilkan untuk Anda.



Aplikasi Sistem (hanya pada tingkat perangkat)

Di bawah "Aplikasi Sistem", semua aplikasi dan layanan yang telah diinstal pada perangkat pengguna akhir oleh produsen perangkat Anda akan dicantumkan untuk Anda.

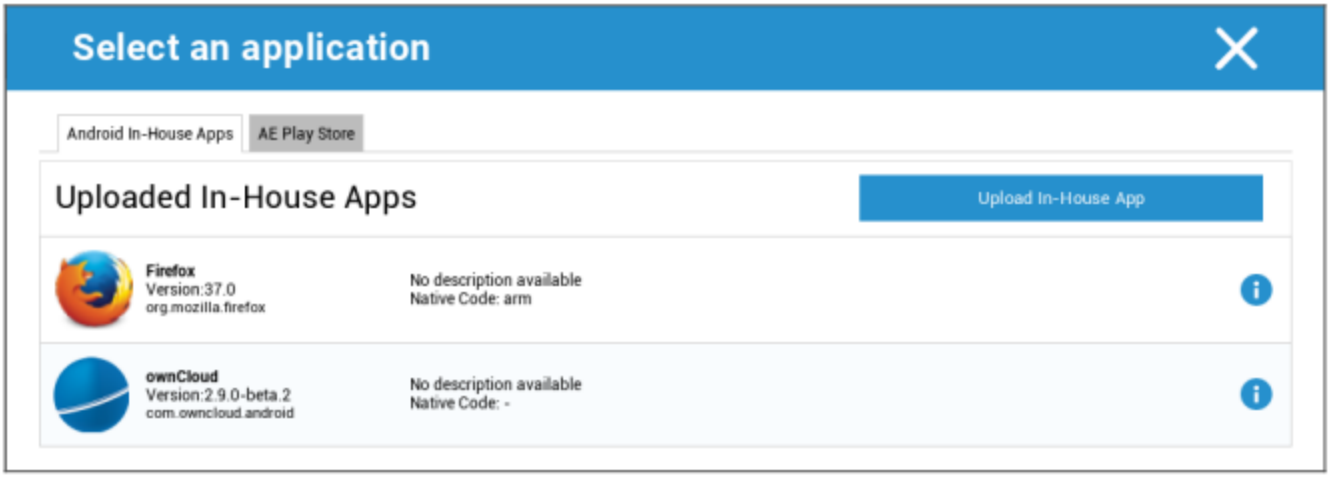


Aplikasi Wajib

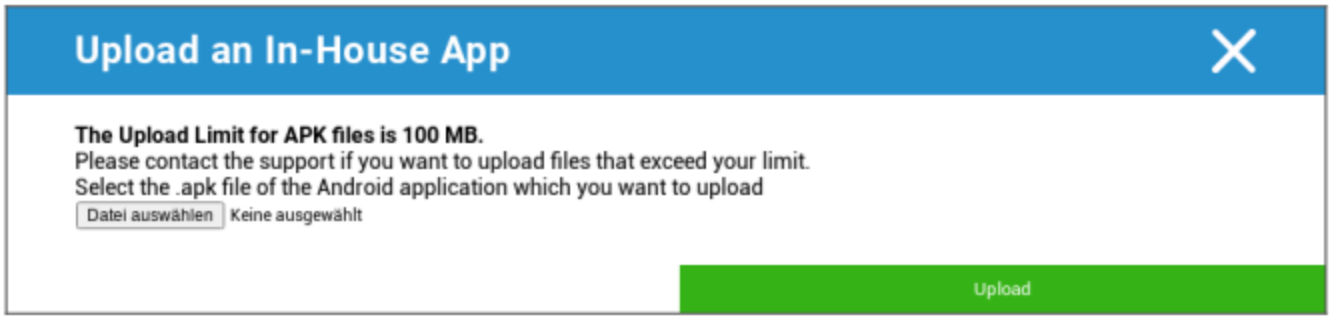
Di bawah Aplikasi Wajib, Anda dapat menetapkan aplikasi wajib yang diamanatkan. Pengguna akan terus diminta untuk menginstal aplikasi yang ditetapkan ini.

Melalui , aplikasi yang diperlukan yang diamanatkan dapat ditentukan.

Ini dapat berupa Aplikasi In-House dari "Aplikasi In-House Android", yang telah Anda unggah di Pengaturan Umum.

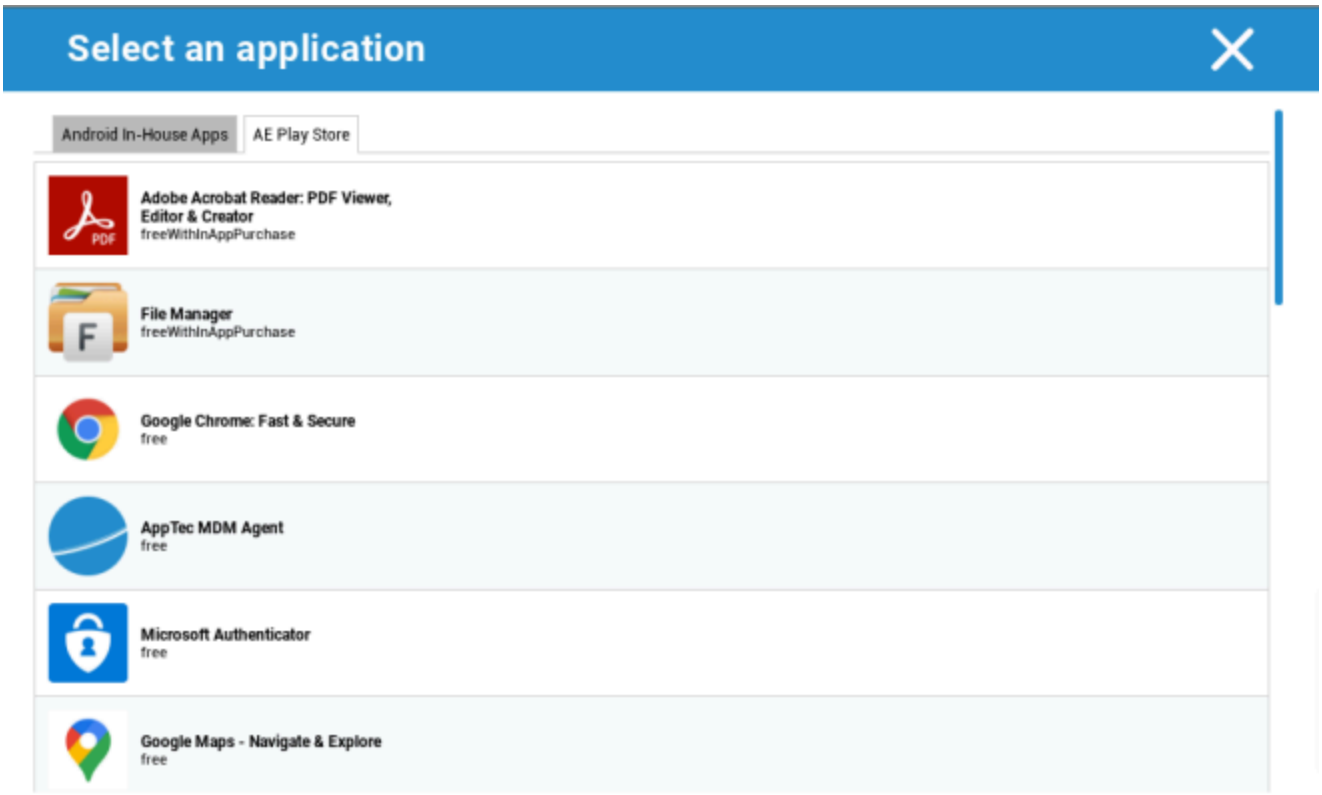


Anda juga dapat langsung memilih dan mengunggah file apk dengan "Unggah Aplikasi In-House".



Jika Anda menginstal Aplikasi In-House, Anda dapat mengaktifkan "Selalu perbarui". Jika ini diaktifkan dan Anda telah menetapkan versi yang lebih baru di DB Aplikasi In-House, aplikasi akan diperbarui pada perangkat.

Atau, bisa juga Aplikasi "AE Play Store" dari Google Work Play Store.



Hanya "Aplikasi AE Play Store" yang disetujui yang akan ditampilkan di tab ini.

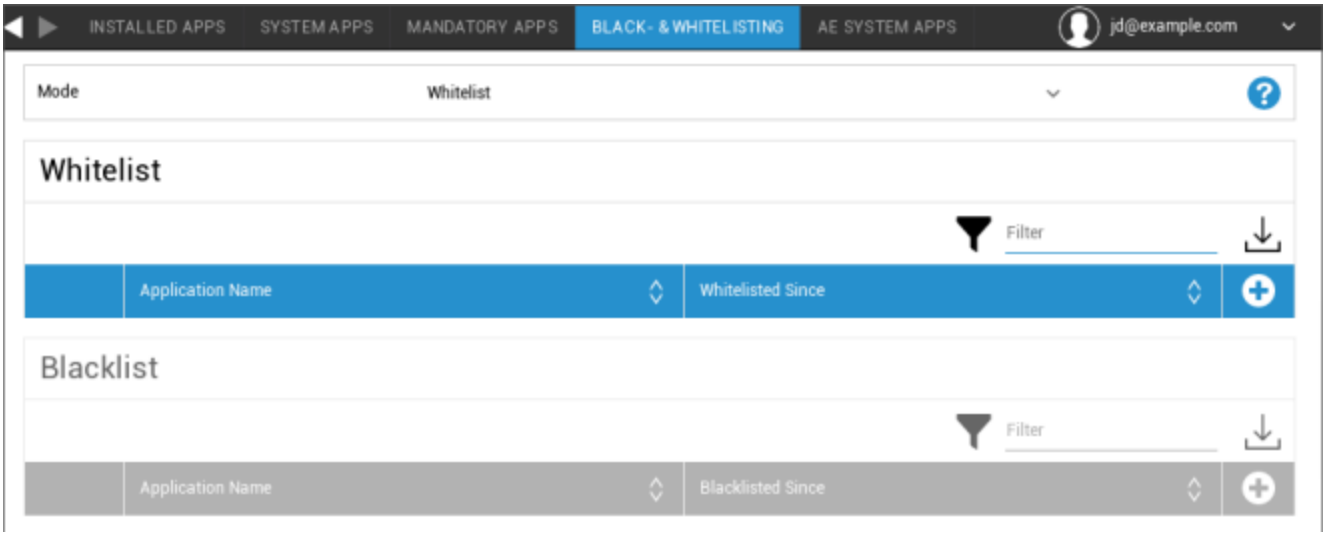
Untuk menyetujui "Aplikasi AE Play Store", silakan masuk ke "Pengaturan Umum" > "Manajemen Aplikasi" > "AE Play

Store" dan tambahkan aplikasi melalui tombol yang akan mengarahkan Anda ke tab "Play Store Apps" (atau Anda
dapat langsung membuka tab "Play Store Apps").

Pada tab "Aplikasi Play Store" Anda dapat mencari aplikasi. Ketika Anda mengeklik sebuah aplikasi, halaman aplikasi akan terbuka
dan di sini Anda dapat menyetujui aplikasi tersebut dengan mengeklik "Setujui".

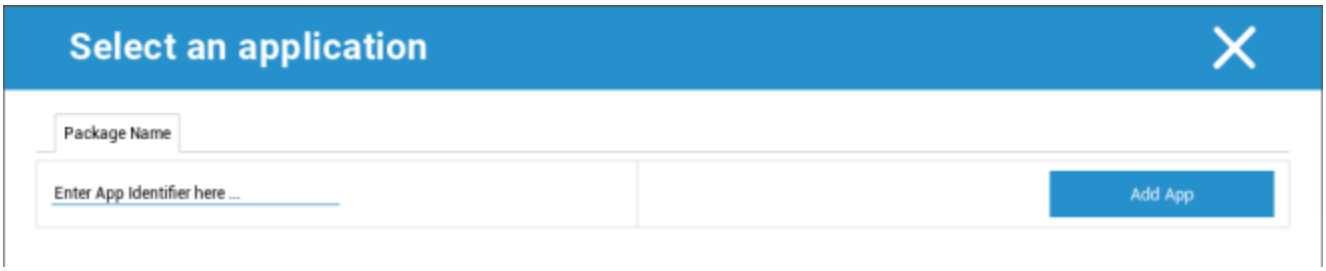
Daftar Hitam & Putih

Di bawah "Daftar Hitam & Putih", Anda dapat memilih antara Mode "Daftar Putih" dan Mode "Daftar Hitam".



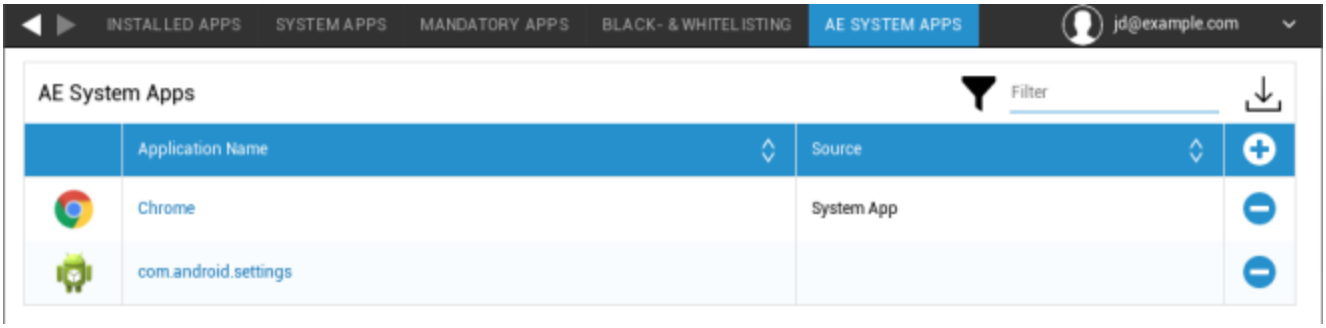
Daftar putih	Hanya aplikasi dan layanan yang ditambahkan ke dalam daftar yang dapat diinstal pada perangkat pengguna akhir. Jika ini sudah diinstal sebelumnya di perangkat pengguna akhir, maka akan diaktifkan dan diatur, sehingga pengguna dapat menjalankannya.
	Semua aplikasi lain yang tidak ditambahkan ke dalam daftar tidak dapat diinstal pada perangkat pengguna akhir. Jika aplikasi ini sudah diinstal sebelumnya di perangkat pengguna akhir, aplikasi ini akan dinonaktifkan dan diatur, sehingga pengguna tidak dapat menjalankannya.
Daftar hitam	Aplikasi dan layanan yang ditambahkan ke dalam daftar tidak dapat diinstal pada perangkat pengguna akhir. Jika sudah diinstal sebelumnya pada perangkat pengguna akhir, aplikasi dan layanan tersebut akan dinonaktifkan dan diatur, sehingga pengguna tidak dapat menjalankannya.
	Semua aplikasi lain yang tidak ditambahkan ke dalam daftar dapat diinstal pada perangkat pengguna akhir. Jika aplikasi-aplikasi ini sudah terinstal di perangkat pengguna akhir, aplikasi-aplikasi ini akan diaktifkan dan diatur, sehingga pengguna dapat menjalankannya.

Melalui , Anda menambahkan aplikasi atau layanan tambahan ke daftar yang sedang digunakan. Melalui , Anda menambahkan aplikasi atau layanan tambahan ke daftar yang sedang tidak aktif. Anda dapat menentukan "Packagename":

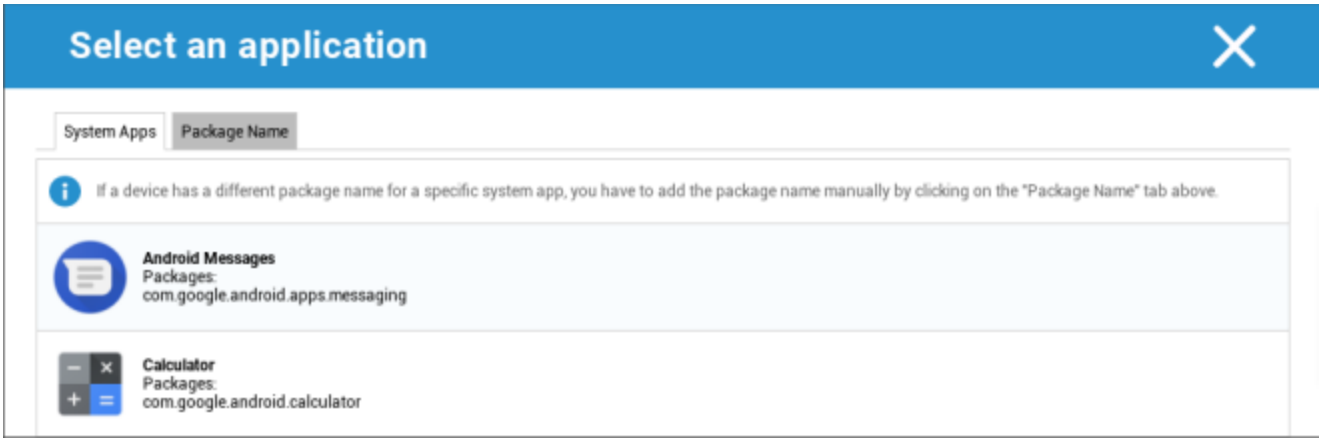

Select an application
Package Name
Enter App Identifier here ...
Add App

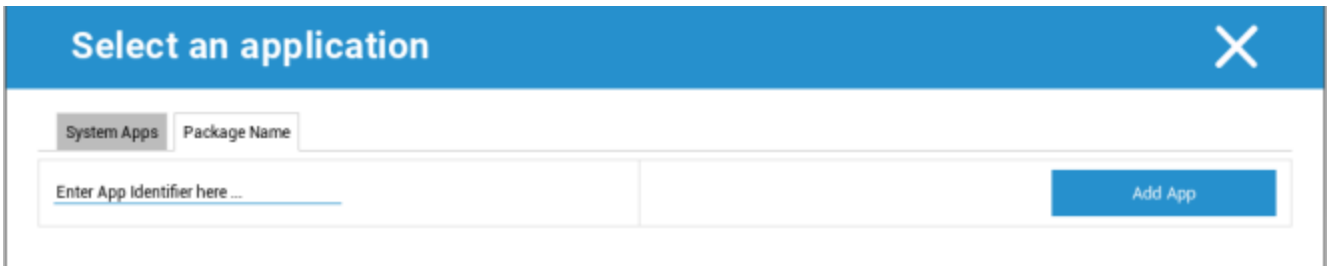
Aplikasi Sistem AE

Di sini Anda dapat menentukan daftar yang berisi aplikasi sistem tertentu yang harus diaktifkan pada perangkat.



Jika Anda mengklik tombol tersebut, Anda dapat memilih dari daftar aplikasi sistem yang disediakan oleh Google atau langsung memasukkan nama paket aplikasi sistem yang harus diaktifkan.





Harap diingat bahwa aplikasi sistem dalam daftar yang disediakan oleh Google hanyalah aplikasi yang dapat menjadi aplikasi sistem, tetapi tidak harus menjadi aplikasi sistem pada perangkat Anda.

Namun, daftar ini hanya memengaruhi aplikasi yang sudah terinstal sebelumnya.

Menambahkan aplikasi yang tidak terinstal sebelumnya pada perangkat Anda tidak akan memengaruhi perangkat Anda, terlepas dari apakah aplikasi tersebut berasal dari daftar yang disediakan oleh Google atau nama paket aplikasi yang dimasukkan secara langsung.

Pembatasan & Pengaturan

Pengaturan Manajemen Aplikasi

Di sini Anda dapat mengonfigurasi perilaku perangkat terkait pembaruan aplikasi.

Perbarui Frekuensi Pemeriksaan	Tentukan dalam interval berapa lama Klien AppTec360 akan mencari pembaruan aplikasi. Nilai default adalah 24 jam.
Ambang Batas Wi-Fi	Aplikasi yang lebih besar dari ukuran yang ditentukan akan diunduh melalui Wi-Fi. Jika "Hanya Wi-Fi" dipilih, semua aplikasi akan diunduh melalui Wi-Fi.

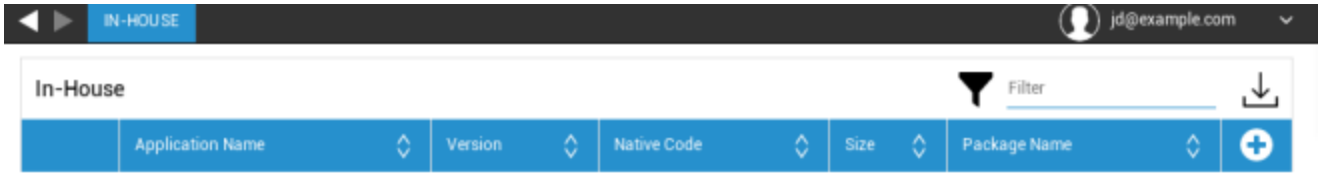
Toko Aplikasi Perusahaan

In-House

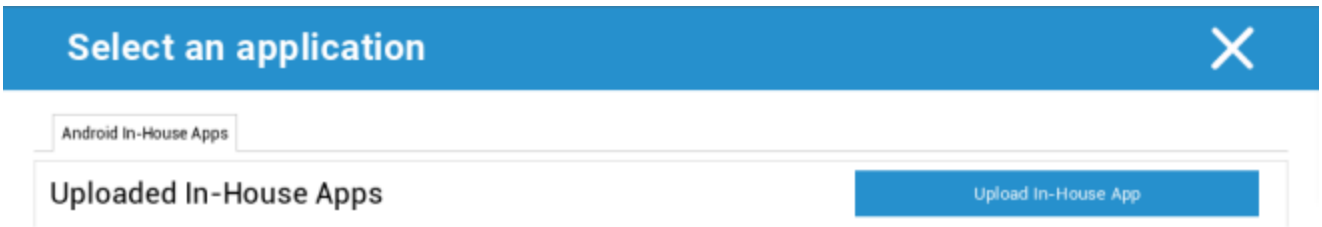
Di bawah poin "In-House", Anda dapat mengunggah dan mendistribusikan aplikasi yang dikembangkan secara internal.

Dengan simbol tersebut, Anda dapat mendistribusikan Aplikasi In-House tambahan.

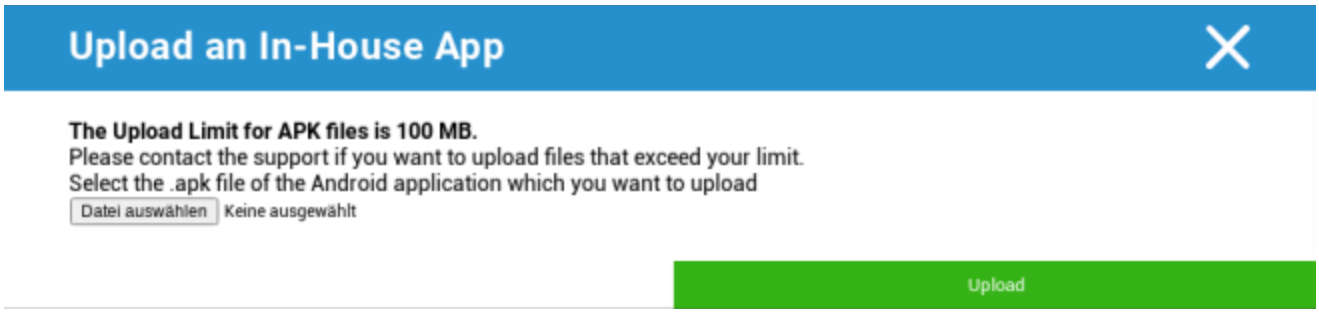
Jika Anda menginstal Aplikasi In-House, Anda dapat mengaktifkan "Selalu perbarui". Jika ini diaktifkan dan Anda telah menetapkan versi yang lebih baru di DB Aplikasi In-House, aplikasi akan diperbarui pada perangkat.



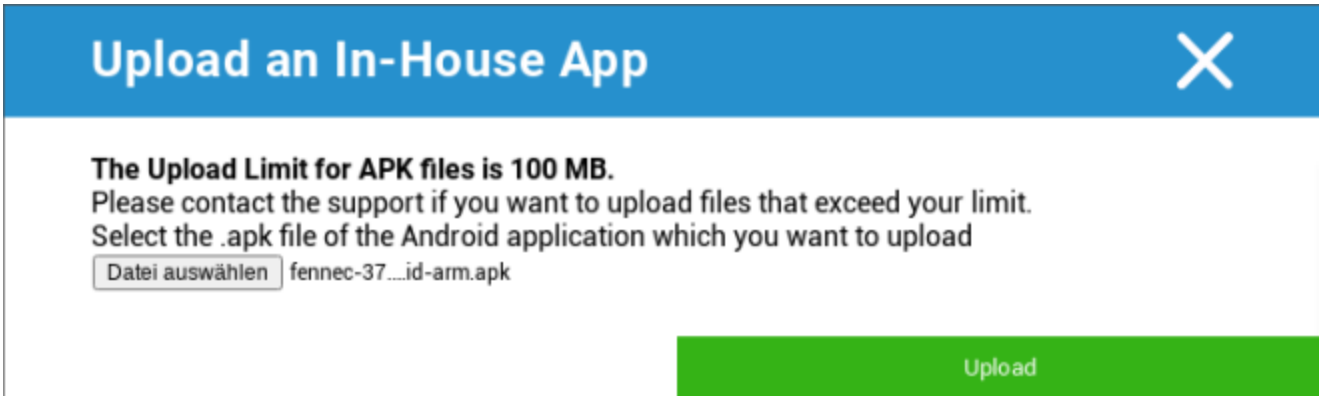
Jika Anda belum mendistribusikan Aplikasi In-House, Anda akan menerima ikhtisar berikut:



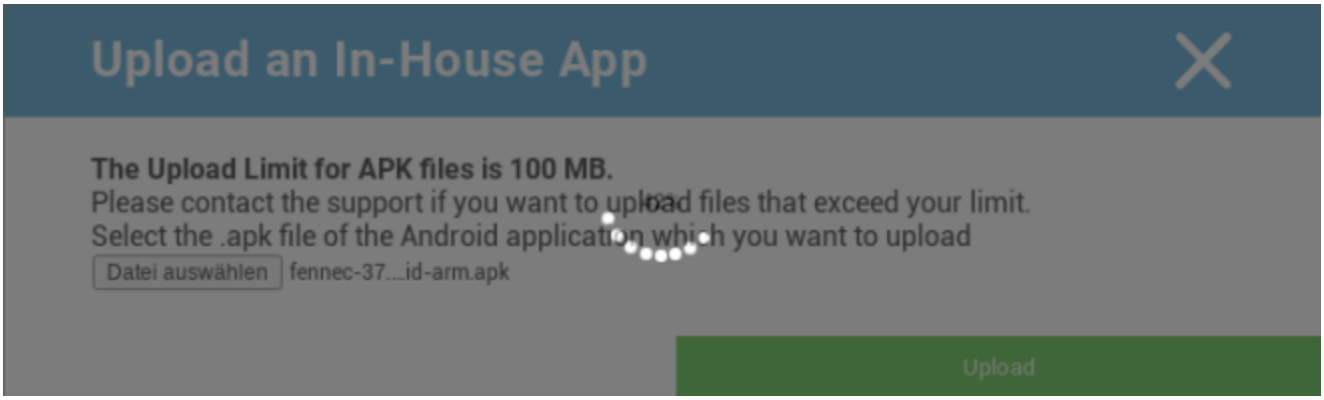
Untuk melakukan ini, klik "Unggah Aplikasi In-House", Anda akan menerima gambaran umum berikut:



Sekarang, pilih dengan "Cari..." file .apk dan kemudian klik "Unggah".



Aplikasi Anda sekarang akan diunggah, di tengah lingkaran Anda akan melihat indikator persentase, yang menunjukkan berapa banyak aplikasi Anda yang telah diunggah.



Jika pengunggahan Aplikasi In-House Anda telah berhasil, Anda dapat menemukan aplikasi yang diunggah
di Katalog Aplikasi Anda.

Pengguna sekarang memiliki opsi untuk melihat dan menginstal aplikasi ini di AppTec360 Store di perangkat pengguna akhir
, di bawah kategori "In-House".

Karena ini tidak melibatkan Aplikasi Google PlayStore, pengguna tidak memerlukan ID Google yang tersimpan di perangkat pengguna akhir masing-masing.

Perusahaan Play Store

AE Play Store

Di sini Anda dapat menambahkan Aplikasi ke Android Enterprise Playstore. Harap diperhatikan bahwa Anda harus menyetujui
Aplikasi dengan Akun Administrator AE Anda sebelum dapat menambahkannya.

Untuk menyetujui aplikasi, lihat petunjuk di Aplikasi Wajib.

Mode Kios & Peluncur

Mode Kios

Mode Kios memungkinkan Anda untuk menentukan terlebih dahulu aplikasi atau URL. Kemudian secara eksklusif dapat
menjalankan/mengunjungi aplikasi dan atau URL ini.

Demikian juga, berbagai tombol perangkat keras dapat dinonaktifkan dalam Mode Kios yang beragam.

Mulai Otomatis	Secara otomatis memulai Mode Kios, segera setelah profil mencapai perangkat pengguna akhir
Mode Kios Terjadwal?	Anda dapat merencanakan waktu untuk Mode Kios, yang kemudian akan dimulai dan diakhiri secara otomatis, pada waktu yang Anda tentukan
Waktu Mulai	Waktu mulai
Waktu dalam menit	Waktu dalam menit, setelah itu Mode Kios akan berakhir lagi

Jenis Aplikasi

Aplikasi Tunggal	Jika Anda ingin memulai Aplikasi dalam Mode Kios, pilih Paket" di bawah "Jenis Aplikasi"
Aplikasi Kios	Klik di sini, untuk memilih aplikasi yang harus dimulai dalam Mode Kios Anda akan menemukan gambaran umum Manajemen Aplikasi yang biasa Anda dapat memilih antara "Google Play Store", "Aplikasi In-House Android", dan "Packagename"

Jenis Aplikasi

URL	Jika Anda ingin meluncurkan URL dalam Mode Kios, pilih "URL" di bawah "Jenis Aplikasi" Kemudian tentukan alamat URL yang Anda inginkan
Menghapus browser setelah tidak aktif	Di sini Anda dapat menentukan interval waktu dalam menit, setelah itu Mode Kios harus diluncurkan kembali
Menghapus Tembolok dan Cookie Web	Jika Anda mengaktifkan fungsi ini, maka setelah memulai ulang Mode Kios, Cache Web (cookie dan gambar yang di-cache) akan dihapus
Kebijakan Asal yang Sama	Jika fungsi ini aktif, maka pengguna hanya dapat menjelajahi subhalaman dari URL yang ditentukan Misalnya, Anda menetapkan URL berikut:www.mypage.com Kemudian, pengguna dapat berselancar di: www.mypage.com/subpage
URL yang masuk daftar putih	Di sini Anda dapat mengelola Daftar Putih, semua URL ini diizinkan Maksimum 1 URL per baris URL harus dimulai dengan http:/ atau https://
URL yang masuk daftar hitam	Di sini Anda dapat mengelola Daftar Hitam, semua URL ini tidak diizinkan Maksimum 1 URL per baris URL harus dimulai dengan http:/ atau https://
Orientasi Layar	Pengaturan ini berkaitan dengan penyesuaian layar Otomatis = otomatis Potret = format vertikal Lanskap = mode lanskap

Multi Aplikasi	Jika Anda memilih Mode Kios "Multi Aplikasi", penggunaan Peluncur AppTec360 akan diberlakukan.
Aplikasi	Aplikasi: Pilih Playstore atau Aplikasi In-House sebagai Aplikasi Kios. Anda juga dapat memasukkan nama paket. Aplikasi Kios yang dipilih harus diinstal pada perangkat. Ingatlah untuk mengatur Aplikasi Kios sebagai wajib. Pintasan pada Layar Beranda: Jika diatur ke "On", pintasan pada homescreen akan dibuat. Jika diatur ke "Nonaktif", Aplikasi akan tetap muncul di Daftar Aplikasi.

Kata Sandi Keluar Diaktifkan	Jika Anda mengaktifkan fungsi ini, maka pengguna dapat mengakhiri Mode Kios dengan kata sandi yang telah Anda tentukan sebelumnya
Keluar dari Kata Sandi	Ini adalah kata sandi yang telah Anda tentukan sebelumnya
Bilah Status Tutup Otomatis	Jika diaktifkan, Status Bar akan secara otomatis ditutup. Dengan opsi tersebut, pengguna dapat melihat informasi di Status Bar, tetapi tidak dapat mengakses fungsinya
Nonaktifkan Bilah Status	Bilah Status berisi Pemberitahuan, Pintasan, dan Informasi. Hanya tersedia untuk perangkat Samsung dengan SAFE 4.0 atau yang lebih tinggi.
Menonaktifkan Tombol Volume	Menonaktifkan tombol volume (hanya tersedia pada perangkat Samsung dengan SAFE 3.0 atau lebih tinggi)
Nonaktifkan Sakelar Hidup / Mati	Nonaktifkan sakelar Nyala/Mati (hanya tersedia pada perangkat Samsung dengan SAFE 3.0 atau lebih tinggi)
Nonaktifkan Tombol Beranda	Nonaktifkan tombol Beranda. Jika fungsi ini telah diaktifkan, maka Mode Kios hanya dapat diakhiri di Konsol AppTec360 (hanya tersedia pada perangkat Samsung dengan SAFE 3.0 atau lebih tinggi)
Menonaktifkan Bilah Navigasi	Dengan ini, Anda dapat menonaktifkan Bilah Navigasi (Kembali/Menu) Jika fungsi ini telah diaktifkan, maka Mode Kios hanya dapat diakhiri di Konsol AppTec360 (hanya tersedia pada perangkat Samsung dengan SAFE 3.0 atau lebih tinggi)

Peluncur AppTec360

Aktifkan Peluncur AppTec360	Aktif: Mengaktifkan Peluncur AppTec360. Pengguna harus mengaturnya sebagai Peluncur default satu kali. Catatan: Jika Mode Kios diaktifkan, dan Mode Kios diatur ke "Multi App", penggunaan peluncur AppTec360 akan diberlakukan.
Ikon Besar	Aktif: Menampilkan Versi Ikon Aplikasi yang lebih besar di Peluncur
Sembunyikan Ikon Aplikasi AppTec360	Aktif: Menyembunyikan Aplikasi AppTec360 sepenuhnya
Sembunyikan Ikon Toko AppTec360	Aktif: Menyembunyikan AppTec360 Enterprise AppStore sepenuhnya

Pengaturan AppTec360

Aktifkan Aplikasi Pengaturan AppTec360	Aplikasi Pengaturan AppTec360 menyediakan kontrol atas koneksi WiFi dan Bluetooth
Mengaktifkan Pengaturan di Multi Aplikasi Mode Kios	Jika diaktifkan, pengguna dapat mengakses Aplikasi Pengaturan AppTec360 saat Mode Kios Multi Aplikasi aktif

Kontrol Jarak Jauh

Splashtop

Untuk memulai sesi kendali jarak jauh untuk perangkat Anda, Aplikasi "Splashtop Streamer" harus diinstal pada perangkat dengan menambahkan Aplikasi ke **Manajemen Aplikasi → Manajer Aplikasi Perusahaan → Aplikasi Wajib**.

Setelah itu, konfigurasikan pengaturan berikut ini untuk Splashtop:

Mengaktifkan Splashtop	Jika diaktifkan, AppTec360 akan mengonfigurasi aplikasi Splashtop untuk memungkinkan kontrol jarak jauh
Menyebarkan Kode	Buka https://my.splashtop.com dan masuk ke akun Splashtop Anda. Klik "Tambah Komputer" dan salin 12 digit kode penerapan dari halaman yang muncul.
Mengatur Custom Deploy Gateway?	Menyebarkan Gateway
Menyebarkan Domain / Host Gateway	Menyebarkan Gateway
Verifikasi Sertifikat	Verifikasi Sertifikat

Kemudian Anda dapat menggunakan opsi Splashtop Remote Control menu konteks (roda gigi di sebelah bilah pencarian, ketika perangkat dipilih atau klik kanan pada perangkat di pohon) untuk memulai sesi remote control.

Penampil Tim

Untuk memulai sesi kendali jarak jauh untuk perangkat Anda, Aplikasi "TeamViewer QuickSupport" harus diinstal pada perangkat dengan menambahkan Aplikasi ke **Manajemen Aplikasi → Manajer Aplikasi Perusahaan → Aplikasi Wajib**.

Kemudian Anda dapat menggunakan opsi **TeamViewer Remote Control** menu konteks (roda gigi di sebelah bilah pencarian, ketika perangkat dipilih atau klik kanan pada perangkat di pohon) untuk memulai sesi remote control.

Manajemen Konten

Kotak Konten

Di sini Anda dapat mengaktifkan ContentBox.

Segera setelah Anda mengalihkan "Aktifkan ContentBox" ke "Aktif", Aplikasi ContentBox terpisah akan diinstal
secara otomatis pada perangkat pengguna akhir.

Peramban yang Aman

Di sini Anda dapat mengonfigurasi pengaturan untuk AppTec360 Secure Browser.

Segera setelah Anda mengganti bagian di "Secure Browser" ke "On", Aplikasi Browser terpisah akan diinstal secara otomatis pada perangkat pengguna akhir.

Memerlukan Kata Sandi	Mengharuskan pengguna untuk mengatur dan menggunakan kata sandi untuk mengakses browser.
Panjang kata sandi minimal yang diperlukan	Tetapkan jumlah karakter yang diperlukan untuk kata sandi
Kualitas Kata Sandi yang Diperlukan	Mengatur kualitas kata sandi yang diperlukan
Batasi Unduhan / Buka Dalam	
Membatasi Unggahan	
Unggah Daftar Putih	Daftar URL yang akan selalu diizinkan untuk diunggah.
Izinkan Salin	Memungkinkan menyalin, memotong, atau berbagi teks di dalam halaman web.
Izinkan Pengambilan Layar	Izinkan pengambilan tangkapan layar.
Frekuensi pembersihan data	Pilih dengan frekuensi yang mana, SEMUA data pengguna (riwayat, cache, dll.) harus dihapus secara otomatis.
Penanda Perusahaan	Penanda akan muncul di folder "Penanda perusahaan" di penanda browser. Mereka tidak dapat diedit oleh pengguna.
Sembunyikan Bilah Alamat	
Daftar Putih Dalam Peramban (tanpa Gerbang Universal)	Mengaktifkan daftar putih URL sisi klien. • Penanda Perusahaan selalu masuk daftar putih • Hanya didukung untuk 100 URL saja • Silakan gunakan Gerbang Universal untuk Daftar Hitam dan Daftar Putih tanpa batas
URL yang masuk daftar putih	Daftar URL yang diizinkan.
Daftar Hitam dan Putih berbasis gateway	Daftar hitam memiliki persyaratan sebagai berikut:

	• AppTec360 Universal Gateway yang berfungsi ("Pengaturan Umum" → "Universal Gateway") • Konfigurasi VPN yang berfungsi dengan server DNS tertentu ("Pengaturan Umum" → "Universal Gateway" → "Pengaturan VPN") • Konfigurasi Daftar Hitam ("Pengaturan Umum" → "Gerbang Universal" → "Daftar Hitam Domain") • Sambungan VPN yang valid di profil ("Manajemen Koneksi" → "VPN")

API tambahan

Samsung KNOX

Pembatasan

Izinkan Kartu SD	
Izinkan Penulisan Kartu SD	
Izinkan Pengambilan Layar	
Izinkan Papan Klip	
Mencadangkan pengaturan dan data aplikasi di Google Cloud	
Memulihkan pengaturan dari Google Cloud saat menginstal ulang aplikasi	
Izinkan Debugging USB	
Izinkan Laporan Kerusakan Google	
Izinkan Reset Pabrik	
Izinkan Peningkatan OTA	
Mengizinkan penyimpanan host USB	Jika diaktifkan, pengguna dapat menyambungkan pen drive (penyimpanan USB portabel), HD eksternal, atau pembaca kartu Secure Digital (SD), dan dipasang sebagai drive penyimpanan pada perangkat.
Izinkan Pemutar Media USB (MTP, PTP)	
Izinkan Mikrofon	Menonaktifkan mikrofon untuk aplikasi pihak ketiga
Izinkan NFC (Komunikasi Jarak Dekat)	
Izinkan Sumber Tidak Dikenal (Pemuatan Samping APK)	Jika diaktifkan, pemuatan Aplikasi (file APK) diperbolehkan. Setelah pengaturan ini dinonaktifkan, pengguna harus mengaktifkannya secara manual ketika Anda mengizinkan kembali pemasangan APK dari sumber yang tidak dikenal.

Izinkan Pembuatan Pengguna	Jika diaktifkan, pengguna diizinkan untuk membuat beberapa akun pada perangkat, misalnya Akun Tamu

Email

Alamat email	
Protokol server yang masuk	
Alamat server yang masuk	
Port server yang masuk	
Login/nama pengguna server yang masuk	
Kata sandi server yang masuk	
Server yang masuk menggunakan SSL	
Server masuk menggunakan TLS	
Server yang masuk menerima semua sertifikat	
Protokol server keluar	
Alamat server keluar	
Port server keluar	
Server Keluar menggunakan kredensial tambahan	Jika dinonaktifkan, sistem akan menggunakan kredensial yang masuk untuk server yang keluar.
Login/nama pengguna server keluar	
Kata Sandi Server Keluar	
Server keluar menggunakan SSL	
Server keluar menggunakan TLS	
Server keluar menerima semua sertifikat	
Tetapkan Tanda Tangan	
Tanda tangan	Catatan: Untuk beberapa perangkat, tanda tangan harus ditentukan dalam format HTML.
Memberi tahu pengguna saat menerima eMail baru	

Pertukaran

Alamat email	
Nama Host Server	Nama host dari Server Exchange
Nama Login	Nama pengguna yang digunakan untuk masuk ke Exchange Server
Domain	Jika Konfigurasi Gateway ACL diaktifkan dan bidang Domain tidak kosong, AppTec360 Universal Gateway akan mengautentikasi perangkat dengan nama berikut "Domain\Nama Login
Kata sandi	
Jumlah hari sebelumnya untuk disinkronkan	
Frekuensi untuk menyinkronkan eMail	
Sinkronisasi saat Roaming	
Tetapkan Tanda Tangan	
Tanda tangan	Catatan: Untuk beberapa perangkat, tanda tangan harus ditentukan dalam format HTML.
Akun default	
Gunakan Lapisan Soket Aman (SSL)	
Gunakan Transport Layer Security (TLS)	
Menerima semua sertifikat	

APN

Nama Tampilan APN	
Nama Titik Akses	Nama APN
Protokol server keluar	
MCC - Kode Negara Seluler	Biarkan kosong untuk menggunakan mmc dari SIM yang terpasang
MNC - Kode Jaringan Seluler	Biarkan kosong untuk menggunakan mnc dari SIM yang terpasang
Alamat Server	
Nomor port server	
Alamat proxy server	
Alamat server MMS	Biarkan kosong untuk default
Nomor port MMS	Biarkan kosong untuk default
Alamat proxy MMS	Biarkan kosong untuk default
Nama pengguna	
Kata sandi	
Jenis Titik Akses	Jenis yang diterima adalah "default", "mms", "supl".
	Jika null atau kosong dilewatkan, secara default "default,supl,mms" digunakan.
	Biarkan kosong untuk default.
APN yang disukai	

Bluetooth

Izinkan penemuan Perangkat melalui Bluetooth	
Izinkan Pemasangan Bluetooth	
Mengizinkan perangkat Headset Bluetooth	
Mengizinkan perangkat bebas genggam Bluetooth	
Mengizinkan perangkat Bluetooth A2DP	A2DP, Profil Distribusi Audio Lanjutan memungkinkan streaming audio antar perangkat
Mengizinkan Panggilan Keluar	
Izinkan Transfer Data melalui Bluetooth	
Izinkan Penambatan Bluetooth	
Izinkan koneksi ke Komputer melalui Bluetooth	

Koneksi

Hanya Izinkan Panggilan DaruratAzinkan Wi-Fi	
Tingkat Keamanan Minimum Jaringan Wi-Fi	
Melarang pengguna menambahkan jaringan Wi-Fi	Pembatasan ini hanya dapat diaktifkan jika setidaknya satu Profil Wi-Fi aktif ditetapkan dalam Manajemen Koneksi
Izinkan SMS & MMS	
Izinkan Sinkronisasi selama Roaming	
Izinkan Roaming Suara	

Android Enterprise – Perangkat yang Dikelola Sepenuhnya dengan Profil Kerja (COPE)

Penjelasan Umum tentang COPE

COPE adalah singkatan dari **Corporate Owned Personally Enabled**.

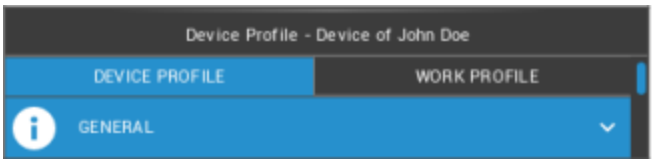
Mode COPE memungkinkan perangkat Android untuk didaftarkan sebagai **Android Enterprise - Perangkat yang Dikelola Sepenuhnya** dengan profil **Android Enterprise - Container** yang terintegrasi.

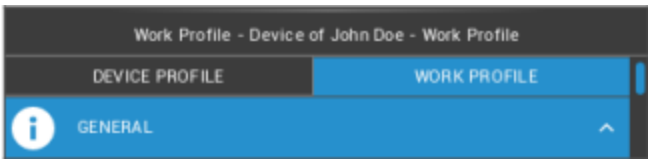
Ini bisa berupa perangkat Android yang sudah terdaftar sebagai **Android Enterprise - Perangkat Terkelola Sepenuhnya** dan di mana **Android Enterprise - Kontainer** juga disiapkan, atau perangkat Android yang baru terdaftar yang langsung terdaftar sebagai **Android Enterprise - Perangkat Terkelola Sepenuhnya** bersama **Android Enterprise - Kontainer** di atasnya.

Mode COPE hanya tersedia untuk perangkat dengan Android 8, 9 dan 10

Konfigurasi Profil untuk Perangkat COPE

Karena tidak ada profil Konfigurasi untuk mode COPE itu sendiri, konfigurasi **Android Enterprise - Perangkat yang Dikelola Sepenuhnya** dan **Android Enterprise - Wadah** dipisahkan menjadi dua profil di dalam profil COPE. Anda dapat beralih di antara dua profil untuk konfigurasi masing-masing profil dengan mengklik tombol masing-masing di sisi kiri konsol:





Kedua profil dapat dikonfigurasikan seperti yang dijelaskan untuk masing-masing profil:

Android Enterprise - Perangkat yang Dikelola Sepenuhnya

Perusahaan Android - Wadah

Mengembalikan ke Perangkat yang Dikelola Sepenuhnya AE

Profil **Android Enterprise - Kontainer** dapat dihapus seperti yang dijelaskan di **Manajemen Seluler**.

Dengan menghapus profil Container, profil COPE akan diubah menjadi profil **Android Enterprise - Perangkat yang Dikelola Sepenuhnya**.

Android Enterprise – Konfigurasi Kontainer

Tergantung pada apakah Anda saat ini telah memilih profil grup atau perangkat, ikhtisar dan sub-poinnya akan berbeda - harap pertimbangkan hal ini dengan saksama!

Umum

Ikhtisar Profil (hanya pada tingkat profil)

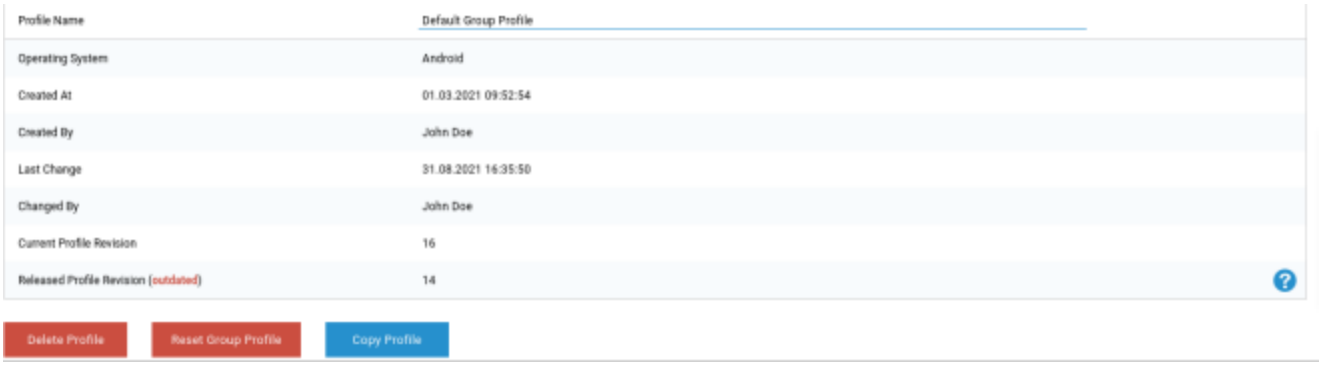
Jika Anda berada dalam sebuah profil, Anda akan menerima gambaran umum singkat tentang profil tersebut, terkait nama, OS, tanggal pembuatan, penulis, dll.

Nama Profil	Nama profil - dapat langsung diganti namanya di sini
Sistem Operasi	OS yang valid untuk profil
Dibuat di	Tanggal pembuatan
Dibuat oleh	Dibuat oleh
Perubahan Terakhir	Tanggal perubahan terakhir
Diubah oleh	Pengguna yang melakukan perubahan terakhir pada profil ini
Revisi Profil Saat Ini	Berapa kali profil telah diperbarui
Revisi Profil yang Dirilis	Berapa kali profil telah diperbarui dan telah ditetapkan perangkat

Menghapus Profil	Menghapus Profil
Mengatur Ulang Profil Grup	Mengatur Ulang Profil Grup
Salin Profil	Salin Profil

Ikhtisar profil grup (hanya pada tingkat grup)

Ketika membuka profil grup, Anda akan mendapatkan ikhtisar singkat profil.



Nama Profil	Nama profil (dapat diubah di sini)
Sistem Operasi	Sistem Operasi profil ini untuk
Dibuat di	Waktu pembuatan
Dibuat oleh	Pembuat profil
Perubahan Terakhir	Waktu perubahan terakhir pada profil
Diubah oleh	Akun yang melakukan perubahan terakhir
Revisi Profil Saat Ini	Revisi status profil yang disimpan
Revisi Profil yang Dirilis	Menetapkan revisi profil ("Tetapkan sekarang"). Jika label menunjukkan "(usang)" di belakang teks, itu berarti Anda telah menyimpan profil tetapi belum menetapkannya, sehingga perangkat masih akan mendapatkan versi yang lebih lama.

Ikhtisar Perangkat (hanya pada tingkat perangkat)

Jika Anda menggunakan perangkat, Anda akan menerima rekap ikhtisar perangkat yang dipilih, berikut ini yang terdapat di sini:

Nama Perangkat	Nama perangkat
Lokasi	Koordinat lokasi
Nomor Telepon	Nomor telepon
Aplikasi Wajib yang Ditetapkan	Jumlah Aplikasi Wajib yang ditetapkan
Versi OS	Versi OS perangkat
Sistem Operasi	Sistem Operasi (Android Enterprise)
Nomor Seri	Nomor seri perangkat
Kepemilikan Perangkat	Perangkat perusahaan atau pribadi
Jenis Perangkat	Perangkat yang Dikelola Pekerjaan AE
Berakar	Status, menunjukkan apakah perangkat telah di-root
Sesuai	Sesuai dengan pedoman
Alamat IP	Alamat IP perangkat
Terakhir terlihat	Titik waktu, ketika perangkat terakhir kali terhubung ke AppTec
Dorongan Terakhir	Titik waktu, ketika dorongan terakhir dikirim ke perangkat
Penugasan Pengguna	Pengguna atau grup yang ditetapkan untuk perangkat ini

Revisi Konfigurasi

Di sini Anda menerima ikhtisar profil grup mana yang ditetapkan ke perangkat.

Jika Anda mengklik profil grup, Anda akan mendapatkan akses langsung ke profil ini dan Anda dapat melakukan pengaturan.

Dengan simbol ini, Anda dapat mengembalikan aplikasi yang didistribusikan ke pengaturan profil grup.

Dengan simbol ini, Anda dapat mengembalikan semua aplikasi yang digunakan ke pengaturan profil grup.

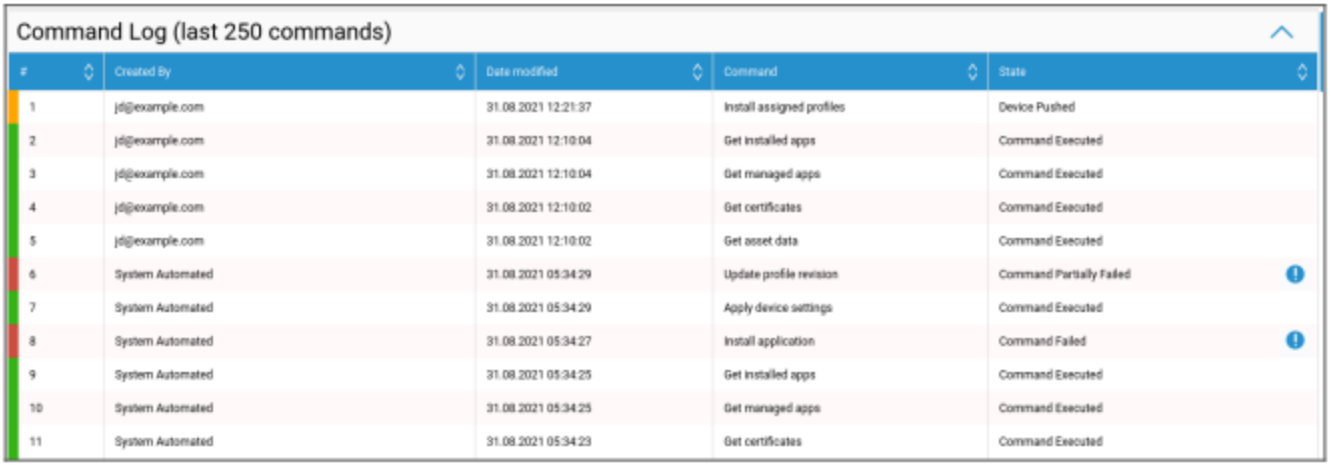
"Revisi terbaru tersedia" menunjukkan bahwa profil grup telah diubah dan disimpan namun belum ditetapkan. Profil grup harus ditetapkan dengan "Tetapkan sekarang" pada tingkat grup untuk menerapkan perubahan ke perangkat.

Log Perangkat (hanya pada tingkat perangkat)

Di sini Anda akan menerima berbagai log perangkat. Jika perlu, Anda dapat langsung mengetahui penyebab kesalahan di sini.

Log Perintah

Di sini Anda dapat melihat perintah mana yang dikeluarkan untuk perangkat dan bagaimana statusnya.



Kemungkinan status perintah

Perangkat Didorong	Permintaan push telah dikirim ke layanan push (misalnya APNS) untuk memberi tahu perangkat agar terhubung kembali ke server EMM.
Perintah Dibuat	Perintah ini dibuat dalam sistem.
Perintah Terkirim	Perintah dikirim ke perangkat setelah perangkat terhubung ke server.
Perintah Dieksekusi	Perintah berhasil dijalankan.
Perintah Gagal	Perintah gagal. *
Perintah Gagal Sebagian	Tergantung pada OS perangkat, beberapa perintah mungkin akan dikelompokkan bersama. Dalam hal ini, beberapa bagian dari grup perintah ini gagal. *
Perintah Dieksekusi, akhirnya Gagal	Perintah itu dijalankan tetapi mungkin tidak.
Perintah Ditolak	Perintah tersebut ditolak oleh pengguna.
Dibuang	Perintah telah dibuang. Misalnya karena digantikan oleh perintah lain atau perangkat didaftarkan ulang dan perintah lama dihapus

*Jika terdapat tanda seru di belakang pesan, Anda dapat memperoleh informasi lebih lanjut dengan mengarahkan kursor ke ikon tersebut.

Pengaturan Perangkat

Konfigurasi Klien

Di sini Anda dapat melakukan konfigurasi berikut ini pada perangkat Android Anda:

Di luar Waktu Kepatuhan	Batas waktu respons pengguna setelah tindakan penegakan diterapkan.
Tindakan penegakan setelah batas waktu kepatuhan	Tindakan penegakan ketika pengguna tidak melakukan tindakan yang mengarah pada status perangkat yang patuh
Frekuensi Pengumpulan Data	Frekuensi pengumpulan informasi perangkat/GPS yang akan dikumpulkan
Frekuensi Detak Jantung Perangkat	Interval di mana perangkat harus menghubungi Server AppTec Min. 1 menit Max. 24 jam
Mengaktifkan Pembaruan Lokasi	Jika diaktifkan, perangkat akan mengirimkan pembaruan lokasi ke Server AppTec
Waktu Pembaruan Lokasi	Menentukan dalam interval waktu berapa perangkat mengirimkan pembaruan lokasi ke AppTec
Gunakan Akurasi Lokasi Google untuk Pembaruan Lokasi	Jika diaktifkan, lokasi jaringan akan digunakan untuk pembaruan lokasi (jika ini dinonaktifkan pada "Pembatasan", maka pengaturan ini tidak akan memengaruhi apa pun)
Gunakan Lokasi GPS untuk Pembaruan Lokasi	Jika diaktifkan, GPS akan digunakan untuk pembaruan lokasi
Izinkan Lokasi Tiruan (Palsu)	Memungkinkan pemalsuan informasi lokasi melalui aplikasi pihak ketiga
Tindakan Kehilangan Koneksi	Jika diaktifkan, Anda dapat menentukan tindakan jika perangkat tidak mendapatkan koneksi ke server MDM dalam interval detak jantung. Misalnya, jika perangkat memiliki waktu detak jantung 5 menit, perangkat akan tersambung ke server pada pukul 10:35 pagi. Setelah itu perangkat meninggalkan jangkauan Wi-Fi. Detak jantung berikutnya pada pukul 10:40 pagi akan gagal, dan tindakan yang ditentukan akan dieksekusi.
Tindakan	Tindakan yang harus diambil, segera setelah perangkat menjadi tidak sesuai. • Lock Perangkat = perangkat kunci

	• Wipe Device (Hapus Perangkat) = perangkat akan dikembalikan ke pengaturan pabrik • Wipe Device & SD Card = perangkat akan dikembalikan ke pengaturan pabrik dan penyimpanan SD Card akan dihapus
Ambang batas	Anda dapat menentukan ambang batas Detak Jantung yang gagal yang diperlukan untuk memicu tindakan yang ditentukan.

Mode Penegakan Kebijakan	Default:	Pengguna akan diminta secara berkala untuk melakukan tindakan yang belum diselesaikan
	Penegakan Kebijakan yang Malas:	Pengguna tidak akan pernah diminta untuk melakukan tindakan yang belum selesai. Semua tindakan terbuka akan ditampilkan di Klien AppTec
	Penegakan Kebijakan yang Agresif:	Pengguna akan diminta tanpa henti untuk melakukan tindakan yang luar biasa
Kunci Versi AppTec	Jika diaktifkan, kode versi untuk aplikasi AppTec dapat ditentukan. Klien AppTec hanya akan memperbarui ke versi yang ditentukan. Versi yang lebih baru akan diabaikan. Penurunan versi TIDAK dimungkinkan.	
Kode Versi	Kode versi untuk aplikasi AppTec yang akan dikunci.	
Menonaktifkan Pemberitahuan AppTec	Jika dinonaktifkan, Klien AppTec tidak akan menampilkan Pemberitahuan di Bilah Pemberitahuan. Dengan demikian pengguna dapat menutup klien AppTec melalui task manager. Jika klien AppTec ditutup, beberapa fitur termasuk Mode Kios dan Daftar Hitam/Putih Aplikasi tidak akan berfungsi dengan baik. Perangkat Samsung menawarkan mekanisme perlindungan untuk Klien AppTec. Notifikasi dinonaktifkan secara default pada perangkat Samsung yang mendukung API KNOX. Pemberitahuan tidak boleh dinonaktifkan pada perangkat dengan Android 8.0 atau lebih tinggi.	

Wallpaper

Mengatur Wallpaper khusus	Mengaktifkan/menonaktifkan wallpaper khusus
Wallpaper	Mengatur mode wallpaper untuk menggunakan kode warna atau gambar
Tentukan Warna	Tentukan warna latar belakang sebagai nilai heksa, misalnya #000000 untuk hitam atau #ffffff sebagai putih
Mengatur Gambar sebagai Wallpaper	Unggah file gambar yang ingin Anda gunakan sebagai wallpaper

Manajemen Aset (hanya pada tingkat perangkat)

Info Perangkat

Model	Penunjukan model perangkat
Sistem Operasi	OS
Versi OS	Versi OS
Nomor Seri	Nomor seri
Nama Perangkat	Nama perangkat
Status Baterai	Status baterai
Memori Bebas / Total	Memori bebas / Total memori
Samsung Aman	Antarmuka Samsung SAFE, diperlukan untuk berbagai opsi pengaturan
Tersedia Kartu SD	Tersedia Kartu SD
Kartu SD Ditiru	Kartu SD ditiru
Kartu SD Dapat Dilepas	Kartu SD dapat dilepas
Memori Bebas SD / Total Memori	Memori SD Bebas / Total Kartu SD

Wi-Fi

Alamat IP	Alamat IP perangkat
MAC WiFi	Alamat MAC WiFi

Seluler

Status	Status (kartu SIM terpasang)
Nomor Telepon	Nomor Telepon
Roaming (Suara / Data)	Roaming untuk suara / data
Status Roaming	Status roaming saat ini
Alamat IP	Alamat IP
Operator/Pengangkut	Operator/Pengangkut
Teknologi Seluler	Teknologi Seluler
IMEI	Nomor IMEI
ICCID	Ini adalah ID untuk kartu SIM, yang sering kali juga merupakan Smartcard atau Kartu Sirkuit Terpadu (ICC)
IMSI	Identitas Pelanggan Seluler Internasional (IMSI) menyediakan identifikasi yang pasti bagi pengguna jaringan seluler GSM dan UMTS IMSI terdiri dari maksimum 15 digit dan dikonfigurasikan dengan cara berikut: • Kode Negara Seluler (Mobile Country Code (MCC)), 3 digit • Kode Jaringan Seluler (MNC), 2 atau 3 digit • Nomor Identifikasi Pelanggan Seluler (MSIN), 1-10 digit
PKS/MNC saat ini	Lihat "SIM MCC/MNC"
SIM PKS / MNC	Kode Negara Seluler adalah pengidentifikasi negara yang ditetapkan oleh ITU sesuai Standar E.212. Kode ini berfungsi bersama dengan Kode Jaringan Seluler (Mobile Network Code/MNC) untuk identifikasi jaringan seluler. Berarti negara/Kode Jaringan Seluler kartu SIM. Jika Anda roaming ke jaringan seluler lain, maka secara logika, "MCC/MNC saat ini" dan "MCC/MNC SIM", akan berbeda.

Bluetooth

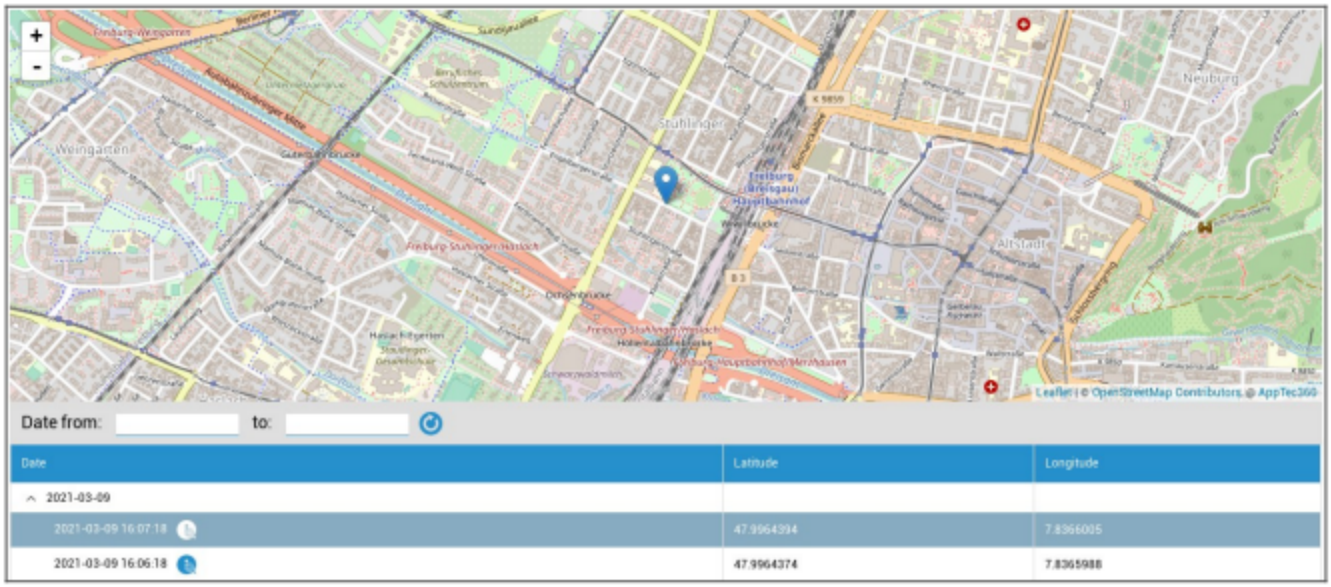
Bluetooth MAC	Alamat MAC Bluetooth

Manajemen Keamanan

Anti Pencurian (hanya pada tingkat perangkat)

Informasi GPS (hanya pada tingkat perangkat)

Di sini Anda dapat menetapkan lokasi perangkat saat ini/terakhir. Pelokalan dapat dilindungi dengan satu atau bahkan dua kata sandi - Lihat: Pengaturan Umum - Privasi - Akses GPS



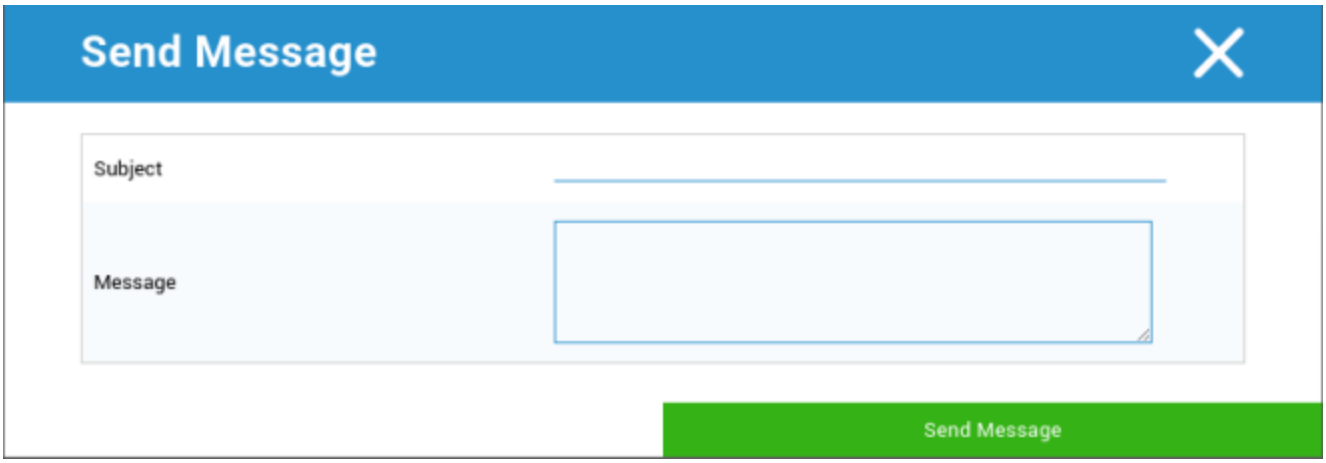
Hapus & Kunci (hanya pada tingkat perangkat)

Di bawah "Wipe & Lock", Anda dapat melakukan tiga tindakan berikut ini:

Penghapusan Penuh	Perangkat dipulihkan kembali ke pengaturan pabrik (data perusahaan dan data pribadi dihapus). Hanya berfungsi untuk Profil Kerja yang Disempurnakan
Penghapusan Perusahaan	Hanya data perusahaan yang dihapus dari perangkat pengguna akhir (semua aplikasi, data, dll. yang disediakan oleh AppTec)
Layar Kunci	Kunci layar diaktifkan, cukup untuk membuka kunci perangkat dengan kata sandi/PIN perangkat

Pesan (hanya pada tingkat perangkat)

Di sini Anda dapat mengisi subjek dan pesan dan mengirimkannya ke perangkat pengguna akhir



Konfigurasi Keamanan

Kode Sandi Perangkat

Di bawah "Kode Sandi" Anda dapat mengamanatkan kata sandi perangkat, opsi pengaturan berikut tersedia untuk Anda

Panjang kata sandi minimum	Menetapkan, jumlah minimum simbol yang harus dimiliki kata sandi	
Kualitas kata sandi	Tidak ditentukan	Kebijakan ini tidak memiliki persyaratan untuk kata sandi.
	Biometrik Lemah	Kebijakan ini memungkinkan teknologi pengenalan biometrik dengan keamanan rendah. Hal ini menyiratkan teknologi yang dapat mengenali identitas seseorang hingga sekitar 3 digit PIN (deteksi palsu kurang dari 1 dari 1.000).
	Sesuatu.	Kebijakan ini membutuhkan semacam kata sandi atau pola yang harus ditetapkan, tetapi tidak memberlakukan aturan tertentu.
	Abjad	Pengguna harus memasukkan kata sandi yang mengandung setidaknya karakter alfabet (atau simbol lainnya).
	Alfanumerik	Pengguna harus memasukkan kata sandi yang mengandung setidaknya kedua karakter tersebut, yaitu karakter numerik dan abjad (atau simbol lainnya).
	Kompleks	Pengguna harus memasukkan kata sandi yang setidaknya terdiri dari sebuah huruf, angka dan simbol khusus, secara default. Dengan kualitas kata sandi ini, kata sandi dapat dibatasi untuk mengandung berbagai rangkaian karakter, seperti setidaknya huruf besar, dll.
Panjang kata sandi minimum	Tetapkan jumlah karakter yang diperlukan untuk kata sandi. Misalnya, Anda dapat mewajibkan PIN atau kata sandi memiliki setidaknya enam karakter.	
Digit numerik minimum yang diperlukan dalam kata sandi	Digit numerik minimum yang diperlukan dalam kata sandi	
Huruf kecil minimum yang diperlukan dalam kata sandi	Huruf kecil minimum yang diperlukan dalam kata sandi	

Huruf besar minimum yang diperlukan dalam kata sandi	Huruf besar minimum yang diperlukan dalam kata sandi
Karakter non-huruf minimum yang diperlukan dalam kata sandi	Karakter non-huruf minimum yang diperlukan dalam kata sandi
Simbol minimum yang diperlukan dalam kata sandi	Simbol minimum yang diperlukan dalam kata sandi

Kunci waktu tidak aktif maksimum	Ketidakaktifan pengguna maksimum hingga kunci waktu
Batas waktu kedaluwarsa kata sandi	Menetapkan, setelah interval waktu mana kata sandi kedaluwarsa dan kata sandi baru harus dikeluarkan
Pembatasan riwayat kata sandi	Jumlah kata sandi yang pernah digunakan sebelumnya yang tidak diizinkan
Percobaan kata sandi maksimum yang gagal	Menetapkan, seberapa sering kata sandi dapat dimasukkan secara tidak benar, sebelum penghapusan perangkat secara menyeluruh akan dilakukan
Izinkan Otentikasi Biometrik	Memungkinkan autentikasi melalui sidik jari atau pemindaian iris mata. Hanya untuk Samsung KNOX 2.1 dan yang lebih tinggi

Kode Sandi Kontainer

Di bawah "Kode Sandi" Anda dapat mengamanatkan kata sandi kontainer, opsi pengaturan berikut ini tersedia untuk Anda

Panjang kata sandi minimum	Menetapkan, jumlah minimum simbol yang harus dimiliki kata sandi	
Kualitas kata sandi	Tidak ditentukan	Kebijakan ini tidak memiliki persyaratan untuk kata sandi.
	Biometrik Lemah	Kebijakan ini memungkinkan teknologi pengenalan biometrik dengan keamanan rendah. Hal ini menyiratkan teknologi yang dapat mengenali identitas seseorang hingga sekitar 3 digit PIN (deteksi palsu kurang dari 1 dari 1.000).
	Sesuatu.	Kebijakan ini membutuhkan semacam kata sandi atau pola yang harus ditetapkan, tetapi tidak memberlakukan aturan tertentu.
	Abjad	Pengguna harus memasukkan kata sandi yang mengandung setidaknya karakter alfabet (atau simbol lainnya).
	Alfanumerik	Pengguna harus memasukkan kata sandi yang mengandung setidaknya kedua karakter tersebut, yaitu karakter numerik dan abjad (atau simbol lainnya).
	Kompleks	Pengguna harus memasukkan kata sandi yang setidaknya terdiri dari sebuah huruf, angka dan simbol khusus, secara default. Dengan kualitas kata sandi ini, kata sandi dapat dibatasi untuk mengandung berbagai rangkaian karakter, seperti setidaknya huruf besar, dll.
Panjang kata sandi minimum	Tetapkan jumlah karakter yang diperlukan untuk kata sandi. Misalnya, Anda dapat mewajibkan PIN atau kata sandi memiliki setidaknya enam karakter.	
Digit numerik minimum yang diperlukan dalam kata sandi	Digit numerik minimum yang diperlukan dalam kata sandi	
Huruf kecil minimum yang diperlukan dalam kata sandi	Huruf kecil minimum yang diperlukan dalam kata sandi	
Huruf besar minimum yang	Huruf besar minimum yang diperlukan dalam kata sandi	

diperlukan dalam kata sandi	
Karakter non-huruf minimum yang diperlukan dalam kata sandi	Karakter non-huruf minimum yang diperlukan dalam kata sandi
Simbol minimum yang diperlukan dalam kata sandi	Simbol minimum yang diperlukan dalam kata sandi

Kunci waktu tidak aktif maksimum	Ketidakaktifan pengguna maksimum hingga kunci waktu
Batas waktu kedaluwarsa kata sandi	Menetapkan, setelah interval waktu mana kata sandi kedaluwarsa dan kata sandi baru harus dikeluarkan
Pembatasan riwayat kata sandi	Jumlah kata sandi yang pernah digunakan sebelumnya yang tidak diizinkan
Percobaan kata sandi maksimum yang gagal	Menetapkan, seberapa sering kata sandi dapat dimasukkan secara tidak benar, sebelum penghapusan perangkat secara menyeluruh akan dilakukan

Anti Virus

Pemindaian Otomatis	Mengaktifkan pemindaian otomatis secara berkala
Interval Pemindaian	Interval untuk pemeriksaan (Cepat / Penuh)
Pemindaian Otomatis Penuh	Mengaktifkan pemindaian otomatis penuh
Pembaruan Otomatis	Mengaktifkan pembaruan otomatis
Perbarui Interval Pemeriksaan	Seberapa sering aplikasi dan basis datanya harus diperbarui (virus/kode yang rusak)
Perlindungan Aplikasi	Mengaktifkan pemindaian aplikasi otomatis
Perlindungan Kartu SD	Mengaktifkan pemindaian Kartu SD otomatis
Pembaruan Khusus Wi-Fi	Ketika diaktifkan, pembaruan hanya akan diterapkan ketika perangkat berhasil tersambung ke jaringan Wi-Fi

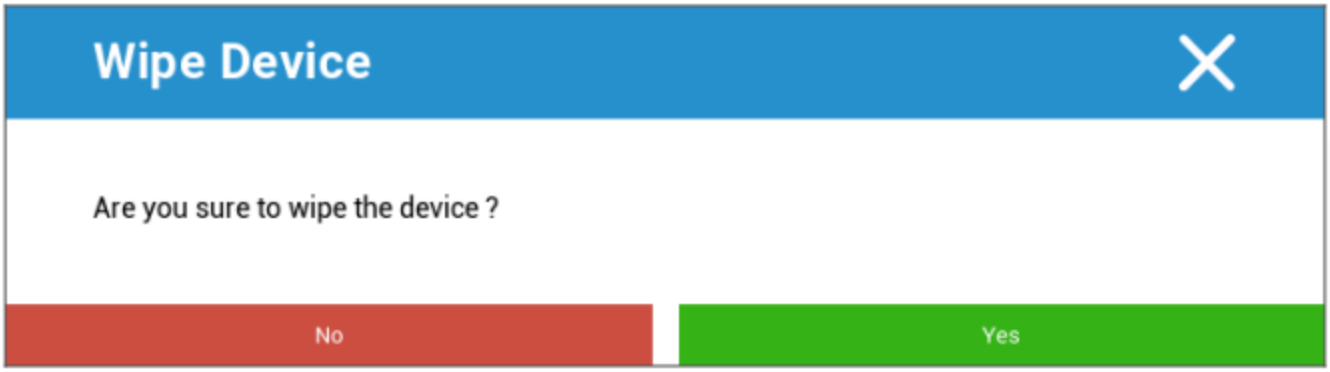
Akhir Masa Pakai (hanya pada tingkat perangkat)

Menghapus (hanya pada tingkat perangkat)

Di bawah "Wipe", Anda dapat memulihkan perangkat ke pengaturan pabrik (Hanya pada Enhanced Work Profile (Profil Kerja yang Disempurnakan).

Di sini, data perusahaan dan data pribadi akan dihapus pada perangkat pengguna akhir.

Dengan klik pada "Simbol Minus", Anda akan menerima pesan berikut ini:



Dengan "Ya", Anda dapat melakukan penghapusan.

Di bawah "Hapus Laporan", item berikut ini dapat ditampilkan

Dihapus oleh	Riwayat siapa yang melakukan penghapusan
Tanggal	Tanggal
Status	Status (mis. jika Penghapusan berhasil dilakukan)

Pengaturan Pembatasan

Pembatasan

Di sini, berbagai hal dapat dibatasi dan diblokir.

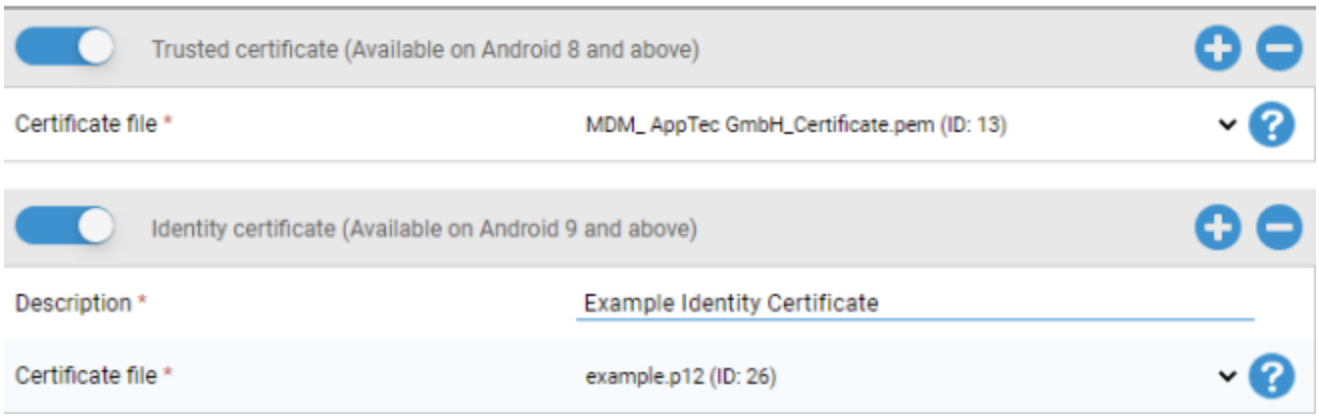
Penegakan Kepatuhan	Mode Prompt User - Pengguna akan diminta untuk memenuhi tindakan yang diperlukan. Mode Lock-Down Container - Sembunyikan semua aplikasi sampai semua persyaratan terpenuhi
Kebijakan Izin Runtime	Meminta pengguna untuk permintaan izin baru Selalu mengabulkan permintaan izin baru yang baru Selalu tolak permintaan izin baru Peringatan: Beberapa Aplikasi mengalami masalah dalam mengenali izin jika ini diatur secara otomatis. Jika Anda selalu memberikan izin dan mengalami masalah dengan aplikasi yang mengatakan bahwa izin tidak ada, atur ini ke "meminta pengguna" dan instal ulang aplikasi
Izinkan papan klip keluar	Memungkinkan salin dan tempel dari dalam wadah ke luar
Izinkan Resolusi ID Penelepon	Menampilkan nama untuk panggilan masuk berdasarkan kontak dalam wadah
Izinkan Resolusi Pencarian Kontak	Memungkinkan untuk mencari nama dalam kontak kontainer saat melakukan panggilan
Izinkan Berbagi Kontak Bluetooth	Memungkinkan akses ke kontak kontainer di dalam mobil
Memblokir Sinar NFC Keluar	Menonaktifkan NFC untuk Wadah
Izinkan Sumber Tidak Dikenal	Jika diaktifkan, pengguna dapat memuat Aplikasi secara terpisah dengan menginstal file .apk.
Izinkan Debugging USB	Jika diaktifkan, pengguna dapat mengaktifkan USB Debugging.
Melarang Modifikasi Akun	Melarang pembuatan, penghapusan, dan modifikasi Akun di dalam kontainer Perlu diingat bahwa beberapa aplikasi perlu membuat atau memodifikasi akun agar berfungsi seperti yang diharapkan

Pembatasan Profil Kerja. Hanya tersedia di perangkat Android 11 dan yang lebih tinggi, dengan Profil Kerja yang Disempurnakan	
Melarang Kamera	Menentukan apakah kamera tidak diizinkan dalam profil kerja.
Nonaktifkan Bluetooth	Menentukan apakah bluetooth dilarang di profil kerja.
Mengaktifkan Perlindungan Reset Pabrik	Aktifkan ini untuk menimpa Perlindungan Pengaturan Ulang Pabrik Android ke Akun Google yang Anda tentukan di "Pengaturan Umum" → "Konfigurasi Android" → "Android Enterprise" → "Perlindungan Pengaturan Ulang Pabrik" Jika ini diaktifkan dan Anda mengatur ulang perangkat, Anda harus memberikan Akun Google yang telah dikonfigurasikan untuk menyiapkan perangkat lagi.
Kontrol Pembaruan OS	Aktifkan ini untuk mengatur perilaku pembaruan menjadi otomatis, berjendela, atau ditunda.
Perbarui Kebijakan	Otomatis: Instal secara otomatis segera setelah pembaruan tersedia. Berjendela: Menginstal secara otomatis dalam jendela pemeliharaan harian. Ini juga mengonfigurasi aplikasi Play untuk diperbarui dalam jendela. Ini sangat disarankan untuk perangkat kios karena ini adalah satu-satunya cara agar aplikasi yang disematkan secara terus-menerus di latar depan dapat diperbarui oleh Play. Tunda: Menunda penginstalan otomatis hingga maksimum 30 hari.

Pembatasan Profil Pribadi. Hanya tersedia di perangkat Android 11 dan yang lebih tinggi, dengan Profil Kerja yang Disempurnakan	
Melarang Kamera	Menentukan apakah kamera tidak diperbolehkan dalam profil pribadi.
Nonaktifkan Bluetooth	Menentukan apakah bluetooth dilarang di profil pribadi.
Izinkan Sumber Tidak Dikenal	Jika diaktifkan, pengguna profil kerja dapat memuat Aplikasi secara terpisah dengan menginstal file .apk.

Manajemen Sertifikat

Di sini Anda dapat mendistribusikan Sertifikat Terpercaya dan Sertifikat Identitas ke perangkat Anda. Android 8 atau lebih tinggi diperlukan untuk mendistribusikan Sertifikat Terpercaya dan Android 9 atau lebih tinggi diperlukan untuk mendistribusikan Sertifikat Identitas.



Dengan tanda "+", Anda dapat menambahkan beberapa sertifikat.

Sertifikat Tepercaya harus dalam format PEM.

Sertifikat Identitas harus dalam format PKCS12.

Manajemen Koneksi

Wifi

Untuk pengaturan ini, lakukan pra-konfigurasi perangkat pengguna akhir, untuk akses ke Access internal
Points

Pengidentifikasi Set Layanan (SSID)	SSID untuk jaringan yang akan disambungkan
Jaringan Tersembunyi	Aktifkan, jika AP tidak menyiarkan SSID

Jenis Keamanan

Menetapkan jenis keamanan AP

WEP

Kata sandi	Kata sandi untuk AP

WPA/WPA2

Kata sandi	Kata sandi untuk AP

802.1x EAP

Metode EAP

PENYANDANG DISABILITAS	Identitas	Identitas
	Kata sandi	Kata sandi

PEAP	Protokol Otentikasi Fase 2	tidak ada	Tidak ada protokol tambahan
		MSCHAPV2	Protokol MSCHAPV2
		GTC	Protokol GTC
	Sertifikat CA	Sertifikat CA	
	Identitas	Identitas	
	Identitas Anonim	Identitas anonim	
	Kata sandi	Kata sandi	

TTLS	Protokol Otentikasi Fase 2	tidak ada	Tidak ada protokol tambahan
		PAP	Protokol PAP
		MSCHAP	Protokol MSCHAP
		MSCHAPV2	Protokol MSCHAPV2
		GTC	Protokol GTC
	Sertifikat CA	Sertifikat CA	
	Identitas	Identitas	
	Identitas Anonim	Identitas Anonim	
	Kata sandi	Kata sandi	

TLS	Sertifikat CA	Sertifikat CA
	Identitas	Identitas
	Kata sandi	Kata sandi

VPN

Nama Koneksi	Nama Koneksi VPN

Jenis VPN

VPN

Klien VPN

Klien VPN AppTec	
Konfigurasi Gateway	Pilih Konfigurasi VPN Gateway (Lihat **Pengaturan Umum > Gateway Universal > Pengaturan VPN**)
VPN yang selalu aktif	Mengaktifkan Penguncian Asli
Mengaktifkan Penguncian AppTec	Mengaktifkan Penguncian AppTec

Bawaan (Hanya tersedia pada perangkat Samsung)			
Jenis Koneksi	PPTP	Server	Server
		Mengaktifkan Enkripsi PPTP	Mengaktifkan Enkripsi PPTP
	L2TP / IPSec PSK	Server	Server
		Kunci Pra-Berbagi IPSec	Kunci Pra-Berbagi IPSec
		Aktifkan Rahasia L2TP	Aktifkan Rahasia L2TP
		Rahasia L2TP	Rahasia L2TP
	IPSec XAuth PSK	Server	Server
		Pengidentifikasi IPSec	Pengidentifikasi IPSec
		Kunci Pra-Berbagi IPSec	Kunci Pra-Berbagi IPSec
Domain Pencarian DNS	Domain Pencarian DNS		
Pengaturan Pakar	Server DNS	Server DNS	
	Rute Penerusan	Rute Penerusan	

Buka VPN		
Server	Server	
Profil OpenVPN	Profil OpenVPN	
Aplikasi OpenVPN	OpenVPN untuk Android (disarankan)	
	OpenVPN Connect	
Pengaturan Pakar	Server DNS	Server DNS
	Rute Penerusan	Rute Penerusan

Samsung / Strong Swan			
Jenis Koneksi	PPTP	Server	Server
		Nama pengguna	Nama pengguna
		Kata sandi	Kata sandi
		Mengaktifkan Enkripsi PPTP	Mengaktifkan Enkripsi PPTP
	L2TP / IPSec PSK	Server	Server
		Kunci Pra-Berbagi IPSec	Kunci Pra-Berbagi IPSec
		Nama pengguna	Nama pengguna
		Kata sandi	Kata sandi
		Aktifkan Rahasia L2TP	Rahasia L2TP
	IPSec XAuth PSK	Server	Server
		Pengidentifikasi IPSec	Pengidentifikasi IPSec
		Kunci Pra-Berbagi IPSec	Kunci Pra-Berbagi IPSec
		Nama pengguna	Nama pengguna
		Kata sandi	Kata sandi
Pengaturan Pakar	Server DNS	Server DNS	
	Rute Penerusan	Rute Penerusan	

Cisco Any Connect		
Server	Server	
Mode Sertifikat	Dinonaktifkan	Dinonaktifkan
	Otomatis	Otomatis
Pengaturan Pakar	Server DNS	Server DNS
	Rute Penerusan	Rute Penerusan

VPN Per-Aplikasi

Klien VPN

Klien VPN AppTec		
Konfigurasi Gateway	Pilih Konfigurasi VPN Gateway (Lihat **Pengaturan Umum > Gateway Universal > Pengaturan VPN**)	
Aplikasi VPN	Aplikasi VPN	
VPN yang selalu aktif	Mengaktifkan Penguncian Asli	VPN yang selalu aktif
Mengaktifkan Penguncian AppTec	Mengaktifkan Penguncian AppTec	

Samsung / Strong Swan			
Jenis Koneksi	PPTP	Server	Server
		Aplikasi VPN	Aplikasi VPN
		Nama pengguna	Nama pengguna
		Kata sandi	Kata sandi
		Mengaktifkan Enkripsi PPTP	Mengaktifkan Enkripsi PPTP
	L2TP / IPSec PSK	Server	Server
		Aplikasi VPN	Aplikasi VPN
		Kunci Pra-Berbagi IPSec	Kunci Pra-Berbagi IPSec
		Nama pengguna	Nama pengguna
		Kata sandi	Kata sandi
		Aktifkan Rahasia L2TP	Rahasia L2TP
	IPSec XAuth PSK	Server	Server
		Aplikasi VPN	Aplikasi VPN
		Pengidentifikasi IPSec	Pengidentifikasi IPSec
		Kunci Pra-Berbagi IPSec	Kunci Pra-Berbagi IPSec
		Nama pengguna	Nama pengguna
		Kata sandi	Kata sandi
Pengaturan Pakar	Server DNS	Server DNS	
	Rute Penerusan	Rute Penerusan	

Pembatasan

Di sini Anda dapat mengatur pembatasan, terkait dengan manajemen koneksi

Izinkan Roaming Data	Izinkan data seluler saat roaming
Paksa Roaming Data	Jika diaktifkan, roaming untuk data seluler akan diaktifkan secara permanen (tidak disarankan!) Pengaturan ini menimpa pengaturan "Izinkan Data Roaming"!
Gunakan Sistem http Server Proxy	Penggunaan server proxy HTTP, yang disediakan oleh pengaturan sistem dalam pengaturan, bergantung pada jaringan yang terhubung (WiFi atau APN)

Manajemen PIM

Pertukaran Gmail

Info: Konfigurasi ini akan diterapkan pada aplikasi Gmail. Jadi, Anda harus menyetujui dan menginstal Gmail.

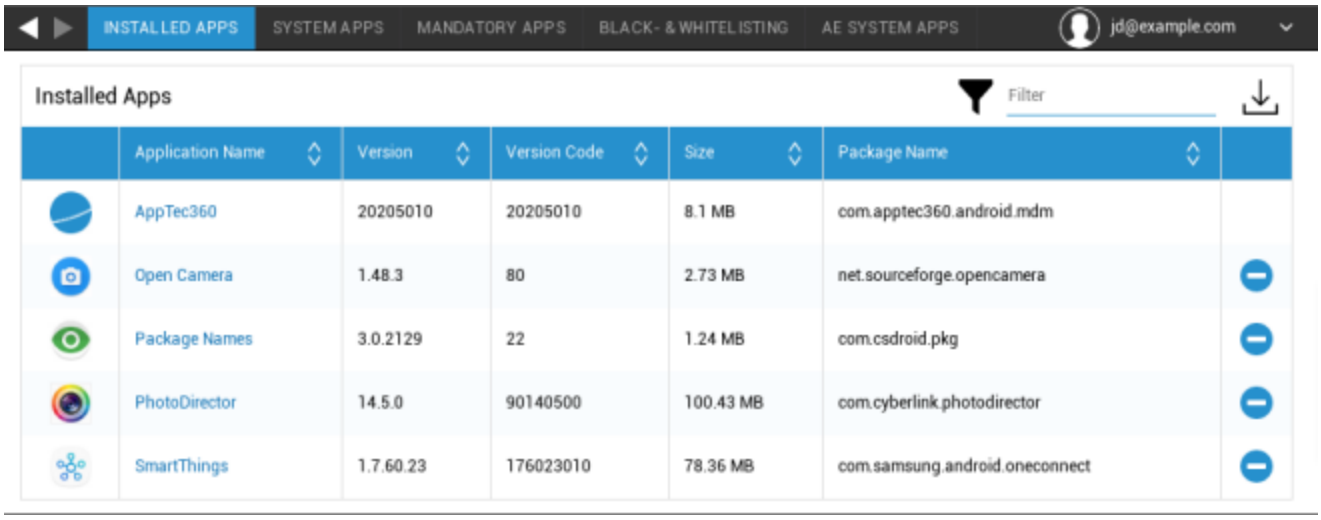
Alamat email	Alamat email pengguna yang diberikan Harap perhatikan "Placeholder", yang dapat Anda gunakan untuk bekerja dengan kredensial dan Anda tidak melakukan perubahan secara manual pada setiap perangkat Dengan sekali klik, Anda dapat menampilkannya sendiri
Nama Host Server	Alamat server dari Server Exchange Anda
Nama login	Nama Login untuk masing-masing perangkat pengguna akhir, harap perhatikan juga "Placeholder di sini
Tanda tangan	Tanda tangan dapat dilampirkan (Petunjuk: Beberapa perangkat memerlukan format HTML untuk tanda tangan)
Jumlah hari sebelumnya untuk disinkronkan	Jumlah hari, menentukan kapan email disinkronkan kembali
Pengenal Perangkat	Sebuah string yang berisi EAS DeviceID. Ini adalah bagian dari Protokol EAS dan akan digunakan dalam beberapa aplikasi
Gunakan Lapisan Soket Aman (SSL)	Gunakan koneksi SSL
Menerima semua sertifikat	Semua sertifikat diterima. Pilih opsi ini, jika Exchange Server Anda menggunakan sertifikat yang ditandatangani sendiri
Izinkan akun yang tidak dikelola	Izinkan pengguna untuk menambah atau menghapus akun Exchange apa pun, selain akun yang ditentukan dalam konfigurasi terkelola ini. Jika pengaturan ini diaktifkan, Anda tidak dapat mencegah pengguna menambahkan akun Exchange lain ke Gmail. Anda juga tidak dapat mengontrol berbagi data antara aplikasi lain dan akun Exchange yang ditambahkan oleh pengguna. Pengaturan ini harus diaktifkan hanya jika pengguna Anda perlu mengelola lebih dari satu akun Exchange di Gmail.
Sertifikat Klien	Sertifikat Klien. Hanya diperlukan jika Server Mail Anda mengharapkan hal ini ada.

Manajemen Aplikasi

Manajer Aplikasi Perusahaan

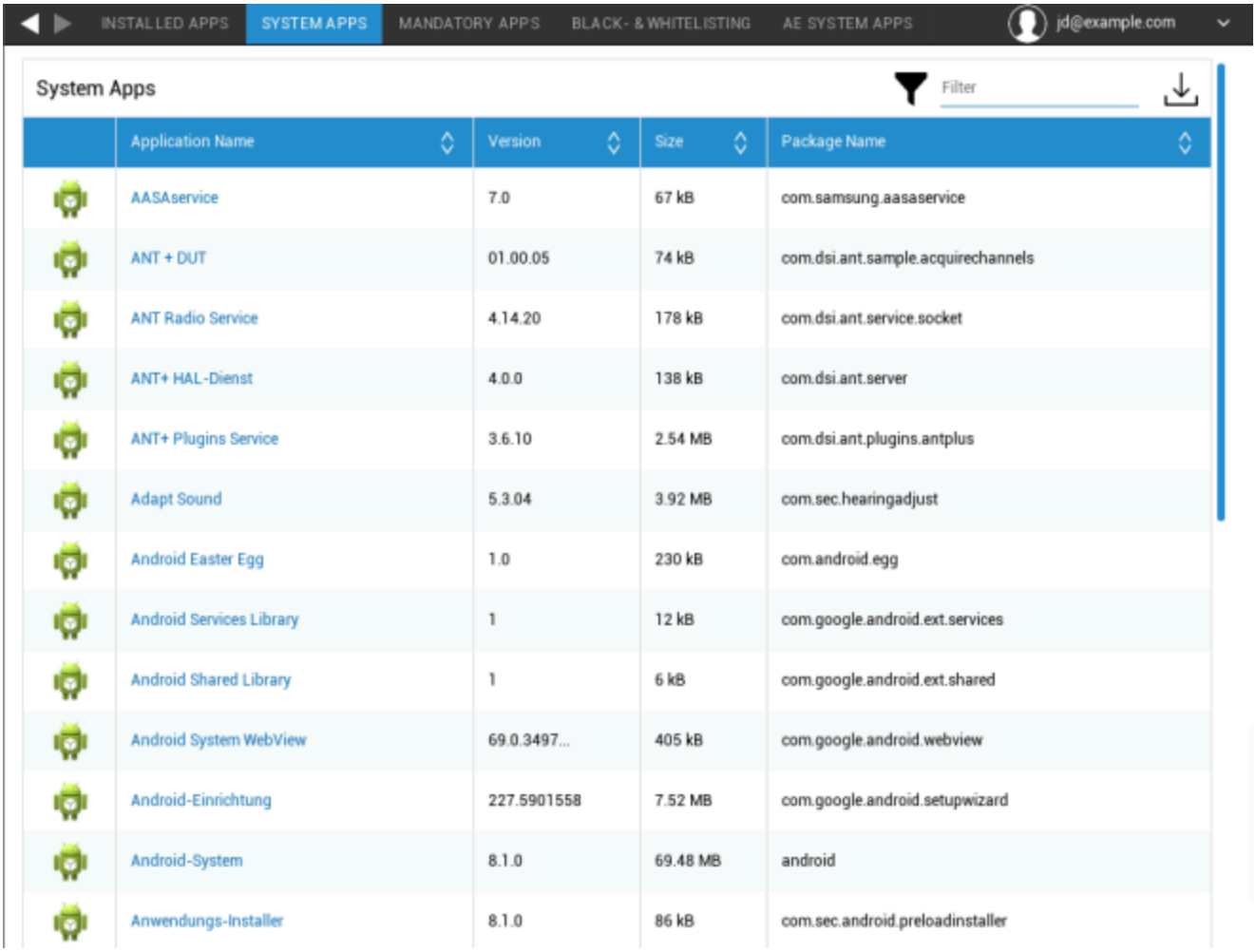
Aplikasi Terinstal (hanya pada tingkat perangkat)

Di sini semua Aplikasi yang saat ini terinstal di dalam kontainer akan ditampilkan untuk Anda.



Aplikasi Sistem (hanya pada tingkat perangkat)

Di bawah "Aplikasi Sistem", semua aplikasi dan layanan yang telah diinstal pada perangkat pengguna akhir oleh produsen perangkat Anda akan dicantumkan untuk Anda.

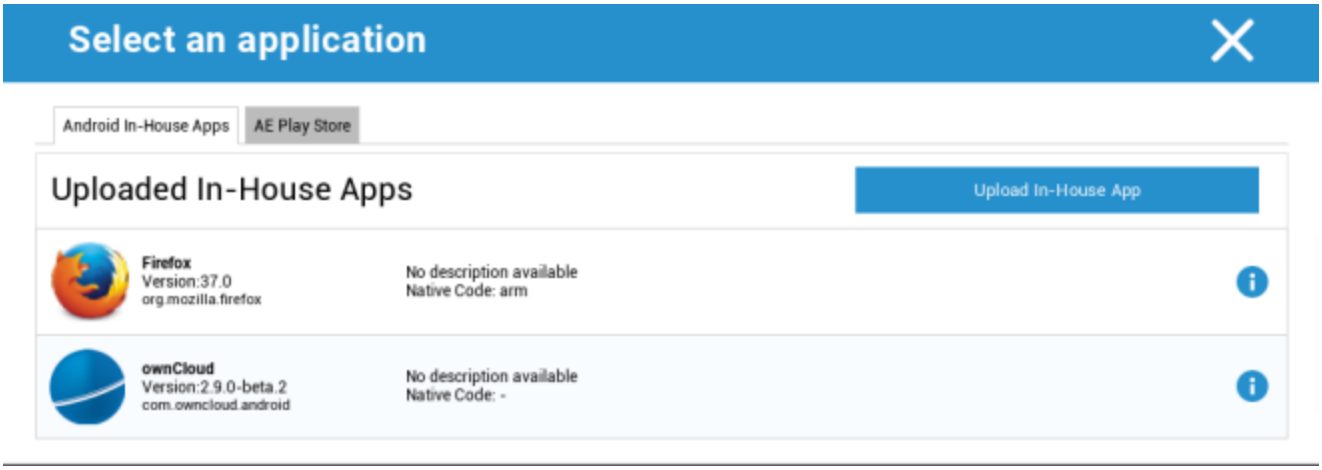


Aplikasi Wajib

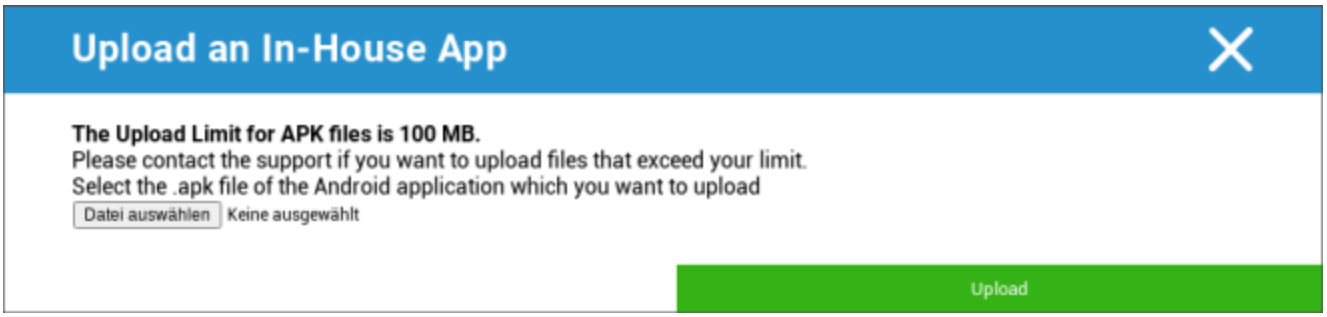
Di bawah Aplikasi Wajib, Anda dapat menetapkan aplikasi wajib yang diamanatkan. Pengguna akan terus diminta untuk menginstal aplikasi yang telah ditetapkan ini, jika ini adalah Aplikasi InHouse. Aplikasi Play Store akan diinstal secara otomatis.

Melalui , aplikasi yang diperlukan yang diamanatkan dapat ditentukan.

Ini dapat berupa Aplikasi In-House dari "Aplikasi In-House Android", yang telah Anda unggah di Pengaturan Umum.

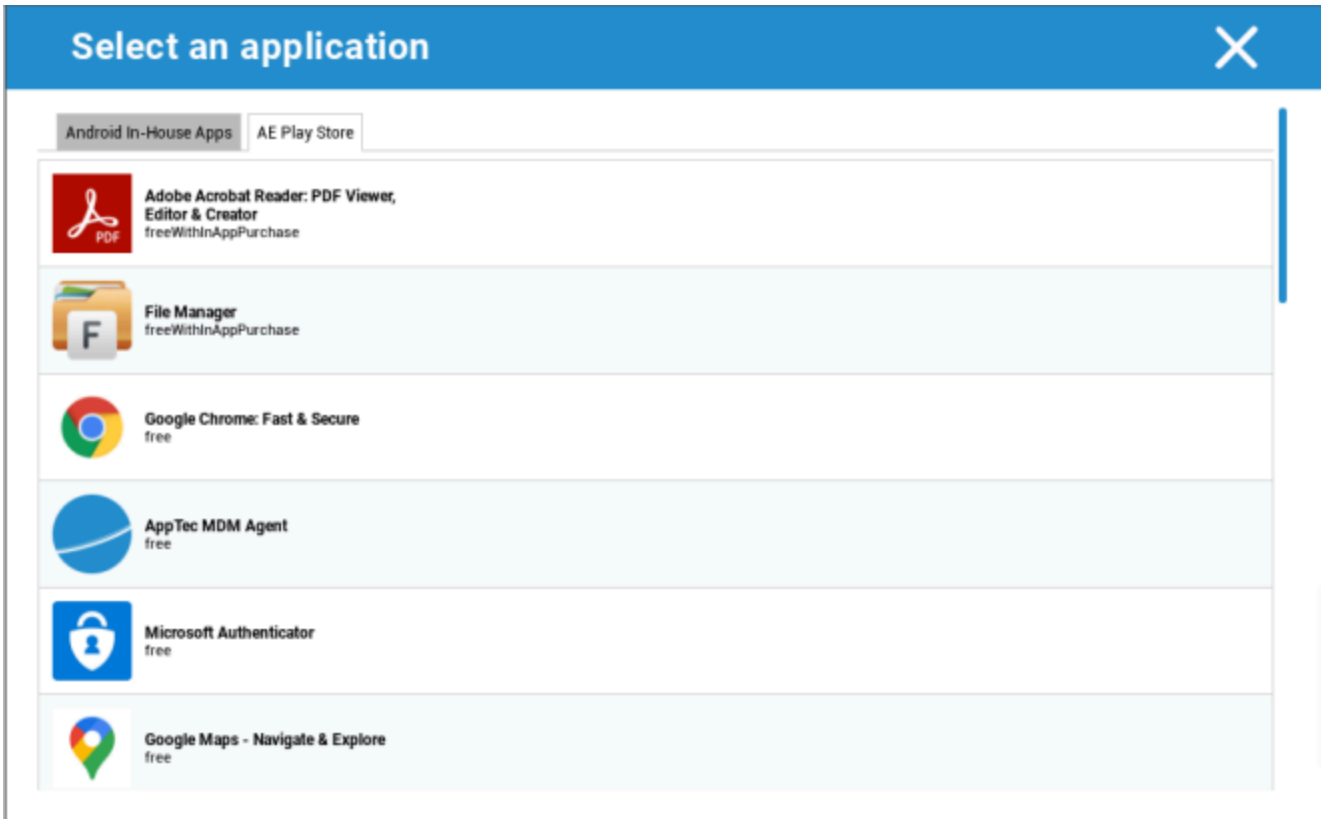


Anda juga dapat langsung memilih dan mengunggah file apk dengan "Unggah Aplikasi In-House".



Jika Anda menginstal Aplikasi In-House, Anda dapat mengaktifkan "Selalu perbarui". Jika ini diaktifkan dan Anda telah menetapkan versi yang lebih baru di DB Aplikasi In-House, aplikasi akan diperbarui pada perangkat.

Atau, bisa juga Aplikasi "AE Play Store" dari Google Work Play Store.



Hanya "Aplikasi AE Play Store" yang disetujui yang akan ditampilkan di tab ini.

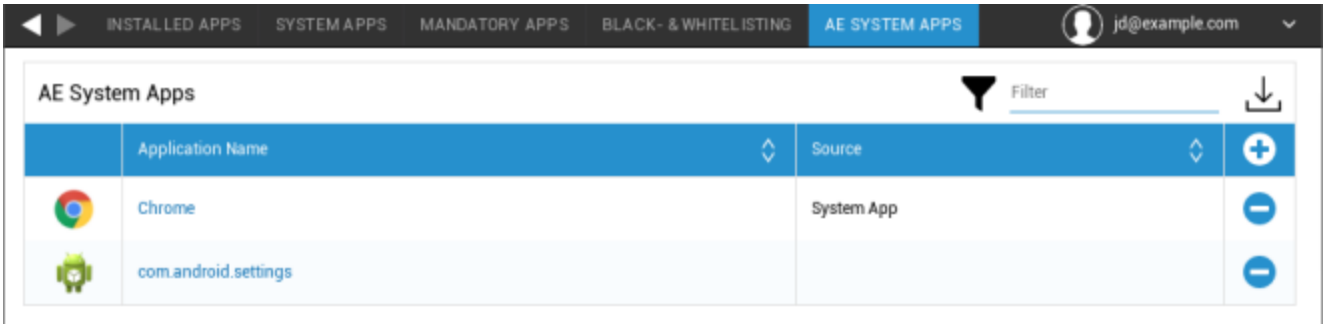
Untuk menyetujui "Aplikasi AE Play Store", silakan masuk ke "Pengaturan Umum" > "Manajemen Aplikasi" > "AE Play

Store" dan tambahkan aplikasi melalui tombol yang akan mengarahkan Anda ke tab "Play Store Apps" (atau Anda dapat langsung membuka tab "Play Store Apps").

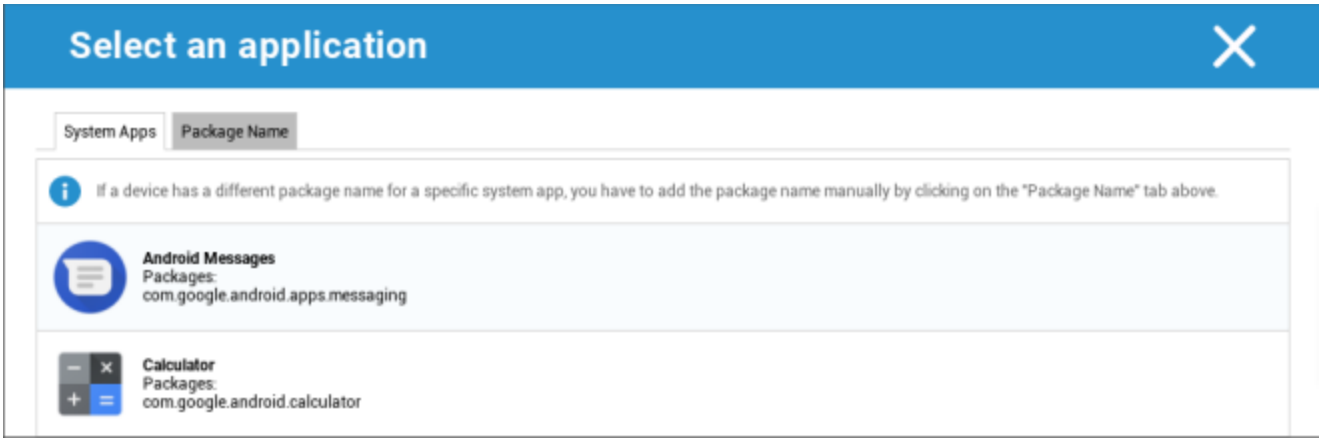
Pada tab "Aplikasi Play Store", Anda dapat mencari aplikasi. Ketika Anda mengeklik sebuah aplikasi, halaman aplikasi akan terbuka dan di sini Anda dapat menyetujui aplikasi tersebut dengan mengeklik "Setujui".

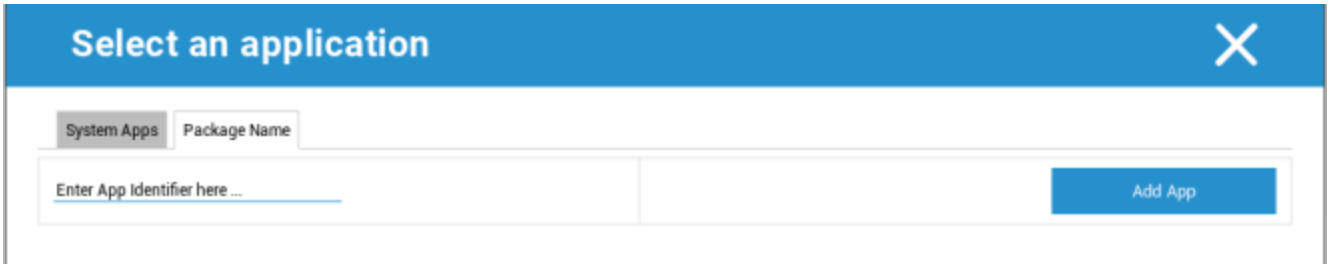
Aplikasi Sistem AE

Di sini Anda dapat menentukan daftar yang berisi aplikasi sistem tertentu yang harus diaktifkan pada perangkat.



Jika Anda mengklik tombol tersebut, Anda dapat memilih dari daftar aplikasi sistem yang disediakan oleh Google atau langsung memasukkan nama paket aplikasi sistem yang harus diaktifkan.





Harap diingat bahwa aplikasi sistem dalam daftar yang disediakan oleh Google hanyalah aplikasi yang dapat menjadi aplikasi sistem, tetapi tidak harus menjadi aplikasi sistem pada perangkat Anda.

Namun, daftar ini hanya memengaruhi aplikasi yang sudah terinstal sebelumnya.

Menambahkan aplikasi yang tidak terinstal sebelumnya pada perangkat Anda tidak akan memengaruhi perangkat Anda, terlepas dari apakah aplikasi tersebut berasal dari daftar yang disediakan oleh Google atau nama paket aplikasi yang dimasukkan secara langsung.

Pembatasan & Pengaturan

Pengaturan Manajemen Aplikasi

Di sini Anda dapat mengonfigurasi perilaku perangkat terkait pembaruan aplikasi.

Perbarui Frekuensi Pemeriksaan	Tentukan dalam interval berapa lama Klien AppTec akan mencari pembaruan aplikasi. Nilai default adalah 24 jam.
Ambang Batas Wi-Fi	Aplikasi yang lebih besar dari ukuran yang ditentukan akan diunduh melalui Wi-Fi. Jika "Hanya Wi-Fi" dipilih, semua aplikasi akan diunduh melalui Wi-Fi.

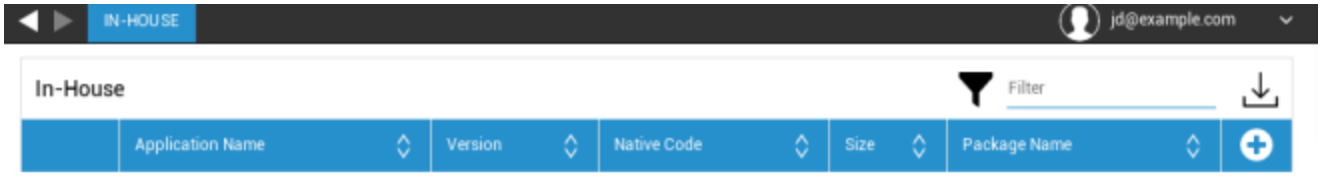
Toko Aplikasi Perusahaan

In-House

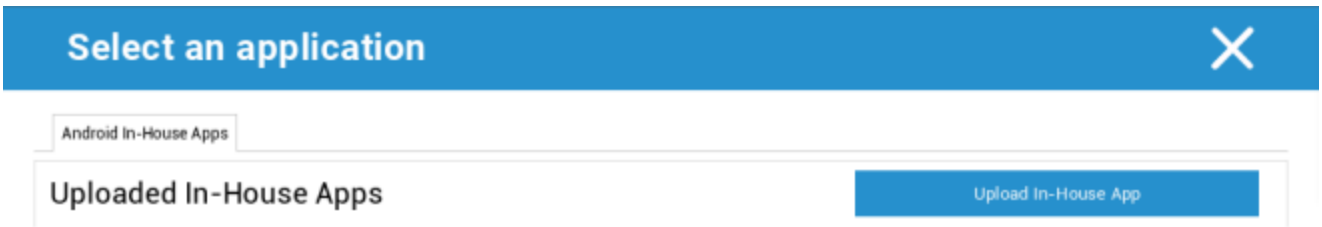
Di bawah poin "In-House", Anda dapat mengunggah dan mendistribusikan aplikasi yang dikembangkan secara internal.

Dengan simbol tersebut, Anda dapat mendistribusikan Aplikasi In-House tambahan.

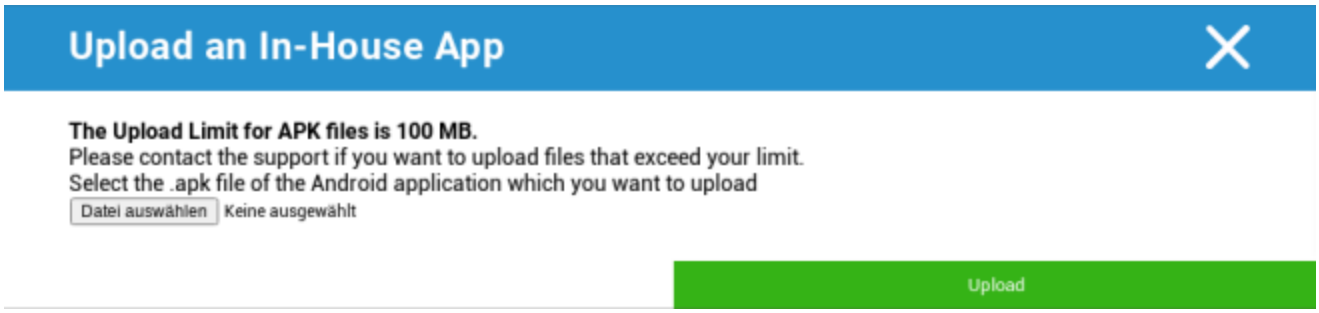
Jika Anda menginstal Aplikasi In-House, Anda dapat mengaktifkan "Selalu perbarui". Jika ini diaktifkan dan Anda telah menetapkan versi yang lebih baru di DB Aplikasi In-House, aplikasi akan diperbarui pada perangkat.



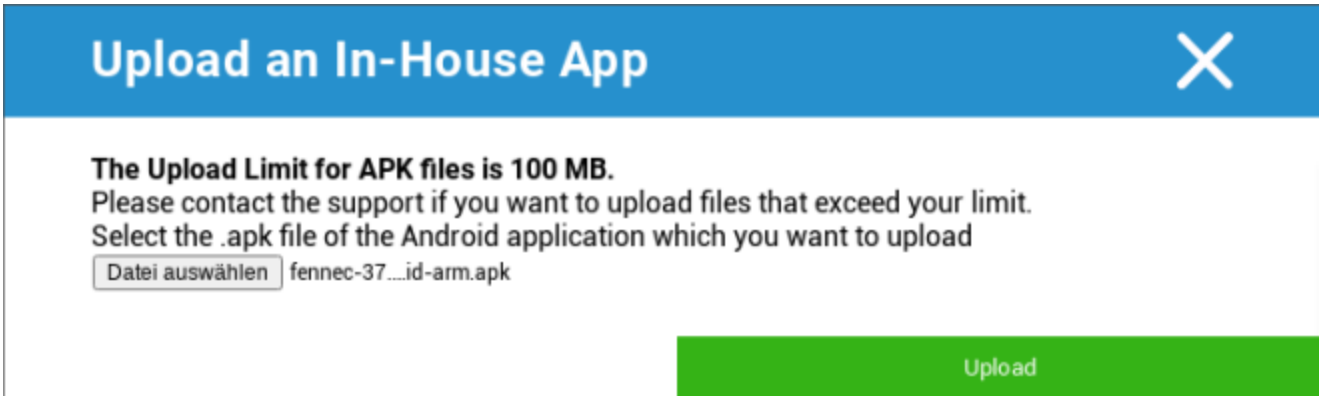
Jika Anda belum mendistribusikan Aplikasi In-House, Anda akan menerima ikhtisar berikut:



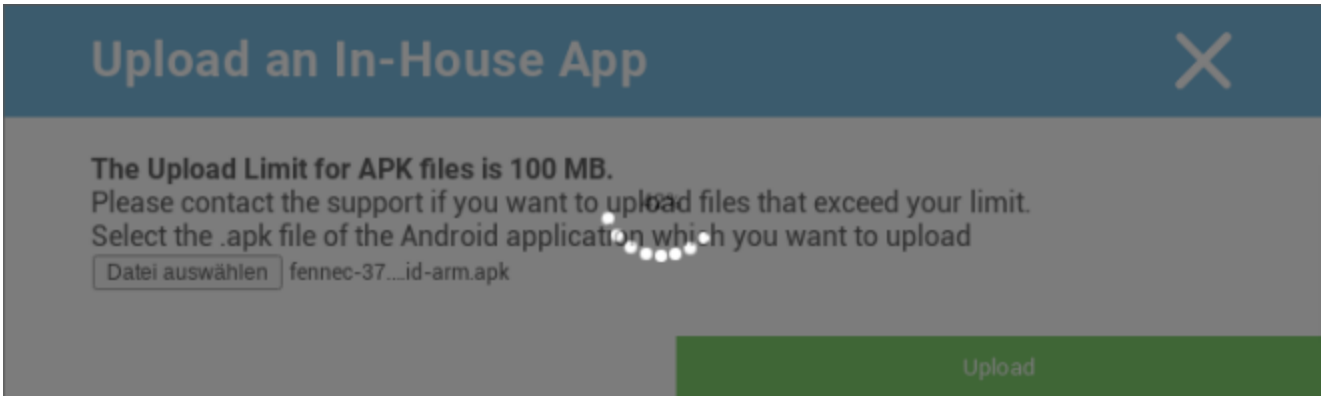
Untuk melakukan ini, klik "Unggah Aplikasi In-House", Anda akan menerima gambaran umum berikut:



Sekarang, pilih dengan "Cari..." file .apk dan kemudian klik "Unggah".



Aplikasi Anda sekarang akan diunggah, di tengah lingkaran Anda akan melihat indikator persentase, yang menunjukkan berapa banyak aplikasi Anda yang telah diunggah.



Jika pengunggahan Aplikasi In-House Anda berhasil, Anda dapat menemukan aplikasi yang diunggah di Katalog Aplikasi.

Pengguna sekarang memiliki opsi untuk melihat dan menginstal aplikasi ini di AppTec Store pada perangkat pengguna akhir, di bawah kategori "In-House".

Karena ini tidak melibatkan Aplikasi Google PlayStore, pengguna tidak memerlukan ID Google yang tersimpan di perangkat pengguna akhir masing-masing.

Perusahaan Play Store

AE Play Store

Di sini Anda dapat menambahkan Aplikasi ke Android Enterprise Playstore. Harap diperhatikan bahwa Anda harus menyetujui Aplikasi dengan Akun Administrator AE Anda sebelum menambahkannya.

Untuk menyetujui aplikasi, lihat petunjuk di Aplikasi Wajib.

Manajemen Konten

Kotak Konten

Di sini Anda dapat mengaktifkan ContentBox.

Segera setelah Anda mengalihkan "Aktifkan ContentBox" ke "Aktif", Aplikasi ContentBox terpisah akan diinstal secara otomatis pada perangkat pengguna akhir.

Peramban yang Aman

Di sini Anda dapat mengonfigurasi pengaturan untuk AppTec Secure Browser.

Segera setelah Anda mengganti bagian di "Secure Browser" ke "On", Aplikasi Browser terpisah akan diinstal secara otomatis pada perangkat pengguna akhir.

Memerlukan Kata Sandi	Mengharuskan pengguna untuk mengatur dan menggunakan kata sandi untuk mengakses browser.
Panjang kata sandi minimal yang diperlukan	Tetapkan jumlah karakter yang diperlukan untuk kata sandi
Kualitas Kata Sandi yang Diperlukan	Mengatur kualitas kata sandi yang diperlukan
Batasi Unduhan / Buka Dalam	
Membatasi Unggahan	
Unggah Daftar Putih	Daftar URL yang akan selalu diizinkan untuk diunggah.
Izinkan Salin	Memungkinkan menyalin, memotong, atau berbagi teks di dalam halaman web.
Izinkan Pengambilan Layar	Izinkan pengambilan tangkapan layar.
Frekuensi pembersihan data	Pilih dengan frekuensi yang mana, SEMUA data pengguna (riwayat, cache, dll.) harus dihapus secara otomatis.
Penanda Perusahaan	Penanda akan muncul di folder "Penanda perusahaan" di penanda browser. Mereka tidak dapat diedit oleh pengguna.
Sembunyikan Bilah Alamat	
Daftar Putih Dalam Peramban (tanpa Gerbang Universal)	Mengaktifkan daftar putih URL sisi klien. • Penanda Perusahaan selalu masuk daftar putih • Hanya didukung untuk 100 URL saja • Silakan gunakan Gerbang Universal untuk Daftar Hitam dan Daftar Putih tanpa batas
URL yang masuk daftar putih	Daftar URL yang diizinkan.
Daftar Hitam dan Putih berbasis gateway	Daftar hitam memiliki persyaratan sebagai berikut:

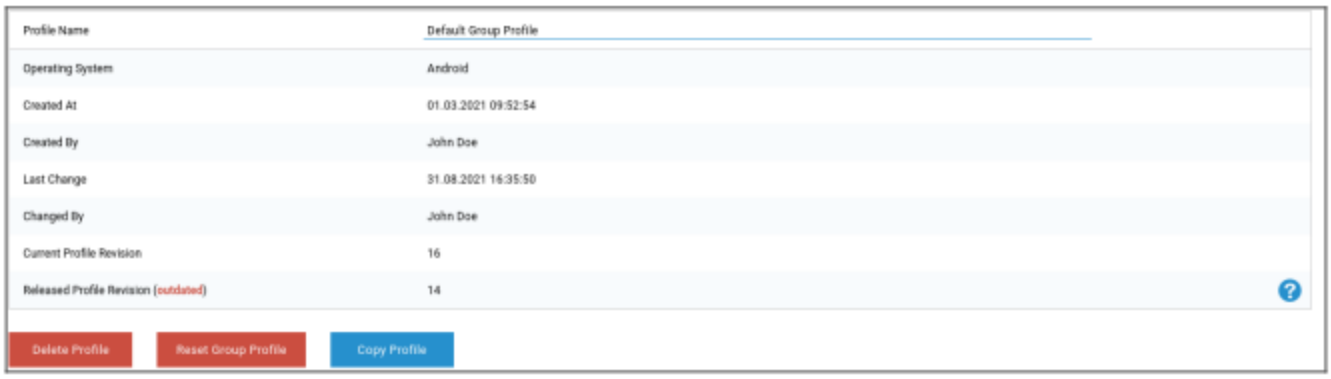
	• AppTec Universal Gateway yang berfungsi ("Pengaturan Umum" → "Universal Gateway") • Konfigurasi VPN yang berfungsi dengan server DNS tertentu ("Pengaturan Umum" → "Universal Gateway" → "Pengaturan VPN") • Konfigurasi Daftar Hitam ("Pengaturan Umum" → "Gerbang Universal" → "Daftar Hitam Domain") • Sambungan VPN yang valid di profil ("Manajemen Koneksi" → "VPN")

Konfigurasi Android

Umum

Ikhtisar profil grup (hanya pada tingkat grup)

Ketika membuka profil grup, Anda akan mendapatkan ikhtisar singkat profil.



Nama Profil	Nama profil (dapat diubah di sini)
Sistem Operasi	Sistem Operasi profil ini untuk
Dibuat di	Waktu pembuatan
Dibuat oleh	Pembuat profil
Perubahan Terakhir	Waktu perubahan terakhir pada profil
Diubah oleh	Akun yang melakukan perubahan terakhir
Revisi Profil Saat Ini	Revisi status profil yang disimpan
Revisi Profil yang Dirilis	Menetapkan revisi profil ("Tetapkan sekarang"). Jika label menunjukkan "(usang)" di belakang teks, itu berarti Anda telah menyimpan profil tetapi belum menetapkannya, sehingga perangkat masih akan mendapatkan versi yang lebih lama.

Ikhtisar Perangkat (hanya pada tingkat perangkat)

Jika Anda menggunakan perangkat, Anda akan menerima rekap ikhtisar perangkat yang dipilih, berikut ini yang terdapat di sini:

Nama Perangkat	Nama perangkat
Lokasi Terakhir Diketahui	Koordinat GPS terakhir yang diketahui
Nomor Telepon	Nomor telepon
Aplikasi Wajib yang Ditetapkan	Jumlah aplikasi wajib yang ditetapkan
Versi OS	Versi OS perangkat
Sistem Operasi	Sistem Operasi (Android / iOS / Windows Phone)
Nomor Seri	Nomor seri perangkat
Kepemilikan Perangkat	Perangkat perusahaan atau pribadi
Jenis Perangkat	Telepon atau Tablet
Berakar	Status, menunjukkan apakah perangkat telah di-root
Sesuai	Sesuai dengan pedoman
Alamat IP	Alamat IP
Terakhir terlihat	Titik waktu, ketika perangkat terakhir kali terhubung ke AppTec
Dorongan Terakhir	Titik waktu, saat server mengirim dorongan ke perangkat
Penugasan Pengguna	Menu tarik-turun untuk menetapkan perangkat ke pengguna lain

Revisi Konfigurasi (hanya pada tingkat perangkat)

Di sini Anda akan menerima ikhtisar profil grup mana yang ditetapkan ke perangkat.

Jika Anda mengklik profil grup, Anda akan mengakses profil secara langsung dan dapat melakukan pengaturan.

Dengan simbol ini, Anda dapat mengembalikan aplikasi yang ditetapkan ke pengaturan profil grup.

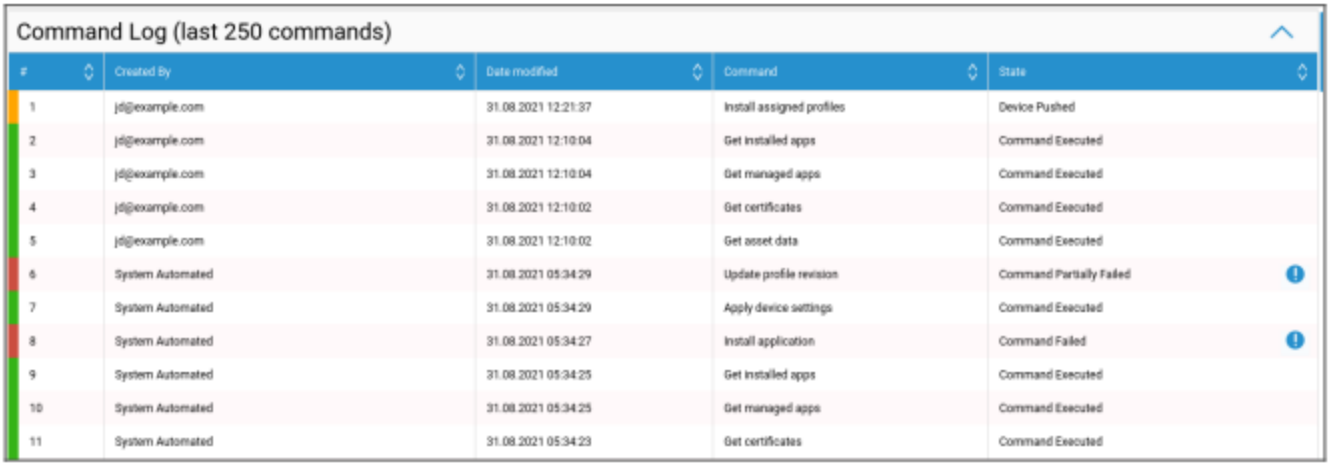
Dengan simbol tersebut, Anda dapat mengatur ulang profil perangkat agar tidak memiliki pengaturan sama sekali.

"Revisi terbaru tersedia" menunjukkan bahwa profil grup telah diubah dan disimpan namun belum ditetapkan. Profil grup harus ditetapkan dengan "Tetapkan sekarang" pada tingkat grup untuk menerapkan perubahan ke perangkat.

Log Perangkat (hanya pada tingkat perangkat)

Log Perintah

Di sini Anda dapat melihat perintah mana yang dikeluarkan untuk perangkat dan bagaimana statusnya.



Perintah yang dibuat oleh "System Automated" secara otomatis dibuat oleh sistem.

Kemungkinan status perintah

Perangkat Didorong	Permintaan push telah dikirim ke layanan push (misalnya APNS) untuk memberi tahu perangkat agar terhubung kembali ke server EMM.
Perintah Dibuat	Perintah ini dibuat dalam sistem.
Perintah Terkirim	Perintah dikirim ke perangkat setelah perangkat terhubung ke server.
Perintah Dieksekusi	Perintah berhasil dijalankan.
Perintah Gagal	Perintah gagal. *
Perintah Gagal Sebagian	Tergantung pada OS perangkat, beberapa perintah mungkin akan dikelompokkan bersama. Dalam hal ini, beberapa bagian dari grup perintah ini gagal. *
Perintah Dieksekusi, akhirnya Gagal	Perintah itu dijalankan tetapi mungkin tidak.
Perintah Ditolak	Perintah tersebut ditolak oleh pengguna.
Dibuang	Perintah telah dibuang. Misalnya karena digantikan oleh perintah lain atau perangkat didaftarkan ulang dan perintah lama dihapus

*Jika terdapat tanda seru di belakang pesan, Anda dapat memperoleh informasi lebih lanjut dengan mengarahkan kursor ke ikon tersebut.

Pengaturan Perangkat

Konfigurasi Klien

Di sini Anda dapat melakukan konfigurasi berikut ini pada perangkat Android Anda:

Pesan peringatan setelah menonaktifkan Manajemen Perangkat	Pesan peringatan yang dibuat setelah menonaktifkan Manajemen Perangkat
Di luar Waktu Kepatuhan	Batas waktu, setelah itu "Tindakan Penegakan setelah kepatuhan" akan dilakukan, jika perangkat tidak patuh. Min. 1 menit Max. 24 jam
Tindakan penegakan setelah batas waktu kepatuhan	Tindakan yang harus diambil, segera setelah perangkat menjadi tidak sesuai. • tidak melakukan apa-apa = tidak ada tindakan • Perangkat Kunci = perangkat kunci • Wipe Device (Hapus Perangkat) = perangkat akan dikembalikan ke pengaturan pabrik
Frekuensi Pengumpulan Data	Frekuensi pengumpulan informasi perangkat/GPS yang akan dikumpulkan
Frekuensi Detak Jantung Perangkat	Interval di mana perangkat harus menghubungi Server AppTec360 Min. 1 menit Max. 24 jam
Mengaktifkan Pembaruan Lokasi	Jika diaktifkan, perangkat akan mengirimkan pembaruan lokasi ke Server AppTec360
Waktu Pembaruan Lokasi	Menentukan dalam interval waktu berapa perangkat mengirimkan pembaruan lokasi ke AppTec
Gunakan Akurasi Lokasi Google untuk Pembaruan Lokasi	Jika diaktifkan, Akurasi Lokasi Google (sebelumnya dikenal sebagai lokasi jaringan) akan digunakan untuk pembaruan lokasi (jika ini dinonaktifkan di bawah "Pembatasan", maka pengaturan ini tidak akan memengaruhi apa pun)
Gunakan Lokasi GPS untuk Pembaruan Lokasi	Jika diaktifkan, GPS akan digunakan untuk pembaruan lokasi

Izinkan Lokasi Tiruan (Palsu)	Memungkinkan pemalsuan informasi lokasi melalui aplikasi pihak ketiga
Tindakan Kehilangan Koneksi	Memungkinkan Anda menetapkan tindakan tertentu yang akan dilakukan setelah sejumlah detak jantung gagal
Mode Penegakan Kebijakan	Menentukan seberapa agresif Klien AppTec360 meminta pengguna untuk melakukan tindakan tertentu yang memerlukan input pengguna. Interval (Default) = bertanya dalam interval, sehingga pengguna dapat meletakkannya di latar belakang untuk sementara waktu. Tidak Ada Peringatan = tidak ada popup untuk interaksi yang diperlukan. Anda harus membuka Klien AppTec360 secara manual untuk memeriksa apakah ada tindakan yang diperlukan Peringatan Konstan = Pengguna hanya dapat melakukan tindakan yang diperlukan. Klien AppTec360 akan memaksakan diri di latar depan jika pengguna mencoba menghindarinya
Kunci Versi AppTec360	Memungkinkan Anda menentukan versi Klien AppTec360 yang merupakan versi maksimum yang diperbarui oleh klien itu sendiri.

Wallpaper

Di sini Anda dapat menentukan wallpaper khusus.

"Tentukan Warna" memungkinkan Anda menentukan warna dalam format heksa (misalnya, #000000). Hanya nilai heksa yang diperbolehkan.

"Tetapkan Gambar sebagai Wallpaper" memungkinkan Anda mengunggah gambar. Perlu diketahui bahwa perangkat yang berbeda dengan peluncur dan versi OS yang berbeda, akan bekerja secara berbeda. Tidak ada garis panduan umum untuk ukuran dan rasio, karena hal ini tergantung pada perangkat.

Gunakan JPG (atau JPEG) atau PNG untuk format file.

Manajemen Aset (hanya pada tingkat perangkat)

Manajemen Aset

Info Perangkat

Model	**Penunjukan model perangkat**
Sistem Operasi	OS
Versi OS	Versi OS
Dukungan AE	Dukungan untuk Android Enterprise (Kontainer dan dikelola sepenuhnya)
Nomor Seri	Nomor seri
Nama Perangkat	Nama perangkat
Status Baterai	Status baterai
Memori Bebas / Total	Memori bebas / Total memori
Samsung KNOX	Tingkat API Samsung KNOX
Tersedia Kartu SD	Tersedia Kartu SD
Kartu SD Ditiru	Kartu SD ditiru
Kartu SD Dapat Dilepas	Kartu SD dapat dilepas
Memori Bebas SD / Total Memori	Memori SD Bebas / Total Kartu SD

Wi-Fi

Alamat IP	Alamat IP perangkat
MAC WiFi	Alamat MAC WiFi

Seluler

Status	Status (kartu SIM terpasang)
Nomor Telepon	Nomor Telepon
Roaming (Suara / Data)	Roaming untuk suara / data
Status Roaming	Status roaming saat ini
Alamat IP	Alamat IP
Operator/Pengangkut	Operator/Pengangkut
Teknologi Seluler	Teknologi Seluler
IMEI	Nomor IMEI
ICCID	Ini adalah ID untuk kartu SIM, yang sering kali juga merupakan Smartcard atau Kartu Sirkuit Terpadu (ICC)
IMSI	Identitas Pelanggan Seluler Internasional (IMSI) menyediakan identifikasi yang pasti bagi pengguna jaringan seluler GSM dan UMTS IMSI terdiri dari maksimum 15 digit dan dikonfigurasikan dengan cara berikut: • Kode Negara Seluler (Mobile Country Code (MCC)), 3 digit • Kode Jaringan Seluler (MNC), 2 atau 3 digit • Nomor Identifikasi Pelanggan Seluler (MSIN), 1-10 digit
PKS/MNC saat ini	Lihat "SIM MCC/MNC"
SIM PKS / MNC	Kode Negara Seluler adalah pengidentifikasi negara yang ditetapkan oleh ITU sesuai Standar E.212. Kode ini berfungsi bersama dengan Kode Jaringan Seluler (Mobile Network Code/MNC) untuk identifikasi jaringan seluler. Berarti negara/Kode Jaringan Seluler kartu SIM. Jika Anda roaming ke jaringan seluler lain, maka secara logika, "MCC/MNC saat ini" dan "MCC/MNC SIM", akan berbeda.

Bluetooth

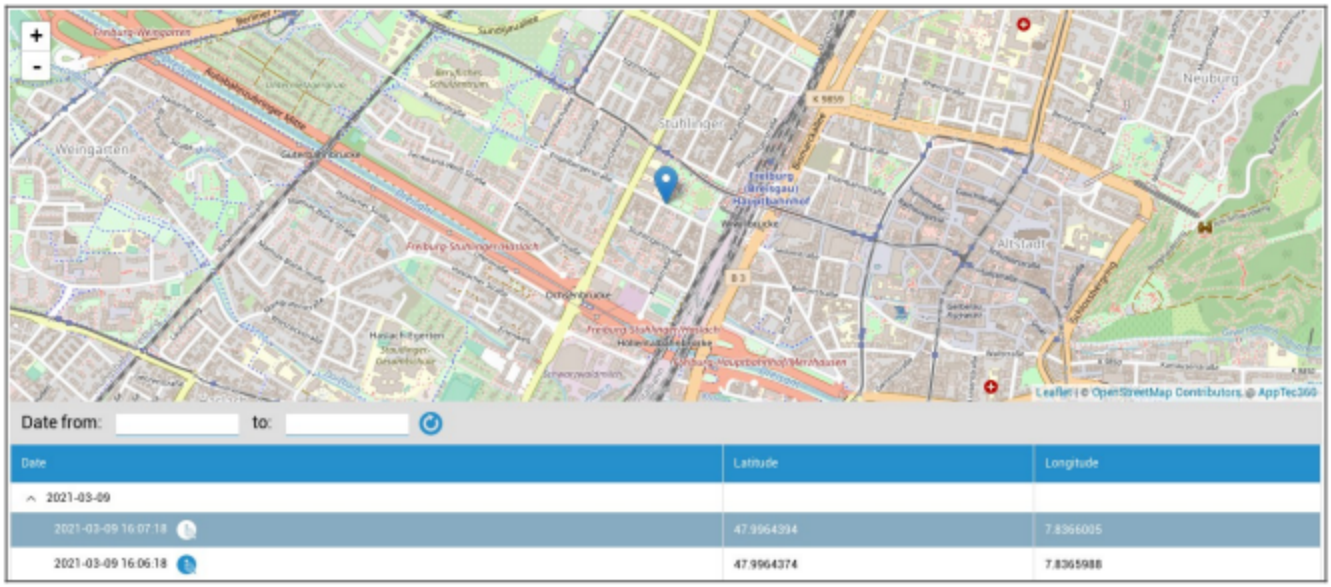
Bluetooth MAC	Alamat MAC Bluetooth

Manajemen Keamanan

Anti Pencurian (hanya pada tingkat perangkat)

Informasi GPS (hanya pada tingkat perangkat)

Di sini Anda dapat menetapkan lokasi perangkat saat ini/terakhir. Pelokalan dapat dilindungi dengan satu atau bahkan dua kata sandi - Lihat: Pengaturan Umum - Privasi - Akses GPS



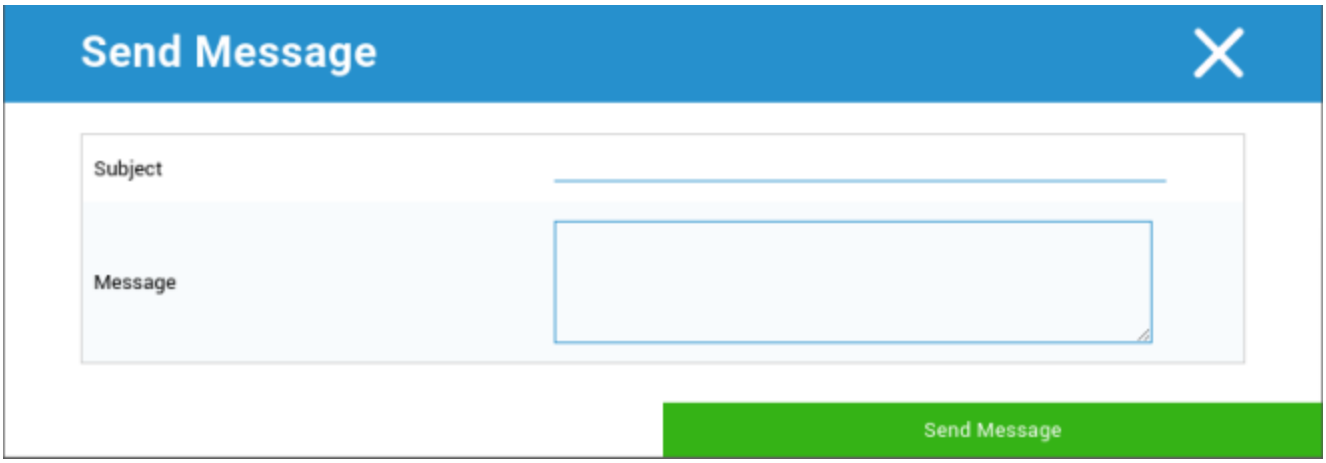
Hapus & Kunci (hanya pada tingkat perangkat)

Di bawah "Wipe & Lock", Anda dapat melakukan tiga tindakan berikut ini:

Penghapusan Penuh	Perangkat dipulihkan kembali ke pengaturan pabrik (data perusahaan dan data pribadi dihapus)
Penghapusan Perusahaan	Hanya data perusahaan yang dihapus dari perangkat pengguna akhir (semua aplikasi, data, dll. yang disediakan oleh AppTec360)
Layar Kunci	Kunci layar diaktifkan, cukup untuk membuka kunci perangkat dengan kata sandi/PIN perangkat

Pesan (hanya pada tingkat perangkat)

Anda dapat mengisi subjek dan pesan dan mengirimkannya ke perangkat pengguna akhir. Pesan ini akan ditampilkan di Klien AppTec360.



Konfigurasi Keamanan

Kode Sandi

Di bawah "Kode Sandi" Anda dapat mengamanatkan kata sandi perangkat, opsi pengaturan berikut tersedia untuk Anda

Panjang kata sandi minimum	Menetapkan, jumlah minimum simbol yang harus dimiliki kata sandi
Kualitas kata sandi	Kekuatan kata sandi Tidak ditentukan = tidak ditentukan Setiap kata sandi tidak masalah = setiap kata sandi dapat diterima setidaknya karakter numerik = harus berisi setidaknya karakter numerik setidaknya karakter kompleks = harus mengandung setidaknya karakter khusus setidaknya karakter alfanumerik = harus berisi setidaknya karakter alfanumerik setidaknya karakter alfabet = harus mengandung setidaknya karakter alfabet
Kunci waktu tidak aktif maksimum	Batas waktu layar maksimum. Ini hanya mengonfigurasi nilai maksimum yang dapat dipilih oleh pengguna
Huruf kecil minimum yang diperlukan dalam kata sandi	Huruf kecil minimum yang diperlukan dalam kata sandi
Huruf besar minimum yang diperlukan dalam kata sandi	Huruf besar minimum yang diperlukan dalam kata sandi
Karakter non-huruf minimum yang diperlukan dalam kata sandi	Karakter non-huruf minimum yang diperlukan dalam kata sandi
Digit numerik minimum yang diperlukan dalam kata sandi	Digit numerik minimum yang diperlukan dalam kata sandi
Simbol minimum yang diperlukan dalam kata sandi	Simbol minimum yang diperlukan dalam kata sandi
Batas waktu kedaluwarsa kata sandi	Menetapkan, setelah interval waktu mana kata sandi kedaluwarsa dan kata sandi baru harus dikeluarkan
Pembatasan riwayat kata sandi	Jumlah kata sandi yang pernah digunakan sebelumnya yang tidak diizinkan
Percobaan kata sandi maksimum yang gagal	Menetapkan, seberapa sering kata sandi dapat dimasukkan secara tidak benar, sebelum penghapusan perangkat secara menyeluruh akan dilakukan

Enkripsi

Di bawah titik ini, Anda dapat mengenkripsi memori perangkat internal, serta memori kartu SD.

Memerlukan Enkripsi Penyimpanan	Jika pengaturan ini diaktifkan, memori perangkat akan dienkripsi, selama perangkat mendukung fungsi ini. Setelah memori perangkat dienkripsi untuk pertama kalinya, maka tidak mungkin lagi untuk membuka enkripsi. Demikian juga, Kebijakan Kata Sandi akan secara otomatis dialihkan ke 6 simbol alfanumerik
Memerlukan Enkripsi Kartu SD	Pengaturan ini hanya berlaku untuk perangkat Samsung! Jika pengaturan ini diaktifkan, kartu SD eksternal dapat dienkripsi dan hanya dapat dibuka enkripsinya secara manual pada perangkat pengguna akhir. Demikian juga, Kebijakan Kata Sandi akan secara otomatis dialihkan ke 6 simbol alfanumerik

Anti Virus

Mengaktifkan AntiVirus akan menginstal Ikarus pada perangkat. Perlu diketahui bahwa hal ini memerlukan lisensi terpisah yang dapat dimasukkan di Pengaturan Umum → Manajemen Aplikasi → Aplikasi Pihak Ketiga.

Pemindaian Otomatis	Menentukan apakah Ikarus memindai secara otomatis atau tidak dan seberapa sering Ikarus melakukan pemindaian ini Mengaktifkan "Pemindaian Otomatis Penuh" akan melakukan pemindaian penuh. Jika tidak, pemindaian cepat akan dilakukan
Pembaruan Otomatis	Mengaktifkan pembaruan otomatis basis data virus dan mengatur seberapa sering hal ini terjadi
Perlindungan Aplikasi	Mengaktifkan Pemindaian Aplikasi selain Pemindaian biasa yang hanya memindai File
Perlindungan Kartu SD	Mengaktifkan Perlindungan Kartu SD. Tanpa ini, pemindaian terbatas pada penyimpanan lokal
Pembaruan Khusus Wi-Fi	Membatasi Pembaruan ke Wi-Fi

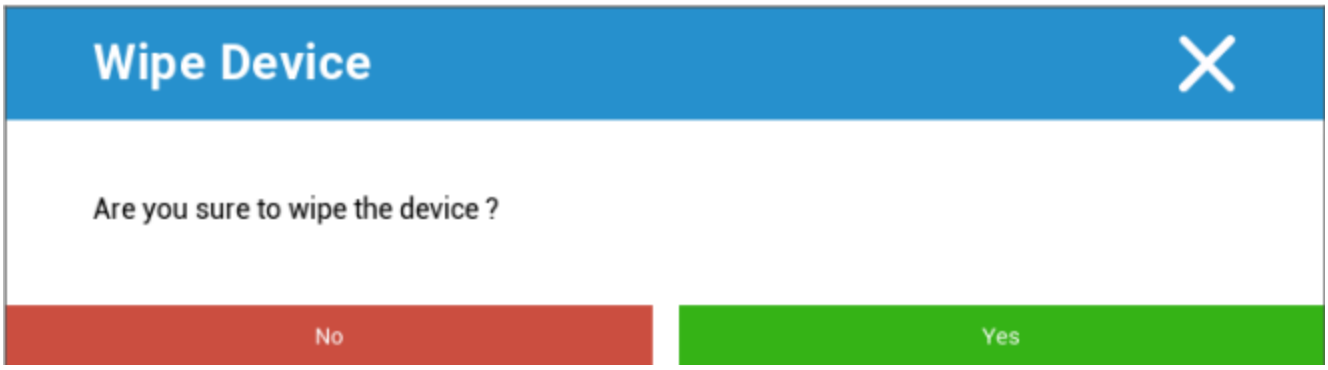
Akhir Masa Pakai (hanya pada tingkat perangkat)

Menghapus (hanya pada tingkat perangkat)

Di bawah "Hapus", Anda dapat memulihkan perangkat ke pengaturan pabrik. Di sini, data perusahaan dan data pribadi akan dihapus pada perangkat pengguna akhir.

Dengan mengklik "Simbol Minus", Anda akan menerima pesan berikut

Menghapus Kartu SD juga?	Memori kartu SD juga akan terhapus



Dengan "Ya", Anda dapat melakukan penghapusan.

Di bawah "Hapus Laporan", item berikut ini dapat ditampilkan

Dihapus oleh	Riwayat siapa yang melakukan penghapusan
Tanggal	Tanggal
Status	Status (mis. jika Penghapusan berhasil dilakukan)

Pengaturan Pembatasan

Pembatasan

Di sini, berbagai hal dapat dibatasi dan diblokir.

Aktifkan Kamera	Izinkan penggunaan kamera
Paksa Sinkronisasi Otomatis	Berkaitan dengan antarmuka "Sinkronisasi" On = sinkronisasi diaktifkan secara permanen Mati = sinkronisasi dinonaktifkan secara permanen Pilihan pengguna = dipilih oleh pengguna
Paksa Bluetooth	Aktif = Bluetooth diaktifkan secara permanen Mati = Bluetooth dinonaktifkan secara permanen Pilihan pengguna = dipilih oleh pengguna
Paksa GPS	Aktif = GPS diaktifkan secara permanen Mati = GPS dinonaktifkan secara permanen Pilihan pengguna = dipilih oleh pengguna
Memaksa Akurasi Lokasi Google	Aktif = Pelokalan internet permanen Off = Penonaktifan permanen pelokalan internet Pilihan pengguna = dipilih oleh pengguna

Untuk perangkat Samsung dengan antarmuka KNOX 1.0 atau yang lebih tinggi, opsi pengaturan berikut ini tersedia.

Izinkan Kartu SD	Izinkan Kartu SD
Izinkan Penulisan Kartu SD	Izinkan "tulis" pada Kartu SD
Izinkan Pengambilan Layar	Izinkan pengambilan layar
Izinkan Papan Klip	Izinkan papan klip
Mencadangkan pengaturan dan data aplikasi di Google Cloud	Nonaktif = menonaktifkan Pencadangan Google Aktif = aktifkan Cadangan Google Pilihan Pengguna = dipilih oleh pengguna
Izinkan Debugging USB	Izinkan Debugging USB (digunakan, misalnya, untuk pembuatan log perangkat (ADB))
Izinkan Laporan Kerusakan Google	Izinkan Laporan Kerusakan Google dikirim dari aplikasi
Izinkan Reset Pabrik	Memungkinkan pengguna mengembalikan perangkat ke pengaturan pabrik
Izinkan Peningkatan OTA	Izinkan Pembaruan "Melalui Udara"
Mengizinkan penyimpanan host USB	Jika diaktifkan, memori USB, dalam bentuk pembaca kartu HD atau SD, dapat dihubungkan
Izinkan Pemutar Media USB (MTP, PTP)	Izinkan Pemutar Media USB (MTP, PTP)
Izinkan Mikrofon	Aktif = mengizinkan mikrofon untuk Aplikasi Pihak Ketiga Mati = memblokir mikrofon untuk Aplikasi Pihak Ketiga Pilihan Pengguna = pengguna dapat memilih, jika Aplikasi Pihak Ketiga memiliki akses ke mikrofon
Izinkan NFC (Komunikasi Jarak Dekat)	Izinkan NFC
Izinkan Sumber Tidak Dikenal (Pemuatan Samping APK)	Jika diaktifkan, pemuatan Aplikasi (file APK) diperbolehkan. Setelah pengaturan ini dinonaktifkan, pengguna harus mengaktifkannya secara manual ketika Anda mengizinkan kembali pemasangan APK dari sumber yang tidak dikenal.
Izinkan Pembuatan Pengguna	Memungkinkan pembuatan beberapa pengguna

Pemilik Perangkat AE

(Perangkat harus dalam Mode Pemilik Perangkat Android Enterprise) Disarankan untuk membuat perangkat sebagai perangkat "Android Enterprise" dan bukan perangkat "Android".

Keamanan	
Membatalkan Lokasi Berbagi	Menentukan apakah pengguna dilarang mengaktifkan berbagi lokasi.
Tidak Mengizinkan Boot Aman	Menentukan apakah pengguna tidak diizinkan untuk mem-boot ulang perangkat ke mode boot aman.
Tidak Mengizinkan Pengaturan Ulang Jaringan	Menentukan apakah pengguna dilarang mengatur ulang pengaturan jaringan dari Pengaturan.
Membatalkan pengaturan ulang pabrik	Menentukan apakah pengguna dilarang mengatur ulang perangkat.
Mengaktifkan ADB	Memungkinkan Koneksi ke PC melalui ADB
Nonaktifkan Pelindung Kunci	Menonaktifkan Pelindung Kunci
Info Layar Kunci Pemilik Perangkat	Mengatur informasi pemilik perangkat yang akan ditampilkan pada layar kunci.
Penegakan Kepatuhan	Mode Prompt User - Pengguna akan diminta untuk memenuhi tindakan yang diperlukan. Mode Lock-Down Container - Sembunyikan semua aplikasi sampai semua persyaratan terpenuhi

Manajemen Aplikasi	
Izinkan Tautan Aplikasi Lintas Profil	Memungkinkan aplikasi di profil induk menangani tautan web dari profil yang dikelola.
Membatalkan Kontrol Aplikasi	Menentukan apakah pengguna dilarang memodifikasi aplikasi di Pengaturan atau peluncur.
Melarang Pemasangan Aplikasi	Menentukan apakah pengguna dilarang menginstal aplikasi.
Larang Menghapus Instalasi Aplikasi	Menentukan apakah pengguna dilarang menghapus instalasi aplikasi.
Kebijakan Izin Runtime	Menentukan bagaimana permintaan izin baru dari aplikasi akan ditangani.
Izinkan Sumber Tidak Dikenal	Jika diaktifkan, pengguna dapat memuat Aplikasi secara terpisah dengan menginstal file .apk.

Konektivitas	
Membatalkan Konfigurasi Jaringan Seluler	Menentukan apakah pengguna dilarang mengkonfigurasi jaringan seluler.
Tidak Mengizinkan Konfigurasi Penambatan	Menentukan apakah pengguna dilarang mengkonfigurasi Tethering & hotspot portabel.
Membatalkan Konfigurasi VPN	Menentukan apakah pengguna dilarang mengkonfigurasi VPN.
Nonaktifkan Konfigurasi Wifi	Menentukan apakah pengguna dilarang mengubah titik akses WiFi.
Memblokir Sinar NFC Keluar	Menentukan apakah pengguna tidak diizinkan menggunakan NFC untuk memancarkan data dari aplikasi.
Mengunci Konfigurasi WiFi	Pengaturan ini mengontrol apakah konfigurasi WiFi yang dibuat oleh aplikasi Pemilik Perangkat harus dikunci (yaitu, hanya dapat diedit atau dihapus oleh Aplikasi Pemilik Perangkat, bukan oleh aplikasi Pengaturan).
Mengaktifkan Roaming Data	Mengaktifkan Roaming Data

Bluetooth	
Nonaktifkan Bluetooth	Menentukan apakah bluetooth dilarang pada perangkat. Memerlukan Android 8.0
Melarang Berbagi Bluetooth	Menentukan apakah berbagi bluetooth keluar dilarang pada perangkat. Memerlukan Android 8.0
Nonaktifkan Konfigurasi Bluetooth	Menentukan apakah pengguna dilarang mengkonfigurasi bluetooth.

Manajemen Akun	
Melarang penambahan profil terkelola	Menentukan apakah pengguna dilarang menambahkan profil terkelola. Memerlukan Android 8.0
Melarang menambahkan Pengguna	Menentukan apakah pengguna dilarang menambahkan pengguna baru.
Tidak mengizinkan Hapus Profil Terkelola	Menentukan apakah profil terkelola dari pengguna ini dapat dihapus, selain oleh pemilik profil. Memerlukan Android 8.0
Melarang Modifikasi Akun	Menentukan apakah pengguna dilarang menambah dan menghapus akun, kecuali jika akun tersebut ditambahkan secara terprogram oleh Authenticator.

Telepon	
Melarang Panggilan Keluar	Menentukan bahwa pengguna tidak diizinkan melakukan panggilan telepon keluar.
Melarang SMS	Menentukan bahwa pengguna tidak diizinkan mengirim atau menerima pesan SMS.

Sistem	
Melarang Pembuatan Jendela	Menentukan bahwa jendela selain jendela aplikasi tidak boleh dibuat.
Membatalkan setelan Ikon Pengguna	Menentukan apakah pengguna tidak diizinkan untuk mengubah ikon mereka.
Membatalkan Pengaturan Wallpaper	Pembatasan pengguna untuk tidak dapat menetapkan wallpaper.
Nonaktifkan Bilah Status	Menonaktifkan bilah status akan memblokir notifikasi, pengaturan cepat, dan hamparan layar lainnya yang memungkinkan keluar dari perangkat sekali pakai.
Mengaktifkan Waktu Otomatis	Mengatur waktu secara otomatis.
Mengaktifkan Zona Waktu Otomatis	Mengatur zona waktu secara otomatis.
Tetap menyala saat dicolokkan	Perangkat akan tetap aktif selama terhubung ke sumber daya.

Penyimpanan	
Nonaktifkan nonaktifkan Verifikasi Aplikasi	Menentukan apakah pengguna dilarang menonaktifkan verifikasi aplikasi.
Melarang Memasang Media Fisik	Menentukan apakah pengguna dilarang memasang media eksternal fisik.
Mengaktifkan Layanan Cadangan	Layanan pencadangan mengelola semua mekanisme pencadangan dan pemulihan pada perangkat. Mengatur ini ke false (tidak benar) akan mencegah data dicadangkan atau dipulihkan. Layanan pencadangan dinonaktifkan secara default. Memerlukan Android 8.0
Mengaktifkan Penyimpanan Massal USB	Mengaktifkan penggunaan Penyimpanan Massal USB.

Keyboard	
Larang Pengisian Otomatis	Menentukan apakah pengguna tidak diizinkan menggunakan Layanan IsiOtomatis. Memerlukan Android 8.0
Larang Salin & Tempel antar Profil	Menentukan apakah yang disalin di papan klip profil ini dapat ditempelkan di profil terkait.

Suara	
Tidak Mengizinkan Penyesuaian Volume	Menentukan apakah pengguna dilarang menyesuaikan volume master.
Membolehkan Membunyikan Mikrofon	Menentukan apakah pengguna dilarang menyesuaikan volume mikrofon.
Membisukan Perangkat	Bisukan perangkat.

Kebijakan Pembaruan Sistem	
Kontrol Pembaruan OS	Aktifkan ini untuk mengatur perilaku pembaruan menjadi otomatis, berjendela, atau ditunda.

Wadah BYOD

Perusahaan Android

Perusahaan Android

Mengaktifkan Android Enterprise	Aktifkan Android Enterprise (AE). AE didukung sejak Android 5.1 dan yang lebih baru.
Penegakan Kepatuhan	Mode Prompt User - Pengguna akan diminta untuk memenuhi tindakan yang diperlukan. Mode Lock-Down Container - Sembunyikan semua aplikasi sampai semua persyaratan terpenuhi
Kebijakan Izin Runtime	Meminta pengguna untuk permintaan izin baru Selalu mengabulkan permintaan izin baru yang baru Selalu tolak permintaan izin baru Peringatan: Beberapa Aplikasi mengalami masalah dalam mengenali izin jika ini diatur secara otomatis. Jika Anda selalu memberikan izin dan mengalami masalah dengan aplikasi yang mengatakan bahwa izin tidak ada, atur ini ke "meminta pengguna" dan instal ulang aplikasi
Izinkan papan klip keluar	Memungkinkan salin dan tempel dari dalam wadah ke luar
Izinkan Resolusi ID Penelepon	Menampilkan nama untuk panggilan masuk berdasarkan kontak dalam wadah
Izinkan Resolusi Pencarian Kontak	Memungkinkan untuk mencari nama dalam kontak kontainer saat melakukan panggilan
Izinkan Berbagi Kontak Bluetooth	Memungkinkan akses ke kontak kontainer di dalam mobil
Memblokir Sinar NFC Keluar	Menonaktifkan NFC untuk Wadah
Izinkan Sumber Tidak Dikenal	Jika diaktifkan, pengguna dapat memuat Aplikasi secara terpisah dengan menginstal file .apk.
Izinkan Debugging USB	Jika diaktifkan, pengguna dapat mengaktifkan USB Debugging.
Melarang Modifikasi Akun	Melarang pembuatan, penghapusan, dan modifikasi Akun di dalam kontainer Perlu diingat bahwa beberapa aplikasi perlu membuat atau memodifikasi akun agar berfungsi seperti yang diharapkan

Pertukaran Gmail

Memungkinkan Anda mengonfigurasi Gmail di dalam Container. Perlu diketahui bahwa mengaktifkan konfigurasi ini tidak secara otomatis menginstal aplikasi. Anda masih harus menambahkan aplikasi ini sebagai aplikasi wajib.

Alamat email	Alamat email
Nama Host Server	Nama Host Server
Nama Login	Nama Login
Tanda tangan	Tanda tangan
Jumlah hari sebelumnya untuk disinkronkan	Jumlah hari sebelumnya untuk disinkronkan.
Pengenal Perangkat	Pengenal EAS. Biarkan ini kosong jika lingkungan Anda tidak memerlukannya
Gunakan Lapisan Soket Aman (SSL)	Mengaktifkan Penggunaan SSL. Menonaktifkan ini dapat menurunkan keamanan
Menerima semua sertifikat	Menerima semua sertifikat. Mengaktifkan ini dapat menurunkan keamanan
Izinkan akun yang tidak dikelola	Memungkinkan pengguna untuk menambahkan akun tambahan
Sertifikat Klien	Unggah sertifikat klien jika server Exchange Anda memerlukannya

Aplikasi Sistem AE

Di sini Anda dapat mengaktifkan Aplikasi Sistem untuk Wadah Perusahaan Android. Harap diingat bahwa aplikasi yang ditentukan harus ada dalam penyimpanan sistem, jika tidak, tidak akan terjadi apa-apa.

Kode Sandi Kontainer

Hanya untuk Android 7.0 atau lebih tinggi

Memungkinkan Anda mengatur persyaratan kata sandi tertentu untuk kontainer.

Panjang kata sandi minimum	Menetapkan, jumlah minimum simbol yang harus dimiliki kata sandi
Kualitas kata sandi	Kekuatan kata sandi Tidak ditentukan = tidak ditentukan Setiap kata sandi tidak masalah = setiap kata sandi dapat diterima setidaknya karakter numerik = harus berisi setidaknya karakter numerik setidaknya karakter kompleks = harus mengandung setidaknya karakter khusus setidaknya karakter alfanumerik = harus berisi setidaknya karakter alfanumerik setidaknya karakter alfabet = harus mengandung setidaknya karakter alfabet
Kunci waktu tidak aktif maksimum	Waktu Maksimum hingga kontainer terkunci. Ini hanya mengonfigurasi nilai maksimum yang dapat dipilih oleh pengguna
Huruf kecil minimum yang diperlukan dalam kata sandi	Huruf kecil minimum yang diperlukan dalam kata sandi
Huruf besar minimum yang diperlukan dalam kata sandi	Huruf besar minimum yang diperlukan dalam kata sandi
Karakter non-huruf minimum yang diperlukan dalam kata sandi	Karakter non-huruf minimum yang diperlukan dalam kata sandi
Digit numerik minimum yang diperlukan dalam kata sandi	Digit numerik minimum yang diperlukan dalam kata sandi
Simbol minimum yang diperlukan dalam kata sandi	Simbol minimum yang diperlukan dalam kata sandi
Batas waktu kedaluwarsa kata sandi	Menetapkan, setelah interval waktu mana kata sandi kedaluwarsa dan kata sandi baru harus dikeluarkan
Pembatasan riwayat kata sandi	Jumlah kata sandi yang pernah digunakan sebelumnya yang tidak diizinkan
Percobaan kata sandi maksimum yang gagal	Menetapkan, seberapa sering kata sandi dapat dimasukkan secara salah, sebelum wadah dihapus

Samsung KNOX

Aktivasi

Di sini Anda dapat mengaktifkan Samsung KNOX Container. Perlu diketahui bahwa hal ini tidak lagi didukung oleh Samsung pada Android 10 atau lebih tinggi. Gunakan Android Enterprise Container pada Android 10 atau lebih tinggi

Kode Sandi Knox

Menetapkan panduan yang berhubungan dengan pengaturan kata sandi perangkat

Panjang kata sandi minimum	Menetapkan, berapa banyak simbol yang harus dimiliki kata sandi
Kualitas kata sandi	Kekuatan kata sandi Setiap kata sandi baik-baik saja = Setiap kata sandi baik-baik saja Setidaknya karakter numerik = Karakter numerik minimum harus ada Setidaknya karakter kompleks = Karakter khusus minimum harus ada Minimal karakter alfanumerik = Karakter alfanumerik minimum harus ada Setidaknya karakter alfabet = Karakter alfabet minimum harus ada
Diperlukan karakter kompleks minimum	Karakter kompleks minimum harus ada
Batas Waktu Tidak Aktif Maksimum	Batas waktu tidak aktif pengguna maksimum, sebelum mengunci keyboard
Izinkan Otentikasi Sidik Jari	Mengizinkan autentikasi sidik jari
Izinkan Otentikasi Iris Mata	Memungkinkan autentikasi pengenalan iris mata
Usia Kata Sandi Maksimal	Menetapkan, setelah jam berapa kata sandi berakhir dan kata sandi baru harus dikeluarkan
Riwayat Kata Sandi yang Tersimpan	Jumlah kata sandi sebelumnya yang tidak diizinkan
Percobaan kata sandi maksimum yang gagal	Menetapkan, seberapa sering kata sandi mungkin dikirimkan secara tidak benar, sebelum penghapusan perangkat secara menyeluruh dilakukan

Keamanan Knox

Membatasi fungsi perangkat tertentu

Aktifkan Kamera	Izinkan penggunaan kamera

Izinkan Samsung KNOX App Store	Izinkan penggunaan Samsung KNOX App Store
Izinkan Layanan Google Play	Izinkan Layanan Google Play
Izinkan Browser	Izinkan penggunaan browser asli
Izinkan Tangkapan Layar	Izinkan pembuatan Tangkapan Layar
Izinkan Impor Kontak	Jika diaktifkan, akses kontak perangkat dari KNOX Container diperbolehkan
Izinkan Ekspor Kontak	Jika diaktifkan, akses ke kontak KNOX dari perangkat diperbolehkan
Izinkan Impor Kalender	Jika diaktifkan, akses kalender perangkat dari KNOX Container diperbolehkan
Izinkan Ekspor Kalender	Jika diaktifkan, akses ke kalender KNOX dari perangkat diperbolehkan
Izinkan Keypad yang Tidak Aman	Mengizinkan penggunaan Keypad yang Tidak Aman
Aktifkan Impor File	Aktifkan Impor File ke dalam Wadah KNOX
Mengaktifkan Ekspor File	Aktifkan Ekspor File dari Wadah KNOX

Pertukaran Knox

Di sini Anda dapat mengonfigurasi Exchange-Profile untuk KNOX Container

Alamat email	Alamat email pengguna yang diberikan Harap perhatikan "Placeholder", yang dapat Anda gunakan untuk bekerja dengan kredensial dan Anda tidak melakukan perubahan secara manual pada setiap perangkat Dengan mengeklik **Tampilkan Placeholder**, Anda dapat menampilkannya sendiri
Nama Host Server	Alamat server dari Server Exchange Anda
Nama login	Nama Login untuk masing-masing perangkat pengguna akhir, harap perhatikan juga "Placeholder" di sini
Domain	Alamat domain
Kata sandi (hanya pada tingkat perangkat)	Secara opsional, setiap perangkat dapat diberikan kata sandi, jika masih kosong, pengguna akan diminta untuk memasukkan Kata Sandi Exchange mereka
Jumlah hari sebelumnya untuk disinkronkan	Jumlah hari, menentukan kapan email disinkronkan kembali
Tanda tangan	Tanda tangan dapat dilampirkan
Akun Default	Menetapkan, bahwa akun email ini adalah akun standar
Gunakan Lapisan Soket Aman (SSL)	Gunakan koneksi SSL
Gunakan Transport Layer Security (TLS)	Gunakan koneksi TLS
Menerima semua sertifikat	Semua sertifikat diterima. Pilih opsi ini, jika Exchange Server Anda menggunakan sertifikat yang ditandatangani sendiri

Knox eMail

Alamat email	Alamat email pengguna yang diberikan Harap perhatikan "Placeholder", yang dapat Anda gunakan untuk bekerja dengan kredensial dan Anda tidak melakukan perubahan secara manual pada setiap perangkat Dengan mengeklik **Tampilkan Placeholder**, Anda dapat menampilkannya sendiri
Protokol server yang masuk	Protokol server yang masuk IMAP atau POP
Alamat server yang masuk	Alamat server yang masuk
Port server yang masuk	Port server yang masuk
Login/nama pengguna server yang masuk	Login/nama pengguna server yang masuk
Kata sandi server yang masuk	Kata sandi server yang masuk
Server yang masuk menggunakan SSL	Server yang masuk menggunakan SSL
Server masuk menggunakan TLS	Server masuk menggunakan TLS
Server yang masuk menerima semua sertifikat	Server yang masuk menerima semua jenis sertifikat
Protokol server keluar	Protokol server keluar SMTP
Port server keluar	Port server keluar
Server Keluar menggunakan kredensial tambahan	Kredensial tambahan untuk Server keluar. Jika ini diatur ke "off", maka pengaturan server masuk akan digunakan
Login/nama pengguna server keluar	Login/nama pengguna server keluar
Kata sandi server keluar	Kata sandi server keluar
Server keluar menggunakan SSL	Server keluar menggunakan SSL
Server keluar menggunakan TLS	Server keluar menggunakan TLS

Server keluar menerima semua sertifikat	Server keluar menerima semua jenis sertifikat
Tanda tangan	Di sini tanda tangan dapat dilampirkan
Memberi tahu pengguna saat menerima eMail baru	Memberi tahu pengguna saat menerima eMail baru

Aplikasi Knox

Buat aplikasi di sini yang ingin Anda distribusikan ke perangkat pengguna akhir. Aplikasi-aplikasi ini akan tersedia di KNOX-Container. Untuk menambahkan aplikasi, lanjutkan seperti yang Anda lakukan di menu Aplikasi Wajib

Nama Aplikasi	Nama Aplikasi
Wajib Sejak	Titik waktu, ketika aplikasi ditambahkan
Sumber	Sumber aplikasi (Play Store | In-House)

Dengan mengeklik simbol, masing-masing aplikasi dapat dihapus kembali

Manajemen Koneksi

Wifi

Untuk pengaturan ini, lakukan pra-konfigurasi perangkat pengguna akhir, untuk akses ke Titik Akses internal

Pengidentifikasi Set Layanan (SSID)	SSID untuk jaringan yang akan disambungkan
Jaringan Tersembunyi	Aktifkan, jika AP tidak menyiarkan SSID
Jenis Keamanan	Menetapkan jenis keamanan AP

Jenis Keamanan

WEP

Kata sandi	Kata sandi untuk AP

WPA/WPA2

Kata sandi	Kata sandi untuk AP

802.1x EAP

Metode EAP	

PENYANDANG DISABILITAS	Identitas	Identitas
	Kata sandi	Kata sandi

PEAP	Protokol Otentikasi Fase 2	tidak ada	Tidak ada protokol tambahan
		MSCHAPV2	Protokol MSCHAPV2
		GTC	Protokol GTC
	Sertifikat CA	Sertifikat CA	
	Identitas	Identitas	
	Identitas Anonim	Identitas anonim	
	Kata sandi	Kata sandi	

Metode EAP	

TTLS	Protokol Otentikasi Fase 2	tidak ada	Tidak ada protokol tambahan
		PAP	Protokol PAP
		MSCHAP	Protokol MSCHAP
		MSCHAPV2	Protokol MSCHAPV2
		GTC	Protokol GTC
	Sertifikat CA	Sertifikat CA	
	Identitas	Identitas	
	Identitas Anonim	Identitas Anonim	
	Kata sandi	Kata sandi	

TLS	Sertifikat CA	Sertifikat CA
	Identitas	Identitas
	Kata sandi	Kata sandi

VPN

Jenis Koneksi	**Menetapkan jenis koneksi VPN**

Jika Anda memilih "Per-App VPN" sebagai Jenis VPN, Klien VPN yang tersedia akan berubah. VPN Per-Aplikasi membatasi VPN untuk aplikasi tertentu dan memulai koneksi VPN secara otomatis jika aplikasi tertentu dimulai.

Klien VPN AppTec360	Menggunakan Klien VPN AppTec360 yang dikombinasikan dengan Universal Gateway
Nama Koneksi	Nama koneksi VPN
Konfigurasi Gateway	Pilih Konfigurasi VPN dari Universal Gateway
Selalu menggunakan VPN	Memaksa VPN untuk selalu aktif, sehingga seluruh lalu lintas melewati VPN.
Mengaktifkan Penguncian Asli	Memblokir semua jaringan ketika perangkat tidak terhubung ke VPN. Gunakan ini dengan hati-hati karena ini dapat menyebabkan terputusnya koneksi jika tidak dikonfigurasi dengan benar. Hanya untuk Android Enterprise pada Android 7 atau lebih tinggi
Aktifkan Penguncian AppTec360	Memblokir penggunaan semua Aplikasi hingga koneksi VPN dimulai

Cisco AnyConnect	
Nama Koneksi	Nama koneksi VPN
Server	Alamat server
Mode Sertifikat	Dinonaktifkan = dinonaktifkan Otomatis = otomatis

L2TP (Hanya KNOX)	Hanya tersedia di perangkat Samsung
Nama Koneksi	Nama koneksi
Server	Alamat server
Aktifkan Rahasia L2TP	
Domain Pencarian DNS	Domain pencarian DNS

Jenis Koneksi	**Menetapkan jenis koneksi VPN**

PPTP (Hanya KNOX)	Hanya tersedia di perangkat Samsung
Nama Koneksi	Nama koneksi VPN
Server	Alamat server
Mengaktifkan Enkripsi	Mengaktifkan enkripsi
Domain Pencarian DNS	Domain pencarian DNS

L2TP / IPSec PSK (Hanya KNOX)	Hanya tersedia di perangkat Samsung
Nama Koneksi	Nama koneksi VPN
Server	Alamat server
Kunci Pra-Berbagi IPSec	Kunci yang telah dibagikan sebelumnya untuk autentikasi
Aktifkan Rahasia L2TP	
Rahasia L2TP	
Domain Pencarian DNS	Domain pencarian DNS

IPSec XAuth PSK (Khusus KNOX)	Hanya tersedia di perangkat Samsung
Nama Koneksi	Nama koneksi VPN
Server	Alamat server
Pengidentifikasi IPSec	Nama pengguna untuk koneksi
Kunci Pra-Berbagi IPSec	Kata sandi untuk koneksi
Domain Pencarian DNS	Domain pencarian DNS

OpenVPN	
Nama Koneksi	Nama koneksi

Profil OpenVPN	Di sinilah konten file .ovpn akan disalin
Aplikasi OpenVPN	Ada dua aplikasi yang berbeda untuk penggunaan OpenVPN Kami merekomendasikan aplikasi "OpenVPN untuk Android". Tetapi sebagai alternatif, aplikasi "OpenVPN Connect" dapat digunakan

Pembatasan

Di sini Anda dapat menetapkan pembatasan, sehubungan dengan manajemen koneksi.

Izinkan Roaming Data	Izinkan data seluler saat roaming
Paksa Roaming Data	Jika diaktifkan, roaming untuk data seluler akan diaktifkan secara permanen (tidak disarankan!) Pengaturan ini menimpa pengaturan "Izinkan Data Roaming"!
Pengaturan berikut ini hanya tersedia pada Samsung KNOX 2.0 atau yang lebih tinggi	
Izinkan Panggilan Darurat Saja	Izinkan Panggilan Darurat Saja
Izinkan WiFi	Izinkan WiFi
Tingkat Keamanan Minimum Jaringan WiFi	Tingkat keamanan minimum jaringan WiFi Terbuka = semua jenis WiFi diizinkan
Melarang pengguna untuk menambahkan jaringan WiFi	Pengguna tidak boleh menambahkan jaringan WiFi sendiri Pengaturan ini hanya dapat dilakukan, jika profil WiFi ditentukan di bawah "Manajemen Koneksi"
Izinkan SMS & MMS	Semua = Semua lalu lintas SMS & MMS diperbolehkan Hanya SMS Masuk = Hanya pesan SMS masuk yang diperbolehkan Hanya SMS Keluar = Hanya pesan SMS keluar yang diperbolehkan Tidak ada = Tidak ada lalu lintas SMS / MMS yang diizinkan
Izinkan Sinkronisasi selama Roaming	Izinkan Sinkronisasi selama Roaming Aktif = diaktifkan Mati = dinonaktifkan Pilihan pengguna = pilihan pengguna
Izinkan Roaming Suara	Izinkan Roaming Suara Aktif = diaktifkan Mati = dinonaktifkan Pilihan Pengguna = pilihan pengguna
Gunakan Sistem http Server Proxy	Penggunaan server proxy HTTP, yang disediakan oleh pengaturan sistem dalam pengaturan, bergantung pada jaringan yang terhubung (WiFi atau APN)

APN

Pengaturan berikut ini hanya tersedia pada Samsung SAFE 2.0 atau yang lebih tinggi!

Nama Tampilan APN	Nama Tampilan APN	
Nama Titik Akses	Nama APN	
Protokol server keluar	Tidak diatur	
	Tidak ada	
	PAP	Protokol PAP
	BAB	Protokol CHAP
	PAP atau CHAP	Baik protokol PAP atau CHAP
MCC - Kode Negara Seluler	MCC dimasukkan di sini, biarkan bidang ini kosong, jika MCC kartu SIM yang dimasukkan harus digunakan	
MNC - Kode Jaringan Seluler	MNC dimasukkan di sini, biarkan bidang ini kosong, jika MNC kartu SIM yang dimasukkan harus digunakan	
Alamat server	Alamat server	
Nomor port server	Nomor port server	
Alamat proxy server	Alamat proxy server	
Alamat server MMS	Alamat server MMS, untuk Standar, silakan kosongkan	
Nomor port MMS	Nomor port MMS	
Alamat proxy MMS	Alamat proxy MMS	
Nama pengguna	Nama pengguna	
Kata sandi	Kata sandi	
Jenis Titik Akses	Jenis yang diizinkan adalah: "default", "mms", "supl" Jika bidang ini dikosongkan, maka "default,supl,mms" akan digunakan	
APN yang disukai	APN lebih disukai	

Bluetooth

Di sini, berbagai pengaturan Bluetooth dapat dilakukan.

Pengaturan berikut ini hanya tersedia pada Samsung KNOX 1.0 atau yang lebih tinggi!

Izinkan penemuan Perangkat melalui Bluetooth	Memungkinkan penemuan perangkat melalui Bluetooth
Izinkan Pemasangan Bluetooth	Izinkan pemasangan Bluetooth
Mengizinkan perangkat Headset Bluetooth	Mengizinkan perangkat Headset Bluetooth
Mengizinkan perangkat bebas genggam Bluetooth	Mengizinkan perangkat bebas genggam Bluetooth
Mengizinkan perangkat Bluetooth A2DP	Memungkinkan streaming audio Bluetooth A2DP antar perangkat
Mengizinkan Panggilan Keluar	Mengizinkan panggilan keluar melaluiBT
Izinkan Transfer Data melalui Bluetooth	Memungkinkan transfer data melalui Bluetooth
Izinkan Penambatan Bluetooth	Memungkinkan penggunaan perangkat sebagai modem (koneksi internet Bluetooth)
Izinkan koneksi ke Komputer melalui Bluetooth	Izinkan koneksi ke Komputer melalui Bluetooth

Manajemen PIM

Pertukaran

Hanya tersedia untuk Samsung KNOX 1.0 atau yang lebih tinggi!

Alamat email	Alamat email pengguna yang diberikan Harap perhatikan "Placeholder", yang dapat Anda gunakan untuk bekerja dengan kredensial dan Anda tidak melakukan perubahan secara manual pada setiap perangkat Dengan mengeklik **Tampilkan Placeholder**, Anda dapat menampilkannya sendiri
Nama Host Server	Alamat server dari Server Exchange Anda
Nama login	Nama Login untuk masing-masing perangkat pengguna akhir, harap perhatikan juga "Placeholder di sini
Domain	Alamat domain
Kata sandi (hanya pada tingkat perangkat)	Secara opsional, masing-masing perangkat dapat diberikan kata sandi, jika masih kosong, pengguna akan diminta untuk memasukkan Kata Sandi Exchange mereka
Jumlah hari sebelumnya untuk disinkronkan	Jumlah hari, menentukan kapan email disinkronkan kembali
Tanda tangan	Tanda tangan dapat dilampirkan (Petunjuk: Beberapa perangkat memerlukan format HTML untuk tanda tangan)
Akun Default	Menetapkan, bahwa akun email ini adalah akun standar
Gunakan Lapisan Soket Aman (SSL)	Gunakan koneksi SSL
Gunakan Transport Layer Security (TLS)	Gunakan koneksi TLS
Menerima semua sertifikat	Semua sertifikat diterima. Pilih opsi ini, jika Exchange Server Anda menggunakan sertifikat yang ditandatangani sendiri

eMail

Di sini, Anda dapat mendistribusikan akun IMAP dan POP ke masing-masing perangkat pengguna akhir.

Pengaturan berikut ini hanya tersedia pada Samsung KNOX 1.0 atau yang lebih tinggi!		
Alamat email	Alamat email pengguna yang diberikan Harap perhatikan "Placeholder", yang dapat Anda gunakan untuk bekerja dengan kredensial dan Anda tidak melakukan perubahan secara manual pada setiap perangkat Dengan mengeklik **Tampilkan Placeholder**, Anda dapat menampilkannya sendiri	
Protokol server yang masuk	Protokol server yang masuk	IMAP atau POP
Alamat server yang masuk	Alamat server yang masuk	
Port server yang masuk	Port server yang masuk	
Login/nama pengguna server yang masuk	Login/nama pengguna server yang masuk	
Kata sandi server yang masuk (hanya pada tingkat perangkat)	Kata sandi server yang masuk (hanya pada tingkat perangkat)	
Server yang masuk menggunakan SSL	Server yang masuk menggunakan SSL	
Server masuk menggunakan TLS	Server masuk menggunakan TLS	
Server yang masuk menerima semua sertifikat	Server yang masuk menerima semua jenis sertifikat	
Protokol server keluar	Protokol server keluar	SMTP
Port server keluar	Port server keluar	
Server Keluar menggunakan kredensial tambahan	Kredensial tambahan untuk server keluar. Jika ini diatur ke "off", maka pengaturan server masuk akan digunakan	
Login/nama pengguna server keluar	Login/nama pengguna server keluar	
Kata sandi server keluar (hanya pada tingkat perangkat)	Kata sandi server keluar	

Server keluar menggunakan SSL	Server keluar menggunakan SSL
Server keluar menggunakan TLS	Server keluar menggunakan TLS
Server keluar menerima semua sertifikat	Server keluar menerima semua jenis sertifikat
Tanda tangan	Tanda tangan dapat dilampirkan di sini (Petunjuk: Beberapa perangkat memerlukan format HTML untuk tanda tangan)
Memberi tahu pengguna saat menerima eMail baru	Memberi tahu pengguna saat menerima email baru

Pertukaran AE Gmail

Info: Konfigurasi ini akan diterapkan pada aplikasi Gmail. Jadi, Anda harus menyetujui dan menginstal Gmail.

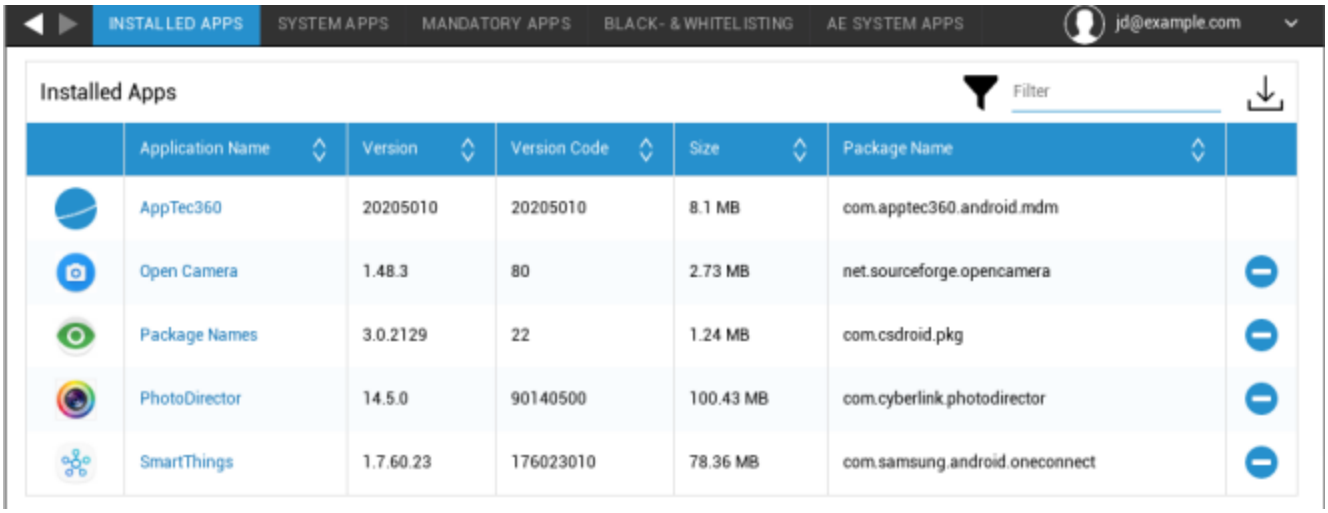
Alamat email	Alamat email pengguna yang diberikan Harap perhatikan "Placeholder", yang dapat Anda gunakan untuk bekerja dengan kredensial dan Anda tidak melakukan perubahan secara manual pada setiap perangkat Dengan mengeklik Tampilkan Placeholder, Anda dapat menampilkannya sendiri
Nama Host Server	Alamat server dari Server Exchange Anda
Nama login	Nama Login untuk masing-masing perangkat pengguna akhir, harap perhatikan juga "Placeholder di sini
Tanda tangan	Tanda tangan dapat dilampirkan (Petunjuk: Beberapa perangkat memerlukan format HTML untuk tanda tangan)
Jumlah hari sebelumnya untuk disinkronkan	Jumlah hari, menentukan kapan email disinkronkan kembali
Pengenal Perangkat	Pengenal EAS. Biarkan ini kosong jika lingkungan Anda tidak memerlukannya
Gunakan Lapisan Soket Aman (SSL)	Gunakan koneksi SSL
Menerima semua sertifikat	Semua sertifikat diterima. Pilih opsi ini, jika Exchange Server Anda menggunakan sertifikat yang ditandatangani sendiri
Izinkan akun yang tidak dikelola	Memungkinkan pengguna untuk menambahkan akun tambahan
Sertifikat Klien	Unggah sertifikat klien jika server Exchange Anda memerlukannya

Manajemen Aplikasi

Manajer Aplikasi Perusahaan

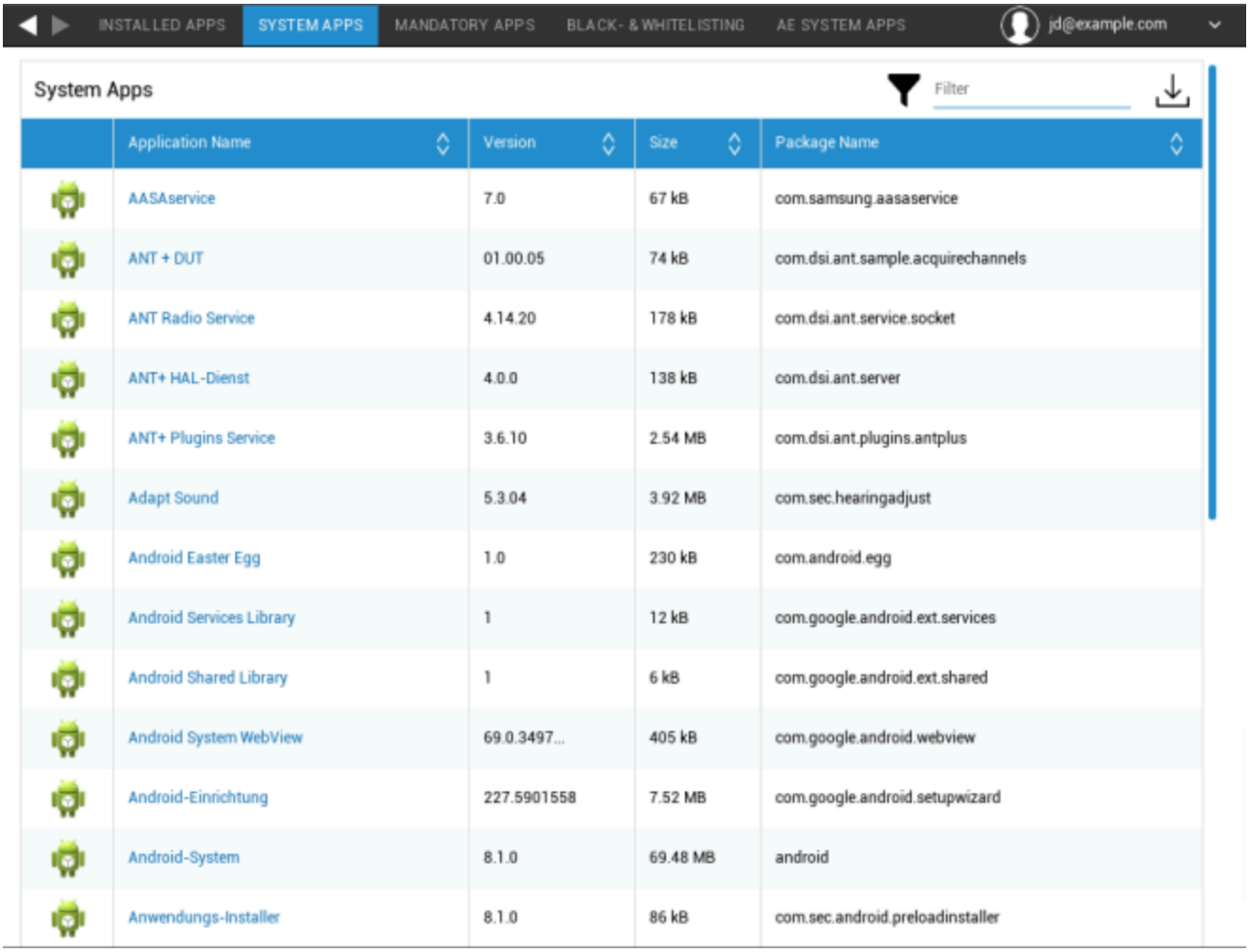
Aplikasi Terinstal (hanya pada tingkat perangkat)

Di sini semua Aplikasi akan ditampilkan untuk Anda yang saat ini terinstal pada perangkat pengguna akhir.


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

Aplikasi Sistem (hanya pada tingkat perangkat)

Di bawah "Aplikasi Sistem", semua sistem yang sudah terinstal akan dicantumkan dengan nama paket dan versinya.



Aplikasi Wajib

Di Aplikasi Wajib Anda dapat menentukan aplikasi mana yang harus diinstal pada perangkat. Tergantung pada konfigurasi dan perangkat Anda, aplikasi akan diinstal secara otomatis atau pengguna akan diminta untuk menginstalnya.

Perlu diketahui bahwa disarankan untuk menggunakan Android Enterprise untuk manajemen aplikasi yang mudah.

Skenario tersebut seperti yang tercantum di bawah ini:

Aplikasi Play Store Normal

Instalasi Aplikasi Playstore selalu membutuhkan interaksi pengguna. Selain itu, Akun Google harus dikonfigurasi pada perangkat.

Instalasi Aplikasi InHouse

Pada Perangkat Samsung, aplikasi ini akan diinstal secara diam-diam. Satu-satunya pengecualian adalah kontainer, di mana pengguna harus mengonfirmasi penginstalan.

Dalam skenario lain, pengguna harus mengonfirmasi instalasi aplikasi.

Aplikasi Play Store Perusahaan Android

Aplikasi ini akan selalu terinstal secara diam-diam, tanpa interaksi pengguna.

Untuk Menambahkan aplikasi wajib, klik "+" dan pilih aplikasi yang diinginkan dari daftar. Perlu diketahui bahwa Anda tidak dapat menginstal aplikasi dari Tab "Google Play Store", jika perangkat dikonfigurasikan dengan Android Enterprise baik sebagai dikelola sepenuhnya atau sebagai kontainer.

Jika menggunakan Android Enterprise, pilih aplikasi dari bagian "AE Play Store". Untuk membuat aplikasi tersedia di sini, konfirmasikan aplikasi di Google Enterprise Play Store dengan membuka Pengaturan Umum → AE Play Store → Aplikasi Play Store.

Ketika menghapus aplikasi wajib, aplikasi tersebut juga akan dihapus dari perangkat.

Anda dapat mengklik nama aplikasi dalam daftar aplikasi wajib dan membuka tab "konfigurasi" untuk mengonfigurasi aplikasi. Hal ini memerlukan penggunaan Android Enterprise dan aplikasi harus mendukungnya. Oleh karena itu, opsi yang tersedia tergantung pada aplikasi yang dipilih.

Aplikasi Sistem AE

Di sini Anda dapat mengaktifkan Aplikasi Sistem untuk perangkat Android Enterprise. Harap diingat bahwa aplikasi yang ditentukan harus ada di penyimpanan sistem, jika tidak, tidak akan terjadi apa-

apa. 296

Pembatasan & Pengaturan

Daftar Hitam & Putih

Di sini Anda dapat menentukan daftar hitam atau daftar putih. Semua aplikasi yang ada di daftar hitam akan diblokir. Semua aplikasi yang tidak ada dalam daftar putih akan diblokir. Daftar hitam yang kosong tidak akan memblokir apa pun, sedangkan daftar putih yang kosong akan memblokir semuanya*.

**Semua aplikasi wajib dan aplikasi dari Enterprise App Store akan dimasukkan ke dalam daftar putih secara otomatis. Anda tidak perlu menambahkannya secara manual*

Ketika mengklik "+", Anda dapat mencari aplikasi yang ingin Anda tambahkan ke daftar hitam atau putih atau memasukkan nama paket secara manual.

Pembatasan Aplikasi Sys

Di bawah "Pembatasan Aplikasi Sys" Anda dapat, antara lain, memblokir aplikasi dan layanan yang sudah diinstal sebelumnya, sesuai keinginan.

Nonaktifkan Browser	Menonaktifkan browser standar
Menonaktifkan Kalender	Menonaktifkan kalender asli
Nonaktifkan Kalkulator	Menonaktifkan kalkulator
Nonaktifkan Browser Chrome	Nonaktifkan browser Chrome
Nonaktifkan Jam	Nonaktifkan jam
Menonaktifkan Kontak	Menonaktifkan Kontak
Nonaktifkan Dialer	Menonaktifkan dialer asli
Menonaktifkan eMail	Menonaktifkan email
Nonaktifkan Pertukaran	Menonaktifkan akun Exchange
Nonaktifkan Facebook	Menonaktifkan aplikasi Facebook
Nonaktifkan Galeri	Menonaktifkan aplikasi galeri asli
Menonaktifkan Gmail	Menonaktifkan Gmail
Menonaktifkan Google Buku	Menonaktifkan Google Buku
Nonaktifkan Google Play Kios	Nonaktifkan Google Play Kios
Nonaktifkan Google Maps	Nonaktifkan Google Maps
Nonaktifkan Google Musik	Nonaktifkan Google Musik
Nonaktifkan Film Google	Nonaktifkan Film Google
Nonaktifkan Google Play Store	Menonaktifkan Google Play Store (App Store publik)
Nonaktifkan Google Plus	Nonaktifkan Google Plus
Nonaktifkan Pencarian Google	Nonaktifkan Pencarian Google
Nonaktifkan Google Talk / Google Hangouts	Nonaktifkan Google Talk / Google Hangouts
Menonaktifkan Pemutar Musik	Menonaktifkan aplikasi pemutar musik asli
Menonaktifkan Pengaturan	Menonaktifkan pengaturan perangkat
Nonaktifkan Perangkat Sim	Menonaktifkan layanan Sim Toolkit
Menonaktifkan SMS / MMS	Menonaktifkan SMS / MMS
Menonaktifkan Street View	Menonaktifkan layanan Street View
Nonaktifkan Youtube	Nonaktifkan Youtube

Aplikasi Samsung

Di bawah "Samsung Apps", Anda dapat menentukan pengaturan dan/atau pembatasan tambahan untuk perangkat Samsung.

Nonaktifkan AllShare Play / Samsung Link	Nonaktifkan AllShare Play / Samsung Link
Menonaktifkan ChatON	Menonaktifkan ChatON
Menonaktifkan Game Hub	Menonaktifkan Game Hub
Menonaktifkan Bermain Grup	Menonaktifkan Bermain Grup
Menonaktifkan Bantuan	Menonaktifkan Bantuan Samsung
Nonaktifkan KNOX	Nonaktifkan Wadah Samsung KNOX
Menonaktifkan Memo	Menonaktifkan Memo Suara
Nonaktifkan File Saya	Nonaktifkan File Saya
Menonaktifkan Pembaca Optik	Menonaktifkan Pembaca Optik
Menonaktifkan Kantor Polaris	Menonaktifkan Kantor Polaris
Menonaktifkan Hub Pembaca / Buku Samsung	Menonaktifkan Hub Pembaca / Buku Samsung
Menonaktifkan S Memo	Menonaktifkan aplikasi Samsung Memo
Menonaktifkan Penerjemah S	Menonaktifkan aplikasi Samsung Translator
Menonaktifkan S Voice	Nonaktifkan S Asisten suara
Menonaktifkan Aplikasi Samsung	Nonaktifkan Samsung App Store
Menonaktifkan Samsung Hub	Menonaktifkan Toko Hiburan Samsung
Menonaktifkan Pemutar Video	Menonaktifkan Pemutar Video
Menonaktifkan Perekam Suara	Menonaktifkan Perekam Suara
Menonaktifkan WatchON	Nonaktifkan WatchON (mensimulasikan remote control)

Aplikasi Huawei

Di bawah "Aplikasi Huawei", Anda dapat menentukan pengaturan dan/atau pembatasan tambahan pada perangkat Huawei.

Menonaktifkan DLNA	Menonaktifkan DLNA
Nonaktifkan Pemasang Aplikasi	Nonaktifkan Pemasang Aplikasi
Nonaktifkan Manajer File	Nonaktifkan Manajer File
Nonaktifkan Manajer Pencadangan	Nonaktifkan Manajer Pencadangan
Nonaktifkan Pembaruan Sistem	Nonaktifkan Pembaruan Sistem
Nonaktifkan Kotak Alat	Nonaktifkan Kotak Alat
Nonaktifkan Cuaca	Nonaktifkan Cuaca
Menonaktifkan Radio FM	Menonaktifkan Radio FM

Pengaturan Manajemen Aplikasi

Di sini Anda dapat menentukan perilaku pembaruan Aplikasi InHouse.

Frekuensi Pemeriksaan Pembaruan menentukan seberapa sering Aplikasi AppTec360 mencari pembaruan untuk aplikasi InHouse. Setelah versi baru terdeteksi, versi tersebut akan diunduh dan diinstal.

Ambang Batas Wi-Fi menentukan apakah pengunduhan harus dibatasi pada koneksi Wi-Fi jika Aplikasi lebih besar daripada Ambang Batas yang Anda konfigurasikan. Jika lebih kecil atau Anda tidak menentukan ambang batas, aplikasi akan diunduh dalam Wi-Fi dan jaringan seluler.

Toko Aplikasi Perusahaan

Perlu diketahui bahwa aplikasi yang ditambahkan di sini (Enterprise App Store) TIDAK akan membuat aplikasi tersebut terinstal secara otomatis di perangkat. Pengguna harus membuka Enterprise App Store pada perangkat dan menginstal aplikasi secara manual.

Jika Anda ingin menginstal Aplikasi secara otomatis pada perangkat, silakan buka "Manajemen Aplikasi" → "Manajer Aplikasi Perusahaan" → "Aplikasi Wajib" dan tambahkan aplikasi yang diinginkan di sana.

Di bawah poin ini, Anda dapat mendistribusikan Aplikasi opsional kepada pengguna Anda.

Playstore

Klik "+" untuk menambahkan aplikasi Play Store ke toko. Jika menggunakan Android Enterprise, buka "Manajemen Aplikasi Play Store Enterprise". Perlu diketahui juga bahwa Akun Google harus dikonfigurasi pada → perangkat untuk menginstal aplikasi yang ditentukan di sini.

In-House

Di bawah poin "In-House", Anda dapat mengunggah dan mendistribusikan aplikasi yang dikembangkan secara internal.

Klik "+" untuk menambahkan aplikasi InHouse ke toko aplikasi perusahaan yang kemudian dapat diinstal oleh pengguna. Dalam dialog ini Anda juga dapat mengunggah aplikasi InHouse baru.

Perusahaan Play Store

Perlu diketahui bahwa aplikasi yang ditambahkan di sini (Enterprise Play Store) TIDAK akan membuat aplikasi tersebut terinstal secara otomatis di perangkat. Pengguna harus membuka Play Store pada perangkat dan menginstal aplikasi secara manual.

Jika Anda ingin menginstal Aplikasi secara otomatis pada perangkat, silakan buka "Manajemen Aplikasi" → "Manajer Aplikasi Perusahaan" → "Aplikasi Wajib" dan tambahkan aplikasi yang diinginkan di sana.

Di bawah poin ini, Anda dapat mendistribusikan Aplikasi opsional kepada pengguna Anda.

Di sini Anda dapat menambahkan Aplikasi ke Android Enterprise Playstore. Harap diperhatikan bahwa Anda harus menyetujui Aplikasi di Pengaturan Umum → AE Play Store → Aplikasi Play Store. Aplikasi ini akan ditambahkan ke Google Play Store biasa.

Perlu diketahui juga, bahwa Anda harus terlebih dulu menentukan Tata Letak dengan Aplikasi di Pengaturan Umum → Manajemen Aplikasi → AE Play Store → Tata Letak Toko.

Aplikasi harus berada di Layout sebelum Anda berhasil menambahkannya ke toko.

Mode Kios & Peluncur

Mode Kios

Mode Kios memungkinkan Anda untuk menentukan terlebih dahulu aplikasi atau URL. Kemudian secara eksklusif hanya dapat menjalankan/mengunjungi aplikasi dan atau URL ini.

Demikian juga, berbagai tombol perangkat keras dapat dinonaktifkan dalam Mode Kios yang beragam.

Mulai Otomatis	Secara otomatis memulai Mode Kios, segera setelah profil mencapai perangkat pengguna akhir
Mode Kios Terjadwal?	Anda dapat merencanakan waktu untuk Mode Kios, yang kemudian akan dimulai dan diakhiri secara otomatis, pada waktu yang Anda tentukan
Waktu Mulai	Waktu mulai
Waktu dalam menit	Waktu dalam menit, setelah itu Mode Kios akan berakhir lagi

Jenis Aplikasi

Aplikasi Tunggal	Jika Anda ingin memulai Aplikasi dalam Mode Kios, pilih Paket" di bawah "Jenis Aplikasi"
Aplikasi Kios	Klik di sini, untuk memilih aplikasi yang harus dimulai dalam Mode Kios Anda akan menemukan gambaran umum Manajemen Aplikasi yang biasa Anda dapat memilih antara "Google Play Store", "Aplikasi In-House Android", dan "Packagename"

Jenis Aplikasi

URL	Jika Anda ingin meluncurkan URL dalam Mode Kios, pilih "URL" di bawah "Jenis Aplikasi" Kemudian tentukan alamat URL yang Anda inginkan
Menghapus browser setelah tidak aktif	Di sini Anda dapat menentukan interval waktu dalam menit, setelah itu Mode Kios harus diluncurkan kembali
Menghapus Tembolok dan Cookie Web	Jika Anda mengaktifkan fungsi ini, maka setelah memulai ulang Mode Kios, Cache Web (cookie dan gambar yang di-cache) akan dihapus
Kebijakan Asal yang Sama	Jika fungsi ini aktif, maka pengguna hanya dapat menjelajahi subhalaman dari URL yang ditentukan Misalnya, Anda menetapkan URL berikut:www.mypage.com Kemudian, pengguna dapat berselancar di: www.mypage.com/subpage
URL yang masuk daftar putih	Di sini Anda dapat mengelola Daftar Putih, semua URL ini diizinkan Maksimum 1 URL per baris URL harus dimulai dengan http:/ atau https://
URL yang masuk daftar hitam	Di sini Anda dapat mengelola Daftar Hitam, semua URL ini tidak diizinkan Maksimum 1 URL per baris URL harus dimulai dengan http:/ atau https://
Orientasi Layar	Pengaturan ini berkaitan dengan penyesuaian layar Otomatis = otomatis Potret = format vertikal Lanskap = mode lanskap

Multi Aplikasi	Jika Anda memilih Mode Kios "Multi Aplikasi", penggunaan Peluncur AppTec360 akan diberlakukan.
Aplikasi	Aplikasi: Pilih Playstore atau Aplikasi In-House sebagai Aplikasi Kios. Anda juga dapat memasukkan nama paket. Aplikasi Kios yang dipilih harus diinstal pada perangkat. Ingatlah untuk mengatur Aplikasi Kios sebagai wajib. Pintasan pada Layar Beranda: Jika diatur ke "On", pintasan pada homescreen akan dibuat. Jika diatur ke "Nonaktif", Aplikasi akan tetap muncul di Daftar Aplikasi.

Kata Sandi Keluar Diaktifkan	Jika Anda mengaktifkan fungsi ini, maka pengguna dapat mengakhiri Mode Kios dengan kata sandi yang telah Anda tentukan sebelumnya
Keluar dari Kata Sandi	Ini adalah kata sandi yang telah Anda tentukan sebelumnya
Bilah Status Tutup Otomatis	Jika diaktifkan, Status Bar akan secara otomatis ditutup. Dengan opsi tersebut, pengguna dapat melihat informasi di Status Bar, tetapi tidak dapat mengakses fungsinya
Nonaktifkan Bilah Status	Status Bar berisi Pemberitahuan, Pintasan, dan Informasi. Hanya tersedia untuk perangkat Samsung dengan KNOX 1.0 atau yang lebih tinggi.
Menonaktifkan Tombol Volume	Nonaktifkan tombol volume (hanya tersedia pada perangkat Samsung dengan KNOX 1.0 atau lebih tinggi)
Nonaktifkan Sakelar Hidup / Mati	Nonaktifkan sakelar Nyala/Mati (hanya tersedia pada perangkat Samsung dengan KNOX 1.0 atau lebih tinggi)
Nonaktifkan Tombol Beranda	Nonaktifkan tombol Beranda. Jika fungsi ini telah diaktifkan, maka Mode Kios hanya dapat diakhiri di Konsol AppTec360 (hanya tersedia pada perangkat Samsung dengan KNOX 1.0 atau lebih tinggi)
Menonaktifkan Bilah Navigasi	Dengan ini, Anda dapat menonaktifkan Bilah Navigasi (Kembali/Menu) Jika fungsi ini telah diaktifkan, maka Mode Kios hanya dapat diakhiri di Konsol AppTec360 (hanya tersedia pada perangkat Samsung dengan KNOX 1.0 atau lebih tinggi)

Pengaturan Pembaruan Aplikasi	
Izinkan Pembaruan Aplikasi	Pengguna akan diminta untuk melakukan pembaruan aplikasi bahkan ketika Mode Kios aktif. Pada perangkat dengan Samsung KNOX, aplikasi akan diperbarui secara diam-diam.
Jendela Pembaruan	Tetapkan interval di mana pengguna akan diminta untuk menginstal pembaruan aplikasi.

Penampil Tim	
Mengaktifkan Akses Tanpa Pengawasan	Jika diaktifkan, administrator dapat mengontrol perangkat dari jarak jauh tanpa interaksi pengguna. Aplikasi TeamViewer Host harus diinstal pada perangkat.

Peluncur AppTec360

Aktifkan Peluncur AppTec360	Aktif: Mengaktifkan Peluncur AppTec360. Pengguna harus mengaturnya sebagai Peluncur default satu kali. Catatan: Jika Mode Kios diaktifkan, dan Mode Kios diatur ke "Multi App", penggunaan peluncur AppTec360 akan diberlakukan.
Ikon Besar	Aktif: Menampilkan Versi Ikon Aplikasi yang lebih besar di Peluncur
Sembunyikan Ikon Aplikasi AppTec360	Aktif: Menyembunyikan Aplikasi AppTec360 sepenuhnya
Sembunyikan Ikon Toko AppTec360	Aktif: Menyembunyikan AppTec360 Enterprise AppStore sepenuhnya

Pengaturan AppTec360

Aktifkan Aplikasi Pengaturan AppTec360	Aplikasi Pengaturan AppTec360 menyediakan kontrol atas koneksi WiFi dan Bluetooth
Mengaktifkan Pengaturan di Multi Aplikasi Mode Kios	Jika diaktifkan, pengguna dapat mengakses Aplikasi Pengaturan AppTec360 saat Mode Kios Multi Aplikasi aktif

Kontrol Jarak Jauh

Splashtop

Menampilkan status saat ini dari Splashtop Setup (Pengaturan Splashtop). Di sini Anda akan melihat langkah-langkah yang perlu Anda lakukan untuk mengakses perangkat dari jarak jauh melalui Splashtop. Di sini Anda juga perlu memasukkan kode deploy yang bisa Anda dapatkan dari situs web Splashtop. Kode deploy diperlukan untuk menyambungkan ke perangkat.

Peninjau tim

Menampilkan status saat ini dari Pengaturan Teamviewer. Di sini Anda akan melihat langkah-langkah yang perlu Anda lakukan untuk mengakses perangkat dari jarak jauh melalui Teamviewer.

Manajemen Konten

Kotak konten

Di sini Anda dapat mengaktifkan Contentbox untuk perangkat ini. Setelah diaktifkan, Aplikasi Contentbox akan diinstal pada perangkat.

Peramban yang Aman

Di sini Anda dapat mengaktifkan Peramban Aman untuk perangkat ini. Setelah diaktifkan, Aplikasi Peramban Aman akan diinstal pada perangkat. Browser ini dapat dikonfigurasi untuk menawarkan Browser Web pada perangkat yang terbatas pada kebutuhan Anda.

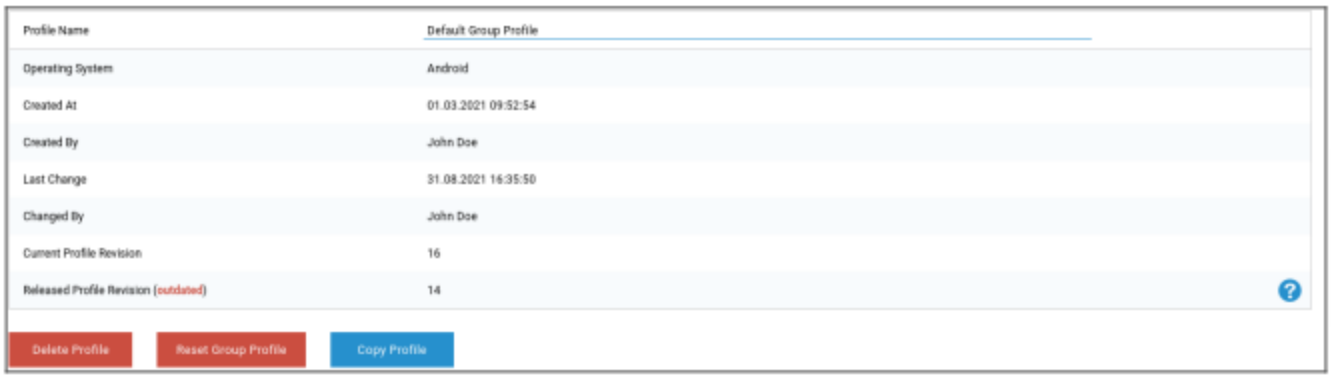
Memerlukan Kata Sandi	Mengharuskan pengguna untuk mengatur dan menggunakan kata sandi untuk mengakses browser.
Batasi Unduhan / Buka Dalam	Memblokir Unduhan dari Situs Web
Membatasi Unggahan	Membatasi Unggahan ke URL tertentu. Tidak memberikan URL untuk memblokir Unggahan sepenuhnya
Izinkan Salin	Memungkinkan menyalin, memotong, atau berbagi teks di dalam halaman web.
Izinkan Pengambilan Layar	Izinkan pengambilan tangkapan layar.
Frekuensi pembersihan data	Pilih dengan frekuensi yang mana, SEMUA data pengguna (riwayat, cache, dll.) harus dihapus secara otomatis.
Penanda Perusahaan	Penanda akan muncul di folder "Penanda perusahaan" di penanda browser. Penanda ini tidak dapat diedit oleh pengguna.
Sembunyikan Bilah Alamat	Menyembunyikan Bilah Alamat sehingga Pengguna tidak melihat URL yang dikunjungi
Daftar Putih Dalam Peramban (tanpa Gerbang Universal)	Mengaktifkan daftar putih URL sisi klien. - Penanda Perusahaan selalu masuk daftar putih - Didukung untuk 100 URL saja - Silakan gunakan Gerbang Universal untuk Daftar Hitam dan Daftar Putih tanpa batas
Daftar Hitam dan Putih berbasis gateway	Daftar hitam memiliki persyaratan sebagai berikut: - AppTec360 Universal Gateway yang berfungsi ("Pengaturan Umum" → "Universal Gateway") - Konfigurasi VPN yang berfungsi dengan server DNS yang ditentukan ("Pengaturan Umum" → "Universal Gateway" → "Pengaturan VPN") - Konfigurasi Daftar Hitam ("Pengaturan Umum" → "Universal Gateway" → "Domain Blacklist") - Sambungan VPN yang valid di profil ("Manajemen Koneksi" → "VPN")

Konfigurasi PC Windows 10

Umum

Ikhtisar profil grup (hanya pada tingkat grup)

Ketika membuka profil grup, Anda akan mendapatkan ikhtisar singkat profil.



Nama Profil	Nama profil (dapat diubah di sini)
Sistem Operasi	Sistem Operasi profil ini untuk
Dibuat di	Waktu pembuatan
Dibuat oleh	Pembuat profil
Perubahan Terakhir	Waktu perubahan terakhir pada profil
Diubah oleh	Akun yang melakukan perubahan terakhir
Revisi Profil Saat Ini	Revisi status profil yang disimpan
Revisi Profil yang Dirilis	Menetapkan revisi profil ("Tetapkan sekarang"). Jika label menunjukkan "(usang)" di belakang teks, itu berarti Anda telah menyimpan profil tetapi belum menetapkannya, sehingga perangkat masih akan mendapatkan versi yang lebih lama.

Ikhtisar Perangkat (hanya pada tingkat perangkat)

Ikhtisar ringkasan perangkat, yang berisi hal-hal berikut ini:

Nama PC	Nama PC
Klien	Perangkat tipe Windows
Lokasi Terakhir Diketahui	Lintang dan bujur dari lokasi terakhir perangkat yang diketahui
Aplikasi Wajib yang Ditetapkan	Jumlah Aplikasi Wajib yang ditetapkan ke perangkat
UID PC	UID dari PC
Edisi OS	Menampilkan Edisi Windows Anda
Versi OS	Versi Windows yang saat ini diinstal
Membangun OS	Versi Windows saat ini
Sistem Operasi	Sistem Operasi yang saat ini diinstal
Nomor Seri	Nomor Seri Perangkat
Kepemilikan Perangkat	Jenis Kepemilikan yang dikonfigurasi
Jenis Perangkat	Jenis Perangkat
Berakar	Menunjukkan apakah Perangkat telah di-root
Sesuai	Menunjukkan apakah perangkat sudah sesuai
Terakhir terlihat	Tanggal dan waktu, saat perubahan dilakukan pada profil
Penugasan Pengguna	Menampilkan pengguna atau grup yang saat ini ditetapkan untuk perangkat ini. Anda dapat memindahkan perangkat dengan memilih pengguna atau grup yang berbeda dari daftar tarik-turun.

Pengaturan

Izinkan Pembaruan Otomatis	Mengizinkan atau melarang pembaruan OS otomatis.

Revisi Konfigurasi (hanya pada tingkat perangkat)

Di sini Anda akan menerima ikhtisar profil grup mana yang ditetapkan ke perangkat.

Jika Anda mengklik profil grup, Anda akan mengakses profil secara langsung dan dapat melakukan pengaturan.

Dengan simbol ini, Anda dapat mengembalikan aplikasi yang ditetapkan ke pengaturan profil grup.

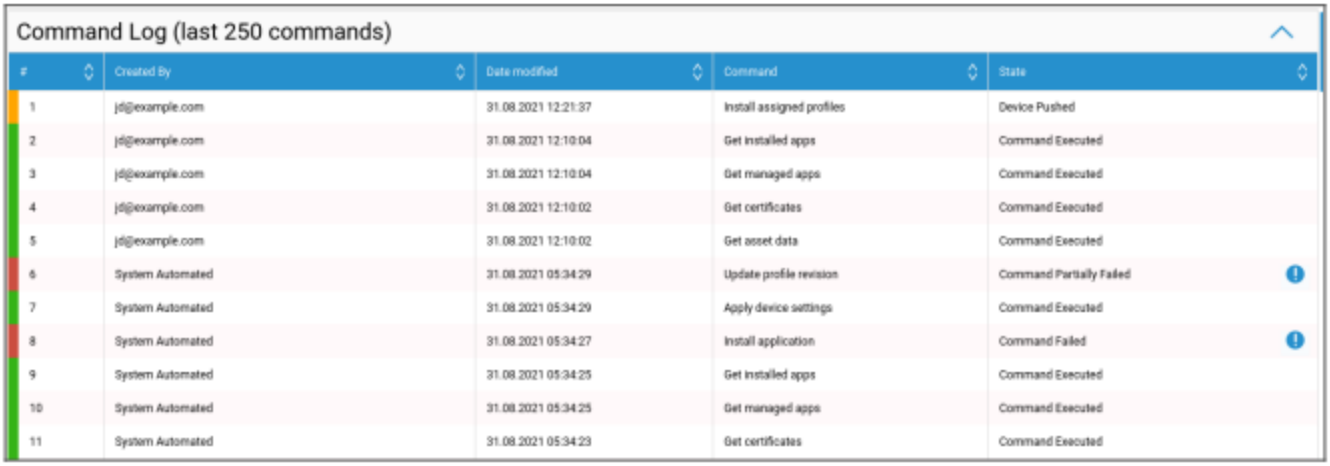
Dengan simbol tersebut, Anda dapat mengatur ulang profil perangkat agar tidak memiliki pengaturan sama sekali.

"Revisi terbaru tersedia" menunjukkan bahwa profil grup telah diubah dan disimpan namun belum ditetapkan. Profil grup harus ditetapkan dengan "Tetapkan sekarang" pada tingkat grup untuk menerapkan perubahan ke perangkat.

Log Perangkat (hanya pada tingkat perangkat)

Log Perintah

Di sini Anda dapat melihat perintah mana yang dikeluarkan untuk perangkat dan bagaimana statusnya.



Perintah yang dibuat oleh "System Automated" secara otomatis dibuat oleh sistem.

Kemungkinan status perintah

Perangkat Didorong	Permintaan push telah dikirim ke layanan push (misalnya APNS) untuk memberi tahu perangkat agar terhubung kembali ke server EMM.
Perintah Dibuat	Perintah ini dibuat dalam sistem.
Perintah Terkirim	Perintah dikirim ke perangkat setelah perangkat terhubung ke server.
Perintah Dieksekusi	Perintah berhasil dijalankan.
Perintah Gagal	Perintah gagal. *
Perintah Gagal Sebagian	Tergantung pada OS perangkat, beberapa perintah mungkin akan dikelompokkan bersama. Dalam hal ini, beberapa bagian dari grup perintah ini gagal. *
Perintah Dieksekusi, akhirnya Gagal	Perintah itu dijalankan tetapi mungkin tidak.
Perintah Ditolak	Perintah tersebut ditolak oleh pengguna.
Dibuang	Perintah telah dibuang. Misalnya karena digantikan oleh perintah lain atau perangkat didaftarkan ulang dan perintah lama dihapus

*Jika terdapat tanda seru di belakang pesan, Anda dapat memperoleh informasi lebih lanjut dengan mengarahkan kursor ke ikon tersebut.

Manajemen Aset (hanya pada tingkat perangkat)

Info Perangkat

Produsen	Produsen perangkat
Model	Model perangkat
Nomor Model	Nomor Model
Sistem Operasi	Sistem operasi
Versi OS	Versi OS
Nomor Seri	Nomor Seri
ExchangeID	ExchangeID
Total RAM	Total RAM
Resolusi Tampilan	Resolusi tampilan
Bahasa Telepon	Bahasa perangkat
Versi Firmware	Versi firmware
Versi Klien DM	Versi Klien Manajemen Perangkat
Versi Perangkat Keras	Versi perangkat keras perangkat
Arsitektur CPU	Arsitektur CPU (jenis prosesor)

Seluler

Jaringan Operator SIM	Jaringan operator
Nomor Telepon	Nomor Telepon
Status Roaming	Status Roaming
IMEI	IMEI
IMSI	IMSI
Firmware Modem	Firmware Modem

Info Sinkronisasi

Koneksi DM Instan	Perangkat harus segera membuat koneksi ke AppTec
Waktu Coba Ulang Awal	Waktu percobaan ulang awal untuk koneksi pertama ini
Mencoba Ulang Koneksi	Jumlah percobaan ulang koneksi baru, setelah pemutusan koneksi dari Connection Manager atau kesalahan tingkat WinInet
Waktu Tidur Maksimum	Waktu tidur maksimum setelah kesalahan pengiriman paket
Mencoba Ulang Sinkronisasi Pertama	Waktu untuk tahap pertama setelah pendaftaran
Interval Percobaan Ulang Pertama	Waktu untuk tahap pertama setelah pendaftaran
Mencoba Ulang Sinkronisasi Kedua	Waktu untuk tahap kedua setelah pendaftaran
Interval Coba Ulang Kedua	Waktu untuk tahap kedua setelah pendaftaran
Mencoba Ulang Sinkronisasi Reguler	Waktu untuk tahapan tambahan setelah pendaftaran
Interval Coba Ulang Reguler	Waktu untuk tahapan tambahan setelah pendaftaran

Manajemen Keamanan

Anti Pencurian (hanya pada tingkat perangkat)

Informasi GPS (hanya pada tingkat perangkat)

Di sini Anda dapat menetapkan lokasi perangkat saat ini/terakhir. Pelokalan dapat dilindungi dengan satu atau bahkan dua kata sandi - Lihat: "Pengaturan Umum" > "Privasi" > "Akses GPS"

Pengaturan GPS

Aktifkan Pelacakan GPS	Mengaktifkan sinkronisasi informasi GPS secara teratur.
Interval Pelacakan	Mengatur interval sinkronisasi informasi GPS.

Konfigurasi Keamanan

Kode Sandi

Panjang Kata Sandi Minimum	Panjang kata sandi minimum	
Komposisi Kata Sandi	Menentukan jumlah karakter tertentu yang harus ada dalam kata sandi Ini terdiri dari huruf besar, huruf kecil, angka, dan simbol khusus	
Kualitas Kata Sandi	Di sini Anda dapat mengatur kualitas kata sandi	
	Alfanumerik	Hanya angka dan huruf
	Numerik	Hanya angka
	Numerik atau Alfanumerik	Angka atau angka dan huruf
Kunci Waktu Tidak Aktif Maksimum	Jumlah menit pengguna tidak aktif pada perangkat, setelah itu perangkat akan terkunci. Pengguna harus membuka kunci perangkat setelah waktu ini, dengan memasukkan kata sandi perangkat.	
Kedaluwarsa Kata Sandi	Mengatur waktu hingga kata sandi baru harus ditetapkan	
Pembatasan Riwayat Kata Sandi	Jumlah kata sandi yang pernah digunakan sebelumnya, yang tidak diizinkan	
Upaya Kata Sandi Maksimum yang Gagal	Berapa kali kata sandi salah dimasukkan, sebelum perangkat dibersihkan sepenuhnya	

Antivirus

Pengaturan antivirus - Mengatur konfigurasi pemindaian	
Jenis pemindaian	Memilih apakah akan melakukan pemindaian cepat atau pemindaian penuh
Mengatur mulai pemindaian	Memilih waktu pada hari dimana Windows Defender akan memulai pemindaian
Frekuensi pemindaian	Memilih hari pemindaian Windows Defender harus dijalankan
Frekuensi pembaruan tanda tangan	Menentukan interval dalam jam yang akan digunakan untuk memeriksa tanda tangan

Jenis file konfigurasi untuk pemindaian	
Memungkinkan pemindaian file arsip	Mengizinkan atau melarang pemindaian arsip (seperti .zip) saat diakses.
Memungkinkan pemindaian skrip	Mengizinkan atau melarang fungsionalitas Pemindaian Skrip Windows Defender.
Izinkan pemindaian email	Mengizinkan atau melarang pemindaian email.
Memungkinkan pemindaian file jaringan	Mengizinkan atau melarang pemindaian file jaringan.
Memungkinkan pemindaian penuh terhadap drive jaringan yang dipetakan	Mengizinkan atau melarang pemindaian drive jaringan yang dipetakan (hanya diaktifkan bila pemindaian penuh diaktifkan).
Kontrol pemindaian dua arah	Mengontrol kumpulan file mana yang harus dipantau.
Memungkinkan pemindaian penuh pada drive yang dapat dilepas	Mengizinkan atau melarang pemindaian penuh pada drive yang dapat dilepas. Hanya selama pemindaian penuh dimulai.

Jenis file yang akan dikecualikan dari pemindaian	
Abaikan jenis file untuk pemindaian	Tentukan satu set jenis ekstensi file. Setiap ekstensi file untuk setiap bidang.
Abaikan jalur direktori	Tentukan satu set jalur direktori agar tidak memindainya. Satu jalur per bidang. Contoh: "C:\Example", "C:\Windows", atau "C:\Users".
Mengecualikan proses dari pemindaian	Mengecualikan file yang telah dibuka oleh proses tertentu dari pemindaian Microsoft Defender Antivirus. . Satu jalur per bidang. Contoh: "C:\myFile.exe", "C:\Windows\myProcess.exe", "C:\myScript.bat

Pengaturan Ekstra	
Memungkinkan pemantauan waktu nyata	Mengizinkan atau melarang fungsionalitas Pemantauan Realtime Windows Defender
Izinkan pemantauan Perilaku	Mengizinkan atau melarang fungsionalitas Pemantauan Perilaku Windows
Izinkan Perlindungan Cloud	Mengizinkan atau melarang Windows Defender mengirim informasi ke Microsoft tentang masalah apa pun yang ditemukannya. Microsoft akan menganalisis informasi tersebut, mempelajari lebih lanjut tentang masalah yang memengaruhi perangkat, dan menawarkan solusi yang lebih baik
	Perilaku untuk mengirim sampel
Izinkan perlindungan Windows Defender IOAV	Mengizinkan atau melarang perlindungan Windows Defender IOAV
Izinkan akses ke UI "Perlindungan Akses Aktif" Pembela	
Faktor beban CPU rata-rata	Mewakili faktor beban CPU rata-rata untuk pemindaian Windows Defender (dalam persen)

Penanganan malware	
Tingkat keparahan rendah	Anda dapat menentukan untuk setiap tingkat keparahan bagaimana perangkat menangani malware. Opsi yang tersedia adalah: • Bersih • Karantina • Menghapus • Izinkan • Ditentukan oleh pengguna • Blokir
Tingkat keparahan sedang	
Tingkat keparahan tinggi	
Tingkat keparahan yang parah	
Hari untuk mempertahankan Malware yang telah dibersihkan	Periode waktu dalam hari di mana file/item karantina akan disimpan di sistem. Nilai defaultnya adalah 0, yang membuat item tetap dalam karantina, dan tidak secara otomatis menghapusnya. Nilai maksimum adalah 90.

Pusat Keamanan

Pusat Keamanan Windows - Pengaturan untuk Keamanan Windows	
Nonaktifkan UI perlindungan virus & ancaman	
Sembunyikan UI Pemulihan Data Ransomware	
Nonaktifkan UI perlindungan akun	
Nonaktifkan Firewall dan UI perlindungan Jaringan	
Menonaktifkan UI kontrol Aplikasi dan Browser	
Membatalkan perubahan pada perlindungan Eksploitasi	Melarang pengguna untuk membuat perubahan pada pengaturan perlindungan Eksploitasi
Menonaktifkan UI keamanan perangkat	
Sembunyikan pemecahan masalah TPM	Menyembunyikan pengaturan pemecahan masalah TPM
Nonaktifkan tombol Hapus TPM	
Menonaktifkan kinerja perangkat dan UI kesehatan	
Menonaktifkan UI opsi keluarga	

Sesuaikan Roti Bakar	
Mengaktifkan info dukungan yang disesuaikan	Aktifkan untuk menampilkan info kontak dukungan yang disesuaikan untuk perusahaan Anda di bagian kanan bawah aplikasi pusat keamanan.
Alamat email	Mengatur alamat email perusahaan
Nama perusahaan	Tetapkan nama perusahaan
Telepon perusahaan	Mengatur telepon perusahaan
URL Bantuan	Mengatur URL bantuan perusahaan

Pengaturan Ekstra	
Menonaktifkan notifikasi	Nonaktifkan tampilan Pemberitahuan Pusat Keamanan Windows Defender.
Menyembunyikan rekomendasi pembaruan firmware TPM	Sembunyikan rekomendasi untuk memperbarui Firmware TPM ketika firmware yang rentan terdeteksi.
Menampilkan nama perusahaan dan opsi kontak	Tampilkan nama perusahaan dan opsi kontak Anda di kartu kontak yang keluar di Pusat Keamanan Windows Defender.
Sembunyikan Boot Aman	Menyembunyikan area Boot Keamanan.
Menyembunyikan kontrol area pemberitahuan keamanan	Menyembunyikan kontrol area notifikasi Keamanan Windows.

Konfigurasi Firewall

Konfigurasi firewall - Pengaturan global	
Abaikan set otentikasi	Abaikan seluruh rangkaian autentikasi jika tidak mendukung semua rangkaian autentikasi yang ditentukan dalam rangkaian tersebut
Jenis antrian paket	Menentukan bagaimana penskalaan untuk perangkat lunak di sisi penerimaan diaktifkan untuk penerimaan terenkripsi dan menghapus jalur maju untuk skenario gateway terowongan IPsec.
Nonaktifkan melakukan pemfilteran FTP yang sesuai dengan keadaan	Jika dinonaktifkan, maka tidak akan melakukan pemfilteran Protokol Transfer File (FTP) untuk mengizinkan koneksi sekunder
Waktu menganggur asosiasi keamanan	Bidang ini mengkonfigurasi waktu idle asosiasi keamanan, dalam detik. Asosiasi keamanan dihapus setelah lalu lintas jaringan tidak terlihat selama periode waktu yang ditentukan ini.
Pengkodean kunci yang telah disandikan sebelumnya	Mengatur pengkodean kunci yang telah di-preshared
Pengecualian IPSec	Mengonfigurasi pengecualian Protokol Internet
Pemeriksaan daftar pencabutan sertifikat	

Profil Firewall (Profil Domain / Profil Pribadi / Profil Publik)	
Aktifkan Firewall untuk profil ini	
Menonaktifkan notifikasi	Nonaktifkan menampilkan notifikasi kepada pengguna ketika aplikasi diblokir untuk mendengarkan pada port.
Memblokir respons unicast ke siaran multicast	
Menerapkan aturan firewall aplikasi yang diotorisasi	Jika tidak diberlakukan, aturan firewall aplikasi resmi di toko lokal akan diabaikan dan tidak diberlakukan
Menerapkan aturan firewall port global	Jika tidak diberlakukan, aturan firewall port global di toko lokal diabaikan dan tidak diberlakukan. Pengaturan hanya memiliki arti jika diatur atau dicacah di penyimpanan Kebijakan Grup atau jika dicacah dari penyimpanan GroupPolicyRSoPStore
Menerapkan aturan firewall	Jika tidak diberlakukan, aturan firewall dari toko lokal akan diabaikan dan tidak diberlakukan
Menerapkan aturan keamanan koneksi	Jika tidak diberlakukan, aturan keamanan koneksi dari toko lokal akan diabaikan dan tidak diberlakukan
Tindakan keluar default	Tindakan yang dilakukan firewall secara default pada koneksi keluar
Tindakan masuk default	Tindakan yang dilakukan firewall secara default pada koneksi masuk
Menonaktifkan mode Stealth	Mode siluman adalah mekanisme di Windows Firewall yang membantu mencegah pengguna jahat menemukan informasi tentang komputer jaringan dan layanan yang mereka jalankan.
Menonaktifkan pencegahan agar tidak merespons lalu lintas yang tidak diminta	Jika dinonaktifkan, aturan mode siluman firewall tidak boleh mencegah komputer host merespons lalu lintas jaringan yang tidak diminta jika lalu lintas tersebut diamankan oleh IPsec

Aturan Firewall

Aturan Firewall	
Nama	Nama aturan
Deskripsi	Deskripsi aturan
Tindakan	Tentukan apakah aturan ini akan memblokir lalu lintas, atau mengizinkannya. Harap pertimbangkan bahwa opsi Blokir juga dapat memblokir lalu lintas (tergantung pada konfigurasi lainnya) antara server MDM dan Perangkat
Arah	
Aktifkan Edge traversal (Hanya tersedia jika **Arah** diatur ke **lalu lintas masuk**)	Menunjukkan bahwa lalu lintas masuk tertentu diizinkan untuk melakukan tunneling di seluruh NAT dan perangkat edge lainnya menggunakan teknologi tunneling Teredo.

Program & layanan	
Tentukan aplikasi, semua sebaliknya	Jika tidak diaktifkan, maka akan mempertimbangkan semua aplikasi
Paket Nama Keluarga	Nama Keluarga Paket yang akan diterapkan aturan tersebut.
Jalur file aplikasi	Aplikasi lengkap seperti C:\Windows\System\Notepad.exe yang akan diterapkan aturan
Nama Biner yang Memenuhi Syarat	Nama Biner Berkualifikasi Penuh yang akan diterapkan oleh aturan. FQBN adalah sebuah string dalam bentuk berikut: {Penerbit\Produk\Nama File,Versi}
Nama Layanan	Masukkan nama Layanan (misalnya "EventLog"). Anda bisa mendapatkan daftar Nama Layanan di Powershell dengan menjalankan perintah "Get-Service".

Protokol & port				
Protokol	Protokol yang digunakan oleh aturan.			
	Nilai yang tersedia: - Apa saja - Kustom - HOPORT - ICMPv4 - IGMP - TCP - UDP - IPv6 - Rute IPv6 - IPv6-Frag - GRE - ICMPv6 - IPv6-NoNxt - Opsi IPv6 - VRRP - PGM - L2TP	Apabila diatur ke Custom (Khusus)	Masukkan nomor protokol antara 0 dan 255	Nomor protokol
		Apabila diatur ke TCP atau UDP	Tentukan port lokal, jika tidak, semua akan digunakan	Port lokal yang akan digunakan aturan, port rentang juga diperbolehkan
			Pelabuhan Lokal	Port tunggal atau serangkaian port. Misalnya 100-120,200,300-320.
			Tentukan port jarak jauh, jika tidak, semua akan digunakan	Port jarak jauh yang akan digunakan aturan, port jangkauan juga diperbolehkan
			Port Jarak Jauh	Port tunggal atau serangkaian port. Misalnya 100-120,200,300-320.

Cakupan	
Tentukan IP lokal, IP apa pun jika tidak	Kumpulan IP lokal, dapat juga berupa rentang IP yang dipisahkan oleh -
Alamat IP lokal	Kumpulan IP tunggal atau serangkaian IP yang dipisahkan oleh -
Tentukan IP jarak jauh, IP jarak jauh apa pun jika tidak	Tentukan satu set IP jarak jauh, bisa juga serangkaian IP yang dipisahkan dengan "-".
Alamat IP jarak jauh	Menentukan IP tunggal atau rentang IP
Token	Token yang dapat diatur bersama dengan Alamat Jarak Jauh. Token Intranet, RmtIntranet, dan Ply2Renders didukung pada Windows 10, versi 1809 dan yang lebih baru.

Pengaturan Lanjutan

Tentukan profil, semua akan digunakan jika tidak	Jika dinonaktifkan, semua profil akan digunakan
Domain	Profil Domain
Pribadi	Profil Pribadi
Publik	Profil Publik
Tentukan antarmuka, semua akan digunakan jika tidak	Jika dinonaktifkan, semua antarmuka akan digunakan
Jaringan Area Lokal	Antarmuka Jaringan Area Lokal
Akses Jarak Jauh	Antarmuka Akses Jarak Jauh
Nirkabel	Antarmuka nirkabel

Kepala Sekolah Lokal	
Menambahkan pengguna lokal yang diotorisasi	Izinkan untuk menambahkan daftar pengguna lokal yang akan menggunakan aturan ini
Pengguna yang berwenang	Daftar pengguna lokal yang diotorisasi untuk aturan ini. Pengguna harus dalam format Security Description Definition Language (SDDL), misalnya PC_NAME\USERNAME. Bidang ini tidak boleh diisi jika nama layanan diatur untuk menggunakan aturan ini

Pengaturan Pembatasan

Fungsionalitas Perangkat

Izinkan Kartu SD	Mengizinkan penggunaan kartu SD
Izinkan Kamera	Izinkan penggunaan kamera
Izinkan Layanan Lokasi	Mengizinkan layanan lokasi perangkat
Izinkan Pemuatan Aplikasi di Samping	Mengizinkan penginstalan Aplikasi dari sumber yang tidak dikenal
Izinkan Mode Pengembang	Mengizinkan mode pengembang
Izinkan Roaming Data Seluler	Mengizinkan roaming data seluler
Izinkan Cortana	Izinkan asisten suara Cortana
Izinkan Pencarian menggunakan Lokasi	Izinkan pencarian menggunakan lokasi
Izinkan Menambahkan Akun Email Non Microsoft	Tentukan apakah pengguna diizinkan untuk menambahkan akun email non-MSA.
Izinkan Koneksi Akun Microsoft	Tentukan apakah mengizinkan penggunaan akun MSA untuk autentikasi dan layanan koneksi yang tidak terkait email.
Izinkan Sinkronisasi Pengaturan Saya	Memungkinkan sinkronisasi pengaturan di seluruh perangkat
Nama Domain yang Dilindungi Perusahaan	Menentukan nama domain perusahaan yang dipisahkan dengan ";".
Izinkan Pengguna untuk menonaktifkan Pemulihan Sistem	Memungkinkan pengguna menonaktifkan Pemulihan Sistem. **PERINGATAN!** Fitur ini hanya boleh digunakan pada perangkat yang dimiliki atau disediakan oleh perusahaan atau organisasi perusahaan atau pada perangkat yang dimiliki pengguna, di mana pengguna mengizinkan perangkat tersebut dikelola sepenuhnya oleh perusahaan. Jika Anda menonaktifkan pengaturan kebijakan ini, Pemulihan Sistem akan dinonaktifkan, dan Wizard Pemulihan Sistem tidak

	dapat diakses. Opsi untuk mengonfigurasi Pemulihan Sistem atau membuat titik pemulihan melalui Perlindungan Sistem juga dinonaktifkan.
Izinkan Pembatalan Pendaftaran Pengguna	Memungkinkan pengguna untuk menghapus bagian korporat dari perangkat dan dengan demikian memutuskan sambungan dari Server AppTec360. Jika hal ini terjadi, maka perangkat tidak dapat lagi dikelola. **PERINGATAN!** Fitur ini hanya boleh digunakan pada perangkat yang dimiliki atau disediakan oleh perusahaan atau organisasi perusahaan atau pada perangkat yang dimiliki pengguna, di mana pengguna mengizinkan perangkat tersebut dikelola sepenuhnya oleh perusahaan. Jika Anda menonaktifkan pengaturan kebijakan ini, pengguna tidak akan dapat menghapus pendaftaran MDM. Tentukan apakah pengguna diizinkan untuk menghapus akun tempat kerja melalui panel kontrol tempat kerja. Server MDM selalu dapat menghapus akun dari jarak jauh.

BitLocker

Konfigurasi BitLocker

Pengaturan Umum	
Memerlukan enkripsi perangkat	Meminta pengguna untuk mengaktifkan enkripsi perangkat Tergantung pada edisi Windows dan konfigurasi sistem, pengguna mungkin akan ditanya: - Untuk mengonfirmasi bahwa enkripsi dari penyedia lain tidak diaktifkan. - Untuk mematikan Enkripsi Drive BitLocker, lalu nyalakan kembali BitLocker.
Metode enkripsi	
Metode enkripsi untuk drive sistem operasi	
Metode enkripsi untuk drive data tetap	
Metode enkripsi untuk drive data yang dapat dilepas	
Menonaktifkan peringatan tentang enkripsi disk pihak ketiga	Nonaktifkan prompt peringatan tentang layanan enkripsi disk pihak ketiga yang digunakan pada perangkat. Mulai Windows 10, versi 1803, pengaturan ini hanya didukung untuk perangkat yang bergabung dengan Azure Active Directory.
Izinkan menjalankan enkripsi saat pengguna non-administrator masuk	Hanya didukung untuk perangkat yang bergabung dengan Azure Active Directory

Ekstensi AppTec360	
Enkripsi senyap	Jika dipilih bersama dengan "Require device encryption" (Memerlukan enkripsi perangkat), Layanan Manajemen AppTec360 akan menjalankan enkripsi senyap otomatis pada drive perangkat.
Secara otomatis menghasilkan kredensial pengguna	Drive OS yang dienkripsi akan dilindungi dengan kredensial pengguna yang dibuat secara otomatis. Baik PIN TPM, jika tersedia TPM atau kata sandi tekstual 6 digit. Kredensial yang dihasilkan akan dikirim ke alamat email yang terdaftar untuk perangkat tertentu. Jika opsi ini dimatikan, satu-satunya perlindungan yang memungkinkan untuk enkripsi senyap adalah menggunakan TPM. Dalam hal ini, untuk perangkat tanpa TPM, enkripsi senyap akan gagal.
Mengenkripsi drive tetap	Drive data tetap yang tersedia juga akan dienkripsi dan dilindungi dengan "Buka Kunci Otomatis" menggunakan kunci yang tersimpan pada drive OS.

Pengaturan Drive OS

Memerlukan autentikasi tambahan saat memulai	Pengaturan ini memungkinkan Anda untuk mengonfigurasi apakah BitLocker memerlukan autentikasi setiap kali komputer dinyalakan. Pengaturan ini diterapkan selama penyiapan BitLocker. Jika Anda mengaktifkan pengaturan ini, pengguna dapat mengonfigurasi opsi pengaktifan lanjutan di wizard penyiapan BitLocker.
Blokir BitLocker tanpa TPM yang kompatibel	
Hanya TPM	
TPM dan PIN	
TPM dan kunci	
TPM, kunci dan PIN	Jika Anda ingin mewajibkan penggunaan PIN dan USB flash drive (kunci), pengguna harus menyiapkan BitLocker menggunakan alat baris perintah "manage-bde" dan bukannya wizard penyiapan Enkripsi Drive BitLocker.

Memerlukan panjang PIN minimum	
	Karakter minimum

Mengonfigurasi pesan dan URL pemulihan pra-boot	Konfigurasikan seluruh pesan pemulihan atau ganti URL yang ada yang ditampilkan pada layar pemulihan tombol pra-boot saat drive OS terkunci. Catatan: Tidak semua karakter dan bahasa didukung dalam pra-boot. Sangat disarankan agar Anda menguji apakah karakter yang Anda gunakan muncul dengan benar pada layar pemulihan pra-boot.
	Opsi pesan pemulihan pra-boot
	Pesan pemulihan khusus
	URL pemulihan khusus

Opsi pemulihan drive OS		Pengaturan ini memungkinkan Anda untuk mengontrol bagaimana drive sistem operasi yang dilindungi BitLocker dipulihkan tanpa adanya kredensial yang diperlukan. Pengaturan ini diterapkan selama penyiapan BitLocker. Secara default, agen pemulihan data berbasis sertifikat diizinkan, opsi pemulihan dapat ditentukan oleh pengguna termasuk kata sandi pemulihan dan kunci pemulihan dan informasi pemulihan tidak dicadangkan ke AD DS.
	Agen pemulihan data berbasis Sertifikat Blokir	Tentukan apakah agen pemulihan data dapat digunakan dengan drive sistem operasi yang dilindungi BitLocker. Sebelum agen pemulihan data dapat digunakan, agen tersebut harus ditambahkan dari item Kebijakan Kunci Publik di Konsol Manajemen Kebijakan Grup atau Editor Kebijakan Grup Lokal. Baca Panduan Penerapan Enkripsi Drive BitLocker di Microsoft TechNet untuk informasi lebih lanjut tentang cara menambahkan agen pemulihan data.
	Pengaturan kata sandi pemulihan BitLocker	
	Pengaturan kunci pemulihan BitLocker	
	Menyimpan informasi pemulihan BitLocker ke Layanan Domain Direktori Aktif	
	Konfigurasi penyimpanan pemulihan AD DS BitLocker	Menyimpan paket kunci mendukung pemulihan data dari drive yang telah rusak secara fisik.
	Memerlukan penyimpanan data pemulihan ke AD DS	Mencegah pengguna mengaktifkan BitLocker kecuali jika komputer terhubung ke domain dan

Pengaturan Drive Tetap	
Opsi pemulihan drive tetap	Pengaturan ini memungkinkan Anda untuk mengontrol bagaimana drive tetap yang dilindungi BitLocker dipulihkan tanpa adanya kredensial yang diperlukan. Pengaturan ini diterapkan selama penyiapan BitLocker. Secara default, agen pemulihan data berbasis sertifikat diizinkan, opsi pemulihan dapat ditentukan oleh pengguna termasuk kata sandi pemulihan dan kunci pemulihan dan informasi pemulihan tidak dicadangkan ke AD DS.
Agen pemulihan data berbasis Sertifikat Blokir	
Pengaturan kata sandi pemulihan BitLocker	
Pengaturan kunci pemulihan BitLocker	
Menyimpan informasi pemulihan BitLocker ke Layanan Domain Direktori Aktif	
Konfigurasi penyimpanan pemulihan AD DS BitLocker	Menyimpan paket kunci mendukung pemulihan data dari drive yang telah rusak secara fisik.
Memerlukan penyimpanan data pemulihan ke AD DS	Mencegah pengguna mengaktifkan BitLocker kecuali jika komputer terhubung ke domain dan cadangan informasi pemulihan BitLocker ke AD DS berhasil. Catatan: Kata sandi pemulihan dibuat secara otomatis.
Menolak akses tulis ke drive tetap yang tidak dilindungi	

Pengaturan Drive yang Dapat Dilepas	
Menolak akses tulis ke drive lepasan yang tidak dilindungi	Menolak akses tulis ke drive data yang dapat dilepas yang tidak dilindungi oleh Bitlocker. Catatan: Jika "Disk yang dapat dilepas: Tolak akses tulis" diaktifkan dalam kebijakan grup, pengaturan kebijakan ini akan diabaikan.
Menolak akses tulis ke perangkat yang dikonfigurasi di organisasi lain	Hanya drive dengan bidang identifikasi yang sesuai dengan bidang identifikasi komputer yang akan diberikan akses tulis. Bidang-bidang ini ditentukan oleh pengaturan kebijakan grup "Berikan pengidentifikasi unik untuk organisasi Anda".

Status BitLocker

Di sini Anda bisa melihat status drive terenkripsi BitLocker saat ini

C [OS Drive]
Status Enkripsi
Terenkripsi (%)
Status Perlindungan
Metode Enkripsi
Pelindung Kunci
Kata Sandi Pemulihan

Dengan mengklik tombol "Putar kata sandi pemulihan", Anda dapat memutar kata sandi pemulihan BitLocker.

Manajemen Sertifikat

Daftar Sertifikat

Berikut ini adalah daftar sertifikat yang diinstal pada perangkat yang sedang ditampilkan.

Konfigurasi Sertifikat

Di sini Anda dapat mengonfigurasi sertifikat dan bagaimana sertifikat tersebut akan diinstal pada perangkat.

Sertifikat tepercaya	
Deskripsi	Deskripsi sertifikat
Cakupan	Ruang lingkup penerapan sertifikat: Pengguna saat ini vs Perangkat
Toko sertifikat	"Sertifikat Tidak Tepercaya" hanya tersedia mulai Windows 10, versi 1803
File sertifikat	Unggah file PKCS#1

Sertifikat identitas			
Deskripsi	Deskripsi sertifikat		
Cakupan	Ruang lingkup penerapan sertifikat: Pengguna saat ini vs Perangkat		
Lokasi utama	Penyedia Penyimpanan Kunci untuk menginstal kunci pribadi.		
		TPM. Gagal jika tidak ada TPM	
	TPM. Jika tidak ada TPM, kembali ke Perangkat Lunak KSP		
	Penyedia Penyimpanan Kunci Perangkat Lunak		Tandai kunci pribadi sebagai dapat diekspor
	Windows Hello untuk Bisnis	Nama wadah	Menentukan nama wadah Windows Hello for Business (sebelumnya dikenal sebagai Microsoft Passport for Work).
		Teks prompt PIN	Menentukan teks khusus yang akan ditampilkan pada prompt PIN Windows Hello for Business selama pendaftaran sertifikat.
Kredensial	Unggah File PKCS # 12		

SCEP

Deskripsi	Deskripsi Server SCEP		
Ruang Lingkup Penyebaran	Ruang lingkup penerapan sertifikat: Perangkat saat ini vs Pengguna		
URL Server SCEP	Satu atau beberapa server yang menerbitkan sertifikat melalui SCEP		
Subjek	Representasi nama X.500. Contoh: "C=US, O=Microsoft Corporation, CN=foo, 1.2.5.3=bar"		
Nama alternatif subjek	Jenis	Alamat email	
		DNS	
		URI	
		Nama Pengguna Utama (UPN)	
Sidik jari CA	Sidik jari SHA1 dari sertifikat Otoritas Sertifikat. E.g. 31:8F:1E:78:5C:D5:12:9F:7E:3B:AD:F3:1C:C0:19:03:96:43:A9:E5		
Unit masa berlaku	Hari, Bulan atau Tahun		
Masa berlaku			
Tantangan	Digunakan sebagai rahasia yang telah dibagikan sebelumnya untuk pendaftaran otomatis		
Mencoba kembali	Berapa kali perangkat harus mencoba ulang jika server mengirimkan respons PENDING. Nilai default adalah 5. Nilai maksimum adalah 30.		
Penundaan percobaan ulang	Jumlah menit untuk menunggu sebelum mencoba kembali. Nilai default adalah 5. Nilai minimum adalah 1.		
Ukuran kunci	Ukuran kunci dalam bit		
Algoritma hash	Rangkaian algoritma hash		
Penggunaan tombol	Ekstensi penggunaan kunci mendefinisikan tujuan (misalnya, enkripsi, tanda tangan) dari kunci yang terkandung dalam sertifikat. Setidaknya salah satu dari "Tanda tangan digital" atau "Penguraian kunci" harus dipilih.		
Penggunaan kunci yang diperpanjang	Menentukan penggunaan kunci yang diperluas, tergantung pada konfigurasi server SCEP. Tentukan daftar OID yang sesuai, misalnya 1.3.6.1.5.5.7.3.2 (Otentikasi Klien)		
Lokasi utama	Penyedia Penyimpanan Kunci untuk menginstal kunci pribadi.		

		TPM. Gagal jika tidak ada TPM	
	TPM. Jika tidak ada TPM, kembali ke Perangkat Lunak KSP		
	Penyedia Penyimpanan Kunci Perangkat Lunak		
	Windows Hello untuk Bisnis	Nama wadah	Menentukan nama wadah Windows Hello for Business (sebelumnya dikenal sebagai Microsoft Passport for Work).
		Teks prompt PIN	Menentukan teks khusus yang akan ditampilkan pada prompt PIN Windows Hello for Business selama pendaftaran sertifikat.

Manajemen Koneksi

Wifi

Pada pengaturan ini, lakukan pra-konfigurasi perangkat pengguna akhir untuk akses ke Titik Akses internal

Pengidentifikasi Set Layanan (SSID)	SSID ke jaringan, tempat koneksi akan dibuat
Gabung Otomatis	Aktifkan penggabungan otomatis ke jaringan
Jaringan Tersembunyi	Aktifkan, jika AP tidak menyiarkan SSID

Jenis Keamanan

Menetapkan jenis keamanan AP

Sistem Terbuka WEP	
Kata sandi	Kata sandi untuk AP

WPA PSK	
Kata sandi	Kata sandi untuk AP

WPA EAP	
Jenis Otentikasi	Jenis autentikasi, hanya dapat dilakukan dengan "PEAP-MSCAHPv2"
Hubungkan Kembali dengan Cepat	Perangkat dapat beralih di antara Titik Akses, tanpa harus mengautentikasi dirinya sendiri lagi
Akses Tamu	Pengguna tidak memiliki akun dan karenanya harus mendaftar sebagai tamu
Pemeriksaan Karantina	Klien harus melakukan Pemeriksaan NAP (Network Access Protection) dan membagikan hasilnya kepada sistem, yang kemudian memutuskan, apakah klien dapat terhubung
Memerlukan Pengikatan Kripto	Otentikasi hanya dapat dilakukan melalui Pengikatan Kripto
Validasi Server	Klien memeriksa, apakah sertifikat server valid. Jika demikian, koneksi akan dibuat
Meminta Sertifikat	Memungkinkan pengguna untuk menerima sertifikat yang tidak tepercaya
Nama Server	Menawarkan opsi untuk menampilkan nama RADIUS-Server, yang menawarkan autentikasi dan otorisasi jaringan

WPA2-PSK	
Kata sandi	Kata sandi AP

WPA2 EAP	
Jenis Otentikasi	Jenis Otentikasi, hanya dapat dilakukan dengan "PEAP-MSCAHPv2"
Hubungkan Kembali dengan Cepat	
Akses Tamu	
Pemeriksaan Karantina	Mengaktifkan perlindungan akses jaringan NAP
Memerlukan Pengikatan Kripto	Otentikasi hanya dapat dilakukan melalui Pengikatan Kripto
Validasi Server	
Meminta Sertifikat	Meminta sertifikat server yang telah divalidasi, nama, atau autentikasi sertifikat Root (CA)
Nama Server	Daftar server yang harus dipercaya oleh perangkat
Tidak ada	Tidak ada keamanan yang mapan
Gunakan Server Proxy	Penggunaan server proxy
Alamat Server	Alamat server proxy
Port Server	Port Server Server Proxy

Gunakan Server Proxy

Aktifkan penggunaan server proxy.

Alamat Server	Alamat server proxy yang digunakan oleh jaringan ini.
Port Server	Port server proxy yang digunakan oleh jaringan ini.

Pembatasan Wifi

Di sini Anda dapat menentukan berbagai pembatasan Wifi.

Izinkan WiFi	Mengizinkan/menolak WiFi
Izinkan Berbagi Internet	Mengizinkan penggunaan Hotspot
Izinkan Hubungkan Otomatis ke Hot Spot WiFi Sense	Izinkan Hubungkan Otomatis ke Hot Spot WiFi Sense
Izinkan Konfigurasi WiFi Manual	Memungkinkan pengguna untuk terhubung ke jaringan WiFi, yang belum ditentukan oleh AppTec
Frekuensi Pemindaian WLAN	Menetapkan interval Pemindaian WLAN. Di sini, nilai yang lebih tinggi meningkatkan kemampuan untuk mengenali jaringan WIFI.

VPN

Lakukan pengaturan yang sesuai di sini, untuk mengonfigurasi koneksi VPN

Nama Koneksi	Nama koneksi yang ditunjukkan		
Jenis VPN	Sambungan VPN Per-Aplikasi digunakan untuk mengamankan lalu lintas Aplikasi tertentu.		
	VPN	Selalu Aktif	Ini akan secara otomatis menyambungkan VPN pada saat masuk dan akan tetap tersambung hingga pengguna memutuskan sambungan secara manual.
	VPN Per-Aplikasi	Aplikasi VPN	Tentukan Aplikasi yang menggunakan Koneksi VPN ini
		Penguncian Per-Aplikasi	Penguncian Per-Aplikasi membuat aplikasi yang dipilih hanya memiliki konektivitas melalui koneksi VPN ini. Fitur ini tergantung pada Windows Defender Firewall.
	Profil WIP	Domain WIP untuk koneksi ini	ID Perusahaan, yang diperlukan untuk menyambungkan profil VPN ini dengan kebijakan Perlindungan Informasi Windows (WIP)

Jenis koneksi

VPN AppTec360	
Untuk "AppTec360 VPN", pemuatan aplikasi harus diizinkan. Aktifkan "Izinkan Pemuatan Aplikasi" di "Manajemen Keamanan" → "Pengaturan Pembatasan" → "Fungsionalitas Perangkat".	
Konfigurasi Gateway	Untuk mengonfigurasi koneksi VPN dengan daftar hitam, pilih konfigurasi VPN dengan server DNS tertentu. Anda dapat mengatur konfigurasi VPN di "Pengaturan Umum" → "Gerbang Universal" → "Pengaturan VPN".

IKEv2		
Server	Daftar server VPN	
Terowongan Perangkat	Aktifkan koneksi sebelum pengguna masuk.	
Metode otentikasi	EAP	EAP XML
	Sertifikat Mesin	
Algoritma enkripsi		
Algoritme pemeriksaan integritas		
Grup Diffie-Hellman		
Algoritma transformasi cipher		
Algoritme transformasi otentikasi		
Kelompok kerahasiaan maju sempurna (PFS)		

PPTP		
Server	Daftar server VPN	
Metode otentikasi	EAP	EAP XML

L2TP		
Server	Daftar server VPN	
Metode otentikasi	EAP	EAP XML
Algoritma enkripsi		
Algoritme pemeriksaan integritas		
Grup Diffie-Hellman		
Algoritma transformasi cipher		
Algoritme transformasi otentikasi		
Kelompok kerahasiaan maju sempurna (PFS)		

Otomatis		
Server	Daftar server VPN	
Metode otentikasi	EAP	EAP XML

Konfigurasi VPN Umum

Ingat kredensial pada setiap kali masuk	
Mendaftarkan alamat IP dengan DNS internal	
Aturan penyaringan lalu lintas jaringan	Batasi koneksi VPN dengan seperangkat aturan yang ditetapkan.
Daftar pencarian akhiran DNS	Akhiran DNS untuk ditambahkan ke daftar pencarian DNS untuk merutekan nama pendek.
Aturan Tabel Kebijakan Penyelesaian Nama (NRPT)	Aturan Tabel Kebijakan Resolusi Nama (NRPT) menentukan bagaimana DNS menyelesaikan nama ketika tersambung ke VPN.
Deteksi jaringan tepercaya	Daftar akhiran DNS untuk mengidentifikasi jaringan tepercaya.
Terowongan terpisah	Split tunneling berarti lalu lintas dapat melewati antarmuka apa pun sebagaimana ditentukan oleh tumpukan jaringan.
Rute terowongan terpisah	Daftar rute yang akan ditambahkan ke tabel perutean untuk antarmuka VPN.
Penyiapan proxy	Mengkonfigurasi Proxy yang digunakan dengan jaringan ini
Alamat Proxy	Alamat server proxy sebagai nama host yang memenuhi syarat atau alamat IP.
Pelabuhan	Port server proxy.
URL Konfigurasi Otomatis Proxy	URL untuk mengambil pengaturan proxy secara otomatis.

Pembatasan VPN

Di sini Anda dapat menentukan berbagai pembatasan VPN.

Izinkan Pengaturan VPN	Panduan ini mengizinkan/melarang pengguna untuk menonaktifkan dan mengubah pengaturan VPN
Izinkan VPN melalui Seluler	Mengizinkan/melarang perangkat untuk membuat koneksi VPN, jika perangkat menggunakan data seluler
Izinkan VPN Roaming melalui Seluler	Mengizinkan/melarang perangkat untuk membuat koneksi VPN, jika perangkat sedang roaming

Bluetooth

Di sini Anda dapat menetapkan, apakah Bluetooth harus diizinkan/dilarang.

Izinkan Bluetooth	Mengaktifkan/menonaktifkan Bluetooth

Manajemen PIM

Sinkronisasi Aktif Pertukaran

Penyiapan akun ActiveSync pada perangkat pengguna akhir

Nama Akun	Nama akun email
Nama Host Server	Alamat server/FQDN
Nama Domain	Domain server
Alamat email	Alamat email
Nama Pengguna	Nama pengguna
Kata Sandi Pengguna	Secara opsional, Anda sudah bisa melampirkan kata sandi ke pengguna di sini
Gunakan SSL	Gunakan koneksi SSL
Interval Sinkronisasi	Di sini interval sinkronisasi dapat ditetapkan Sinkronisasi manual = Pengguna harus mengunduh email mereka dan melakukan sinkronisasi manual
Filter Usia Surat	Jumlah waktu, hingga email harus disinkronkan Tanpa filter = tidak terbatas
Tingkat Log	Penetapan tingkat pencatatan untuk lalu lintas ActiveSync
Sinkronisasi Email	Diaktifkan = email disinkronkan
Sinkronisasi Kontak	Diaktifkan = kontak disinkronkan
Sinkronisasi Kalender	Diaktifkan = kalender disinkronkan
Tugas Sinkronisasi	Diaktifkan = tugas disinkronkan

eMail

Pembuatan akun POP3/IMAP4 pada perangkat pengguna akhir.

Deskripsi Akun	Nama akun email
Nama Pengirim	Nama pengirim yang ditampilkan
Nama Domain	Nama domain untuk akun email
Alamat email	Alamat email pengguna
Nama Pengguna	Nama pengguna
Kata Sandi Pengguna	Secara opsional, Anda sudah bisa melampirkan kata sandi ke pengguna di sini
Kredensial Server Keluar Alternatif	Di sini dapat ditentukan, jika kredensial lain diperlukan untuk server keluar
Nama Domain Keluar	Nama domain keluar
Nama Pengguna Server Keluar	Nama pengguna server keluar
Kata Sandi Server Keluar	Kata sandi server keluar
Protokol Email	POP3 atau IMAP4, dapat digunakan sebagai protokol
Nama Host Server Surat Masuk	Nama host server surat masuk
Gunakan SSL untuk Surat Masuk	Gunakan SSL untuk email masuk
Nama Host Server Surat Keluar	Nama host server surat keluar
Gunakan SSL untuk Surat Keluar	Gunakan SSL untuk email keluar
Otentikasi Server Keluar	Diperlukan otentikasi server keluar
Interval Sinkronisasi	Di sini interval sinkronisasi dapat ditetapkan Sinkronisasi manual = Pengguna harus mengunduh email mereka dan melakukan sinkronisasi manual
Filter Usia Surat	Jumlah waktu, hingga email harus disinkronkan Tanpa filter = tidak terbatas

Manajemen Aplikasi

Manajer Aplikasi Perusahaan

Aplikasi Terinstal

Berikut ini adalah daftar aplikasi yang saat ini terinstal pada perangkat yang sedang ditampilkan.

Aplikasi Wajib

Di sini Anda dapat mengonfigurasi daftar aplikasi yang wajib ada pada perangkat.

Daftar ini akan diperiksa setiap kali perangkat terhubung ke MDM dan menginstal semua aplikasi dalam daftar ini yang kebetulan tidak diinstal pada perangkat, terlepas dari apakah aplikasi tersebut telah dihapus atau tidak pernah diinstal sebelumnya.

Anda dapat mengunggah Aplikasi In-House Windows 10 dan kemudian menambahkannya ke daftar ini atau Anda dapat menambahkan konfigurasi Microsoft Office yang perlu dikonfigurasikan terlebih dahulu di "Pengaturan Umum" > "Manajemen Aplikasi" > "Microsoft Office".

Pembatasan Aplikasi Sys

Aplikasi Kotak Masuk
Mengizinkan Alarm dan Jam
Izinkan Kalkulator
Izinkan Kamera
Izinkan Dukungan Kontak
Izinkan Cortana
Izinkan Penjelajah File
Izinkan Memulai
Izinkan Musik Groove
Izinkan Peta
Izinkan Pengiriman Pesan
Izinkan Microsoft Edge
Izinkan Film Dan TV
Izinkan Uang
Izinkan Berita
Izinkan OneDrive
Izinkan OneNote
Izinkan Kalender Dan Surat Outlook
Izinkan Orang
Izinkan Telepon
Izinkan Foto
Izinkan Powerpoint
Izinkan Pengaturan
Izinkan Skype
Izinkan Olahraga
Izinkan Toko
Izinkan Perekam Suara
Izinkan Dompet
Izinkan Cuaca

Izinkan Hub Umpan Balik Windows
Izinkan Word
Izinkan Xbox

Halaman Pengaturan
Izinkan Tempat Kerja Akun
Izinkan Info Lanjutan
Izinkan Pojok Aplikasi
Izinkan Blokir dan Filter
Izinkan Profil Warna
Izinkan Mode Mengemudi
Izinkan Email dan Akun
Izinkan Ekualiser
Izinkan Keyboard
Izinkan Bilah Navigasi
Mengizinkan Mode Pesawat Jaringan
Izinkan Berbagi Internet Jaringan
Izinkan Layanan Jaringan
Izinkan Wi-Fi Jaringan
Izinkan Bluetooth Sistem PC
Izinkan Nilai Perangkat Anda
Izinkan Pembaruan Pemulihan
Izinkan Berbagi
Izinkan Mulai
Izinkan Bahasa Waktu
Izinkan Wilayah Waktu
Izinkan Layar Kunci Default Windows
Izinkan Akun Kantor atau Sekolah

Daftar Hitam & Putih

Di bawah "Daftar Hitam & Putih", Anda dapat memilih antara Mode "Daftar Putih" dan Mode "Daftar Hitam".

Daftar putih	Hanya aplikasi dan layanan yang ditambahkan ke dalam daftar yang dapat diinstal pada perangkat pengguna akhir. Jika ini sudah diinstal sebelumnya di perangkat pengguna akhir, maka akan diaktifkan dan diatur, sehingga pengguna dapat menjalankannya.
	Semua aplikasi lain yang tidak ditambahkan ke dalam daftar tidak dapat diinstal pada perangkat pengguna akhir. Jika aplikasi ini sudah diinstal sebelumnya di perangkat pengguna akhir, aplikasi ini akan dinonaktifkan dan diatur, sehingga pengguna tidak dapat menjalankannya.
Daftar hitam	Aplikasi dan layanan yang ditambahkan ke dalam daftar tidak dapat diinstal pada perangkat pengguna akhir. Jika sudah diinstal sebelumnya pada perangkat pengguna akhir, aplikasi dan layanan tersebut akan dinonaktifkan dan diatur, sehingga pengguna tidak dapat menjalankannya.
	Semua aplikasi lain yang tidak ditambahkan ke dalam daftar dapat diinstal pada perangkat pengguna akhir. Jika aplikasi-aplikasi ini sudah terinstal di perangkat pengguna akhir, aplikasi-aplikasi ini akan diaktifkan dan diatur, sehingga pengguna dapat menjalankannya.

Melalui , Anda menambahkan aplikasi atau layanan tambahan ke daftar yang sedang digunakan.

Melalui , Anda menambahkan aplikasi atau layanan tambahan ke daftar yang saat ini tidak aktif.

Anda dapat menambahkan aplikasi dari "Windows App Store" atau langsung memasukkan "Pengenal Aplikasi" untuk ditambahkan ke daftar hitam atau putih.

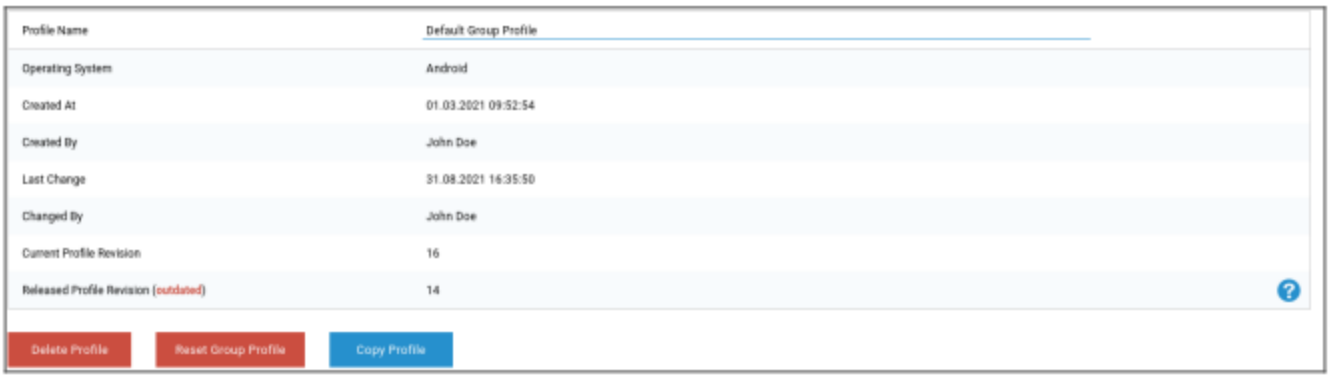
Konfigurasi MacOS

Tergantung pada apakah Anda telah memilih profil atau perangkat, tampilan dan sub-poinnya akan berbeda - harap perhatikan dengan saksama hal ini!

Umum

Ikhtisar profil grup (hanya pada tingkat grup)

Ketika membuka profil grup, Anda akan mendapatkan ikhtisar singkat profil.



Nama Profil	Nama profil (dapat diubah di sini)
Sistem Operasi	Sistem Operasi profil ini untuk
Dibuat di	Waktu pembuatan
Dibuat oleh	Pembuat profil
Perubahan Terakhir	Waktu perubahan terakhir pada profil
Diubah oleh	Akun yang melakukan perubahan terakhir
Revisi Profil Saat Ini	Revisi status profil yang disimpan
Revisi Profil yang Dirilis	Menetapkan revisi profil ("Tetapkan sekarang"). Jika label menunjukkan "(usang)" di belakang teks, itu berarti Anda telah menyimpan profil tetapi belum menetapkannya, sehingga perangkat masih akan mendapatkan versi yang lebih lama.

Ikhtisar Perangkat (hanya pada tingkat perangkat)

Ikhtisar ringkasan perangkat.

Nama Perangkat	Nama perangkat
Model	Model
Sistem Operasi	Sistem Operasi
Nomor Seri	Nomor seri perangkat
Kepemilikan Perangkat	Jenis Kepemilikan yang dikonfigurasi
Jenis Perangkat	Jenis Perangkat
Sesuai	Menunjukkan apakah perangkat sudah sesuai
Alamat IP	Alamat IP perangkat yang tersambung ke server dari
Terakhir terlihat	Waktu koneksi terakhir dari perangkat
Dorongan Terakhir	Waktu dorongan terakhir yang dikirim ke perangkat
Penugasan	Di sini Anda dapat memindahkan perangkat ke pengguna atau grup lain

Revisi Konfigurasi (hanya pada tingkat perangkat)

Di sini Anda akan menerima ikhtisar profil grup mana yang ditetapkan ke perangkat.

Jika Anda mengklik profil grup, Anda akan mengakses profil secara langsung dan dapat melakukan pengaturan.

Dengan simbol ini, Anda dapat mengembalikan aplikasi yang ditetapkan ke pengaturan profil grup.

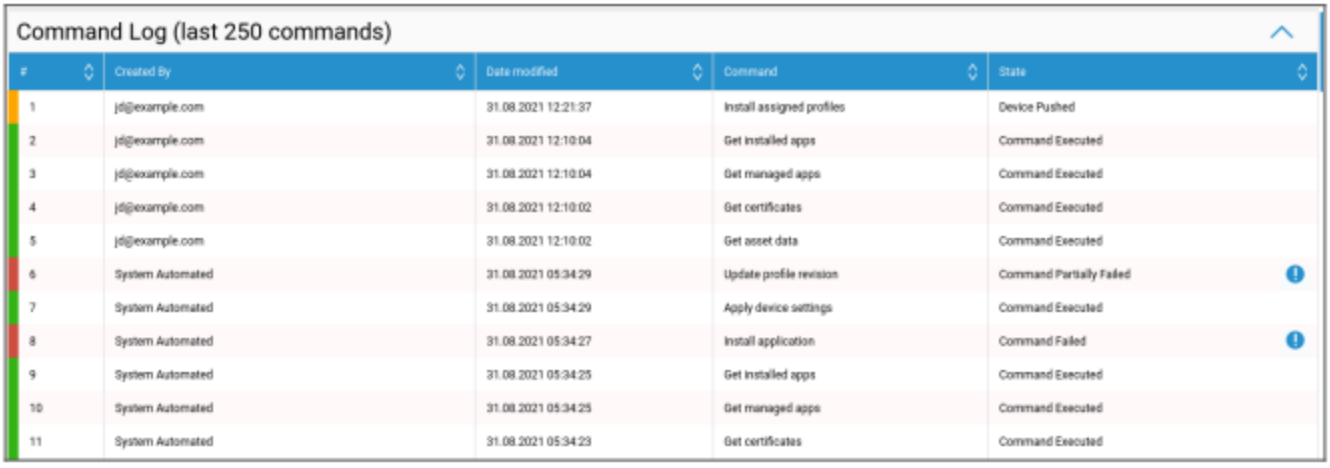
Dengan simbol tersebut, Anda dapat mengatur ulang profil perangkat agar tidak memiliki pengaturan sama sekali.

"Revisi terbaru tersedia" menunjukkan bahwa profil grup telah diubah dan disimpan namun belum ditetapkan. Profil grup harus ditetapkan dengan "Tetapkan sekarang" pada tingkat grup untuk menerapkan perubahan ke perangkat.

Log Perangkat (hanya pada tingkat perangkat)

Log Perintah

Di sini Anda dapat melihat perintah mana yang dikeluarkan untuk perangkat dan bagaimana statusnya.



Perintah yang dibuat oleh "System Automated" secara otomatis dibuat oleh sistem.

Kemungkinan status perintah

Perangkat Didorong	Permintaan push telah dikirim ke layanan push (misalnya APNS) untuk memberi tahu perangkat agar terhubung kembali ke server EMM.
Perintah Dibuat	Perintah ini dibuat dalam sistem.
Perintah Terkirim	Perintah dikirim ke perangkat setelah perangkat terhubung ke server.
Perintah Dieksekusi	Perintah berhasil dijalankan.
Perintah Gagal	Perintah gagal. *
Perintah Gagal Sebagian	Tergantung pada OS perangkat, beberapa perintah mungkin akan dikelompokkan bersama. Dalam hal ini, beberapa bagian dari grup perintah ini gagal. *
Perintah Dieksekusi, akhirnya Gagal	Perintah itu dijalankan tetapi mungkin tidak.
Perintah Ditolak	Perintah tersebut ditolak oleh pengguna.
Dibuang	Perintah telah dibuang. Misalnya karena digantikan oleh perintah lain atau perangkat didaftarkan ulang dan perintah lama dihapus

*Jika terdapat tanda seru di belakang pesan, Anda dapat memperoleh informasi lebih lanjut dengan mengarahkan kursor ke ikon tersebut.

Manajemen Aset (hanya pada tingkat perangkat)

Info Perangkat

Nomor Model	Nomor Model
Nama host	Nama host
Nama Host Lokal	Nama Host Lokal
Sistem Operasi	Sistem operasi
Versi OS	Versi OS
UDID	UDID
Memori Bebas / Total	Memori Bebas / Total

WiFi

Alamat IP	Alamat IP
MAC WiFi	MAC WiFi

Seluler

Nomor Telepon	Nomor Telepon
Status Roaming	Status Roaming
Roaming (Suara / Data)	Roaming (Suara / Data)
Alamat IP	Alamat IP
Operator/Pengangkut	Operator/Pengangkut
Jaringan Operator SIM	Jaringan operator
Versi Operator	Versi Operator
ICCID	ICCID
PKS/MNC saat ini	PKS/MNC saat ini
SIM PKS / MNC	SIM PKS / MNC

Bluetooth

Bluetooth MAC	Bluetooth MAC

Manajemen Pembaruan (hanya pada tingkat perangkat)

Perbarui Info

Tab ini menampilkan informasi tentang pengaturan pembaruan sistem pada perangkat.

Pemeriksaan otomatis diaktifkan	Jika sistem memeriksa pembaruan secara otomatis.
Pembaruan Aplikasi Otomatis diaktifkan	Jika sistem akan menginstal pembaruan aplikasi secara otomatis.
Pembaruan OS otomatis diaktifkan	Jika sistem akan menginstal pembaruan OS secara otomatis.
Keamanan Otomatis-Pembaruan diaktifkan	Jika sistem akan menginstal pembaruan keamanan secara otomatis.
Pembaruan Aplikasi Latar Belakang-Download diaktifkan	Jika sistem akan mengunduh pembaruan aplikasi di latar belakang.
URL Katalog	URL ke katalog pembaruan perangkat lunak yang digunakan klien.
Adalah katalog default	Jika "ya", Katalog adalah katalog default.
Lakukan pemeriksaan berkala	Jika "ya", mulailah pemindaian baru.
Tanggal pemindaian sebelumnya	Tanggal pemindaian pembaruan perangkat lunak terakhir.
Hasil pemindaian sebelumnya	Kode hasil pemindaian pembaruan perangkat lunak terakhir.

Manajemen Keamanan

Anti Pencurian

Bersihkan & Kunci

Penghapusan Penuh	Mengirim perintah untuk mengatur ulang perangkat ke pengaturan pabrik
Penghapusan Perusahaan	Hapus MDM dari perangkat dan hapus semua Data MDM (mis. Akun, Aplikasi)
Layar Kunci	Membuat perangkat kembali ke layar kunci

Konfigurasi Keamanan

Kode Sandi

Penonaktifan kode diperbolehkan	Menentukan apakah pengguna dipaksa untuk menetapkan PIN. Cukup dengan menetapkan nilai ini (dan bukan yang lain), pengguna akan dipaksa untuk memasukkan kode sandi, tanpa memaksakan panjang atau kualitasnya.
Izinkan nilai sederhana	Izinkan pengguna untuk menggunakan string angka yang sama, meningkat dan menurun (mis. 1234, 1111)
Memerlukan nilai alfanumerik	Kata sandi harus terdiri dari setidaknya satu huruf
Panjang kode sandi minimum	Panjang kata sandi minimal
Jumlah minimum karakter kompleks	Jumlah minimal simbol alfanumerik dalam kata sandi
Usia kode sandi maksimum	Jumlah hari, setelah itu kata sandi harus diubah
Kunci Otomatis Maksimum	Waktu maksimum, setelah itu perangkat terkunci
Masa tenggang maksimum untuk penguncian perangkat	Jumlah waktu perangkat dapat dikunci tanpa meminta kode sandi saat membuka kunci
Usia kode sandi maksimum (1-730 hari, atau tidak sama sekali)	Hari dimana kode sandi harus diubah
Riwayat kode sandi (1-50 kode sandi, atau tidak ada)	Jumlah kode sandi unik sebelum digunakan kembali

Sertifikat

PKCS # 1	
Deskripsi	Masukkan Deskripsi untuk Sertifikat
Kredensial	Unggah File pkcs1

PKCS # 12	
Deskripsi	Masukkan Deskripsi untuk Sertifikat
Kredensial	Unggah File pkcs12.

Pengaturan Pembatasan

Fungsionalitas Perangkat

Izinkan Kamera	Izinkan penggunaan kamera
Izinkan Game Center	Jika salah, Game Center dinonaktifkan dan ikonnya dihapus dari layar Utama.
Mengizinkan permainan multipemain	Jika salah, melarang permainan multipemain.
Izinkan menambahkan teman Game Center	Jika salah, melarang menambahkan teman ke Game Center.
Mengizinkan Perpustakaan Foto iCloud	Jika diatur ke salah, menonaktifkan Perpustakaan Foto iCloud. Foto apa pun yang tidak diunduh sepenuhnya dari Perpustakaan Foto iCloud ke perangkat akan dihapus dari penyimpanan lokal.
Izinkan ID Sentuh	Jika salah, mencegah Touch ID membuka kunci perangkat.

iCloud

Memblokir fungsi tertentu selama pemasangan iCloud

Mengizinkan sinkronisasi dokumen	Mengizinkan sinkronisasi dokumen
Izinkan Sinkronisasi Rantai Kunci iCloud	Izinkan Sinkronisasi Rantai Kunci iCloud
Mengizinkan Catatan iCloud	Jika salah, melarang layanan MacOS iCloud Notes
Mengizinkan BTMM iCloud	Jika salah, melarang layanan MacOS Kembali ke Mac Saya iCloud.
Mengizinkan iCloud FMM	Jika salah, menonaktifkan layanan MacOS Find My Mac iCloud.
Mengizinkan Penanda iCloud	Jika salah, batalkan sinkronisasi MacOS iCloud Bookmark.
Mengizinkan Mail iCloud	Jika salah, melarang layanan MacOS Mail iCloud.
Mengizinkan Kalender iCloud	Jika salah, melarang layanan MacOS Cloud iCloud.
Mengizinkan Pengingat iCloud	Jika salah, menonaktifkan layanan Pengingat iCloud.
Mengizinkan Buku Alamat iCloud	Jika salah, melarang layanan Buku Alamat MacOS iCloud.

Manajemen Media

Keluarkan saat Logout	Keluarkan semua media yang dapat dilepas saat Logout
Izinkan Jaringan	Izinkan akses untuk media jaringan
Izinkan Disk Internal	Izinkan akses untuk disk internal.
Memerlukan Otentikasi	Memerlukan Otentikasi untuk penggunaan media ini
Hanya Baca	Pengguna hanya dapat membaca data dari media
Izinkan Disk Eksternal	Izinkan akses untuk disk eksternal.
Memerlukan Otentikasi	Memerlukan Otentikasi untuk penggunaan media ini
Hanya Baca	Pengguna hanya dapat membaca data dari media
Izinkan penggunaan Gambar Disk	Izinkan akses untuk Gambar.
Memerlukan Otentikasi	Memerlukan Otentikasi untuk penggunaan media ini
Hanya Baca	Pengguna hanya dapat membaca data dari media
Izinkan penggunaan DVD-RAM	Izinkan akses untuk disk DVD-RAM.
Memerlukan Otentikasi	Memerlukan Otentikasi untuk penggunaan media ini
Hanya Baca	Pengguna hanya dapat membaca data dari media
Mengizinkan penggunaan DVD	Izinkan akses untuk disk DVD.
Memerlukan Otentikasi	Memerlukan Otentikasi untuk penggunaan media ini
Mengizinkan penggunaan CD	Izinkan akses untuk disk CD.
Memerlukan Otentikasi	Memerlukan Otentikasi untuk penggunaan media ini

Manajemen Koneksi

Wi-Fi

Di sini Anda dapat menambahkan dan mengonfigurasi koneksi Wi-Fi

Pengidentifikasi Set Layanan (SSID)	SSID jaringan, tempat koneksi akan dibuat
Gabung Otomatis	Mengaktifkan penggabungan otomatis untuk jaringan
Jaringan Tersembunyi	Aktifkan, jika AP tidak menyiarkan SSID
Pengaturan Proxy	Mengkonfigurasi Proxy untuk setiap Titik Akses
Tidak ada	Jangan gunakan Server Proxy
Manual	Membuat Proxy manual
URL Server Proxy	Alamat untuk mengakses Pengaturan Proxy
Pelabuhan	Menetapkan port untuk Proxy
Otentikasi	Nama pengguna untuk autentikasi pada Proxy
Kata sandi	Kata sandi untuk autentikasi pada Proxy
Otomatis	Membuat Proxy secara otomatis
URL Server Proxy	URL untuk file pengaturan proxy
Jenis Keamanan	Menetapkan Jenis Keamanan untuk AP
WEP	
Kata sandi	Kata sandi untuk AP
WPA/WPA2	
Kata sandi	Kata sandi untuk AP
WEP Enterprise - WPA / WPA2 Enterprise / Perusahaan apa pun	Lihat Kesalahan Tabel: Sumber referensi tidak ditemukan di bawah ini
Tidak ada	Tidak menetapkan keamanan
Menonaktifkan pengacakan alamat MAC	Menonaktifkan pengacakan alamat MAC untuk jaringan Wi-Fi tersebut saat terhubung ke jaringan. Ini juga menunjukkan peringatan privasi di Pengaturan yang menunjukkan bahwa jaringan telah mengurangi perlindungan privasi.

Konfigurasi Wi-Fi Perusahaan

Catatan: Hanya tersedia bila "Jenis Keamanan" diatur ke Jenis Perusahaan.

Protokol	Protokol otentikasi didukung pada jaringan target
TLS	Mengaktifkan / Menonaktifkan Penggunaan
TTLS	Mengaktifkan / Menonaktifkan Penggunaan
Otentikasi Bagian Dalam	Protokol autentikasi yang harus digunakan: PAP, CHAP, MSCHAP, MSCHAPv2
LEAP	Mengaktifkan / Menonaktifkan Penggunaan
PEAP	Mengaktifkan / Menonaktifkan Penggunaan
EAP-FAST	Mengaktifkan / Menonaktifkan Penggunaan
EAP-SIM	Mengaktifkan / Menonaktifkan Penggunaan
Gunakan PAC	Penggunaan PAC (Kontrol Akses Terproteksi)
PAC Penyediaan	Konfigurasi PAC Penyediaan
PAC Penyediaan Secara Anonim	Anonim Penyediaan PAC
Otentikasi	
Nama pengguna	Nama pengguna otentikasi
Jangan gunakan Per-Koneksi Kata sandi	Jangan gunakan Kata Sandi Per-Koneksi
Kata sandi	Kata sandi yang akan digunakan
Sertifikat Identitas	Unggah/pilih sertifikat autentikasi
Identitas Luar	Identitas yang dapat dilihat secara eksternal
Kepercayaan	
Sertifikat Terpercaya 1	Unggah sertifikat tepercaya pertama
Sertifikat Terpercaya 2	Unggah sertifikat tepercaya kedua
Sertifikat Terpercaya 3	Unggah sertifikat tepercaya ketiga
Server Tepercaya Nama Sertifikat	Nama-nama sertifikat server yang diharapkan (dalam daftar yang dipisahkan koma)

VPN

Tergantung pada Jenis Koneksi yang dipilih, bidang yang berbeda mungkin terlihat.

Nama Koneksi	Nama Profil VPN
Jenis VPN	
VPN	Semua lalu lintas jaringan perangkat akan dialihkan melalui koneksi VPN.
Jenis Koneksi	Menetapkan jenis koneksi VPN
IPsec (cisco)	Protokol IPsec oleh cisco
L2TP	Protokol L2TP
SSL khusus	Koneksi melalui SSL Khusus
IKEv2	Protokol IKEv2
Pengaturan Proxy	Mengkonfigurasi Proxy untuk koneksi VPN
Tidak ada	Tidak menetapkan Proxy
Manual	Membuat Proxy secara manual
URL Server Proxy	Alamat untuk akses ke Pengaturan Proxy
Pelabuhan	Menetapkan port untuk Proxy
Otentikasi	Nama pengguna untuk autentikasi di Proxy
Kata sandi	Kata sandi untuk autentikasi di Proxy
Otomatis	Membuat Proxy secara otomatis
URL Server Proxy	URL untuk akses ke pengaturan Proxy

Proksi HTTP

Jenis Proxy	
Manual	Membuat Proxy secara manual
URL Server Proxy	Alamat untuk akses ke Pengaturan Proxy
Pelabuhan	Menetapkan port Proxy
Otentikasi	Nama pengguna untuk autentikasi di Proxy
Kata sandi	Kata sandi untuk autentikasi di Proxy
Otomatis	Membuat Proxy secara otomatis
URL PAC Proksi	URL PAC Proksi
Izinkan koneksi langsung jika PAC tidak dapat dijangkau	Izinkan koneksi langsung (tanpa VPN), jika PAC tidak dapat dijangkau
Izinkan melewati proxy untuk mengakses jaringan captive	Izinkan melewati proxy untuk mengakses jaringan internal captive

AirPrint

Alamat IP	Alamat IP printer
Jalur Sumber Daya	Jalur yang pasti ke perangkat AirPrint

AirPlay

Nama Perangkat	Nama perangkat
Kata sandi	Memasangkan kata sandi
Daftar putih	Tentukan daftar perangkat yang dapat dipasangkan secara eksklusif dengan perangkat tersebut

Manajemen PIM

Sinkronisasi Aktif Pertukaran

Nama Akun	Nama akun.
Alamat email	Alamat akun (misalnya max@company.com)
Nama Host Server	Nama Host Internal
Nama Login	"Domain" dan "Nama Login" harus dikosongkan agar perangkat dapat meminta pengguna.
Domain	"Domain" dan "Nama Login" harus dikosongkan agar perangkat dapat meminta pengguna. Jika Konfigurasi Gateway ACL diaktifkan dan bidang Domain tidak kosong, AppTec360 Universal Gateway akan mengautentikasi perangkat dengan nama berikut "Domain\Nama Login"
Kata sandi	Kata sandi untuk akun (misalnya secretUserPassword)
Hari-hari Terakhir Mail untuk Disinkronkan	Jumlah hari terakhir email yang akan disinkronkan
Gunakan SSL	Gunakan SSL untuk Host Pertukaran Internal
Opsi Lanjutan	Tampilkan Opsi Lanjutan
Port Server	Port Internal
Jalur Server	Jalur Internal
Nama Host Eksternal	Host Eksternal
Port Eksternal	Port Eksternal
Jalur Eksternal	Jalur Eksternal
Gunakan SSL untuk Eksternal Host Pertukaran	Gunakan SSL untuk Host Pertukaran Eksternal

eMail

Pengaturan akun POP3 / IMAP pada perangkat pengguna akhir

Deskripsi Akun	Nama des Akun Email
Jenis Akun	
IMAP	
Awalan Jalur	Awalan Jalur untuk folder khusus
POP	
Nama Tampilan Pengguna	Nama tampilan pengguna
Alamat email	Alamat email pengguna

Surat Masuk	Pengaturan server yang masuk
Alamat Server Surat	Alamat Server Surat
Port Server Surat	Port Server Surat
Nama Pengguna	Nama pengguna masing-masing
Jenis Otentikasi	Jenis Otentikasi
Tidak ada	Tidak Ada Jenis Otentikasi
Kata sandi (hanya pada tingkat perangkat)	Permintaan kata sandi
Tantangan-Tanggapan MDM	
NTLM	Otentikasi NTLM
HTTP MD5 Digest	
Gunakan SSL	Gunakan SSL, jika diperlukan

Surat Keluar	Pengaturan server keluar
Alamat Server Surat	Alamat Server Surat
Port Server Surat	Port Server Surat
Nama Pengguna	Nama Pengguna masing-masing
Jenis Otentikasi	
Tidak ada	Tidak ada metode otentikasi
Kata sandi (hanya pada tingkat perangkat)	Permintaan kata sandi
Tantangan-Tanggapan MDM	
NTLM	Otentikasi NTLM
HTTP MD5 Digest	
Gunakan SSL	Gunakan SSL, jika diperlukan
Kata sandi keluar sama dengan kata sandi masuk	Kata sandi keluar sama dengan kata sandi masuk
Gunakan hanya dalam surat	Aktifkan, jika semua email keluar akan dikirim melalui Aplikasi Mail

CalDav

Mengonfigurasi pengaturan dan distribusi Akun CalDav

Deskripsi Akun	Menampilkan nama akun
Nama host	Nama host dan/atau alamat IP
Pelabuhan	Pelabuhan Akun CalDav
URL utama	URL Utama Akun
Nama pengguna	Nama pengguna CalDav masing-masing
Kata sandi (hanya pada tingkat perangkat)	Kata sandi CalDav masing-masing
Gunakan SSL	Gunakan SSL, jika diperlukan

CardDav

Mengonfigurasi pengaturan dan distribusi Akun CardDav

Deskripsi Akun	Menampilkan nama akun
Nama host	Nama host dan/atau alamat IP
Pelabuhan	Pelabuhan Akun CardDav
URL utama	URL Utama Akun
Nama pengguna	Nama pengguna CardDav masing-masing
Kata sandi (hanya pada tingkat perangkat)	Kata sandi CardDav masing-masing
Gunakan SSL	Gunakan SSL, jika diperlukan

LDAP

Di area ini, siapkan koneksi LDAP, untuk memungkinkan pertukaran sertifikat dinamis, antara perangkat pengguna akhir dan Direktori Aktif.

Harap diperhatikan bahwa pengguna yang dipilih memerlukan izin baca masing-masing.

Deskripsi Akun	Deskripsi Akun
Nama Pengguna Akun	Pengguna untuk akses LDAP
Kata Sandi Akun	Kata sandi untuk akses LDAP
Nama Host Akun	Nama host/alamat IP Server LDAP
Gunakan SSL	Gunakan SSL, jika diperlukan

Pada bagian kedua, Anda dapat menentukan filter individual untuk pencarian di registri LDAP.

Deskripsi	Cakupan	Basis Pencarian
Deskripsi filter	Tingkat pencarian di registri LDAP	Menentukan filter individual

Dasbor & Pelaporan

Pengaturan Dasbor

Di sini Anda dapat melihat dasbor yang ada, mengeditnya, atau membuat dasbor baru. Setiap Dasbor memiliki kumpulan data masing-masing untuk ditampilkan dan konfigurasi grafik.

Kontrol Pengaturan Dasbor

Publik	Mengatur Dasbor menjadi publik, sehingga pengguna lain dapat melihat Dasbor. Pengguna tentu saja harus dapat masuk dan melihat Dasbor. Jika "Publik" tidak diaktifkan, hanya pembuat yang dapat melihatnya.
Default	Mengatur Dasbor sebagai default sehingga secara otomatis terbuka saat Anda mengakses Tampilan Dasbor berikutnya.
	Menampilkan Dasbor dan grafiknya
	Menghapus Dasbor
	Edit Nama dan Pengaturan Dasbor
	Membuat salinan Dasbor
	Menambahkan Dasbor yang benar-benar baru

Tampilan Dasbor

Ini menunjukkan Data dan Grafik dari Dasbor yang dipilih dan juga memungkinkan Anda untuk mengubahnya.

Kontrol Dasbor

	Memungkinkan Anda menentukan data mana yang ditampilkan di Dasbor, jumlah data yang akan ditampilkan, dan dalam ukuran berapa data tersebut akan ditampilkan
	Membawa Anda kembali ke Ikhtisar Dasbor
	Mengatur ulang Dasbor yang sedang dibuka ke pengaturan default
	Menyimpan semua perubahan yang Anda lakukan pada Dasbor yang sedang dibuka (misalnya data mana yang akan ditampilkan)
	Mengubah jenis bagan menjadi bagan pilar
	Mengubah jenis bagan menjadi diagram lingkaran
	Mengubah jenis bagan menjadi bagan donat
	Mengubah jenis bagan menjadi bagan area kutub
	Mengubah urutan penyortiran

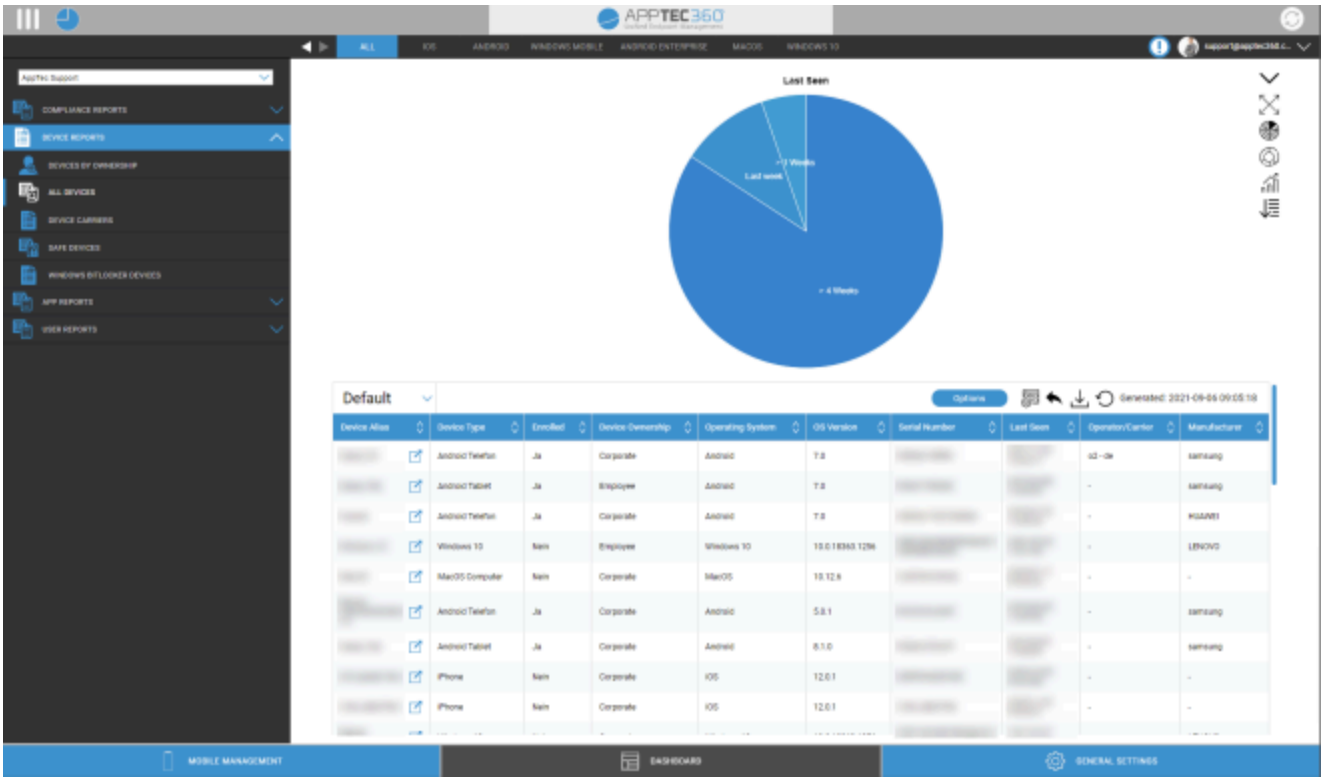
Pelaporan yang Diperpanjang

"Pelaporan yang Diperluas" menawarkan ikhtisar dan grafik terperinci tentang informasi perangkat dan pengguna.

Terdapat beberapa Laporan default, namun semuanya dapat diubah secara manual untuk menambah atau menghapus data yang akan ditampilkan.

Harap diperhatikan bahwa Anda hanya dapat mengubah data yang ditampilkan secara manual. Kategori laporan yang dipilih menentukan data yang menjadi dasarnya. Misalnya, Anda tidak akan pernah bisa melihat perangkat Android dalam laporan iOS di Laporan Perangkat Semua Perangkat iOS

Pada bagian kiri atas Anda dapat membatasi data pelaporan untuk grup tertentu (dan semua sub grupnya). Secara default, ini diatur ke simpul akar Anda, sehingga akan memperhitungkan SEMUA perangkat dan pengguna.



Kontrol Pelaporan yang Diperluas

Dalam setiap ikhtisar, Anda dapat menggunakan fungsi berikut untuk mengubah laporan dengan cara apa pun yang Anda inginkan:

	Sembunyikan grafik (Jika grafik ditampilkan)
	Tampilkan grafik (Jika grafik disembunyikan)
	Perluas bagan (Jika bagan diciutkan)
	Bagan yang diciutkan (Jika bagan diperluas)
	Mengubah jenis bagan menjadi bagan pilar
	Mengubah jenis bagan menjadi diagram lingkaran
	Mengubah jenis bagan menjadi bagan donat
	Mengubah jenis bagan menjadi bagan area kutub
	Mengubah urutan penyortiran
	Ubah bagian berikut ini tentang ikhtisar yang ditampilkan: • Menambah/menghapus kolom • Menentukan urutan tampilan kolom-kolom • Menampilkan/menyembunyikan grafik di atas tabel • Pilih kolom yang digunakan untuk grafik • Memfilter data tabel Anda
	Buka manajer pengaturan untuk menyimpan dan memuat berbagai laporan
	Mengatur ulang Laporan yang sedang dibuka ke default
	Ekspor laporan saat ini sebagai file .csv
	Membuat ulang data dan memuat ulang laporan saat ini

Anda dapat menemukan daftar semua laporan default pada halaman berikutnya.

Laporan Kepatuhan

Perangkat yang di-root

Ikhtisar perangkat yang telah di-root/jailbreak.

Kolom-kolom default dari laporan ini:

Alias Perangkat
Pemilik Perangkat
Surat elektronik
Sistem Operasi
Nomor Telepon
Terakhir terlihat
Produsen

Perangkat Roaming

Ikhtisar semua perangkat yang sedang roaming

Kolom-kolom default dari laporan ini:

Alias Perangkat
Pemilik Perangkat
Surat elektronik
Jenis Perangkat
Sistem Operasi
Nomor Telepon
Terakhir terlihat

Perangkat yang Diaktifkan Roaming

Ikhtisar semua perangkat yang telah mengaktifkan roaming tetapi tidak harus sedang roaming.

Kolom-kolom default dari laporan ini:

Alias Perangkat
Pemilik Perangkat
Surat elektronik
Jenis Perangkat
Sistem Operasi
Nomor Telepon
Terakhir terlihat

Perangkat yang Diawasi

Ikhtisar semua perangkat yang diawasi dalam mode yang diawasi (hanya iOS)

Kolom-kolom default dari laporan ini:

Alias Perangkat
Pemilik Perangkat
Surat elektronik
Jenis Perangkat
Terakhir terlihat

Perangkat Tidak Aktif

Ikhtisar semua perangkat yang tidak tersambung ke server dalam 7 hari terakhir

Kolom-kolom default dari laporan ini:

Alias Perangkat
Pemilik Perangkat
Surat elektronik
Jenis Perangkat
Sistem Operasi
Terakhir terlihat

Laporan Perangkat

Perangkat berdasarkan Kepemilikan

Di sini Anda dapat melihat berapa banyak perangkat yang saat ini telah digunakan sebagai perangkat perusahaan (perangkat perusahaan) dan perangkat karyawan (perangkat pribadi).

Kolom-kolom default dari laporan ini:

Alias Perangkat
Pemilik Perangkat
Jenis Perangkat
Kepemilikan Perangkat
Sistem Operasi

Semua Perangkat

Di sini Anda dapat melihat ikhtisar semua perangkat dengan informasi yang paling penting.

Kolom-kolom default dari laporan ini:

Alias Perangkat
Jenis Perangkat
Terdaftar
Kepemilikan Perangkat
Sistem Operasi
Versi OS
Nomor Seri
Terakhir terlihat
Operator/Pengangkut
Produsen

Pembawa Perangkat

Di sini Anda dapat melihat gambaran umum mengenai operator (penyedia layanan seluler).

Kolom-kolom default dari laporan ini:

Alias Perangkat
Pemilik Perangkat
Surat elektronik
Sistem Operasi
Versi OS
Operator/Pengangkut

Perangkat AMAN

Di sini Anda dapat melihat ikhtisar perangkat mana saja yang menggunakan Versi SAFE.

Karena ikhtisar dan/atau SAFE hanya tersedia untuk perangkat Samsung, Anda tidak akan melihat tab biasa di bawah poin ini.

Kolom-kolom default dari laporan ini:

Alias Perangkat
Pemilik Perangkat
Surat elektronik
Jenis Perangkat
Terakhir terlihat
Versi AMAN

Perangkat BitLocker Windows

Di sini Anda bisa melihat ikhtisar perangkat Windows yang menggunakan BitLocker.

Kolom-kolom default dari laporan ini:

Alias Perangkat
Pemilik Perangkat
Surat elektronik

Status BitLocker

Laporan Aplikasi

Di sini Anda mendapatkan berbagai ikhtisar terkait aplikasi. Dalam semua laporan ini, Anda dapat mengklik sebuah entri untuk melihat lebih jauh versi mana yang diinstal pada perangkat dan seberapa sering. Dalam tampilan ini, Anda dapat mengklik versi tertentu lagi untuk melihat perangkat mana saja yang telah menginstal versi tertentu.

Catatan: Mungkin diperlukan beberapa waktu hingga sistem mendapatkan informasi terbaru dari perangkat. Selain itu, laporan tidak diperbarui setiap menit. Anda mungkin perlu bersabar untuk melihat status saat ini jika Anda baru saja menetapkan aplikasi atau versi baru. Memuat ulang laporan secara manual akan memaksa laporan untuk menampilkan data terbaru yang tersedia

Aplikasi Terinstal

Di sini Anda mendapatkan gambaran umum semua aplikasi yang terinstal.

Kolom-kolom default dari laporan ini:

Nama	Nama aplikasi dan/atau layanan yang bersangkutan
Pengenal	ID aplikasi/layanan yang pasti
Jumlah Total	Seberapa sering aplikasi/layanan ini diinstal pada perangkat pengguna akhir

Aplikasi yang Paling Banyak Diinstal

Di sini Anda mendapatkan gambaran umum tentang aplikasi yang paling banyak diinstal.

Kolom-kolom default dari laporan ini:

Nama	Nama aplikasi dan/atau layanan yang bersangkutan
Pengenal	ID aplikasi/layanan yang pasti
Jumlah Total	Seberapa sering aplikasi/layanan ini diinstal pada perangkat pengguna akhir

Aplikasi Wajib

Di sini Anda mendapatkan gambaran umum tentang aplikasi wajib (yang diwajibkan).

Kolom-kolom default dari laporan ini:

Nama	Nama aplikasi dan/atau layanan yang bersangkutan
Pengenal	ID aplikasi/layanan yang pasti
Sumber Aplikasi	AppStore mana yang terlibat: • Google PlayStore (Android) • iTunes AppStore (iOS)
OS	Sistem Operasi

Aplikasi dalam Daftar Hitam

Di sini Anda mendapatkan gambaran umum tentang semua aplikasi yang masuk daftar hitam.

Kolom-kolom default dari laporan ini:

Nama	Nama aplikasi dan/atau layanan yang bersangkutan
Pengenal	ID aplikasi/layanan yang pasti
Sumber Aplikasi	AppStore mana yang terlibat: • Google PlayStore (Android) • iTunes AppStore (iOS)
OS	Sistem Operasi

Laporan Pengguna

Tarif

Di sini Anda mendapatkan gambaran umum tentang tarif telepon dan kartu SIM pengguna Anda.

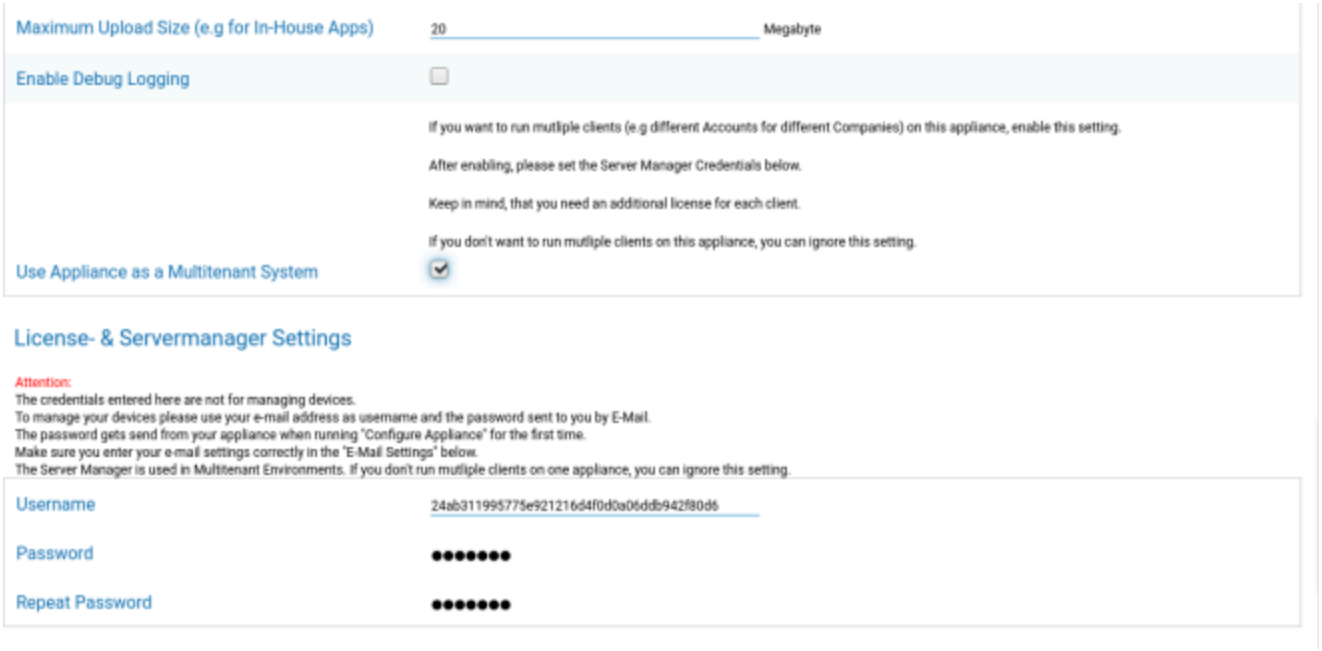
Kolom-kolom default dari laporan ini:

Surat elektronik
Nama
nomor telepon
pembawa
tarif
opsi
harga
kontrakDibatalkan
contractStart
selama Waktu
mobileAndData
dataVolume
multiSIM
jenis
simCardSerial1
simCardSerial2
simCardSerial3
pin1
pin2
puk1
puk2
catatan

Manajemen Multitenant

AppTec360 EMM mampu meng-host beberapa penyewa terpisah, masing-masing dengan pengguna dan grup, izin, dan pengaturan global mereka sendiri.

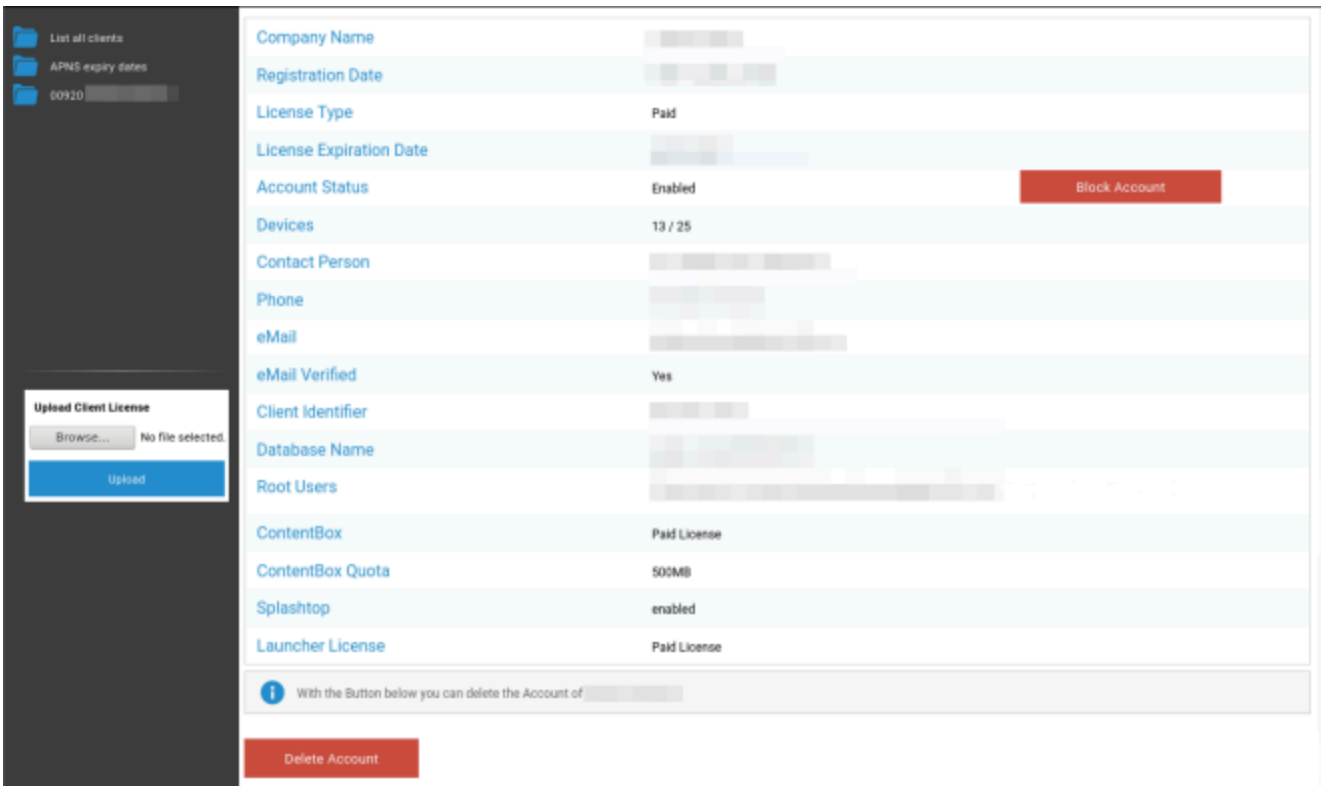
Untuk mengaktifkan kemampuan Multitenant, Anda harus mengaktifkannya di antarmuka konfigurasi Alat di "Langkah Ketiga - Pengaturan Server".



Pada menu baru, tetapkan nama pengguna dan kata sandi untuk Servermanager. Simpan pengaturan dan jalankan "Konfigurasi Alat" di "Langkah Lima - Perjanjian Lisensi" untuk menerapkan pengaturan.

Setelah konfigurasi selesai, Anda sekarang dapat masuk dengan kredensial yang telah ditetapkan melalui antarmuka Manajemen Seluler normal.

Setelah login, Anda dapat melihat tampilan berikut ini.



Di sebelah kiri Anda dapat melihat semua penyewa (dalam kasus ini hanya satu dengan id 920) dan di sebelah kanan informasi tentang klien ini. Anda juga memiliki opsi untuk memblokir akses ke akun serta menghapus klien (PERHATIAN: Hal ini akan menghapus semua data yang berhubungan dengan klien tersebut).

Di sebelah kiri Anda dapat mengunggah lisensi klien baru, yang dapat berupa pembaruan lisensi untuk klien yang sudah ada atau lisensi baru yang secara otomatis membuat klien baru. Ketika klien baru dibuat, email yang berisi kata sandi masuk secara otomatis dikirim ke alamat email yang digunakan untuk mengeluarkan lisensi.

Untuk mendapatkan lisensi klien yang baru atau yang telah diperbarui (misalnya, ketika membutuhkan lebih banyak lisensi perangkat), hubungi perwakilan penjualan Anda.

Tampilan tambahan

Daftar semua klien

Menampilkan gambaran umum tentang semua klien dalam sistem.

ID Klien	ID Klien
Pengenal	Pengenal Klien
Basis data	Basis data
Nama Perusahaan	Nama perusahaan
eMail	Orang yang dapat dihubungi eMail
Terverifikasi	Apakah email orang yang dihubungi diverifikasi atau tidak
Negara	Negara
Perangkat	Jumlah perangkat yang terdaftar
Tanggal Pendaftaran	Titik waktu pemberian lisensi
Login Terakhir	Login akun admin terakhir
Lisensi	Tampilan jenis lisensi (Gratis|Berbayar)
Lisensi CB	Jenis lisensi ContentBox (Gratis|Berbayar)
Status	Status AppTec-Klien saat ini
Kadaluarsa	Menampilkan, jika lisensi telah kedaluwarsa
iOS	Jumlah Perangkat iOS
Android	Jumlah Perangkat Android
Windows Mobile	Jumlah Perangkat Windows Mobile
MacOS	Jumlah Perangkat MacOS
Windows 10	Jumlah Perangkat Windows 10
Perusahaan Android	Jumlah Perangkat Perusahaan Android
IOS BYOD (Pendaftaran Pengguna)	Jumlah Perangkat IOS BYOD (Pendaftaran Pengguna)
IoT	Jumlah Perangkat IoT

Tanggal kedaluwarsa APNS

Menampilkan ikhtisar semua tanggal kedaluwarsa sertifikat APNS dari semua klien.

ID Klien	ID Klien
Nama Perusahaan	Nama Perusahaan
Tanggal Kedaluwarsa	Tanggal kedaluwarsa untuk sertifikat Apple APNS
Info	Informasi tentang kedaluwarsa

Kontak

Ada pertanyaan tambahan? Cukup hubungi kami di bawah:

Untuk pertanyaan teknis umum

support@apptec360.com

+41 61 511 3210

Untuk pertanyaan yang terkait dengan pemasangan alat virtual

consulting@apptec360.com

+41 61 511 3214

Penafian