AppTec360 Kurumsal Mobil Yönetici ve ContentBox

Yönetim Kılavuzu | Sürüm 5.0 (202110)

İçindekiler

- Kapatma Cihazı
- Cihazı Yeniden Başlat
- Alarm ve Kayıp Modu | Kayıp Modunu Devre Dışı Bırak
- Cihazı Sil
- Silme Cihazı
- Enterprise Wipe | MDM'yi Kaldır
- Mesaj Gönder
- TeamViewer Uzaktan Kumanda
- Kayıt Talebi Gönder

Android

- Cihazı Düzenle
- Parolayı Temizle
- Kilit Cihazı
- Cihazı Sil
- Silme Cihazı
- MDM'yi kaldırın
- Mesaj Gönder
- COPE Moduna Dönüştür
- Kayıt Talebi Gönder
- Eski Cihazı Taşıma

Pencereler

- Cihazı Düzenle
- Cihazı Sil
- Enterprise Wipe | MDM'yi Kaldır
- TeamViewer Uzaktan Kumanda
- Kayıt Talebi Gönder

İçerik Yönetimi

- Grup Dosyaları
- Dosya Gezgini
- Denetim İzi
- Çöp
- Harici Depolama

Denetim Günlüğü

iOS Yapılandırması

- SecurePIM Güvenlik
- SecurePIM Tarayıcı
- Değişim

Bağlantı Yönetimi

- Wi-Fi
  - Proxy Kurulumu
  - Güvenlik Türü
- VPN
  - VPN Türü
    - VPN
    - Uygulama Başına VPN
  - Proxy Kurulumu
- APN
- Hücresel
- HTTP Proxy
- AirPrint
- AirPlay

PIM Yönetimi

- Exchange Active Sync
- e-Posta
  - Gelen Posta
  - Giden Posta
- CalDav
- Abone Olunan Takvimler
- LDAP

Web Yönetimi

- Webclips
- Web İçerik Filtresi

Uygulama Yönetimi

- Kurumsal Uygulama Yöneticisi
  - Yüklü Uygulamalar (yalnızca cihaz düzeyinde)
  - Zorunlu Uygulamalar
    - Kurulum seçenekleri
  - Web Uygulamaları

- Kısıtlama ve Ayarlar
  - Kara Listeye Alınan / Beyaz Listeye Alınan Uygulamalar
  - SysApp Kısıtlamaları
  - App-VPN
  - Uygulama Ayarları
- Kurumsal Uygulama Mağazası
  - iTunes Uygulamaları
  - Şirket İçi
- Kiosk Modu
  - Uygulama Türü
    - Paket
    - URL
  - Kiosk Modu Ayarları

Android Enterprise – Tam Yönetilen Cihaz Yapılandırması

Genel

- Grup profiline genel bakış (yalnızca grup düzeyinde)
- Cihaza Genel Bakış (yalnızca cihaz düzeyinde)
- Konfigürasyon Revizyonu (sadece cihaz seviyesinde)
- Cihaz Günlüğü (yalnızca cihaz düzeyinde)
  - Komut Günlüğü
  - Olası komut durumları
- Cihaz Ayarları
  - İstemci Yapılandırması
  - Duvar Kağıdı

Varlık Yönetimi (yalnızca cihaz düzeyinde)

- Cihaz Bilgisi
  - Wi-Fi
- Hücresel
- Bluetooth

Güvenlik Yönetimi

- Hırsızlığa Karşı Koruma (yalnızca cihaz düzeyinde)
  - GPS Bilgileri (yalnızca cihaz düzeyinde)
  - Sil ve Kilitle (yalnızca cihaz düzeyinde)
  - Mesaj (yalnızca cihaz düzeyinde)

- Güvenlik Yapılandırması
  - Cihaz Parolası
  - AntiVirüs
- Kullanım Ömrü Sonu (yalnızca cihaz düzeyinde)
  - Silme (yalnızca cihaz düzeyinde)
- Kısıtlama Ayarları
  - Kısıtlamalar
- Sertifika Yönetimi

Bağlantı Yönetimi

- Wifi
  - Güvenlik Türü
    - WEP
    - WPA/WPA2
    - 802.1x EAP
- VPN
  - VPN Türü
    - VPN
    - Uygulama Başına VPN
- Kısıtlamalar

PIM Yönetimi

- Gmail Değişimi

Uygulama Yönetimi

- Kurumsal Uygulama Yöneticisi
  - Yüklü Uygulamalar (yalnızca cihaz düzeyinde)
  - Sistem Uygulamaları (yalnızca cihaz düzeyinde)
  - Zorunlu Uygulamalar
  - Kara ve Beyaz Liste
  - AE Sistem Uygulamaları
- Kısıtlamalar ve Ayarlar
  - Uygulama Yönetimi Ayarları
- Kurumsal Uygulama Mağazası
  - Şirket İçi
- Kurumsal Play Store
  - AE Play Store
- Kiosk Modu ve Başlatıcı

- Varlık Yönetimi (yalnızca cihaz düzeyinde)
  - Cihaz Bilgisi
    - Wi-Fi
  - Hücresel
  - Bluetooth
- Güvenlik Yönetimi
  - Hırsızlığa Karşı Koruma (yalnızca cihaz düzeyinde)
    - GPS Bilgileri (yalnızca cihaz düzeyinde)
    - Sil ve Kilitle (yalnızca cihaz düzeyinde)
    - Mesaj (yalnızca cihaz düzeyinde)
  - Güvenlik Yapılandırması
    - Cihaz Parolası
    - Konteyner Şifresi
    - AntiVirüs
  - Kullanım Ömrü Sonu (yalnızca cihaz düzeyinde)
    - Silme (yalnızca cihaz düzeyinde)
  - Kısıtlama Ayarları
    - Kısıtlamalar
  - Sertifika Yönetimi
- Bağlantı Yönetimi
  - Wifi
    - Güvenlik Türü
      - WEP
      - WPA/WPA2
      - 802.1x EAP
  - VPN
    - VPN Türü
      - VPN
      - Uygulama Başına VPN
  - Kısıtlamalar
- PIM Yönetimi
  - Gmail Değişimi
- Uygulama Yönetimi
  - Kurumsal Uygulama Yöneticisi
    - Yüklü Uygulamalar (yalnızca cihaz düzeyinde)

- Güvenlik Yapılandırması
  - Şifre
  - Şifreleme
  - AntiVirüs
- Kullanım Ömrü Sonu (yalnızca cihaz düzeyinde)
  - Silme (yalnızca cihaz düzeyinde)
- Kısıtlama Ayarları
  - Kısıtlamalar
  - AE Cihaz Sahibi

BYOD Konteyner

- Android Kurumsal
  - Android Kurumsal
  - Gmail Değişimi
  - AE Sistem Uygulamaları
  - Konteyner Şifresi
- Samsung KNOX
  - Aktivasyon
  - Knox Parolası
  - Knox Güvenlik
  - Knox Exchange
  - Knox e-Posta
  - Knox Uygulamaları

Bağlantı Yönetimi

- Wifi
  - Güvenlik Türü
    - WEP
    - WPA/WPA2
    - 802.1x EAP
- VPN
- Kısıtlamalar
- APN
- Bluetooth

PIM Yönetimi

- Değişim
- e-Posta

- AE Gmail Değişimi

Uygulama Yönetimi

- Kurumsal Uygulama Yöneticisi
  - Yüklü Uygulamalar (yalnızca cihaz düzeyinde)
  - Sistem Uygulamaları (yalnızca cihaz düzeyinde)
  - Zorunlu Uygulamalar
  - AE Sistem Uygulamaları
- Kısıtlamalar ve Ayarlar
  - Kara ve Beyaz Liste
  - Sistem Uygulama Kısıtlamaları
    - Samsung Uygulamaları
    - Huawei Uygulamaları
  - Uygulama Yönetimi Ayarları
- Kurumsal Uygulama Mağazası
  - Playstore
  - Şirket İçi
- Kurumsal Play Store
- Kiosk Modu ve Başlatıcı
  - Kiosk Modu
  - AppTec360 Başlatıcı
  - AppTec360 Ayarları

Uzaktan Kumanda

- Splashtop
- Teamviewer

İçerik Yönetimi

- İçerik kutusu
- Güvenli Tarayıcı

Yapılandırma Windows 10 PC

Genel

- Grup profiline genel bakış (yalnızca grup düzeyinde)
- Cihaza Genel Bakış (yalnızca cihaz düzeyinde)
- Ayarlar
- Konfigürasyon Revizyonu (sadece cihaz seviyesinde)
- Cihaz Günlüğü (yalnızca cihaz düzeyinde)

- Komut Günlüğü
- Olası komut durumları
- Varlık Yönetimi (yalnızca cihaz düzeyinde)
  - Cihaz Bilgisi
  - Hücresel
  - Senkronizasyon Bilgisi
- Güvenlik Yönetimi
  - Hırsızlığa Karşı Koruma (yalnızca cihaz düzeyinde)
    - GPS Bilgileri (yalnızca cihaz düzeyinde)
    - GPS Ayarları
  - Güvenlik Yapılandırması
    - Şifre
    - Antivirüs
    - Güvenlik Merkezi
    - Güvenlik Duvarı Yapılandırması
    - Güvenlik Duvarı Kuralları
  - Kısıtlama Ayarları
    - Cihaz İşlevselliği
  - BitLocker
    - BitLocker Yapılandırması
    - BitLocker Durumu
  - Sertifika Yönetimi
    - Sertifika Listesi
    - Sertifika Yapılandırması
    - SCEP
- Bağlantı Yönetimi
  - Wifi
    - Güvenlik Türü
    - Proxy Sunucusu Kullan
  - Wifi Kısıtlamaları
  - VPN
    - Bağlantı türü
    - Genel VPN Yapılandırmaları
  - VPN Kısıtlamaları
  - Bluetooth
- PIM Yönetimi
  - Exchange Active Sync

- e-Posta
- Uygulama Yönetimi
  - Kurumsal Uygulama Yöneticisi
    - Yüklü Uygulamalar
    - Zorunlu Uygulamalar
    - Sistem Uygulama Kısıtlamaları
    - Kara ve Beyaz Liste

MacOS Yapılandırması

Genel

- Grup profiline genel bakış (yalnızca grup düzeyinde)
- Cihaza Genel Bakış (yalnızca cihaz düzeyinde)
- Konfigürasyon Revizyonu (sadece cihaz seviyesinde)
- Cihaz Günlüğü (yalnızca cihaz düzeyinde)
  - Komut Günlüğü
  - Olası komut durumları

Varlık Yönetimi (yalnızca cihaz düzeyinde)

- Cihaz Bilgisi
- WiFi
- Hücresel
- Bluetooth

Güncelleme Yönetimi (yalnızca cihaz düzeyinde)

- Güncelleme Bilgileri

Güvenlik Yönetimi

- Hırsızlığa Karşı
  - Sil ve Kilitle
- Güvenlik Yapılandırması
  - Şifre
  - Sertifika
- Kısıtlama Ayarları
  - Cihaz İşlevselliği
  - iCloud
  - Medya Yönetimi

Bağlantı Yönetimi

- Wi-Fi

Genel Bakış

AppTec360’a Giriş

AppTec'in Kurumsal-Mobil-Yönetim-Çözümü, sezgisel yönetim konsolu ile tüm mobil cihazları yönetme ve yapılandırma seçeneği sunar. Bu senaryoda, EMM sunucusu kendi ortamınızda çalışabilir veya bulut tabanlı çözümümüzü kullanabilirsiniz.

Kurumsal uygulamaların akıllı telefonlara merkezi olarak yüklenmesi konusunda bile doğru yere geldiniz. Enterprise Mobile Manager ile kurumsal uygulamaları ve belgeleri saniyeler içinde cihazlara dağıtabilir veya istenmeyen uygulamaları beyaz/kara listeye alarak engelleyebilirsiniz.

Şirketlerde özel cihazların kullanılması, akıllı telefon ve tabletlerin güvenliğini sağlamak için yeni bir zorluk oluşturmaktadır. Çalışanların akıllı telefonlarını giderek daha fazla kullanmak istemeleri nedeniyle, BT yöneticileri çok sayıda farklı türde cihazı korumak zorundadır. Tüm cihazların ve bunlarda depolanan hassas verilerin güvenliğini sağlamanıza ve bunları sezgisel bir konsoldan yönetmenize yardımcı olacağız.

Desteklenen Cihaz İşletim Sistemleri

AppTec360 iOS, Android ve Windows cihazları için destek sunar. Söz konusu platformların işlev kapasitesinin bir işletim sisteminden diğerine farklı olabileceğini lütfen unutmayın.

- Apple iOS 11.0 veya üzeri*
- Apple macOS 10.11 veya üstü
- Bulut Sürümünde Google Android 4.4 veya üstü**
- OnPrem Sürümünde Google Android 4.1 veya üstü**
- MS Windows 10 veya üstü*** (Masaüstü-Bilgisayar, Dizüstü Bilgisayar ve Tablet)

**Apple tarafından kayıt sürecinde yapılan köklü değişiklikler nedeniyle iOS 10 veya önceki sürümlere sahip cihazların kaydedilemeyeceğini lütfen unutmayın.*

***Cihazlar, üretici tarafından artık desteklenmeyen bir sürüm kullanıyor olsalar bile bağlanabilir ve yapılandırılabilir. Belirli bir Android Sürümü gerektiren özellikler olabileceğini lütfen unutmayın. Destek vakalarında, üreticinin resmi desteğini takip ediyoruz. Üretici tarafından artık desteklenmeyen eski bir sürümden kaynaklanan sorunlar veya hatalar olması durumunda, yalnızca sınırlı destek sunma hakkımızı saklı tutarız.*

****Windows'un Ev Sürümü, İşletim Sisteminin sınırlamaları nedeniyle desteklenmemektedir. Üretici tarafından hala desteklenen bir işletim sistemi sürümü kullanmanızı şiddetle tavsiye ederiz. Sadece uyumluluk için değil, aynı zamanda güvenlik nedenleriyle de. Bu nedenle iOS 12 veya üstünü ve Android 9 veya üstünü öneriyoruz.*

Desteklenen LDAP Dizinleri

- Microsoft Active Directory
- Açık LDAP

"Desteklenen Cihaz İşletim Sistemleri" ve "Desteklenen LDAP Dizinleri" hakkında güncel bilgilere buradan ulaşabilirsiniz:

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

Apple Cihazlarında “Gözetimli Mod” Açıklaması

Denetimli Mod, iOS cihazları için genişletilmiş bir arayüzü temsil eder.

Sırasıyla yapılandırılan cihazda, son kullanıcı cihazının işlevselliği ile ilgili ek sınırlamalar uygulanabilir. Bunlar aynı zamanda yönetim el kitabında da yer alır ve bir afişle işaretlenir.

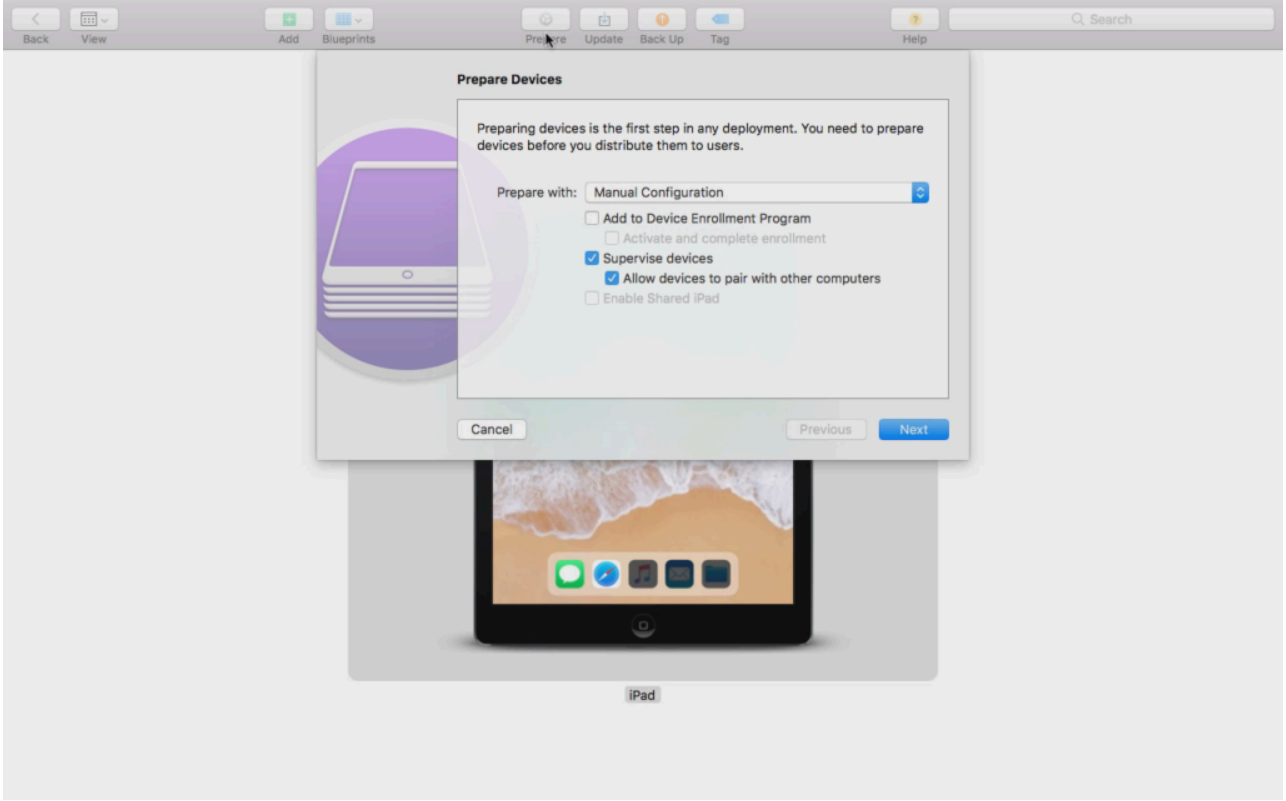
Denetimli Modda kullanılabilir

"Denetimli Mod", "Apple Configurator" programı ile etkinleştirilebilir. Apple Configurator, bir yapılandırma aracı olarak (USB arayüzü üzerinden) yeni iOS cihazlarında varsayılan ayarları ayarlayabilir.

Araç yalnızca yapılandırma profillerini değil, uygulamaları da yükleyebilir. Ücretsizdir, ancak bir Mac bilgisayar gerektirir.

Denetimli modu etkinleştirin

1. Apple Configurator'ı açın



2. Cihaza tıklayın ve "Hazırla "yı seçin
3. "Manuel Yapılandırma" ve "Cihazları denetle "yi seçin
4. "İleri" üzerine tıklayın
5. (İsteğe bağlı) Şimdi cihazın kaydedileceği bir MDM Sunucusu ekleyebilirsiniz. Bunun için bağlantı "Genel Ayarlar - iOS Yapılandırması - Yapılandırıcı ve URL" bölümünde bulunabilir Kuruluşunuzu seçin veya yeni bir tane oluşturun
6. Kuruluşunuzu seçin veya yeni bir tane oluşturun
7. İlk kurulumda hangi adımların atlanması gerektiğini seçin ve "İleri "ye tıklayın (DİKKAT: Devam etmek cihazınızı silecektir!)

Şimdi cihazınız denetimli moda alınacaktır. Bu işlem birkaç dakika sürebilir. İşlem tamamlandıktan sonra cihaz yeniden başlatılacaktır.

Artık cihazınız denetleniyor!

DEP’e bir cihaz ekleme

Aygıtlarınız iOS 11 veya daha yüksek bir sürümdeyse Apple Configurator'ı kullanarak DEP'e (Aygıt Kayıt Programı) aygıt da ekleyebilirsiniz.

DEP Hakkında Daha Fazla Bilgi: https://www.apple.com/business/dep/

Bir cihazı denetlediğiniz gibi aynı adımları izleyin ve ek olarak "Cihaz Kayıt Programına Ekle" seçeneğini işaretleyin. Daha önce Apple Configurator ile DEP'e hiç giriş yapmadıysanız, DEP giriş bilgileriniz istenecektir.

İşlem tamamlandıktan sonra, cihaz DEP Sunucusu "Apple Configurator 2 Tarafından Eklenen Cihazlar" bölümünde bulunabilir. Artık bu Sunucuyu kullanabilir ve yönetim konsoluna bağlayabilir veya cihazı zaten var olan bir sunucuya aktarabilirsiniz.

Artık DEP'e başarıyla bir cihaz eklediniz!

Android Enterprise'ın Açıklaması

Android Enterprise nedir?

Android Enterprise, bir MDM ile yönetilen iş cihazlarının daha iyi kontrol edilmesini sağlar. Bu, yöneticilerin android cihazları üzerinde tam kontrole sahip olmalarını veya şirket verilerini konteyner cihazlarındaki özel verilerden ayırmalarını sağlar. Ayrıca Android Enterprise, cihazların daha kolay kaydedilmesine ve kolay uygulama dağıtımına olanak tanır.

Android Enterprise'ı kullanmak için gerekenler nelerdir?

Android Enterprise herkes tarafından ücretsiz olarak kullanılabilir. Tüm Android Enterprise özelliklerini etkinleştirmek için MDM'ye yalnızca bir google hesabı bağlamanız gerekir. Bununla ilgili daha fazla bilgiyi Android Enterprise bölümünde bulabilirsiniz.

Android Enterprise, Geliştirilmiş Çalışma Profili (aşağıya bakınız) haricinde Android 5.1 veya üzeri cihazlarda kullanılabilir. Daha kolay bir kayıt için en az Android 7 veya üstünü ya da mevcut tüm özelliklerden yararlanmak için Android 11'i öneriyoruz.

Android Enterprise ile mevcut modlar nelerdir?

Android Enterprise'ı kullanırken kullanabileceğiniz 3 farklı mod vardır.

AE Tam Yönetilen Cihaz (İş Yönetilen): Yalnızca iş için kullanılan, tam olarak yönetilen bir cihaz. Bu, yöneticinin cihaz üzerinde tam kontrol sahibi olmasını sağlar. Bu, cihazın özel kullanımına izin vermez. Cihazları bu moda kaydetmek için cihazların sıfırlanması ve bir QR Kodu ile kaydedilmesi (bkz. AE Kaydı) veya Knox Kaydı veya Zero Touch ile kaydedilmesi gerekir.

AE BYOD Konteyneri: BYOD (kendi cihazını getir) Konteyneri, kullanıcıların şirket verilerine ayrı bir konteynerdeki özel telefonlarından erişmelerini sağlar. Bu modda, özel uygulamalar şirket verilerini ve uygulamalarını göremez ve bunun tersi de geçerlidir. Cihazları bu moda kaydetmek için AppTec uygulaması indirilmeli ve bir QR Kodu taranmalıdır. Konsolda bir cihaz oluşturun ve cihaz türü olarak "AE Container (BYOD & Enahnced Work Profile)" seçin. QR Kodunu almak için yeni oluşturulan cihazdaki QR Koduna tıklayın ve ilk anahtarı "Legacy & BYOD" olarak ayarlayın.

AE Geliştirilmiş İş Profili: (Android 11 veya üstü gerektirir) Yukarıda bahsedilen BYOD Konteyneri şirket verilerini özel bir cihaza getirirken, Geliştirilmiş İş Profili aynı şeyi şirkete ait bir cihaz için yapar. Aynı konteyneri oluşturur, ancak yöneticiye cihaz üzerinde biraz daha fazla kontrol sağlar, böylece kullanıcı MDM'yi cihazdan kolayca kaldıramaz. Konsolda bir cihaz oluşturun ve cihaz türü olarak "AE Container (BYOD & Enahnced Work Profile)" seçin. QR Kodunu almak için yeni oluşturulan cihazdaki QR Koduna tıklayın ve ilk anahtarı "Geliştirilmiş Çalışma Profili" olarak ayarlayın. Bu QR Kodu, cihazı sıfırladıktan ve AE Kaydı'nda Yöntem 1'de açıklandığı gibi ekrana 6 kez dokunduktan sonra taranabilir.

Android Enterprise cihazlarına nasıl uygulama atayabilirim?

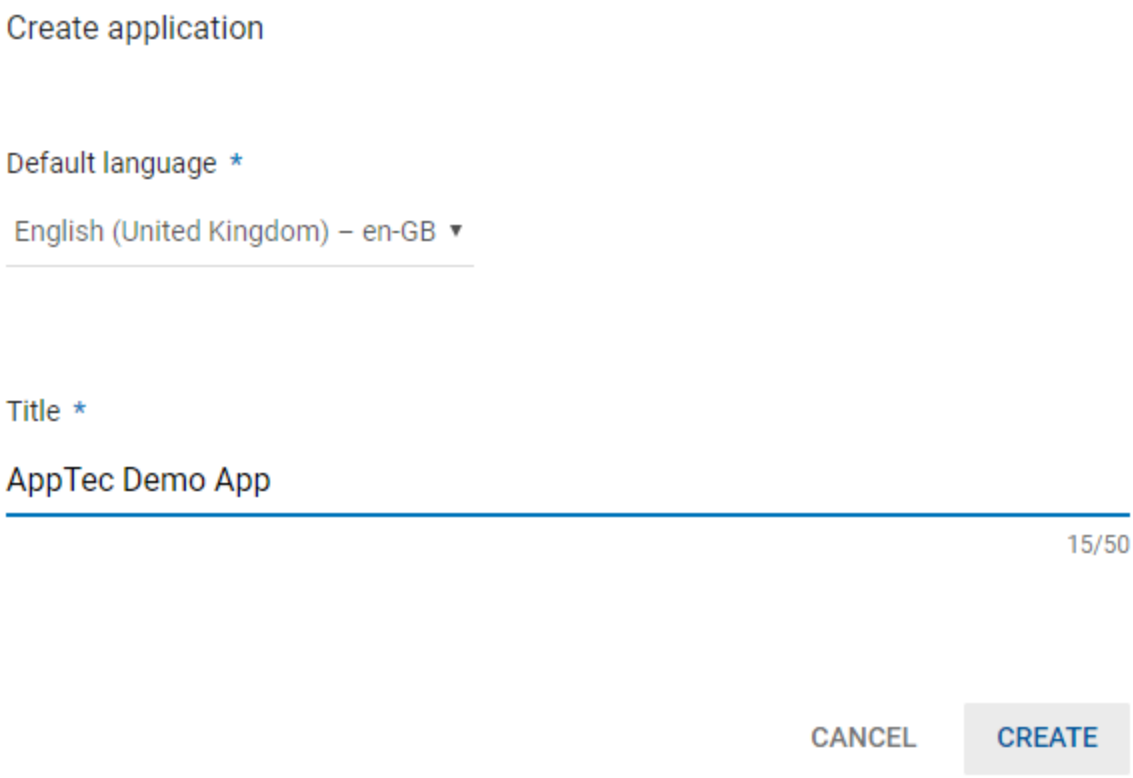
Öncelikle Genel Ayarlar → Uygulama Yönetimi → AE Play Store → Play Store Uygulamaları bölümünde kullanmak istediğiniz Uygulamaları onaylamanız gerekir. Bir uygulamayı onayladıktan sonra, "+" işaretine tıklayarak ve "AE Play Store" sekmesinden uygulamayı seçerek profilinizin zorunlu uygulama listesine → atayabilirsiniz. Bu, uygulamayı otomatik olarak indirecek ve yükleyecektir. Cihaz üzerinde herhangi bir google hesabı gerekmez ve kullanıcının bunu onaylaması veya izin vermesi gerekmez.

Kendi Uygulamalarınızı Google Play Store'a yükleyin

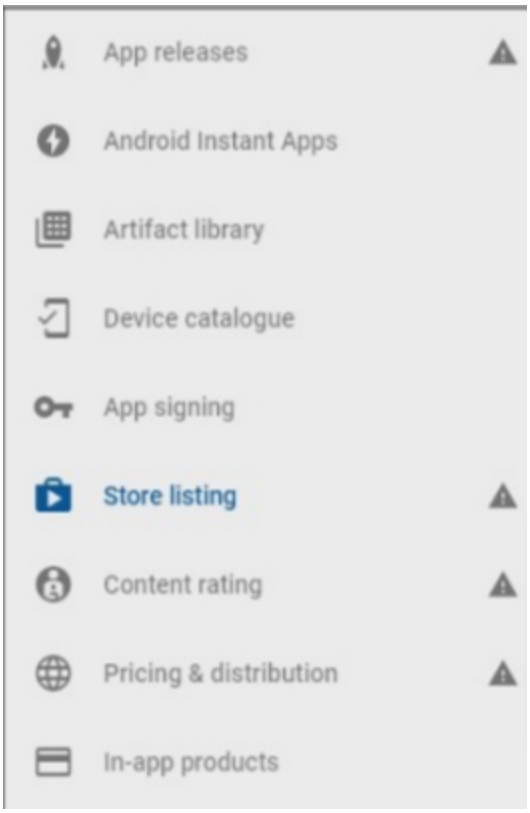
Kurum içi uygulamalarınızı Google Play Store'a yüklemeniz mümkündür. Bu şekilde Play Store'un güncelleme mekanizması gibi farklı avantajlardan yararlanabilirsiniz.

Bunu yapmak için bir Google Geliştirici Hesabına ihtiyacınız vardır. Google Play Console'u kullanarak giriş yapın(https://play.google.com/apps/publish)

"Uygulama Oluştur" seçeneğine tıklayın. Varsayılan dilinizi ve uygulamanın başlığını seçin.



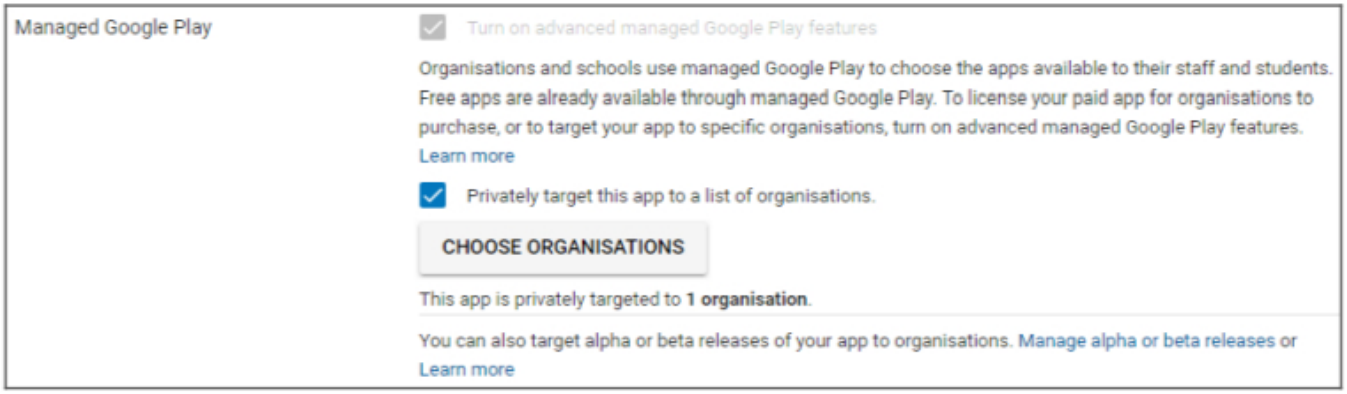
Takip eden sayfada, uygulamanızla ilgili farklı ayrıntıları girmeniz istenecektir.



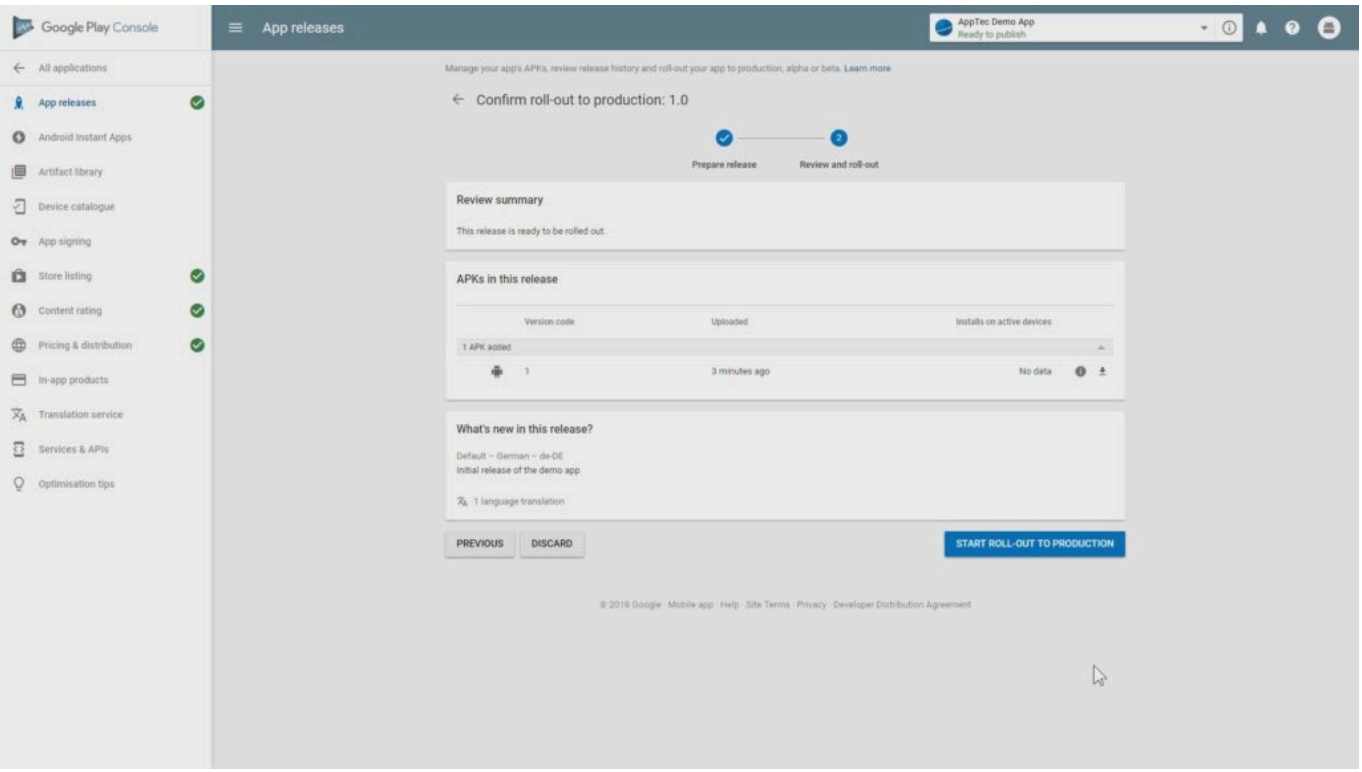
Tüm detayları girdikten sonra, sol tarafta farklı ipucu sembolleri göreceksiniz.

Hangi adımların kaldığını görmek için üzerlerine gelin ve bunları istediğiniz sırayla takip edin.

Not: "Fiyatlandırma ve Dağıtım" altındaki "Yönetilen Google Play" bölümündeki iki onay kutusunu işaretlediğinizden emin olun. Aksi takdirde uygulama herkese açık olacak ve herkes tarafından erişilebilecektir. Ayrıca dağıtım için ülkeyi seçtiğinizden emin olun.



Her adımı tamamladıktan sonra "Uygulama yayınları "na gidebilirsiniz. Taslağınızı son haline getirmek ve uygulamayı yayınlamak için "Gözden Geçir" ve "Üretime Sunmaya Başla "ya tıklayın.



Uygulamanın Play Store'da kullanıma sunulması biraz zaman alacaktır. İşlem tamamlandıktan sonra, uygulamanızı Play for Work mağazasında arayabilir ve onaylayabilirsiniz. Bundan sonra, tıpkı diğer uygulamalarda yaptığınız gibi EMM konsolunu kullanarak uygulamayı cihazlara atayabilirsiniz.

Gereksinimler ve Kurulum

Gereksinimler

Sistem gereksinimleri

Sanal cihaz Açık Sanallaştırma Formatında (VMWare, VirtualBox, Citrix Xen Server) ve sıkıştırılmış .vhdx (Hyper-V) dosyası* olarak mevcuttur.

*Not: Hyper-V kullanılırken makine Generation 1 ile oluşturulmalıdır.

Sanal diskin hedef boyutu 20 GB'tır ve makine 4 GB RAM gerektirir.

Cihaz Debian 9 64bit tabanlıdır

İçe aktarılan makineyi en yeni uyumluluğa yükseltin (örneğin VMWare'de) ve makine işletim sistemi türünün hipervizörünüzde doğru ayarlandığından emin olun.

Lisans anahtarı

Sunucuyu başarılı bir şekilde etkinleştirmek ve kurmak için geçerli bir lisans dosyasına ihtiyacınız olacaktır. Doğrudan AppTec360'tan ve/veya ilgili satıcınızdan bir tane edinebilirsiniz.

IP-Adresi ve DNS Çözünürlüğü

AppTec360 cihazına, lisansın verildiği ana bilgisayar adını kullanan cihaz tarafından erişilebilir olmalıdır.

Windows 10 cihazlarını kaydetmek için ayrıca cihaza işaret eden "enterpriseenrollment." şeklinde ek bir alt alan adı kurmanız gerekir.

SSL Sertifikası

Cihazlara giden ve cihazlardan gelen tüm bağlantıların SSL kullanılarak güvence altına alınması gerektiğinden, cihaz tarafından güvenilen bir Sertifika Yetkilisi tarafından verilen ana bilgisayar adı için geçerli bir sertifikaya ihtiyacınız vardır. Sertifika için özel anahtar, parola koruması olmadan yüklenmelidir. Çoğu durumda, cihazların sunucu sertifikasını tanıması için CA için bir ara sertifika gereklidir.

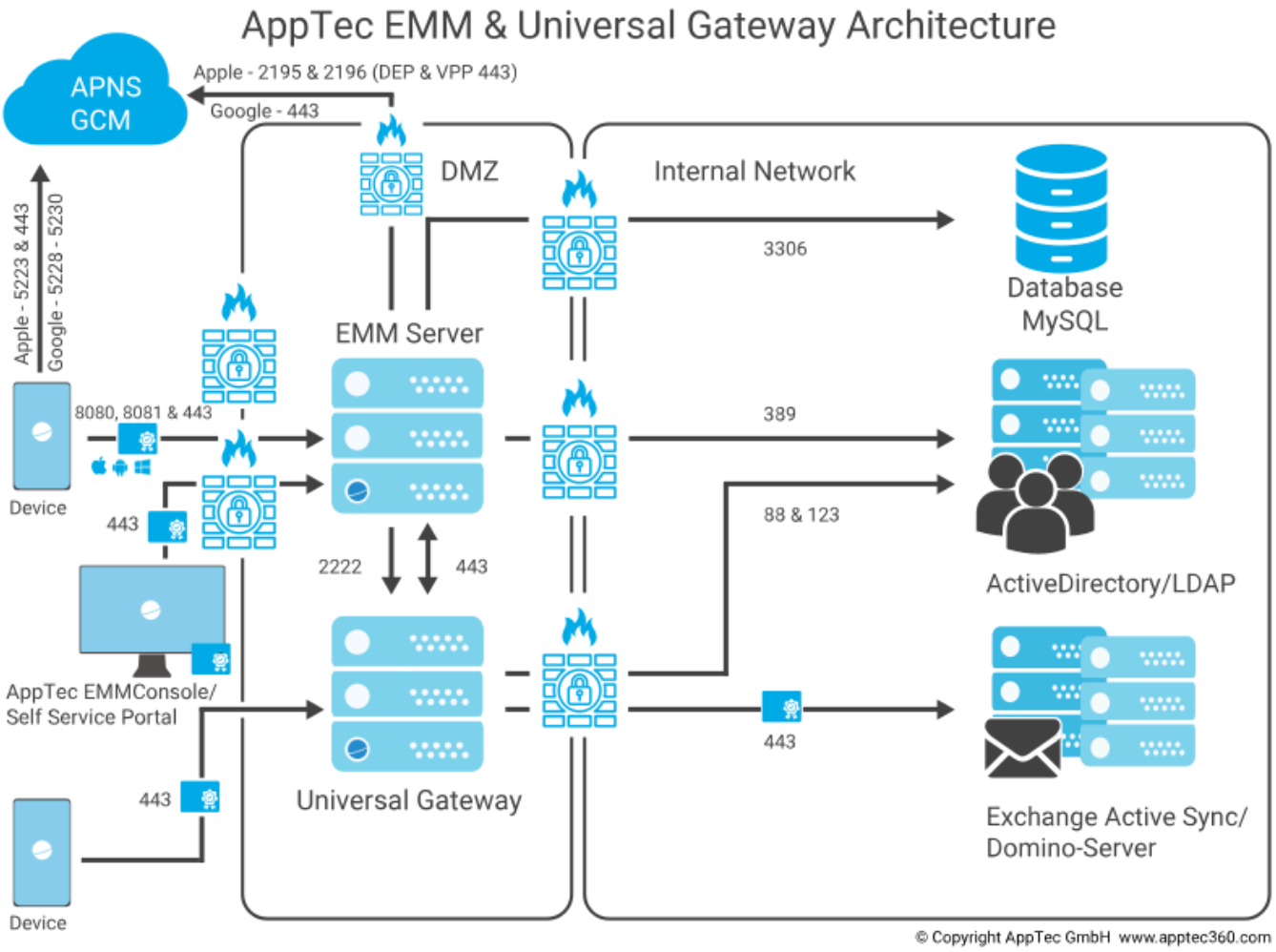
Windows 10 cihazları, enterpriseenrollment alt alan adınız için özel bir sertifika gerektirecektir.

Cihaz sürümü 202104 ile başlayarak, otomatik olarak oluşturulan Let's Encrypt sertifikalarını da kullanabilirsiniz (İkinci Adım - SSL Sertifikası bölümünde açıklanmıştır).

SMTP Sunucusu

AppTec360 EMM'nin e-posta göndermesine izin vermek için (örneğin cihaz kaydı ve hesap doğrulama için) bir e-posta sunucusu ve/veya bir e-posta rölesi gereklidir.

Güvenlik Duvarı Kuralları



Bu diyagram, kullanmak istediğiniz hizmetlere bağlı olarak hangi bağlantının gerekli olduğunu gösterir.

Daha ayrıntılı bir açıklama için bir sonraki sayfadaki tabloya bakın.

Herhangi biri (harici/Cihazlar)	→	**AppTec360 Appliance / emmconsole.com**
Limanlar	443	Yönetim, Kurumsal AppStore ve Windows Phone İletişimi
	8080	Android ve iOS İletişimi
	80	Let´s Encrypt ilk kez kuruluyor. Daha sonra 443 kullanır.
Herhangi biri (Cihazlar)	→	**Herhangi biri (harici)**
Limanlar	5223, 443	Apple Push Service, proxy olmadan erişilebilir olmalıdır, Fallback olarak 443, bkz. https://support. apple.com/en-us/HT203609
	5228-5230	Android Push Hizmeti (FCM), proxy olmadan erişilebilir olmalıdır
AppTec360 Cihaz	→	**Etki Alanı Denetleyicisi**
Limanlar	389, (LDAPS 636)	LDAP ile kullanıcı senkronizasyonu
AppTec360 Cihaz	→	**Herhangi bir**
Liman	443	Android Push Hizmeti (GCM) için kullanılır AppStore / Play Store araması
AppTec360 Cihaz	→	**emmconsole.com**
Limanlar	443	AppTec360 Appliance Güncellemeleri, APNS sertifikası oluşturma
AppTec360 Cihaz	→	**Apple Ağı (17.0.0.0/8)**
Limanlar	2195, 2196	Apple Push Hizmeti ve Geri Bildirim Hizmeti
	443	DEP & VPP

Güvenlik Güncellemeleri

Debian işletim sistemi, en yeni güvenlik düzeltmelerini almak için düzenli olarak güncellenmelidir. Ancak Debian'ın daha yeni bir ana sürümüne manuel olarak yükseltme yapmadığınızdan emin olun. AppTec360 EMM daha yeni bir ana sürümle uyumlu olduğunda, bir cihaz güncellemesinde yükseltme için bir yol ekleyeceğiz.

Sanal Uygulamanın Varsayılan Parolaları

Giriş Kullanıcısı (Root girişi devre dışıdır. Yönetim görevleri için "sudo" kullanın)

apptec

Giriş Şifresi

apptec

MySQL Kök Kullanıcısı

kök

MySQL Kök Parolası

apptec

MySQL Varsayılan Kullanıcısı

AppTec

MySQL Varsayılan Kullanıcı Parolası

AppTec

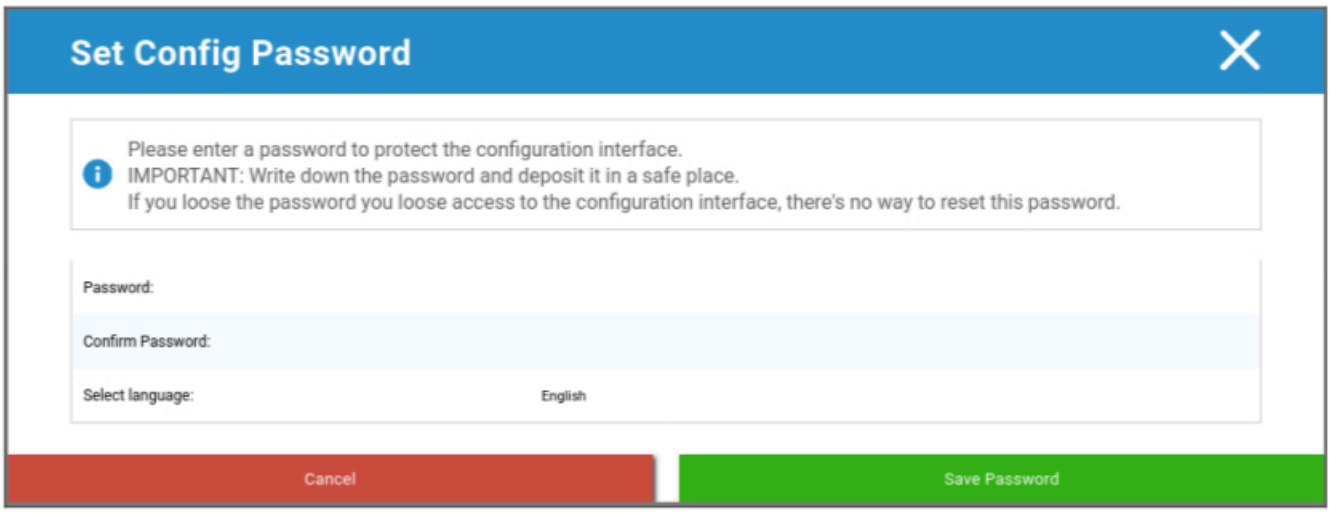
Sanal Uygulamanın Yapılandırılması

Önemli: Sanal Uygulamanın yapılandırmasına başlamadan önce ekran çözünürlüğü en az 1280 x 800 piksel olarak ayarlanmalıdır.

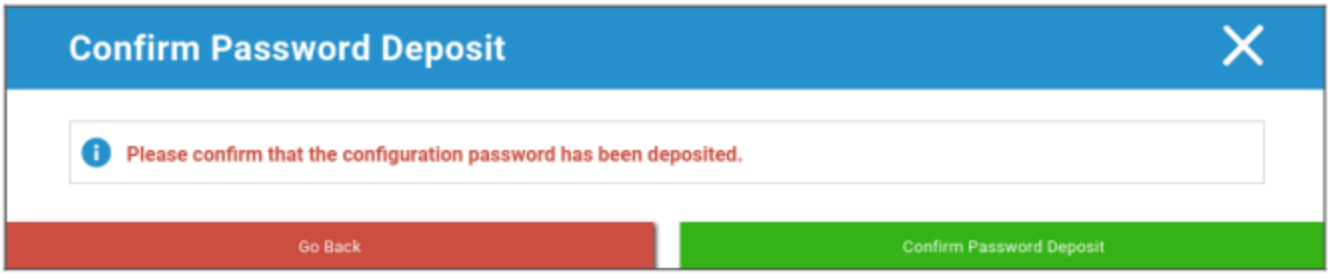
Cihaza uzun süre giriş yaptıktan sonra, Firefox otomatik olarak başlatılmalı ve yapılandırma arayüzünü görüntülemelidir.

Hazırlık

Öncelikle yapılandırma arayüzü için bir parola sağlamanız gerekir. Bu parola, yapılandırma arayüzüne girilen tüm bilgileri ve dosyaları şifrelemek için kullanılır. Burada ayrıca arayüzün görüntülenmesi gereken dili de ayarlayabilirsiniz (daha sonra değiştirilebilir).

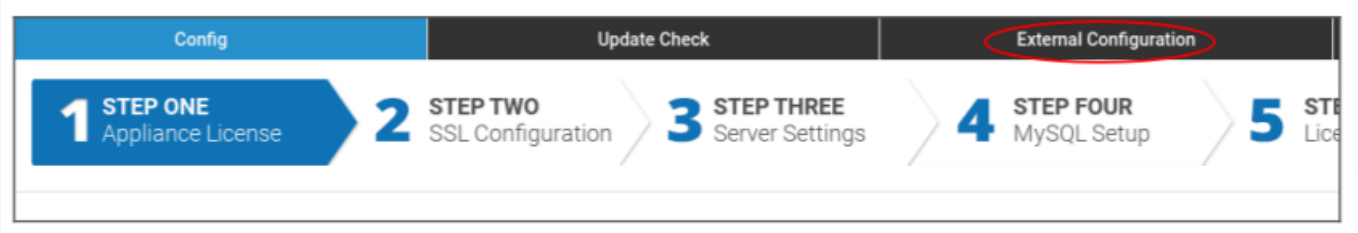


Parola yalnızca AppTec360 Destek tarafından sıfırlanabilir, bu nedenle güvenli bir yere koyduğunuzdan ve yaklaşan açılır pencereyi onayladığınızdan emin olun.



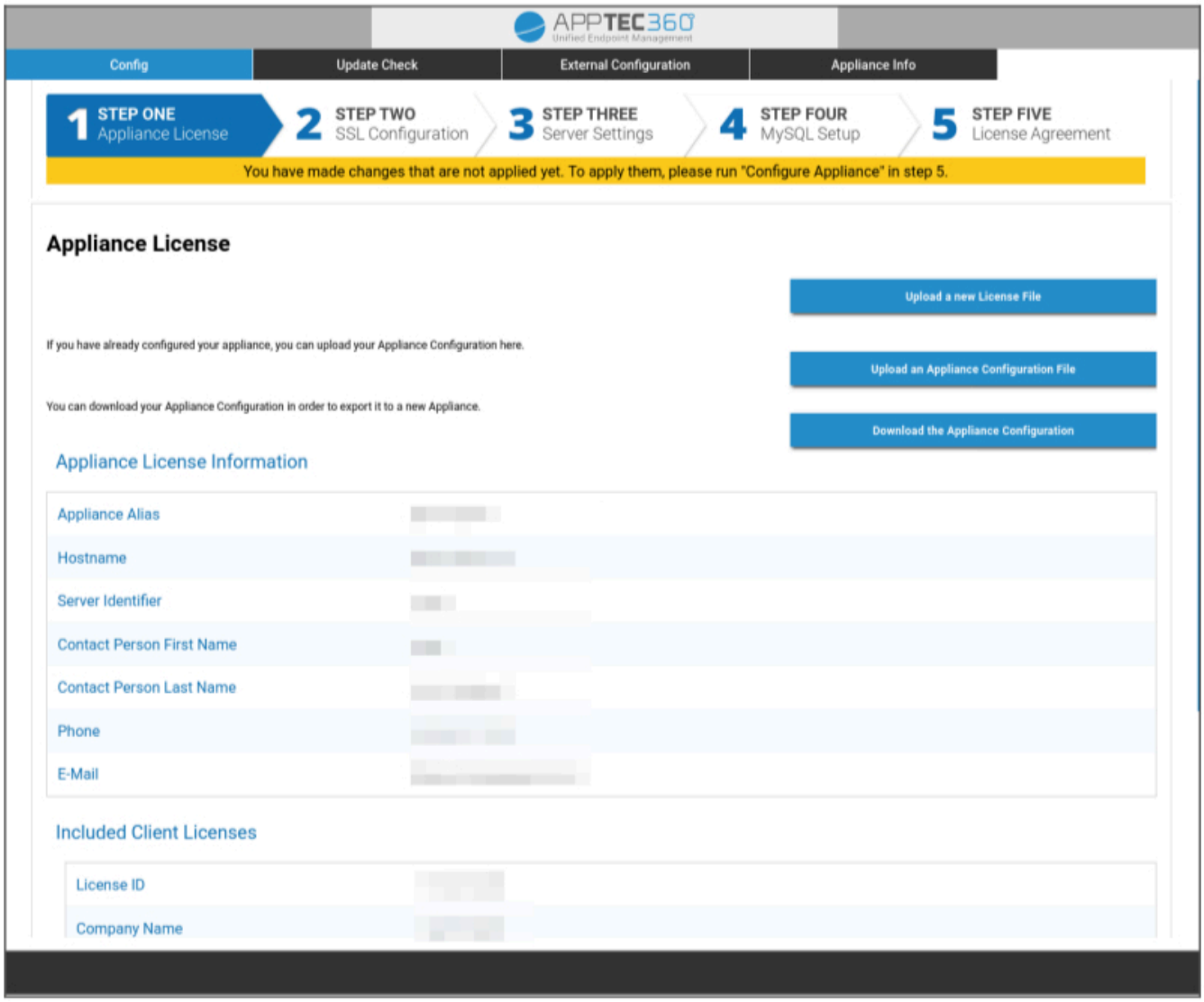
Harici ana bilgisayardan yapılandırma

Kurulum sürecini kolaylaştırmak için yapılandırma sayfasını uzaktan erişilebilir hale getirebilirsiniz. Bunu yapmak için "Harici ana bilgisayardan yapılandırma" bölümündeki adımları izleyin.



Birinci Adım – Cihaz Lisansı

1. Lütfen AppTec'ten aldığınız lisans dosyasını yükleyin.
2. Lisans dosyası başarıyla yüklendiyse, aşağıdaki ekran görüntüsünde olduğu gibi cihaz lisans bilgilerini görebilirsiniz.



İkinci Adım – SSL Sertifikası

Let's Encrypt kullanarak otomatik sertifika kurulumunu kullanabilir veya sertifikaları kendiniz sağlayabilirsiniz (daha fazla bilgi için SSL-Sertifika bölümüne bakın).

Otomatik

Sertifika, Let's Encrypt hizmeti kullanılarak otomatik olarak oluşturulacaktır.

AppTec360 EMM, etki alanının doğrulanması için HTTP-01 meydan okumasını kullanır; bu, bir sertifikanın ilk talebi için HTTP bağlantı noktasının internetten açık olması gerektiği anlamına gelir. Sonraki yenileme talepleri HTTPS üzerinden doğrulanabilir.

Radyo düğmelerini "Otomatik (Let's Encrypt)" olarak değiştirin ve "DEĞERLERİ KAYDET" düğmesine basın. Sertifika, Adım Beş - Lisans Sözleşmesi'ndeki yapılandırma uygulanırken otomatik olarak istenecektir. Gerekirse sertifika otomatik olarak yenilenecek ve sertifika süresi dolmak üzereyse (yenilemenin başarısız olabileceği anlamına gelir) bir e-posta alacaksınız.

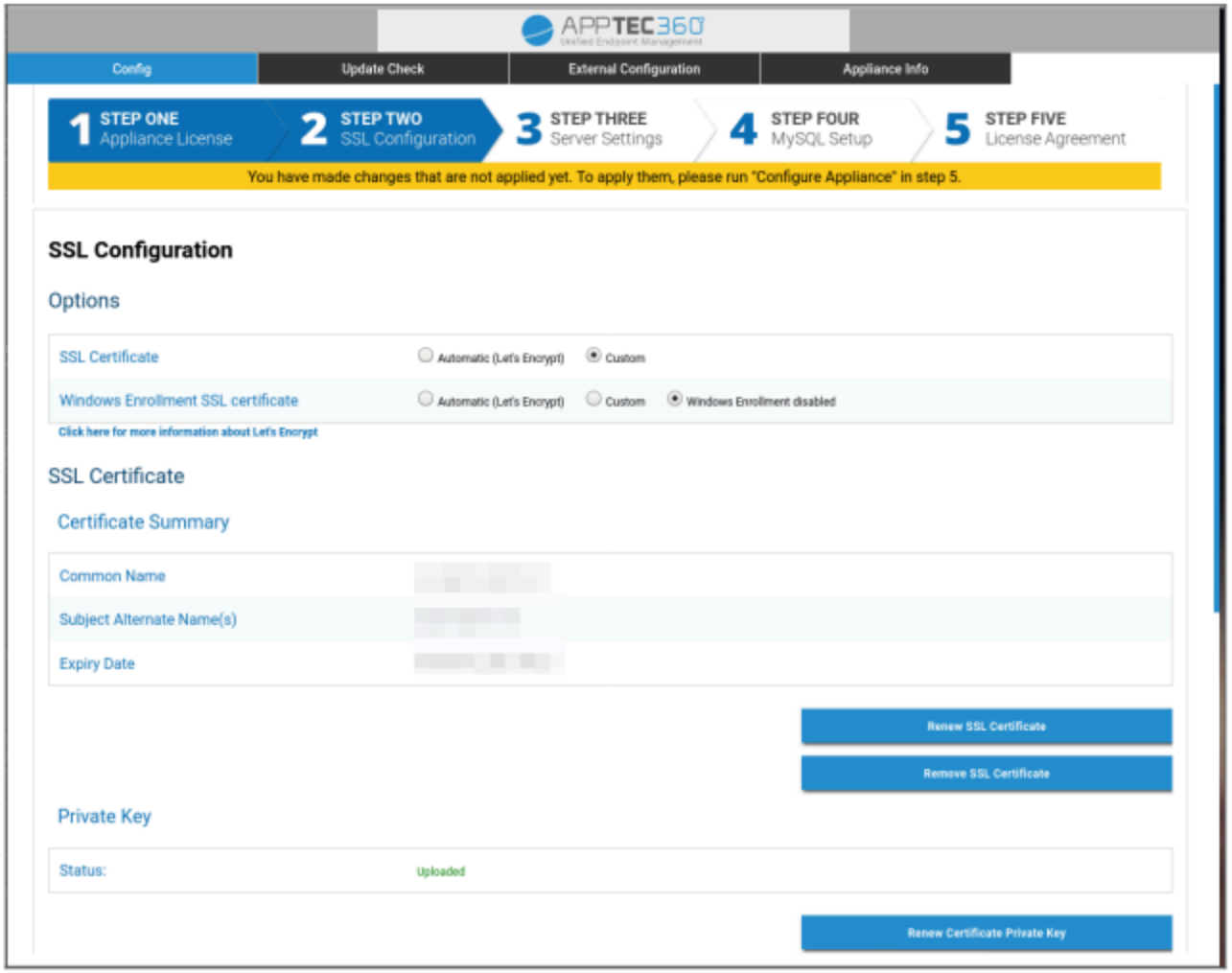
Özel

1. Lisanslı ana bilgisayar adınız için SSL Sertifikasını yükleyin. Ana bilgisayar adını Birinci Adım - Cihaz Lisansı bölümünde görebilirsiniz.

2. Lütfen sertifikanın özel anahtarını ve gerekirse ara sertifikayı da yükleyin.

Önemli: Anahtar parola korumalı olmamalıdır. Eğer öyleyse, lütfen yüklemeden önce şifreyi kaldırın.

İpucu: Windows 10 cihazlarını da kullanmak istiyorsanız, "Windows Kaydı SSL sertifikası "nı etkinleştirmeniz ve alt alan adınız için sertifika, özel anahtar ve ara sertifikayı (IP-Adresi ve DNS Çözünürlüğü bölümünde açıklanmıştır) sayfanın alt kısmına yüklemeniz gerekir.



Üçüncü Adım – Sunucu Ayarları

1. Lütfen global bir destek e-posta adresi girin. Bu adres, kullanıcılarınıza gönderilecek e-postalarda kullanılacaktır, böylece cihazlarıyla ilgili herhangi bir sorun olması durumunda kiminle iletişime geçeceklerini bilirler.
2. Sistem tarafından e-posta göndermek için kullanılacak E-Posta Ayarlarını sağlayın. Ayarlar, kullanıcıya e-posta göndermek ve ayrıca Hata Raporlarını ve Özellik İsteklerini"support@apptec360.com"adresine göndermek için kullanılacaktır. E-posta ayarlarınızı kaydettikten sonra "E-Posta Yapılandırmasını Test Et" seçeneğine tıklayarak ve talimatları izleyerek doğrulamanız gerekir.

Dördüncü Adım – MySQL Kurulumu

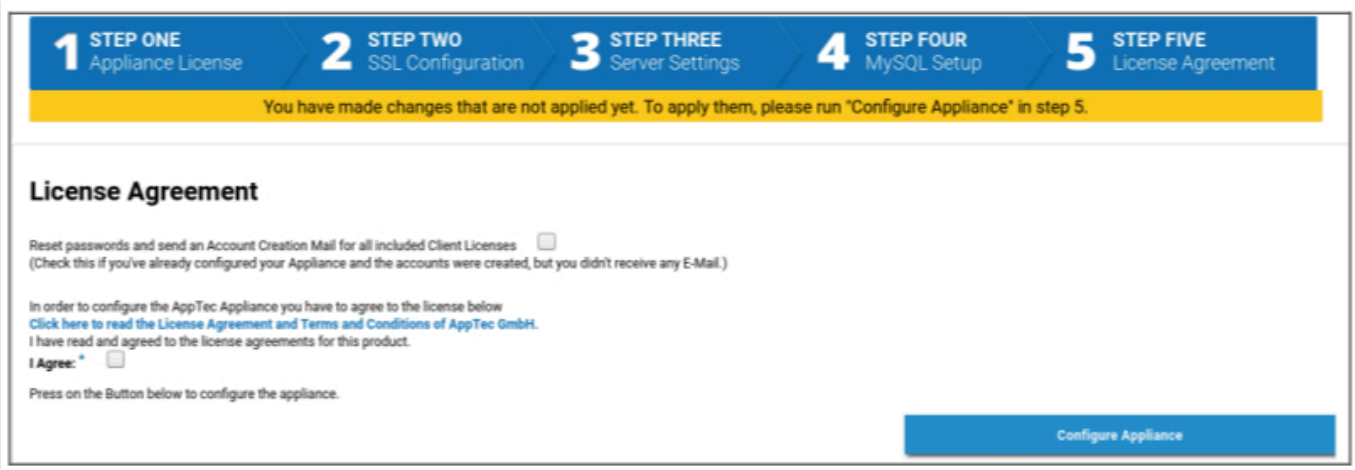
1. Dahili veritabanını kullanmak istiyorsanız bu adımı atlayabilirsiniz. Aksi takdirde harici veritabanı sunucunuzun bağlantı bilgilerini girebilirsiniz.


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)

Beşinci Adım – Lisans Sözleşmesi

1. Lütfen lisans sözleşmesini okuyun.
2. "Kabul Ediyorum" seçeneğini işaretleyin ve ayarları uygulamak için "Cihazı Yapılandır" düğmesine basın.

İpucu: Ayarları uygulamak için 5 adımda ayarları her değiştirdiğinizde "Configure Appliance" çalıştırmanız gerekecektir.



Tebrikler!

Sanal cihazın yapılandırmasını tamamladınız.

Lisans için verdiğiniz adrese şifrenizi içeren bir e-posta gönderildi (Birinci Adım - Cihaz Lisansı'nda "Dahil Edilen İstemci Lisansları" bölümünde görülebilir).

Artık bu şifreyi ve şifreyi aldığınız e-posta adresini kullanarak konsola giriş yapabilirsiniz.

Konsolda oturum açmak için lütfen tarayıcınızın adres çubuğuna konsolun ana bilgisayar adını girin.

Cihazınızın ana bilgisayar adını Birinci Adım - Cihaz Lisansı bölümünde bulabilirsiniz.

Sorun Giderme

1. Beşinci Adım - Lisans Sözleşmesi'nde cihazı yapılandırırken bir e-posta almadınız:

Üçüncü Adım - Sunucu Ayarları bölümündeki e-posta ayarlarınızın doğru olduğundan emin olun. Parolayı yeniden göndermek için "Cihazı Yapılandır "ı tekrar çalıştırmadan önce Adım Beş - Lisans Sözleşmesi'nde "Parolaları sıfırla ve dahil edilen tüm İstemci Lisansları için bir Hesap Oluşturma Postası gönder" seçeneğini işaretleyin.

2. Beşinci Adım - Lisans Sözleşmesi'ndeki yapılandırma sırasında Let's Encrypt ile ilgili bir hata aldınız:

Cihazın 80 numaralı bağlantı noktasındaki etki alanı adı ile erişilebilir olduğundan emin olun. Let's encrypt ayrıca "/var/log/letsencrypt" dosyasına sorun gidermeye yardımcı olabilecek bir günlük yazar.

Güvenlik Önerileri

AppTec360 cihazınızın güvenliğini sağlamak için aşağıdaki adımları uygulamanız önerilir.

Bu tam bir talimat seti değildir, sadece temel bir yapılandırma için bir öneridir.

- AppTec360 kullanıcısı için parolayı değiştirme
- MySQL kullanıcıları "root "ve "AppTec" için parolayı değiştirin ve Dördüncü Adım - MySQL Kurulumunu uygun şekilde güncelleyin
- Varsayılan SSH sunucu bağlantı noktasını değiştirme
- Konsolunuzda 80 numaralı bağlantı noktasını engelleyin ve gelen HTTP trafiğine izin vermeyin, yalnızca HTTPS kullanın. Yapılandırıldıktan sonra, HTTPS üzerinden harici bir yapılandırma da mümkündür.
- Üçüncü Adım - Sunucu Ayarları'nın alt kısmında yönetim arayüzüne erişimi yalnızca belirli Ips'lerle kısıtlayın
- Güvenlik duvarını yapılandırma

Genel Ayarlar

Hesaba Genel Bakış

Hesap Bilgileri

Genel Bakış

Burada, AppTec360 hesabınıza genel bir bakış görebilirsiniz.

Şirket Adı	Şirketinizin adı
Oluşturulma Tarihi	Hesabınızın oluşturulma tarihi
Lisans Türü	Ücretli = ücretli lisans Ücretsiz = ücretsiz lisans Not: OnPremise Appliance üzerindeki hesaplar teknik nedenlerden dolayı her zaman ödenmiş olarak gösterilecektir
Müşteri Tanımlayıcı	Hesabınızın tanımlayıcısı (Bu müşteri numaranız DEĞİLDİR)
Lisans Bitiş Tarihi	AppTec360 lisansınızın son kullanma tarihi
ContentBox Lisansı	Ücretsiz = 25 cihaz için ücretsiz lisans Ücretli = x cihaz için ücretli lisans
Başlatıcı	Android için özel başlatıcıyı kullanıp kullanamayacağınızı gösterir
Cihazlar	Şu anda kullanılan / toplam lisans sayısı
İlgili Kişi	Sağlanan irtibat kişisi
Telefon	Verilen telefon numarası
e-Posta*	Sağlanan e-posta adresi
Kök Kullanıcı	Giriş yapabilen Kök Kullanıcılar
Yazılım Sürümü	Güncel Yazılım Sürümü

**Not: Burada gösterilen e-posta adresi, Hesabı kaydetmek için girdiğiniz e-posta adresidir. Buna bağlı olarak kullanıcı/cihaz ağacında bir kullanıcı oluşturulacak ve değiştirilebilecektir. Bu kullanıcıyı düzenlemek, giriş yapmak için kullanmanız gereken e-posta adresini değiştirir ancak hesaba genel bakıştaki bilgileri değiştirmez*.

Hata Raporu

Bir hata raporu, sorunları veya hataları bildirmek için doğrudan desteğe gönderilebilir ve hesabınız ve kurulumunuz hakkında bilgi ve günlükler içerir.

Konu	Hata raporunun konusu. Bunu mevcut bir destek biletine eklemek istiyorsanız bir bilet numarası ekleyin.
Beklenen Davranış	Ne yaptığınızı ve ne olmasını beklediğinizi ayrıntılı olarak açıklayın
Gerçek Davranış	Tam olarak ne olduğunu ayrıntılı olarak açıklayın. Lütfen hata mesajlarını aynen alıntılayın. Eke ekran görüntüleri eklemeniz de yardımcı olur.
Sorunu ne zaman yaşadınız?	Lütfen belirli bir hata mesajı/problemi aldığınız zamanı kesin olarak belirtin. En iyi durumda saniyeleri de dahil edin, örneğin 18:55:27
Sorun tekrarlanabilir mi? Evet ise, nasıl (ayrıntılı olarak)?	Sorunu nasıl yeniden üretebileceğinizi ayrıntılı olarak açıklayın.
Bu özellik daha önce beklediğiniz gibi çalıştı mı? Evet ise, ne zamana kadar?	Bilmiyorsanız boş bırakın.
Bu sorun ortaya çıkmadan önce sistemde yapılan belirli değişiklikler var mıydı? Evet ise, ne gibi değişiklikler oldu (ayrıntılı olarak)?	Konuyla ilgisiz olduğunu düşünseniz bile, sorun ortaya çıkmadan önce yaptığınız son değişiklik veya eylemin ne olduğunu her zaman belirtin.
Uygulanabilirse: Hangi cihaz modelleri ve işletim sistemi sürümleri etkileniyor?	Lütfen her zaman tam işletim sistemi sürümünü belirtin (örn. iOS 14.7.1 veya Android 11)
Uygulanabilirse: Cihazın genel IP adresi ve/veya Seri Numarası nedir?	Tüm cihazlar etkilenmiş olsa bile en az bir tanesinin adını verin.
Günlük dosyalarını dahil et	Hata raporuyla birlikte günlük dosyasını göndermek için bunu işaretleyin. Bunun yapılması tavsiye edilir.
Mevcut VPP durumunu Apple'dan alın ve hata raporuna ekleyin	VPP Lisans Atamaları hakkında bilgi içerir. Bunu yalnızca destek tarafından istenirse veya sorununuz VPP ile ilgiliyse etkinleştirin.
Eklenti	Yararlı olabilecek herhangi bir dosya ekleyin (örneğin, bir hata mesajının ekran görüntüleri)

Özellik İsteği

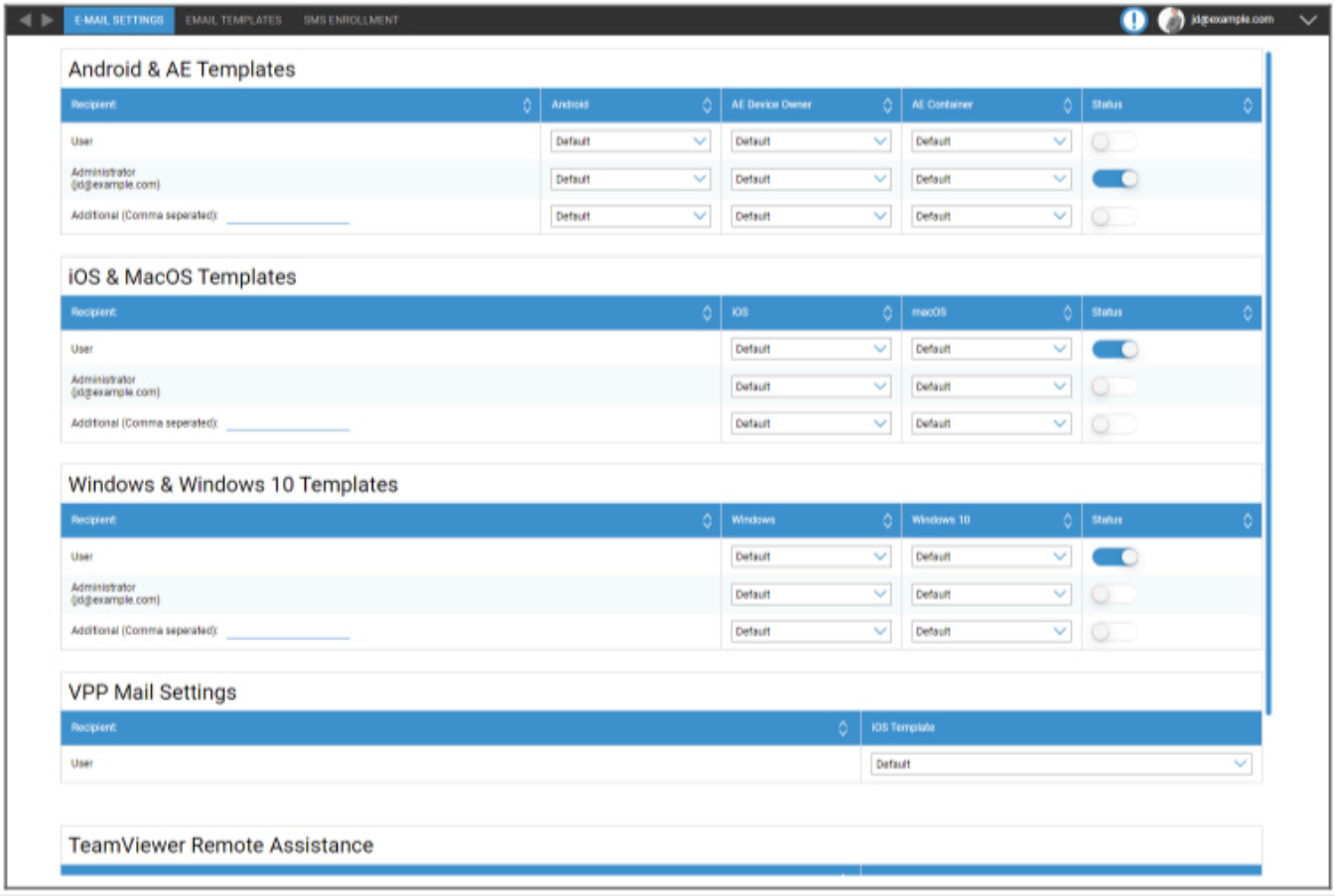
Bir özellik talebi doğrudan desteğe gönderilebilir. Bu, belirli bir özellik için bir talep veya aşağıdakiler için bir iyileştirme içerebilir

Özet	Probleminizin kısa bir özeti
Açıklama	Sorununuzun ayrıntılı bir açıklaması, lütfen mümkün olduğunca spesifik olun
Eklenti	Hata raporuna dosya ekleme

Global Yapılandırma

e-Posta Ayarları

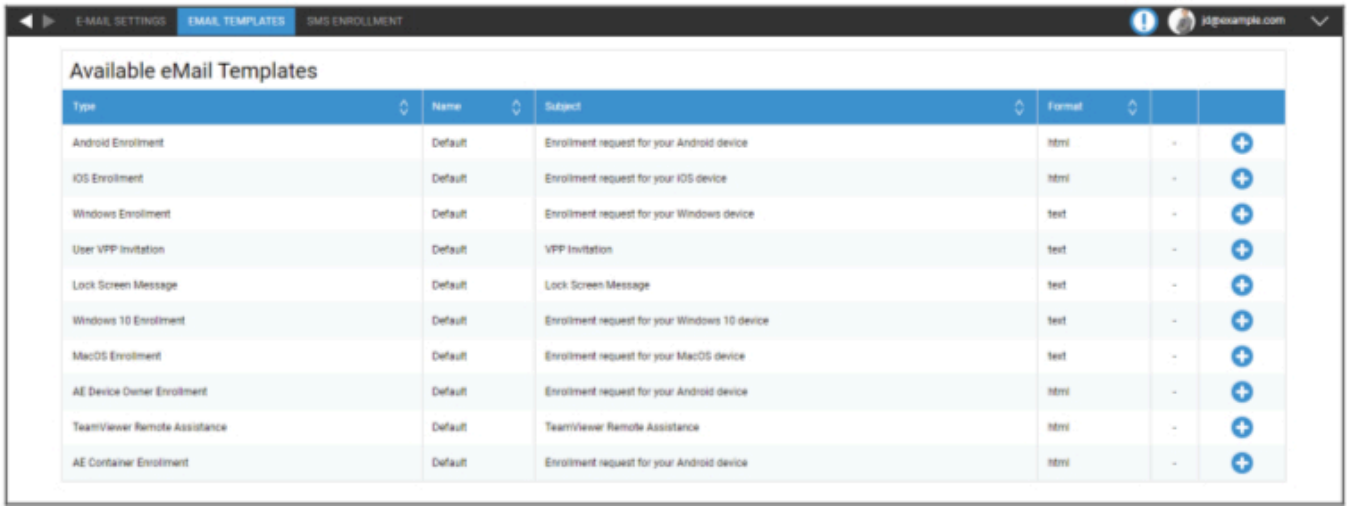
Burada, bir kayıt talebi oluşturulduğunda kimin posta alacağını ve bu posta için hangi metin şablonunun kullanılacağını tanımlayabilirsiniz.



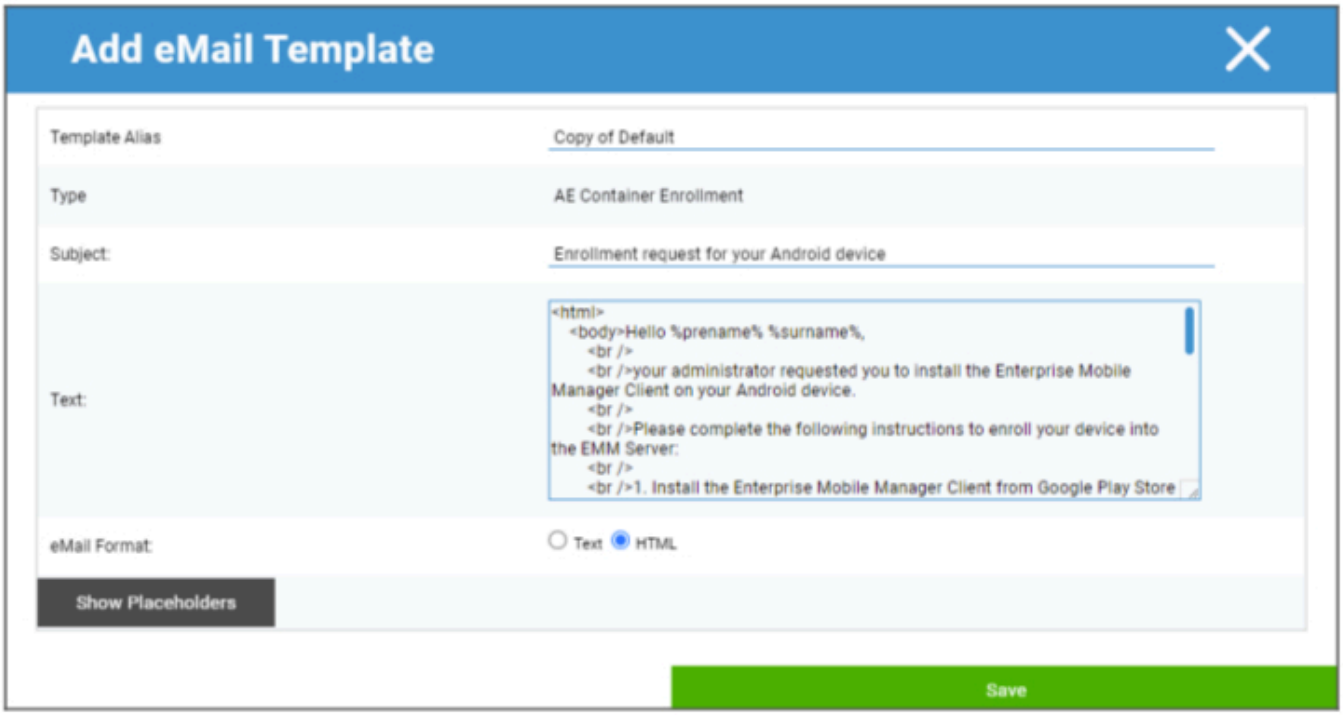
e-Posta Şablonları

Burada farklı senaryolar için şablonlarınızı oluşturabilir ve düzenleyebilirsiniz. Bunlar normal metin biçiminde veya HTML biçiminde olabilir. HTML ile metninizin biçimlendirmesini daha iyi kontrol edebilirsiniz.

Varsayılan şablonlar düzenlenemez veya silinemez.



Yer tutucuları otomatik olarak değiştirilecek değişken olarak da kullanabilirsiniz. Mevcut Yer Tutucuları görmek için düzenleme sırasında "Yer Tutucuları Göster" seçeneğine tıklayın. Farklı Kategorilerin farklı Yer Tutucuları vardır.



SMS Kaydı

Burada SMS Kayıt işlemini gerçekleştirebilir/etkinleştirebilirsiniz.

(Varsayılan: devre dışı)

Ayrıca, kaç SMS Kredisinin hala kullanılabilir olduğunu gösteren bir ekran göreceksiniz.

SMS Kredilerinin ayrıca satın alınması gerekir.

Gizlilik

GPS Erişimi

Burada her cihaz için GPS Görünümünü 1 veya 2 parola ile koruyabilirsiniz (dört göz prensibi). Bir cihazın konumuna her erişmeye çalıştığınızda parola(lar)ınızı girmeniz istenecektir.

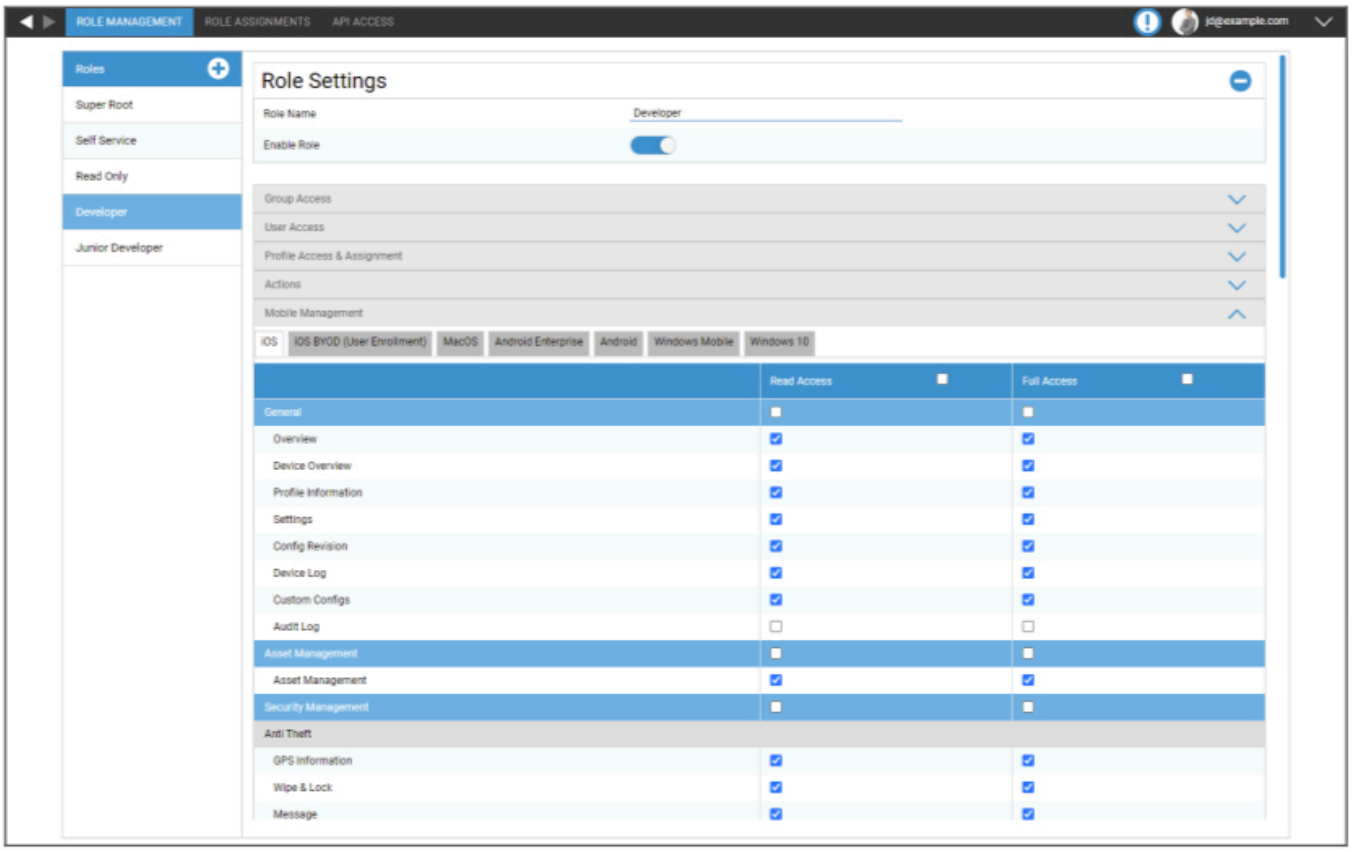
GPS Ayarlarına erişimi kısıtlama	Kapalı = işlev kapalıdır ve yerelleştirme için şifre gerekmez
	Açık = işlev açıktır ve yerelleştirme için bir şifre gereklidir
Koruma Yöntemi	Tek şifre kullan = yerelleştirme için tek şifre kullan
	İki parola kullan = yerelleştirme için iki parola kullan
Şifre Girin (1)	Seçilen şifreyi girin
Şifreyi Tekrarla (1)	Seçilen şifreyi yeniden girin
isteğe bağlı: Şifre 2'yi girin	Seçilen 2. şifreyi girin
isteğe bağlı: Şifre 2'yi tekrarla	Seçilen 2. şifreyi tekrar girin

Not: Parolanızı/parolalarınızı ayarladıktan sonra, tamamen etkinleştirilmeden önce bir kez daha girmeniz gerekir.

Rol Tabanlı Erişim

Rol Yönetimi

Roller, bir kullanıcının yönetim konsolunda oturum açtığında neleri görebileceğini ve yapabileceğini tanımlar. Bu, oturum açabilen ancak sınırlı işlevselliğe sahip kullanıcılar oluşturmanıza olanak tanır.



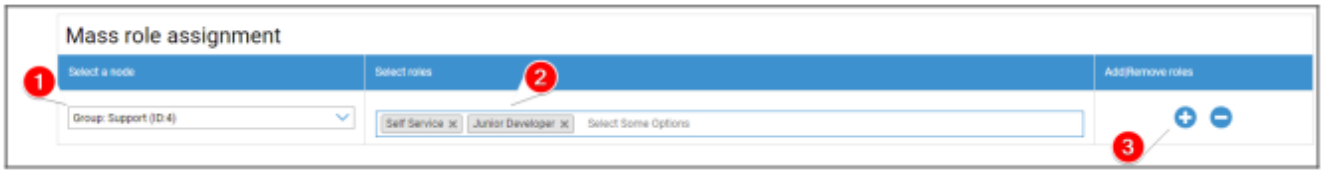
Süper Kök Rolü, her zaman her şeyi görebilen ve değiştirebilen varsayılan bir roldür. Değiştirilemez veya silinemez. Self Servis Rolü yalnızca kendi kullanıcısını ve cihazlarını görebilir. Self Servis ve özel bir rolü birleştirerek örneğin kullanıcıların kendi başlarına ve yalnızca kendi kullanıcıları için oturum açmalarına ve cihazları kaydetmelerine izin verebilirsiniz.

Özel Roller manuel olarak etkinleştirilebilir veya devre dışı bırakılabilir. Yeni Roller varsayılan olarak devre dışıdır. Engelli rolüne sahip kullanıcılar, bu role sahip değilmiş gibi çalışır. Bu, örneğin belirli bir rolü eylemlerinden geçici olarak kısıtlamanıza olanak tanır.

Tüm İzinler "Okuma Erişimi" ve "Tam Erişim" arasında bölünmüştür. Bir Role Okuma Erişimi vermek, konsolun belirli bir bölümünü görmelerini sağlar. Onlara Tam Erişim vermek, Rolün konsolun belirli bir bölümünü görmesini ve değiştirmesini sağlar.

Rol Atamaları

Burada, bir role sahip olan tüm kullanıcılara genel bir bakış elde eder ve hangisine sahip olduklarını görürsünüz. Ayrıca buradan kullanıcılara veya tüm gruplara bir rol atayabilirsiniz:

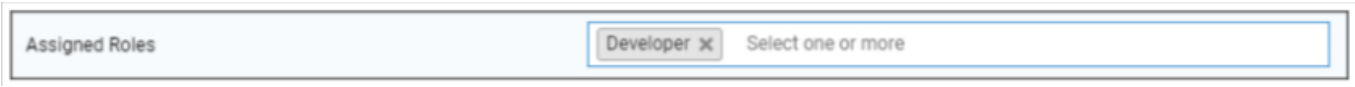


1. Hangi grup veya kullanıcı için rol eklemek veya kaldırmak istediğinizi seçin. Tek bir kullanıcı seçebilir veya bir grup seçebilirsiniz. Bir grup seçerken, yaptığınız değişiklik o gruptaki tüm kullanıcıları ve seçilen gruptaki alt grupların tüm kullanıcılarını etkileyecektir.
2. Hangi rolü eklemek veya kaldırmak istediğinizi seçin. Bir veya birden fazla rol seçebilirsiniz.
3. . Hangi işlemi gerçekleştirmek istediğinizi seçin. "+" işaretine tıklandığında, kullanıcı(lar) zaten sahip değilse seçilen roller eklenir. "-" işaretine tıklandığında seçilen roller kullanıcı(lar)dan kaldırılır. Henüz herhangi bir rolü olmayan bir kullanıcıya rol eklerseniz, kullanıcı için otomatik olarak "Giriş Yapabilir" özelliğini etkinleştirecektir.
4. İşlemi bitirmek için kaydedin. Daha önce rolü olmayan ve "Giriş Yapabilir" seçeneği devre dışı bırakılmış olan kullanıcılar otomatik olarak şifre belirleme bağlantısı içeren bir posta alacaktır.

Toplu rol atamasının altında, atanan rollere genel bakışı bulabilirsiniz. Belirli kullanıcılar için rolleri manuel olarak da değiştirebilirsiniz.

Bir rolün atanması

Bir kullanıcıya rol atamak için gruplarınızın, kullanıcılarınızın ve cihazlarınızın ağacını bulabileceğiniz Mobil Yönetim'e gitmeniz gerekir. Bir rol atamak için kullanıcıyı düzenleyin. Alternatif olarak, yukarıda belirtilen yöntemi yalnızca tek kullanıcılar için de kullanabilirsiniz.



API Erişimi

AppTec360 REST API'ye Erişim

AppTec360 REST API, Managment Console'da oluşturulması gereken bir kimlik doğrulama belirteci (API anahtarı) ve bir özel anahtar gerektirir.

Bunu yapmak için AppTec360 EMM'de oturum açın ve şu adrese gidin

Genel Ayarlar → Rol Tabanlı Erişim → API Erişimi öğelerini seçin ve yeni bir Anahtar ekleyin.

API anahtarı için izinleri geçerli olacak bir kullanıcı seçmeniz gerekir.

Özel anahtar yalnızca bir kez indirilebilir. İndirme işlemi başladıktan sonra anahtar silinecek ve "İndir" düğmesi kaybolacaktır.

Özel anahtarınızı kaybederseniz yeni bir API anahtarı oluşturmanız gerekir.

Genel Kurallar

- REST API temel URL'nin altında mevcuttur:

/public/external/api

- Tüm talepler POST aracılığıyla gönderilmelidir.
- REST API yalnızca HTTPS üzerinden yapılan istekleri destekler.
- Talepler aşağıdaki Başlıkları içermelidir:

Başlık Adı	Başlık Değeri	Açıklama
İçerik türü	application/json	sabit
auth	123...xyz	"API Erişimi" Sekmesinden API Anahtarı
imza	Base64 kodlu imza	ile oluşturulan yükün imzası "API Erişimi" Sekmesinden özel Anahtar

- İstek gövdesi, aşağıdaki değerleri içermesi gereken json kodlu bir nesne olmalıdır:

Saha	Alan Örnek Değer	Açıklama
api	v2/device/listdevices	API'nin adı
zaman	1529662725	İstemci makinenin Unix Zaman Damgası (UTC). İzin verilen maksimum zaman farkı istemci ve sunucu arasında 30 dakikalar.

- Başarı durumunda API istenen verileri (aşağıdaki Sorgulara bakın) ve bir HTTP durum kodu 200 döndürür.
- Bir hata oluşursa, HTTP durum kodu hataya bağlı olarak 4xx ile 5xx arasında olacaktır ve yanıt nesnesi, insan tarafından okunabilir hata mesajlarının bir listesini içeren "errors" anahtarına sahip bir dizi içerecektir.
- Bir aygıt için eşleşen veri yoksa boş bir dizi döndürülür.
- Eğer bir cihaz kimliği mevcut değilse, geri dönüş verisi null olacaktır.

Talep örneği

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]}}

Sorgular

Tüm cihazları listele

İşlevsellik: Cihaz Kimliği, IMEI ve Seri Numarasını içeren tüm cihazların bir listesini döndürür
API URI: v2/device/listdevices
Zorunlu Parametreler: yok
İsteğe Bağlı Parametreler: yok

Örnek İstek Gövdesi


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


Örnek Yanıt Gövdesi


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

(GPS) konumlarının listesini al

İşlevsellik: Cihaz kimlikleri için saklanan tüm konum günlüğü girdilerinin bir listesini döndürür
API URI: v2/device/listposition
Zorunlu Parametreler: "ids" - Cihaz Kimlikleri Dizisi
İsteğe Bağlı Parametreler: yok

Örnek İstek Gövdesi


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


Örnek Yanıt Gövdesi


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

Varlık haritasını al

İşlevsellik:
Get any asset data kullanılarak talep edilecek tüm depolanmış olası varlıkların bir listesini döndürür. Verileri talep etmek için insan tarafından okunabilir formu veya varlık etiketini kullanabilirsiniz.
API URI: v2/device/getassetmap
Zorunlu Parametreler: yok
İsteğe Bağlı Parametreler: yok

Örnek İstek Gövdesi

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

Örnek Yanıt Gövdesi

Bu yanıt okunabilirlik açısından kısaltılmıştır.

{
"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": []
}

Herhangi bir varlık verisini alın

İşlevsellik: Cihaz kimlikleri için istenen varlık verilerinin bir listesini döndürür
API URI: v2/device/getassetdata
Zorunlu Parametreler: "ids" - Cihaz Kimlikleri Dizisi
İsteğe Bağlı Parametreler:
"assetkeys" - Döndürülecek varlık veri anahtarları. Belirtilmezse, mevcut tüm varlık verileri geri döndü. Get asset map kullanarak varlık anahtarlarının bir listesini alabilirsiniz.

Örnek İstek Gövdesi


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


Örnek Yanıt Gövdesi


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

Python3'te Örnek Kod

```
! /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-XXXXXXXXXX.pem"
apptecAPIAuthToken = "7eXXXXXXXXXXXXXXXXXXXXXXXXXX20"
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)
```

Elma Yapılandırması

APNS Sertifikası

Burada bir APNS Sertifikası yükleyebilirsiniz. Bu, iOS ve MacOS cihazlarını yönetmek için gereklidir.

Not: APNS Sertifikası sadece bir yıl için geçerlidir. Bunun süresi dolmadan yenilenmesi gerekmektedir. Yenileme süreci oluşturma süreciyle aynıdır (aşağıya bakınız) ve sadece birkaç dakika sürer.

Bunu zamanında yenilemeyi unutursanız, halihazırda kayıtlı cihazlarınızda değişiklik yapamazsınız **ve tüm cihazları tekrar kaydetmeniz gerekir** .

Adım 1

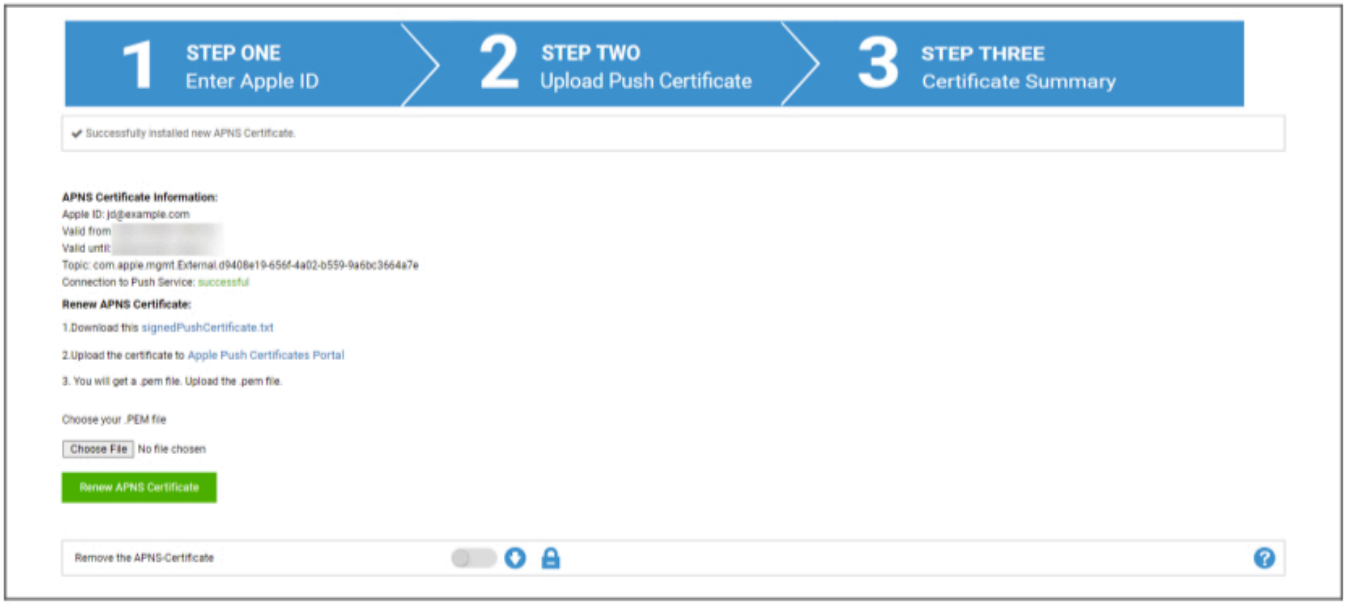
- İlk olarak, APNS Sertifikası oluşturmak için kullanmak istediğiniz Apple Kimliğinizi girin.

Not: Bu Apple Kimliği yalnızca APNS Sertifikası oluşturmak için kullanılır. Bu Apple Kimliğinin aygıtlarla hiçbir ilgisi yoktur ve aygıtlar bu Apple Kimliğini bilmeyecektir. Ayrıca APNS Sertifikasını yenilemek için de bu Apple Kimliğine erişmeniz gerekir. Bu nedenle, genel bir Apple Kimliği kullanmanız ve giriş verilerini belgelemeniz önerilir. APNS Sertifikasının süresi dolmadan önce Apple Kimliğinin kullanılan Posta Adresine bir Hatırlatma gönderilir.

- Devam etmek için "Sonraki Adım "a tıklayın.
- (isteğe bağlı) Yanlışlıkla sildiyseniz, önceden silinmiş APNS Sertifikasını da kurtarabilirsiniz

Adım 2

- signedPushCertificate.txt dosyasını indirin
- https://identity.apple.com/pushcert/ adresine gidin ve 1. Adımdaki Apple Kimliği ile giriş yapın
- "Sertifika Oluştur" üzerine tıklayın
- (isteğe bağlı) bir Not girin. Birden fazla kiracıyı yönetiyorsanız, onları kolayca tanımlamak için bu yararlı olabilir.
- Önceden indirilmiş signedPushCertificate.txt dosyasını seçmek için "Dosya Seç "e tıklayın
- "Yükle" üzerine tıklayın.
- Şimdi bir APNS Sertifikası oluşturduğunuza dair onayı göreceksiniz.
- "İndir "e tıklayın ve kaydedin.
- Yönetim konsoluna geri dönün.
- "Dosya Seç" üzerine tıklayın ve yüklemek istediğiniz APNS Sertifikasını seçin.
- "Yükle" üzerine tıklayın



Adım 3

Artık APNS Sertifikasını başarıyla kurdunuz ve artık iOS ve MacOS aygıtlarını yönetebilirsiniz.

3. Adımda, halihazırda kullandığınız APNS Sertifikasına genel bir bakış göreceksiniz.

Ayrıca, ekranda gösterilen adımları izleyerek APNS Sertifikasını yenileme seçeneğiniz de vardır. Süresi dolmadan önce yenilemeyi unutmayın.

APNS Sertifikasını yenilerken, Adım 3'te gösterilen Apple Kimliği ile giriş yapmayı ve ayrıca daha önce kullanılan sertifikayı yenilemeyi ve yeni bir sertifika oluşturmamayı unutmayın. APNS Sertifikasının "konusunu" 3. Adımda ve Apple Push Sertifika Portalında "i" üzerine tıkladığınızda göreceksiniz. Bu, Sertifikayı tanımlayan benzersiz kimliktir. Bu, doğru olanı belirlemenize ve doğru olanı yenilemenize yardımcı olacaktır.

Yenileme sırasında "Hata: Push Sertifikasının farklı bir konusu var!" mesajı alıyorsanız, bu başka bir Sertifikayı yenilediğiniz veya yeni bir Sertifika oluşturduğunuz anlamına gelir.

Yeni bir Sertifika yüklemek istiyorsanız, örneğin daha önce kullandığınız Apple Kimliğine artık erişemiyorsanız, önce mevcut yüklenmiş Sertifikayı silmeniz gerekir.

Her halükarda APNS Sertifikasını silmek, siz onları tekrar kaydedinceye kadar mevcut kayıtlı cihazlar için artık değişiklik yapamayacağınız anlamına gelir. Bu nedenle, buna hazırlıklı olduğunuzdan emin olun ve Sertifikayı yalnızca başka bir yol yoksa kaldırın.

Yönetilen Erişim

Burada iOS Aygıtları için Kullanıcı Kaydını ve iOS Aygıtları için Paylaşılan iPad'i etkinleştirebilirsiniz.

Kullanıcı Kaydı

'Kullanıcı Kaydı' BYOD cihazları için özel bir mod sağlar.

Her kullanıcı için Apple Business Portal'da yönetilen bir Apple kimliği oluşturulmalıdır.

Kayıt işlemi sırasında kullanıcılardan Apple-ID kimlik bilgileri istenecektir.

'Kullanıcı Kaydı', MDM tarafından yalnızca sınırlı sayıda ayar ve kısıtlamanın yapılandırılmasına izin verdiği için kullanıcı için maksimum güvenliği garanti eder.

Yönetilen Alan:

Kullanıcının e-posta adresini yönetilen Apple-ID ile eşlemek için kullanılan Etki Alanı ('@appleid.company.com' biçiminde olmalıdır). john.doe@example.com, john.doe@appleid.company.com ile eşlenecektir.

Yönetilen Etki Alanınızı görmek için Apple Business Manager'ı kontrol edin

Paylaşılan iPad

Paylaşılan bir iPad, özel bir DEP Profili ile yapılandırılmış bir DEP aygıtıdır.

Bu, birden fazla kullanıcının yönetilen Apple-ID'lerini kullanarak aygıtta oturum açmasına olanak tanır.

Yönetilen Apple kimliği Apple Business Portal veya Apple School Manager'da oluşturulmalıdır.

Paylaşılan bir iPad'de oturum açan kullanıcılardan yönetilen Apple-ID kimlik bilgileri istenir.

Yönetilen Alan:

Kullanıcının e-posta adresini yönetilen Apple-ID ile eşlemek için kullanılan Etki Alanı ('@appleid.company.com' biçiminde olmalıdır). john.doe@example.com, john.doe@appleid.company.com ile eşlenecektir.

Yönetilen Etki Alanınızı görmek için Apple Business Manager'ı kontrol edin

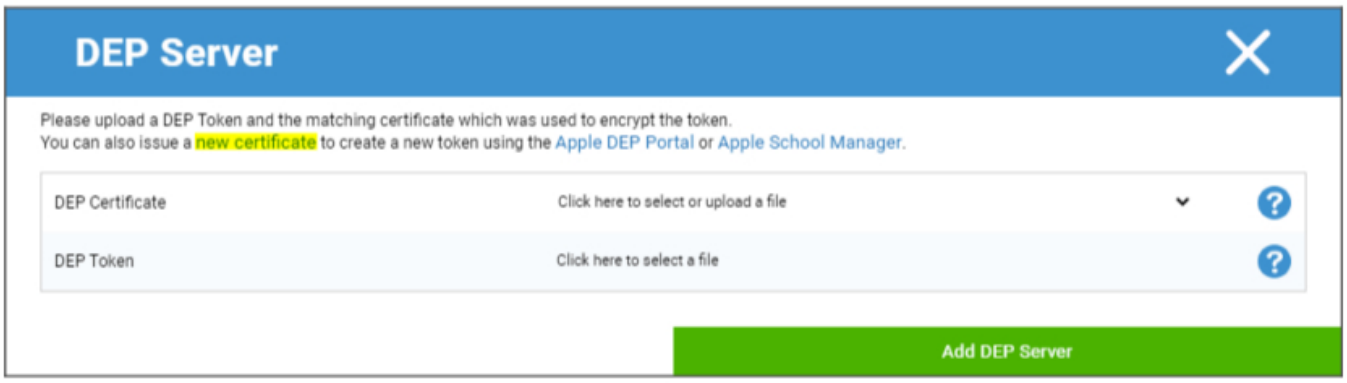
DEP

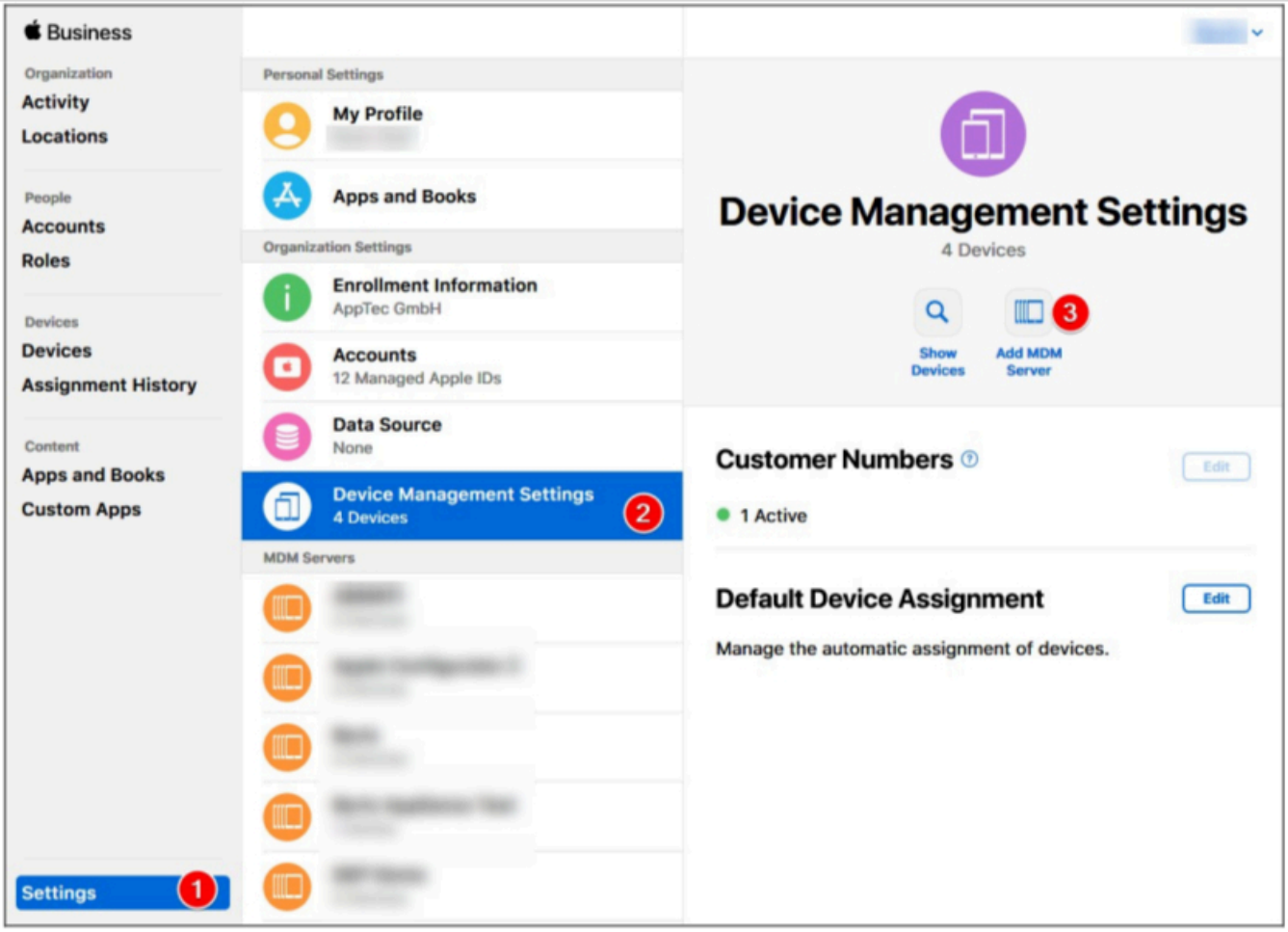
DEP (Cihaz Kayıt Programı) cihazları MDM'ye kolayca kaydetmenizi sağlar. DEP kullanıldığında, cihaz kurulurken cihazlar otomatik olarak MDM'ye bağlanacaktır. Ayrıca iOS'ta genellikle zorunlu olan kurulum adımlarının neredeyse tamamını atlayabilirsiniz.

Cihazları DEP'i destekleyen bir satıcıdan satın almanız gerektiğini unutmayın. Daha fazla bilgi için satıcınıza veya Apple'a başvurun.

DEP Hakkında Daha Fazla Bilgi: https://www.apple.com/business/dep/

Bir DEP Belirteci eklemek için "+" işaretine tıklayın. Açılır pencerede, metindeki "yeni sertifika" seçeneğine tıklayın (aşağıdaki resimde sarı ile işaretlenmiştir). Bu işlem bir DEP sertifikası oluşturacak ve indirecektir. Daha sonra Apple İşletme Yöneticisine(https://business.apple.com/) veya Apple Okul Yöneticisine(https://school.apple.com/) gidin.

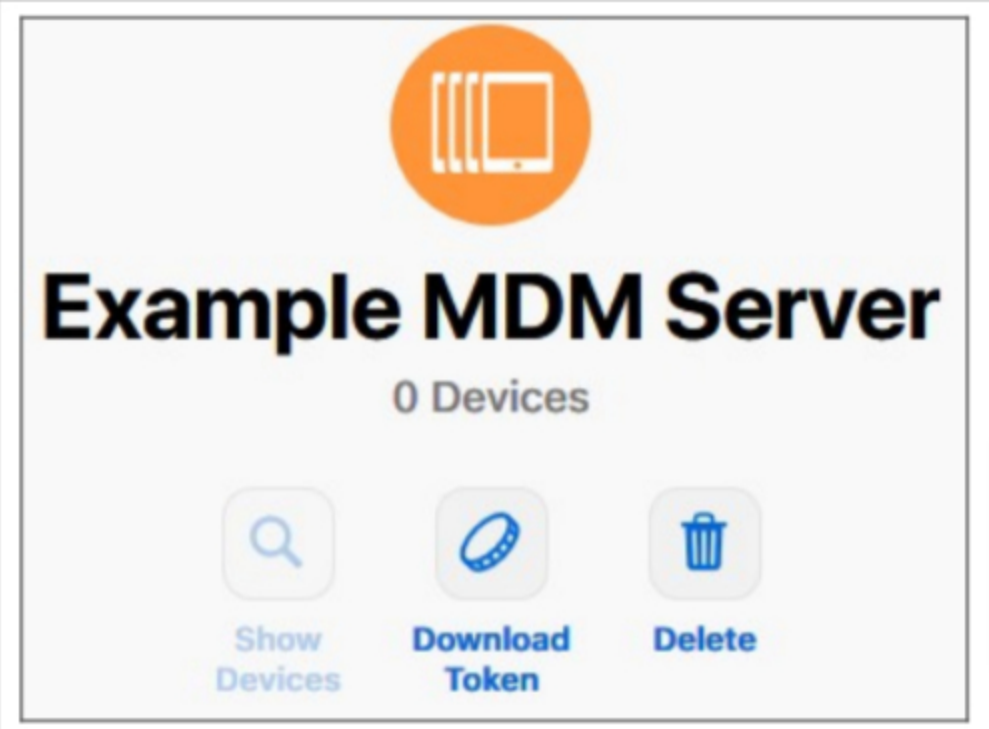




Apple Business Manager'da, yukarıdaki resimde gösterildiği gibi adımları izleyin. Ayarlar → Cihaz Yönetimi Ayarları → MDM Sunucusu Ekle.

Sunucuya istediğiniz ismi verin ve daha önce indirdiğiniz DEP Sertifikasını MDM Sunucu Ayarları → Genel Anahtarı Yükle altında yükleyin ve "Kaydet "e tıklayın.

Şimdi "Token İndir" seçeneğine sahip olacaksınız. Buna tıklayın ve kaydedin. Token yalnızca 1 yıl boyunca geçerlidir. Ancak tekrar "Token İndir "e tıkladığınızda size yeni bir tane verilecektir, bu da token'ı yenilemeyi çok kolaylaştırır.



Artık daha önce DEP Sertifikasını indirdiğiniz MDM'ye geri dönebilirsiniz. Sekmeyi kapatmadıysanız, DEP Sunucusu ekleme açılır penceresi hala açık olmalı ve DEP Sertifikası zaten seçili olmalıdır. Artık Token'ınızı "DEP Token" alanına yükleyebilir ve DEP Sunucusu'na tıklayabilirsiniz.

"**Aygıtlar**" sütununda bu DEP Sunucusuna atanmış olan aygıtların miktarını göreceksiniz. Bu DEP sunucusuna eklenen cihazlar, Mobil Yönetim'deki DEP Havuzunda otomatik olarak oluşturulacaktır.

Tüm DEP cihazlarınıza ve durumlarına genel bir bakış için bu numaraya tıklayabilirsiniz.

Not: İş akışınıza veya Business Manager'daki yapılandırmanıza bağlı olarak, bu cihazları DEP Sunucusuna manuel olarak atamanız gerekebilir. Yeni aygıtlar için Apple Business Manager'da varsayılan bir DEP Sunucusu da ayarlayabilirsiniz.

"**Profiller**" sütununda sahip olduğunuz DEP Profillerinin Miktarını görürsünüz. Ayrıca DEP Profillerinizle ilgili ayrıntıları görmek için bu numaraya tıklayabilir ve eski/kullanılmayan profilleri buradan silebilirsiniz. Şu anda bunları değiştirmek mümkün değildir. Bir değişiklik yapmak istiyorsanız, yeni bir tane oluşturmanız gerekir.

"**Son Senkronizasyon**" sütununda DEP Sunucusunu manuel olarak senkronize edebilir (örneğin DEP'e yeni bir cihaz eklediyseniz) ve son başarılı**Senkronizasyonun**tarihini görebilirsiniz.

"**Otomatik**Profil" sütununda bir DEP profilini otomatik varsayılan olarak ayarlayabilirsiniz. Bu profil yeni cihazlara otomatik olarak atanacaktır. Bir Otomatik Profil ayarlamazsanız, her seferinde yeni cihazlara manuel olarak bir profil atamanız gerekir.

"**Profil Ekle**" sütununda yeni bir DEP profili ekleyebilirsiniz. Cihaz bunu cihaz kurulumunun başında alacaktır. DEP profili cihazın nasıl kurulacağını ve hangi kurulum adımlarının atlanacağını tanımlar.

Not: Bir cihaz kaydedildikten sonra, bu ayarlar yalnızca fabrika ayarlarına sıfırlama yapılarak ve cihaz yeni bir profille kaydedilerek değiştirilebilir. Bu özellikle "**Çıkarılabilir**" ve "**Eşleştirmeye izin**ver" için geçerlidir. "**Eşleştirmeye izin**ver" durumunda bunu açmanız önerilir, çünkü bu MDM kısıtlamaları yoluyla devre dışı bırakılabilir, ancak DEP profilinde devre dışı bırakılırsa tekrar etkinleştirilemez.

"**Düzenle**" sütununda, örneğin Token'ı yenilerken yeni bir token yükleyebilirsiniz.

Yapılandırıcı ve URL

Havuz Kayıt URL'leri

Burada bir kayıt URL'si ve belirli bir kayıt miktarı ve belirli bir tarihe kadar geçerli olan bir kayıt QR Kodu oluşturabilirsiniz. Bu, yalnızca bir bağlantı veya QR kodu ile birden fazla cihazı kaydetmenize olanak tanır.

Bu URL veya QR Kodu ile kaydedilen cihazlar Mobil Yönetimdeki Havuzda yer alır ve daha sonra bunları manuel olarak bir gruba veya kullanıcıya atamanız gerekir.

Not: bu yalnızca manuel kayıt içindir. Aygıtları Apple Configurator aracılığıyla kaydediyorsanız bu URL'yi kullanmayın

MDM Profili – Apple Configurator

Apple Configurator aracılığıyla aygıtları kaydederken ihtiyaç duyduğunuz URL'yi buradan alabilirsiniz. Apple Configurator ile aygıtları hazırlarken aynı süreçte aygıtları MDM'e ekleyebilirsiniz. Apple Configurator bunun için bu URL'yi gerektirir.

Apple Configurator aracılığıyla eklenen aygıtlar Mobil Yönetim'deki Havuz'da yer alır ve daha sonra bunları manuel olarak bir gruba veya kullanıcıya atamanız gerekir.

Ayrıca burada Apple Configurator aracılığıyla cihazları kaydetmek için kullanılabilecek bir .mobileconfig dosyası bulacaksınız. Yine de URL'nin kullanılması tavsiye edilir.

Android Yapılandırması

Android Yapılandırması

Korumayı Kaldır	Bu işlev etkinleştirilirse, kullanıcı MDM Yöneticisi tarafından belirlenen şifreyi girmeden cihaz yöneticisini devre dışı bırakamaz. Parola kayıt sırasında belirlenir, bu nedenle parolayı güncellemek için cihazların yeniden kaydedilmesi gerekir. Cihaz yöneticilerini kaldırmak için iki seçenek vardır: 1. Cihaz üzerinde manuel olarak ◦ Cihazda EMM Uygulamasını açın ◦ Durum sekmesine geçin ◦ "Korumayı Kaldır" üzerine dokunun ◦ Parolayı girin Konsoldaki "Parola Geçmişi "nden doğru parolayı almak için Revizyon'u kullanabilirsiniz. ◦ Aşağı kaydırın ve yeni eklenen noktaya dokunun, "AppTec360 MDM Uygulamasını kaldırmak için dokunun" (bu görevi gerçekleştirmek için 20 saniyeniz var) ◦ "AppTec360 MDM Uygulamasını Kaldır" diyaloğunu "tamam" ile onaylayın. Bu, cihazın konsoldan kaydını kaldıracaktır. ◦ Uygulamayı cihazdan kaldırmak için "AppTec360 MDM kaldırılacak" diyaloğunu "UNINSTALL" ile onaylayın 2. otomatik (Konsol) ◦ Konsolda Cihazı seçin ◦ Mavi dişli simgesine tıklayın ve "Enterprise Wipe "ı seçin Not: Yalnızca Android 4.x ve daha düşük sürümlerde veya KNOX API'ye sahip cihazlarda (Samsung cihazları) kullanılabilir
Şifreyi Kaldır (Revizyon x)	Kullanıcının cihaz yöneticisini kaldırabileceği belirlenmiş şifre Revizyon x = sayaç, şifrenin ne sıklıkla değiştirildiği Kullanıcının hangi şifreye ihtiyacı olduğu önemlidir, çünkü cihaz AppTec360 Sunucusu ile

	iletişim kurmamış olabilir ve bu nedenle en yeni şifre henüz iletilmemiştir
Şifre Geçmişi	Mavi düğmeye ("Geçmişi Göster") tıkladığınızda, daha önce oluşturulmuş şifreleri görüntüleyebilirsiniz
Genişletilmiş Kaldırma Koruması	Bu Seçenek, GÜVENLİ olmayan cihazlara karşı koruma sağlar Bu ayar etkin olduğu sürece, cihaz yöneticisini kolayca devre dışı bırakmak mümkün değildir
Kullanıcıdan engellenen Uygulamaları kaldırmasını ister misiniz?	Mümkünse, engellenen Uygulamalar yalnızca engellenmekle kalmaz, aynı zamanda otomatik olarak kaldırılır. Otomatik kaldırma mümkün değilse kullanıcıdan engellenen Uygulamaları kaldırması istenecektir.
Akıllı Sistem Uygulama Engelleme	Beyaz Liste etkinleştirilmişse, Android MDM İstemcisi kullanıcı tarafından yüklenen tüm Uygulamaları engeller. Beyaz Liste modunda tüm başlatılabilir Sistem Uygulamalarını engellemek için bu ayarı etkinleştirin.

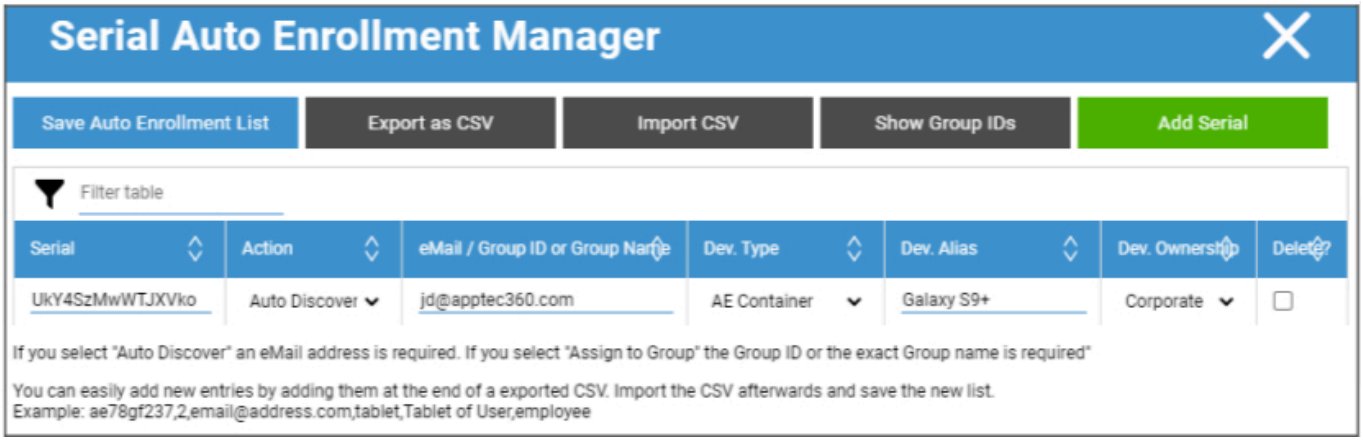
Otomatik Kayıt

Burada, AppTec360 MDM İstemcisi cihazda açıldığında cihazlarınızı otomatik olarak kaydetmek için Otomatik Kayıt özelliğini etkinleştirebilirsiniz.

Önemli: Bu kayıt yöntemi kullanımdan kaldırılmıştır ve artık Android 10 veya üzeri sürümlerde çalışmamaktadır. Her halükarda Android 7 veya daha üstünü kullanırken cihazları Android Enterprise tam yönetimli olarak kaydetmelisiniz. Android Enterprise BYOD konteynerini kullanmak istiyorsanız ve Android 10 veya daha yüksek bir sürüm kullanıyorsanız, cihazı kimlik bilgileri, QR Kodu veya SMS yoluyla manuel olarak kaydetmeniz gerekir. Her neyse, Otomatik Kayıt Listesi hala örneğin AE Kaydı, Knox Kaydı vb. için kayıt sürecini otomatikleştirmek için kullanılmaktadır.

Her neyse, Otomatik Kayıt Listesi hala örneğin AE Kaydı, Knox Kaydı vb. için kayıt sürecini otomatikleştirmek için kullanılmaktadır.

"Seri Yöneticisi" veya "IMEI Yöneticisi "ne tıklayarak sırasıyla cihazlarınızın Seri veya IMEI numaralarını ekleyebilirsiniz. Cihazlarınız için her ikisini de yapmanız gerekmez, sadece biri yeterlidir.



Eylem , cihazların havuza mı, bir kullanıcıya mı yoksa bir gruba mı kaydedileceğini tanımlar.

Ayrıca bir .csv dosyasını dışa ve içe aktarabilir ve girişlerinizi anahtar kelimelere göre filtreleyebilirsiniz.

Android Kurumsal

Burada Android Enterprise'ı kurabilirsiniz. Bu, tüm Android Enterprise özelliklerini kullanmak için gereklidir.

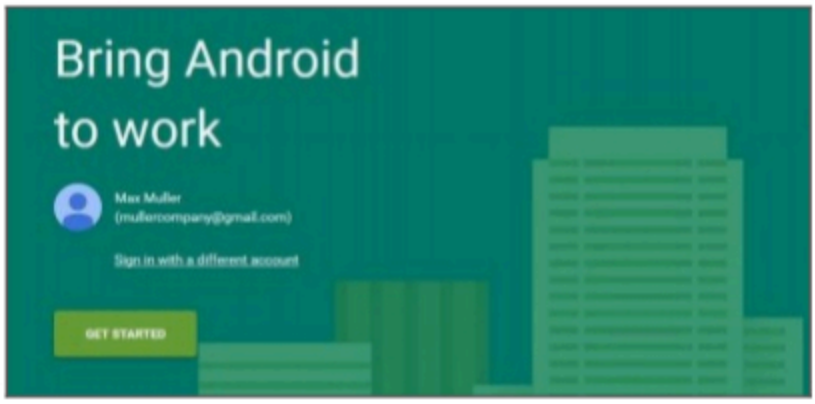
Birinci Yöntem: Android Kurumsal Hesabı (Google Hesabı)

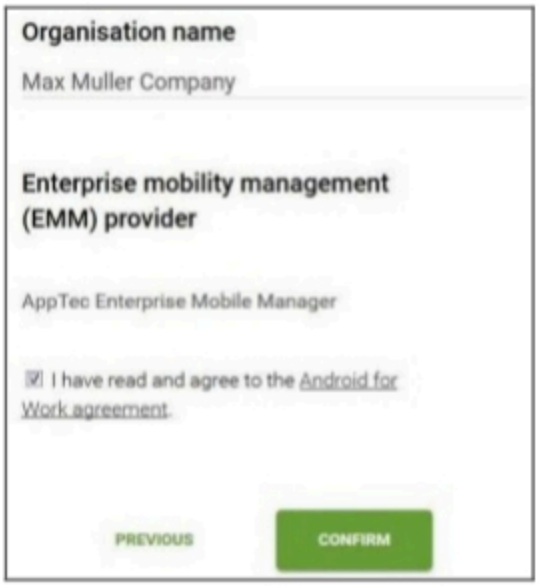
Önce "Kurulumu Hazırla" düğmesine basın, kısa bir süre sonra "Kurulumu Başlat" düğmesi olmalıdır.

Bu sizi Google'ın Android Kurumsal Kurulum Sayfasına götürecektir.

Henüz giriş yapmadıysanız, kullanmak istediğiniz Google Hesabı ile giriş yapın ve "Başla" düğmesine basın.

Şimdi şirketinizin adını girebilirsiniz. Bunu yaptıktan sonra onay kutusunu işaretleyin ve "Onayla" düğmesine basın





Son adımda kaydınızı tamamlayabilir ve konsola geri dönebilirsiniz. Her şey yolunda gittiyse şöyle görünmesi gerekir:

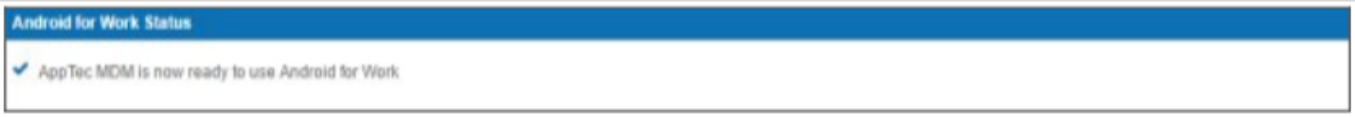
Artık Android Enterprise Container'ınızı yapılandırmaya başlayabilirsiniz.

İkinci Yöntem: G-Suite Hesabı

"G-Suite Kullan" seçeneğine basın ve Google Yönetici Hesabınıza giriş yapın. Orada "Güvenlik" -> "Daha fazlasını göster" -> "Android için EMM sağlayıcısını yönet" seçeneğine gidin ve bir Token oluşturun. Not: G-Suite Hesabınızda Android Kurumsal Ayarlarını görmüyorsanız, "Daha fazla uygulama ve hizmet alın" bölümüne gitmeniz ve Android cihaz yönetimini eklemeniz gerekir. Şimdi konsolumuza Token'ı ve birincil Etki Alanınızı girin ve "Değişiklikleri Kaydet "e tıklayın. İşiniz bittiğinde, "Android Kurumsal Hesabını Kullan" seçeneğine tıklayın.

Şimdi "Hizmet Hesabı Oluştur" Düğmesini görmelisiniz. Tıkla. Bu işlem birkaç dakika sürebilir.

Her şey çalıştıysa, şöyle görünmesi gerekir:



Artık Android Enterprise Container'ınızı yapılandırmaya başlayabilirsiniz.

Fabrika Ayarlarına Sıfırlama Koruması

Fabrika Ayarlarına Sıfırlama Koruması ile cihazınızı istediğiniz bir google hesabına bağlayabilirsiniz, bu da mevcut bir google hesabına bağlanmayı geçersiz kılar. Fabrika Ayarlarına Sıfırlama Korumasını kullanmak için önce burada ayarlamanız ve daha sonra profillerinizde etkinleştirmeniz gerekir.

Fabrika Ayarlarına Sıfırlama Korumasını ayarlamak için "FRP Kurulumu" üzerine tıklayın ve ekrandaki talimatları izleyin.

NOT: Adımları dikkatlice okuyun ve uygulayın. Yanlış google Hesabına otomatik olarak giriş yapmaktan kaçınmak için bunu yeni bir gizli tarayıcı penceresinde yapmanızı öneririz. Yanlış bir kimlik girmeniz veya kullanılan Google Hesabına erişiminizi kaybetmeniz durumunda kendinizi cihazdan tamamen kilitleyebilirsiniz!

AE Kaydı

Burada Android Enterprise Ernollment'ı etkinleştirebilirsiniz. Bu Yöntemi kullanmak Cihazlarınızı Android Kurumsal Cihaz Sahibi Moduna kaydedecektir. Bu modda cihaz üzerinde tam kontrole sahip olacaksınız.

AE Kaydını Etkinleştir	AE Kaydını etkinleştirir Dikkat: AE Kaydını devre dışı bırakırsanız, mevcut QR Kodları ve önceden yapılandırılmış NFC programlayıcı cihazları çalışmayı durduracaktır. AE Kaydını tekrar etkinleştirirseniz, NFC push yapılandırmalarını yeniden göndermeniz / yeni QR kodları oluşturmanız gerekir.
Otomatik Keşfi Etkinleştir	Bir cihaz "AE Kaydı" yoluyla kendini kaydettirdiğinde, sistem Seri / IMEI Beyaz Listesinde ("Genel Ayarlar" > "Android Yapılandırması" > "Otomatik Kayıt") ayarlanan bilgilere dayanarak cihazı bir kullanıcıya atamaya çalışacaktır.
Bilinmeyen Cihazları Engelle	Yalnızca Seri / IMEI Beyaz Listesinde ("Genel Ayarlar" > "Android Yapılandırması" > "Otomatik Kayıt") beyaz listeye alınmış cihazların kaydolmasına izin verilir.

Yöntem 1 ve 2 ile ilgili not: "Hoş Geldiniz Ekranı" fabrika ayarlarına sıfırlama işleminden sonra gördüğünüz ilk ekranı ifade eder. Bu, kullandığınız android sürümüne ve/veya cihaz modeline bağlı olarak farklı görünebilir.

Yöntem 1: QR Kod Kaydı

(Android 7.0 veya üstü gerektirir) Android 7 veya üstünü çalıştırıyorsanız her zaman bu yöntemi kullanmanızı öneririz.

1. Cihazı fabrika ayarlarına sıfırlama
2. Aşağıdaki iki yöntemden birini kullanarak Kayıt için QR Kodu oluşturun:
    - "Genel Ayarlar -> Android Yapılandırması -> AE Kaydı" bölümünde "QR Kodu Oluştur" seçeneğine tıklayın. Depolama şifrelemesini atlamak isteyip istemediğinizi ve/veya tüm sistem uygulamalarının kaldırılıp kaldırılmayacağını seçin.
    - (alternatif olarak) Mevcut bir Aygıt seçin. "Cihaza Genel Bakış" bölümünde görüntülenen QR Koduna tıklayın. Depolama şifrelemesini atlamak isteyip istemediğinizi ve/veya tüm sistem uygulamalarının kaldırılıp kaldırılmayacağını seçin.
3. Şimdi cihazınızın Karşılama Ekranına 6 kez dokunun. Bu QR Kayıt Modunu başlatmalıdır.
4. Şimdi bir kablosuz ağa bağlanın ve QR kod okuyucu yüklenene kadar kısa bir süre bekleyin
5. Şimdi QR kodunu tarayın
6. Bu kadar. Cihazınız artık Android Kurumsal Cihaz Moduna kayıtlıdır.
    - a. QR Kodunu "Genel Ayarlar "da kullandıysanız, cihazınızı "Havuz -> AE Cihaz Sahibi Cihazlar" bölümünde bulabilirsiniz. (İpucu: Cihazları görmek için siteyi yeniden yüklemeniz

gerekebilir). "Otomatik Keşfi Etkinleştir" seçeneğini işaretlediyseniz, Otomatik Keşif kullanıcınız içinde bulabilirsiniz.

- Mevcut bir cihaz profilinin QR kodunu kullandıysanız, cihaz bu profile kaydedilecektir.

Yöntem 2: NFC Kaydı

(NFC ve Android 6.0 veya üstü gerektirir)

Hazırlık: WiFi bilgilerinizi "Genel Ayarlar -> Android Yapılandırması -> AE Kaydı -> NFC provizyonu için veriler" bölümüne girin. Şimdi programlayıcı olacak cihazı aramak için "NFC Cihazı "nı kullanın. Bu cihaz, kayıt bilgilerini NFC aracılığıyla diğer cihazlara göndermek için kullanılacaktır.

1. Cihazınızı Fabrika Ayarlarına Sıfırlama
2. Programlayıcınızda AppTec360'tan NFC eşleştirme uygulamasını açın
3. Depolama şifrelemesini atlamak isteyip istemediğinizi ve/veya tüm sistem uygulamalarının kaldırılıp kaldırılmayacağını seçin.
4. Her iki cihazı da arka arkaya tutun
5. Şimdi Android Kurumsal Kaydı
6. Şimdi cihazınızı konsolda bulabilirsiniz
    - a. Havuzda, Otomatik Keşfet'i yapılandırmadıysanız
    - b. Kullanıcı içinde, Otomatik Keşfet için yapılandırdığınız
    - c. İpucu: Cihazları görmek için siteyi yeniden yüklemeniz gerekebilir

Yöntem 3: Google Hesabı

(Android 5.1 veya üstü gerektirir)

(Not: Bu yöntemi kullanıyorsanız, cihaz otomatik olarak kaydedilmeyecektir. Bunun yerine manuel olarak kaydetmeniz veya Otomatik Kaydı kullanarak işlemi otomatikleştirmeniz gerekir).

1. Cihazınızı Fabrika Ayarlarına Sıfırlama
2. Bir google hesabıyla giriş yapana kadar kurulum adımlarını izleyin
3. Kullanıcı Adı/Mail olarak "afw#apptec" girin
4. "İleri" üzerine dokunun
5. Cihazınız artık bir Android Kurumsal Cihazdır

KNOX Kayıt

Burada KNOX Kaydını etkinleştirebilir ve KNOX Dağıtım Portalında bir KNOX Kayıt Profili oluşturmak için ihtiyacınız olan bilgileri bulabilirsiniz. Bunu yapılandırmak ve kullanmak için KNOX Dağıtım Portalında bir Hesaba ihtiyacınız vardır.

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

KNOX Kaydını Etkinleştir	KNOX Kaydını etkinleştirir. Dikkat: KNOX Kaydını devre dışı bırakırsanız, mevcut MDM profilleri çalışmayı durduracaktır. KNOX Kaydını tekrar etkinleştirirseniz, MDM Profilinizin "Özel JSON Verileri" alanını güncellemeniz gerekir
Otomatik Keşfi Etkinleştir	Bir cihaz kendini "KNOX Kaydı" ile kaydettirdiğinde, sistem Seri / IMEI Beyaz Listesinde ("Genel Ayarlar" > "Android Yapılandırması" > "Otomatik Kayıt") ayarlanan bilgilere dayanarak bir kullanıcıya atamaya çalışacaktır.

1. Samsung KNOX Mobil Kayıt Portalına giriş yapın https://eukme.samsungknox.com/itadmin
2. "MDM Profilleri "ne gidin
3. "Ekle" üzerine tıklayın
4. "MDM'm için Sunucu URI'si gerekli değil" seçeneğini seçin ve "İleri "ye tıklayın
5. Şimdi yönetim konsolunda gösterilen bilgilerle bir profil oluşturun

Şimdi bu KNOX Kayıt Profili, cihazları doğrudan Samsung'dan alırsanız, Samsung tarafından doğrudan cihaza yüklenebilir.

Alternatif olarak KNOX Dağıtım Uygulamasını indirebilir, KNOX Dağıtım Hesabınızla giriş yapabilir ve KNOX Kayıt Profilini NFC aracılığıyla diğer cihazlara gönderebilirsiniz.

Cihazda bir KNOX Kayıt Profili yüklüyse, Uygulamamızı indirecek ve çalışan bir internet bağlantısı varsa cihazı kaydedecektir.

KNOX Kaydı yoluyla kaydedilen cihazlar "Havuz -> KNOX Kaydı" bölümünde veya Otomatik Keşif'te belirlediğiniz kullanıcı içinde bulunabilir.

Sıfır Dokunuş

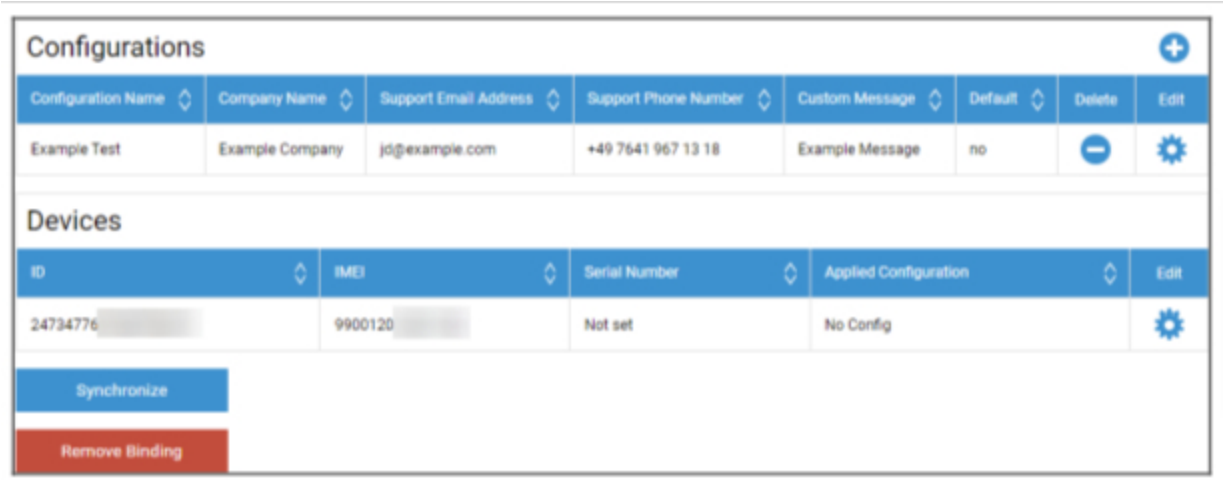
Zero-Touch ile cihazlarınızı dokunmaya gerek kalmadan kolayca kaydedebilir veya cihazın kendisinde herhangi bir şey yapılandırabilirsiniz. Tek yapmanız gereken cihazı açmak, normal şekilde yapılandırmaya devam etmek ve cihaz MDM'nin nasıl kurulacağı ve bağlanacağı ile ilgili tüm bilgileri tamamen otomatik olarak alacaktır.

Zero-Touch'ı kullanmak için cihazlarınızı Zero-Touch'ı destekleyen bir Bayiden satın almanız gerekir. Aynı Bayi, Zero-Touch Portal'da sizin için bir Hesap da oluşturuyor. Prosedür hakkında daha fazla bilgi almak için veya Zero-Touch Portal'a erişirken sorun yaşarsanız Bayinizle iletişime geçin.

Kurulumu başlatmak için "Kurulumu Başlat" üzerine tıklayın. Zero-Touch Portalına erişimi olan Google Hesabınızı seçmeniz gereken bir giriş sayfasına yönlendirileceksiniz.

NOT: HERHANGİ bir Hesap seçmek mümkündür. Bu yüzden bu adımda doğru Hesabı seçtiğinizden emin olun. Cihazlarınızı/yapılandırmalarınızı göremiyorsanız, büyük olasılıkla yanlış Hesabı kullanmışsınızdır.

Oturum açma işlemini tamamladıktan sonra aşağıdaki gibi görünecektir:



Bir Yapılandırma eklemek için "+" işaretine tıklayın ve alanları ekranda gösterildiği gibi doldurun. Yapılandırmayı varsayılan Yapılandırma olarak etkinleştirirseniz, yeni cihazlara otomatik olarak atanacaktır. Varsayılan bir yapılandırma oluşturmak veya ayarlamak, bunu mevcut cihazlara atamaz.

Bir cihazın atanmış Yapılandırması yoksa, normal bir cihaz olarak kurulacak ve MDM'ye bağlanmayacaktır. Bu nedenle cihazlarınıza atanmış bir Yapılandırma olduğundan emin olun.

Hesabınızı bağladıktan, cihazlarınız görünür olduktan ve onlara atanmış bir Yapılandırmanız olduktan sonra, cihazları ayarlamaya başlayabilirsiniz.

Cihazları Otomatik Kayıt Listesine ekleyebilirsiniz, böylece belirli bir gruba veya kullanıcıya otomatik olarak kaydedilirler. Otomatik Kayıt listesinde herhangi bir yapılandırma yapmadıysanız, cihazlar Havuza kaydedilecektir.

Windows Yapılandırması

Windows Yapılandırması

Burada, Windows 10 bilgisayarınızda aşağıdaki yapılandırmaları etkinleştirme seçeneğine sahipsiniz:

Anında DM Bağlantısı	
İlk Yeniden Deneme Süresi	Cihaza ilk bağlantı denemesini kurar, bu değer katlanarak artar
Bağlantı Yeniden Denemeleri	Bir bağlantı hatası sırasında DM-istemcisinin kaç bağlantı denemesi yapması gerektiğini belirtir
Maksimum Uyku Süresi	Bir bağlantı hatasından sonra maksimum uyku süresini belirtir
İlk Senkronizasyon Yeniden Denemeleri	İlk bağlantıdan sonra cihazın sunucu ile iletişim kuracağı aralıklar
İlk Yeniden Deneme Aralığı	"İlk Senkronizasyon Yeniden Denemeleri" ile ilgilidir Burada süreler dakika cinsinden listelenmiştir Örneğin "First Sync Retries" altında "2" değeri ve "First Retry Interval" altında "4 Minutes" değeri listelenir, bu şekilde cihaz ilk bağlantıdan sonra her 4 dakikada bir 2 kez iletişim kurar
İkinci Senkronizasyon Yeniden Denemeleri	"İlk Senkronizasyon Tekrar Denemeleri" tamamlandıktan sonra cihazın sunucu ile iletişim kurması gereken aralıklar
İkinci Yeniden Deneme Aralığı	"İlk Yeniden Deneme Aralığı" ile aynı prensip - sadece burada "İkinci Senkronizasyon Yeniden Denemeleri" için geçerlidir
Düzenli Senkronizasyon Yeniden Denemeleri	Cihazın gelecekte sunucu ile ne sıklıkta iletişim kurması gerektiğine ilişkin aralıklar Varsayılan: "Sonsuz" Bu değeri değiştirmemenizi öneririz, çünkü "10" girerseniz, cihaz sunucuyla 10x iletişim kuracak ve sonra duracaktır Bu nedenle, AppTec360 sunucusuyla iletişim kesilir!
Düzenli Yeniden Deneme Aralığı	"Birinci/İkinci Yeniden Deneme Aralığı" ile aynı prensip - sadece burada gelecek için ayarları uygular
Düzenli Yeniden Deneme Aralığı	"Birinci/İkinci Yeniden Deneme Aralığı" ile aynı prensip - sadece burada gelecek için ayarları uygular

ContentBox

Konfigürasyon

Burada ContentBox'ı yapılandırabilirsiniz. Cihazdaki ContentBox Uygulaması ile erişilebilen ContentBox'a gruplar için dosyalar yerleştirebilirsiniz.

ContentBox'ı Etkinleştir	ContentBox'ı etkinleştirin. ContentBox'ı kullanmıyorsanız bunu devre dışı bırakmak, Şirket İçi makinelerde kaynak tasarrufu sağlayabilir.
Harici ContentBox yüklemesini kullanma	ContentBox kendi Nextcloud'unuzla da çalıştırılabilir.
URL	Nextcloud varlığının tam URL'si
Kök Kullanıcı	Nextcloud Hesabının Kök Kullanıcısı
Kök Şifre	Nextcloud Hesabının kök parolası
Varsayılan grup klasörü izinleri	Varsayılan grup klasörü izinleri, grup tarafından ayrı ayrı değiştirilebilir (Mobil Yönetim'de)
Grup klasörünü alt gruplarla paylaşma	Etkinse, her alt grup ana grubun tüm klasörlerini okuyabilir, ayrıca her grup için ayrı ayrı yapılandırılabilir (Mobil Yönetim)
Alt gruplar için izinler	Alt gruplar için izinler her grup için ayrı ayrı yapılandırılabilir (Mobil Yönetim)
Paylaşıma izin ver	Kullanıcının içeriği Bağlantılar aracılığıyla paylaşmasına izin verir, her grup için ayrı ayrı yapılandırılabilir
MB cinsinden Maksimum Dosya Yükleme Boyutu	Bir dosyanın maksimum boyutu Standart: 512 MB Maksimum yapılandırma: 2048
WebDAV Kimlik Bilgileri	
WebDAV URL'si	ContentBox'ı WebDAV ile de açabilirsiniz. Lütfen aşağıdaki klasörleri hiçbir koşulda silmeyin: /apptecgroups /apptecgroups/AppTecGroup-X
Kök Kullanıcı	Kök Kullanıcıların Adı
Şifre	Kök Kullanıcıların Parolası

ContentBox ile senkronizasyon otomatik olarak gerçekleşir. Bununla birlikte, "Synchronize ContentBox" ile manuel bir senkronizasyon gerçekleştirebilirsiniz.

Ayrıca, burada ContentBox'ı her bir cihazda etkinleştirebilir/devre dışı bırakabilirsiniz.

Bu yalnızca ContentBox'ı ek olarak lisanslamadıysanız, ContentBox'ı test edebileceğiniz 25 cihaza hala erişiminiz varsa geçerlidir - burada bunu ilgili cihazlar için etkinleştirebilirsiniz.

LDAP Yapılandırması

LDAP'ye Genel Bakış

Burada, kullanıcıları ve grupları toplu olarak içe aktarmak için LDAP aracılığıyla Active Directory'nize bir bağlantı kurabilirsiniz. Senkronizasyonun manuel olarak gerçekleştirilmesi gerekir. Farklı sistemlere veya farklı konfigürasyonlara/filtrelere sahip birden fazla LDAP bağlantısı yapılandırabilirsiniz.

Sunucu Adı	Sunucunun Görünen Adı
Tip	Şu anda yalnızca LDAP'yi destekleyen Aktif Dizinler desteklenmektedir
LDAP Etki Alanı	Birincil LDAP Etki Alanı (örn. example.com)
LDAP Ana Bilgisayarı	Yalnızca LDAP ana bilgisayarına verilen LDAP Etki Alanı altında erişilemiyorsa gereklidir.
Liman	Standart Bağlantı Noktasını kullanmak için boş bırakın (SSL için 389 veya 636)
Kullanıcı Adı	Örneğin CN=John,OU=Users,DC=EXAMPLE,DC=COM Not: Çoğu sistem kullanıcı adını bu biçimde ister ve "John "u Kullanıcı Adı olarak kabul etmez
Şifre	
Şifreyi Onayla	
Bağlantı Güvenliği	Not: SSL veya TLS kullanılırken, Active Directory'nin sertifikası kontrol edilecektir. Bu kendinden imzalıysa, kök CA'yı Şirket İçi Makinenin güven deposuna eklemeniz gerekir. Bulut üzerindeyseniz, Active Directory'nin güvenilir bir sertifika sağlaması gerekir, aksi takdirde bağlantı yalnızca Şifreleme olmadan çalışır
Otomatik Senkronizasyon.	Genel LDAP ayarlarında belirtilen zaman aralığında LDAP dizininin otomatik senkronizasyonunu etkinleştirir.
Baz DN	Tüm dizini senkronize etmek istemiyorsanız, burada bir OU belirtebilirsiniz. Örneğin OU=AndroidUsers,OU=Users,DC=EXAMPLE,DC=COM
Üyesi	İçe aktarılan tüm kullanıcılar seçilen gruba eklenecektir
Sadece aktif kullanıcılar mı?	Etkinleştirildiğinde, userAccountControl özniteliği dikkate alınacak, bu özniteliğe sahip olmayan kullanıcılar içe aktarılmayacaktır.
LDAP Filtresi	Hangi Kullanıcıların içe aktarılacağını filtrelemek için LDAP Filtresini kullanabilirsiniz
Regex Filtresi	Hangi Kullanıcıların içe aktarılacağını filtrelemek için Regex Filtresini kullanabilirsiniz

Test Bağlantısı	Yapılandırmayı kaydederken bağlantıyı test eder
Senkronizasyonda dizin yapısını sıfırlayın?	Doğruysa, tüm LDAP girişleri LDAP ağacındaki orijinal konumlarına geri taşınacaktır. Etkinleştirilmesi önerilir.
Silinen kullanıcıları ve grupları yeniden içe aktarma?	Etkinleştirildiğinde, silinen kullanıcılar ve gruplar yeniden oluşturulur. Etkinleştirilmesi önerilir.
Senkronizasyon silme işlemleri?	Etkinleştirildiğinde, gruplar ve kullanıcılar LDAP sunucusunda silindiklerinde silinecektir. Ayrıca silinen kullanıcıların cihazları da silinecektir.

LDAP Yapılandırmalarınızın listesinin altında, sistemin otomatik olarak senkronize edileceği süreyi tanımlayabilirsiniz. Otomatik senkronizasyon için yalnızca uygun seçeneği etkinleştirilmiş olan LDAP Yapılandırmalarını kullanır.

Uygulama Yönetimi

Şirket İçi Uygulama DB

Android

Burada şirketinizin geliştirdiği Android Uygulamalarını yükleyebilir ve bunları daha sonra Mobil Yönetim'de cihaz veya grup profillerinde dağıtabilirsiniz.

Lütfen Google Play Store'da bulunmayan Uygulamaları yalnızca bu şekilde dağıtmanızı tavsiye ettiğimizi unutmayın.

Yüklemek istediğiniz bir Uygulamanın APK'sını yüklemek için "+" işaretine tıklayın. Şu anda yalnızca APK formatı desteklenmektedir.

OnPremise Appliance'lardaki yükleme sınırı, Appliance Yapılandırmasının 3. Adımında artırılabilir. Bulutta Yükleme Sınırını artırmak istiyorsanız, daha fazla bilgi için lütfen destek ekibiyle iletişime geçin.

Genellikle APK'ların içeriklerinden biraz daha küçük olduğunu unutmayın. APK işlem sırasında paketinden çıkarıldığı için yükleme işleminin bu nedenle başarısız olması mümkündür. Örneğin, 95 MB'lık bir APK'nın 100 MB'lık bir yükleme sınırı ile başarısız olması mümkündür. Bu durumda, yukarıda belirtildiği gibi yükleme sınırını artırın.

Ayrıca APK'yı önce manuel olarak bir test cihazına taşımanızı (örneğin USB aracılığıyla) ve cihazın Dosyalar uygulamasıyla manuel olarak yüklemeyi denemenizi tavsiye ederiz. Bu herhangi bir nedenle çalışmazsa, MDM aracılığıyla da başarısız olur.

Hedefi Güncelle

"Hedefi Güncelle" özelliği ile bir uygulamanın hangi sürümünün yüklenmesi gerektiğini veya bir uygulama için "Güncel tut" seçeneğini etkinleştirdiyseniz bir uygulamanın hangi sürüme güncellenmesi gerektiğini seçebilirsiniz.

Bir Güncelleme Hedefi seçmediyseniz, en yüksek sürüm kullanılacaktır.

Android'in uygulamaların sürümünü düşüremeyeceğini unutmayın. Ayrıca "Sürüm Kodu "nun bir sürümün daha yüksek, daha düşük veya aynı olup olmadığını belirlediğini unutmayın. Bu nedenle, bir güncelleme oluştururken uygulamanızda bu sürümü doğru şekilde artırdığınızdan emin olun.

iOS

Burada geliştirdiğiniz iOS Uygulamalarını yükleyebilir ve daha sonra Mobil Yönetim'de cihaz veya grup profilinizde dağıtabilirsiniz.

Yüklemek istediğiniz bir Uygulamanın IPA'sını yüklemek için "+" işaretine tıklayın. Şu an için sadece IPA formatı desteklenmektedir.

OnPremise Appliance'lardaki yükleme sınırı, Appliance Yapılandırmasının 3. Adımında artırılabilir. Bulutta Yükleme Sınırını artırmak istiyorsanız, daha fazla bilgi için lütfen destek ekibiyle iletişime geçin.

Hedefi Güncelle

"Hedefi Güncelle" özelliği ile bir uygulamanın hangi sürümünün yüklenmesi gerektiğini veya bir uygulama için "Güncel tut" seçeneğini etkinleştirdiyseniz bir uygulamanın hangi sürüme güncellenmesi gerektiğini seçebilirsiniz.

Bir Güncelleme Hedefi seçmediyseniz, en yüksek sürüm kullanılacaktır.

MacOS

Burada geliştirdiğiniz MacOS Uygulamalarını yükleyebilir ve daha sonra Mobil Yönetim'de cihaz veya grup profilinizde dağıtabilirsiniz.

Yüklemek istediğiniz bir Uygulamanın PKG'sini yüklemek için "+" işaretine tıklayın. Şu an için yalnızca PKG formatı desteklenmektedir.

OnPremise Appliance'lardaki yükleme sınırı, Appliance Yapılandırmasının 3. Adımında artırılabilir. Bulutta Yükleme Sınırını artırmak istiyorsanız, daha fazla bilgi için lütfen destek ekibiyle iletişime geçin.

Hedefi Güncelle

"Hedefi Güncelle" işlevi ile bir uygulamanın hangi sürümünün yükleneceğini veya bir uygulama için "Güncel tut" seçeneğini etkinleştirdiyseniz bir uygulamanın hangi sürüme güncelleneceğini seçebilirsiniz.

Bir Güncelleme Hedefi seçmediyseniz, en yüksek sürüm kullanılacaktır.

Windows 10

Burada Windows 10 Uygulamalarını yükleyebilir ve daha sonra cihaz veya grup profilinizdeki Mobil Yönetim'de dağıtabilirsiniz.

Yüklemek istediğiniz bir Uygulamanın APPX, APPXBUNDLE veya MSI'ını yüklemek için "+" işaretine tıklayın. Şu an için yalnızca APPX, APPXBUNDLE veya MSI formatı desteklenmektedir.

Ayrıca bir Uygulama için, istenen Uygulamayı yüklemeden önce otomatik olarak dağıtılacak ve yüklenecek olan Bağımlılıkları yükleyebilir ve tanımlayabilirsiniz.

OnPremise Appliance'lardaki yükleme sınırı, Appliance Yapılandırmasının 3. Adımında artırılabilir. Bulutta Yükleme Sınırını artırmak istiyorsanız, daha fazla bilgi için lütfen destek ekibiyle iletişime geçin.

Hedefi Güncelle

"Hedefi Güncelle" işlevi ile bir uygulamanın hangi sürümünün yükleneceğini veya bir uygulama için "Güncel tut" seçeneğini etkinleştirdiyseniz bir uygulamanın hangi sürüme güncelleneceğini seçebilirsiniz.

Bir Güncelleme Hedefi seçmediyseniz, en yüksek sürüm kullanılacaktır.

Win32 Paketi (.exe)

Ayrıca .exe dosyalarını/yükleyicileri cihazlarınıza dağıtabilirsiniz.

Paket adı	MDM'de görüntülenecek ad
Açıklama	MDM'de gösterilen açıklama
Paket dosyası	Yalnızca .zip dosyalarına izin verilir. Dağıtmak istediğiniz dosyaları bu zip dosyasına yerleştirin.
Dağıtım bağlamı	**Sistem**: Yükleme komutu "Kullanıcı "dan daha yüksek olan sistem ayrıcalıklarıyla çalışır. Ayrıca "Sistem" kullanıldığında işlemin kullanıcı arayüzü yoktur, bu nedenle sessiz olacaktır ve kullanıcı profiline, örneğin %AppDat% gibi ortam değişkenlerine erişilemez. **Kullanıcı**: Yükleme komutunun kullanıcı profiline erişimi vardır ve gerekirse kullanıcı arayüzünü görüntüleyebilir. Not: Bazı süreçler yalnızca bir bağlamda çalışıyor olabilir. Örneğin, bir yazılım kendisini AppData'ya yüklerse, yalnızca "Kullanıcı" seçildiğinde çalışacaktır
Yükleme komutu	Programı yüklemek için kullanılan komut. Örneğin, kökünde "setup.exe" içeren ve sessiz kurulum için "/s" parametresini destekleyen bir zip dosyası için yükleme komutu "setup.exe /s" olacaktır. Farklı yazılımların farklı parametrelere sahip olabileceğini unutmayın.
Kaldırma komutu	Yazılımı MDM aracılığıyla kaldırmak için çalıştırılacak komut. Bu genellikle kaldırıcıya işaret eder. Örneğin "C:\Program Files\ExampleSoftware\uninstall.exe".
Gereksinimler	
Not: Yazılımın yüklenmesi için belirlenen tüm gereksinimlerin karşılanması gerekir. Aksi takdirde yüklenmeyecektir. Bazı alanlar zorunlu olabilir. Bir gereksinim için herhangi bir değer belirlenmemişse, gereksinim yok sayılır.	
İşletim sistemi mimarisi	İşletim sistemi mimarisi
Min İşletim Sistemi Sürümü	Min İşletim Sistemi Sürümü
Minimum boş disk alanı (MB)	Minimum boş disk alanı (MB)
Minimum fiziksel bellek (MB)	Minimum fiziksel bellek (MB)
Minimum mantıksal işlemci sayısı	Minimum mantıksal işlemci sayısı

Min CPU Hızı (MHz)	Min CPU Hızı (MHz)
Ek Gereksinimler	İsterseniz ek gereksinim kontrolleri gerçekleştirmek için kuralları manuel olarak da tanımlayabilir veya buraya bir komut dosyası yükleyebilirsiniz.
Algılama Kuralları	
Tespit yöntemi	Burada, uygulamanın cihazda yüklü olup olmadığının nasıl tespit edileceğini tanımlayabilirsiniz. Yükleme komutları yalnızca bu kurallar uygulamanın YÜKLENMEDİĞİNİ tespit ettiğinde çalıştırılacaktır. Kaldırma komutları yalnızca bu kurallar uygulamanın yüklü olmadığını tespit ettiğinde çalışır. **Kuralları manuel olarak tanımlayın**: Örneğin belirli bir dosya, klasör, MSI veya kayıt defteri anahtarının mevcut olup olmadığını kontrol etmek için bir veya daha fazla kuralı manuel olarak tanımlamanızı sağlar. Verilen algılama kurallarının tümü doğruysa, uygulamanın mevcut olduğu kabul edilir. Komut **dosyası kullanın**: Kendi kontrollerinizle kendi komut dosyanızı yükleyin. Kod "$TRUE" değerini döndürürse, uygulamanın mevcut olduğu kabul edilir.
Algılama kuralları	

Uygulama Ayarları

iOS Uygulama Ayarları

Burada, zorunlu uygulamalara veya kurumsal uygulama mağazasına bir uygulama eklemek için varsayılan ayarları tanımlayabilirsiniz.

Not: Bu yalnızca uygulama eklerken varsayılan olarak seçili olanları ayarlar. Bu, zorunlu uygulamalara veya kurumsal uygulama mağazasına zaten eklenmiş olan uygulamalar için mevcut ayarları DEĞİŞTİRMEZ.

Güncel kalın	Uygulamayı otomatik olarak güncel tutar. Bir güncelleme yayınlandıktan sonra uygulamanın güncellenmesinin 7 güne kadar sürebileceğini lütfen unutmayın.
Yönetilmediğinde sollama	Bir Uygulama zaten yönetilmeyen (kullanıcı tarafından) olarak yüklenmişse, uygulama MDM tarafından üstlenilecek ve yönetilecektir.
MDM profili kaldırıldığında uygulamayı kaldırma	MDM kaldırıldığında Uygulamayı kaldırır.
Uygulama verilerinin yedeklenmesini önleme	Uygulama verilerinin yedeklenmesini önler.

Android Uygulama Ayarları

Burada, zorunlu uygulamalara veya kurumsal uygulama mağazasına bir uygulama eklemek için varsayılan ayarları tanımlayabilirsiniz.

Not: Bu yalnızca ekleme sırasında varsayılan olarak seçili olanı ayarlar. Bu, zorunlu uygulamalara veya kurumsal uygulama mağazasına zaten eklenmiş olan uygulamaların ayarlarını DEĞİŞTİRMEZ.

Güncel kalın	Uygulamayı otomatik olarak güncel tutar. Yalnızca InHouse Uygulamaları için kullanılabilir.
Kontrollü AppTec360 EMM İstemci Güncellemesi	Etkinleştirilirse, Yöneticiler AppTec360 EMM İstemcisi için güncelleme hedefini belirleyebilir. AppTec360 EMM İstemcisinin mevcut tüm sürümlerinin bir listesi "Genel Ayarlar" → "Uygulama Yönetimi" → "Şirket İçi Uygulama Veritabanı" → "Android" bölümünde gösterilecektir.

Üçüncü Taraf Uygulamaları

Android

Burada Ikarus için Aktivasyon Kodunuzu ayarlayabilirsiniz.

Bunu "Aktivasyon Kodunu Kullan" olarak ayarlayın ve Aktivasyon Kodunuzu buraya girin.

Not: Kod girildikten ve kaydedildikten sonra, Kod henüz cihaza gönderilen profile eklenmez. Kodun profile eklenmesi için profilinizde herhangi bir değişiklik yapmanız gerekir. Örneğin, Profildeki herhangi bir Anahtarı kapalı → açık → kapalı olarak değiştirin - Kaydet → Şimdi ata.

iOS

Burada SecurePIM Lisansınızı girebilirsiniz. Lisansı girdikten sonra "Değişiklikleri Kaydet" düğmesine basın ve SecurePIM seçeneklerini kullanabilirsiniz.

VPP / KNOX Premium

Apple Toplu Satın Alma Programı (VPP), ücretli ve ücretsiz Uygulamaları cihazlarınıza kolayca dağıtmanıza olanak tanır. Bu, cihazlarda bir Apple Kimliğine ihtiyaç duymadığınız, kullanıcıların kurulumu onaylaması gerekmediği (denetimli), kullanıcıların Apple Kimliğinin şifresini girmek zorunda kalmayacağı ve ücretli Uygulamaları her Cihazda tekrar satın almadan kolayca dağıtabileceğiniz için şiddetle tavsiye edilir.

VPP'yi kullanmak için Apple Business Manager'a kaydolmanız gerekir.

VPP Lisansları

Burada VPP Uygulamalarınız, kaç Lisansın kullanıldığı ve kaçının kullanılabilir olduğu hakkında genel bir bakış elde edebilirsiniz.

Tekerleğe tıkladığınızda hangi cihazlara bir Lisans atandığını ve bu Atamanın Durumunun ne olduğunu görebilirsiniz.

Tıklandığında, MDM'de atanan Lisanslar ile Apple tarafında atanan Lisansları karşılaştıran VPP Önbelleği yenilenir. Bu, bazı durumlarda Lisans Sorunlarını çözebilir.

VPP Token

Burada, Ayarlar → Uygulamalar ve Kitaplar bölümündeki Apple İşletme Yöneticisi'nde bulabileceğiniz VPP Token'ınızı yükleyebilirsiniz. Birden fazla VPP Jetonu yükleyebilirsiniz.

Apple Business Manager'da yeni bir Token indirerek, "Düzenle" Çarkına tıklayarak ve yenisini yükleyerek bir Token'ı yenileyebilirsiniz.

"VPP Modu" Lisans Atamasının nasıl işleneceğine karar verir. Senaryonuza bağlı olarak farklı modlar kullanmanız gerekir:

Cihazlar QR Kodu, Link, Apple Configurator veya DEP aracılığıyla kaydedilirken "Cihaz tabanlı" kullanılmalıdır.

Aygıtlar Kullanıcı Kaydı ile veya Paylaşılan iPad olarak kaydedilmişse "Kullanıcı tabanlı" gereklidir.

"Otomatik Lisans Yönetimi "ni etkinleştirirseniz, bir gruptan diğerine taşınan kullanıcılara, taşındıkları grup profiline göre otomatik olarak Apple VPP lisansları atanacaktır.

Taşındıkları gruptaki mevcut Apple VPP lisansları iptal edilmeyecektir.

Bir gruba eklenen yeni kullanıcılara, ilgili grup profiline göre otomatik olarak Apple VPP Lisansları atanacaktır.

KNOX Premium Anahtar

Samsung KNOX Konteynerini kullanmak için KNOX Premium Anahtarınızı buraya girebilirsiniz.

Lütfen bunun Android 10'dan bu yana artık desteklenmediğini unutmayın. Bunun yerine Android Enterprise Container'ı kullanın.

App Store Ayarları

Bölge ve Dil

Burada, Uygulama Yönetiminde Uygulama Arama için varsayılan Dili ve Bölgeyi ayarlayabilirsiniz.

Lütfen iTunes ayarının, sistemin belirli uygulamalar hakkındaki bilgileri nasıl alacağını da tanımladığını unutmayın. Listelerinizde garip bir şekilde görüntülenen Uygulamalarla karşılaşırsanız (örneğin eksik simge), belirli bir Uygulamanın kullanılamadığı bir bölge ayarlamış olabilirsiniz.

AE Play Store

Burada Uygulamaları onaylamak, Play Store'a kendi Uygulamalarınızı yüklemek veya kendi Web Uygulamalarınızı oluşturmak için Android Kurumsal Cihazlar için Play Store'a yönelik tüm Seçenekleri bulabilirsiniz.

Onaylı Uygulamalar

Burada onayladığınız tüm Uygulamalara Genel Bakış elde edebilirsiniz.

Play Store Uygulamaları

Bu, Play Store'u gösteren bir iFrame yükleyecektir. İstediğiniz herhangi bir Uygulamayı arayın, üzerine tıklayın ve onaylayın. Uygulamayı onaylarken, gerekli izinlerin değişmesi durumunda onayın iptal edileceğini de tanımlayabilirsiniz. Uygulamaları onaylarken bu ayarları varsayılan olarak bırakmanızı öneririz.

Bir Uygulama onaylandıktan sonra, onu profillerinize ekleyebilirsiniz.

"Onayla" düğmesi onayladıktan sonra "Onayı iptal et" olarak değişecektir, böylece artık ihtiyacınız yoksa Uygulamaları her zaman kaldırabilirsiniz.

Özel Uygulamalar

Burada kendi Uygulamanızı Google Play Store'a özel bir Uygulama olarak yükleyebilirsiniz. Bu, Uygulamayı Google Hizmetleri aracılığıyla dağıtmanıza ve onlar aracılığıyla güncellemenize olanak

tanır. Bu aynı zamanda kendi Uygulamalarınızın normalde gerekli olan kullanıcı onayı olmadan yüklenebilmesi avantajına da sahiptir.

Web Uygulamaları

Burada, Uygulamalar gibi atanabilen belirli Web Sayfalarına bağlantılar olan Web Uygulamaları oluşturabilirsiniz.

Ayrıca buna özel bir Simge verebilir ve tam olarak nasıl görüntüleneceğini tanımlayabilirsiniz.

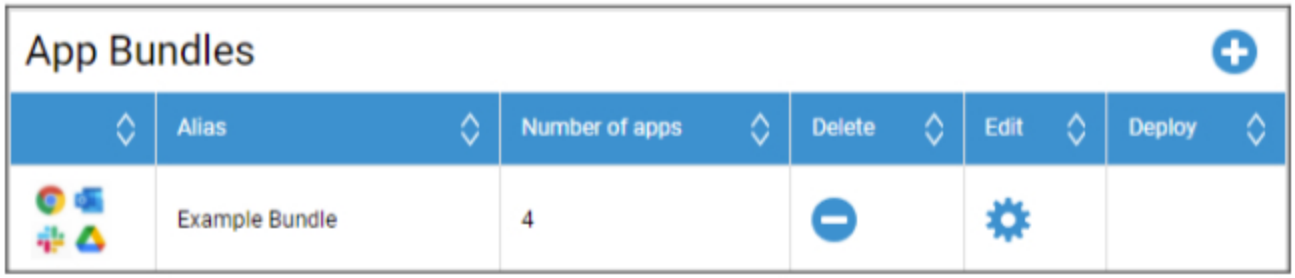
Mağaza Düzeni

Mağaza Düzeni, Uygulamaların Play Store'da nasıl görüntüleneceğini veya hiç görüntülenip görüntülenmeyeceğini tanımlar.

Kullanıcının manuel olarak yüklemesi için Play Store'daki Uygulamaları göstermek istiyorsanız, bunların Düzen'de buraya eklenmesi gerektiğini unutmayın **VE** profilinde Enterprise Play Store'a yönlendirin. Bir Uygulamayı bunlardan yalnızca birine eklerseniz, görüntülenmeyecektir.

Uygulama Paketi

Uygulama Paketleri ile tek bir tıklamayla cihaz veya grup profillerine atanabilen uygulama grupları tanımlayabilirsiniz.



Yeni bir Uygulama Paketi oluşturmak için "+" işaretine tıklayın. Bir Uygulama Paketi oluşturduktan sonra, Pakete çeşitli Kaynaklardan uygulamalar eklemek için "Düzenle "ye tıklayabilirsiniz.

Diğer tüm Uygulamalar gibi profillere bir Paket eklenebilir. Uygulama eklerken, Paketlerinizin bulunduğu "Uygulama Paketleri" adlı ekstra bir Sekmeye sahip olacaksınız.

Bir Uygulama Paketinde herhangi bir değişiklik yaparsanız, "Dağıt" sütununda bir Düğme görünecektir. Bu, bu değişiklikleri bu Paketi içeren tüm profillere göndermenizi sağlayacaktır. Bu nedenle, bir Pakete uygulama ekledikten veya kaldırdıktan sonra bunu manuel olarak yapmanız gerektiğini unutmayın.

Uzaktan Kumanda

TeamViewer

TeamViewer Bağlayıcısı

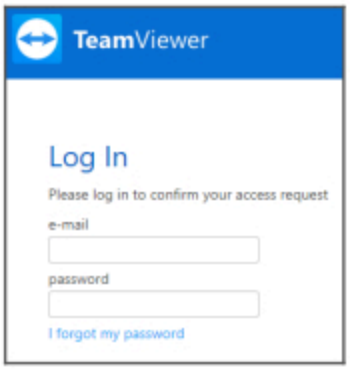
Not: Bulut sürümümüzün ücretsiz denemesinde TeamViewer hesabınızı bağlayamazsınız. Bunun yerine otomatik olarak bağlanan ücretsiz bir demo hesabınız olacak.

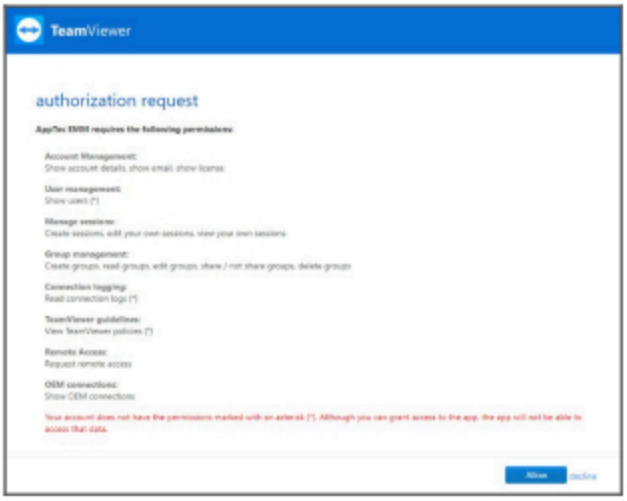
Genel Ayarlar -> Uzaktan Kumanda -> TeamViewer'a gidin. Burada TeamViewer Hesabınızı konsola bağlayabilir veya şu anda bağlı olan hesabınız hakkındaki bilgileri görebilirsiniz. Ayrıca "Aktif Oturumlar" bölümüne giderek o anda aktif olan tüm oturumları görüntüleyebilirsiniz.

Hesabınızı bağlamak için "Kurulumu Başlat "a tıklayın.

Bunu yapmak sizi TeamViewer hesabınızla giriş yapmanız gereken yeni bir sayfaya yönlendirecektir.

Oturum açtıktan sonra, AppTec360 MDM'yi bu hesabı kullanması için yetkilendirmiş olursunuz. Bunu onayladıktan sonra birkaç saniye beklemeniz gerekir ve Hesap bağlanır.


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


TeamViewer
authorization request

TeamViewer QuickSupport'u Yükleme

"TeamViewer QuickSupport" uygulamasını cihaz profilinizin veya grup profilinizin zorunlu uygulamalarına ekleyin ve "Şimdi Ata "ya tıklayın. Uygulama cihaza yüklenene kadar bekleyin.

Uygulamanın yüklü olmadığı bir cihaza erişmeye çalışırsanız, cihaz yapılandırmasına bağlı olarak uygulama yüklenir veya uygulamanın yüklenmesi istenir.

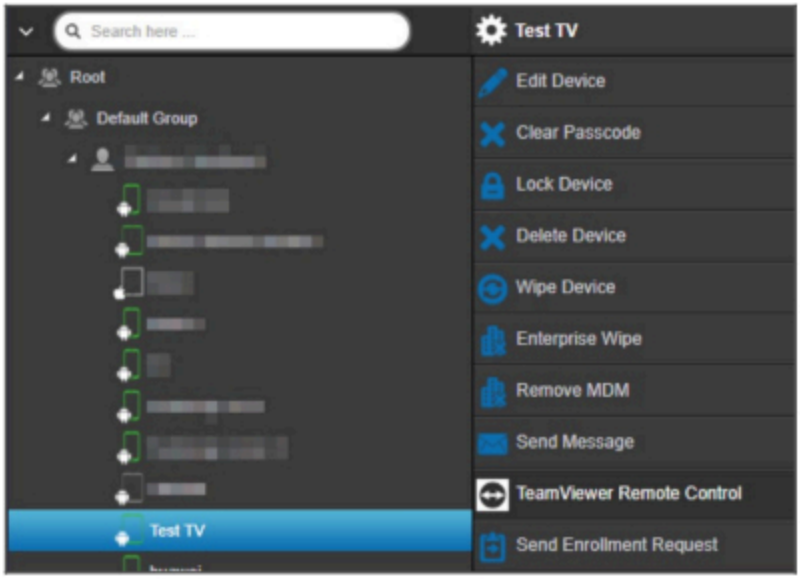
Cihazınızı Uzaktan Kontrol Edin

Cihazınızı uzaktan kontrol etmek için cihazı seçin, tekerleğe tıklayın ve "TeamViewer Uzaktan Kontrol "ü seçin

Zaten aktif bir oturum varsa, eski oturumu kullanabilir veya yeni bir oturum oluşturabilirsiniz.

Yeni bir TeamViewer Oturumu oluşturmak istediğinizi onaylayın.

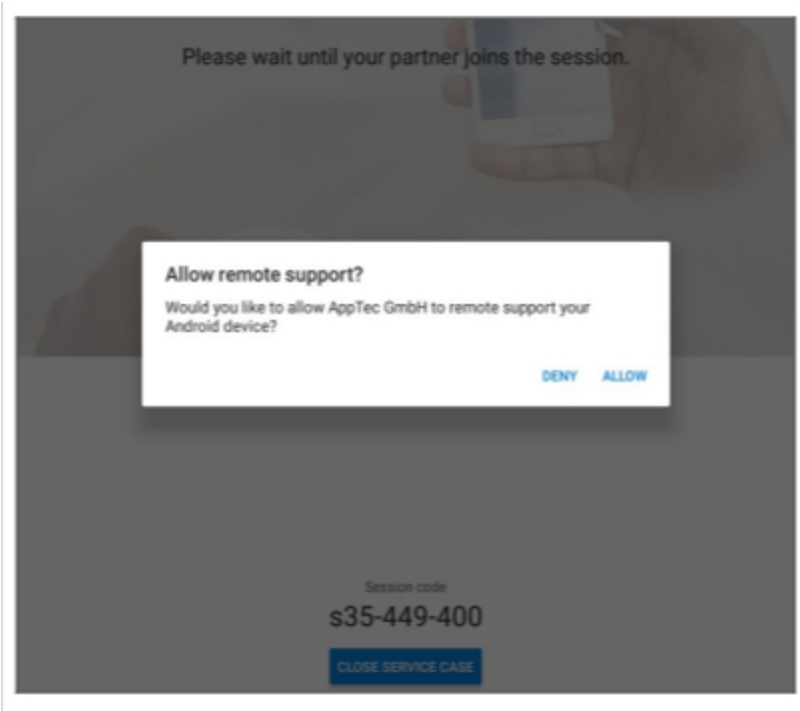
Birkaç saniye sonra TeamViewer Oturumunuz için bir bağlantı alacaksınız. Bu bağlantıyı yeni bir pencerede açmak için "Başlat "a tıklayabilirsiniz.


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

Bu bağlantı, yüklü TeamViewer'ınızı açacak ve sizi cihazınıza bağlayacaktır.

Şimdi uzaktan kontrol etmek için cihazın kendisinde bağlantıyı onaylamanız gerekir.

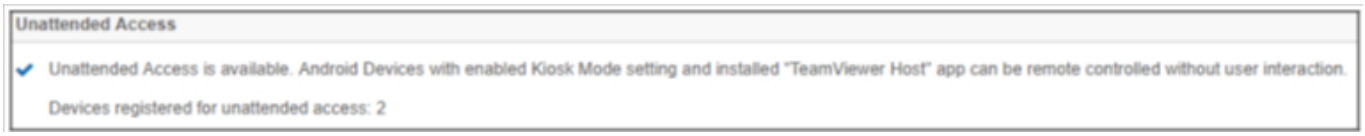


iOS kullanıyorsanız AppTec360 MDM İstemcisinde bir mesaj alacaksınız. Bu bağlantı ile cihaz uzak oturuma katılacaktır. Cihazın bildirim ayarlarına bağlı olarak, bir bildirim almamanız ve AppTec360 MDM İstemcisini manuel olarak açmanız gerekebilir.

Bazı Android cihazlarda (örneğin Samsung) eklenti olarak ek bir uygulama yüklemek gerekir. Cihazınızda bu gerekliyse, cihazdaki TeamViewer uygulaması sizi bu konuda bilgilendirecektir.

Gözetimsiz Erişim

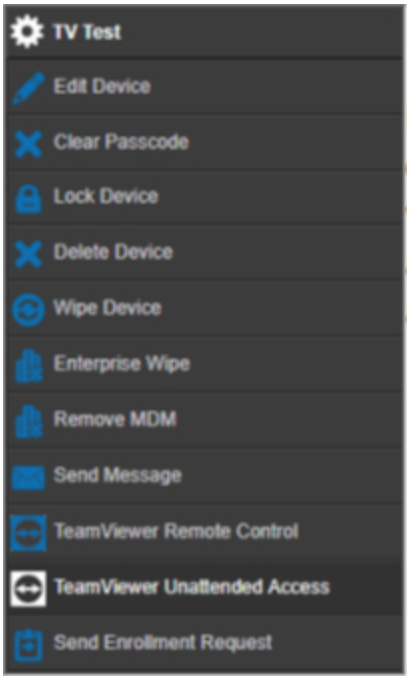
Not: Katılımsız Erişim yalnızca Android cihazlarda mümkündür.



TeamViewer Hesabınız bir "Tensor" veya "Kurumsal" Lisans kullanıyorsa, cihazdaki bağlantıyı kabul etmeden cihazlarınıza bağlanabilirsiniz.

Hesabınızı bağladıktan sonra bunu "Genel Ayarlar" bölümünden kontrol edebilirsiniz

Katılımsız erişimi kullanmak için, "TeamViewer Host" uygulamasını yüklemeniz ve profilinizdeki "Kiosk Modu ve Başlatıcı" altında "Katılımsız Erişimi Etkinleştir" seçeneğini etkinleştirmeniz gerekir. Lütfen bunun yalnızca Kiosk Modunu kullanıyorsanız mümkün olduğunu unutmayın.



Şimdi cihazınızı seçip tekerleğe tıklarsanız gözetimsiz erişimi seçebilirsiniz. Bu, cihazın kendisinde herhangi bir onaya gerek kalmadan sizi cihazınıza bağlayacaktır. Cihazınıza erişmek için Bağlantıyı almanızın birkaç dakika sürebileceğini lütfen unutmayın.

Splashtop

Splashtop seçeneğini etkinleştirirseniz, profillerinizde Splashtop yapılandırma seçeneklerini görürsünüz.

Splashtop'u kullanmak için Splashtop Streamer'ı (com.splashtop.streamer.csrs) profilinizde zorunlu uygulama olarak ayarlamanız gerekir. Daha sonra Splashtop Yapılandırmasını profilinizdeki "Uzaktan Kumanda" bölümünden etkinleştirebilirsiniz. Bunu etkinleştirmek Splashtop Streamer uygulamasını yapılandıracaktır. Splashtop Streamer kullanıyorsanız ancak MDM ile birlikte kullanmıyorsanız, bunu kapalı bırakmalısınız.

Profilinizde "Uzaktan Kumanda" altında bir dağıtım kodu da ayarlamanız gerekir. https://my.splashtop.com adresine gidin ve Splashtop hesabınıza giriş yapın. "Bilgisayar Ekle "ye tıklayın ve çıkan sayfadaki 12 haneli dağıtım kodunu kopyalayın.

Dağıtım Kodu olmadan uzaktan kumanda mümkün DEĞİLDİR.

Bunu yaptıktan sonra, cihazınıza sağ tıklayabilir ve "Splashtop Uzaktan Kumanda" seçeneğine tıklayarak bir uzaktan Oturum başlatabilirsiniz

Sim Kart Yönetimi

CSV Toplu İçe Aktarma

Bu, atanmış Sim Kartlarınıza ve onlarla ilgili tüm bilgilere genel bir bakış gösterir. Bu, yalnızca cihazlarınız hakkında değil, Sim Kartlarınız hakkında da tüm bilgilere tek bir sistemde sahip olmanıza yardımcı olur.

NOT: Bu bir manuel yönetim/dokümantasyondur. İşletim sistemlerinin gizlilik/güvenlik mekanizmaları nedeniyle bu verilerin cihazlardan otomatik olarak alınması mümkün değildir.

Bu listeyi CSV olarak da dışarı ve içeri aktarabilirsiniz.

Taşıyıcı ve Tarife

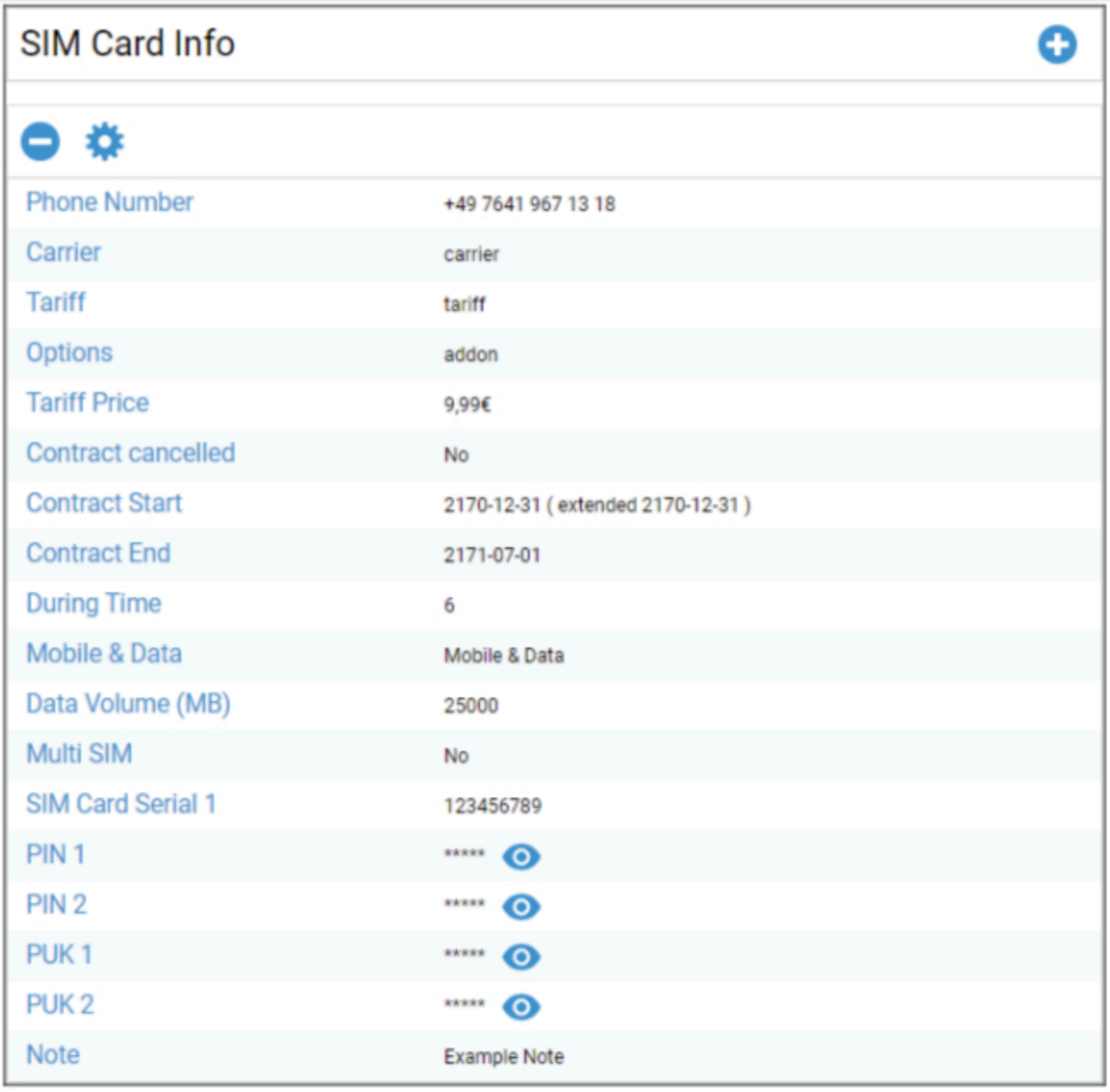
Bir Sim kart eklemek için, önce bir veya birden fazla taşıyıcı eklemek için Düğmeye tıklayın.

Daha sonra bir taşıyıcıya Tarife eklemek için "Tarife Bilgileri" üzerindeki "+" işaretine tıklayın.

İsteğe bağlı olarak böyle bir şeyiniz varsa aşağıya isteğe bağlı Eklentiler ekleyebilirsiniz.

Bu, gerçek bir Sim Kart eklemek için ihtiyacınız olan her şeyi hazırladı. Sim Kartlar şu anda bir Kullanıcıya atanmıştır. Bu nedenle Mobil Yönetim'e gidin, bir Kullanıcı seçin ve "Sim Karta Genel Bakış "a gidin.

Burada bu kullanıcıların Sim Kartlarını görüyorsunuz. Eğer varsa, düzenleyebilir veya kaldırabilirsiniz. Kullanıcılar birden fazla Sim Karta sahip olabilir.

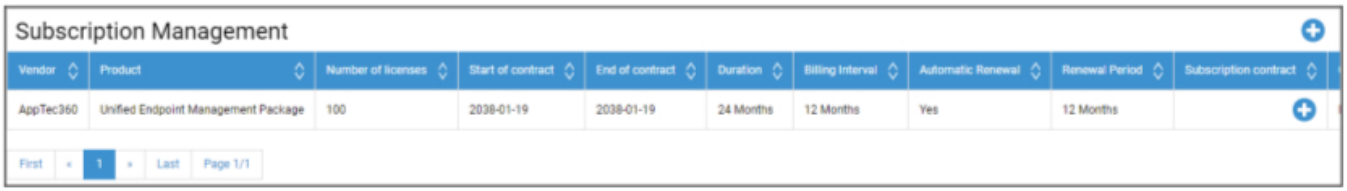


Bir Sim Kart eklemek için "+" işaretine tıklayın ve ihtiyacınız olan tüm Bilgileri ekleyin. Bu Sim Kartlar, Genel Ayarlar → Sim Kart Yönetimi'ndeki tüm Sim Kartlarınızın listesinde de listelenecektir.

Abonelik Yönetimi

Abonelik Yönetimi

Burada, devam eden abonelikleri, ayrıntılarını belgeleyebilir ve ayrıca imzalı sözleşme, fesih mektubu vb. gibi farklı dosyaları saklayabilirsiniz. Ayrıca, abonelik sona ermeden önce size posta yoluyla hatırlatan ve belki de otomatik olarak uzayan hatırlatıcılar da ayarlayabilirsiniz.



Bir abonelik eklemek için üstteki "+" işaretine tıklayın. İstediğiniz kadar abonelik ekleyebilirsiniz.

Bu Abonelikle ilgili dosyaları yüklemek için farklı alanlardaki "+" işaretine tıklayın. Teknik olarak herhangi bir dosya türünü yükleyebilirsiniz, ancak her dosya türünün tarayıcıda önizlenemeyeceğini unutmayın.

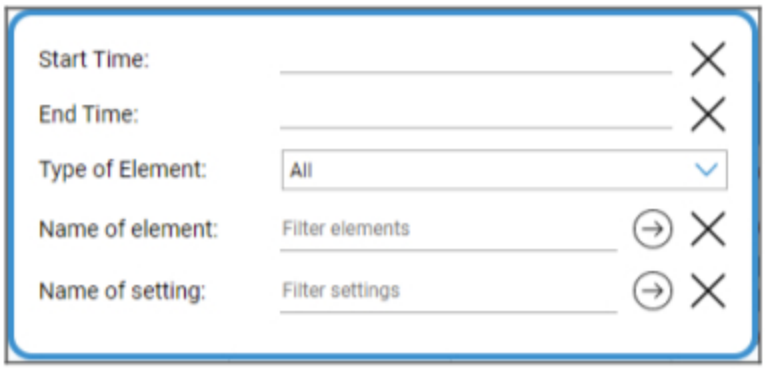
Genel Denetim Günlüğü

Denetim Günlüğü

Burada, yapılan tüm değişiklikleri gösteren genel bir Denetim Günlüğüne sahipsiniz. Bir kullanıcı veya gruptaki Denetim Günlüğü yalnızca bu kullanıcı veya gruba göre değişiklikleri gösterirken, bu konsolun herhangi bir yerinde yapılan HER değişikliği gösterir.

Neyin, kim tarafından, ne zaman ve nerede değiştirildiğini görebilirsiniz. Bazı durumlarda daha fazla ayrıntı görmek için Girişi de genişletebilirsiniz.

Değişikliğin yapıldığı konuma ulaşmak için kullanıcıya veya "Yol / Tür" içindeki girişe tıklamak mümkündür.



Sağ üstte, birçok değişikliğin gerçekleştiği bir ortamda belirli değişiklikleri bulmanıza yardımcı olabilecek bir filtre de tanımlayabilirsiniz.

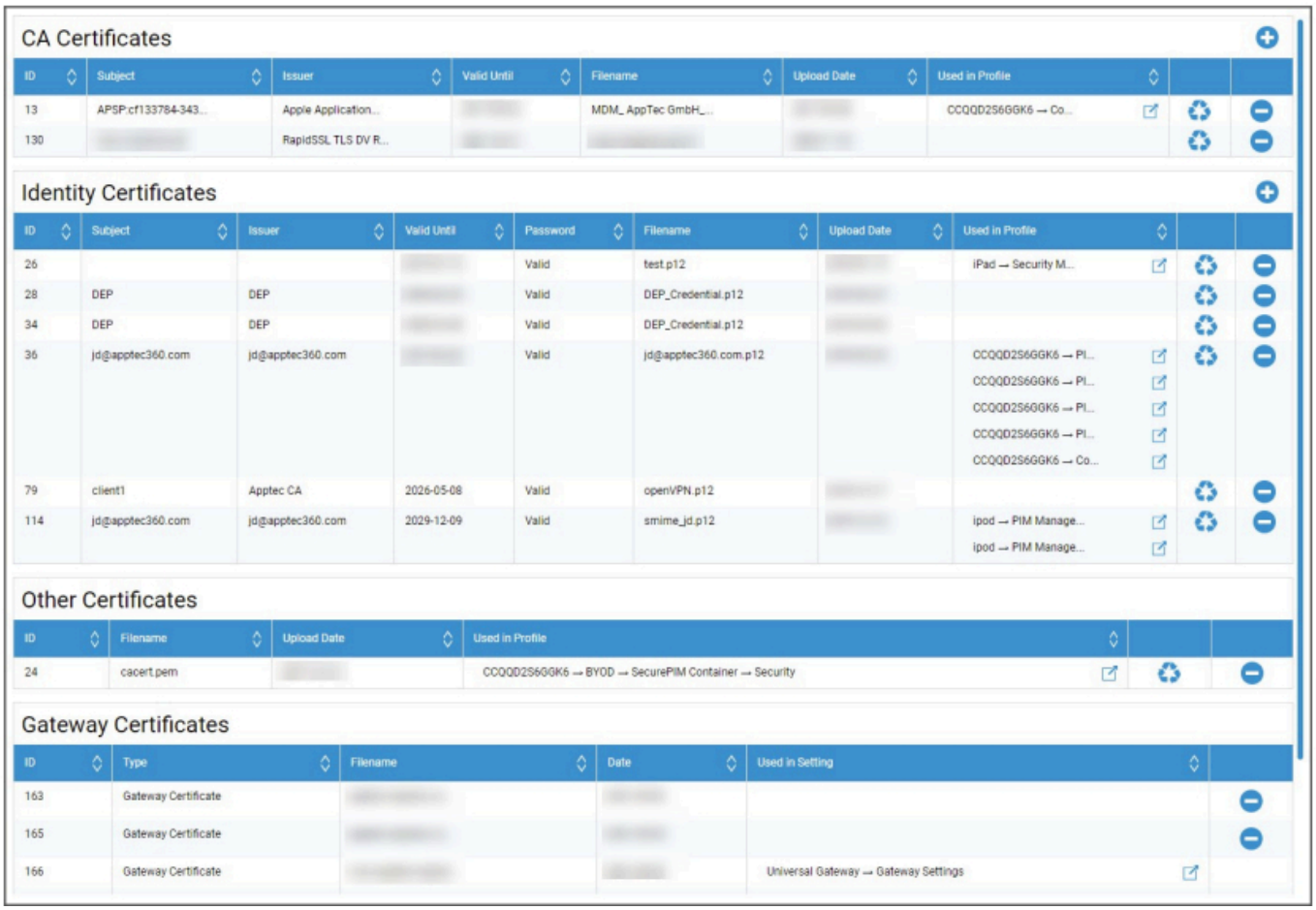
Denetim Günlüğü Ayarları

"Denetim Günlüğü Saklama Süresi" Denetim Günlüklerinin silinmeden önce ne kadar süreyle saklanması gerektiğini tanımlar.

Sertifika Yönetimi

Burada, Konsolda yüklenen ve kullanılan tüm sertifikalara genel bir bakış elde edeceksiniz. Bu sadece genel bir bakış. Örneğin Wi-Fi sertifikaları için gerçek yapılandırma hala ilgili konumdaki profilde yapılır.

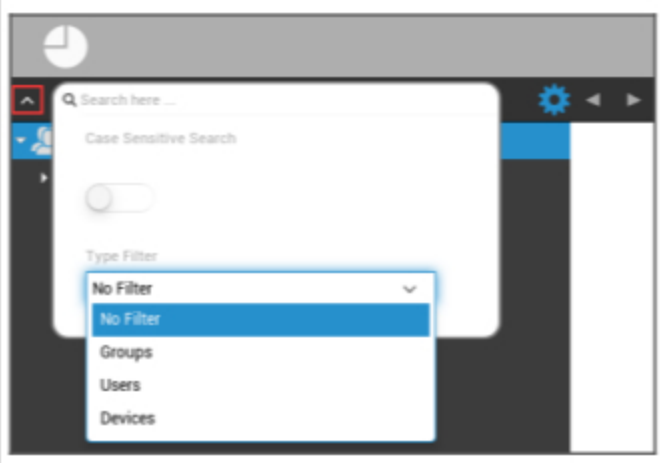
Burada ayrıca, etkilenen profillere otomatik olarak yansıtılacak olan sertifikaları kaldırabilir veya güncelleyebilirsiniz. Herhangi bir sertifikanın hala tam olarak nereye atandığını görmek için "Profilde Kullanılan" bilgisine tıklayın.



Mobil Yönetim

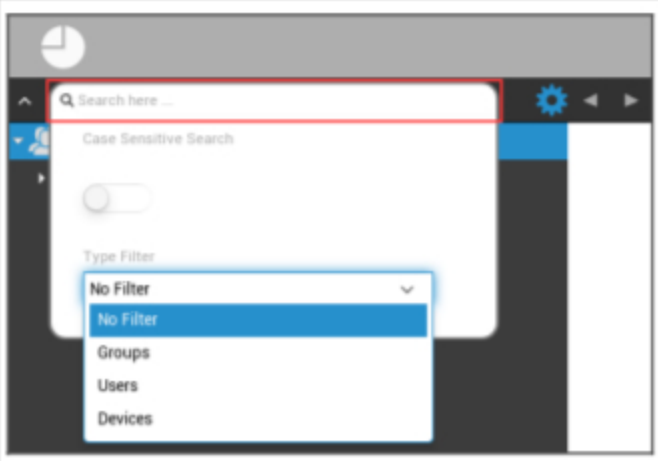
Mobil Yönetim Ekranı

Cihaz filtresi



Ekranın sol üst köşesine tıklayarak, cihazların görüntülenmesi için çeşitli filtreler bulabilirsiniz.

Arama penceresi



Arama penceresi, belirli bir anahtar kelimeyle tüm cihazları ve/veya kullanıcıları aramanıza olanak tanır.

Seçenekler dişli

İlgili sembole tıkladıktan sonra, kullanabileceğiniz seçeneklerin bir listesi görüntülenir.

Bunlar her güncel pencere ile değişir ve ilgili bölümlerde açıklanmıştır.

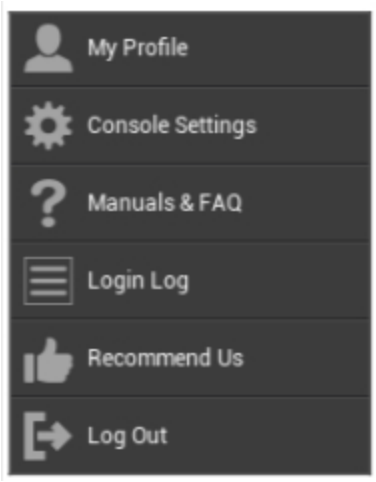
Gezinme okları

Sol oka tıkladığınızda bir önceki sayfaya yönlendirileceksiniz.

Daha sonra, sağ oka tıkladığınızda, az önce ayrıldığınız sayfaya yönlendirileceksiniz.

Yönetim hesap ayarları

Yukarıda görüldüğü gibi e-posta adresine tıklandığında aşağıdaki menü görüntülenir:



Benim profilim	Yöneticilerin hesap ayrıntılarını düzenleme
Konsol Ayarları	Admins hesabı için konsol ayarlarını yapılandırma
Kılavuzlar & SSS	"Genel Ayarlar "da "Kılavuzlar ve SSS" sayfasını görüntüleyin
Giriş Günlüğü	"Oturum Açma Günlüğüne" erişin
Bizi Tavsiye Edin	"Genel Ayarlar "da "Bizi Önerin" sayfasını görüntüleyin
Çıkış Yap	MDM konsolundan çıkış yapın

Kullanıcı Bilgileri

Burada, o anda oturum açmış olan yöneticinin hesap ayrıntılarını düzenleyebilirsiniz.

Kullanıcı Adı	Hesabın kullanıcı adı ve/veya e-posta adresi
İsim	Yöneticilerin ilk adı
Soyadı	Yöneticilerin soyadı
Giriş Adı	Yöneticiler oturum açma adı
e-Posta Adresi	Yöneticilerin e-posta adresi
Alternatif e-Posta adresi	Yöneticilerin alternatif e-posta adresi
Resim	Profil resmi
Telefon Numarası	Yöneticilerin telefon numarası
Cep Telefonu Numarası	Yöneticilerin cep telefonu numarası
Telefon Uzantısı	Telefon uzantısı
Konum	Konum
Pozisyon	Şirketteki pozisyonunuz
Kullanıcı grubu	Yönetici hesabını hangi kullanıcı grubuna atamak istediğinizi seçin
Yorum	Bir yorum girin
Yeni şifre girin	Şifre değişikliği için şifreyi girin
Yeni şifreyi tekrarla	Onaylamak için yeni şifreyi tekrarlayın

Yönetim erişiminin hiyerarşi yapısında yerel bir kullanıcı hesabı olarak da dosyalanabileceğini lütfen unutmayın. Ek bir hizmetli oluşturulmadan bu silinmemelidir!

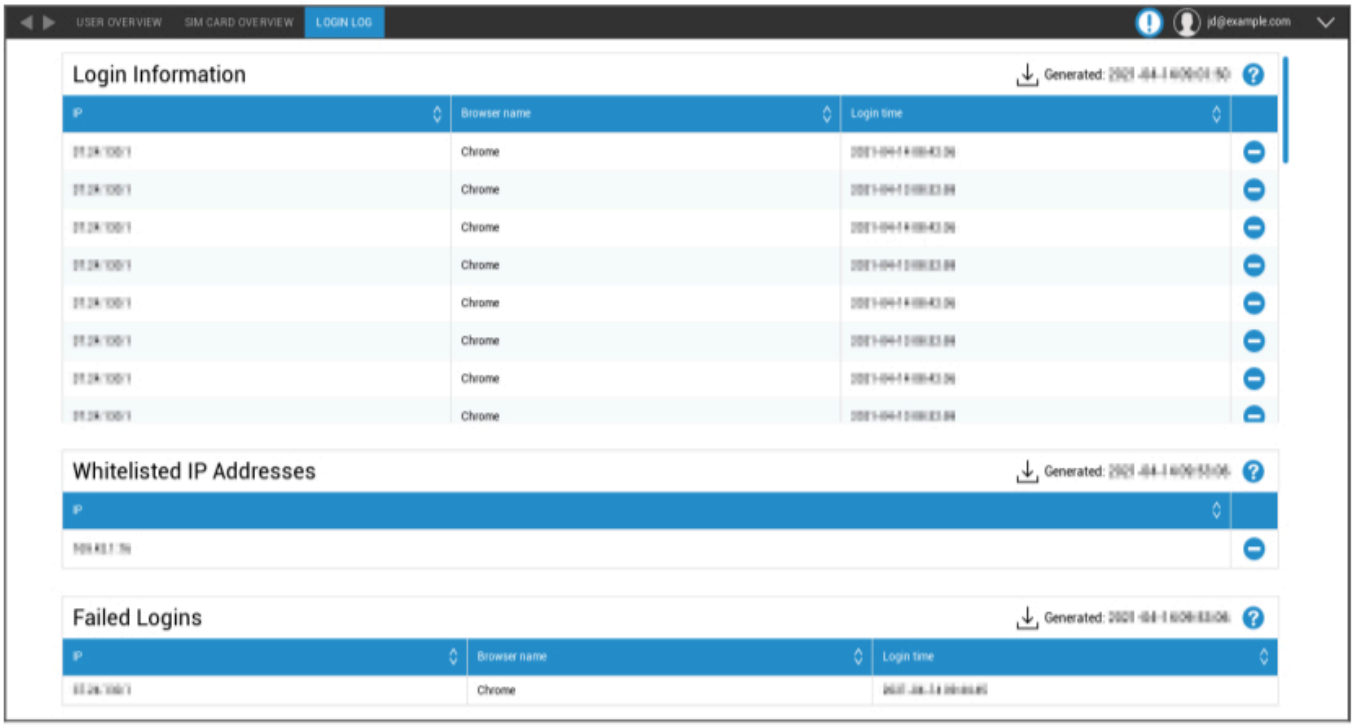
Konsol Ayarları

Burada Yöneticiler hesabı için aşağıdaki konsol ayarlarını yapılandırabilirsiniz:

Dizin Kullanıcı Görüntüleme Seçenekleri	Kullanıcıların ağaçta nasıl etiketlenmesi gerektiğini tanımlayın
Dizin Cihazı Görüntüleme Seçenekleri	Cihazların ağaçta nasıl etiketleneceğini tanımlayın
Oturum Zaman Aşımı	Kullanıcı belirtilen süre içinde hiçbir şey yapmazsa, kullanıcı oturumu kapatılır. Varsayılan değer 60 dakikadır. Lütfen bu ayarı değiştirdikten sonra oturumu kapatıp tekrar açın.
Zaman Dilimi	Kullanılan saat dilimini seçin
Zaman Formatı	Zaman damgalarının nasıl görüntüleneceğini seçin
Konsol Dili	Konsolun görüntülenmesi gereken dili seçin. İngilizce ve Almanca mevcuttur.
Ana Renk	Konsolun renk düzeni için temel olarak kullanılacak bir renk ayarlayabilirsiniz. Renk seçiciyi kullanabilir ya da HTML HEX gösteriminde bir renk girebilirsiniz. 'Pembe', 'sarı' gibi RGB biçimlendiriciler de çalışır.
Kaydet Komutu	"Kaydet" düğmesine basmadan kaydetmeyi tetikleyen tuş kombinasyonu.
İki Faktörlü Kimlik Doğrulama Kullanın	Oturum açarken iki faktörlü kimlik doğrulama kullanımını etkinleştirin. Giriş yaptıktan sonra, giriş yapmak için girmeniz gereken bir kod içeren bir e-posta alacaksınız.
İki Faktörlü Kimlik Doğrulama Zaman Aşımı	Başarılı bir kimlik doğrulamasından sonra sizden iki faktörlü kimlik doğrulaması istenmeyeceği bir süre belirleyin.
Doğrulama Kodunu şu yolla gönderin	Doğrulama kodu seçilen seçeneklere gönderilecektir. Cihaz mesajı, AppTec360 MDM Uygulamasında size ait olan tüm Android ve iOS cihazlarda gösterilecektir.
Giriş yaptıktan sonra giriş mesajı gönder	Etkinleştirilirse, beyaz listede olmayan bir ip adresinden yapılan her giriş için bir e-posta gönderilecektir. E-posta, oturum açma hakkında bilgi içerir (örn. IP, Tarayıcı).

Giriş Günlüğü

Burada, oturum açmış olan yönetici hesabının oturum açma bilgilerini görebilirsiniz.



Giriş Bilgileri	Oturum açmış olan yönetici hesabının konsol tarafından kaydedilen girişlerini içeren bir liste. Bu liste son 30 gün içindeki tüm başarılı girişlerinizi gösterir.
Beyaz Listedeki IP Adresleri	Bu, beyaz listedeki tüm IP adreslerinizin listesidir. Burada listelenen bir IP'den giriş yaparsanız giriş mesajını almazsınız. Yukarıdaki "Oturum Açma Bilgileri" listesinde bir girişin yanındaki düğmeye tıklayarak bu listeye bir IP adresi ekleyebilirsiniz. Bu listedeki veya yukarıdaki "Oturum Açma Bilgileri" listesindeki bir girişin yanındaki düğmeye tıklayarak bir IP adresini bu listeden kaldırabilirsiniz.
Başarısız Girişler	Bu, son 30 gündeki tüm başarısız oturum açma denemelerinin bir listesidir. Eğer 20 dakika içinde en az 3 kez doğru şifreyi giremezseniz, bu listede bir giriş görünecektir. Ayrıca başarısız giriş denemeleri hakkında e-posta yoluyla bilgilendirileceksiniz.

Mobil Yönetimde Kurumsal Yönetim (Root-Node)

Root-Node'a (ilk grup) ulaştığınızda, Mobil Yönetim ile ilgili olarak şirketiniz için çeşitli ayarlar yapabilirsiniz.

Alt Grup Oluşturma	Bir alt grup oluşturun
Kök Düğümü Yeniden Adlandır	Kök Düğümün yeniden adlandırılması (örn. şirketinizin adı)
Toplu Kayıt	Aynı anda birden fazla cihazı / kullanıcıyı kaydetme
Toplu Görevlendirme	Tek bir bakışla ilgili gruplar için bir profil atayın
Hızlı Uygulama Yönetimi	Bir uygulama için (Un-)Kurulum taleplerini ilgili grup cihazlarına gönderme
CSV Kullanıcı İçe Aktarma	Kullanıcıları CSV'den ilgili gruba aktarma

Alt Grup Oluşturma

"Alt Grup Oluştur" ile ek bir alt grup oluşturabilirsiniz.

Alt grubun hangi grup altında atanması gerektiğini belirleyebilirsiniz.

(Varsayılan olarak, kök düğümde bir alt grup olarak atanan yeni bir grup oluşturulur)

Kök Düğümü Yeniden Adlandır

Burada kök adınızı yeniden adlandırabilirsiniz. Bu durumda şirket adının kullanılması yaygındır.

Toplu Kayıt

"Toplu Kayıt" ile birden fazla cihazı ve kullanıcıyı kaydedebilirsiniz.

Kullanıcının kaydı ne şekilde alması gerektiğini doğrudan seçebilirsiniz (e-Posta; alternatif e-Posta; SMS)

Kullanıcının hangi cihazı alacağına bağlı olarak (iOS, Android, Windows Phone), bunu doğrudan burada işaretleyebilirsiniz.

Bunun bir Akıllı Telefon mu yoksa Tablet mi olduğu ayrımı da burada yapılandırılabilir ve bunu bir onay işaretiyle doğru bir şekilde seçmeniz gerekecektir.

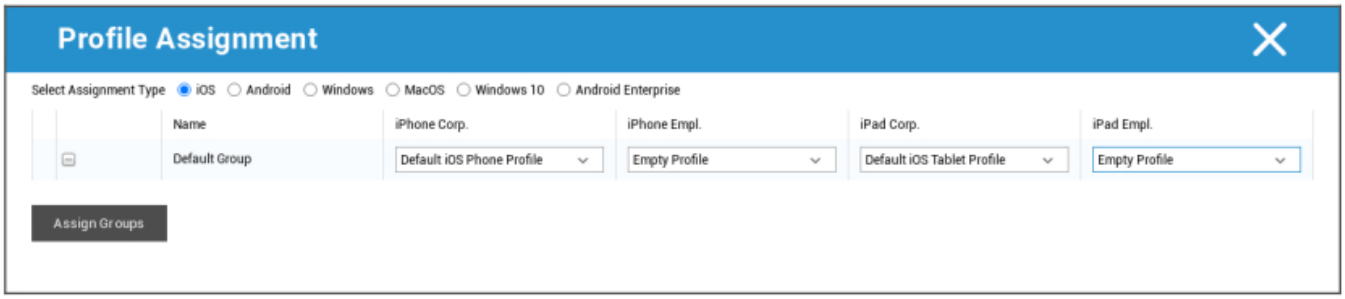
Son adım olarak, ilgili cihazın kurumsal mı yoksa özel (BYOD) mi olduğunu belirleyebilirsiniz.

"CSV Olarak Dışa Aktar" ile Bilgileri bir CSV veri dosyası olarak dışa aktarabilirsiniz. Buna karşılık, CSV veri dosyasını "CSV'yi İçe Aktar" ile de içe aktarabilirsiniz, dosya aşağıdaki örnek gibi görünmelidir:

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

Toplu Görevlendirme

Toplu Atama altında tüm gruplara bir profil atayabilirsiniz, bu iOS - Android - Windows - MacOS - Windows 10 - Android Enterprise olarak ayrılmıştır.

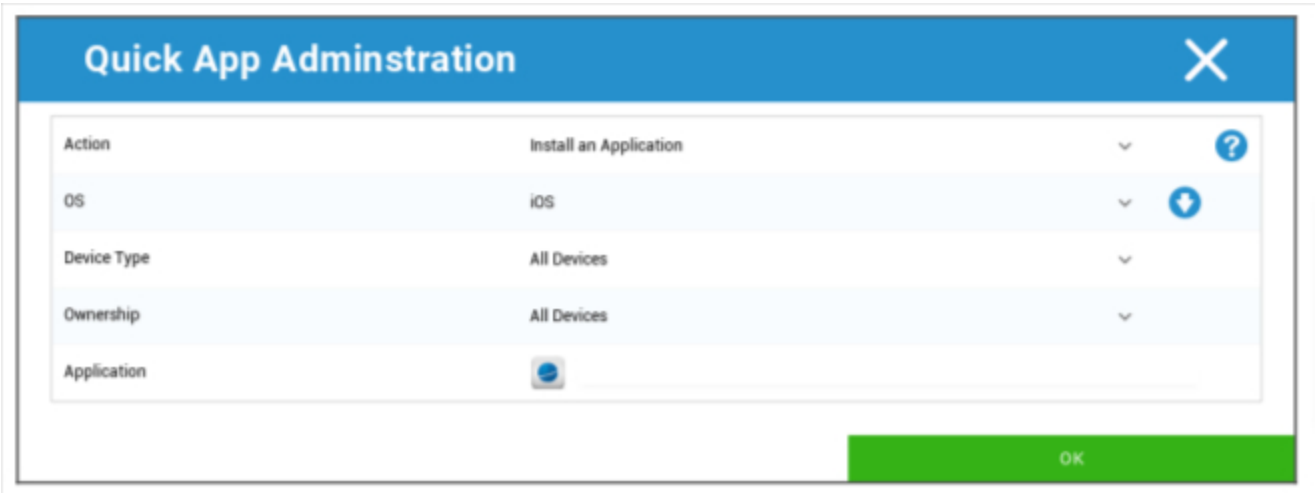


Windows - MacOS - Windows 10 - Android Enterprise

Hızlı Uygulama Yönetimi

Hızlı Uygulama Yönetimi altında, seçtiğiniz bir işletim sistemine belirli bir uygulama için Yükleme veya Kaldırma istekleri gönderebilirsiniz.

Ayrıca, talebin seçilen işletim sisteminin tüm cihaz türlerine mi yoksa yalnızca belirli bir cihaz türüne mi gönderileceğini de tanımlayabilirsiniz.



CSV Kullanıcı İçe Aktarma

Kullanıcıları CSV'den ilgili gruba aktarın.

"CSV Şablonunu İndir" ile, doldurulabilecek (veya referans olarak kullanılabilecek) bir CSV şablon dosyasını dışa aktarabilirsiniz.

Kendi CSV dosyanızı oluşturmak için "Rol Kimliklerini Göster" ve "Grup Kimliklerini Göster" seçeneklerini de referans olarak kullanabilirsiniz.

CSV dosyası "CSV Yükle" ile MDM'ye yüklenebilir.

Son adım olarak, "İçe Aktarmayı Başlat" seçeneğine tıklayarak İçe Aktarmayı başlatabilirsiniz.

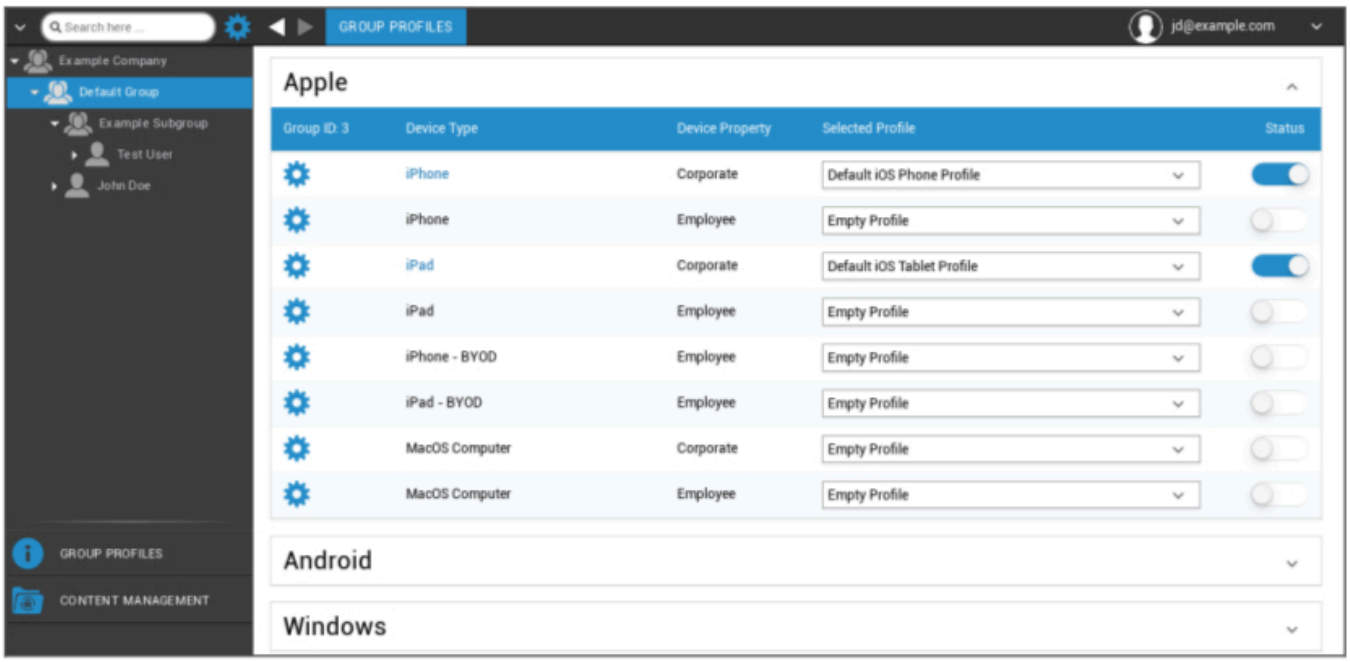
Mobil Yönetimde Grup Yönetimi

Genel bakışa tek bir tıklama, ilgili platformlar için farklı yapılandırma profillerini görüntüler.

Bir profil, AppTec360 ile son kullanıcı cihazında önceden oluşturulabilen tüm ayar seçeneklerini içerir. Her platformda kurumsal cihazlar (Kurumsal) veya Kendi Cihazını Getir cihazları (Çalışan) için profiller oluşturabilirsiniz.

Cihaz gruplarının konfigürasyonlarını, örneğin konuma veya işleve göre farklılaştırmak için, birkaç alt grubun oluşturulması tavsiye edilir.

Lütfen Mobil Yönetim'deki Profil Yönetimi'ne dikkat edin



Dişli menüsü ile ilgili (alt) grup için çeşitli ayarlar yapabilirsiniz.

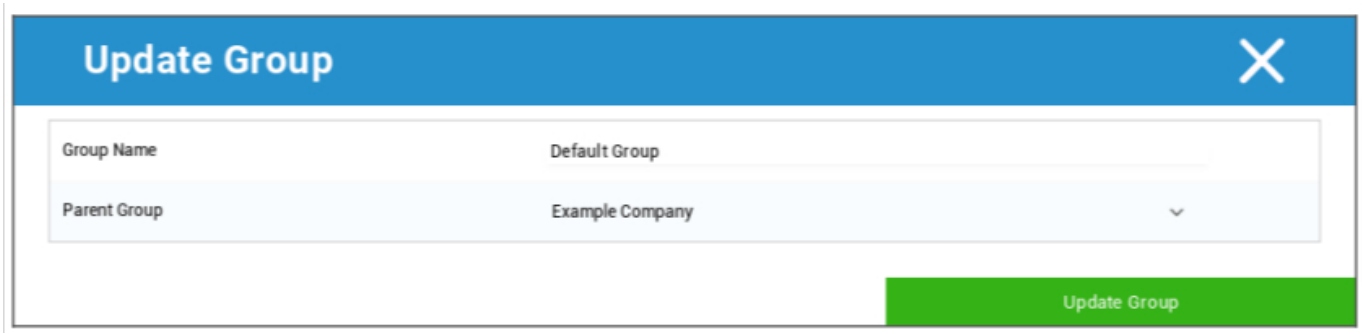
Alt Grup Oluşturma	İlgili (alt) grup için alt grup oluşturun
Seçili Grubu Düzenle	Seçili grubu düzenle
Seçili Grubu Sil	Seçili grubu sil
Toplu kayıt	Seçilen profil için aynı anda birçok cihazı / kullanıcıyı kaydetme
Toplu Görevlendirme	O anda seçili olan gruba profil atama
Alt Grup Oluşturma	İlgili (alt) grup için alt grup oluşturun
Kullanıcı Oluşturma	İlgili (alt) grup için bir kullanıcı oluşturun

Alt Grup Oluşturma

"Alt Grup Oluştur" ile ek bir alt grup oluşturabilirsiniz.

Alt grubun hangi grup altında atanacağını belirleyebilirsiniz (varsayılan olarak, alt grup o anda seçili olan gruba atanır).

Seçili Grubu Düzenle



Burada profili düzenleyebilirsiniz - burada aşağıdaki ayarlar mümkündür:

- Grup adı değiştirilebilir
- Ebeveyn grubu değiştirilebilir

Seçili Grubu Sil

"Seçili Grubu Sil" altında, ilgili gruptaki tüm kullanıcılar ve cihazlar sizin için listelenir. Burada, bunları silme seçeneğiniz vardır.

Bir kullanıcı için aşağıdaki silme komutlarını gerçekleştirebilirsiniz:

Kullanıcı Sil	Kullanıcı silindi
Kullanıcıyı Gruba Taşı:	Kullanıcıyı başka bir gruba taşıyabilirsiniz (aşağıdaki sütun, örn. "Admins)

Bir cihaz için aşağıdaki silme komutlarını uygulayabilirsiniz:

Silme ve Silme	Cihazı silme ve silme
Sistemden Sil	Cihazı yalnızca AppTec'ten kaldırın

Referans: Toplu Kayıt

Referans: Toplu Atama

Kullanıcı Oluşturma

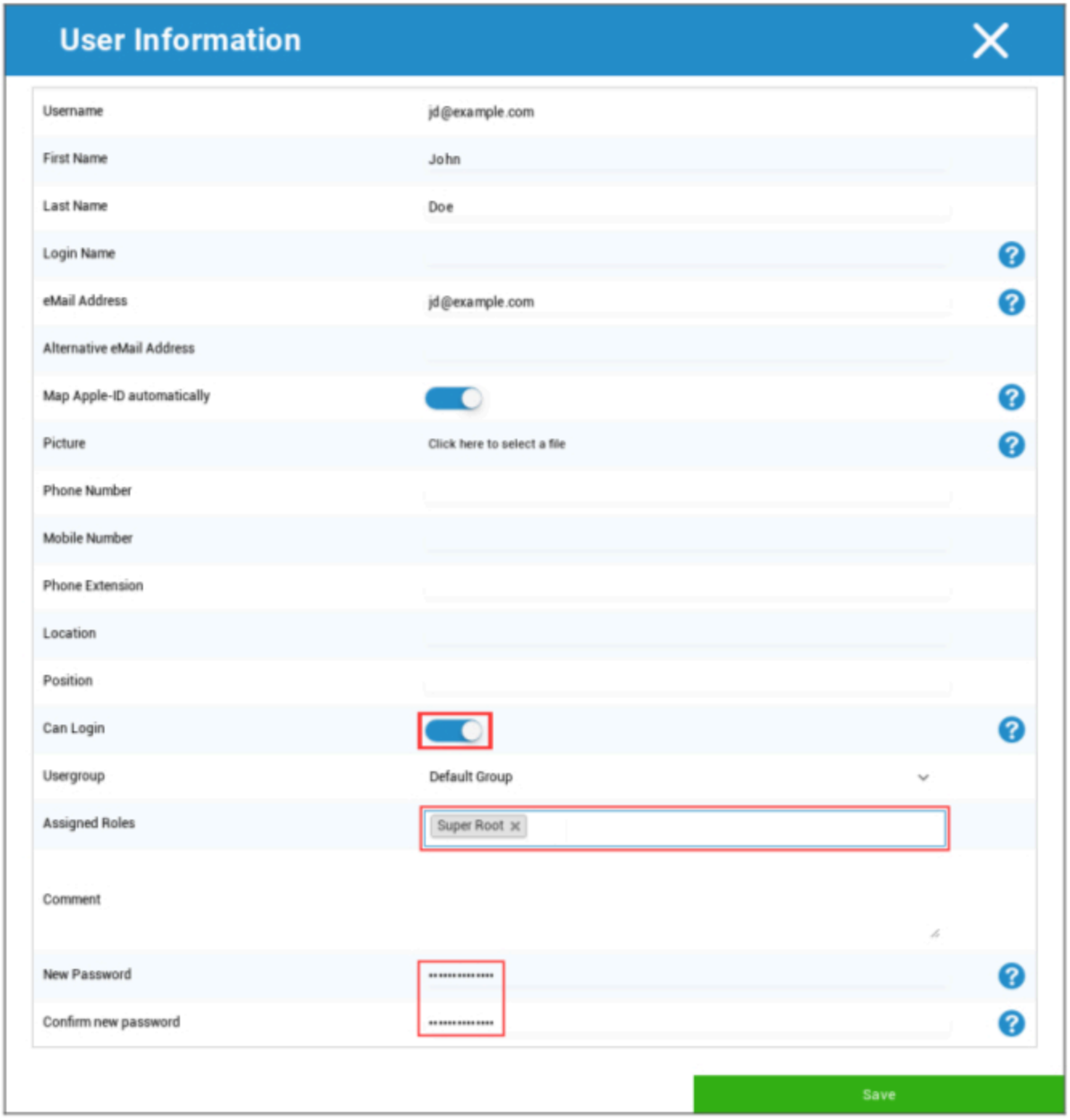
"Kullanıcı Oluştur" ile yeni bir kullanıcı ekleyebilirsiniz.

Yeni bir Yönetici-Kullanıcı oluşturun

Bir Kullanıcıyı Yönetici-Kullanıcı olarak ayarlayabilirsiniz. Bunu yapmak ona konsolda oturum açma ve ayrıca kullanıcıları/grupları/cihazları değiştirme izinlerini verecektir.

Normal bir Kullanıcı oluşturun veya mevcut bir Kullanıcıyı kullanın. Yönetici izinleri vermek istediğiniz Kullanıcıyı seçin, tekerleğe tıklayın ve "Kullanıcıyı Düzenle "yi seçin:

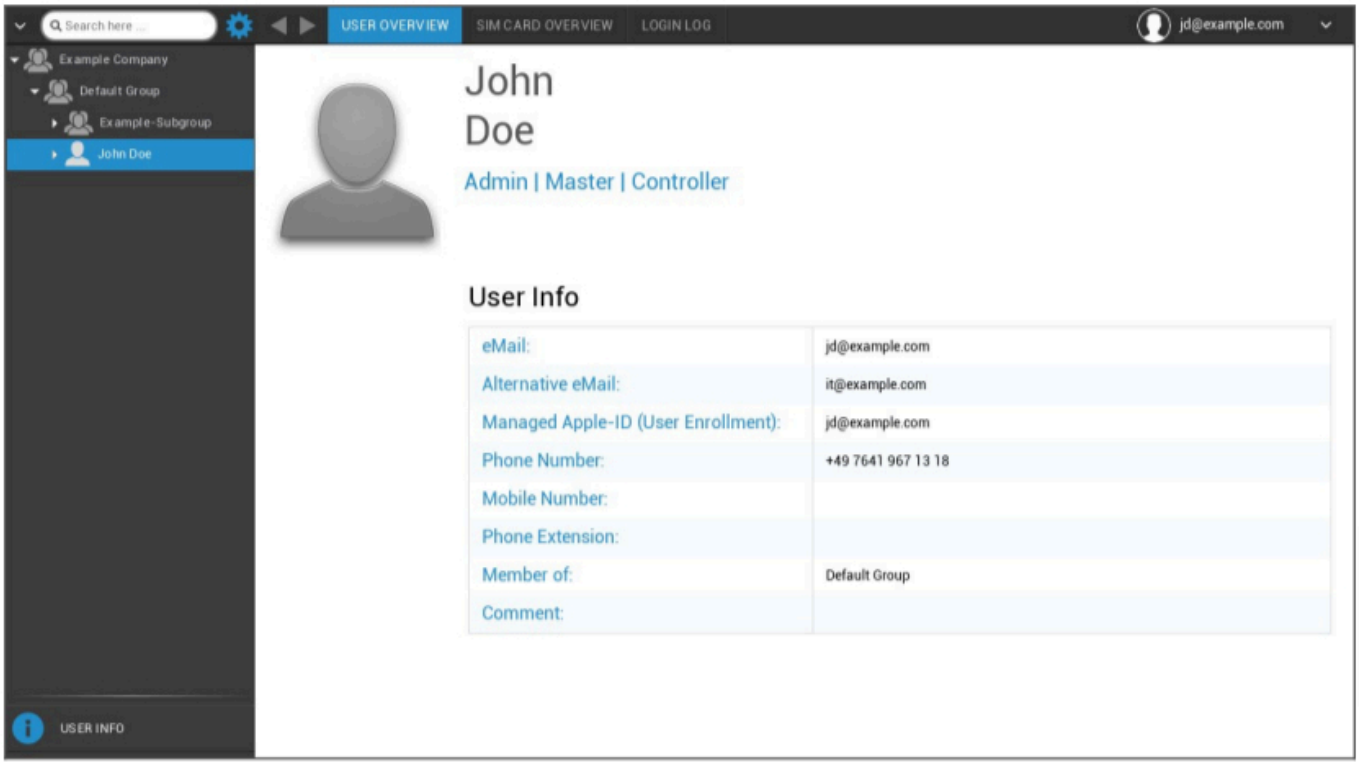
"Giriş Yapabilir" anahtarını etkinleştirin, kullanıcıya "Super-Root" rolünü atayın ve bir parola belirleyin.



Bunu kaydedin ve kullanıcı artık kullanıcı adı ve şifre ile giriş yapabilir.

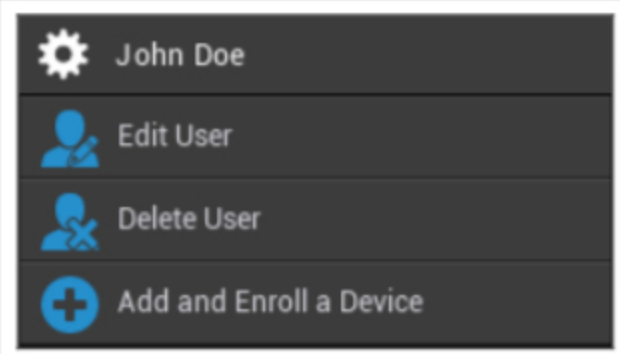
Mobil Yönetimde Kullanıcı Yönetimi

Belirli bir kullanıcıyı seçtiğinizde, aşağıdaki genel bakışı göreceksiniz:



Daha önce "Kullanıcı Oluştur" bölümünde girdiğiniz tüm bilgilere genel bir bakış alacaksınız.

Üstte takılı olan dişli ile aşağıdaki konfigürasyonları gerçekleştirebilirsiniz:



Kullanıcı Adı	Seçilen Kullanıcının Kullanıcı Adı
Kullanıcı Düzenle	Kullanıcı bilgilerini düzenleme
Kullanıcı sil	Kullanıcı sil • Sistemden Sil = Cihaz AppTec'ten kaldırılacaktır

	• Wipe & Delete = Cihaz fabrika ayarlarına geri yüklenecek ve AppTec'ten kaldırılacaktır
Cihaz ekleme ve kaydetme	Seçilen kullanıcı için bir cihaz kaydetme

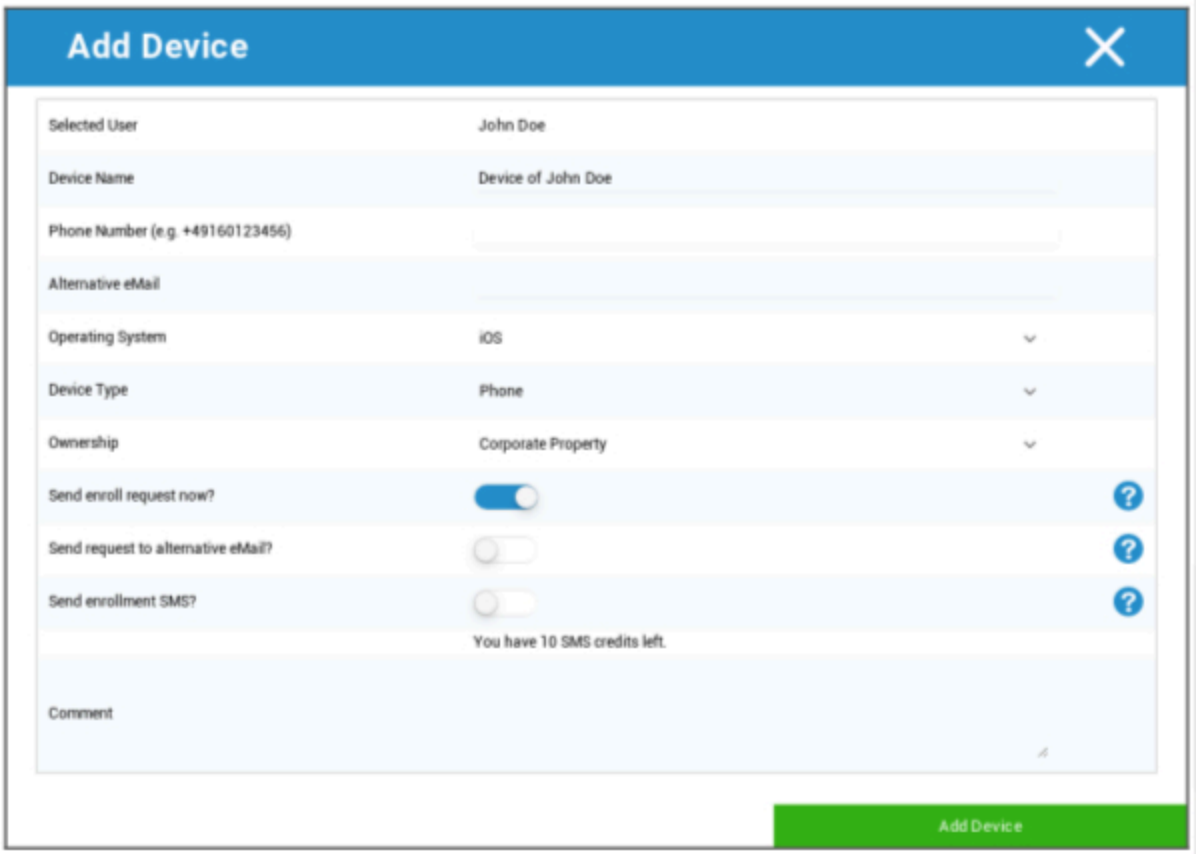
Yönetim erişiminin hiyerarşi yapısında yerel bir kullanıcı hesabı olarak da dosyalanabileceğini lütfen unutmayın. Ek bir hizmetli oluşturulmadan bu silinmemelidir!

Cihaz ekleme ve kaydetme

Burada seçilen kullanım için bir cihaz seçebilirsiniz.

Alternatif olarak cihazları doğrudan bir gruba kaydedebilirsiniz. Bunu yapmak için gruba tıklayın, tekerleğe tıklayın ve "Cihaz ekle ve kaydet "i seçin.

Aşağıdaki genel görünümü görmelisiniz:



Ne tür bir cihaz kaydetmek istediğinize bağlı olarak, aşağıdaki yapılandırmaları gerçekleştirmeniz gerekir:

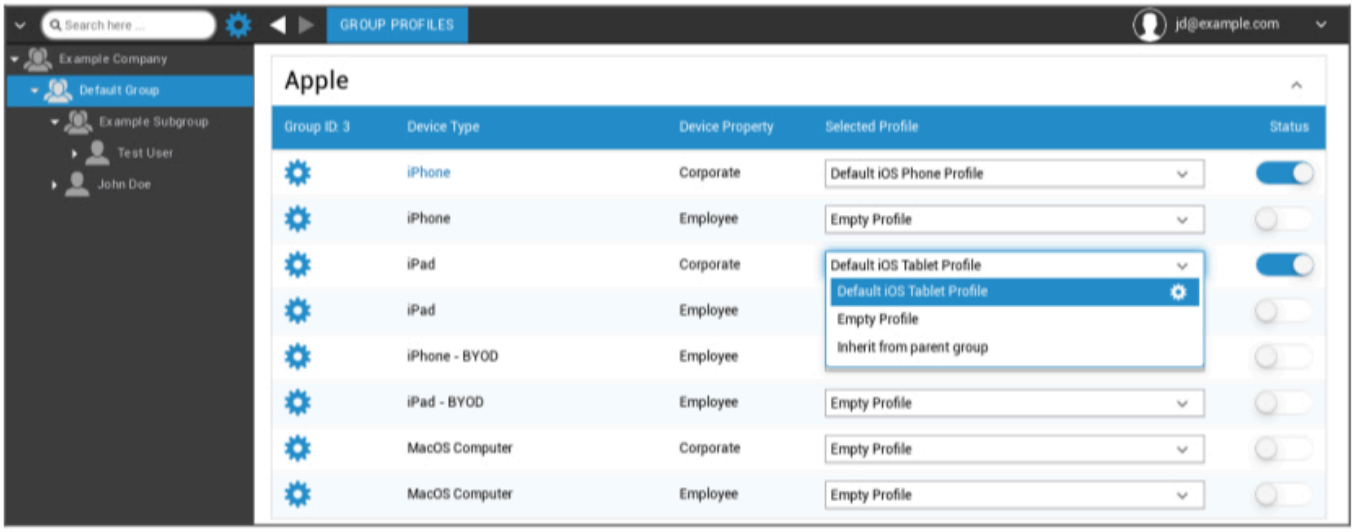
Seçilmiş Kullanıcı	Seçilen kullanıcı (otomatik olarak doldurulacaktır)
Cihaz Adı	Otomatik olarak doldurulacaktır ("kullanıcının adı" için cihaz) - ancak değiştirilebilir
Telefon Numarası	Telefon numarası, otomatik olarak doldurulacaktır (kullanıcı tarafından sağlandığı sürece) - ancak burada eklenebilir veya değiştirilebilir
Alternatif e-Posta	Alternatif e-posta, otomatik olarak doldurulacaktır (kullanıcı tarafından sağlandığı sürece) - ancak burada eklenebilir veya değiştirilebilir
Cihaz Sahibi	Kurumsal Mülk = kurumsal cihaz Çalışan Mülkü = BYOD cihazı
İşletim Sistemini Seçin	Burada, aşağıdaki işletim sistemleri arasından seçim yapabilirsiniz: • iOS • iOS BYOD (Kullanıcı Kaydı) • MacOS • Android Kurumsal • Android • Windows Mobile • Windows 10
Kayıt talebi gönderelim mi?	E-posta hemen ana e-posta adresine gönderilir ve kullanıcıdan cihazını bağlaması istenir
Alternatif e-Posta'ya talep gönderin?	E-postayı ek olarak veya yalnızca ("Kayıt talebi gönderilsin mi?" seçeneğinin devre dışı bırakılması durumunda) alternatif e-posta adresine gönderin ("normal" kayıt talebi e-postasından farklı bir e-posta)
Kayıt SMS'i gönderelim mi?	SMS yoluyla bir kayıt talebi gönderin ("Telefon Numarası" girilmelidir)

Kayıt Talebi gönderildikten sonra, cihaz hemen görüntülenecektir (kırmızı işaretli).

Cihaz başarıyla bağlanır bağlanmaz, kısa bir süre sonra cihaz yeşil renkle işaretlenir ve böylece kısıtlamalar, uygulamalar vb. almaya hazır hale gelir.

Mobil Yönetimde Profil Yönetimi

Bir gruba tıkladıktan sonra, yapılandırılacak tüm cihaz platformlarının ve sırasıyla atanmış profillerin genel bir görünümünü alacaksınız.



	Seçilen profil için yapılandırmayı gerçekleştirin
Cihaz Tipi	Cihaz tipi ve/veya modeli
Cihaz Özelliği	Cihazın sahibi (Kurumsal = kurumsal mülk, Çalışan = özel çalışan cihazı)
Seçilmiş Profil	Seçilen profil (dişli, profilin yapılandırma diyaloğunu açar)
Durum	Açık/Kapalı (profil etkinleştirilir/devre dışı bırakılır)

Vitesi seçtiğinizde, aşağıdaki seçenekleri alacaksınız:

Bir profil oluşturun

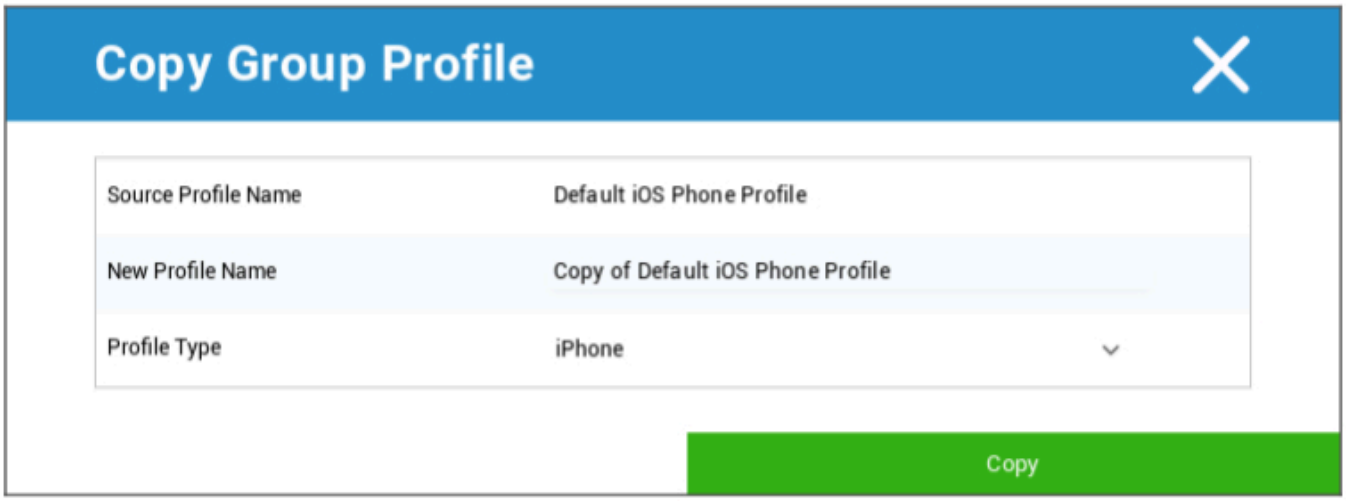
Her giriş ve/veya platform için yeni bir profil oluşturabilir ve yapılandırabilirsiniz. Bu alt noktaya tıkladıktan sonra profil hemen oluşturulacak ve iOS, Android ve Windows Phone yapılandırmasına hemen başlayabilirsiniz.

Profil Düzenle

"Profili Düzenle "ye tıkladıktan sonra, ilgili profil için yapılandırmaları ayarlayabileceğiniz yapılandırma ekranına ulaşacaksınız.

Profil Kopyala

"Profili Kopyala" fonksiyonu yardımıyla, halihazırda var olan bir profilden kurulumları/konfigürasyonları kopyalayabilir ve bunları yeni bir profile ekleyebilirsiniz.

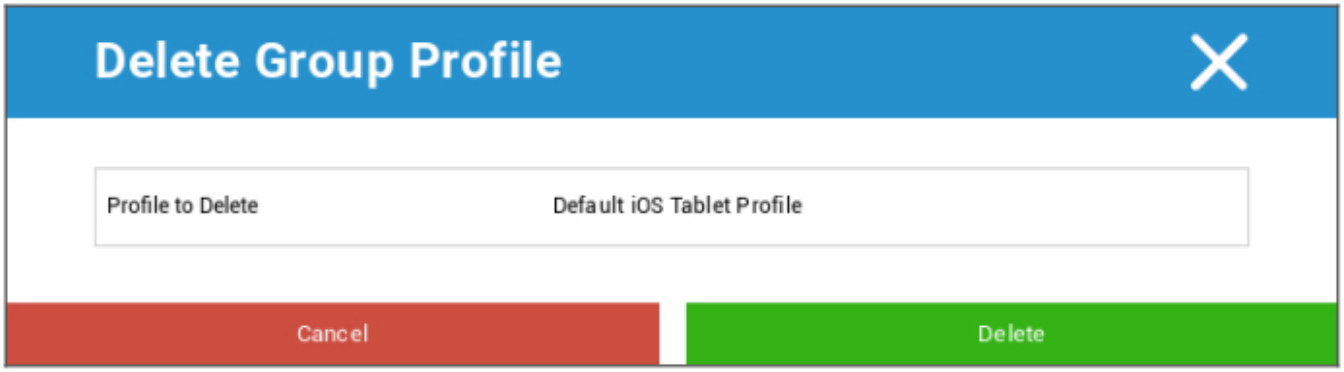


Kaynak Profil Adı	Kopyalanacak profilin adı
Yeni Profil Adı	Yeni profilin adı
Profil Tipi	Profil türü (Telefon/Tablet)

"Kopyala" düğmesine tıkladığınızda profil oluşturulacak ve artık gruba atanabilecektir

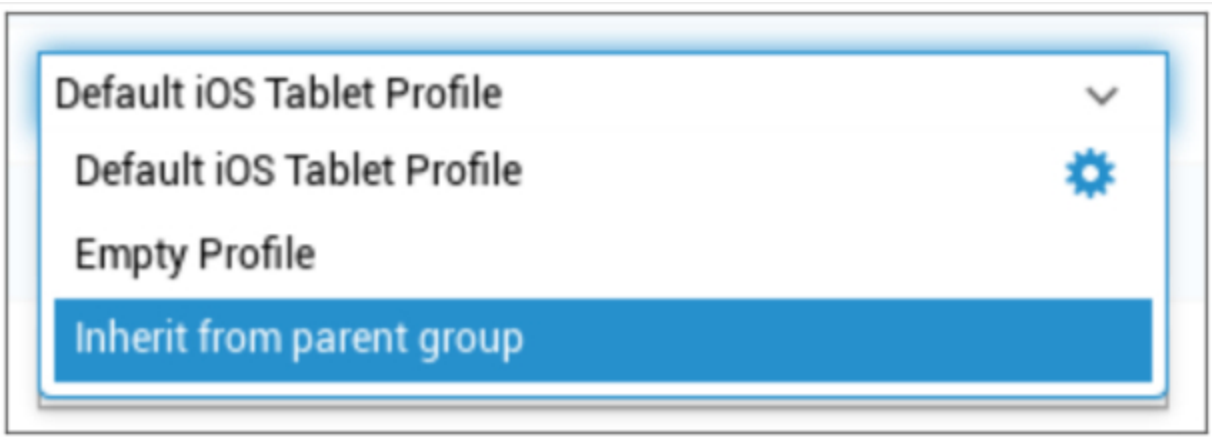
Profil Sil

Burada bir profili kalıcı olarak silebilirsiniz. Silme işlemi ve ardından profil için "Şimdi Ata" işlemi sırasında, yapılandırmanın etkilenen grubun ilgili cihazlarında kaybolacağını ve kurtarılamayacağını lütfen unutmayın!


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

Profillerin Devralınması

Profillerin seçimi sırasında "Ana gruptan devral" seçeneği mevcuttur.



Profil etkinleştirildiğinde, sırasıyla seçilen cihaz (ve ilgili cihaz tipi) için üst grubun profili kullanılacaktır. Bu profilde yapılacak değişikliklerin çok sayıda grubu etkileyebileceğini de lütfen unutmayın.

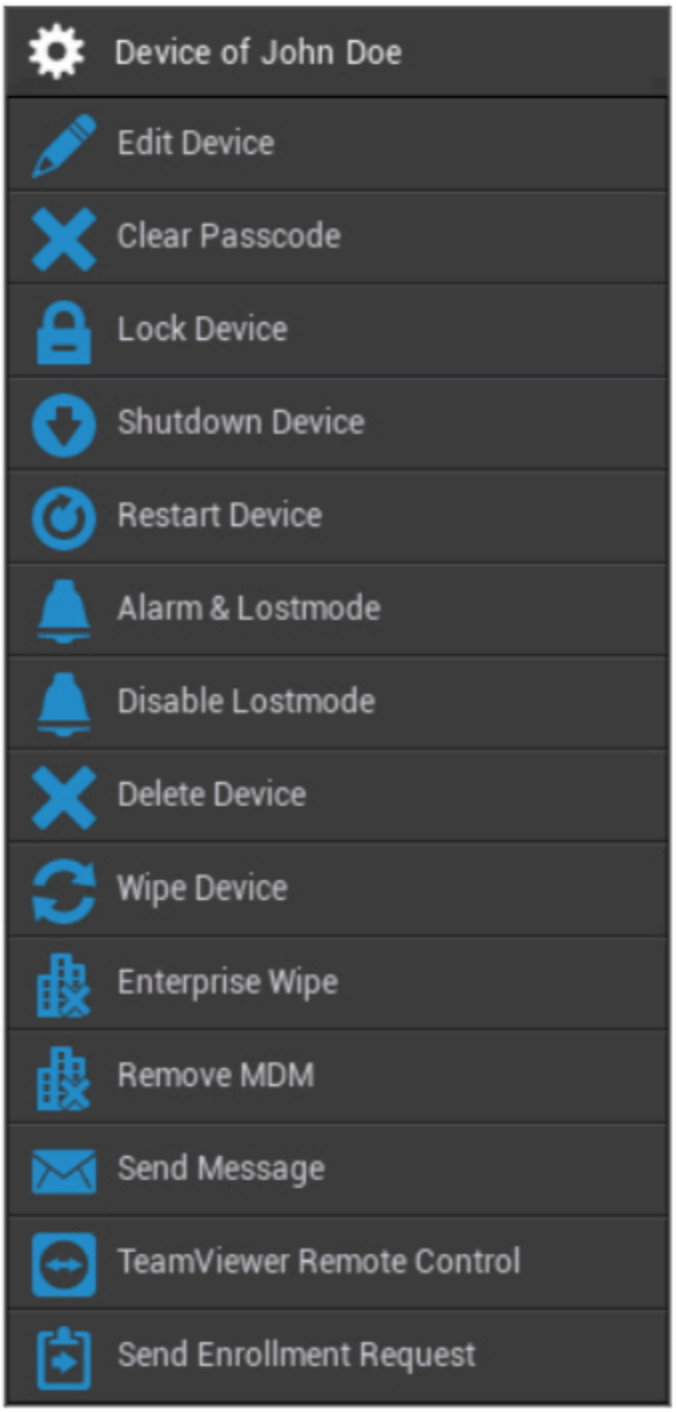
Bu yapılandırma, yeni bir alt grup oluşturulduğunda varsayılan değer olarak ayarlanır.

Boş bir profile karşılık gelen "Boş Profil" yapılandırması da mevcuttur, bu da sonuçta son kullanıcı cihazında yeni yapılandırmaların gerçekleştirilmeyeceği anlamına gelir.

Mobil Yönetimde Cihaz Yönetimi

Bir cihaz seçtiğinizde, "dişli" aracılığıyla çeşitli görevleri gerçekleştirebilirsiniz. Bunlar işletim sistemi platformlarına (iOS, Android Enterprise, Android, Windows Mobile, Windows 10) bağlı olarak farklıdır.

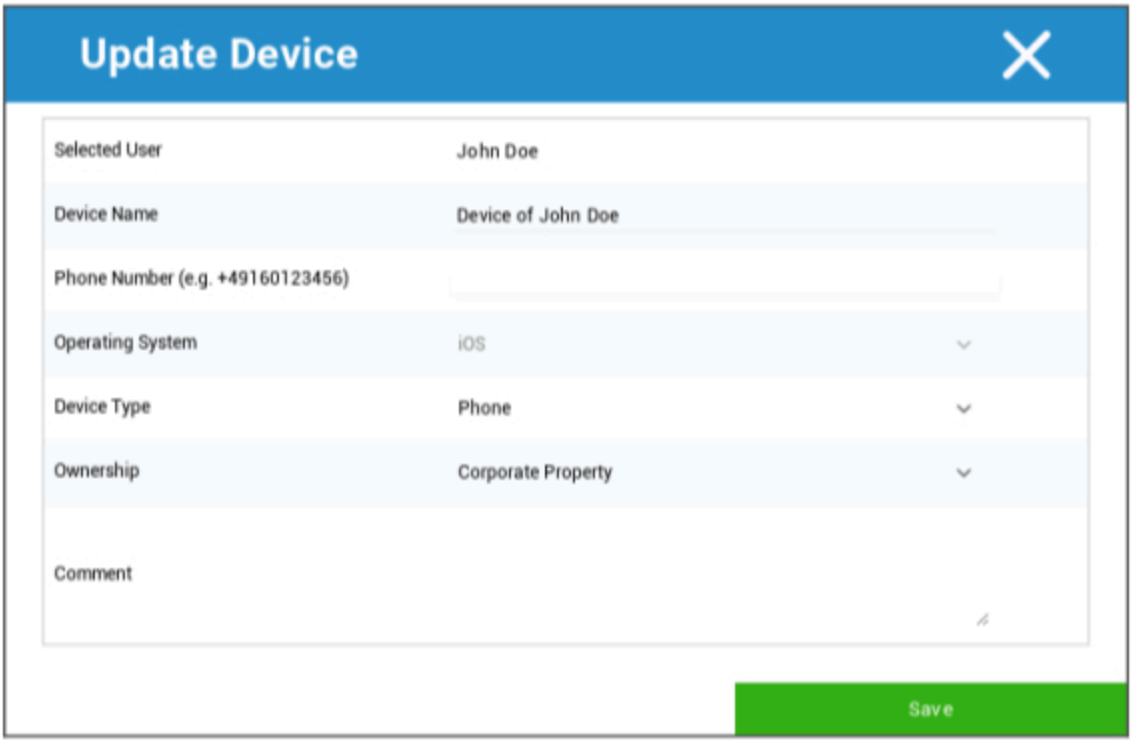
IOS



Cihazı Düzenle	Cihaz düzenleme
Parolayı Temizle	Cihaz şifresi silinir
Kilit Cihazı	Cihazı kilitle (kilit ekranı)
Kapatma Cihazı	Kapatma cihazı

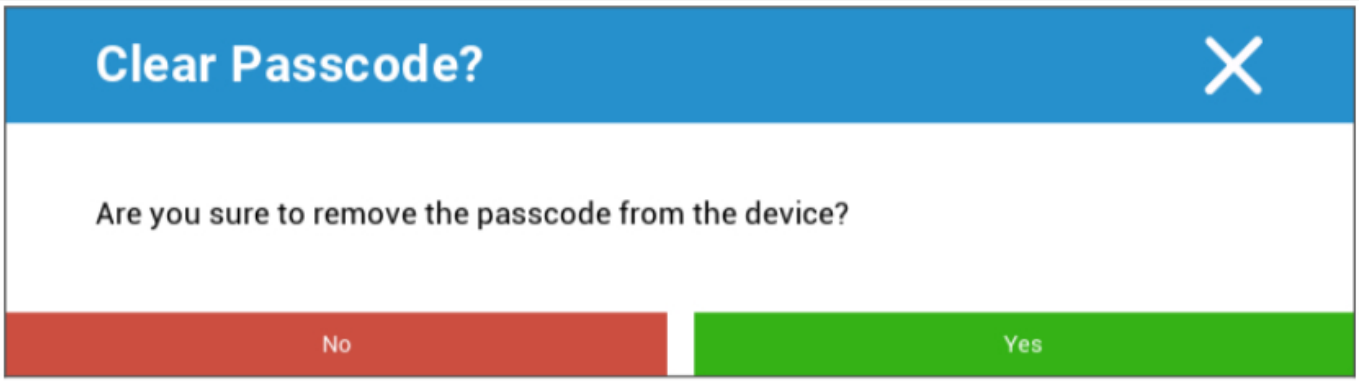
Cihazı Yeniden Başlat	Cihazı yeniden başlatın
Alarm ve Kayıp Modu	Alarmı Başlat & Kayıp Modu
Lostmode'u devre dışı bırak	Lostmode'u devre dışı bırak
Cihazı Sil	Cihazı AppTec'ten kaldırma
Silme Cihazı	Cihazı fabrika ayarlarına geri yükleme
Kurumsal Silme	AppTec360 tarafından sağlanan bilgiler, uygulamalar ve profiller silinir (cihaz MDM'den ayrılır)
MDM'yi kaldırın	
Mesaj Gönder	Cihaza Anlık Bildirimler Gönderme Mesaj AppTec360 Uygulamasında görüntülenecektir (Mesaj Sekmesi)
TeamViewer Uzaktan Kumanda	TeamViewer kullanarak Uzaktan Kontrol Oturumu başlatma
Kayıt Talebi Gönder	Gönder (tekrarlanan) Kayıt talebi

Cihazı Düzenle



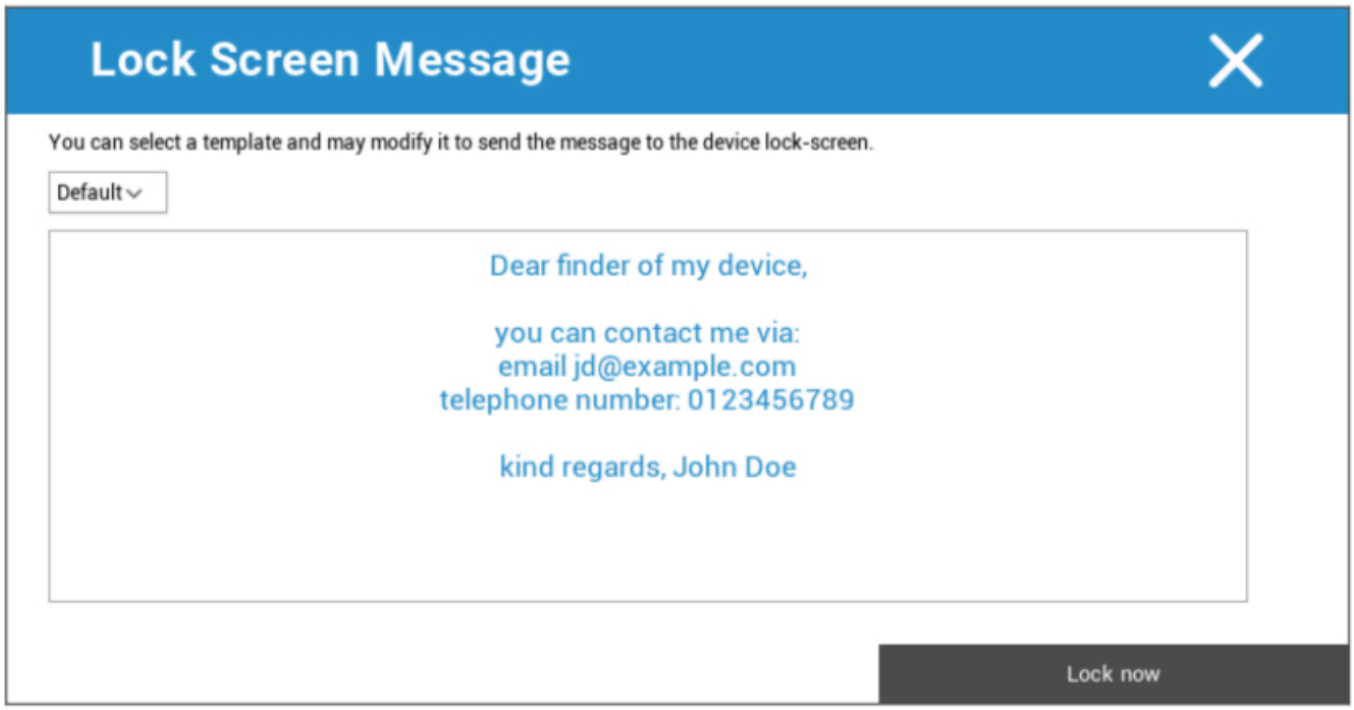
Burada cihazla ilgili çeşitli bilgileri güncelleyebilirsiniz.

Parolayı Temizle



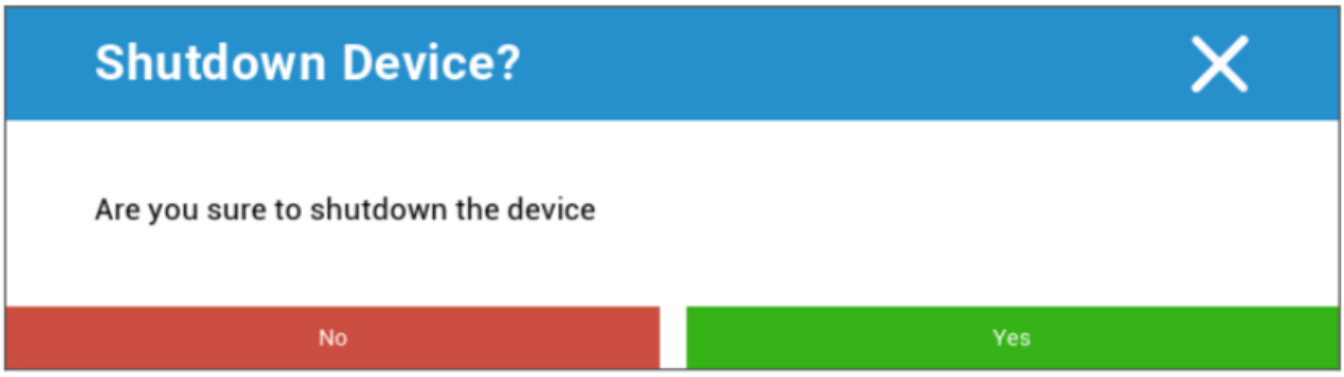
"Parolayı Temizle" altında parolayı cihazdan uzaktan kaldırabilirsiniz. Daha sonra, kullanıcıdan yeni bir şifre belirlemesi istenecektir (Şifre yönergelerine bağlı olarak).

Kilit Cihazı



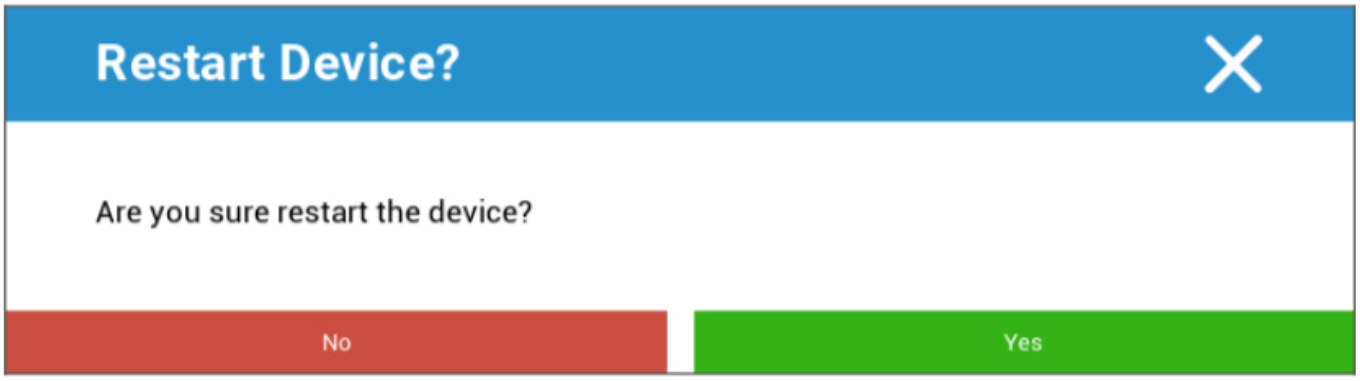
Burada son kullanıcı cihazına bir kilit komutu gönderilir (kilit ekranı).

Kapatma Cihazı



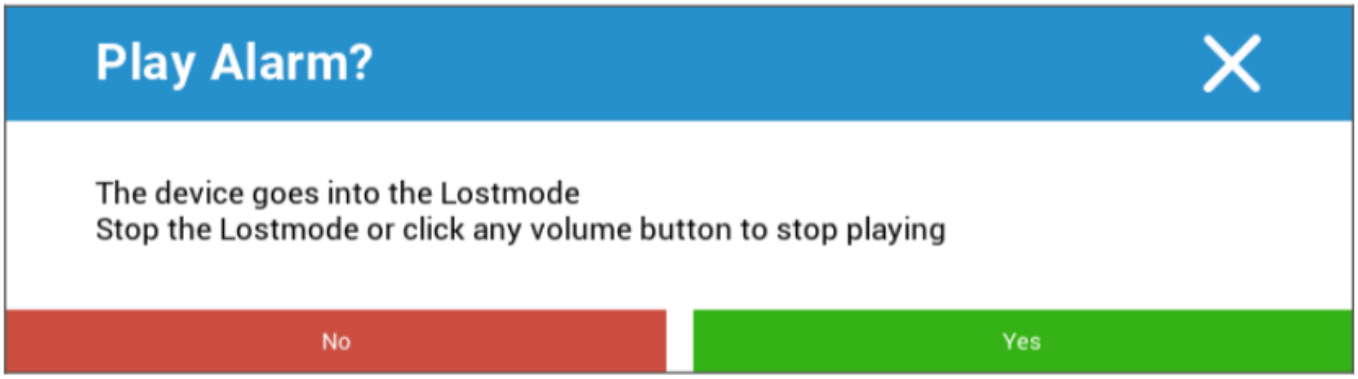
Burada son kullanıcı cihazına bir kapatma komutu gönderilir.

Cihazı Yeniden Başlat

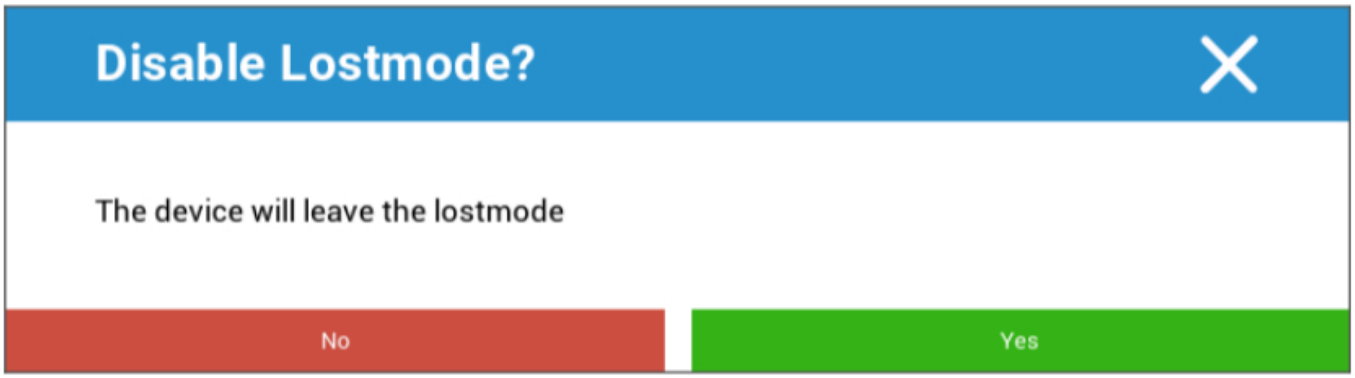


Burada son kullanıcı cihazına bir yeniden başlatma komutu gönderilir.

Alarm ve Kayıp Modu | Kayıp Modunu Devre Dışı Bırak



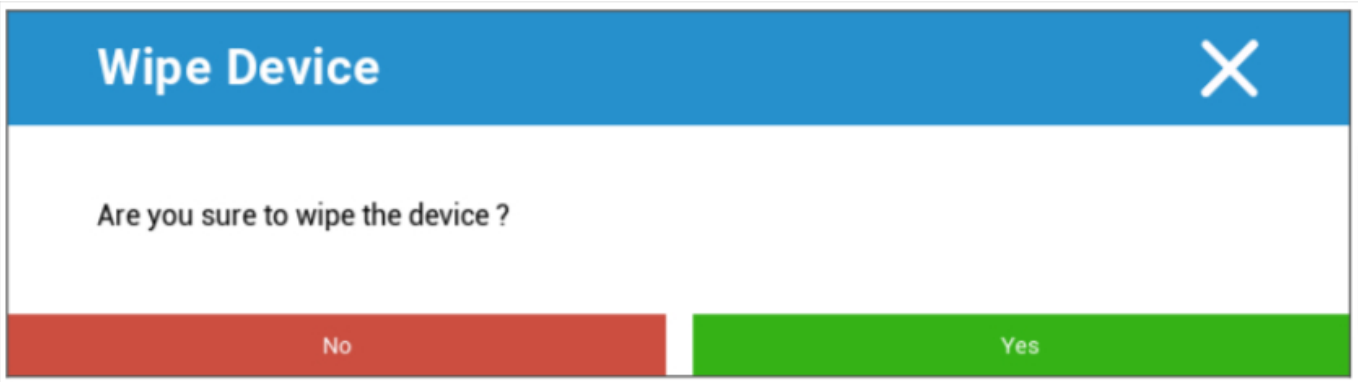
Burada cihaz, cihazı sürekli olarak bir Alarm sesi çalacak şekilde ayarlayan Lostmode'a ayarlanabilir. Lostmode, cihazın herhangi bir ses düğmesine basılarak veya uzaktan "Lostmode'u Devre Dışı Bırak" seçeneğine tıklanarak durdurulabilir:



Cihazı Sil

Burada silme komutu gerçekleştirilebilir. Cihazın yalnızca AppTec360'tan kaldırılıp kaldırılmayacağına ("Sistemden Sil") veya cihazın AppTec360'tan kaldırılıp kaldırılmayacağına ve ayrıca fabrika ayarlarına geri yüklenip yüklenmeyeceğine ("Sil ve Sil) bir kez daha karar verebilirsiniz.

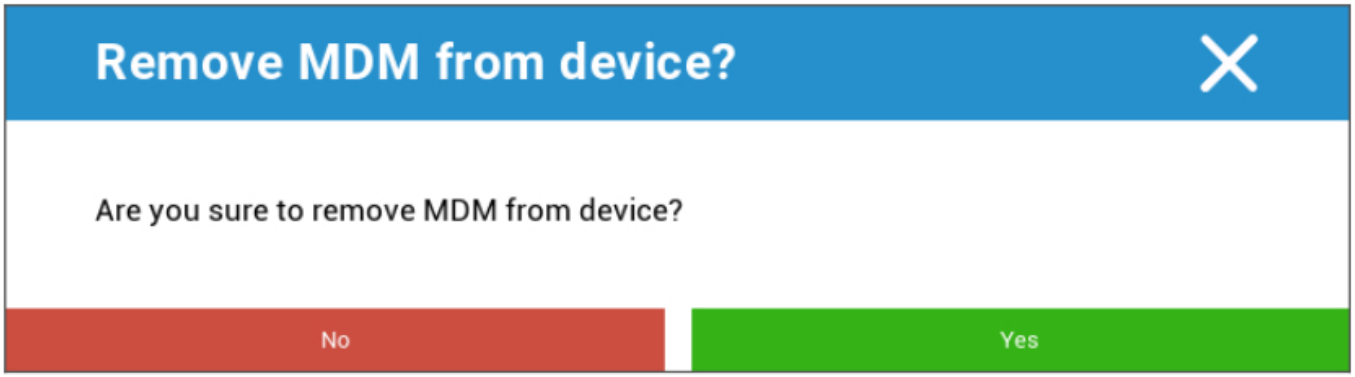
Silme Cihazı



"Cihazı Sil" altında cihazın tamamen silinmesini gerçekleştirebilirsiniz. Cihaz fabrika ayarlarına geri yüklenecektir.

Enterprise Wipe | MDM’yi Kaldır

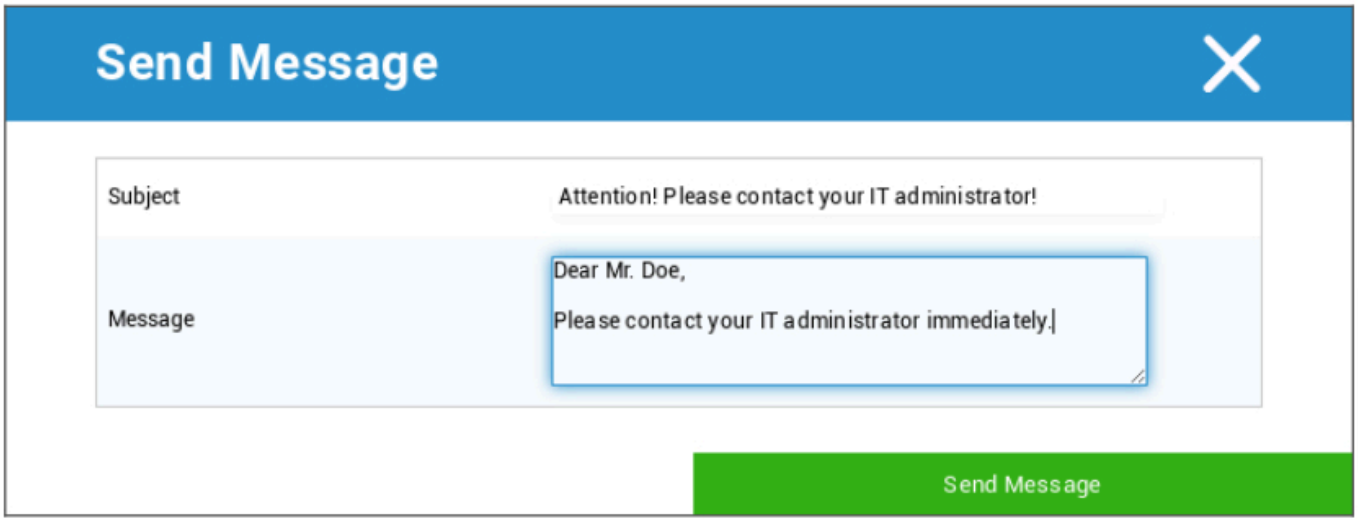
Yalnızca AppTec360 tarafından sağlanan bilgiler, uygulamalar ve profiller silinir. Bu şekilde, kurumsal veriler artık son kullanıcı cihazında bulunmayacaktır. Özel alan etkilenmez ve son kullanıcı cihazında kalmaya devam eder.



"MDM'yi Kaldır" ile son kullanıcı cihazındaki MDM profilini ve AppTec tarafından sağlanan diğer tüm öğeleri kaldırabilirsiniz.

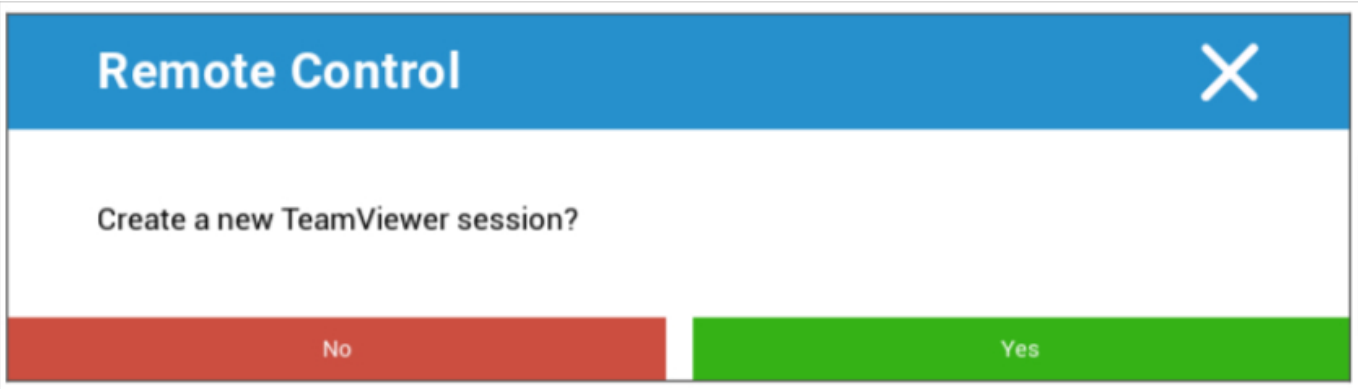
Bu komut "Enterprise Wipe" ile aynı eylemi gerçekleştirir.

Mesaj Gönder



Buradan ilgili cihaza bir Anlık Bildirim gönderebilirsiniz.

TeamViewer Uzaktan Kumanda



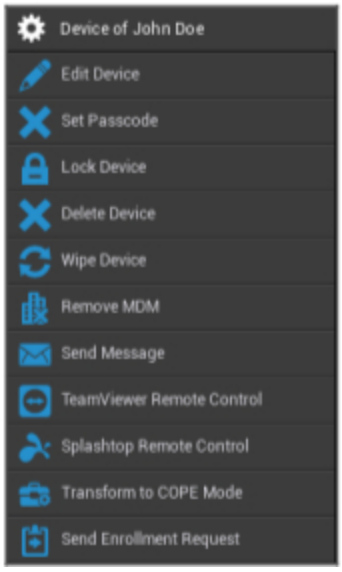
Burada bir Teamviewer Uzaktan Kumanda oturumu başlatılabilir.

Kayıt Talebi Gönder

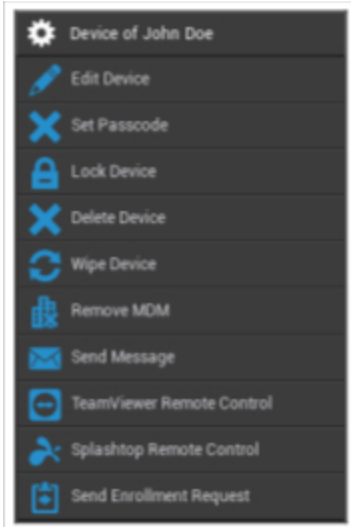
"Kayıt Talebi Gönder" ile ilgili kullanıcıya (tekrar) bir Kayıt Talebi gönderebilirsiniz.

Android

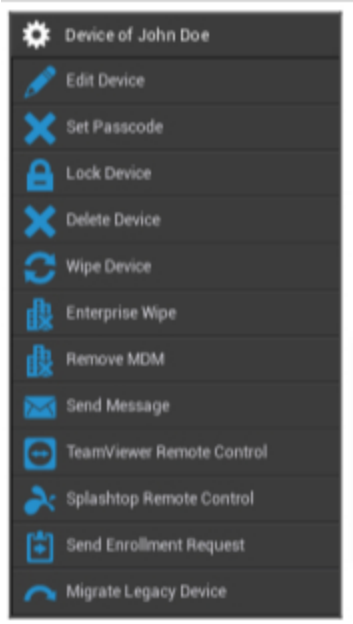
AE Tam Yönetilen Cihaz (İş Yönetilen)



AE Çalışma Profili (Konteyner)



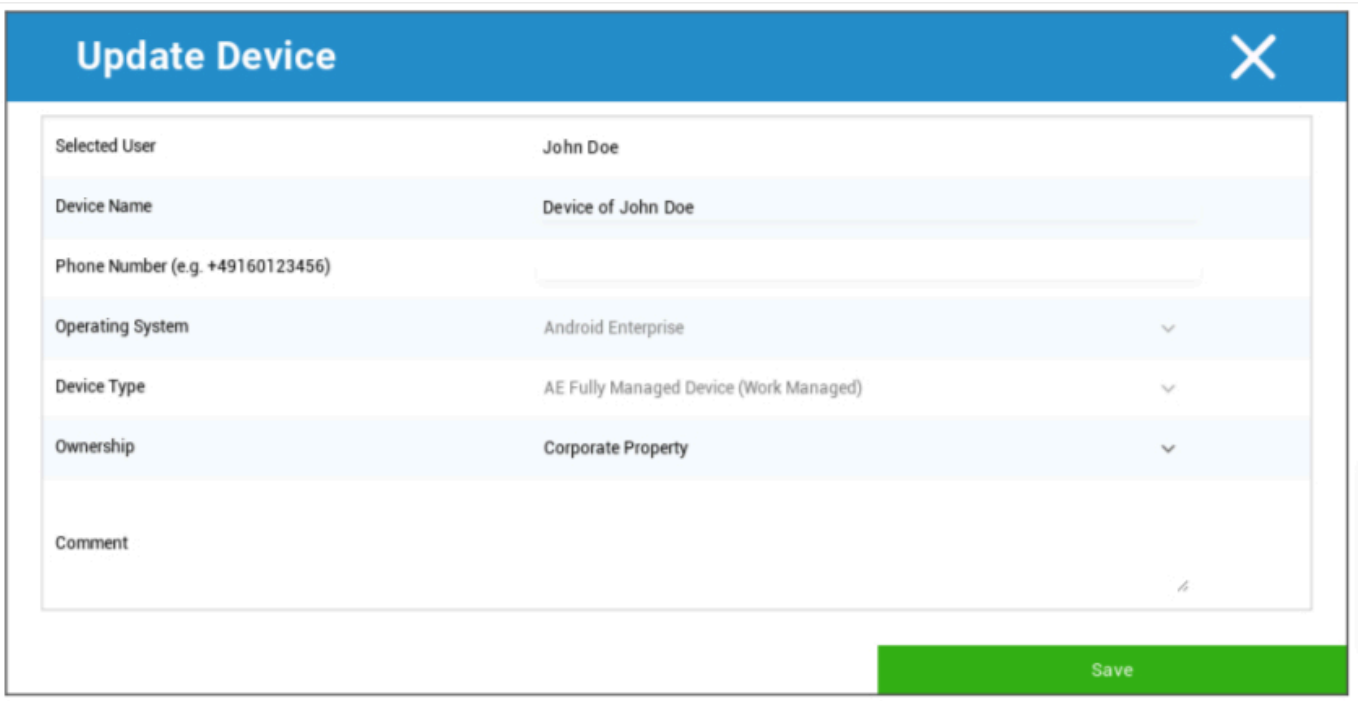
Android Telefon | Tablet



Cihazı Düzenle	Cihaz bilgilerini düzenleme
Parola Ayarla	Cihazın parolasını ayarlama
Kilit Cihazı	Cihazı kilitle (kilit ekranı)
Cihazı Sil	AppTec'ten cihaz silme
Silme Cihazı	Cihazı fabrika ayarlarına geri yükleme
Kurumsal Silme	AppTec360 tarafından sağlanan bilgiler, uygulamalar, profiller silinir (cihaz MDM'den ayrılır)
MDM'yi kaldırın	
Mesaj Gönder	Cihaza anlık bildirimler gönderme Mesaj AppTec360 Uygulamasında görüntülenecektir (Mesaj Sekmesi)
TeamViewer Uzaktan Kumanda	TeamViewer kullanarak bu cihaz için bir Uzaktan Kumanda oturumu başlatın
Splashtop Uzaktan Kumanda	Splashtop kullanarak bu cihaz için bir Uzaktan Kumanda oturumu başlatın
COPE Moduna Dönüştürme (yalnızca AE Tam Yönetilen Cihazda (İş Yönetilen))	Bu AE Tam Yönetilen (İş Yönetimli) Cihazda bir İş Profili Oluşturun
Kayıt Talebi Gönder	(Tekrarlanan) kayıt talebi gönderme
Eski Cihazı Taşıma (yalnızca Cihaz Sahibi Modu Sağlama kullanılarak kaydedildiğinde Android Telefon / Tablette)	Android Telefon / Tablet Profilini AE Tam Yönetilen Cihaz (İş Tarafından Yönetilen) Profiline Taşıma

Cihazı Düzenle

Burada çeşitli cihaz bilgilerini güncelleyebilirsiniz.



Seçilmiş Kullanıcı	Cihaz kullanıcısı
Cihaz Adı	Cihaz adı
Telefon Numarası	Cihaz telefon numarası
İşletim Sistemi	Android Kurumsal Android
Cihaz Tipi	Android Enterprise: • AE Tam Yönetilen Cihaz (İş Yönetilen) • AE Çalışma Profili Modu (yalnızca Konteyner) • AE Çalışma Profili ile Tam Yönetilen Cihaz (COPE) Android: • Telefon • Tablet
Sahiplik	Kurumsal = kurumsal mülk

	Çalışan = çalışan özelliği
Yorum	Cihaz için ek açıklamalar

Parolayı Temizle

Burada seçilen cihazdaki cihaz şifresini kaldırabilirsiniz. Android'de varsayılan olarak parola "123456 "ya ayarlanacaktır - bu daha sonra kullanıcı tarafından değiştirilebilir ve değiştirilmelidir.

Kilit Cihazı

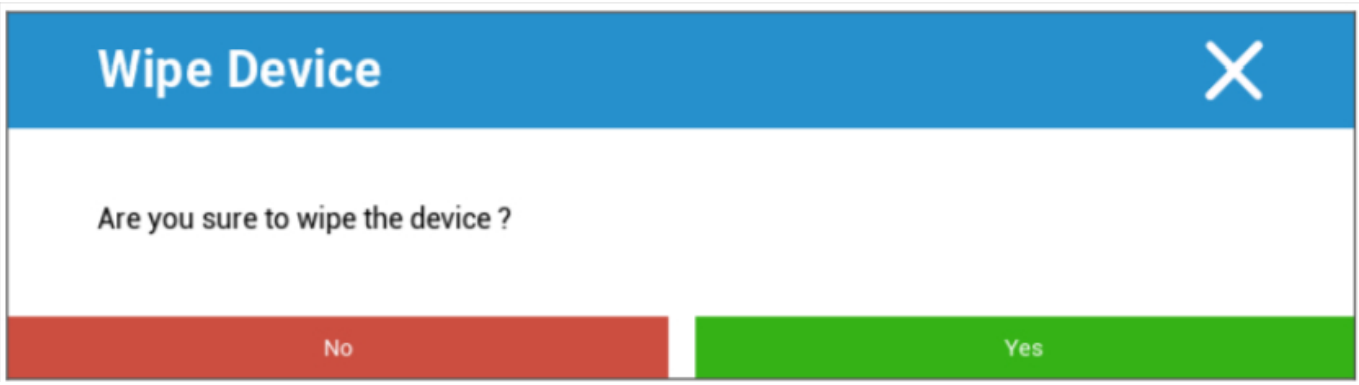
Burada cihaza bir cihaz kilitleme komutu gönderilecektir (kilit ekranı).

Cihazı Sil

Burada bir silme komutu gerçekleştirilebilir. Cihazın yalnızca AppTec360'tan kaldırılıp kaldırılmayacağına ("Sistemden Sil") veya cihazın AppTec360'tan kaldırılıp kaldırılmayacağına ve ek olarak fabrika ayarlarına geri yüklenip yüklenmeyeceğine ("Sil ve Sil) bir kez daha karar verebilirsiniz.

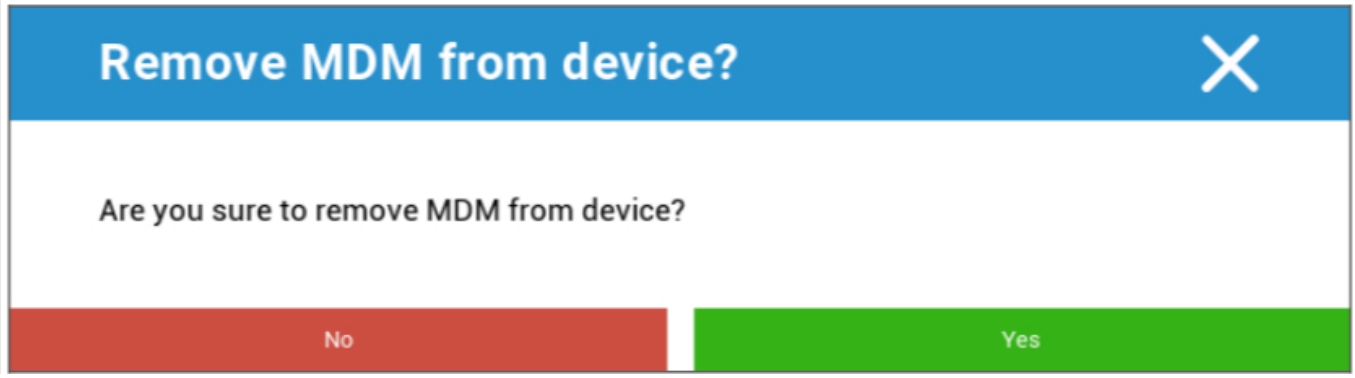
Silme Cihazı

"Cihazı Sil" altında cihazın tamamen silinmesini gerçekleştirebilirsiniz. Cihaz daha sonra fabrika ayarlarına geri döndürülecektir.



Ayrıca, cihaz bir SD kart içeriyorsa, SD kartı silebilirsiniz. Bunu, "SD Kartı da sil?" ayarını yaparak gerçekleştirebilirsiniz. " öğesini "Açık" olarak ayarlayın.

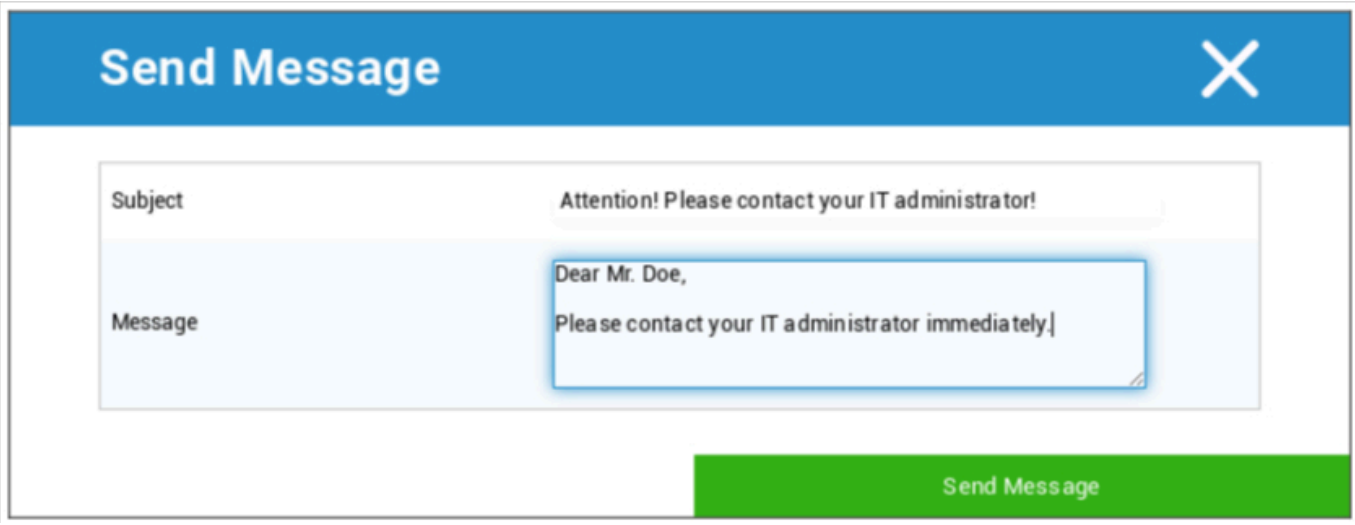
MDM’yi kaldırın



Bu, MDM'den bir ayrım oluşturmak için önerilen yöntemdir.

Yalnızca AppTec360 tarafından sağlanan bilgiler, uygulamalar ve profiller silinir, bu da tüm kurumsal verilerin artık son kullanıcı cihazında bulunmayacağı anlamına gelir. Ancak özel alan etkilenmez ve son kullanıcı cihazında kalmaya devam eder.

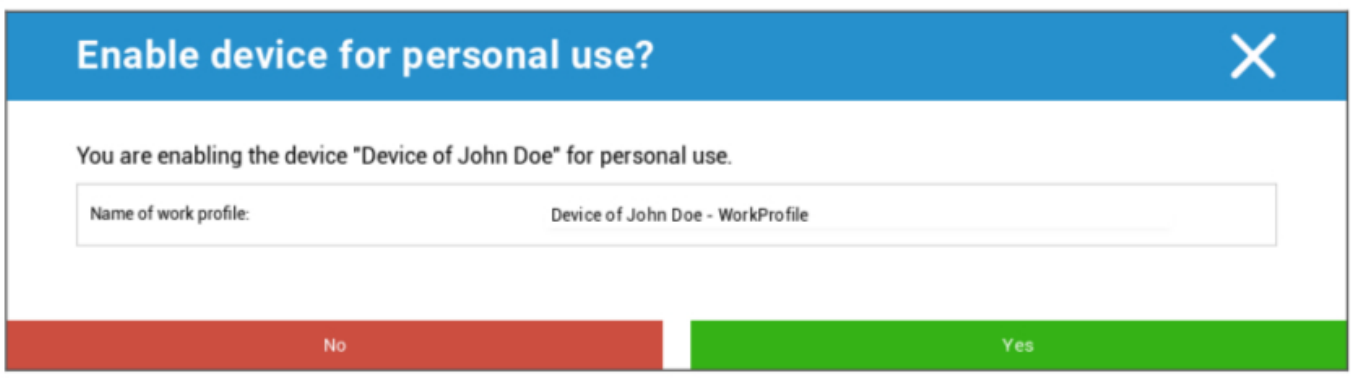
Mesaj Gönder



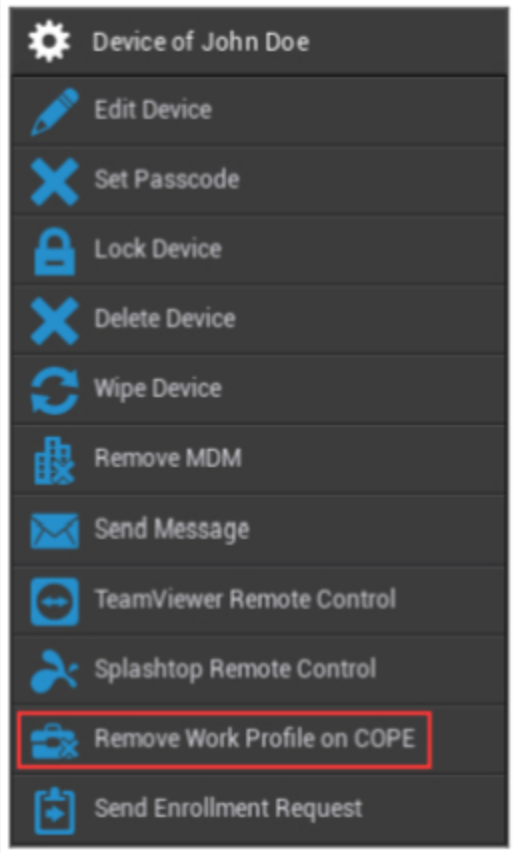
Buradan ilgili son kullanıcı cihazına bir Anlık Bildirim gönderebilirsiniz.

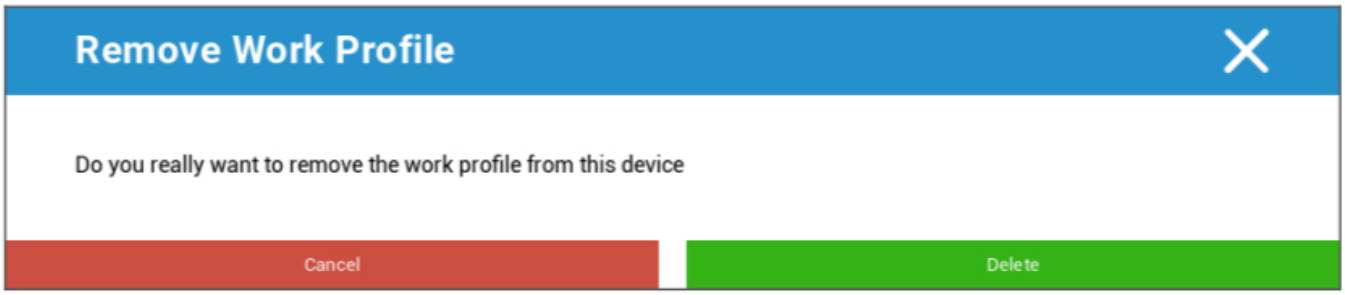
COPE Moduna Dönüştür

Bu AE Tam Yönetilen (İş Yönetimli) Cihazda bir İş Profili Oluşturun



Cihazı COPE Moduna dönüştürdükten sonra, **COPE**'de İş Profilini Kaldır dişli seçeneğine tıklayarak İş **Profilini** kaldırabilirsiniz:




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

Kayıt Talebi Gönder

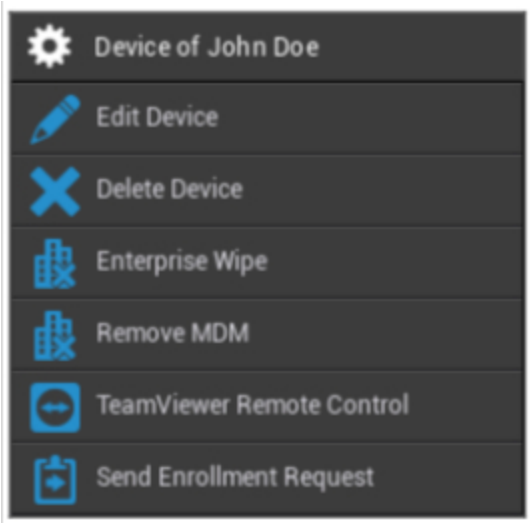
"Kayıt Talebi Gönder" ile ilgili kullanıcıya (tekrar) bir Kayıt Talebi gönderebilirsiniz.

Lütfen yalnızca en yeni Kayıt - Talebin geçerli olduğunu unutmayın.

Eski Cihazı Taşıma

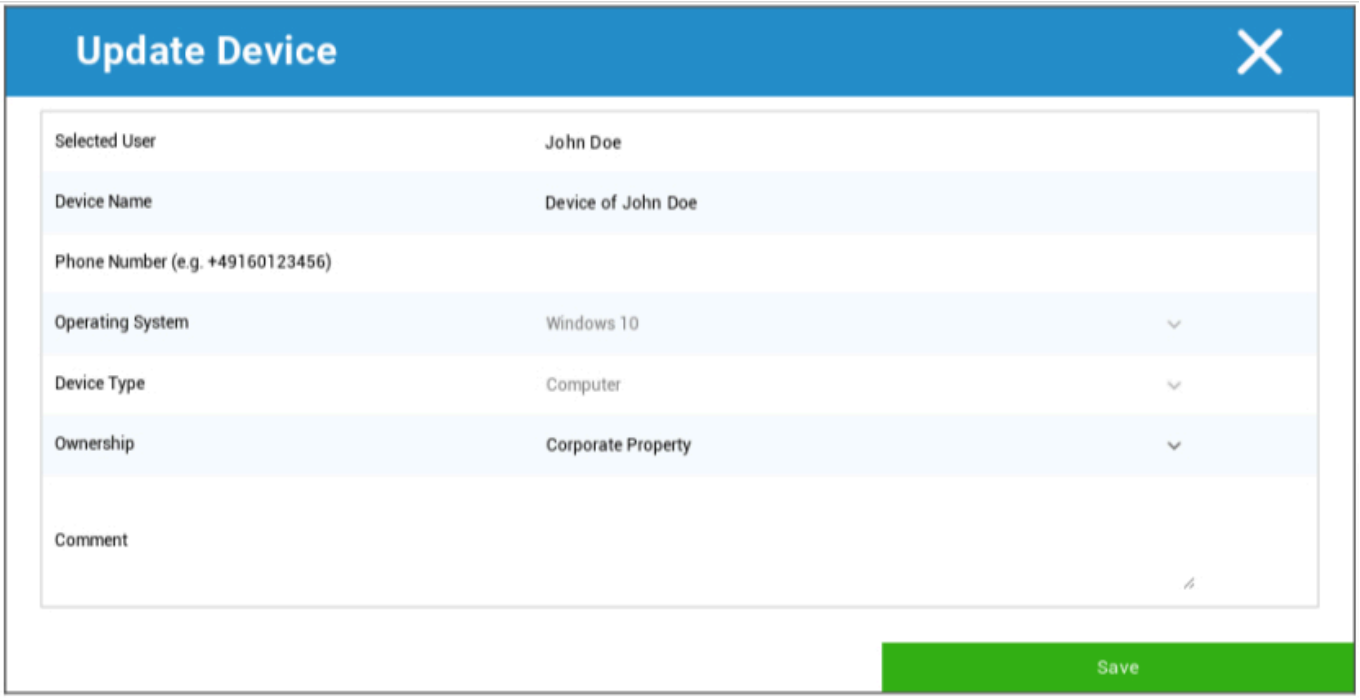
Android Telefon / Tablet Profilini AE Tam Yönetilen Cihaz (İş Tarafından Yönetilen) Profiline Taşıma

Pencereler



Cihaz Adı	Seçilen cihazın adı
Cihazı Düzenle	Cihaz düzenleme
Cihazı Sil	Cihazı AppTec'ten kaldırma
Kurumsal Silme	AppTec360 tarafından sağlanan bilgiler, uygulamalar ve profil silinir
MDM'yi kaldırın	
TeamViewer Uzaktan Kumanda	TeamViewer ile cihazı uzaktan kontrol etme
Kayıt Talebi Gönder	Kayıt isteği gönder (tekrar)

Cihazı Düzenle

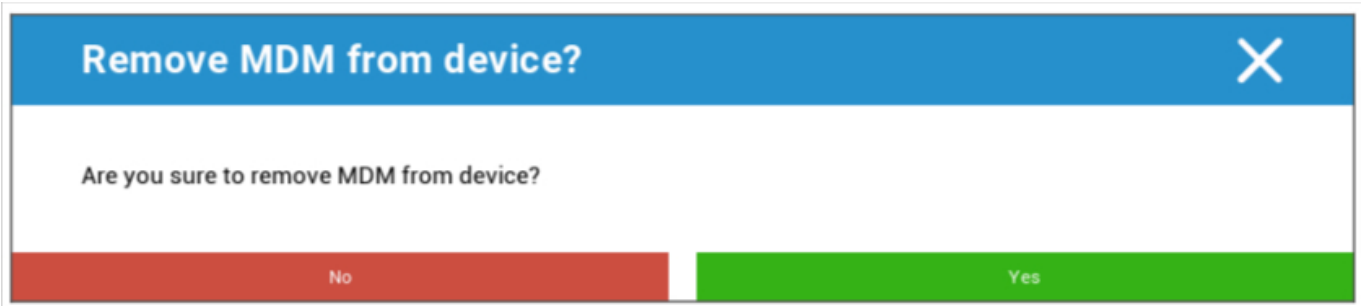


Burada cihazla ilgili çeşitli bilgileri güncelleyebilirsiniz.

Cihazı Sil

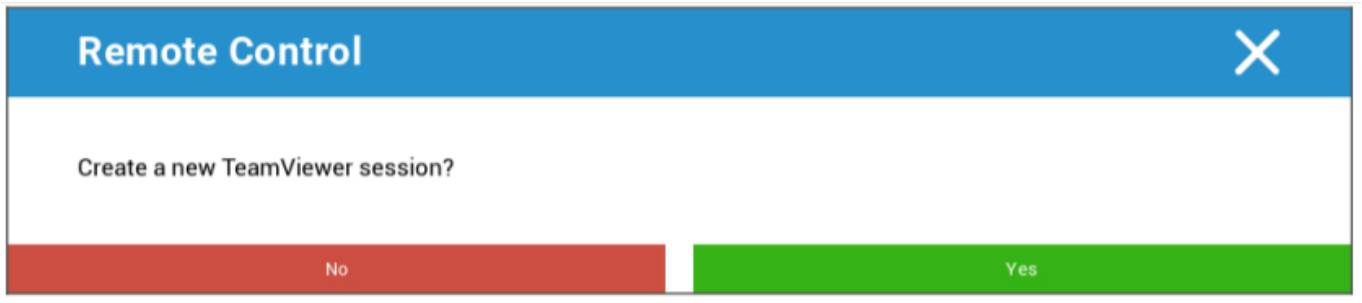
Burada sadece cihazı AppTec360'tan kaldıran silme komutu gerçekleştirilebilir.

Enterprise Wipe | MDM'yi Kaldır



Yalnızca AppTec360 tarafından sağlanan bilgiler, uygulamalar ve profiller silinir. Bu şekilde, kurumsal veriler artık son kullanıcı cihazında bulunmayacaktır. Özel alan etkilenmez ve son kullanıcı cihazında kalmaya devam eder.

TeamViewer Uzaktan Kumanda



Burada, bu cihaz için bir TeamViewer Uzaktan Kumanda oturumu başlatabilirsiniz.

Kayıt Talebi Gönder

"Kayıt Talebi Gönder" ile ilgili kullanıcıya (tekrar) bir Kayıt Talebi gönderebilirsiniz.

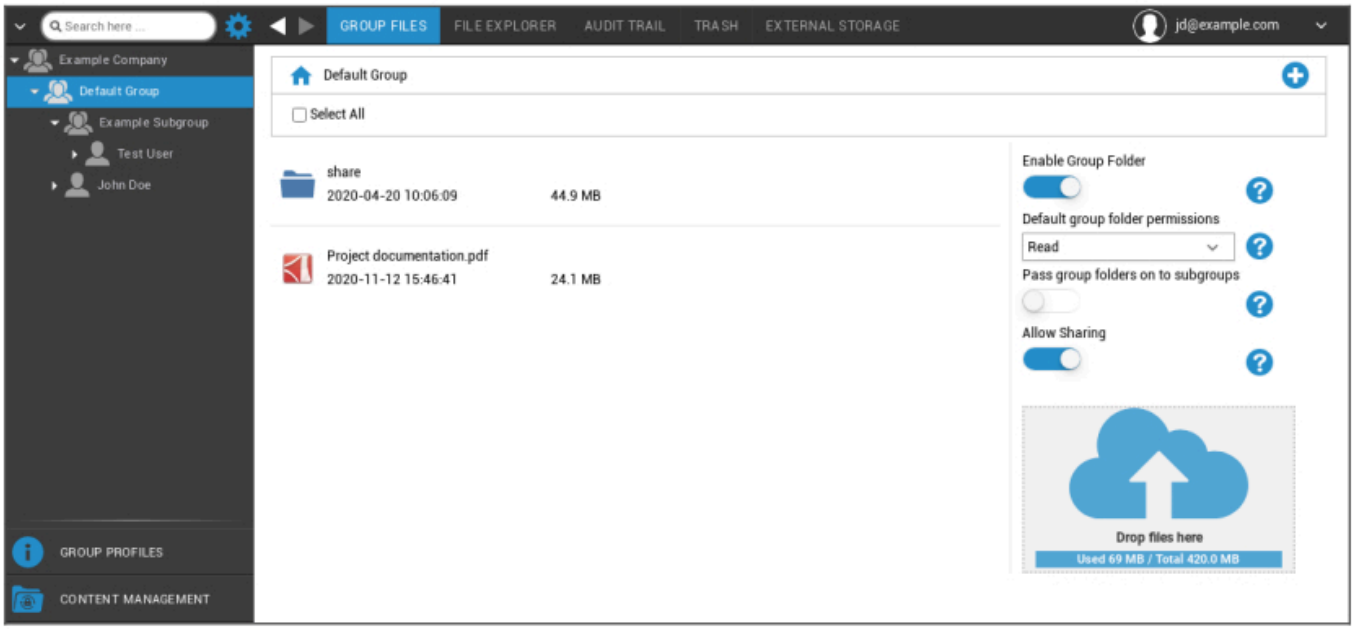
İçerik Yönetimi

Bir gruba dahil olduğunuzda, AppTec'in ContentBox'ını "İçerik Yönetimi" ile yönetebilirsiniz.

Content Box ile belgeleri ve diğer kurumsal verileri son kullanıcı cihazlarına güvenli bir şekilde dağıtabilirsiniz.

Grup Dosyaları

"Grup Dosyaları" ContentBox'ın temel bir parçasını temsil eder. Burada ayarları yapar, belgeleri yükler, yeni klasörler oluşturur vb.



Sağ üst köşedeki sembol ile "Klasör Ekle" ile ilgili gruba atanmış yeni klasörler oluşturabilirsiniz.

Sağ üst köşedeki sembol ile, ilgili gruba atanması gereken "Klasör Ekle" aracılığıyla yeni bir klasör oluşturabilirsiniz.

Klasöre istediğiniz ismi verebilirsiniz.

"Dosya Yükle" aracılığıyla veri yükleyebilirsiniz. Burada Standart-Explorer'ınız açılacaktır. Elbette bu iki işlemi her (alt) klasörde gerçekleştirebilirsiniz.

Sol üst köşedeki sembol ile ana menüye dönebilirsiniz.

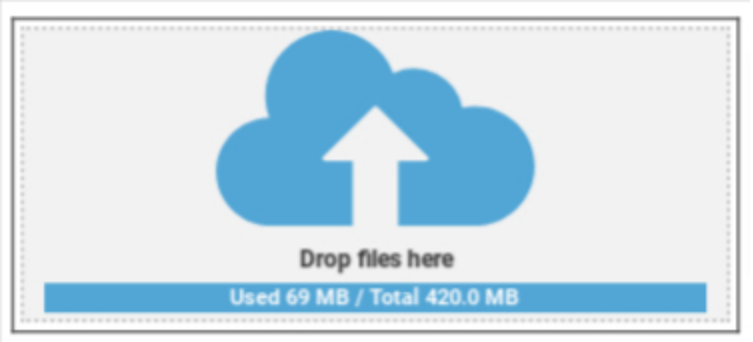
Birkaç klasör ve dosya seçebilir ve bunları "İndir" ile indirebilir veya "Sil" e tıklayarak silebilirsiniz.

Ayrıca tüm dosya ve klasörleri seçerek "İndir" ve "Sil" komutlarını uygulayabilirsiniz.

Farenizi bir klasör veya dosyanın üzerine getirdiğinizde, aşağıdaki genel görünümü göreceksiniz:

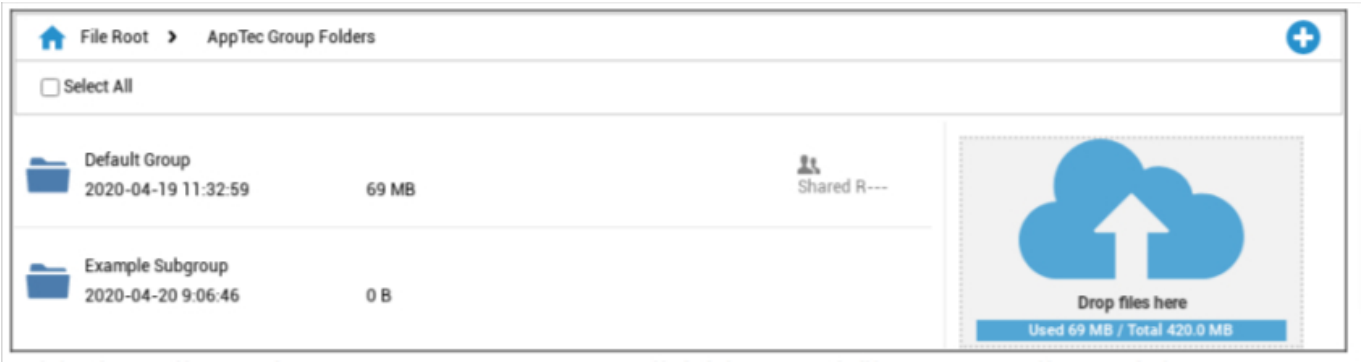
- "Yeniden Adlandır" ile klasörü/dosyayı yeniden adlandırabilirsiniz
- "İndir" ile klasörü/dosyayı indirebilirsiniz
- "Sil" ile klasörü/dosyayı silebilirsiniz

Grup Klasörünü Etkinleştir	Etkinleştirilirse, grubun tüm üyelerinin ilgili klasöre erişimi olur
Varsayılan grup klasörü izinleri	Seçilen gruptaki kullanıcıların izinleri: Okuma = yalnızca okuma izni Güncelle = güncelleme izni Oluştur = oluşturma izni Sil = silme izni
Grup klasörlerini alt gruplara aktarma	Etkinleştirilirse, ilgili alt gruplar ana veri dosyalarına erişebilir
Alt gruplar için izinler	Seçilen alt gruptaki kullanıcıların izinleri: Okuma = yalnızca okuma izni Güncelle = güncelleme izni Oluştur = oluşturma izni Sil = silme izni
Paylaşıma İzin Ver	Etkinleştirilirse, kullanıcı dosyaları bir bağlantı aracılığıyla paylaşabilir



Dosya yüklemek için, bu pencereye Sürükle ve Bırak yoluyla bir dosya çekerek bu alanı kullanabilirsiniz. Internet Explorer yardımıyla bir dosya seçmek ve yüklemek için bu alana da tıklayabilirsiniz.

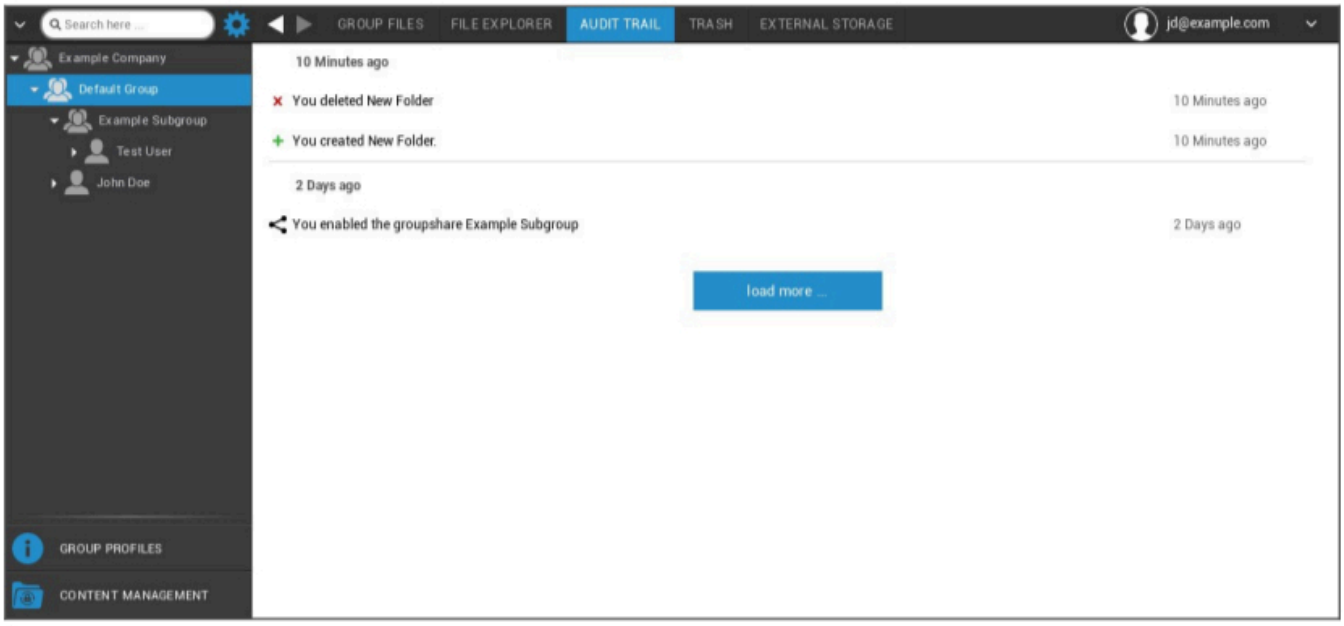
Dosya Gezgini



"Dosya Gezgini" ile tüm klasörleri ve dosyaları - hangi grupta yer aldıklarına bakmaksızın - yönetebilirsiniz.

Ayrıca "Grup Dosyaları" bölümünde öğrendiğiniz ayarları ve düğmeleri de bulacaksınız.

Denetim İzi



"Denetim İzi "nde, geçmişten hangi kullanıcının neyi oluşturduğunu, sildiğini veya paylaştığını görebilirsiniz. Bu şekilde, kurumsal verilerle ne yapıldığını istediğiniz zaman tespit edebilirsiniz.

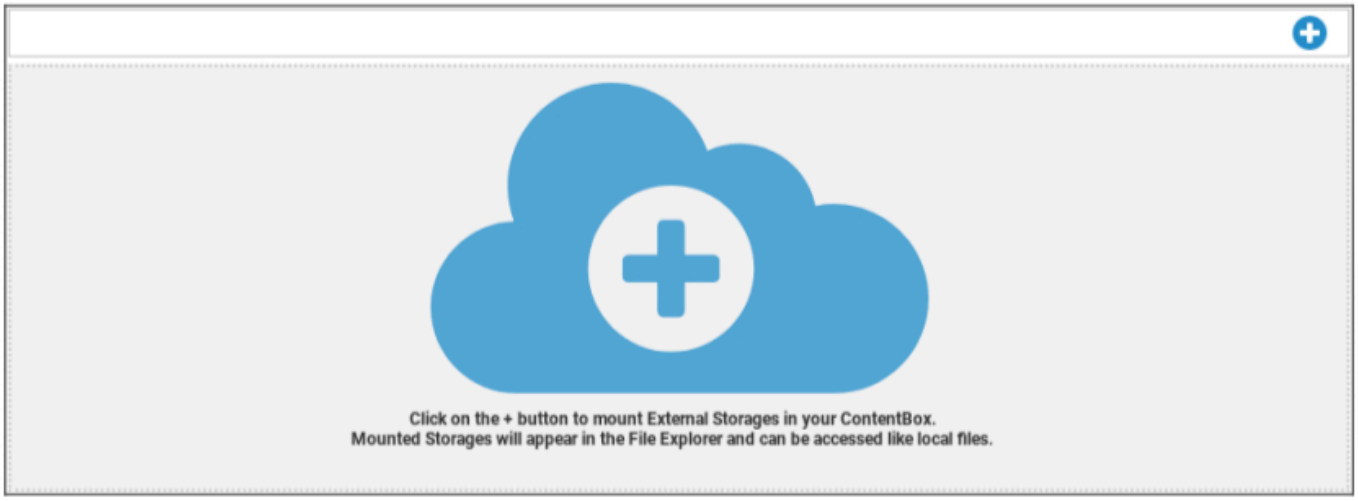
Çöp

Bir şeyi sildiyseniz (yanlışlıkla), "Çöp Kutusu" altındaki klasörleri ve dosyaları görebilir ve isteğinize göre onları kurtarabilirsiniz.

- "Undelete" ile verileri/klasörü kurtarabilirsiniz.
- "Sil" ile verileri/klasörü kalıcı olarak silebilirsiniz - silme komutunu bir kez daha onaylamanız gerekir.

Çöp kutusunda kullanılan depolama kapasitesinin kullanılabilir "Toplam Alanı" azalttığını lütfen unutmayın - bu bir ownCloud gereksinimidir.

Harici Depolama



"Harici Depolama" başlığı altında harici depolamayı bağlayabilirsiniz.

Sembol ile (ek) depolama alanı eklenebilir.

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

Amazon S3	
Ekran Adı	Görünen ad
Erişim Anahtarı	Erişim anahtarı
Gizli Anahtar	Güvenlik anahtarı
Kova	Size atanmış olan alt klasörün kesin kimliği
Ana bilgisayar adı (isteğe bağlı)	Ana bilgisayar adı (isteğe bağlı)
Port (isteğe bağlı)	Port (isteğe bağlı)
Bölge	Bölge (isteğe bağlı)
SSL'yi Etkinleştir	SSL'yi Etkinleştir
Yol Stilini Etkinleştir	Size atanmış olan Yol Adresini Temizle

FTP	
Ekran Adı	Görünen ad
Ev sahibi	Ana Bilgisayar-Adres
Kullanıcı Adı	Kullanıcı Adı
Şifre	Şifre
Kök	Ana menü
Güvenli ftps://	

SFTP	
Ekran Adı	Görünen ad
Ev sahibi	Ana Bilgisayar-Adres
Kullanıcı Adı	Kullanıcı adı
Şifre	Şifre
Kök	Ana menü

ownCloud	
Ekran Adı	Görünen ad
URL	ownCloud URL'si
Kullanıcı Adı	Kullanıcı Adı
Şifre	Şifre
Uzak Alt Klasör	Standart klasör
Güvenli https://	

WebDAV	
Ekran Adı	Görünen ad
URL	WebDAV URL'si
Kullanıcı Adı	Kullanıcı adı
Şifre	Şifre
Kök	Ana menü
Güvenli https://	
Windows Paylaşımı	Windows Share desteği yakında kullanıma sunulacak
SharePoint	Microsoft SharePoint desteği yakında sunulacak

Denetim Günlüğü

Burada, MDM konsolunda gerçekleştirilen eylemler hakkındaki bilgileri kaydeden bir günlük bulabilirsiniz.

Filtre simgesi ile görüntülenen listeye filtreler uygulayabilirsiniz.

Açılır menü **Sayfa başına** öğe: listenin bir sayfasında görüntülenecek öğe miktarını seçebilirsiniz.

Alınan önlem / Değiştirilen ayar	Gerçekleştirilen eylem / Değiştirilen ayar
Değer	Gerçekleştirilen eylemin / değiştirilen ayarın değeri
Kullanıcı	Eylemi gerçekleştiren / ayarı değiştiren kullanıcının adı
Tarih	Bu eylemin gerçekleştirildiği / bu ayarın değiştirildiği zaman damgası
Yol / Tip	Bu eylemin gerçekleştirildiği / bu ayarın değiştirildiği yere giden yol

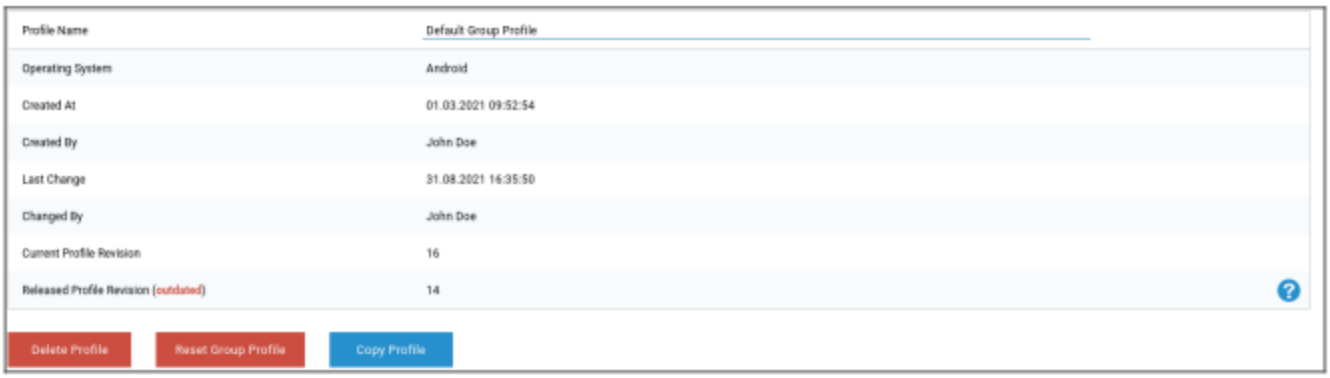
iOS Yapılandırması

Genel

O anda bir grup veya bir cihaz seçmiş olmanıza bağlı olarak, ekran ve alt noktaları farklıdır - lütfen buna dikkat edin!

Grup profiline genel bakış (yalnızca grup düzeyinde)

Bir grup profilini açarken, profile hızlı bir genel bakış elde edersiniz



Profil Adı	Profilin adı (burada değiştirilebilir)
İşletim Sistemi	Profilin ait olduğu İşletim Sistemi
Şu Adreste Oluşturuldu	Yaratılış zamanı
Tarafından Oluşturuldu	Profilin yaratıcısı
Son Değişiklik	Profilde yapılan son değişikliğin zamanı
Tarafından Değiştirildi	Son değişiklikleri yapan hesap
Güncel Profil Revizyonu	Kayıtlı profil durumunun revizyonu
Profil Revizyonu Yayınlandı	Atanmış profil revizyonu ("Şimdi ata"). Etiket metnin arkasında "(eski)" ibaresini gösteriyorsa, bu profili kaydettiğiniz ancak henüz atamadığınız anlamına gelir, bu nedenle cihazlar hala eski sürümü alacaktır.

Genel Bilgiler

Doğrudan cihazın üzerinde olmanız durumunda, seçtiğiniz cihaz hakkında kısa bir genel bakış alacaksınız.

Cihaz Adı	Cihaz adı
Telefon Numarası	Cihaz telefon numarası
Model	Model numarası
İşletim Sistemi	İŞLETIM SISTEMI
Seri Numarası	Cihaz seri numarası
Cihaz Sahipliği	Kurumsal veya özel cihaz Kurumsal = kurumsal cihaz Çalışan = özel cihaz
Cihaz Tipi	Cihaz türü (Tablet veya Telefon)
Jailbroken	Cihazda bir Jailbreak varsa
Gözetim altında	Bunun denetlenen bir cihaz olup olmadığını belirtir
Uyumlu	Herhangi bir yönerge ihlal edilmişse
Son Görülme	Cihazın AppTec360 Sunucusu ile en son ne zaman iletişim kurduğunun durumu

Ayarlar

Bu ayarlar cihaz adını ve önceden tanımlanmış bir arka planı içerir.

Cihazı sistem adına göre adlandırın	AppTec360 Konsolunda (sol hiyerarşi yapısında) verilecek ad, ilgili son kullanıcı cihazındakiyle aynı olacaktır (cihaz ayarlarında görüntülenebilir)
Özel duvar kağıdı kullanma (yalnızca denetimli cihazlar)	Burada, son kullanıcı cihazında görüntülenmesi gereken arka planı önceden tanımlayabilirsiniz (örneğin, cihaz için bir tür kurumsal markalama için) Sadece Denetimli Modda kullanılabilir!
Otomatik işletim sistemi güncellemeleri	Varsa işletim sistemi güncellemelerini zorlar. Yalnızca denetimli moddaki DEP cihazları için.
Özel Yazı Tipleri	Burada özel yazı tipleri ekleyebilirsiniz.
İsim	İsteğe bağlı. Yazı tipi için kullanıcı tarafından görülebilen ad. Bu alan, kurulumdan sonra yazı tipinin gerçek adıyla değiştirilir.
Yazı Tipi	Yazı tipi dosyasını (.otf veya .ttf) yükleyin.

Konfigürasyon Revizyonu

Burada, cihaza hangi grup profilinin atandığına dair genel bir bakış elde edeceksiniz.

Grup profiline tıklarsanız, profile doğrudan erişirsiniz ve ayarları gerçekleştirebilirsiniz.

Sembol ile, atanan uygulamaları grup profilinin ayarlarına geri döndürebilirsiniz.

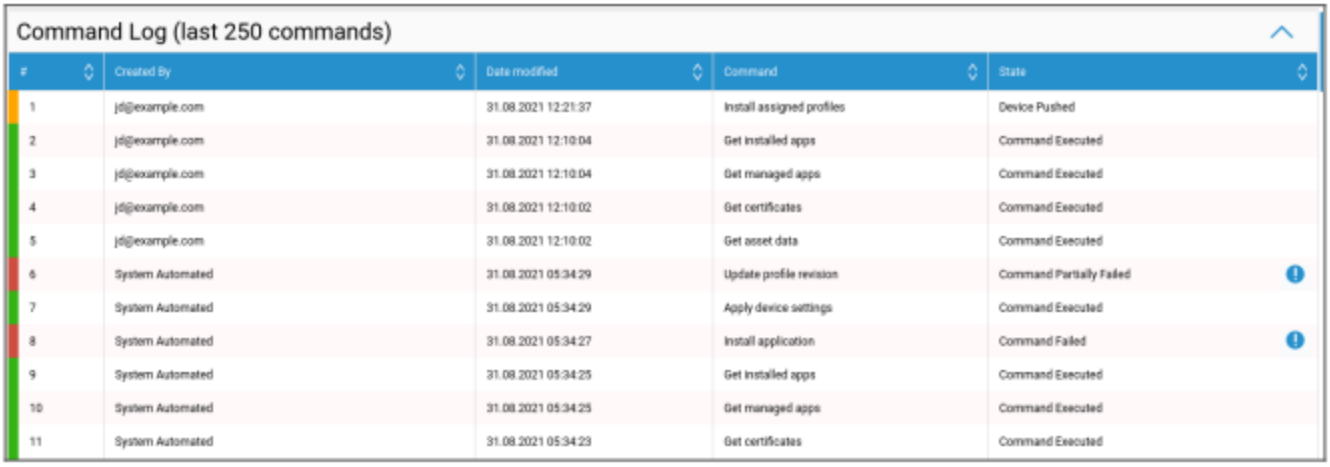
Sembol ile cihaz profilini hiçbir ayara sahip olmayacak şekilde sıfırlayabilirsiniz.

"Newer Revision available" grup profilinin değiştirildiğini ve kaydedildiğini ancak atanmadığını gösterir. Değişiklikleri cihazlara uygulamak için grup profilinin grup düzeyinde "Şimdi ata" ile atanması gerekir.

Cihaz Günlüğü (yalnızca cihaz düzeyinde)

Komut Günlüğü

Burada cihaz için hangi komutların verildiğini ve durumlarının ne olduğunu görebilirsiniz.



"System Automated" tarafından oluşturulan komutlar sistem tarafından otomatik olarak oluşturulur.

Olası komut durumları

Cihaz İtildi	Cihaza EMM sunucusuna geri bağlanmasını söylemek için push hizmetine (örn. APNS) bir push isteği gönderilmiştir.
Komut Oluşturuldu	Komut sistemde oluşturuldu.
Gönderilen Komut	Komut, sunucuya bağlandıktan sonra cihaza gönderildi.
Komut Yürütüldü	Komut başarıyla yürütüldü.
Komut Başarısız	Komut başarısız oldu. *
Komut Kısmen Başarısız	Cihazın işletim sistemine bağlı olarak bazı komutlar birlikte gruplandırılabilir. Bu komut grubunun bazı bölümleri başarısız olmuştur. *
Komut Yürütüldü, sonunda Başarısız Oldu	Komut uygulandı ama belki de uygulanmadı.
Komut Tekrar Gönderildi	Komut bir kullanıcı tarafından yeniden itildi.
Atılmış	Komut iptal edildi. Örneğin, başka bir komutun yerini aldığı için veya cihaz yeniden kaydedildiği ve eski komutlar kaldırıldığı için

Mesajın arkasında bir ünlem işareti varsa, imlecinizi simgenin üzerine getirerek daha fazla bilgi alabilirsiniz.

Varlık Yönetimi (yalnızca cihaz düzeyinde)

Varlık Yönetimi (yalnızca cihaz düzeyinde)

Cihaz Bilgisi

Model	Cihazın model numarası
İşletim Sistemi	İŞLETIM SISTEMI
İşletim Sistemi Sürümü	İşletim sistemi sürümü
Seri Numarası	Seri numarası
UDID	Cihaz UDID'si
Cihaz Adı	Cihaz adı
Gözetim altında	Cihazın denetlenip denetlenmediğini görüntüler
Pil Durumu	Pil durumu

Wi-Fi

IP Adresi	Cihaz IP Adresi
WiFi MAC	WiFi MAC Adresi

Hücresel

Durum	Durum (SIM kart mevcut)
Telefon Numarası	Telefon numarası
Dolaşım Durumu	Mevcut dolaşım durumu
Dolaşım (Ses/Veri)	Ses/veri için dolaşım durumu
IP Adresi	IP Adresi
IMEI	IMEI Numarası
Operatör/Taşıyıcı	Hücresel hizmet sağlayıcı
SIM Taşıyıcı Ağ	SIM taşıyıcı ağı
Taşıyıcı Versiyonu	Taşıyıcı versiyonu
Modem Ürün Yazılımı	Modem ürün yazılımı
Mevcut MCC/MNC	Bkz. "SIM MCC/MNC"
SIM MCC/MNC	Mobil Ülke Kodu, E.212 uyarınca ITU tarafından belirlenmiş bir ülke tanımlamasıdır. Mobil Ağ Kodu (MNC) ile birlikte bir hücresel ağı tanımlamak için kullanılan standart (=ülke kodu) Başka bir hücresel ağa girdiğinizde, "Mevcut MCC/MNC" ve "SIM MCC/MNC" bu nedenle farklıdır.

Bluetooth

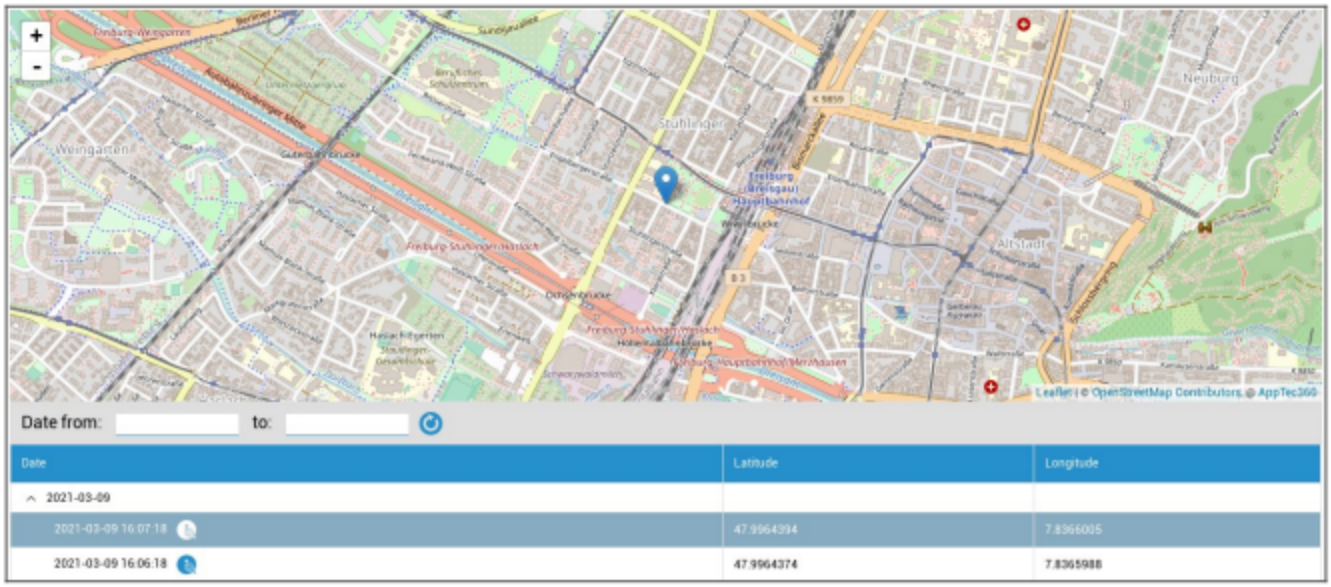
Bluetooth MAC	Bluetooth MAC Adresi

Güvenlik Yönetimi

Hırsızlığa Karşı Koruma (yalnızca cihaz düzeyinde)

GPS Bilgileri (yalnızca cihaz düzeyinde)

Burada cihazın mevcut/son konumunu değerlendirebilirsiniz. Yerelleştirme bir ya da iki parola ile korunabilir - Bkz: Genel Ayarlar - Gizlilik - GPS Erişimi



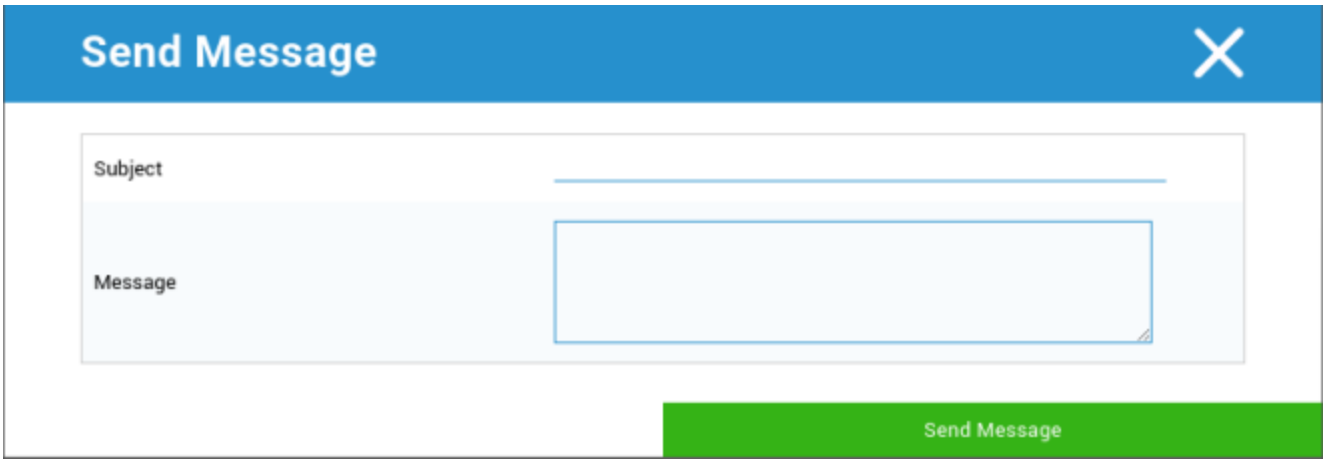
Sil ve Kilitle (yalnızca cihaz düzeyinde)

"Sil ve Kilitle" altında aşağıdaki üç eylemi gerçekleştirebilirsiniz:

Tam Silme	Cihaz fabrika ayarlarına geri döndürülür (kurumsal ve kişisel veriler silinir)
Kurumsal Silme	Son kullanıcı cihazından yalnızca kurumsal veriler kaldırılır (AppTec tarafından sağlanan tüm uygulamalar, veriler vb.)
Kilit Ekranı	Ekran kilidi etkinleştirildiğinde, cihazın kilidini cihaz şifresi/PIN ile açmak yeterlidir
Adli Kilitleme (Yalnızca Denetlenen Cihazlar)	Bu fonksiyon  sembolü ile etkinleştirilirse, cihaz kapatılamayan bir mesaj göstererek kilitlenir. Çalışan ayrıca cihazın kilidini de açamaz. Cihazın kilidini konsolda  sembolü ile sadece yönetici açabilir.
Etkinleştirme Kilidine İzin Ver (Yalnızca Denetlenen Cihazlar)	Bu işlev etkinleştirilirse, iCloud ayarlarında "iPhone'umu Bul" etkinleştirilir etkinleştirilmez cihaz kilitlenecektir

Mesaj (yalnızca cihaz düzeyinde)

Aşağıdaki pencere ile konuyu ve mesajı doldurabilir ve bir son kullanıcı cihazına gönderebilirsiniz:



Güvenlik Yapılandırması

Şifre

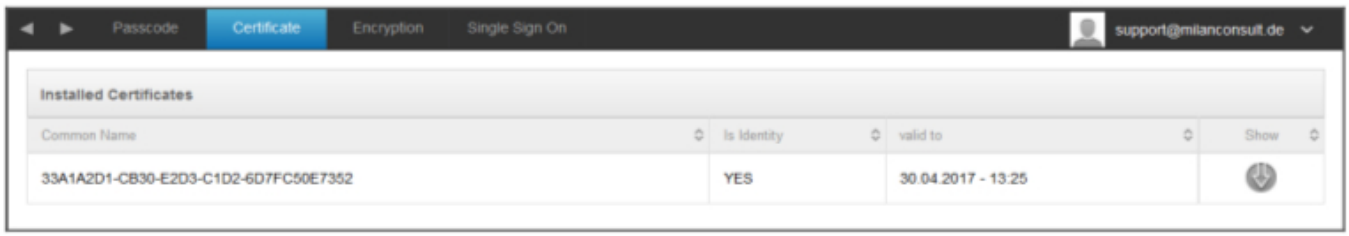
Burada cihaz şifresi için ayarları belirlersiniz

Kod devre dışı bırakmaya izin verildi	Bu ayar etkinleştirildiğinde, bir parola girme istemi yoktur Bir şifre oluşturulduktan sonra devre dışı bırakılamaz
Basit değere izin ver	Kullanıcının aynı, artan ve azalan sayı dizilerini kullanmasına izin verin (örn. 1234, 1111)
Alfanümerik değer gerektir	Parolalar en az bir harf içermelidir
Minimum şifre uzunluğu	Minimum parola uzunluğu
Minimum karmaşık karakter sayısı	Paroladaki minimum alfanümerik sembol sayısı
Maksimum şifre yaşı	Parolanın değiştirilmesi gereken gün sayısı
Maksimum Otomatik Kilit	Cihazın kilitleneceği maksimum süre
Cihaz kilidi için maksimum ödemesiz süre	Cihazın kilitli Bekleme moduna girdiği süre
Maksimum başarısız deneme sayısı	Tam bir cihaz silme işlemi gerçekleştirilmeden önce bir parolanın ne kadar sıklıkla yanlış girilebileceğini belirler
Maksimum şifre yaşı (1-730 gün)	Maksimum parola yaşı
Parola geçmişi (1-50 parola)	Bu sayıdan sonra eski bir parolanın kullanılmasına izin verilir

Çöp kutusuna tıklandığında, unutulan bir cihaz şifresinin silinebileceği Şifre Sıfırlama İletişim Kutusu açılır.

Sertifika (yalnızca cihaz düzeyinde)

Cihazda mevcut olan sertifikaları görüntüler



Şifreleme

Depolama şifrelemesi gerektir	Yüklü cihaz şifreleme işlevini etkinleştirin

Tek Oturum Açma

"Tek Oturum Açma" başlığı altında Kerberos kimlik doğrulamasını yapılandırabilirsiniz.

Burada, Kerberos Belirteçlerini kullanmasına izin verilen erişim kimlik bilgilerini ve ilgili URL'leri / Uygulamaları belirlersiniz.

Denetimli Modda Kullanılabilir	
Hesap Adı	Hesap Adı
Müdür Adı	Kerberos Biletlerinin dağıtılabileceği benzersiz kimlik
Realm	Kullanılacak olan Kerberos Realm'iniz (örn. Etki Alanınız)

Sembol ile ek URL'ler oluşturabilirsiniz.

Bu hesabı sınırlamak için kullanılan URL kalıbı	Kerberos Biletlerinin dağıtılabileceği URL'ler belirlenecek

Sembol ile ek Uygulamalar oluşturabilirsiniz.

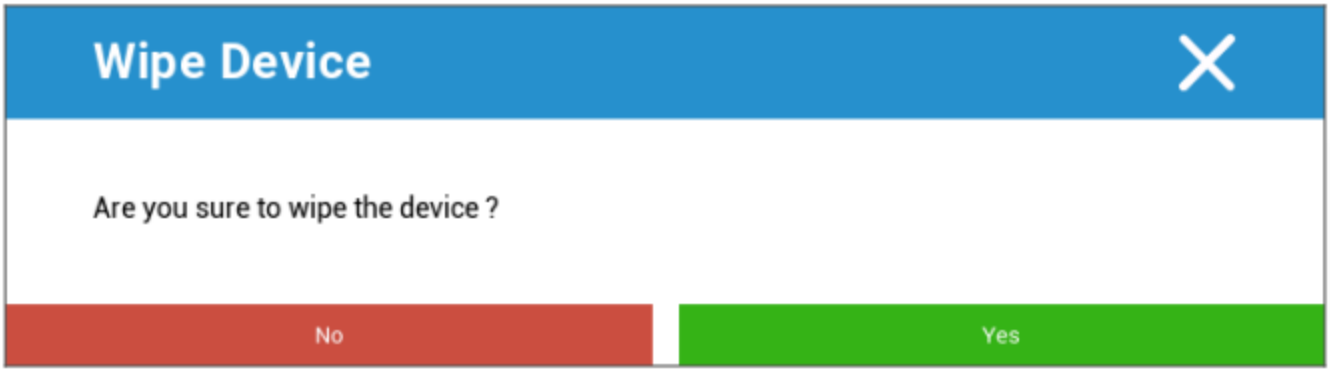
Bu hesabı sınırlamak için uygulamalar	Kerberos Biletlerinin dağıtılabileceği Uygulamalar belirlenecek

Kullanım Ömrü Sonu (yalnızca cihaz düzeyinde)

Silme (yalnızca cihaz düzeyinde)

"Sil" altında, cihazı fabrika ayarlarına geri yükleyebilirsiniz. Burada kurumsal verilerin yanı sıra özel veriler de son kullanıcı cihazında silinecektir.

"Eksi sembolüne" tıkladığınızda aşağıdaki mesajı almalısınız



"Evet" ile silme işlemini gerçekleştirebilirsiniz.

"Silme Raporu" altında aşağıdaki öğeler görüntülenebilir

Tarafından silindi	Silme işlemini kimin yaptığına dair tarihçe
Tarih	Tarih
Durum	Durum (örn. Silme işlemi başarıyla gerçekleştirildiyse)

Kısıtlama Ayarları

Cihaz İşlevselliği

Burada bireysel son kullanıcı cihaz işlevlerini engelleyebilirsiniz

Uygulama yüklemeye izin ver	Uygulamaların yüklenmesine izin ver
Kameraya izin ver	Kamera kullanımına izin verin
FaceTime'a İzin Ver	FaceTime'a İzin Ver
Ekran yakalamaya izin ver	Ekran yakalamaya izin ver
Dolaşımdayken otomatik senkronizasyona izin ver	Dolaşımdayken otomatik senkronizasyona izin ver
Siri'ye İzin Ver	Siri'ye İzin Ver
Sesli aramaya izin ver	Sesli aramaya izin ver
Uygulama içi satın almaya izin ver	Uygulama içi satın almaya izin ver
Tüm satın alımlar için iTunes Store şifresi gerektir	Tüm satın alımlar için iTunes Store şifresi gerektir
Çok oyunculu oyunlara izin ver	Çok oyunculu oyunlara izin ver
Game Center arkadaş eklemeye izin ver	Game Center arkadaş eklemeye izin ver
Yönetilenlerden yönetilmeyenlere açılmaya izin ver	Yönetilen uygulamalardaki içeriğin yönetilmeyen uygulamalarda açılmasına izin ver
Yönetilmeyenlerden yönetilenlere açılmaya izin ver	Yönetilmeyen uygulamalardaki içeriğin yönetilen uygulamalarda açılmasına izin ver
Kilit ekranında bugün görünümüne izin ver	Bu ayar etkin olduğunda, "Bugün" görünümü kilit ekranındaki Bildirim Merkezi'nde görüntülenecektir
Kilit ekranında kontrol merkezine izin ver	Kilit ekranında Denetim Merkezi'ne izin ver
TouchID'ye izin ver	TouchID'ye izin ver
Havadan PKI güncellemelerine izin verin	Havadan PKI güncellemelerine izin verin
Kilitliyken hesap cüzdanına izin ver	Cihaz kilitliyken hesap cüzdanına izin ver
Reklam İzlemeyi Sınırlandırın	Bu işlev Reklam İzlemeyi devre dışı bırakır (örn. reklamverenler kişiselleştirilmiş reklamlar dağıtmak için Reklam İzlemeyi

	kullanamaz)
Handoff'a İzin Ver	Handoff'a İzin Ver
Spotlight'ta internet sonuçlarına izin ver	Spotlight'ta internet sonuçlarına izin verin (örn. Bing veya Wikipedia)
İlk AirPlay eşleştirmesinde parola gerektir	İlk AirPlay eşleştirmesinde parola gerektir
Force Watch Bilek Koruması	Etkinleştirilirse, Apple Watch "Bilek Koruması" (bilek tanıma) kullanmaya zorlanır
iCloud Fotoğraf Arşivi'ne izin ver	iCloud Fotoğraf Arşivi'ne izin verir. İzin verilmezse, iCloud'dan tamamen indirilmemiş olan tüm resimler yerel depolama alanında silinecektir
Denetimli Modda kullanılabilir	
Hesap Değişikliğine İzin Ver	"Posta, kişiler, takvim" değişikliklerine izin ver
AirDrop'a İzin Ver	AirDrop'a İzin Ver
Uygulama Hücresel Değişikliğine İzin Ver	Bu ayar, hangi uygulamaların mobil veri kullanmasına izin verileceği ayarını engeller Bu ayar, örneğin, son kullanıcı cihazında manuel olarak ayarlanabilir ve ardından bu kısıtlama etkinleştirilebilir
Siri'nin web'den kullanıcı tarafından oluşturulan içeriği sorgulamasına izin verin	Belirli web sitelerinde web araması engellenmiştir, örn. Wikipedia, çünkü herkes istediği gibi değişiklik yapabilir
Siri küfür filtresini etkinleştirin	Siri'ye yönelik küfürler sansürlenir
iBook Store'a İzin Ver	iBook Store'a İzin Ver
iBook Store Erotica'ya İzin Ver	iBook Store Erotica'ya İzin Ver
Arkadaşlarımı Bul ayarlarının değiştirilmesine izin ver	Arkadaşlarımı Bul ayarlarının değiştirilmesine izin ver
Oyun Merkezine İzin Ver	Oyun Merkezine İzin Ver
Ev Sahibi Eşleştirmesine İzin Ver	Kontrol bilgisayarı eşleştirme
Yapılandırma profillerinin yüklenmesine izin ver	Yapılandırma profillerinin yüklenmesine izin ver
Uygulamayı Kaldırmaya İzin Ver	Kontrol uygulamalarının kaldırılması
iMessage'a izin ver	iMessage'a izin ver

Tüm içerik ve ayarların silinmesine izin ver	Tüm içerik ve ayarların silinmesine izin ver
Kısıtlamaların yapılandırılmasına izin ver	Kısıtlamaların yapılandırılmasına izin ver
Podcast'e İzin Ver	Podcast'e İzin Ver
Tanım Aramaya İzin Ver	Tanım aramaya izin ver
Tahmini Klavyeye İzin Ver	Tahmini klavyeye izin ver
Otomatik Düzeltmeye İzin Ver	Otomatik düzeltmeye izin ver
UI Uygulama Yüklemesine İzin Ver	Devre dışı bırakılırsa, genel AppStore'dan hiçbir uygulama yüklenemez (simge artık görüntülenmez). Ancak uygulamalar yine de iTunes ve Yapılandırıcı aracılığıyla yüklenebilir
Klavye Kısayollarına İzin Ver	Cihaz fiziksel bir klavyeye bağlıysa klavye kısayollarına izin verin
Apple Watch eşleştirmesine izin ver	Aygıt ile Apple Watch arasında bir eşleşmeyi yasaklar, mevcut bağlantılar sonlandırılır
Parola değişikliğine izin ver	İzin verilmezse, hiçbir cihaz parolası eklenemez, değiştirilemez veya kaldırılamaz
Aygıt adı değişikliğine izin ver	Cihaz adının değiştirilip değiştirilemeyeceğini belirleyen kılavuz
Duvar kağıdı değişikliğine izin ver	Duvar kağıdının değiştirilip değiştirilemeyeceğini belirleyen kılavuz
Otomatik uygulama indirmelerine izin ver	Devre dışı bırakılırsa, satın alınan bir uygulama diğer cihazlara otomatik olarak yüklenmez. Mevcut uygulamaların güncellemeleri için geçerli değildir
Haberlere İzin Verin	iOS aygıtında Haberlere İzin Ver
Kurumsal uygulama güvenine izin ver	Yanlış olarak ayarlanırsa kurumsal uygulamalara güvenilmesini engeller

iCloud

iCloud eşleştirme sırasında belirli işlevleri engelleme

Yedeklemeye izin ver	Yedeklemeye izin ver
Belge senkronizasyonuna izin ver	Belge senkronizasyonuna izin ver
Fotoğraf Akışına İzin Ver	Fotoğraf Akışına İzin Ver
Paylaşılan Fotoğraf Akışına İzin Ver	Paylaşılan Fotoğraf Akışına İzin Ver
Bulut Anahtarlık Senkronizasyonuna İzin Ver	Bulut Anahtarlık Senkronizasyonuna İzin Ver
Yönetilen uygulamaların veri depolamasına izin verin	Yönetilen uygulamaların veri depolamasına izin verin
Kurumsal defterler için notların ve önemli noktaların senkronizasyonuna izin ver	Kurumsal defterler için notlar ve önemli noktalar senkronizasyonuna izin ver
Kurumsal defterlerin yedeklenmesine izin verin	Kurumsal defterlerin yedeklenmesine izin verin

Güvenlik ve Gizlilik

Teşhis verileriyle ilişkili bu işlevleri engelleyin

Tanılama verilerinin Apple'a gönderilmesine izin verin	Tanılama verilerinin Apple'a gönderilmesine izin verin
Kullanıcının güvenilmeyen TLS sertifikalarını kabul etmesine izin ver	Kullanıcının güvenilmeyen TLS sertifikalarını kabul etmesine izin ver
Şifrelenmiş yedeklemeleri zorla	Şifrelenmiş yedeklemeleri zorla

BYOD

Yerleşik iOS Güvenliği (Konteyner)

iOS her zaman yönetilen (iş) ve yönetilmeyen (özel) arasında bir fark yaratabilmiştir. MDM Sisteminden gelen her şey yönetilen olarak değerlendirilir. Örneğin, MDM aracılığıyla bir Uygulama yüklerseniz veya bir Exchange Hesabı yapılandırırsanız, bu iOS tarafından yönetiliyor olarak değerlendirilecektir.

Cihazda manuel olarak yapılandırılan/yüklenen diğer her şey yönetilmeyen olarak değerlendirilecektir. Örneğin, Kullanıcı WhatsApp'ı kendi başına yüklüyorsa veya bir Exchange Hesabı ekliyorsa. Ancak bu ayrılık temasları hiçbir zaman etkilememiştir. Ancak iOS 11.3 (ve üstü) sürümden itibaren bu özellik kişiler için de eklenmiştir.

Bu, işletim sisteminin temel bir işlevi olduğundan, bir şey yüklemenize veya özel bir kap kurmanıza gerek yoktur.

Özel ve iş uygulamalarını/bilgilerini/dosyalarını ayırmak için Yerleşik İşlevi etkinleştirin. Bu ayar, aksi takdirde bu ayrımın bazı kısımlarını yanlışlıkla kapatabilecek diğer bazı işlevleri de devre dışı bırakacaktır.

Aktivasyon

AppTec360 tarafından desteklenen Konteyner Çözümlerini etkinleştirin

Google Divide Container'ı Etkinleştirin	Google Divide Container'ı Etkinleştirin
SecurePIM Konteynerini Etkinleştir	SecurePIM Konteynerini Etkinleştir

SecurePIM Konteynerini etkinleştirdiyseniz, "Etkinleştirme" altında aşağıdaki noktayı da bulacaksınız. Ayrıca, hemen aşağıda açıklanan dört sekme daha açılacaktır.

Destek E-posta Adresi	Bir kullanıcının sorunlarını iletebileceği destek e-posta adresi

SecurePIM Parolası

"SecurePIM Password" altında, parola güvenlik gücü için yönergeleri belirleyebilirsiniz.

Oturum Zaman Aşımı	Burada, SecurePIM arka planda çalıştığında kaç dakika sonra yeni bir parolanın tekrar girilmesi gerektiğini belirleyebilirsiniz
Şifre Uzunluğu	SecurePIM Konteynerine erişim için şifre uzunluğu
Büyük Harf Karakterleri	Minimum büyük harf karakterleri
Küçük Harf Karakterleri	Minimum küçük harf karakterleri
Özel Karakterler	Minimum özel karakterler
Rakamlar	Minimum rakamlar
Silme Uygulaması	SecurePIM içeriği silinmeden önce bir parolanın kaç kez yanlış girilebileceği (Ancak Uygulama hala son kullanıcı cihazında kalır)

SecurePIM Güvenlik

"SecurePIM Güvenliği" altında, çeşitli güvenlik ayarları oluşturabilirsiniz.

Jailbreak Yapılmış Cihazları Algılama	Bu ayar etkinleştirilirse, cihaz jailbreak edilmiş olarak algılanır algılanmaz SecurePIM Konteynerine erişim engellenecektir
Güvenli Metin Alanları	Gönderim alanlarının içeriği şifrelenir, işletim sistemine (iOS) hiçbir bilgi ulaşmaz Not: Bu ayar etkin olduğu sürece, otomatik düzeltme artık kullanılamaz
Kişi Verilerini Cihaza Aktarma	Bu ayar etkinleştirilirse, kullanıcının Exchange Kişilerini kendi yerel cihazına aktarmasına izin verilir Not: Yalnızca ad ve telefon numarası dışa aktarılır
Etkinlik Yerini Göster	Bu ayar etkinleştirilirse, yaklaşan etkinliklerin konumu bildirim çubuğunda görüntülenecektir
Etkinlik Başlığını Göster	Bu ayar etkinleştirilirse, yaklaşan etkinlik başlığının konumu bildirim çubuğunda görüntülenecektir

SecurePIM Tarayıcı

Burada SecurePIM'in tarayıcısını yapılandırabilirsiniz.

Sembol ile yeni bir URL tanımlayabilirsiniz.

Sembol ile tanımlanmış bir URL'yi tekrar kaldırabilirsiniz.

"Beyaz listedeki URL'ler" yüklenebilen URL'lerdir.

"Kara listeye alınmış URL'ler" yüklenemeyen ve bu nedenle engellenen URL'lerdir.

Beyaz Liste girişlerinin Kara Liste girişlerinden daha yüksek önceliğe sahip olduğunu lütfen unutmayın. "Yer İşareti Başlığı" altında bir başlık verebilirsiniz. "Yer İmi URL'si" ile URL adresini yer imi başlığıyla ilişkilendirebilirsiniz - bu şekilde ilgili kullanıcılara bireyselleştirilmiş yer imleri dağıtabilirsiniz.

Değişim

"Exchange" altında bir Exchange hesabı yapılandırabilirsiniz.

ActiveSync E-posta Adresi	Exchange e-posta adresi ("Yer tutuculara" dikkat edin)
ActiveSync Exchange Girişi	Kullanıcı adlarını değiştirin ("Yer tutuculara" dikkat edin)
ActiveSync Exchange Sunucusu	Exchange Sunucusu adresi (FQDN)
ActiveSync Exchange Etki Alanı	Exchange Etki Alanı adresi
Kullanıcı Sertifikası	Kullanıcı sertifikası
Sertifika tabanlı kimlik doğrulama	Kullanıcı bir sertifika ile kimlik doğrulaması yapar
S/MIME Şifrelemesine İzin Ver	Kullanıcının postalarını şifrelemesine izin verir
S/MIME İmzalamaya İzin Ver	Kullanıcının postalarını imzalamasına izin verir
CRL Kontrolü	Aktifse, özel sertifika CRL (Sertifika İptal Listesi) ile karşılaştırılacaktır

Bağlantı Yönetimi

Wi-Fi

Hizmet Seti Tanımlayıcısı (SSID)	Bağlanılacak ağın SSID'si
Otomatik Katıl	Bir ağa katılırken otomatik katılımı etkinleştirin
Gizli Ağ	AP'nin SSID'yi yayınlamaması durumunda etkinleştirin

Proxy Kurulumu

Her Erişim Noktası için bir Proxy Yapılandırılması

Hiçbiri		Vekil Oluşturma
Manuel		Manuel bir Proxy oluşturun
	Proxy Sunucu URL'si	Proxy Ayarlarına erişim için adres
	Liman	Proxy için bağlantı noktası belirleme
	Kimlik Doğrulama	Proxy'de kimlik doğrulama için kullanıcı adı
	Şifre	Proxy'de kimlik doğrulama için şifre
Otomatik		Otomatik olarak bir Proxy oluşturun
Proxy Sunucu URL'si		Proxy ayarlarına erişim için URL

Güvenlik Türü

AP için Güvenlik Türü Oluşturma

WEP	
Şifre	AP için şifre

WPA/WPA2	
Şifre	AP için şifre

WEP Enterprise - WPA / WPA2 Enterprise - Any Enterprise			
	Protokoller		
	TLS	Etkinleştir/Devre Dışı Bırak	
	TTLS	Etkinleştir/Devre Dışı Bırak	
	LEAP	Etkinleştir/Devre Dışı Bırak	
	PEAP	Etkinleştir/Devre Dışı Bırak	
	EAP-FAST	Etkinleştir/Devre Dışı Bırak	
	EAP-SIM	Etkinleştir/Devre Dışı Bırak	
	PAC kullanın		PAC (Korumalı Erişim Kontrolü) Kullanımı
	Provizyon PAC	Provision PAC Yapılandırması	
	Anonim Olarak PAC Sağlama	Anonim PAC Temini	
	İç Kimlik Doğrulamaları	Kullanılması gereken kimlik doğrulama protokolü: PAP, CHAP, MSCHAP, MSCHAPv2	
	Kullanıcı Adı	Kimlik doğrulama kullanıcı adı	
	Bağlantı Başına Parola kullanmayın	Bağlantı Başına Parola kullanmayın	
	Kimlik Belgesi	Kimlik doğrulama sertifikası yükleme/seçme	
	Dış Kimlik	Dışarıdan görülebilen kimlik	
	Güven		
	Güvenilir Sertifika 1	İlk güvenilir sertifikayı yükleme	
	Güvenilir Sertifika 2	İkinci güvenilir sertifikayı yükleme	
	Güvenilir Sertifika 3	Üçüncü güvenilir sertifikayı yükleme	
	Güvenilir Sunucu Sertifika Adları	Beklenen sunucu sertifikalarının adları (virgülle ayrılmış bir listede)	

Hiçbiri	Hiçbir güvenlik oluşturmayın

VPN

Bağlantı Adı	VPN-Profilinin Adı

VPN Türü

VPN

Tüm cihaz ağ trafiği bir VPN bağlantısı üzerinden yönlendirilecektir.

Bağlantı Türü	VPN bağlantı türü oluştur
IPsec (cisco)	Cisco tarafından IPsec protokolü
PPTP	PPTP protokolü
L2TP	L2TP protokolü
Cisco AnyConnect	AnyConnect protokolü
Juniper SSL	Juniper SSL protokolü
F5 SSL	F5 SSL protokolü
SonicWall mConnect	SonicWall mobile Connect
Aruba VIA	Aruba VIA protokolü
Özel SSL	Özel SSL ile Bağlantı
OpenVPN	OpenVPN protokolü

Uygulama Başına VPN

Belirli bir uygulama açıldığında, bir VPN bağlantısı kurulacaktır

Uygulama Başına VPN bağlantısını otomatik olarak başlat		Uygulama Başına VPN bağlantısını otomatik olarak başlat
Bağlantı Türü		VPN bağlantı türü oluştur
	Cisco AnyConnect	AnyConnect protokolü
	Juniper SSL	Juniper SSL protokolü
	F5 SSL	F5 SSL protokolü
	SonicWall mConnect	SonicWall mobile Connect
	Aruba VIA	Aruba VIA protokolü
	Özel SSL	Özel SSL ile Bağlantı
	OpenVPN	OpenVPN protokolü

Proxy Kurulumu

VPN bağlantısı için bir Proxy'nin yapılandırılması

Hiçbiri	Vekil Oluşturma
Manuel	Manuel olarak Proxy oluşturma
Proxy Sunucu URL'si	Proxy Ayarlarına erişim için adres
Liman	Proxy için bağlantı noktası belirleme
Kimlik Doğrulama	Proxy'de kimlik doğrulama için kullanıcı adı
Şifre	Proxy'de kimlik doğrulama için şifre
Otomatik	Otomatik olarak bir Proxy oluşturun
Proxy Sunucu URL'si	Proxy ayarlarına erişim için URL

Yer Tutucuları Göster	AppTec360'ın kullanabileceği tüm mevcut kullanıcı değişkenlerini görüntüler

APN

Erişim Noktası Adı	Erişim Noktası adı
Erişim Noktası Kullanıcı Adı	Erişim Noktası kullanıcı adı
Erişim Noktası Şifresi	Erişim Noktası şifresi
Proxy Sunucusu	Proxy Sunucu adresi
Liman	İlgili Proxy bağlantı noktası

Hücresel

Veri Dolaşımını Etkinleştir	Veri Dolaşımını Etkinleştir
Sesli Dolaşımı Etkinleştir	Sesli Dolaşımı Etkinleştir
Hotspot'u Etkinleştir	Hotspot'u Etkinleştir

HTTP Proxy

Proxy Türü	
Manuel	Manuel olarak bir Proxy oluşturun
Proxy Sunucu URL'si	Proxy Ayarlarına erişim için adres
Liman	Proxy bağlantı noktası oluştur
Kimlik Doğrulama	Proxy'de kimlik doğrulama için kullanıcı adı
Şifre	Proxy'de kimlik doğrulama için şifre
Otomatik	Otomatik olarak bir Proxy oluşturun
Proxy PAC URL'si	Proxy PAC URL'si
PAC'ye erişilemiyorsa doğrudan bağlantıya izin ver	PAC'ye erişilemiyorsa doğrudan bağlantıya izin ver (VPN olmadan)
Tutsak ağlara erişmek için proxy'yi atlamaya izin verin	Tutsak iç ağlara erişmek için proxy'yi atlamaya izin verin

AirPrint

IP Adresi	Yazıcı IP adresi
Kaynak Yolu	AirPrint cihazına giden kesin yol

AirPlay

Cihaz Adı	Cihaz adı
Şifre	Eşleştirme şifresi
Beyaz Liste	Cihazın yalnızca kendisini eşleştirebileceği cihazların bir listesini tanımlayın

PIM Yönetimi

Exchange Active Sync

Hesap Adı	E-posta hesabı adı
Exchange ActiveSync Ana Bilgisayarı	Sunucunun adresi/FQDN
Taşınmaya İzin Ver	E-postaların taşınmasına izin verin
Sadece Postada Kullanın	Etkileşimler yalnızca yerel Posta Uygulamasında gerçekleşebilir
SSL kullanın	SSL şifrelemesini kullanın
Etki Alanı	Sunucu etki alanı
Kullanıcı	Kullanıcı Adı
e-Posta Adresi	e-posta adresi (yalnızca cihaz düzeyinde)
Şifre (yalnızca cihaz düzeyinde)	Kullanıcı şifresi
Kimlik Belgesi	Sunucuda kimlik doğrulama için ilgili sertifikayı seçin
Mail to Sync'in Geçmiş Günleri	E-postaların geri senkronize edilmesine kadar geçecek gün sayısı. Limit Yok = sınırsız
S/MIME'ı Etkinleştir	S/MIME şifrelemesini etkinleştirin
Sertifika İmzalama	İlgili İmzalama Sertifikasını yükleyin
Şifreleme Sertifikası	İlgili Şifreleme Sertifikasını yükleyin

e-Posta

Son kullanıcı cihazında POP3 / IMAP hesaplarının kurulması

Hesap Açıklaması	İsim des E-posta Hesapları		
Hesap Türü	IMAP	Yol Öneki	Özel klasörler için Yol Öneki
	POP		
Kullanıcı Ekran Adı	Kullanıcı ekran adı		
E-posta Adresi	Kullanıcı e-posta adresi		
Taşınmaya İzin Ver	E-postaların taşınmasına izin verin		
S/MIME'ı Etkinleştir	S/MIME şifrelemesini etkinleştirin		
Sertifika İmzalama	İlgili İmzalama Sertifikasını yükleyin		
Şifreleme Sertifikası	İlgili Şifreleme Sertifikasını yükleyin		

Gelen Posta

Gelen sunucu ayarları

Posta Sunucusu Adresi	Posta Sunucusu adresi
Posta Sunucusu Bağlantı Noktası	Posta Sunucusu bağlantı noktası
Kullanıcı Adı	İlgili kullanıcı adı
Kimlik Doğrulama Türü	Kimlik Doğrulama Türü
Hiçbiri	Kimlik Doğrulama Türü Yok
Şifre (yalnızca cihaz düzeyinde)	Parola istemi
MDM Mücadelesi-Yanıt	
NTLM	NTLM-Kimlik Doğrulama
HTTP MD5 Özeti	
SSL kullanın	Gerekirse SSL kullanın

Giden Posta

Giden sunucu ayarları

Posta Sunucusu Adresi	Posta Sunucusu Adresi
Posta Sunucusu Bağlantı Noktası	Posta Sunucusu Bağlantı Noktası
Kullanıcı Adı	İlgili Kullanıcı Adı
Kimlik Doğrulama Türü	
Hiçbiri	Kimlik doğrulama yöntemi yok
Şifre (yalnızca cihaz düzeyinde)	Parola istemi
MDM Mücadelesi-Yanıt	
NTLM	NTLM-Kimlik Doğrulama
HTTP MD5 Özeti	
SSL kullanın	Gerekirse SSL kullanın
Giden şifre gelen ile aynı	Giden şifre gelen ile aynı
Sadece postada kullanın	Tüm giden e-postalar Mail-App aracılığıyla gönderilecekse etkinleştirin

CalDav

Bir CalDav Hesabının kurulumunu ve dağıtımını yapılandırma

Hesap Açıklaması	Hesabın görünen adı
Ana bilgisayar adı	Ana bilgisayar adı ve/veya IP adresi
Liman	CalDav Hesabının Bağlantı Noktası
Ana URL	Hesabın Ana URL'si
Kullanıcı Adı	İlgili CalDav kullanıcı adı
Şifre (yalnızca cihaz düzeyinde)	İlgili CalDav şifresi
SSL kullanın	Gerekirse SSL kullanın

Abone Olunan Takvimler

Abonelikli Takvimlerin kurulumu ve dağıtımı

Açıklama	Hesabın görünen adı
URL	Takvim veritabanının URL'si
Kullanıcı Adı	Takvim aboneliğinin kullanıcı adı
Şifre (yalnızca cihaz düzeyinde)	Takvim aboneliğinin şifresi
SSL kullanın	Gerekirse SSL kullanın

LDAP

Bu alanda, son kullanıcı cihazı ile Active Directory arasında dinamik bir sertifika alışverişine izin vermek için bir LDAP bağlantısı kurun.

Lütfen seçilen kullanıcının ilgili okuma iznine sahip olması gerektiğini unutmayın.

Hesap Açıklaması	Hesap Açıklaması
Hesap Kullanıcı Adı	LDAP erişimi için kullanıcı
Hesap Şifresi	LDAP erişimi için parola
Hesap Ana Bilgisayar Adı	LDAP Sunucusu Ana bilgisayar adı/IP adresi
SSL kullanın	Gerekirse SSL kullanın

İkinci bölümde, LDAP kayıt defterinde arama yapmak için ayrı ayrı filtreler tanımlayabilirsiniz.

Açıklama	Kapsam	Arama Tabanı
Filtre açıklaması	LDAP kayıt defterinde arama düzeyi	Bireysel filtreyi tanımlama

Web Yönetimi

Webclips

Bu konumda, son kullanıcı cihazında bir uygulama olarak görünecek olan web sayfalarına, intranet portallarına vb. bağlantılar içeren yer imlerini tanımlayın.

Etiket	Son kullanıcı cihazındaki bağlantının adı
URL	İlgili web sitesine bağlantı
Çıkarılabilir	Etkinleştirilirse, kullanıcı web klibini kaldırabilir
Simge	Bu diyalog aracılığıyla bağlantı için bir logo yükleyin: Boyutlar 180x180, png formatı
Önceden Hazırlanmış Simge	Etkinleştirilirse, simge üzerinde hiçbir ek efekt (gölge, yansıma) görüntülenmez
Tam Ekran	Web kliplerini açarken tarayıcı tam ekran modunda açılıyor

Web İçerik Filtresi

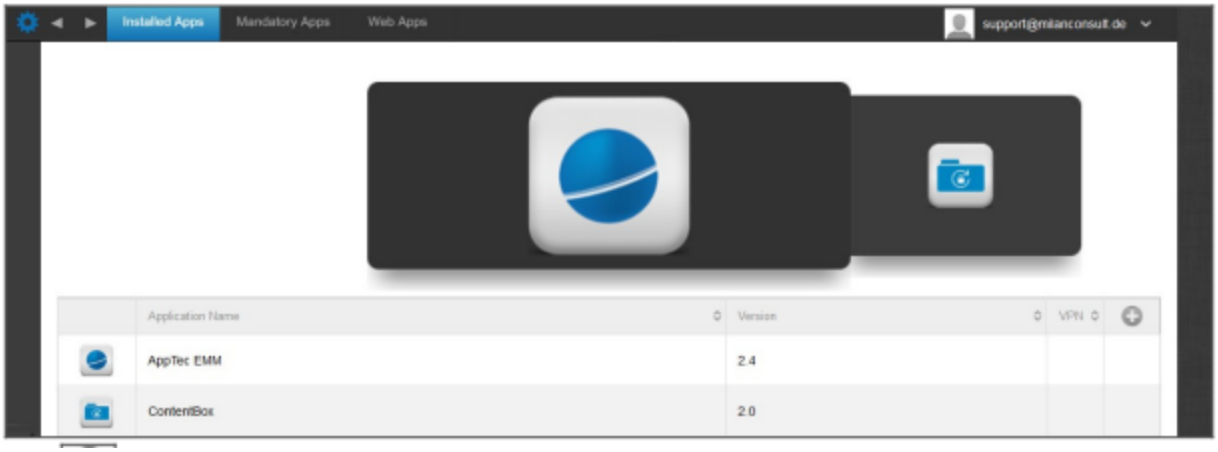
Web İçerik Filtresi, belirli internet sayfalarına erişimi sınırlandırmayı mümkün kılar.

İzin Verilen Web Siteleri	
Yetişkin İçeriğini Sınırlayın	Web filtresi yetişkinlere yönelik içerik için otomatik olarak uygulanır
İzin verilen URL'ler	sembolü ile izin verilen sayfaları ekleyin
Kara Listeye Alınan URL'ler	sembolü ile engellenen sayfaları ekleyin
Yalnızca Belirli Web Siteleri	Yalnızca + sembolü ile ekleyebileceğiniz belirli içerikler görüntülenebilir.

Uygulama Yönetimi

Kurumsal Uygulama Yöneticisi

Yüklü Uygulamalar (yalnızca cihaz düzeyinde)



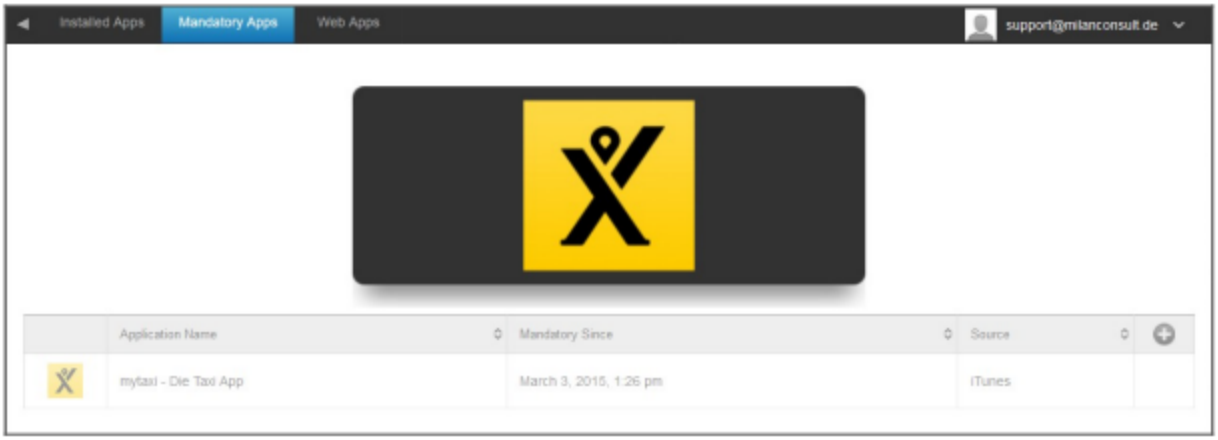
Burada o anda cihazda yüklü olan Uygulamaları görebilirsiniz.

Zorunlu Uygulamalar

Zorunlu Uygulamalar altında, gerekli Uygulamaları zorunlu kılabilirsiniz.

Kullanıcıya söz konusu Uygulamayı yüklemesi sürekli olarak hatırlatılacaktır.

aracılığıyla zorunlu Uygulama tanımlanabilir.



Bu bir Apple App Store Uygulaması olabileceği gibi bir Şirket İçi Uygulama da olabilir.

Bunun denetimli bir cihazı içermesi durumunda, uygulama otomatik olarak yüklenecektir.

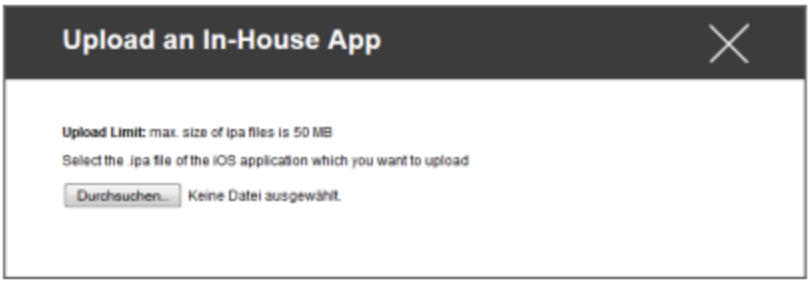
Herkese açık AppStore'dan bir "Apple AppStore" Uygulamasını cihaza gönderebileceğiniz gibi, dahili olarak geliştirilmiş bir Şirket İçi Uygulamayı da cihaza gönderebilirsiniz.

Veya "iOS Şirket İçi Uygulamalar" kategorisinden seçim yapabilir ve Genel Ayarlar altında yüklediğiniz bir Şirket İçi Uygulamayı seçebilirsiniz.

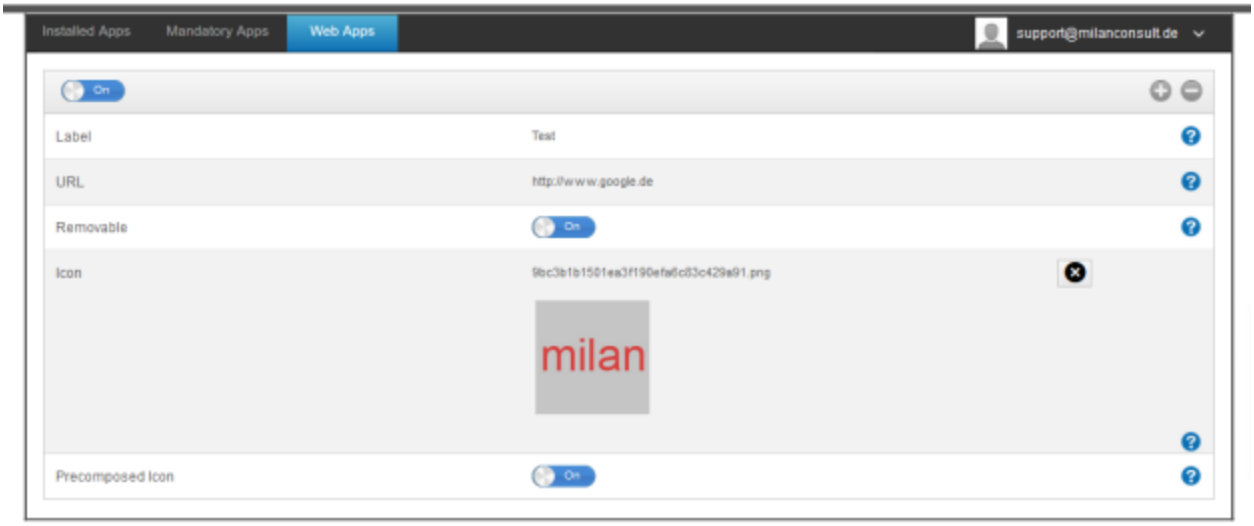
Kurulum seçenekleri

Güncel tutun (yalnızca cihaz başına VPP için desteklenir)	Haftada bir kez, uygulama için bir güncelleme olup olmadığı belirlenecektir. Evet ise, bu güncelleme yüklenecektir Şirket İçi Uygulamalar için Genel Ayarlar'da yapılandırdığınız Güncelleme Hedefi güncelleme işlemi için kullanılacaktır.
Yönetilmediğinde sollama	Uygulama zaten yüklüyse, MDM uygulamayı devralacak ve yönetecektir
MDM profili kaldırıldığında uygulamayı kaldırma	Cihaz yönetiminin kaldırılması durumunda, Uygulama kaldırılacaktır
Uygulama verilerinin yedeklenmesini önleme	Uygulamaya özgü verilerin yedeği oluşturulmayacaktır
Uygulama Ayarı	"Uygulama Ayarları" altında, uygulamaya belirli değerleri ön plana atayabilirsiniz (uygulama desteklediği sürece, gerekirse uygulamanın geliştiricisine sorun).

Ayrıca "Şirket İçi Uygulama Yükle" aracılığıyla doğrudan bir ipa dosyası seçip yükleyebilirsiniz.



Web Uygulamaları



"Web Uygulamaları" başlığı altında, "Web Klipleri" ile benzer şekilde, Web Yönetimi alanında internet sayfalarını veya intranet portallarını son kullanıcı cihazına bir uygulama olarak gönderebilirsiniz. Varsayılan olarak, Web Uygulamaları Webclips altında yapılandırılabilen tam ekran modunda görüntülenecektir.

Etiket	Son kullanıcı cihazındaki bağlantının adı
URL	İlgili Web Sitesine Bağlantı
Çıkarılabilir	Etkinleştirilirse, kullanıcı Webclip'i kaldırabilir
Simge	Bu diyalog aracılığıyla bağlantı için bir logo yükleyin: Boyutlar 180x180, png formatı
Önceden Hazırlanmış Simge	Etkinleştirilirse, simge üzerinde hiçbir ek efekt (gölge, yansıma) görüntülenmez

Kısıtlama ve Ayarlar

Kara Listeye Alınan / Beyaz Listeye Alınan Uygulamalar

Burada, "Genel Ayarlar" bölümündeki ayarlarınıza bağlı olarak engellenen (veya izin verilen) uygulamaları ayarlayabilirsiniz. Bir tıklama bilinen uygulama aramasını getirecektir. Orada eklemek istediğiniz uygulamaları arayabilirsiniz.

Bu işlev için denetlenen bir cihazın gerekli olduğunu unutmayın

SysApp Kısıtlamaları

Cihazınızın belirli uygulamalarını veya işlevlerini engelleme

YouTube kullanımına izin verin	YouTube kullanımına izin verin
iTunes Store'un kullanımına izin ver	iTunes Store'un kullanımına izin ver
Safari kullanımına izin ver	Safari kullanımına izin ver
Otomatik doldurmayı etkinleştir	Otomatik doldurmaya izin verir
Kuvvet dolandırıcılığı uyarısı	Dolandırıcılık uyarısını zorlar
JavScript'i Etkinleştir	JavaScript kullanımını etkinleştirir
Pop-up'ları engelleyin	Her türlü pup-up'ı engeller
Çerezlere İzin Ver	Safari'nin çerezleri ne zaman kabul edeceğini seçme

App-VPN

Sembol aracılığıyla, başlangıçta seçilen VPN bağlantısını otomatik olarak başlatacak uygulamaları tanımlayabilirsiniz.

Uygulama Ayarları

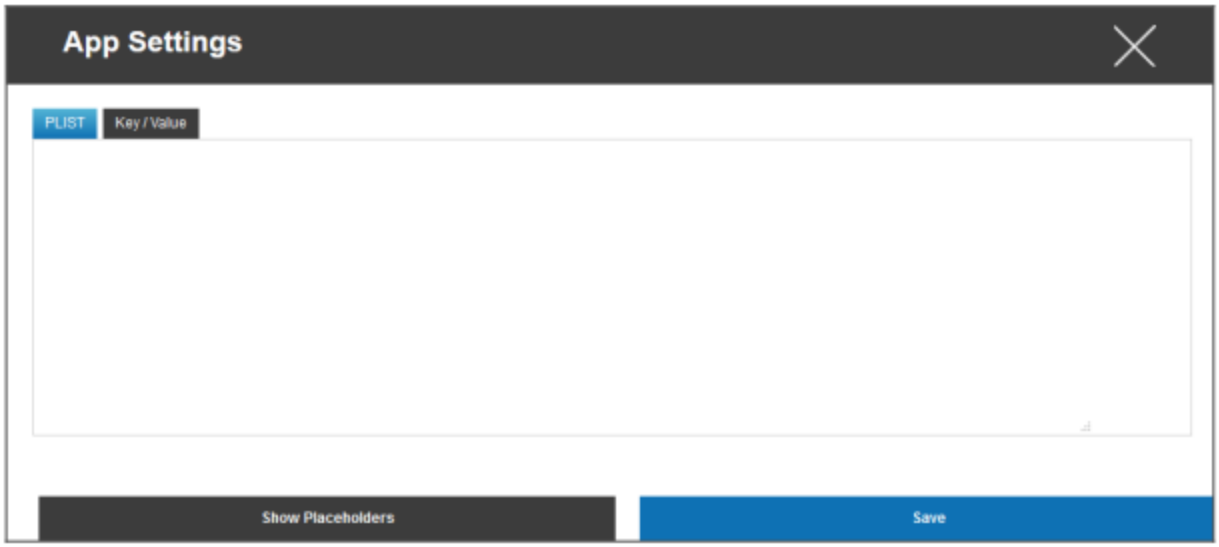
"Uygulama Ayarları" altında, uygulamaya belirli değerleri ön plana atayabilirsiniz (uygulama desteklediği sürece, gerekirse uygulamanın geliştiricisine sorun).

Sembol aracılığıyla bir (ek) uygulama eklersiniz. Bir kez daha AppTec360'ın tanıdık App-Import temsilini bulacaksınız.

Yapılandırmak istediğiniz Uygulamayı burada arayın ve seçin. Ayarlar yalnızca yönetilen uygulamalar için geçerli olacaktır.

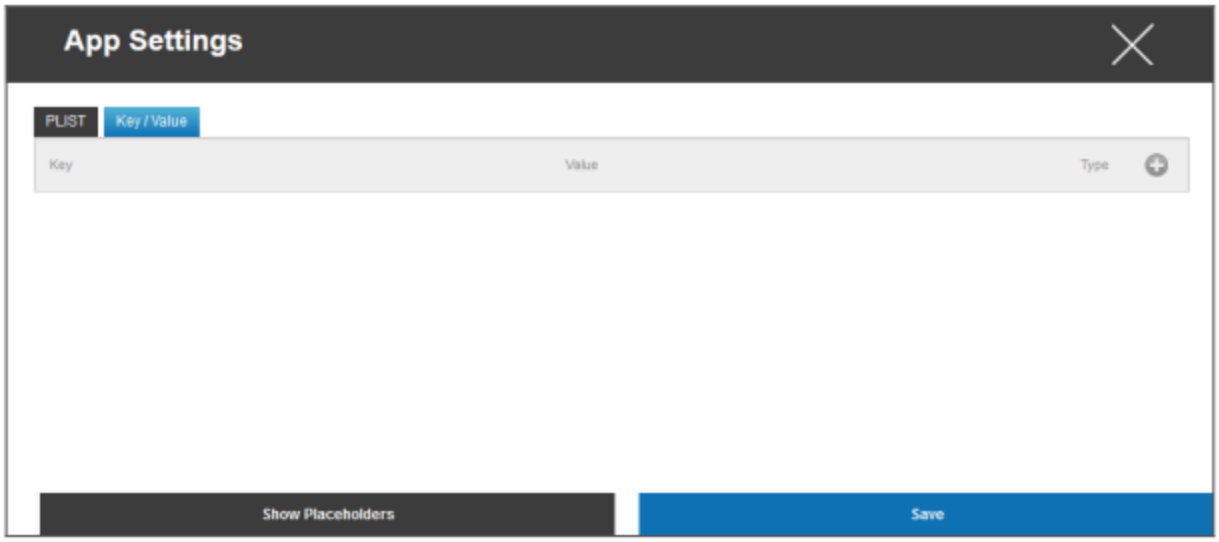
İçe Aktarma işleminin başarılı olması durumunda aşağıdaki ekranı göreceksiniz:

Şimdi, üzerine bir tıklama ile çeşitli yapılandırmalar gerçekleştirebilirsiniz. Daha sonra aşağıdaki genel bakışı alacaksınız:

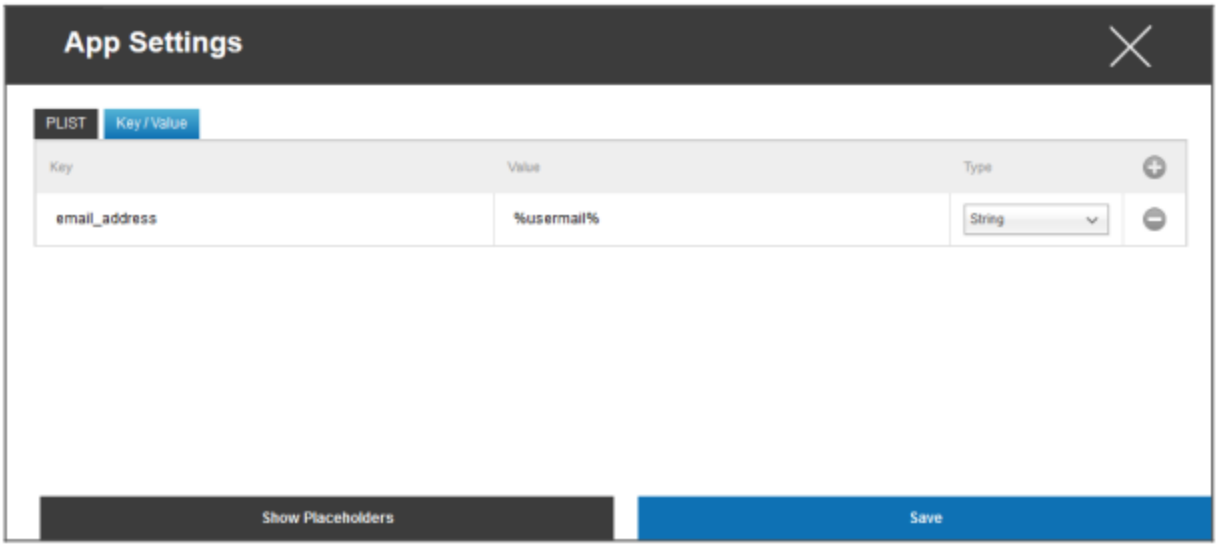


Zaten bir PLIST'iniz (yapılandırmanın kaynak metni) varsa, buraya ekleyebilir ve hepsini "Kaydet" ile kaydedebilirsiniz.

"Anahtar / Değer" altında, Uygulamaya belirli konfigürasyonlar ekleyebilirsiniz



Burada, sembol ile yeni bir anahtar ve değerini oluşturabilirsiniz.



Elbette, AppTec'in tüm yer tutucuları hizmetinizdedir

"Tip" açıklaması:

Dize	Metin
Boolean	Doğru/Yanlış
Sayı	Sayı

Sembol ile bir uygulamayı tekrar kaldırabilirsiniz.

Kurumsal Uygulama Mağazası

iTunes Uygulamaları

Bu noktada, Kullanıcınız için isteğe bağlı Uygulamaları dağıtabilirsiniz.

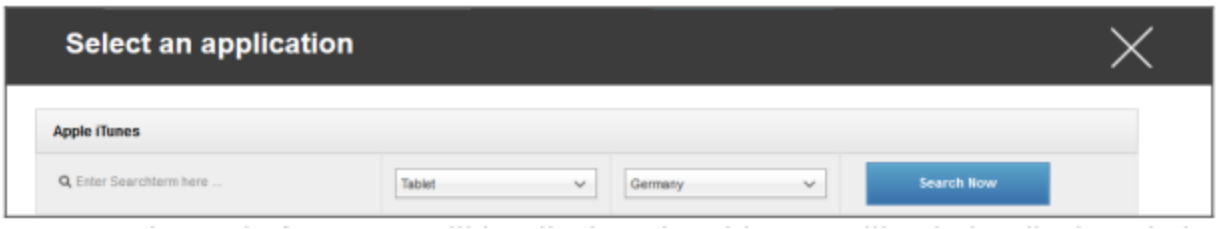
Burada bir Uygulama olması durumunda, AppTec360 Store'un son kullanıcı cihazına otomatik olarak yüklenecektir.

Bunlar sadece resmi Apple App Store'a giden bağlantılardır. Bu nedenle, her son kullanıcı aygıtının bir Apple Kimliği ile donatılması gerekir.

Bu noktada, her kullanıcının kendi Apple Kimliğine sahip olmasını öneririz.

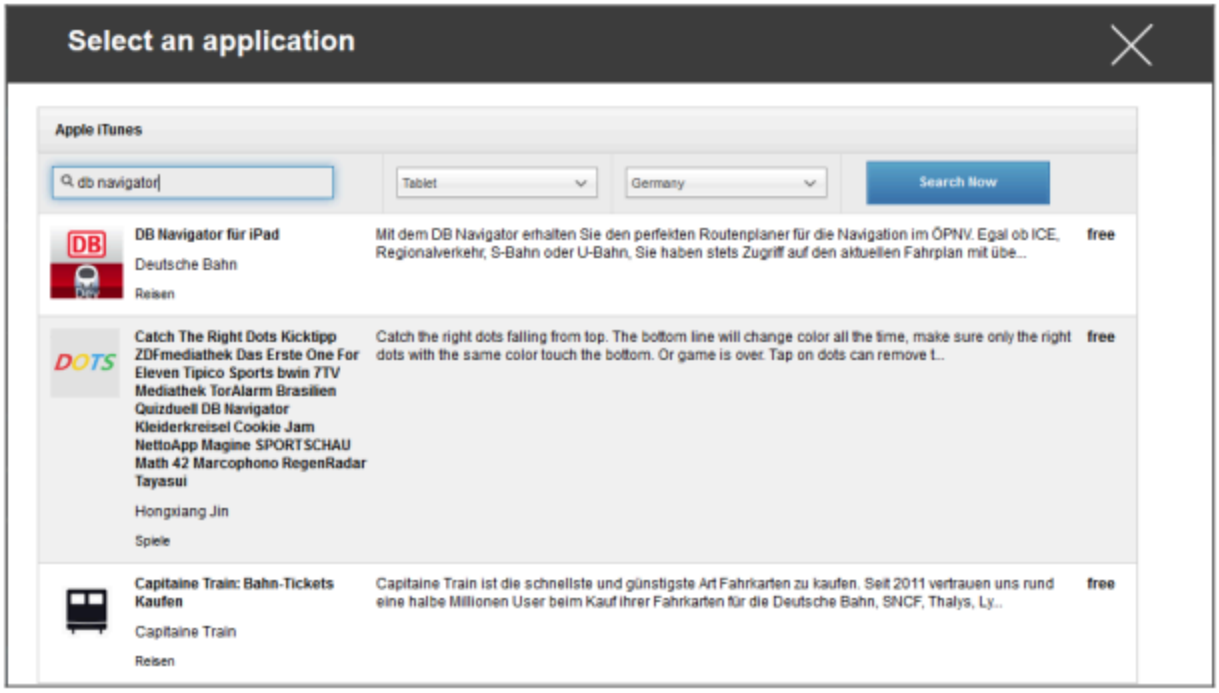
Sembol ile ek Uygulamalar ekleyebilirsiniz.

Bundan sonra, aşağıdaki genel bakışı içeren bir pencere açılmalıdır.



Lütfen yalnızca ücretsiz uygulamaların görüntüleneceğini, ücretli uygulamaların yalnızca VPN aracılığıyla görüntüleneceğini unutmayın.

"Arama Terimini buraya girin..." altında, Apple App Store'da bulunan bir uygulamayı arayabilirsiniz.



Simgeye veya uygulamanın adına tıkladığınızda, ek yapılandırmalar gerçekleştirmeniz tekrar istenecektir.

Güncel kalın	Haftada bir kez, uygulama için bir güncelleme olup olmadığı belirlenecektir. Evet ise, bu güncelleme yüklenecektir
MDM profili kaldırıldığında uygulamayı kaldırma	Cihaz yönetiminin kaldırılması durumunda, Uygulama kaldırılacaktır
Uygulama verilerinin yedeklenmesini önleme	Uygulamaya özgü verilerin yedeği oluşturulmayacaktır
App-VPN	Uygulamayı açtığınızda başlayacak olan bir VPN bağlantısı seçin

"Yükle" düğmesine tıklandıktan sonra uygulama Enterprise App Store'a eklenecek ve AppTec360 AppStore aracılığıyla son kullanıcı cihazına yüklenebilecektir.

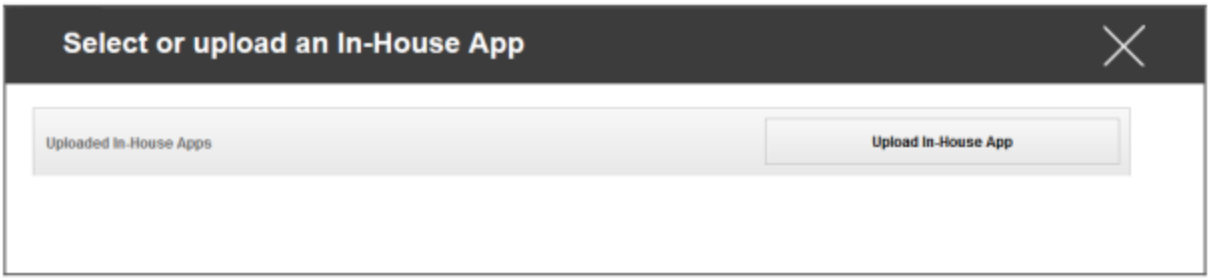
App-Store İçe Aktarma işlemi başarıyla tamamlandıysa, aşağıdaki genel bakışı alacaksınız:

Şirket İçi

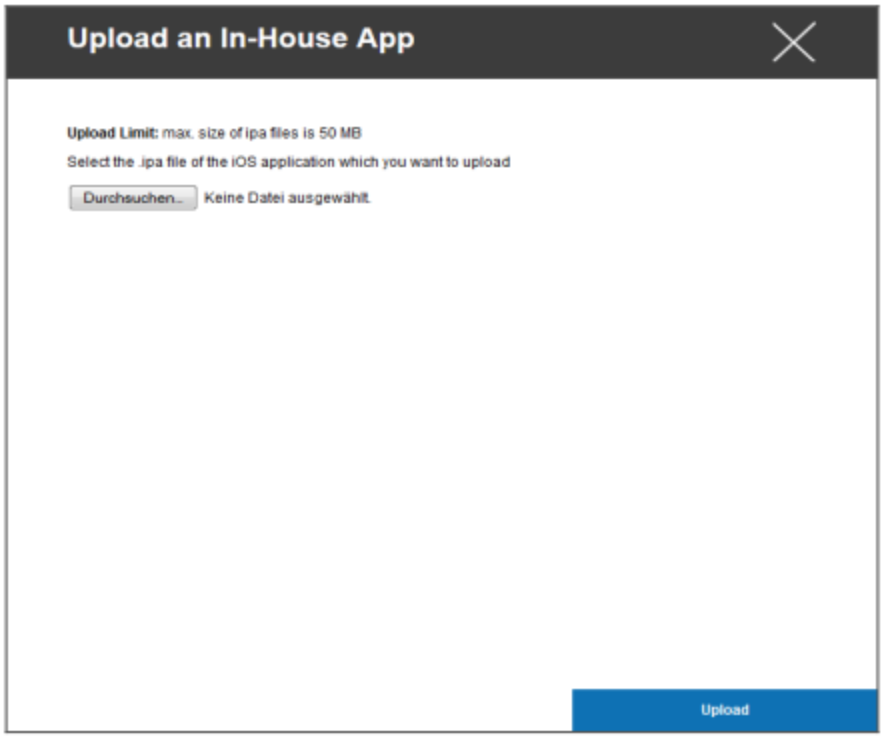
"Şirket İçi" başlığı altında, şirket içinde geliştirilen Uygulamaları yükleyebilir ve dağıtabilirsiniz.

Sembol ile ek Şirket İçi Uygulamaları dağıtabilirsiniz.

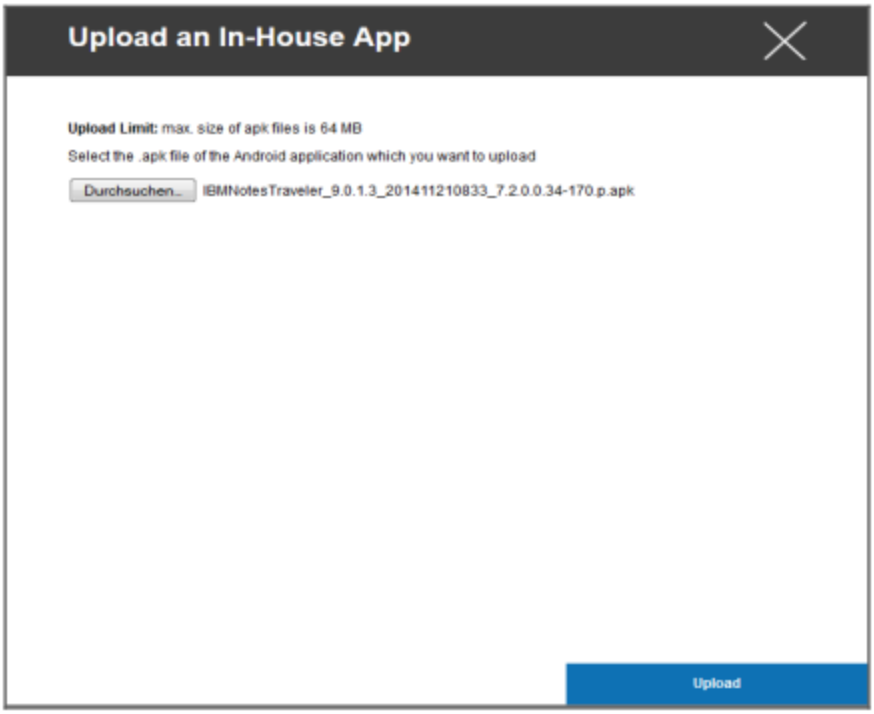
Daha önce hiç Şirket İçi Uygulama dağıtmadıysanız, aşağıdaki genel bakışı alacaksınız:



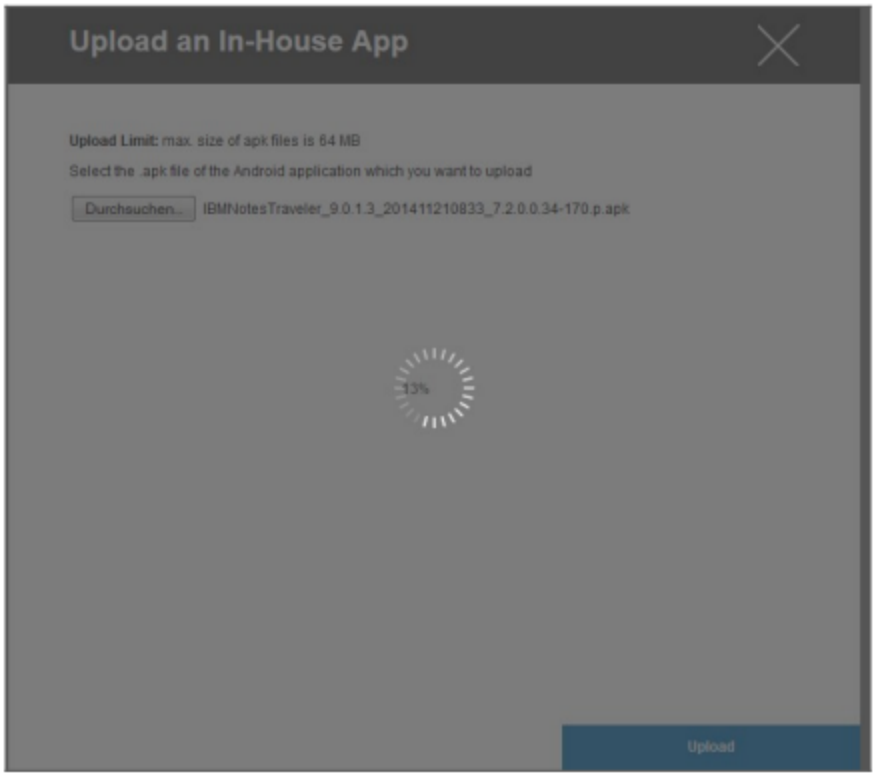
Bunun için "Şirket İçi Uygulama Yükle" seçeneğine tıklayın, ardından aşağıdaki genel bakışı alacaksınız:



Şimdi, "Ara... "yı kullanarak bir .ipa dosyası seçin ve ardından "Yükle "ye tıklayın



Uygulamanız şimdi yüklenecektir. Dairenin ortasında, Uygulamanızın ne kadarının zaten yüklenmiş olduğunun yüzdesini görebilirsiniz.



Şirket İçi Uygulamanın yüklenmesi başarıyla gerçekleştirilmişse, yeni yüklenen uygulamayı Uygulama Kataloğunuzda göreceksiniz.

Kullanıcı artık bu uygulamayı son kullanıcı cihazındaki AppTec360 Mağazasında "Şirket İçi" kategorisi altında görme ve yükleme seçeneğine sahiptir.

Bunun herkese açık bir Apple AppStore Uygulaması içermemesi nedeniyle, kullanıcının son kullanıcı cihazında kayıtlı bir Apple Kimliğine ihtiyacı yoktur.

Kiosk Modu

iOS Kiosk Modu Yalnızca Denetimli Modda Kullanılabilir

Kiosk Modu, bir Uygulamayı veya URL'yi önceden tanımlamanıza olanak tanır, böylece yalnızca bu Uygulamayı/URL'yi çalıştırmak/ziyaret etmek mümkün olur.

Ayrıca, Kiosk Modunda çeşitli donanım düğmelerini devre dışı bırakabilirsiniz.

Uygulama Türü

Paket

Uygulamayı Kiosk Modunda başlatmak istiyorsanız, "Uygulama Türü" altında "Paket "i seçin

Kiosk Uygulaması	Kiosk Modunda başlatılması gereken bir uygulama seçmek için buraya tıklayın Uygulama Yönetiminin güncel genel görünümünü bulacaksınız "Apple iTunes Uygulamaları" ve "iOS Şirket İçi Uygulamaları" arasında seçim yapabilirsiniz

URL

Kiosk Modunda bir URL başlatmak istiyorsanız, "Uygulama Türü" altında "URL "yi seçin

URL	Şimdi, istediğiniz URL adresini tanımlayın
Aynı Menşe Politikası	Bu işlevin etkin olması durumunda, kullanıcı yalnızca önceden tanımlanmış URL'nin alt sayfalarında gezinebilir Örneğin, aşağıdaki URL'yi tanımladıysanız: www.mypage.com, daha sonra kullanıcı www.mypage.com/subpage adresinde gezinebilir
Beyaz Listedeki URL'ler	Burada bir Beyaz Liste tutabilirsiniz, bu URL'lerin tümüne izin verilir Satır başına en fazla 1 URL Bir URL http:/ veya https:// ile başlamalıdır
Kara Listeye Alınan URL'ler	Burada bir Kara Liste tutabilirsiniz, tüm bu URL'lere izin verilmez Satır başına en fazla 1 URL Bir URL http:/ veya https:// ile başlamalıdır
Hareketsizlikten sonra Tarayıcıyı Temizle	Hareketsizlikten sonra Tarayıcı Önbelleği boşaltılacaktır
Çıkış Şifresi Etkin	Bu işlevi etkinleştirirseniz, kullanıcı Kiosk Modunu sizin tarafınızdan önceden tanımlanmış bir parola ile sonlandırma seçeneğine sahip olur
Çıkış Şifresi	Bu, sizin tarafınızdan önceden tanımlanmış olan paroladır

Kiosk Modu Ayarları

Zamanlanmış Kiosk Modu	Günün saatine bağlı olarak Kiosk Modunu ayarlayabilirsiniz, böylece mod önceden belirlenmiş bir zamanda otomatik olarak başlatılır ve sonlandırılır
Başlangıç Zamanı	Başlangıç zamanı
Dakika cinsinden zaman	Kiosk Modunun tekrar sonlandırılması gereken dakika cinsinden süre
Dokunmayı Devre Dışı Bırak	Etkinleştirilirse dokunmatik ekran devre dışı bırakılır
Cihaz Dönüşünü Devre Dışı Bırak	Etkinleştirilirse, otomatik ekran uyarlaması devre dışı bırakılır
Zil Anahtarını Devre Dışı Bırak	Etkinleştirilirse, zil düğmesi devre dışı bırakılır. O andan itibaren, davranış daha önce ayarlanmış olan fonksiyona bağlıdır
Ses düğmelerini devre dışı bırak	Etkinleştirilirse, ses düğmeleri devre dışı bırakılır
Uyku Uyandırma Düğmesini Devre Dışı Bırak	Etkinleştirilirse, açma/kapama düğmesi devre dışı bırakılır
Otomatik Kilidi Devre Dışı Bırak	Etkinleştirilirse, cihaz bekleme moduna geçmez
Seslendirmeyi Etkinleştir	Etkinleştirilirse, Voice Over Assistant etkinleştirilecektir
Yakınlaştırmayı Etkinleştir	Etkinleştirilirse, yakınlaştırma etkinleştirilir
Renkleri Ters Çevirmeyi Etkinleştir	Etkinleştirilirse, ters çevrilmiş ekran modu etkinleştirilir
Assistive Touch'ı Etkinleştir	Etkinleştirilirse, AssistiveTouch etkinleştirilecektir
Konuşma Seçimini Etkinleştir	Etkinleştirilirse, konuşma seçimi etkinleştirilecektir
Mono Sesi Etkinleştir	Etkinleştirilirse, Mono Ses etkinleştirilecektir
VoiceOver	Etkinleştirilirse, kullanıcı VoiceOver'ı etkinleştirebilir
Yakınlaştır	Etkinleştirilirse, kullanıcı Yakınlaştırmayı etkinleştirebilir
Renkleri Ters Çevir	Etkinleştirilirse, kullanıcı ters renkleri etkinleştirebilir
Yardımcı Dokunuş	Etkinleştirilirse, kullanıcı yardımcı dokunmayı etkinleştirebilir

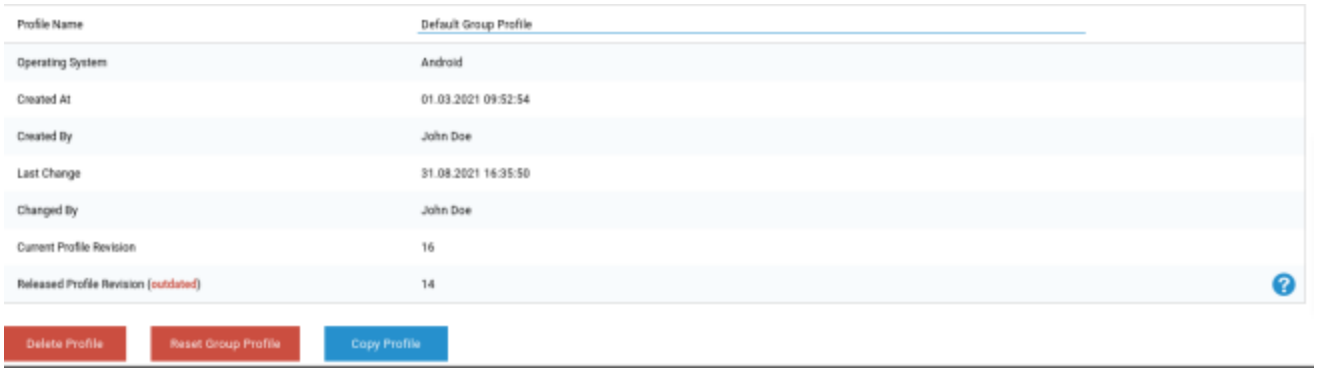
Android Enterprise – Tam Yönetilen Cihaz Yapılandırması

O anda bir grup profili veya bir cihaz seçmiş olmanıza bağlı olarak, genel bakış ve alt noktaları farklılık gösterir - lütfen bunu dikkatlice değerlendirin!

Genel

Grup profiline genel bakış (yalnızca grup düzeyinde)

Bir grup profilini açtığınızda, profile hızlı bir genel bakış elde edersiniz.



Profil Adı	Profilin adı (burada değiştirilebilir)
İşletim Sistemi	Profilin ait olduğu İşletim Sistemi
Şu Adreste Oluşturuldu	Yaratılış zamanı
Tarafından Oluşturuldu	Profilin yaratıcısı
Son Değişiklik	Profilde yapılan son değişikliğin zamanı
Tarafından Değiştirildi	Son değişiklikleri yapan hesap
Güncel Profil Revizyonu	Kayıtlı profil durumunun revizyonu
Profil Revizyonu Yayınlandı	Atanmış profil revizyonu ("Şimdi ata"). Etiket metnin arkasında "(eski)" ibaresini gösteriyorsa, bu profili kaydettiğiniz ancak henüz atamadığınız anlamına gelir, bu nedenle cihazlar hala eski sürümü alacaktır.

Cihaza Genel Bakış (yalnızca cihaz düzeyinde)

Bir cihazda bulunmanız durumunda, seçilen cihazın genel bir özetini alacaksınız, burada aşağıdakiler yer almaktadır:

Cihaz Adı	Cihaz adı
Konum	Konum koordinatları
Telefon Numarası	Telefon numarası
Atanmış Zorunlu Uygulamalar	Atanan Zorunlu Uygulama Sayısı
İşletim Sistemi Sürümü	Cihazın işletim sistemi sürümü
İşletim Sistemi	İşletim Sistemi (Android Enterprise)
Seri Numarası	Cihaz seri numarası
Cihaz Sahipliği	Kurumsal veya özel cihaz
Cihaz Tipi	AE Work Yönetilen Cihaz
Köklü	Cihazın root edilip edilmediğini gösteren durum
Uyumlu	Kılavuza uygun
IP Adresi	Cihazın IP Adresi
Son Görülme	Cihazın AppTec'e en son bağlandığı zaman noktası
Son İtiş	Cihaza son push'un gönderildiği zaman noktası
AE Cihaz Sahibi Modu	Evet
Kullanıcı Ataması	Bu cihazın atandığı kullanıcı veya grup

Konfigürasyon Revizyonu (sadece cihaz seviyesinde)

Burada cihaza hangi grup profilinin atandığına dair bir genel bakış elde edersiniz.

Grup profiline tıklarsanız, bu profile doğrudan erişim sağlarsınız ve ayarları gerçekleştirebilirsiniz.

Bu sembolle, dağıtılan uygulamaları grup profilinin ayarlarına geri döndürebilirsiniz.

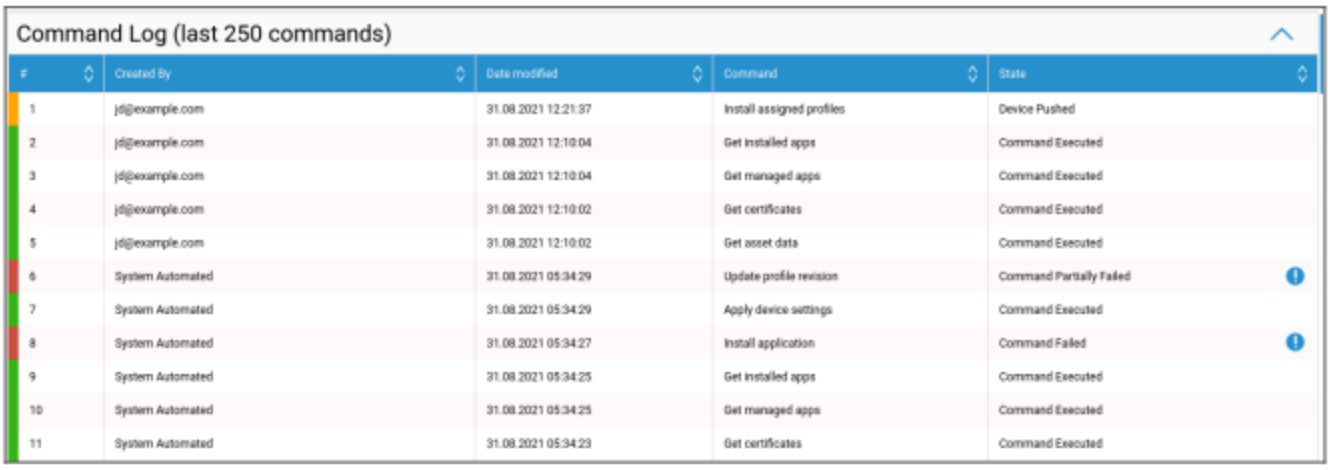
Bu sembolle, kullanılan tüm uygulamaları grup profilinin ayarlarına geri döndürebilirsiniz.

"Newer Revision available" grup profilinin değiştirildiğini ve kaydedildiğini ancak atanmadığını gösterir. Değişiklikleri cihazlara uygulamak için grup profilinin grup düzeyinde "Şimdi ata" ile atanması gerekir.

Cihaz Günlüğü (yalnızca cihaz düzeyinde)

Komut Günlüğü

Burada cihaz için hangi komutların verildiğini ve durumlarının ne olduğunu görebilirsiniz.



"System Automated" tarafından oluşturulan komutlar sistem tarafından otomatik olarak oluşturulur.

Olası komut durumları

Cihaz İtildi	Cihaza EMM sunucusuna geri bağlanmasını söylemek için push hizmetine (örn. APNS) bir push isteği gönderilmiştir.
Komut Oluşturuldu	Komut sistemde oluşturuldu.
Gönderilen Komut	Komut, sunucuya bağlandıktan sonra cihaza gönderildi.
Komut Yürütüldü	Komut başarıyla yürütüldü.
Komut Başarısız	Komut başarısız oldu. *
Komut Kısmen Başarısız	Cihazın işletim sistemine bağlı olarak bazı komutlar birlikte gruplandırılabilir. Bu komut grubunun bazı bölümleri başarısız olmuştur. *
Komut Yürütüldü, sonunda Başarısız Oldu	Komut uygulandı ama belki de uygulanmadı.
Komut Tekrar Gönderildi	Komut bir kullanıcı tarafından yeniden itildi.
Atılmış	Komut iptal edildi. Örneğin, başka bir komutun yerini aldığı için veya cihaz yeniden kaydedildiği ve eski komutlar kaldırıldığı için

Mesajın arkasında bir ünlem işareti varsa, imlecinizi simgenin üzerine getirerek daha fazla bilgi alabilirsiniz.

Cihaz Ayarları

İstemci Yapılandırması

Burada Android cihazınızda aşağıdaki yapılandırmaları gerçekleştirebilirsiniz:

Uyumluluk Dışı Zaman	Zorlama eyleminin uygulanacağı kullanıcı yanıtı zaman aşımı sınırı.
Uyum zaman aşımından sonra yaptırım eylemi	Bir kullanıcı uyumlu bir cihaz durumuna yol açan eylemleri gerçekleştirmediğinde yaptırım eylemi
Veri Toplama Sıklığı	Cihaz/GPS bilgilerinin toplanma sıklığı
Cihaz Kalp Atışı Frekansı	Cihazın AppTec360 Sunucusu ile iletişime geçmesi gereken aralık Min. 1 dakika Max. 24 saat
Konum Güncellemelerini Etkinleştir	Etkinleştirilirse, cihaz konum güncellemelerini AppTec360 Sunucusuna gönderir
Konum Güncelleme Zamanı	Cihazın AppTec360'a konum güncellemelerini hangi zaman aralıklarında göndereceğini belirler
Konum Güncellemesi için Google Konum Doğruluğunu Kullanın	Etkinleştirilirse, konum güncellemeleri için ağ konumu kullanılacaktır ("Kısıtlamalar" altında devre dışı bırakılmışsa, bu ayar hiçbir şeyi etkilemeyecektir)
Konum Güncellemesi için GPS Konumunu Kullanın	Etkinleştirilirse, konum güncellemeleri için GPS kullanılacaktır
Sahte (Fake) Konumlara İzin Ver	Üçüncü taraf uygulamalar aracılığıyla konum bilgilerinin sahtesinin yapılmasına izin verir
Kayıp Bağlantı Eylemi	Etkinleştirilirse, bir cihazın kalp atışı aralığında MDM sunucusuyla bağlantı kurmaması durumu için bir eylem belirleyebilirsiniz. Örneğin, cihazın 5 dakikalık bir kalp atışı süresi varsa, sunucuya saat 10:35'te bağlanır. Bundan sonra cihaz Wi-Fi menzilinden çıkar. Saat 10:40'taki bir sonraki kalp atışı başarısız olacak ve belirtilen eylem gerçekleştirilecektir.
Eylem	Bir cihaz uyumsuz hale gelir gelmez gerçekleştirilecek eylem.

	• Kilit Cihazı = kilit cihazı • Cihazı Sil = cihaz fabrika ayarlarına geri yüklenir • Cihazı ve SD Kartı Sil = cihaz fabrika ayarlarına geri yüklenecek ve SD Kart depolama alanı silinecektir
Eşik	Belirtilen eylemi tetiklemek için gerekli olan başarısız Kalp Atışı eşiğini belirleyebilirsiniz.

İlke Uygulama Modu	Varsayılan değer:	Kullanıcılardan periyodik olarak bekleyen eylemleri gerçekleştirmeleri istenecektir
	Tembel Politika Uygulaması:	Kullanıcılardan hiçbir zaman bekleyen eylemleri gerçekleştirmeleri istenmeyecektir. Tüm açık eylemler AppTec360 İstemcisinde gösterilecektir
	Agresif Politika Uygulaması:	Kullanıcılardan bekleyen eylemleri gerçekleştirmeleri için durmaksızın bilgi istenecektir
AppTec360 Sürüm Kilidi	Etkinleştirilirse, AppTec360 MDM İstemcisi için bir sürüm kodu belirtilebilir. AppTec360 istemcisi yalnızca belirtilen sürüme güncellenecektir. Daha yeni sürümler göz ardı edilecektir. Düşürme mümkün DEĞİLDİR.	
Sürüm Kodu	AppTec360 MDM İstemcisinin kilitleneceği sürüm kodu.	
AppTec360 Bildirimini Devre Dışı Bırak	Devre dışı bırakılırsa AppTec360 İstemcisi Bildirim Çubuğunda bir Bildirim göstermez. Böylece kullanıcılar AppTec360 istemcisini görev yöneticisi aracılığıyla kapatabilir. AppTec360 istemcisi kapalıysa, Kiosk Modu ve Uygulama Siyah / Beyaz Listeleme gibi çeşitli özellikler düzgün çalışmayacaktır. Samsung cihazları AppTec360 İstemcisi için bir koruma mekanizması sunar. KNOX API'lerini destekleyen Samsung cihazlarında bildirim varsayılan olarak devre dışıdır. Bildirim, Android 8.0 veya üzeri sürümlere sahip cihazlarda devre dışı bırakılmamalıdır.	

Duvar Kağıdı

Özel Duvar Kağıdı Ayarla	Özel duvar kağıdını etkinleştirme/devre dışı bırakma
Duvar Kağıdı	Duvar kağıdı modunu bir renk kodu veya bir resim kullanacak şekilde ayarlama
Bir Renk Belirtin	Arka plan rengini hex değeri olarak belirtin, örneğin siyah için #000000 veya beyaz için #ffffff
Resmi Duvar Kağıdı Olarak Ayarla	Duvar kağıdı olarak kullanmak istediğiniz resim dosyasını yükleyin

Varlık Yönetimi (yalnızca cihaz düzeyinde)

Cihaz Bilgisi

Model	Cihaz model tanımı
İşletim Sistemi	İŞLETIM SISTEMI
İşletim Sistemi Sürümü	İşletim sistemi sürümü
Seri Numarası	Seri numarası
Cihaz Adı	Cihaz adı
Pil Durumu	Pil durumu
Boş / Toplam Bellek	Boş / Toplam bellek
Samsung Safe	Samsung SAFE arayüzü, çeşitli ayar seçenekleri için gereklidir
SD Kart Mevcut	SD Kart mevcut
SD Kart Emülasyonlu	SD Kart emülasyonu
SD Kart Çıkarılabilir	SD Kart çıkarılabilir
SD Boş / Toplam Bellek	SD Boş / Toplam SD Kart belleği

Wi-Fi

IP Adresi	Cihaz IP adresi
WiFi MAC	WiFi MAC adresi

Hücresel

Durum	Durum (SIM kart takılı)
Telefon Numarası	Telefon Numarası
Dolaşım (Ses / Veri)	Ses / veri için dolaşım
Dolaşım Durumu	Mevcut dolaşım durumu
IP Adresi	IP adresi
Operatör/Taşıyıcı	Operatör/Taşıyıcı
Hücresel Teknoloji	Hücresel Teknoloji
IMEI	IMEI numarası
ICCID	Bu, SIM kartın kimliğidir, çoğu zaman bir Akıllı Kart veya Entegre Devre Kartı (ICC) da olabilir
IMSI	Uluslararası Mobil Abone Kimliği (IMSI), GSM ve UMTS mobil ağlarında ağ kullanıcılarının kesin bir şekilde tanımlanmasını sağlar IMSI en fazla 15 basamaktan oluşur ve aşağıdaki şekilde yapılandırılır: • Mobil Ülke Kodu (MCC), 3 basamaklı • Mobil Ağ Kodu (MNC), 2 veya 3 basamaklı • Mobil Abone Kimlik Numarası (MSIN), 1-10 hane
Mevcut MCC/MNC	Bkz. "SIM MCC/MNC"
SIM MCC/MNC	Mobil Ülke Kodu, E.212 uyarınca ITU tarafından belirlenen yerleşik bir ülke tanımlayıcısıdır Standart. Bu, mobil ağın tanımlanması için Mobil Ağ Kodu (MNC) ile birlikte çalışır. SIM kartın ülke/Mobil Ağ Kodu anlamına gelir. Başka bir mobil ağda dolaşım yaparsanız, mantıksal olarak "Mevcut MCC/MNC" ve "SIM MCC/MNC" farklı olacaktır.

Bluetooth

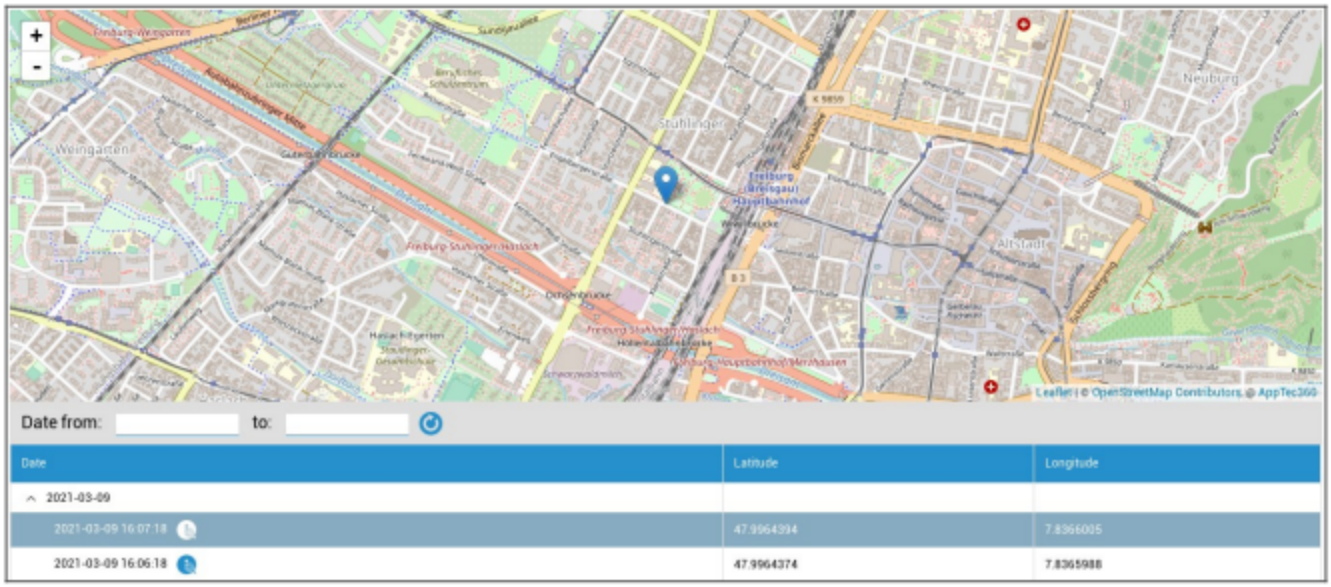
Bluetooth MAC	Bluetooth MAC adresi

Güvenlik Yönetimi

Hırsızlığa Karşı Koruma (yalnızca cihaz düzeyinde)

GPS Bilgileri (yalnızca cihaz düzeyinde)

Burada mevcut/son cihaz konumunu belirleyebilirsiniz. Yerelleştirme bir veya iki parola ile korunabilir - Bkz: Genel Ayarlar - Gizlilik - GPS Erişimi



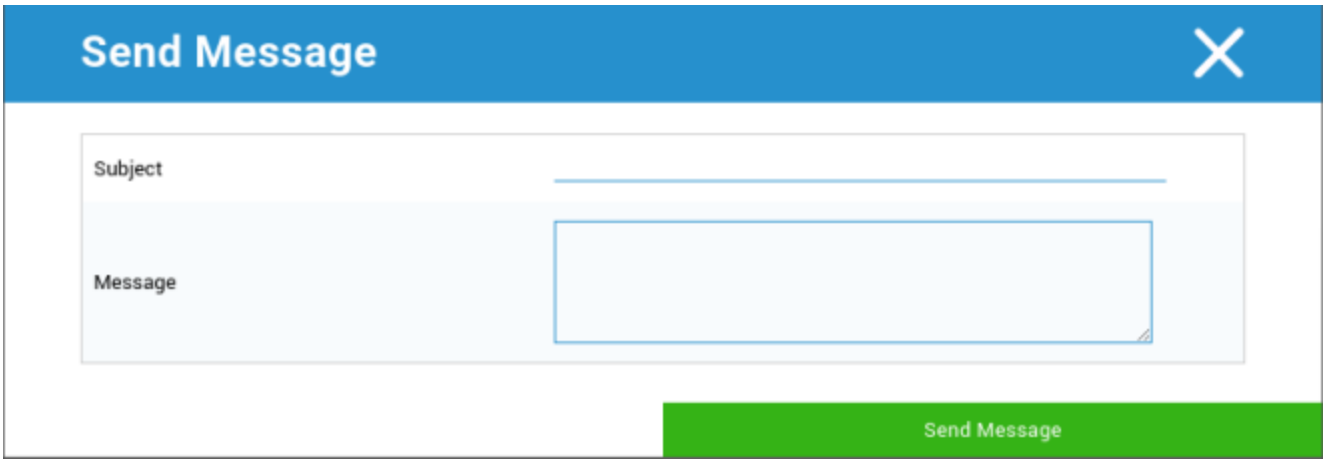
Sil ve Kilitle (yalnızca cihaz düzeyinde)

"Sil ve Kilitle" altında aşağıdaki üç eylemi gerçekleştirebilirsiniz:

Tam Silme	Cihaz fabrika ayarlarına geri döndürülür (kurumsal ve kişisel veriler silinir)
Kurumsal Silme	Son kullanıcı cihazından yalnızca kurumsal veriler kaldırılır (AppTec360 tarafından sağlanan tüm uygulamalar, veriler vb.)
Kilit Ekranı	Ekran kilidi etkinleştirildiğinde, cihazın kilidini cihaz şifresi/PIN ile açmak yeterlidir

Mesaj (yalnızca cihaz düzeyinde)

Burada konuyu ve mesajı doldurabilir ve bir son kullanıcı cihazına gönderebilirsiniz.



Güvenlik Yapılandırması

Cihaz Parolası

"Parola" altında bir cihaz parolası belirleyebilirsiniz, aşağıdaki ayar seçeneklerini kullanabilirsiniz

Minimum parola uzunluğu	Bir parolanın sahip olması gereken minimum sembol sayısını belirler	
Şifre kalitesi	Belirtilmemiş	Bu politikada parola için herhangi bir gereklilik yoktur.
	Biyometrik Zayıf	Bu politika, düşük güvenlikli biyometrik tanıma teknolojisine izin vermektedir. Bu, bir bireyin kimliğini yaklaşık 3 haneli bir PIN koduna kadar tanıyabilen teknolojiler anlamına gelir (yanlış algılama 1.000'de 1'den azdır).
	Bir şey	Bu ilke, bir tür parola veya kalıp belirlenmesini gerektirir, ancak herhangi bir özel kural uygulamaz.
	Alfabetik	Kullanıcı en az alfabetik (veya diğer sembol) karakterler içeren bir parola girmiş olmalıdır.
	Alfanümerik	Kullanıcı, en az hem sayısal hem de alfabetik (veya diğer sembol) karakterleri içeren bir parola girmiş olmalıdır.
	Kompleks	Kullanıcı, varsayılan olarak en az bir harf, bir rakam ve bir özel sembol içeren bir parola girmiş olmalıdır. Bu parola kalitesiyle, parolalar en az bir büyük harf vb. gibi çeşitli karakter kümeleri içerecek şekilde kısıtlanabilir.
Minimum parola uzunluğu	Parola için gerekli karakter sayısını ayarlayın. Örneğin, PIN veya parolaların en az altı karakterden oluşmasını zorunlu tutabilirsiniz.	
Parolada gerekli minimum sayısal basamaklar	Parolada gerekli minimum sayısal basamaklar	
Parolada gereken minimum küçük harf sayısı	Parolada gereken minimum küçük harf sayısı	
Parolada gerekli minimum büyük harfler	Parolada gerekli minimum büyük harfler	

Parolada gerekli minimum harf dışı karakterler	Parolada gerekli minimum harf dışı karakterler
Parolada gereken minimum semboller	Parolada gereken minimum semboller

Maksimum hareketsizlik süresi kilidi	Zaman kilidine kadar maksimum kullanıcı hareketsizliği
Parola sona erme zaman aşımı	Oluşturur, hangi zaman aralığından sonra parolanın süresi dolar ve yeni bir parola verilmelidir
Parola geçmişi kısıtlaması	İzin verilmeyen önceden kullanılmış şifre sayısı
Maksimum başarısız parola denemesi	Tam bir cihaz silme işlemi gerçekleştirilmeden önce bir parolanın ne kadar sıklıkla yanlış girilebileceğini belirler
Biyometrik Kimlik Doğrulamaya İzin Ver	Parmak izi veya iris taraması yoluyla kimlik doğrulamayı etkinleştirir. Sadece Samsung KNOX 2.1 ve üstü için

AntiVirüs

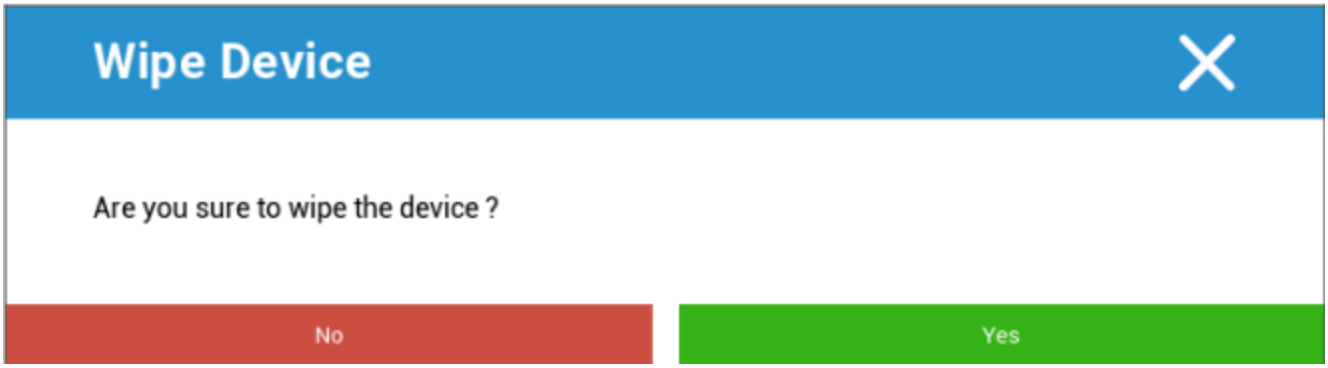
Otomatik Tarama	Periyodik otomatik taramaları etkinleştirin
Tarama Aralığı	Muayene aralığı (Hızlı / Tam)
Tam Otomatik Tarama	Tam otomatik taramaları etkinleştirin
Otomatik Güncellemeler	Otomatik güncellemeleri etkinleştirin
Güncelleme Kontrol Aralığı	Uygulamanın ve veritabanının ne sıklıkla güncellenmesi gerektiği (virüsler / hasarlı kod)
Uygulama Koruması	Otomatik uygulama taramasını etkinleştirin
SD Kart Koruması	Otomatik SD Kart taramasını etkinleştirin
Yalnızca Wi-Fi Güncellemesi	Etkinleştirildiğinde, güncellemeler yalnızca cihaz bir Wi-Fi ağına başarıyla bağlandığında uygulanır

Kullanım Ömrü Sonu (yalnızca cihaz düzeyinde)

Silme (yalnızca cihaz düzeyinde)

"Sil" altında, cihazı fabrika ayarlarına geri yükleyebilirsiniz. Burada kurumsal verilerin yanı sıra özel veriler de son kullanıcı cihazında silinecektir.

"Eksi Sembolü" üzerine tıkladığınızda aşağıdaki mesajı alırsınız:



"Evet" ile silme işlemini gerçekleştirebilirsiniz.

"Silme Raporu" altında aşağıdaki öğeler görüntülenebilir

Tarafından silindi	Silme işlemini kimin yaptığına dair tarihçe
Tarih	Tarih
Durum	Durum (örn. Silme işlemi başarıyla gerçekleştirildiyse)

Kısıtlama Ayarları

Kısıtlamalar

Burada, çeşitli şeyler kısıtlanabilir ve engellenebilir.

Kamerayı Etkinleştir	Kamera kullanımına izin verin	
Otomatik Senkronizasyonu Zorla	Açık	Senkronizasyon kalıcı olarak etkinleştirilir
	Kapalı	Senkronizasyon kalıcı olarak devre dışı bırakılır
	Kullanıcı seçimi	Kullanıcı tarafından seçilir
Bluetooth'u Zorla	Açık	Bluetooth kalıcı olarak etkinleştirilir
	Kapalı	Bluetooth kalıcı olarak devre dışı bırakıldı
	Kullanıcı seçimi	Kullanıcı tarafından seçilir
Kuvvet GPS	Açık	GPS kalıcı olarak etkinleştirilir
	Kapalı	GPS kalıcı olarak devre dışı bırakıldı
	Kullanıcı seçimi	Kullanıcı tarafından seçilir
Kuvvet Ağı Konumu	Açık	Kalıcı internet lokalizasyonu
	Kapalı	İnternet lokalizasyonunun kalıcı olarak devre dışı bırakılması
	Kullanıcı seçimi	Kullanıcı tarafından seçilir

Güvenlik		
Paylaşım Konumuna İzin Verme	Bir kullanıcının konum paylaşımını açmasına izin verilmeyip verilmeyeceğini belirtir.	
Güvenli Önyüklemeye İzin Verme	Kullanıcının cihazı güvenli önyükleme modunda yeniden başlatmasına izin verilmeyip verilmeyeceğini belirtir.	
Ağ Sıfırlamaya İzin Verme	Bir kullanıcının Ayarlar'dan ağ ayarlarını sıfırlamasına izin verilip verilmeyeceğini belirtir.	
Fabrika ayarlarına sıfırlamaya izin verme	Bir kullanıcının cihazı sıfırlamasına izin verilmeyip verilmeyeceğini belirtir.	
ADB'yi Etkinleştir	ADB aracılığıyla bir PC'ye Bağlantıya İzin Verir	
Keyguard'ı Devre Dışı Bırak	Keyguard'ı devre dışı bırakır	
Cihaz Sahibi Kilit Ekranı Bilgisi	Kilit ekranında gösterilecek cihaz sahibi bilgilerini ayarlar.	
Uyum Uygulama	Mod İstemi Kullanıcı	Kullanıcıdan gerekli eylemleri yerine getirmesi istenecektir.
	Mod Kilitleme Konteyneri	Tüm gereksinimler karşılanana kadar tüm uygulamaları gizleyin

Uygulama Yönetimi	
Çapraz Profil Uygulama Bağlantısına İzin Ver	Üst profildeki uygulamaların yönetilen profildeki web bağlantılarını işlemesine izin verir.
Uygulama Kontrolüne İzin Verme	Bir kullanıcının Ayarlar veya başlatıcılardaki uygulamaları değiştirmesine izin verilmeyip verilmeyeceğini belirtir.
Uygulama Yüklemesine İzin Verme	Bir kullanıcının uygulama yüklemesine izin verilmeyip verilmeyeceğini belirtir.
Kaldırma Uygulamalarına İzin Verme	Bir kullanıcının uygulamaları kaldırmasına izin verilmeyip verilmeyeceğini belirtir.
Çalışma Zamanı İzin Politikası	Uygulamalardan gelen yeni izin isteklerinin nasıl ele alınacağını belirtir.
Bilinmeyen Kaynaklara İzin Ver	Etkinleştirilirse, kullanıcılar bir .apk dosyası yükleyerek Uygulamaları yandan yükleyebilir.

Bağlanabilirlik	
Mobil Ağ Yapılandırmasına İzin Verme	Bir kullanıcının mobil ağları yapılandırmasına izin verilmeyip verilmeyeceğini belirtir.
Tethering Yapılandırmasına İzin Verme	Bir kullanıcının Tethering ve taşınabilir hotspot'ları yapılandırmasına izin verilmeyip verilmediğini belirtir.
VPN Yapılandırmasına İzin Verme	Bir kullanıcının VPN yapılandırmasına izin verilmeyip verilmeyeceğini belirtir.
Wifi Yapılandırmasına İzin Verme	Bir kullanıcının WiFi erişim noktalarını değiştirmesine izin verilmeyip verilmeyeceğini belirtir.
Giden NFC Işınına İzin Verme	Kullanıcının uygulamalardan veri ışınlamak için NFC kullanmasına izin verilmeyip verilmeyeceğini belirtir.
WiFi Yapılandırmasını Kilitle	Bu ayar, bir Cihaz Sahibi uygulaması tarafından oluşturulan WiFi yapılandırmalarının kilitli olup olmayacağını kontrol eder (yani, Ayarlar uygulaması tarafından bile değil, yalnızca Cihaz Sahibi Uygulaması tarafından düzenlenebilir veya kaldırılabilir).
Veri Dolaşımını Etkinleştir	Veri Dolaşımını Etkinleştirir

Bluetooth	
Bluetooth'a İzin Verme	Cihazda bluetooth'a izin verilip verilmediğini belirtir. Android 8.0 gerektirir
Bluetooth Paylaşımına İzin Verme	Cihazda giden bluetooth paylaşımına izin verilmeyip verilmediğini belirtir. Android 8.0 gerektirir
Bluetooth Yapılandırmasına İzin Verme	Bir kullanıcının bluetooth yapılandırmasına izin verilmeyip verilmediğini belirtir.

Hesap Yönetimi	
Yönetilen profil eklemeye izin verme	Bir kullanıcının yönetilen profiller eklemesine izin verilmeyip verilmeyeceğini belirtir. Android 8.0 gerektirir
Kullanıcı eklemeye izin verme	Bir kullanıcının yeni kullanıcı eklemesine izin verilmeyip verilmeyeceğini belirtir.
Yönetilen Profili Kaldırmaya İzin Verme	Bu kullanıcının yönetilen profillerinin, profil sahibi dışında kaldırılıp kaldırılamayacağını belirtir. Android 8.0 gerektirir
Hesap Değişikliğine İzin Verme	Authenticator tarafından programlı olarak eklenmediği sürece, bir kullanıcının hesap ekleme ve kaldırma işlemlerine izin verilmeyip verilmeyeceğini belirtir.

Telefon	
Giden Çağrılara İzin Verme	Kullanıcının giden telefon aramaları yapmasına izin verilmediğini belirtir.
SMS'e İzin Verme	Kullanıcının SMS mesajları göndermesine veya almasına izin verilmediğini belirtir.

Sistem	
Pencere Oluşturmaya İzin Verme	Uygulama pencereleri dışındaki pencerelerin oluşturulmaması gerektiğini belirtir.
Kullanıcı Simgesini ayarlamaya izin verme	Bir kullanıcının simgesini değiştirmesine izin verilmeyip verilmeyeceğini belirtir.
Duvar Kağıdı Ayarlamaya İzin Verme	Duvar kağıdı ayarlamaya izin vermemek için kullanıcı kısıtlaması.
Durum Çubuğunu Devre Dışı Bırak	Durum çubuğunun devre dışı bırakılması, tek kullanımlık bir cihazdan kaçmayı sağlayan bildirimleri, hızlı ayarları ve diğer ekran kaplamalarını engeller.
Otomatik Zamanı Etkinleştir	Saati otomatik olarak ayarlar.
Otomatik Saat Dilimini Etkinleştir	Saat dilimini otomatik olarak ayarlar.
Fişe takılıyken açık kalma	Cihaz bir güç kaynağına bağlıyken aktif kalacaktır.

Depolama	
Uygulama Doğrulamayı Devre Dışı Bırak	Bir kullanıcının uygulama doğrulamasını devre dışı bırakmasına izin verilip verilmeyeceğini belirtir.
Fiziksel Ortam Montajına İzin Verme	Bir kullanıcının fiziksel harici medyayı monte etmesine izin verilmeyip verilmeyeceğini belirtir.
Yedekleme Hizmetini Etkinleştir	Yedekleme hizmeti cihazdaki tüm yedekleme ve geri yükleme mekanizmalarını yönetir. Bunun false olarak ayarlanması verilerin yedeklenmesini veya geri yüklenmesini engeller. Yedekleme hizmeti varsayılan olarak kapalıdır. Android 8.0 gerektirir
USB Yığın Depolamayı Etkinleştir	USB Yığın Depolama kullanımını etkinleştirir.

Klavye	
Otomatik Doldurmaya İzin Verme	Bir kullanıcının Otomatik Doldurma Hizmetlerini kullanmasına izin verilip verilmediğini belirtir. Android 8.0 gerektirir
Profiller Arasında Kopyalama ve Yapıştırmaya İzin Verme	Bu profilin panosuna kopyalananların ilgili profillere yapıştırılıp yapıştırılamayacağını belirtir.

Ses	
Hacim Ayarlamasına İzin Verme	Bir kullanıcının ana ses seviyesini ayarlamasına izin verilmeyip verilmeyeceğini belirtir.
Mikrofonun Sesini Açmaya İzin Verme	Bir kullanıcının mikrofon ses düzeyini ayarlamasına izin verilmeyip verilmeyeceğini belirtir.
Sessiz Aygıt	Sessiz cihaz.

Sertifika Yönetimi

Burada Güvenilir Sertifikaları ve Kimlik Sertifikalarını cihazlarınıza dağıtabilirsiniz.

Güvenilir Sertifikaları dağıtmak için Android 8 veya üstü, Kimlik Sertifikalarını dağıtmak için ise Android 9 veya üstü gereklidir.

"+" ile birden fazla sertifika ekleyebilirsiniz.

Güvenilir Sertifikaların PEM formatında olması gerekir.

Kimlik Sertifikalarının PKCS12 formatında olması gerekir

Bağlantı Yönetimi

Wifi

Bu ayar için, dahili Erişime erişim için son kullanıcı cihazlarının ön yapılandırmasını gerçekleştirin Puanlar

Hizmet Seti Tanımlayıcısı (SSID)	Bağlanılacak ağ için SSID
Gizli Ağ	AP'nin SSID'yi yayınlamaması durumunda etkinleştirin

Güvenlik Türü

AP'nin güvenlik türünü belirleyin

WEP

Şifre	AP için şifre

WPA/WPA2

Şifre	AP için şifre

802.1x EAP

EAP-Metodu

PWD	Kimlik	Kimlik
	Şifre	Şifre

PEAP	Faz 2 Kimlik Doğrulama Protokolü	Hiçbiri	Ek protokol yok
		MSCHAPV2	MSCHAPV2 protokolü
		GTC	GTC protokolü
	CA Sertifikası	CA sertifikası	
	Kimlik	Kimlik	
	Anonim Kimlik	Anonim kimlik	
	Şifre	Şifre	

TTLS	Faz 2 Kimlik Doğrulama Protokolü	Hiçbiri	Ek protokol yok
		PAP	PAP protokolü
		MSCHAP	MSCHAP protokolü
		MSCHAPV2	MSCHAPV2 protokolü
		GTC	GTC protokolü
	CA Sertifikası	CA Sertifikası	
	Kimlik	Kimlik	
	Anonim Kimlik	Anonim Kimlik	
	Şifre	Şifre	

TLS	CA Sertifikası	CA sertifikası
	Kimlik	Kimlik
	Şifre	Şifre

VPN

Bağlantı Adı	VPN Bağlantısının Adı

VPN Türü

VPN

VPN İstemcisi

AppTec360 VPN İstemcisi	
Ağ Geçidi Yapılandırması	Ağ Geçidi VPN Yapılandırmasını seçin (Bkz. **Genel Ayarlar > Evrensel Ağ Geçidi > VPN Ayar**ları)
Her Zaman Açık VPN	Yerel Kilitlemeyi Etkinleştir
AppTec360 Kilitlemeyi Etkinleştir	AppTec360 Kilitlemeyi Etkinleştir

Dahili (Yalnızca Samsung cihazlarda mevcuttur)			
Bağlantı Türü	PPTP	Sunucu	Sunucu
		PPTP Şifrelemesini Etkinleştir	PPTP Şifrelemesini Etkinleştir
	L2TP / IPSec PSK	Sunucu	Sunucu
		IPSec Ön Paylaşımlı Anahtar	IPSec Ön Paylaşımlı Anahtar
		L2TP Sırrını Etkinleştir	L2TP Sırrını Etkinleştir
		L2TP Sırrı	L2TP Sırrı
	IPSec XAuth PSK	Sunucu	Sunucu
		IPSec Tanımlayıcı	IPSec Tanımlayıcı
		IPSec Ön Paylaşımlı Anahtar	IPSec Ön Paylaşımlı Anahtar
DNS Arama Alanları	DNS Arama Alanları		
Uzman Ayarları	DNS Sunucuları	DNS Sunucuları	
	Yönlendirme Rotaları	Yönlendirme Rotaları	

Açık VPN		
Sunucu	Sunucu	
OpenVPN Profili	OpenVPN Profili	
OpenVPN Uygulaması	Android için OpenVPN (önerilir)	
	OpenVPN Bağlantısı	
Uzman Ayarları	DNS Sunucuları	DNS Sunucuları
	Yönlendirme Rotaları	Yönlendirme Rotaları

Samsung / Güçlü Kuğu			
Bağlantı Türü	PPTP	Sunucu	Sunucu
		Kullanıcı Adı	Kullanıcı Adı
		Şifre	Şifre
		PPTP Şifrelemesini Etkinleştir	PPTP Şifrelemesini Etkinleştir
	L2TP / IPSec PSK	Sunucu	Sunucu
		IPSec Ön Paylaşımlı Anahtar	IPSec Ön Paylaşımlı Anahtar
		Kullanıcı Adı	Kullanıcı Adı
		Şifre	Şifre
		L2TP Sırrını Etkinleştir	L2TP Sırrı
	IPSec XAuth PSK	Sunucu	Sunucu
		IPSec Tanımlayıcı	IPSec Tanımlayıcı
		IPSec Ön Paylaşımlı Anahtar	IPSec Ön Paylaşımlı Anahtar
		Kullanıcı Adı	Kullanıcı Adı
		Şifre	Şifre
Uzman Ayarları	DNS Sunucuları	DNS Sunucuları	
	Yönlendirme Rotaları	Yönlendirme Rotaları	

Cisco Any Connect		
Sunucu	Sunucu	
Sertifika Modu	Engelli	Engelli
	Otomatik	Otomatik
Uzman Ayarları	DNS Sunucuları	DNS Sunucuları
	Yönlendirme Rotaları	Yönlendirme Rotaları

Uygulama Başına VPN

VPN İstemcisi

AppTec360 VPN İstemcisi		
Ağ Geçidi Yapılandırması	Ağ Geçidi VPN Yapılandırmasını seçin (Bkz. **Genel Ayarlar > Evrensel Ağ Geçidi > VPN Ayar**ları)	
VPN Uygulamaları	VPN Uygulamaları	
Her Zaman Açık VPN	Yerel Kilitlemeyi Etkinleştir	Her Zaman Açık VPN
AppTec360 Kilitlemeyi Etkinleştir	AppTec360 Kilitlemeyi Etkinleştir	

Samsung / Güçlü Kuğu			
Bağlantı Türü	PPTP	Sunucu	Sunucu
		VPN Uygulamaları	VPN Uygulamaları
		Kullanıcı Adı	Kullanıcı Adı
		Şifre	Şifre
		PPTP Şifrelemesini Etkinleştir	PPTP Şifrelemesini Etkinleştir
	L2TP / IPSec PSK	Sunucu	Sunucu
		VPN Uygulamaları	VPN Uygulamaları
		IPSec Ön Paylaşımlı Anahtar	IPSec Ön Paylaşımlı Anahtar
		Kullanıcı Adı	Kullanıcı Adı
		Şifre	Şifre
		L2TP Sırrını Etkinleştir	L2TP Sırrı
	IPSec XAuth PSK	Sunucu	Sunucu
		VPN Uygulamaları	VPN Uygulamaları
		IPSec Tanımlayıcı	IPSec Tanımlayıcı
		IPSec Ön Paylaşımlı Anahtar	IPSec Ön Paylaşımlı Anahtar
		Kullanıcı Adı	Kullanıcı Adı
		Şifre	Şifre
Uzman Ayarları	DNS Sunucuları	DNS Sunucuları	
	Yönlendirme Rotaları	Yönlendirme Rotaları	

Kısıtlamalar

Burada bağlantı yönetimi ile ilgili kısıtlamaları ayarlayabilirsiniz.

Veri Dolaşımına İzin Ver	Dolaşımdayken mobil veriye izin ver
Veri Dolaşımını Zorla	Etkinleştirilirse, mobil veri için dolaşım kalıcı olarak etkinleştirilir (önerilmez!) Bu ayar "Veri Dolaşımına İzin Ver" ayarının üzerine yazılır!
Aşağıdaki ayarlar yalnızca SAFE 2.x veya üzeri sürümlerde mevcuttur	
Yalnızca Acil Durum Çağrılarına İzin Ver	Yalnızca Acil Durum Çağrılarına İzin Ver
WiFi'a İzin Ver	WiFi'a İzin Ver
WiFi Ağı Minimum Güvenlik Seviyesi	WiFi ağı minimum güvenlik seviyesi Açık = her türlü WiFi'a izin verilir
Kullanıcının WiFi ağları eklemesini yasaklayın	Kullanıcı kendisi bir WiFi ağı ekleyemez Bu ayar yalnızca "Bağlantı Yönetimi" altında bir WiFi profili tanımlanmışsa mümkündür
SMS ve MMS'e İzin Ver	Tümü = Tüm SMS ve MMS trafiğine izin verilir Yalnızca Gelen SMS = Yalnızca gelen SMS mesajlarına izin verilir Yalnızca Giden SMS = Yalnızca giden SMS mesajlarına izin verilir Yok = SMS / MMS trafiğine izin verilmez
Dolaşım Sırasında Senkronizasyona İzin Ver	Dolaşım Sırasında Senkronizasyona İzin Ver Açık = etkinleştirildi Kapalı = devre dışı Kullanıcı seçimi = kullanıcının seçimi
Ses Dolaşımına İzin Ver	Ses Dolaşımına İzin Ver Açık = etkinleştirildi Kapalı = devre dışı Kullanıcı Seçimi = kullanıcının seçimi
Sistem http Proxy Sunucusu Kullanma	Sistemin ayarlar bölümünde sağlanan bir HTTP proxy sunucusunun kullanımı bağlı ağa (WiFi veya APN) bağlıdır

PIM Yönetimi

Gmail Değişimi

Bilgi: Bu Yapılandırma Gmail uygulamasına uygulanacaktır. Bu yüzden Gmail'i onaylamanız ve yüklemeniz gerekir.

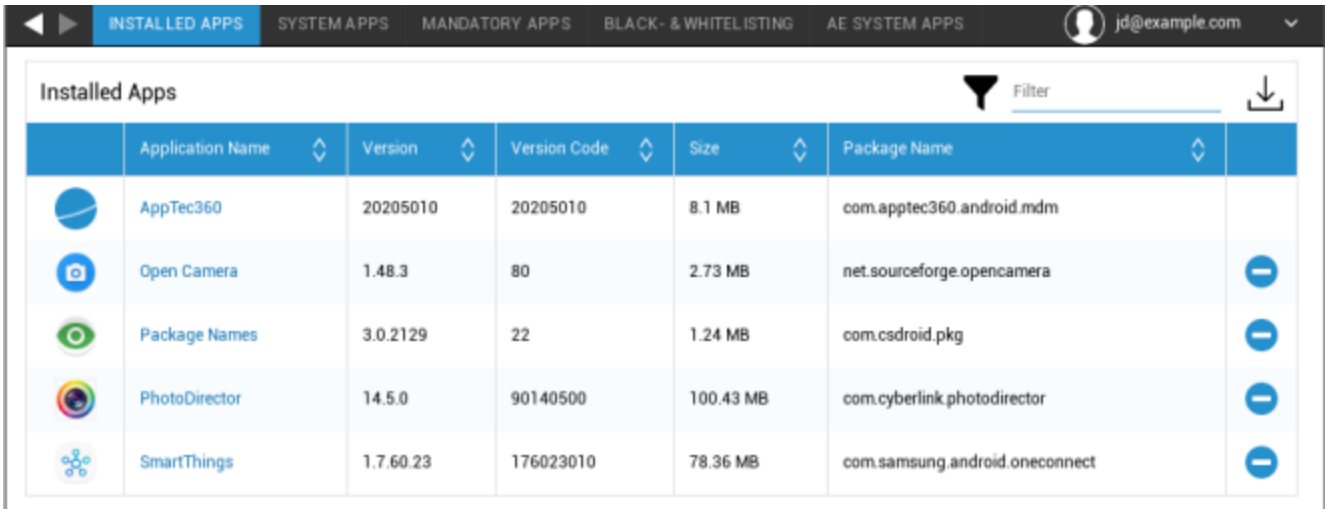
e-Posta Adresi	Sağlanan kullanıcının e-posta adresi Lütfen kimlik bilgileriyle çalışmak için kullanabileceğiniz ve her cihazda manuel olarak değişiklik yapmadığınız "Yer tutuculara" dikkat edin Bir tıklama ile bunları kendiniz için görüntüleyebilirsiniz
Sunucu Ana Bilgisayar Adı	Exchange Sunucularınızın sunucu adresi
Giriş adı	İlgili son kullanıcı cihazı için Oturum Açma Adı, lütfen "Buradaki yer tutuculara da dikkat edin
İmza	Bir imza eklenebilir (İpucu: Bazı cihazlar imza için HTML biçimlendirmesi gerektirir)
Senkronize edilecek önceki gün sayısı	E-postaların ne zaman geri senkronize edileceğini belirleyen gün sayısı
Cihaz Tanımlayıcısı	Ein String der die EAS DeviceID enthält. Bu, EAS Protokollerinin bir parçasıdır ve bazı bölgelerde kullanılabilir
Güvenli Yuva Katmanı (SSL) kullanın	SSL bağlantısı kullanın
Tüm sertifikaları kabul edin	Tüm sertifikalar kabul edilmektedir. Exchange Server'ınız kendinden imzalı bir sertifika kullanıyorsa lütfen bu seçeneği seçin

Uygulama Yönetimi

Kurumsal Uygulama Yöneticisi

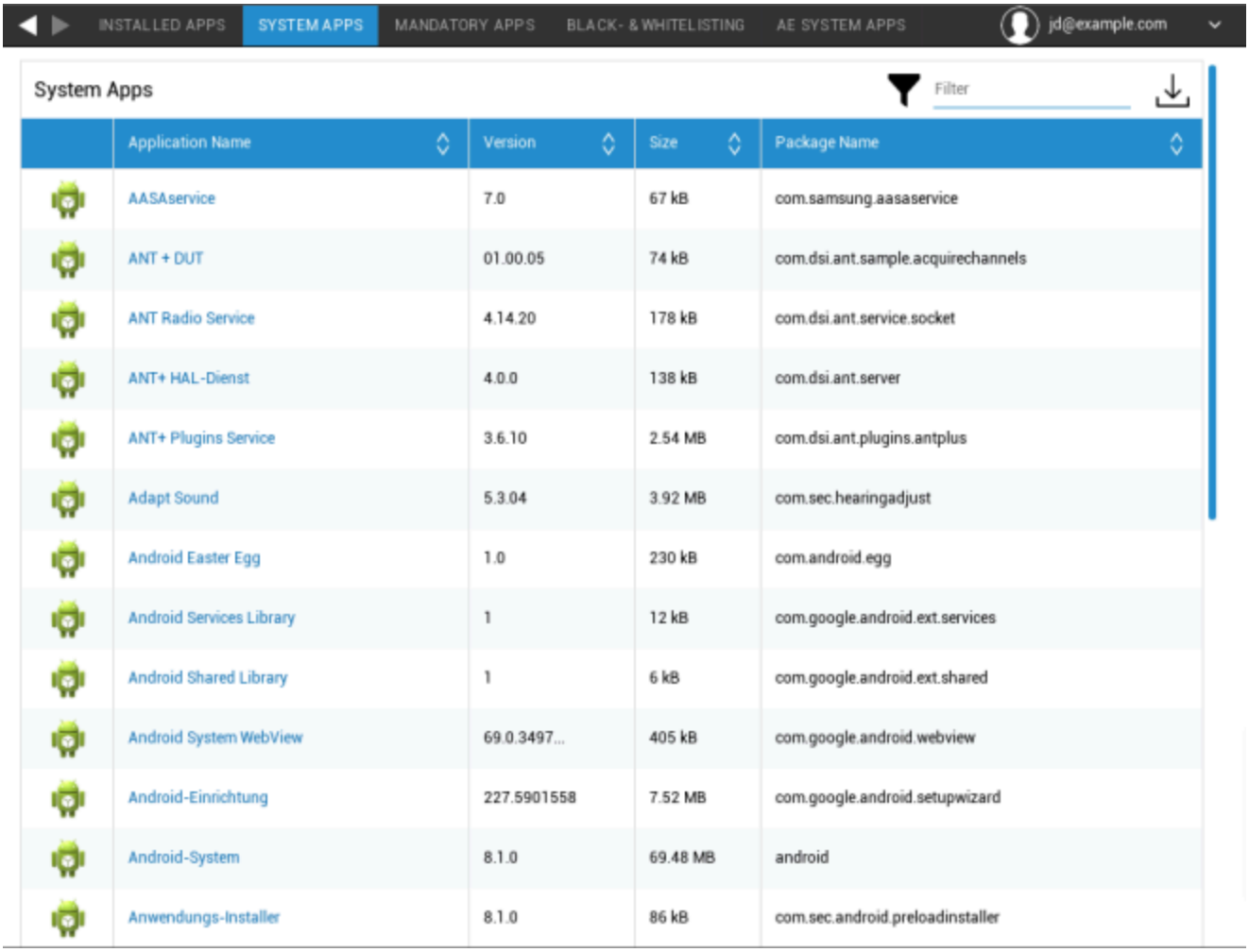
Yüklü Uygulamalar (yalnızca cihaz düzeyinde)

Burada, son kullanıcı cihazında o anda yüklü olan tüm Uygulamalar sizin için görüntülenecektir.



Sistem Uygulamaları (yalnızca cihaz düzeyinde)

"Sistem Uygulamaları" altında, cihaz üreticiniz tarafından son kullanıcı cihazına zaten yüklenmiş olan tüm uygulamalar ve hizmetler sizin için listelenecektir.

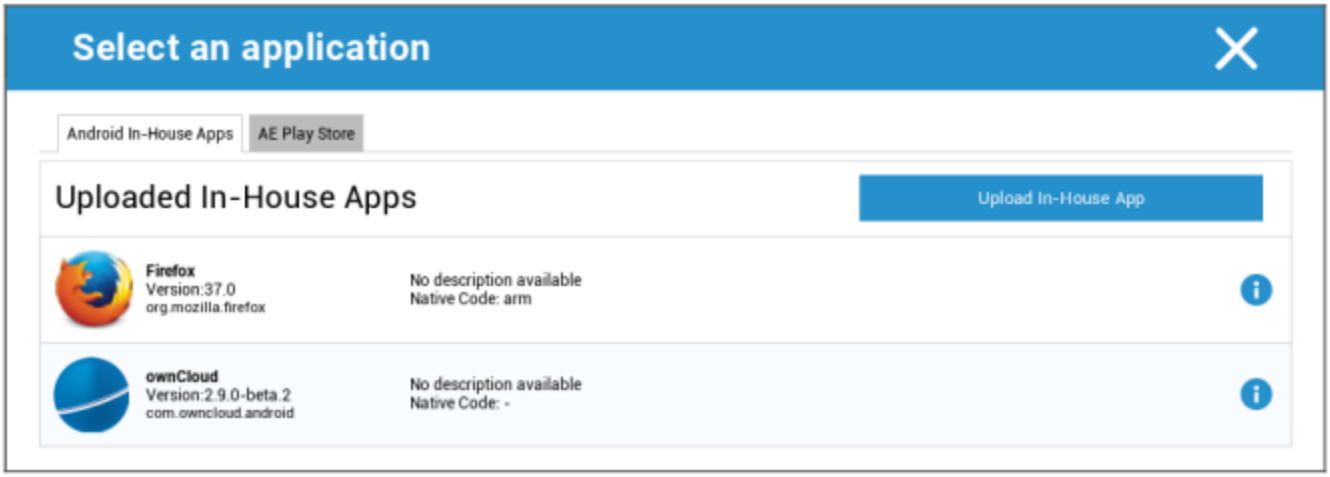


Zorunlu Uygulamalar

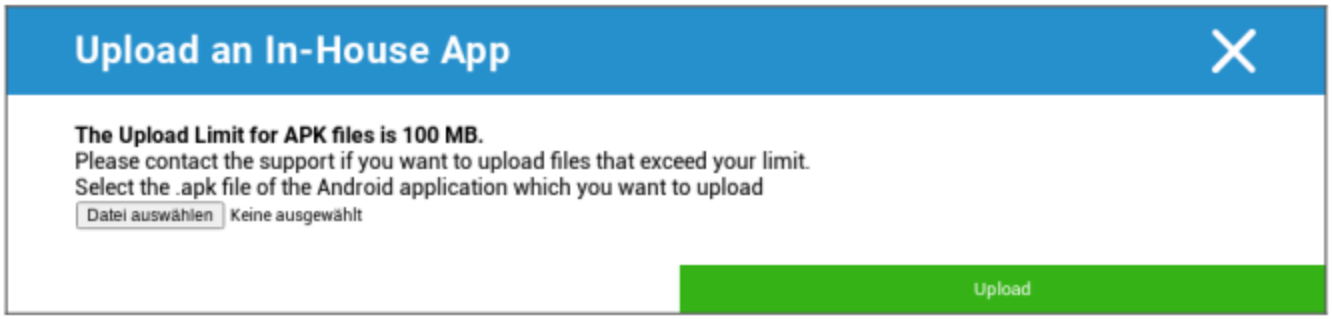
Zorunlu Uygulamalar altında, zorunlu gerekli uygulamaları belirleyebilirsiniz. Kullanıcıdan sürekli olarak bu belirlenmiş uygulamayı yüklemesi istenecektir.

aracılığıyla zorunlu gerekli uygulama tanımlanabilir.

Bu, Genel Ayarlar'da yüklediğiniz "Android Şirket İçi Uygulamalar "dan bir Şirket İçi Uygulama olabilir.

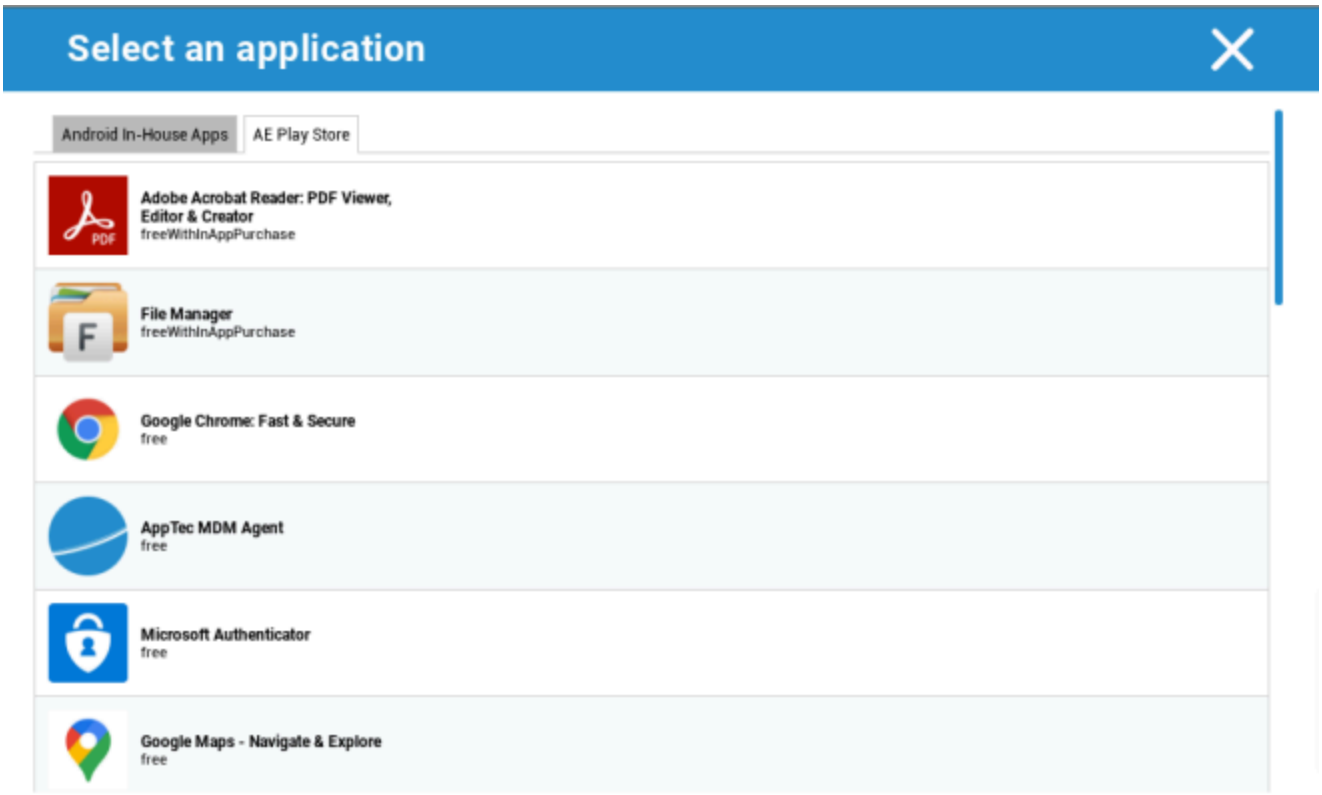


Ayrıca "Şirket İçi Uygulama Yükle" ile doğrudan bir apk dosyası seçip yükleyebilirsiniz.



Bir Şirket İçi Uygulama yüklüyorsanız, "Güncel tut" seçeneğini etkinleştirme olanağına sahip olacaksınız. Bu etkinleştirilmişse ve Şirket İçi Uygulama DB'sinde daha yeni bir sürüm tanımladıysanız, uygulama cihazda güncellenecektir.

Ya da Google Work Play Store'dan bir "AE Play Store" Uygulaması olabilir.



Bu sekmede yalnızca onaylı "AE Play Store Uygulamaları" gösterilecektir.

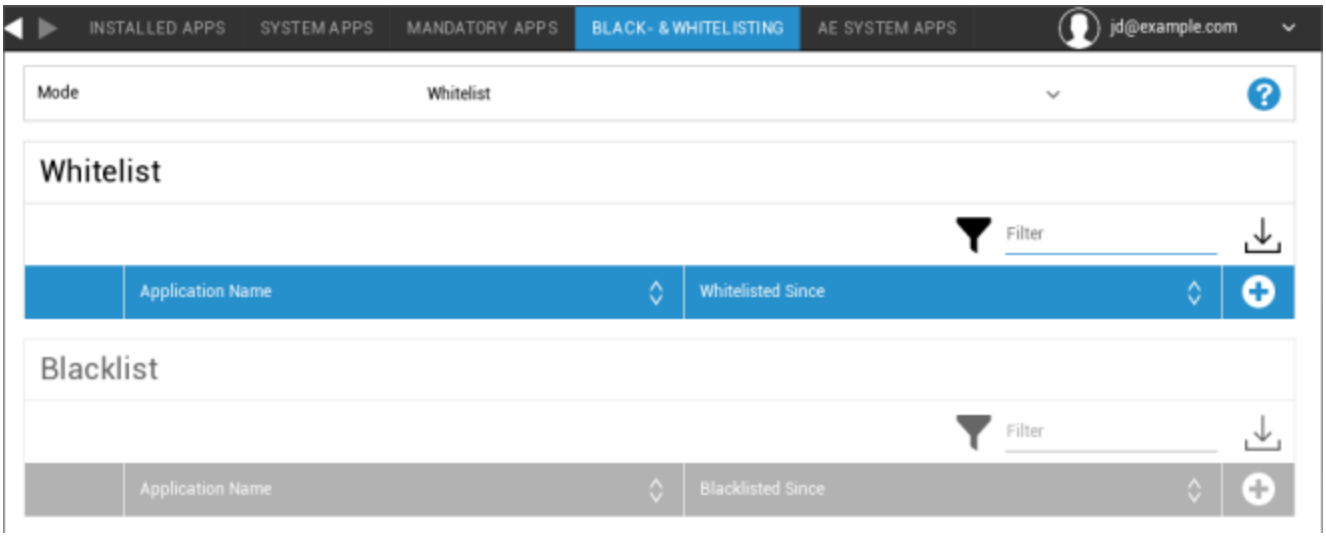
Bir "AE Play Store Uygulaması "nı onaylamak için lütfen "Genel Ayarlar" > "Uygulama Yönetimi" > "AE Play

Mağazası "na gidin ve sizi "Play Store Uygulamaları" sekmesine yönlendirecek düğmeyi kullanarak bir uygulama ekleyin (veya
doğrudan "Play Store Uygulamaları" sekmesine gidebilirsiniz).

"Play Store Uygulamaları" sekmesinde uygulamaları arayabilirsiniz. Bir uygulamaya tıkladığınızda, uygulama sayfası açılır
ve burada "Onayla" düğmesine tıklayarak uygulamayı onaylayabilirsiniz.

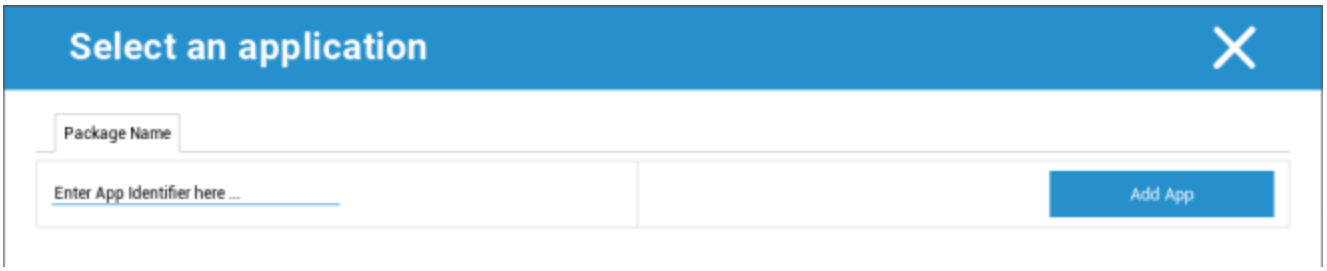
Kara ve Beyaz Liste

"Kara ve Beyaz Liste" altında, "Beyaz Liste" Modu ile "Kara Liste" Modu arasında seçim yapabilirsiniz.



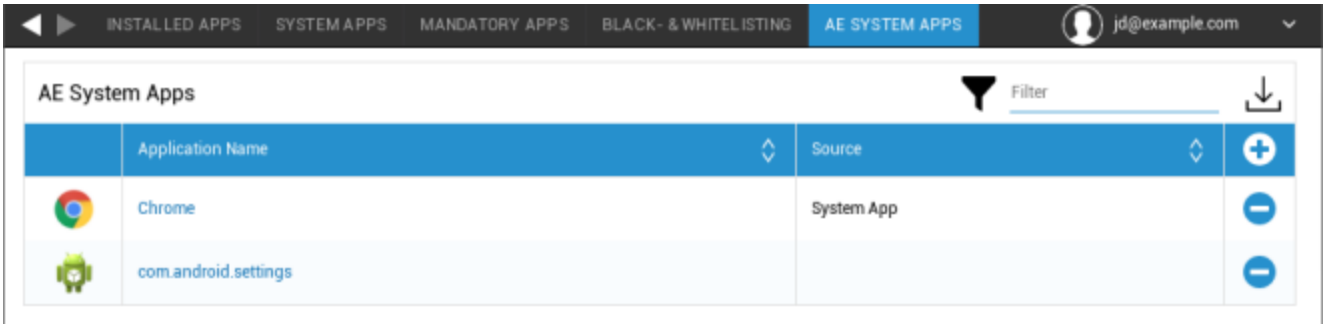
Beyaz Liste	Yalnızca listeye eklenen uygulamalar ve hizmetler son kullanıcı cihazına yüklenebilir. Bunlar son kullanıcı cihazına önceden yüklenmişse, kullanıcının bunları çalıştırabilmesi için etkinleştirilecek ve ayarlanacaktır.
	Listeye eklenmeyen diğer tüm uygulamalar son kullanıcı cihazına yüklenemez. Bunlar son kullanıcı cihazına önceden yüklenmişse, devre dışı bırakılacak ve kullanıcının bunları çalıştıramayacağı şekilde ayarlanacaktır.
Kara Liste	Listeye eklenen uygulamalar ve hizmetler son kullanıcı cihazına yüklenemez. Bunlar son kullanıcı cihazına önceden yüklenmişse, devre dışı bırakılacak ve kullanıcının bunları çalıştıramayacağı şekilde ayarlanacaktır.
	Listeye eklenmeyen diğer tüm uygulamalar son kullanıcı cihazına yüklenebilir. Bunlar son kullanıcı cihazına önceden yüklenmişse, kullanıcının bunları çalıştırabilmesi için etkinleştirilecek ve ayarlanacaktır.

ile o anda kullanılanlar listesine ek uygulamalar veya hizmetler ekleyebilirsiniz.
ile o anda etkin olmayan listeye ek uygulamalar veya hizmetler ekleyebilirsiniz.
Bir "Paket adı" tanımlayabilirsiniz:

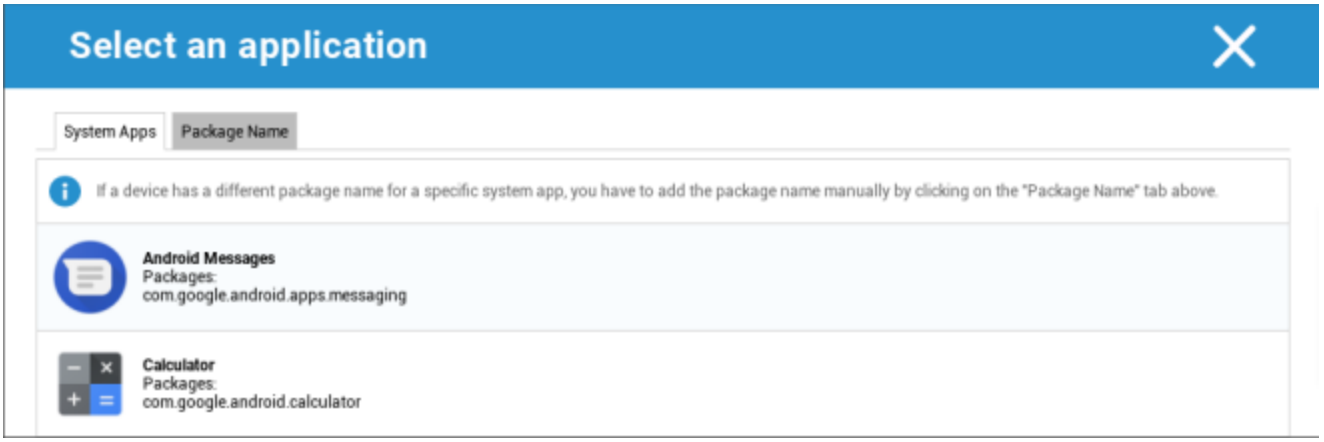

Select an application
Package Name
Enter App Identifier here ...
Add App

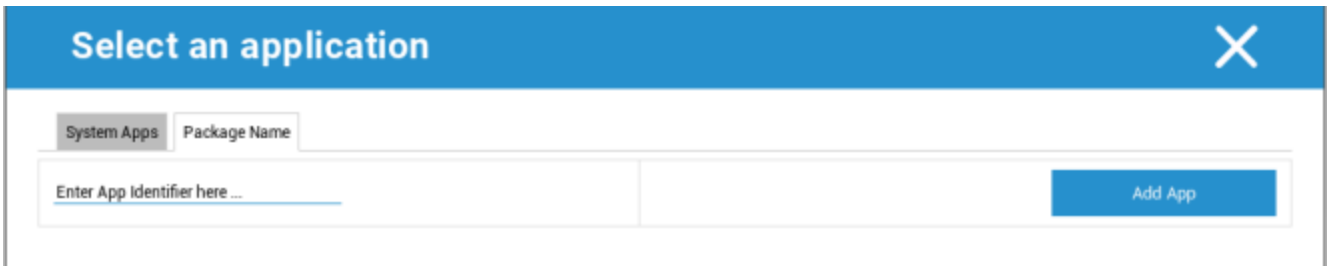
AE Sistem Uygulamaları

Burada, cihazlarda etkinleştirilmesi gereken belirli sistem uygulamalarını içeren bir liste tanımlayabilirsiniz.



Düğmeye tıklarsanız, Google tarafından sağlanan olası sistem uygulamaları listesinden seçim yapabilir veya etkinleştirilmesi gereken bir sistem uygulamasının paket adını doğrudan girebilirsiniz.





Google tarafından sağlanan listedeki sistem uygulamalarının yalnızca sistem uygulaması olabilecek uygulamalar olduğunu, ancak cihazlarınızdaki sistem uygulamaları olmak zorunda olmadığını lütfen unutmayın.

Ancak, bu liste yalnızca önceden yüklenmiş olan uygulamaları etkiler.

Cihazlarınızda önceden yüklü olmayan uygulamaları eklemek, uygulamanın Google tarafından sağlanan listeden olup olmadığına veya uygulamanın paket adının doğrudan girilip girilmediğine

bakılmaksızın cihazlarınızı etkilemeyecektir.

Kısıtlamalar ve Ayarlar

Uygulama Yönetimi Ayarları

Burada cihazın uygulama güncellemelerine ilişkin davranışını yapılandırabilirsiniz.

Güncelleme Kontrol Sıklığı	AppTec360 İstemcisinin uygulama güncellemelerini hangi aralıkta arayacağını belirtin. Varsayılan değer 24 saattir.
Wi-Fi Eşiği	Belirtilen boyuttan daha büyük olan uygulamalar Wi-Fi üzerinden indirilecektir. "Yalnızca Wi-Fi" seçilirse, tüm uygulamalar Wi-Fi üzerinden indirilecektir.

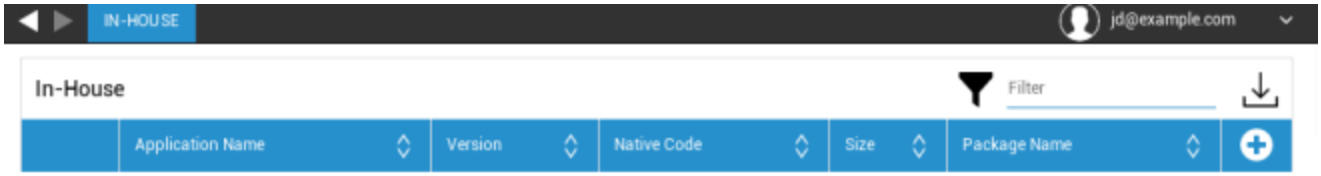
Kurumsal Uygulama Mağazası

Şirket İçi

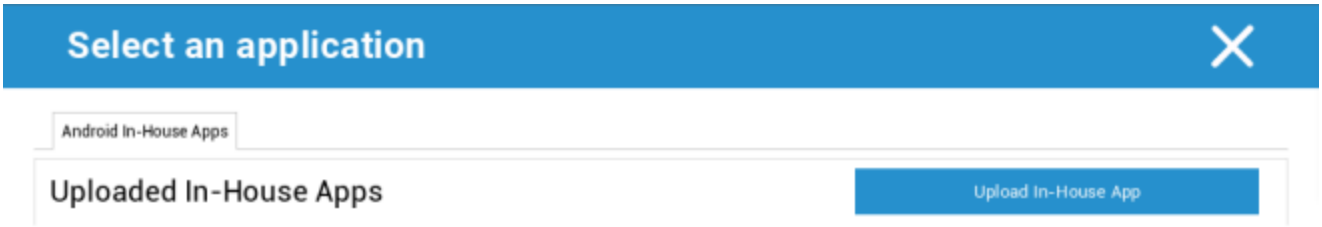
"Şirket İçi" başlığı altında, şirket içinde geliştirilen uygulamaları yükleyebilir ve dağıtabilirsiniz.

Sembol ile ek Şirket İçi Uygulamaları dağıtabilirsiniz.

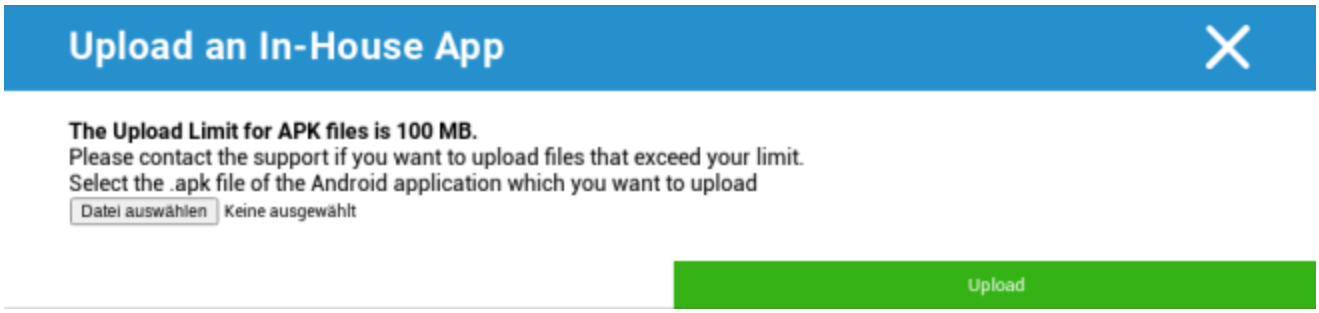
Bir Şirket İçi Uygulama yüklüyorsanız, "Güncel tut" seçeneğini etkinleştirme olanağına sahip olacaksınız. Eğer
bu etkinleştirildiğinde ve Şirket İçi Uygulama DB'sinde daha yeni bir sürüm tanımladığınızda, uygulama
cihaz üzerinde güncellenir.



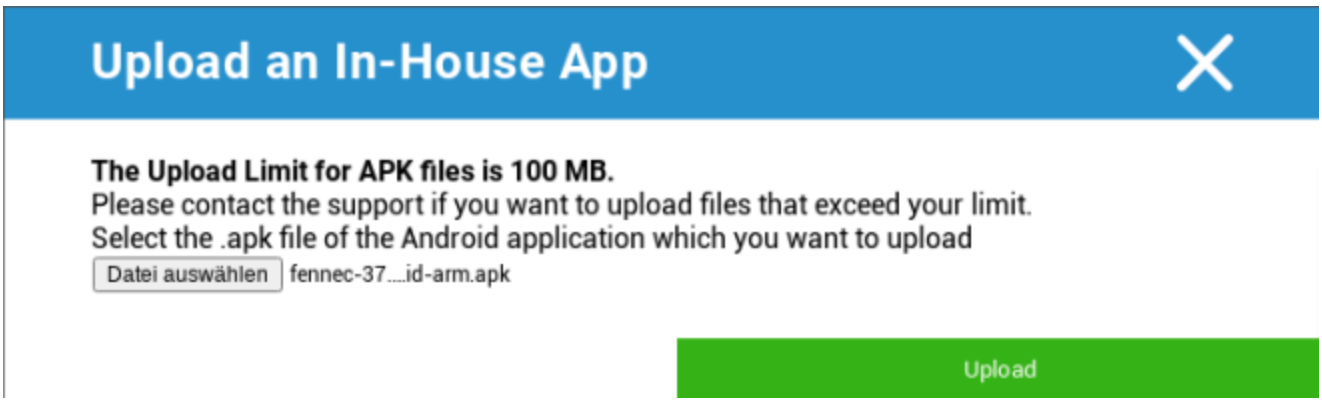
Kurum İçi Uygulamaları dağıtmadıysanız, aşağıdaki genel bakışı alacaksınız:



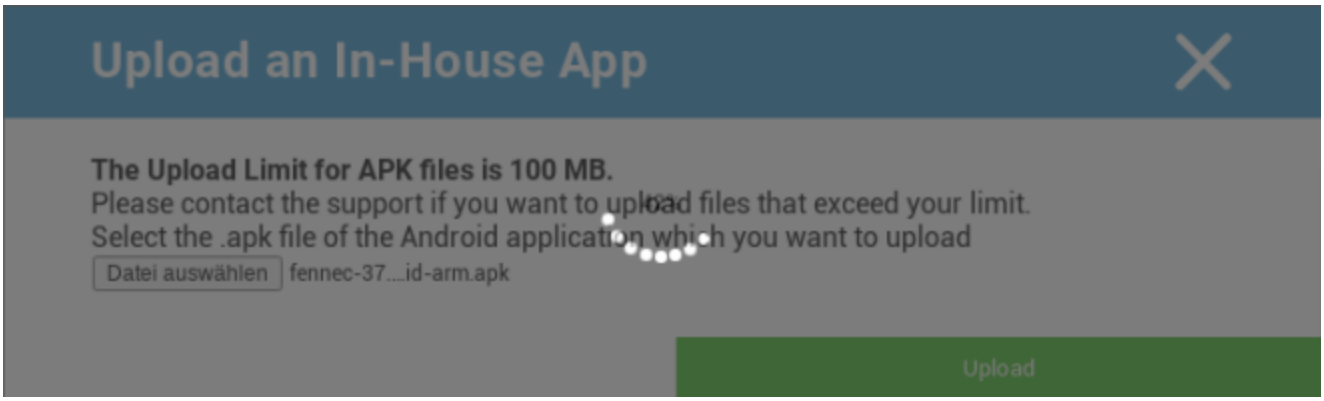
Bunun için "Şirket İçi Uygulama Yükle" seçeneğine tıklayın, ardından aşağıdaki genel bakışı alacaksınız:



Şimdi, "Ara... "yı kullanarak bir .apk dosyası seçin ve ardından "Yükle "ye tıklayın.



Uygulamanız şimdi yüklenecek, dairenin ortasında bir yüzde göstergesi göreceksiniz, Uygulamanızın ne kadarının zaten yüklenmiş olduğunu gösterir.



Şirket İçi Uygulamanızın yüklenmesi başarılı olduysa, yüklenen uygulamayı bulabilirsiniz Uygulama Kataloğunuzda.

Kullanıcı artık bu uygulamayı son kullanıcıdaki AppTec360 Mağazasında görme ve yükleme seçeneğine sahiptir
cihazı, "Şirket İçi" kategorisi altında.

Bunun bir Google PlayStore Uygulaması içermemesi nedeniyle, kullanıcının kayıtlı bir Google İlgili son kullanıcı cihazındaki kimlik.

Kurumsal Play Store

AE Play Store

Buradan Android Enterprise Playstore'a uygulama ekleyebilirsiniz. Lütfen onaylamanız gerektiğini unutmayın
Ekleyebilmeniz için önce AE Yönetici Hesabınız ile uygulamalar.

Bir uygulamayı onaylamak için lütfen Zorunlu Uygulamalar bölümündeki talimatlara bakın.

Kiosk Modu ve Başlatıcı

Kiosk Modu

Kiosk Modu, bir uygulamayı veya URL'yi önceden tanımlamanıza olanak tanır. O zaman sadece aşağıdakiler mümkün olacaktır
bu uygulamayı ve / veya URL'yi çalıştırın / ziyaret edin.

Aynı şekilde, çeşitli donanım düğmeleri Kiosk Modu çeşitliliğinde devre dışı bırakılabilir.

Otomatik Başlatma	Profil son kullanıcı cihazına ulaşır ulaşmaz Kiosk Modunu otomatik olarak başlatır
Zamanlanmış Kiosk Modu?	Kiosk Modu için bir zaman planlayabilirsiniz, bu daha sonra sizin belirlediğiniz bir zamanda otomatik olarak başlayacak ve bitecektir
Başlangıç Zamanı	Başlangıç zamanı
Dakika cinsinden zaman	Kiosk Modunun tekrar sona ermesi gereken dakika cinsinden süre

Uygulama Türü

Tek Uygulama	Uygulamayı Kiosk Modunda başlatmak istiyorsanız, "Uygulama Türü" altında "Paket" seçeneğini seçin
Kiosk Uygulaması	Kiosk Modunda başlatılması gereken bir uygulama seçmek için buraya tıklayın Her zamanki Uygulama Yönetimine genel bakışı bulacaksınız "Google Play Store", "Android Şirket İçi Uygulamalar" ve "Paket Adı" arasında seçim yapabilirsiniz

Uygulama Türü

URL		Kiosk Modunda bir URL başlatmak istiyorsanız, "Uygulama Türü" altında "URL "yi seçin Ardından istediğiniz URL adresini tanımlayın
	Hareketsizlikten sonra tarayıcıyı temizle	Burada, Kiosk Modunun yeniden başlatılması gereken zaman aralığını dakika cinsinden tanımlayabilirsiniz
	Web Önbelleğini ve Çerezleri Temizle	Bu işlevi etkinleştirirseniz, Kiosk Modu yeniden başlatıldıktan sonra Web Önbelleği (çerezler ve önbelleğe alınmış resimler) silinecektir
	Aynı Menşe Politikası	Bu işlev etkinse, kullanıcı yalnızca tanımlanmış bir URL'nin alt sayfalarında gezinebilir Örneğin, aşağıdaki URL'yi tanımladınız:www.mypage.com Ardından, kullanıcı şu adreste gezinebilir: www.mypage.com/subpage
	Beyaz Listedeki URL'ler	Burada bir Beyaz Liste tutabilirsiniz, tüm bu URL'lere izin verilir Satır başına en fazla 1 URL Bir URL http:/ veya https:// ile başlamalıdır
	Kara Listeye Alınan URL'ler	Burada bir Kara Liste tutabilirsiniz, tüm bu URL'lere izin verilmez Satır başına en fazla 1 URL Bir URL http:/ veya https:// ile başlamalıdır
	Ekran Yönü	Bu ayar ekran ayarlarıyla ilgilidir Otomatik = otomatik Portre = dikey format Landscape = manzara modu

Çoklu Uygulama		"Çoklu Uygulama" Kiosk Modunu seçerseniz, AppTec360 Launcher'ın kullanımı zorunlu olacaktır.
	Uygulamalar	Uygulama: Kiosk Uygulaması olarak bir Playstore veya Şirket İçi Uygulama seçin. Bir paket adı girmek de mümkündür. Seçilen Kiosk Uygulaması cihazda yüklü olmalıdır. Kiosk Uygulamasını zorunlu olarak ayarlamayı unutmayın. Ana Ekranda Kısayol: "Açık" olarak ayarlanırsa ana ekranda bir kısayol oluşturulacaktır. "Kapalı" olarak ayarlanırsa Uygulama, Uygulama Listesinde görünmeye devam edecektir.

Çıkış Şifresi Etkin	Bu işlevi etkinleştirirseniz, kullanıcının Kiosk Modunu sizin tarafınızdan önceden tanımlanmış bir parola ile sonlandırması mümkündür
Çıkış Şifresi	Bu, sizin tarafınızdan önceden tanımlanmış olan paroladır
Durum Çubuğunu Otomatik Daralt	Etkinleştirilirse, Durum Çubuğu otomatik olarak harmanlanır. Bu seçenekle kullanıcılar Durum Çubuğundaki bilgileri görebilir, ancak işlevlerine erişemez
Durum Çubuğunu Devre Dışı Bırak	Durum Çubuğu Bildirimler, Kısayollar ve Bilgiler içerir. Yalnızca SAFE 4.0 veya üzeri sürümlere sahip Samsung cihazları için kullanılabilir.
Ses Tuşlarını Devre Dışı Bırak	Ses tuşlarını devre dışı bırakma (yalnızca SAFE 3.0 veya üzeri Samsung cihazlarında kullanılabilir)
Açma / Kapama Anahtarını Devre Dışı Bırak	Açma / Kapama düğmesini devre dışı bırakma (yalnızca SAFE 3.0 veya üzeri Samsung cihazlarında kullanılabilir)
Ana Ekran Düğmesini Devre Dışı Bırak	Ana Ekran düğmesini devre dışı bırakın. Bu işlev etkinleştirildiyse, Kiosk Modu yalnızca AppTec360 Konsolunda sonlandırılabilir (yalnızca SAFE 3.0 veya üzeri Samsung cihazlarında kullanılabilir)
Gezinti Çubuğunu Devre Dışı Bırak	Bununla Gezinti Çubuğunu (Geri / Menü) devre dışı bırakabilirsiniz Bu işlev etkinleştirildiyse, Kiosk Modu yalnızca AppTec360 Konsolunda sonlandırılabilir (yalnızca SAFE 3.0 veya üzeri Samsung cihazlarında kullanılabilir)

AppTec360 Başlatıcı

AppTec360 Başlatıcıyı Etkinleştir	Açık: AppTec360 Başlatıcıyı etkinleştirir. Kullanıcının bunu bir kez varsayılan Başlatıcı olarak ayarlaması gerekir. Not: Kiosk Modu etkinleştirilirse ve Kiosk Modu "Çoklu Uygulama" olarak ayarlanırsa, AppTec360 başlatıcısının kullanımı zorunlu olacaktır.
Büyük Simgeler	Açık: Başlatıcıda Uygulama Simgelerinin daha büyük bir Sürümünü gösterir
AppTec360 Uygulama Simgesini Gizle	Açık: AppTec360 Uygulamasını tamamen gizler
AppTec360 Mağaza Simgesini Gizle	Açık: AppTec360 Enterprise AppStore'u tamamen gizler

AppTec360 Ayarları

AppTec360 Ayarlar Uygulamasını Etkinleştir	AppTec360 Ayarlar Uygulaması WiFi ve Bluetooth bağlantıları üzerinde kontrol sağlar
Çoklu Uygulamada Ayarları Etkinleştir Kiosk Modu	Etkinleştirilirse, kullanıcılar Çoklu Uygulama Kiosk Modu etkinken AppTec360 Ayarlar Uygulamasına erişebilir

Uzaktan Kumanda

Splashtop

Cihazınız için bir uzaktan kumanda oturumu başlatmak için, "Splashtop Streamer" Uygulamasının, **Uygulama Yönetimi** → **Kurumsal Uygulama Yöneticisi** → **Zorunlu Uygulamalar**'a eklenerek cihaza yüklenmesi gerekir.

Daha sonra Splashtop için aşağıdaki ayarları yapılandırın:

Splashtop'u Etkinleştir	Etkinleştirilirse, AppTec360 Splashtop uygulamasını uzaktan kontrole izin verecek şekilde yapılandırır
Kod Dağıtma	https://my.splashtop.com adresine gidin ve Splashtop hesabınıza giriş yapın. "Bilgisayar Ekle "ye tıklayın ve çıkan sayfadaki 12 haneli dağıtım kodunu kopyalayın.
Özel Dağıtım Ağ Geçidini Ayarla?	Ağ Geçidini Dağıtma
Ağ Geçidi Etki Alanı / Ana Bilgisayar Dağıtma	Ağ Geçidini Dağıtma
Sertifika Doğrulama	Sertifika Doğrulama

Ardından, uzaktan kumanda oturumunu başlatmak için içerik menüsündeki Splashtop Uzaktan Kumanda seçeneğini kullanabilirsiniz (cihaz seçildiğinde arama çubuğunun yanındaki dişli veya ağaçtaki cihaza sağ tıklayın).

TeamViewer

Cihazınız için bir uzaktan kumanda oturumu başlatmak için, "TeamViewer QuickSupport" Uygulamasının, **Uygulama Yönetimi** → **Kurumsal Uygulama Yöneticisi** → **Zorunlu Uygulamalar**'a eklenerek cihaza yüklenmesi gerekir.

Ardından, uzaktan kumanda oturumunu başlatmak için içerik menüsündeki **TeamViewer** Uzaktan Kumanda seçeneğini kullanabilirsiniz (cihaz seçildiğinde arama çubuğunun yanındaki dişli veya ağaçtaki cihaza sağ tıklayın).

İçerik Yönetimi

ContentBox

Burada ContentBox'ı etkinleştirebilirsiniz.

"ContentBox'ı Etkinleştir" seçeneğini "Açık" olarak değiştirdiğinizde, ayrı bir ContentBox Uygulaması yüklenecektir
son kullanıcı cihazında otomatik olarak.

Güvenli Tarayıcı

Burada AppTec360 Secure Browser için ayarları yapılandırabilirsiniz.

"Güvenli Tarayıcı" bölümünü "Açık" olarak değiştirdiğinizde, ayrı bir Tarayıcı Uygulaması son kullanıcı cihazına otomatik olarak yüklenir.

Şifre Gerektir	Kullanıcının tarayıcıya erişmek için bir parola ayarlamasını ve kullanmasını gerektirir.
Gerekli minimum parola uzunluğu	Parola için gerekli karakter sayısını ayarlayın
Gerekli Şifre Kalitesi	Gerekli parola kalitesini ayarlayın
İndirmeleri Kısıtla / İçeride Aç	
Yüklemeleri Kısıtla	
Beyaz Liste Yükle	Karşıya yüklemeye her zaman izin verilecek URL'lerin bir listesi.
Kopyalamaya İzin Ver	Web sayfaları içinde metin kopyalamaya, kesmeye veya paylaşmaya izin verin.
Ekran Yakalamaya İzin Ver	Ekran görüntülerinin yakalanmasına izin verin.
Veri temizleme sıklığı	Hangi sıklıkta TÜM kullanıcı verilerinin (geçmiş, önbellek vb.) otomatik olarak kaldırılacağını seçin.
Şirket Yer İmleri	Yer İmleri, tarayıcı yer imlerindeki "Şirket yer imleri" klasöründe görünecektir. Kullanıcı tarafından düzenlenemezler.
Adres Çubuğunu Gizle	
Tarayıcı İçi Beyaz Liste (Universal Gateway olmadan)	İstemci tarafı URL beyaz listesini etkinleştirir. • Şirket Yer İmleri her zaman beyaz listeye alınır • Yalnızca 100 URL için desteklenir • Sınırsız Kara ve Beyaz Liste için lütfen Evrensel Ağ Geçidini kullanın
Beyaz Listedeki URL'ler	İzin verilen URL'lerin bir listesi.
Ağ geçidi tabanlı Kara ve Beyaz Liste	Kara listeye alma aşağıdaki gerekliliklere sahiptir: • Çalışan bir AppTec360 Universal Gateway ("Genel Ayarlar" → "Universal Gateway")

	• Belirlenmiş bir DNS sunucusu ile çalışan bir VPN yapılandırması ("Genel Ayarlar" → "Evrensel Ağ Geçidi" → "VPN Ayarları") • Bir Kara Liste yapılandırması ("Genel Ayarlar" → "Evrensel Ağ Geçidi" → "Etki Alanı Kara Listesi") • Profilde geçerli bir VPN bağlantısı ("Bağlantı Yönetimi" → "VPN")

Ek API

Samsung KNOX

Kısıtlamalar

SD Karta İzin Ver	
SD Kart Yazmaya İzin Ver	
Ekran Yakalamaya İzin Ver	
Panoya İzin Ver	
Ayarları ve uygulama verilerini Google Cloud'da yedekleme	
Bir uygulamayı yeniden yüklerken ayarları Google Cloud'dan geri yükleme	
USB Hata Ayıklamaya İzin Ver	
Google Crash Raporuna İzin Ver	
Fabrika Ayarlarına Sıfırlamaya İzin Ver	
OTA Yükseltmesine İzin Ver	
USB ana bilgisayar depolamasına izin ver	Etkinleştirilirse, kullanıcı herhangi bir kalem sürücüyü (taşınabilir USB depolama), harici HD'yi veya Secure Digital (SD) kart okuyucuyu bağlayabilir ve bu cihazda bir depolama sürücüsü olarak monte edilir.
USB Medya Oynatıcısına İzin Ver (MTP,PTP)	
Mikrofona İzin Ver	Üçüncü taraf uygulamalar için mikrofonu devre dışı bırakır
NFC'ye (Yakın Alan İletişimi) İzin Ver	
Bilinmeyen Kaynaklara İzin Ver (APK Sideloading)	Etkinleştirilirse, Uygulamaların (APK dosyaları) yandan yüklenmesine izin verilir. Bu ayar devre dışı bırakıldıktan sonra, bilinmeyen kaynaklardan APK'ların yüklenmesine yeniden izin verdiğinizde kullanıcının bunu manuel olarak etkinleştirmesi gerekir.

Kullanıcı Oluşturmaya İzin Ver	Etkinleştirilirse, kullanıcının cihazda birden fazla hesap oluşturmasına izin verilir, örneğin Misafir Hesapları

E-posta

e-Posta Adresi	
Gelen sunucu protokolü	
Gelen sunucu adresi	
Gelen sunucu bağlantı noktası	
Gelen sunucu oturum açma/kullanıcı adı	
Gelen sunucu şifresi	
Gelen sunucu SSL kullanır	
Gelen sunucu TLS kullanır	
Gelen sunucu tüm sertifikaları kabul eder	
Giden sunucu protokolü	
Giden sunucu adresi	
Giden sunucu bağlantı noktası	
Giden Sunucu ekstra kimlik bilgileri kullanır	Devre dışı bırakılırsa, sistem giden sunucu için de gelen kimlik bilgilerini kullanır.
Giden sunucu oturum açma adı/kullanıcı adı	
Giden Sunucu Parolası	
Giden sunucu SSL kullanır	
Giden sunucu TLS kullanır	
Giden sunucu tüm sertifikaları kabul eder	
İmzayı Ayarla	
İmza	Not: Bazı cihazlar için imzanın HTML formatında belirtilmesi gerekir.
Yeni e-posta aldığında kullanıcıyı bilgilendir	

Değişim

e-Posta Adresi	
Sunucu Ana Bilgisayar Adı	Exchange Sunucusunun ana bilgisayar adı
Giriş Adı	Exchange Server'da oturum açmak için kullanılan kullanıcı adı
Etki Alanı	Bir ACL Ağ Geçidi Yapılandırması etkinleştirilmişse ve Etki Alanı alanı boş değilse, AppTec360 Universal Gateway cihazın kimliğini aşağıdaki adla doğrulayacaktır "Etki Alanı\Login Adı
Şifre	
Senkronize edilecek önceki gün sayısı	
E-postayı senkronize etme sıklığı	
Dolaşım Sırasında Senkronizasyon	
İmzayı Ayarla	
İmza	Not: Bazı cihazlar için imzanın HTML formatında belirtilmesi gerekir.
Varsayılan hesap	
Güvenli Yuva Katmanı (SSL) kullanın	
Aktarım Katmanı Güvenliği (TLS) kullanın	
Tüm sertifikaları kabul edin	

APN

APN Görünen Adı	
Erişim Noktası Adı	APN'nin Adı
Giden sunucu protokolü	
MCC - Mobil Ülke Kodu	Kurulu SIM'in mmc'sini kullanmak için boş bırakın
MNC - Mobil Ağ Kodu	Yüklü SIM'in mnc'sini kullanmak için boş bırakın
Sunucu Adresi	
Sunucu bağlantı noktası numarası	
Sunucu proxy adresi	
MMS sunucu adresi	Varsayılan için boş bırakın
MMS bağlantı noktası numarası	Varsayılan için boş bırakın
MMS proxy adresi	Varsayılan için boş bırakın
Kullanıcı Adı	
Şifre	
Erişim Noktası Tipi	Kabul edilen türler "default", "mms", "supl "dir.
	Null veya boş geçilirse, varsayılan olarak "default,supl,mms" kullanılır.
	Varsayılan değer için boş bırakın.
Tercih Edilen APN	

Bluetooth

Bluetooth aracılığıyla Cihaz keşfine izin ver	
Bluetooth Eşleştirmesine İzin Ver	
Bluetooth Kulaklık cihazlarına izin ver	
Bluetooth Eller Serbest cihazlarına izin ver	
Bluetooth A2DP cihazlarına izin ver	A2DP, Gelişmiş Ses Dağıtım Profili cihazlar arasında ses akışına izin verir
Giden Aramalara İzin Ver	
Bluetooth ile Veri Aktarımına İzin Ver	
Bluetooth Tethering'e İzin Ver	
Bluetooth ile Bilgisayar bağlantısına izin ver	

Bağlantı

Yalnızca Acil Durum Aramalarına İzin VerWi-Fi'ye İzin Ver	
Wi-Fi Ağı Minimum Güvenlik Seviyesi	
Kullanıcının Wi-Fi ağları eklemesini yasaklayın	Bu kısıtlama yalnızca Bağlantı Yönetimi altında en az bir etkin Wi-Fi Profili tanımlanmışsa etkinleştirilebilir
SMS ve MMS'e İzin Ver	
Dolaşım Sırasında Senkronizasyona İzin Ver	
Ses Dolaşımına İzin Ver	

Android Enterprise – İş Profili ile Tam Yönetilen Cihaz (COPE)

COPE'un Genel Açıklaması

COPE, **Corporate Owned Personally Enabled**'ın kısaltmasıdır.

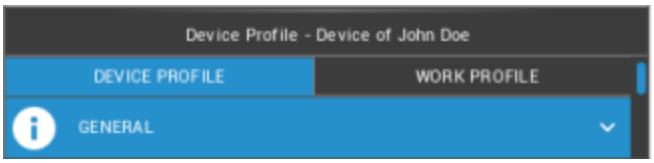
COPE modu, bir Android cihazının entegre Android Enterprise - **Container** profiline sahip bir Android **Enterprise - Tam Yönetilen Cihaz** olarak kaydedilmesini sağlar.

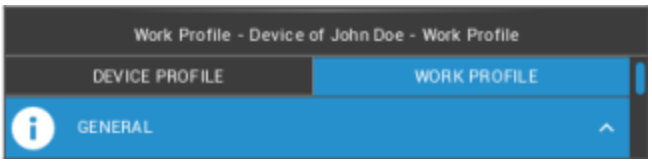
Bu, halihazırda bir Android cihaz olarak kayıtlı olan bir Android cihaz olabilir. **Android Enterprise - Tam Yönetilen Cihaz** ve üzerinde **Android Enterprise - Konteyner** ek olarak kurulur veya doğrudan bir Android cihaz olarak kaydedilen yeni kayıtlı bir Android cihaz **Android Enterprise - Tam Yönetilen Cihaz** ile birlikte **Android Enterprise - Konteyner** üstüne.

COPE modu yalnızca Android 8, 9 ve 10 yüklü cihazlar için kullanılabilir

COPE Cihazları için Profillerin Yapılandırılması

COPE modunun kendisi için bir Yapılandırma profili olmadığından, **Android Enterprise - Tam Yönetilen Cihaz** ve **Android Enterprise - Konteyner** yapılandırması COPE profili içinde iki profile ayrılmıştır. Konsolun sol tarafındaki ilgili düğmeye tıklayarak her bir profilin yapılandırması için iki profil arasında geçiş yapmak mümkündür:





Her iki profil de her bir profil için açıklandığı şekilde yapılandırılabilir:

Android Enterprise - Tam Yönetilen Cihaz

Android Enterprise - Konteyner

AE Tam Yönetilen Cihaza Geri Dönme

Android Enterprise - Container profili **Mobil Yönetim** bölümünde açıklandığı gibi kaldırılabilir.

Konteyner profili kaldırıldığında, COPE profili bir **Android Kurumsal - Tam Yönetilen Cihaz** profiline dönüştürülecektir.

Android Enterprise – Konteyner Yapılandırması

O anda bir grup profili veya bir cihaz seçmiş olmanıza bağlı olarak, genel bakış ve alt noktaları farklılık gösterir - lütfen bunu dikkatlice değerlendirin!

Genel

Profile Genel Bakış (yalnızca profil düzeyinde)

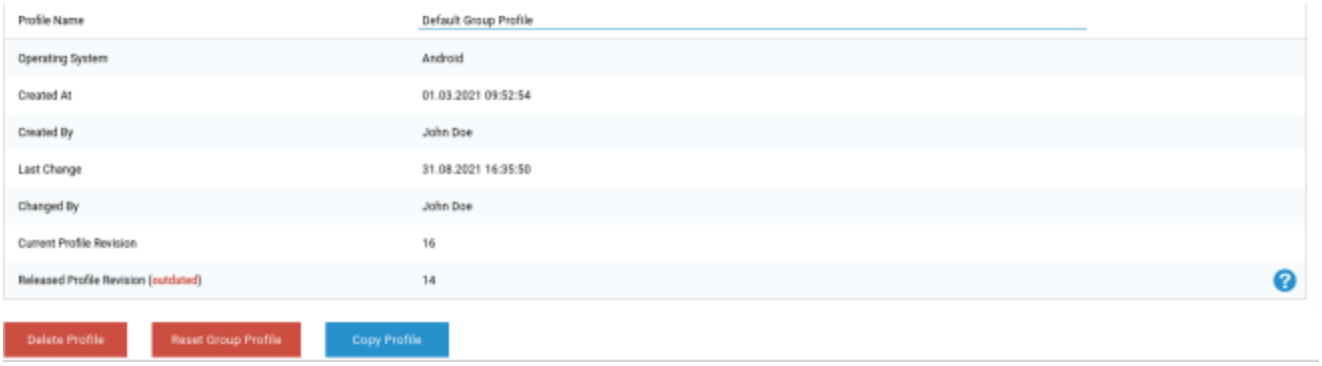
Bir profilin içindeyseniz, isim, işletim sistemi, oluşturma tarihi, yazar vb. açısından profil hakkında kısa bir genel bakış alacaksınız.

Profil Adı	Profil adı - doğrudan buradan yeniden adlandırılabilir
İşletim Sistemi	Profil için geçerli işletim sistemi
Şu Adreste Oluşturuldu	Oluşturulma tarihi
Tarafından Oluşturuldu	Tarafından oluşturuldu
Son Değişiklik	Son değişiklik tarihi
Tarafından Değiştirildi	Bu profilde son değişiklikleri yapan Kullanıcı
Güncel Profil Revizyonu	Profilin halihazırda kaç kez güncellendiği
Profil Revizyonu Yayınlandı	Profilin halihazırda güncellenmiş ve cihaz atanmış olma sayısı

Profil Sil	Profil Sil
Grup Profilini Sıfırla	Grup Profilini Sıfırla
Profil Kopyala	Profil Kopyala

Grup profiline genel bakış (yalnızca grup düzeyinde)

Bir grup profilini açtığınızda, profile hızlı bir genel bakış elde edersiniz.



Profil Adı	Profilin adı (burada değiştirilebilir)
İşletim Sistemi	Profilin ait olduğu İşletim Sistemi
Şu Adreste Oluşturuldu	Yaratılış zamanı
Tarafından Oluşturuldu	Profilin yaratıcısı
Son Değişiklik	Profilde yapılan son değişikliğin zamanı
Tarafından Değiştirildi	Son değişiklikleri yapan hesap
Güncel Profil Revizyonu	Kayıtlı profil durumunun revizyonu
Profil Revizyonu Yayınlandı	Atanmış profil revizyonu ("Şimdi ata"). Etiket metnin arkasında "(eski)" ibaresini gösteriyorsa, bu profili kaydettiğiniz ancak henüz atamadığınız anlamına gelir, bu nedenle cihazlar hala eski sürümü alacaktır.

Cihaza Genel Bakış (yalnızca cihaz düzeyinde)

Bir cihazda bulunmanız durumunda, seçilen cihazın genel bir özetini alacaksınız, burada aşağıdakiler yer almaktadır:

Cihaz Adı	Cihaz adı
Konum	Konum koordinatları
Telefon Numarası	Telefon numarası
Atanmış Zorunlu Uygulamalar	Atanan Zorunlu Uygulama Sayısı
İşletim Sistemi Sürümü	Cihazın işletim sistemi sürümü
İşletim Sistemi	İşletim Sistemi (Android Enterprise)
Seri Numarası	Cihaz seri numarası
Cihaz Sahipliği	Kurumsal veya özel cihaz
Cihaz Tipi	AE Work Yönetilen Cihaz
Köklü	Cihazın root edilip edilmediğini gösteren durum
Uyumlu	Kılavuza uygun
IP Adresi	Cihazın IP Adresi
Son Görülme	Cihazın AppTec'e en son bağlandığı zaman noktası
Son İtiş	Cihaza son push'un gönderildiği zaman noktası
Kullanıcı Ataması	Bu cihazın atandığı kullanıcı veya grup

Konfigürasyon Revizyonu

Burada cihaza hangi grup profilinin atandığına dair bir genel bakış elde edersiniz.

Grup profiline tıklarsanız, bu profile doğrudan erişim sağlarsınız ve ayarları gerçekleştirebilirsiniz.

Bu sembolle, dağıtılan uygulamaları grup profilinin ayarlarına geri döndürebilirsiniz.

Bu sembolle, kullanılan tüm uygulamaları grup profilinin ayarlarına geri döndürebilirsiniz.

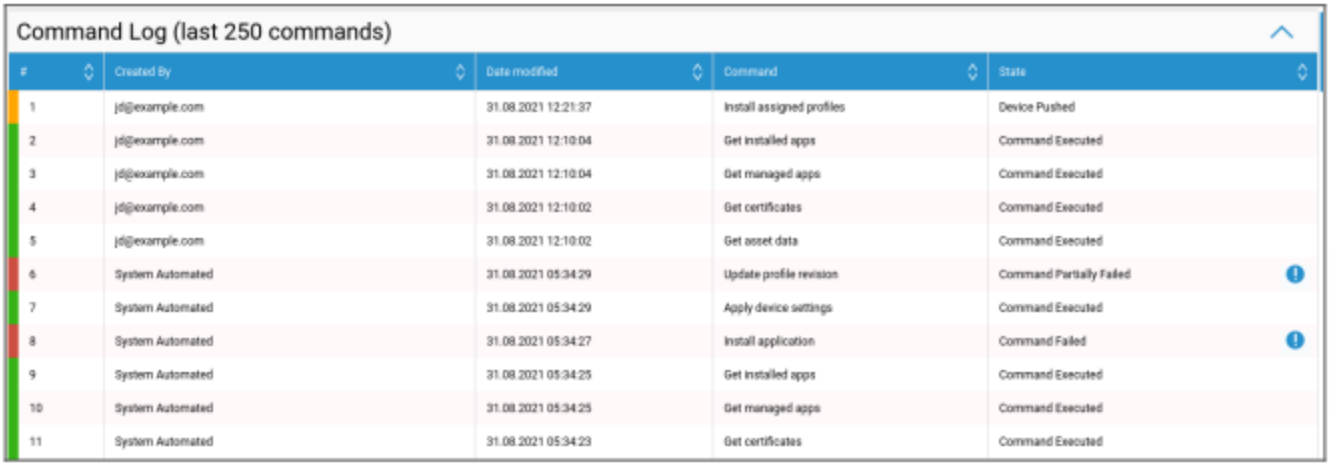
"Newer Revision available" grup profilinin değiştirildiğini ve kaydedildiğini ancak atanmadığını gösterir. Değişiklikleri cihazlara uygulamak için grup profilinin grup düzeyinde "Şimdi ata" ile atanması gerekir.

Cihaz Günlüğü (yalnızca cihaz düzeyinde)

Burada çeşitli cihaz günlükleri alacaksınız. Gerekirse, bir hatanın nedenini doğrudan buradan öğrenebilirsiniz.

Komut Günlüğü

Burada cihaz için hangi komutların verildiğini ve durumlarının ne olduğunu görebilirsiniz.



Olası komut durumları

Cihaz İtildi	Cihaza EMM sunucusuna geri bağlanmasını söylemek için push hizmetine (örn. APNS) bir push isteği gönderilmiştir.
Komut Oluşturuldu	Komut sistemde oluşturuldu.
Gönderilen Komut	Komut, sunucuya bağlandıktan sonra cihaza gönderildi.
Komut Yürütüldü	Komut başarıyla yürütüldü.
Komut Başarısız	Komut başarısız oldu. *
Komut Kısmen Başarısız	Cihazın işletim sistemine bağlı olarak bazı komutlar birlikte gruplandırılabilir. Bu komut grubunun bazı bölümleri başarısız olmuştur. *
Komut Yürütüldü, sonunda Başarısız Oldu	Komut uygulandı ama belki de uygulanmadı.
Komut Tekrar Gönderildi	Komut bir kullanıcı tarafından yeniden itildi.
Atılmış	Komut iptal edildi. Örneğin, başka bir komutun yerini aldığı için veya cihaz yeniden kaydedildiği ve eski komutlar kaldırıldığı için

*Mesajın arkasında bir ünlem işareti varsa, imlecinizi simgenin üzerine getirerek daha fazla bilgi alabilirsiniz.

Cihaz Ayarları

İstemci Yapılandırması

Burada Android cihazınızda aşağıdaki yapılandırmaları gerçekleştirebilirsiniz:

Uyumluluk Dışı Zaman	Zorlama eyleminin uygulanacağı kullanıcı yanıtı zaman aşımı sınırı.
Uyum zaman aşımından sonra yaptırım eylemi	Bir kullanıcı uyumlu bir cihaz durumuna yol açan eylemleri gerçekleştirmediğinde yaptırım eylemi
Veri Toplama Sıklığı	Cihaz/GPS bilgilerinin toplanma sıklığı
Cihaz Kalp Atışı Frekansı	Cihazın AppTec Sunucusu ile iletişime geçmesi gereken aralık Min. 1 dakika Max. 24 saat
Konum Güncellemelerini Etkinleştir	Etkinleştirilirse, cihaz konum güncellemelerini AppTec Sunucusuna gönderir
Konum Güncelleme Zamanı	Cihazın konum güncellemelerini AppTec'e hangi zaman aralıklarında göndereceğini belirler
Konum Güncellemesi için Google Konum Doğruluğunu Kullanın	Etkinleştirilirse, konum güncellemeleri için ağ konumu kullanılacaktır ("Kısıtlamalar" altında devre dışı bırakılmışsa, bu ayar hiçbir şeyi etkilemeyecektir)
Konum Güncellemesi için GPS Konumunu Kullanın	Etkinleştirilirse, konum güncellemeleri için GPS kullanılacaktır
Sahte (Fake) Konumlara İzin Ver	Üçüncü taraf uygulamalar aracılığıyla konum bilgilerinin sahtesinin yapılmasına izin verir
Kayıp Bağlantı Eylemi	Etkinleştirilirse, bir cihazın kalp atışı aralığında MDM sunucusuyla bağlantı kurmaması durumu için bir eylem belirleyebilirsiniz. Örneğin, cihazın 5 dakikalık bir kalp atışı süresi varsa, sunucuya saat 10:35'te bağlanır. Bundan sonra cihaz Wi-Fi menzilinden çıkar. Saat 10:40'taki bir sonraki kalp atışı başarısız olacak ve belirtilen eylem gerçekleştirilecektir.
Eylem	Bir cihaz uyumsuz hale gelir gelmez gerçekleştirilecek eylem. • Lock Cihaz = kilit cihazı • Cihazı Sil = cihaz fabrika ayarlarına geri yüklenir • Cihazı ve SD Kartı Sil = cihaz fabrika ayarlarına geri yüklenecek ve SD Kart depolama alanı silinecektir

Eşik	Belirtilen eylemi tetiklemek için gerekli olan başarısız Kalp Atışı eşiğini belirleyebilirsiniz.

İlke Uygulama Modu	Varsayılan değer:	Kullanıcılardan periyodik olarak bekleyen eylemleri gerçekleştirmeleri istenecektir
	Tembel Politika Uygulaması:	Kullanıcılardan hiçbir zaman bekleyen eylemleri gerçekleştirmeleri istenmeyecektir. Tüm açık eylemler AppTec İstemcisinde gösterilecektir
	Agresif Politika Uygulaması:	Kullanıcılardan bekleyen eylemleri gerçekleştirmeleri için durmaksızın bilgi istenecektir
AppTec Sürüm Kilidi	Etkinleştirilirse, AppTec uygulaması için bir sürüm kodu belirtilebilir. AppTec istemcisi yalnızca belirtilen sürüme güncelleme yapacaktır. Daha yeni sürümler göz ardı edilecektir. Düşürme mümkün DEĞİLDİR.	
Sürüm Kodu	AppTec uygulamasının kilitleneceği sürüm kodu.	
AppTec Bildirimini Devre Dışı Bırak	Devre dışı bırakılırsa AppTec İstemcisi Bildirim Çubuğunda bir Bildirim göstermez. Böylece kullanıcılar AppTec istemcisini görev yöneticisi aracılığıyla kapatabilir. AppTec istemcisi kapalıysa, Kiosk Modu ve Uygulama Siyah / Beyaz Listeleme gibi çeşitli özellikler düzgün çalışmayacaktır. Samsung cihazları AppTec İstemcisi için bir koruma mekanizması sunar. KNOX API'lerini destekleyen Samsung cihazlarında bildirim varsayılan olarak devre dışıdır. Bildirim, Android 8.0 veya üzeri sürümlere sahip cihazlarda devre dışı bırakılmamalıdır.	

Duvar Kağıdı

Özel Duvar Kağıdı Ayarla	Özel duvar kağıdını etkinleştirme/devre dışı bırakma
Duvar Kağıdı	Duvar kağıdı modunu bir renk kodu veya bir resim kullanacak şekilde ayarlama
Bir Renk Belirtin	Arka plan rengini hex değeri olarak belirtin, örneğin siyah için #000000 veya beyaz için #ffffff
Resmi Duvar Kağıdı Olarak Ayarla	Duvar kağıdı olarak kullanmak istediğiniz resim dosyasını yükleyin

Varlık Yönetimi (yalnızca cihaz düzeyinde)

Cihaz Bilgisi

Model	Cihaz model tanımı
İşletim Sistemi	İŞLETIM SISTEMI
İşletim Sistemi Sürümü	İşletim sistemi sürümü
Seri Numarası	Seri numarası
Cihaz Adı	Cihaz adı
Pil Durumu	Pil durumu
Boş / Toplam Bellek	Boş / Toplam bellek
Samsung Safe	Samsung SAFE arayüzü, çeşitli ayar seçenekleri için gereklidir
SD Kart Mevcut	SD Kart mevcut
SD Kart Emülasyonlu	SD Kart emülasyonu
SD Kart Çıkarılabilir	SD Kart çıkarılabilir
SD Boş / Toplam Bellek	SD Boş / Toplam SD Kart belleği

Wi-Fi

IP Adresi	Cihaz IP adresi
WiFi MAC	WiFi MAC adresi

Hücresel

Durum	Durum (SIM kart takılı)
Telefon Numarası	Telefon Numarası
Dolaşım (Ses / Veri)	Ses / veri için dolaşım
Dolaşım Durumu	Mevcut dolaşım durumu
IP Adresi	IP adresi
Operatör/Taşıyıcı	Operatör/Taşıyıcı
Hücresel Teknoloji	Hücresel Teknoloji
IMEI	IMEI numarası
ICCID	Bu, SIM kartın kimliğidir, çoğu zaman bir Akıllı Kart veya Entegre Devre Kartı (ICC) da olabilir
IMSI	Uluslararası Mobil Abone Kimliği (IMSI), GSM ve UMTS mobil ağlarında ağ kullanıcılarının kesin bir şekilde tanımlanmasını sağlar IMSI en fazla 15 basamaktan oluşur ve aşağıdaki şekilde yapılandırılır: • Mobil Ülke Kodu (MCC), 3 basamaklı • Mobil Ağ Kodu (MNC), 2 veya 3 basamaklı • Mobil Abone Kimlik Numarası (MSIN), 1-10 hane
Mevcut MCC/MNC	Bkz. "SIM MCC/MNC"
SIM MCC/MNC	Mobil Ülke Kodu, E.212 uyarınca ITU tarafından belirlenen yerleşik bir ülke tanımlayıcısıdır Standart. Bu, mobil ağın tanımlanması için Mobil Ağ Kodu (MNC) ile birlikte çalışır. SIM kartın ülke/Mobil Ağ Kodu anlamına gelir. Başka bir mobil ağda dolaşım yaparsanız, mantıksal olarak "Mevcut MCC/MNC" ve "SIM MCC/MNC" farklı olacaktır.

Bluetooth

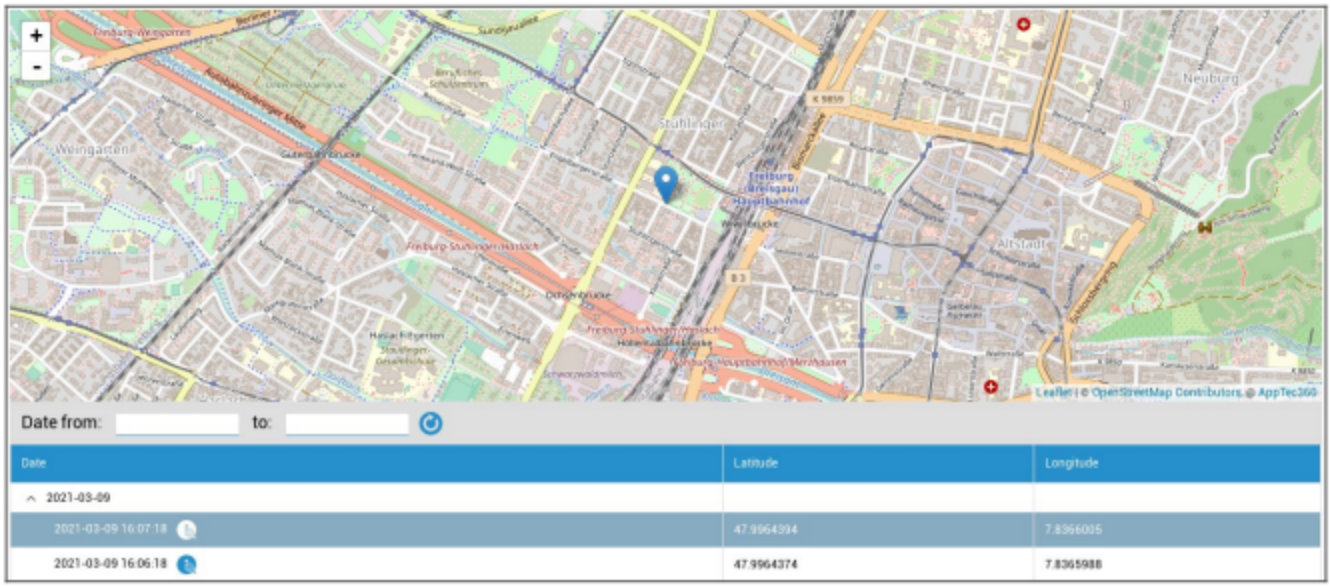
Bluetooth MAC	Bluetooth MAC adresi

Güvenlik Yönetimi

Hırsızlığa Karşı Koruma (yalnızca cihaz düzeyinde)

GPS Bilgileri (yalnızca cihaz düzeyinde)

Burada mevcut/son cihaz konumunu belirleyebilirsiniz. Yerelleştirme bir veya iki parola ile korunabilir - Bkz: Genel Ayarlar - Gizlilik - GPS Erişimi



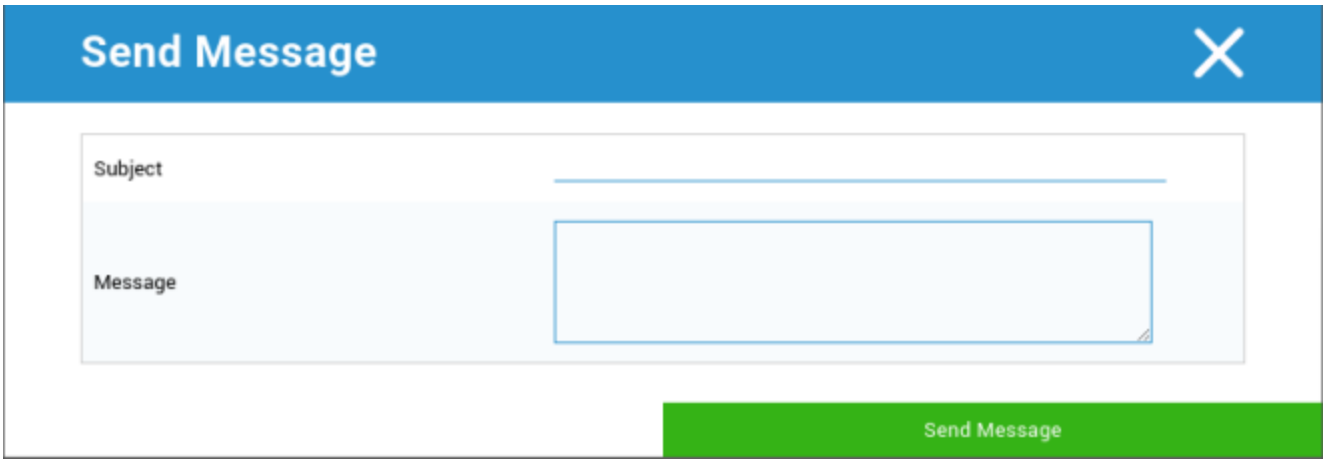
Sil ve Kilitle (yalnızca cihaz düzeyinde)

"Sil ve Kilitle" altında aşağıdaki üç eylemi gerçekleştirebilirsiniz:

Tam Silme	Cihaz fabrika ayarlarına geri döndürülür (kurumsal ve kişisel veriler silinir). Yalnızca Geliştirilmiş Çalışma Profili için çalışır
Kurumsal Silme	Son kullanıcı cihazından yalnızca kurumsal veriler kaldırılır (AppTec tarafından sağlanan tüm uygulamalar, veriler vb.)
Kilit Ekranı	Ekran kilidi etkinleştirildiğinde, cihazın kilidini cihaz şifresi/PIN ile açmak yeterlidir

Mesaj (yalnızca cihaz düzeyinde)

Burada konuyu ve mesajı doldurabilir ve bir son kullanıcı cihazına gönderebilirsiniz



Güvenlik Yapılandırması

Cihaz Parolası

"Parola" altında bir cihaz parolası belirleyebilirsiniz, aşağıdaki ayar seçeneklerini kullanabilirsiniz

Minimum parola uzunluğu	Bir parolanın sahip olması gereken minimum sembol sayısını belirler	
Şifre kalitesi	Belirtilmemiş	Bu politikada parola için herhangi bir gereklilik yoktur.
	Biyometrik Zayıf	Bu politika, düşük güvenlikli biyometrik tanıma teknolojisine izin vermektedir. Bu, bir bireyin kimliğini yaklaşık 3 haneli bir PIN koduna kadar tanıyabilen teknolojiler anlamına gelir (yanlış algılama 1.000'de 1'den azdır).
	Bir şey	Bu ilke, bir tür parola veya kalıp belirlenmesini gerektirir, ancak herhangi bir özel kural uygulamaz.
	Alfabetik	Kullanıcı en az alfabetik (veya diğer sembol) karakterler içeren bir parola girmiş olmalıdır.
	Alfanümerik	Kullanıcı, en az hem sayısal hem de alfabetik (veya diğer sembol) karakterleri içeren bir parola girmiş olmalıdır.
	Kompleks	Kullanıcı, varsayılan olarak en az bir harf, bir rakam ve bir özel sembol içeren bir parola girmiş olmalıdır. Bu parola kalitesiyle, parolalar en az bir büyük harf vb. gibi çeşitli karakter kümeleri içerecek şekilde kısıtlanabilir.
Minimum parola uzunluğu	Parola için gerekli karakter sayısını ayarlayın. Örneğin, PIN veya parolaların en az altı karakterden oluşmasını zorunlu tutabilirsiniz.	
Parolada gerekli minimum sayısal basamaklar	Parolada gerekli minimum sayısal basamaklar	
Parolada gereken minimum küçük harf sayısı	Parolada gereken minimum küçük harf sayısı	
Parolada gerekli minimum büyük harfler	Parolada gerekli minimum büyük harfler	

Parolada gerekli minimum harf dışı karakterler	Parolada gerekli minimum harf dışı karakterler
Parolada gereken minimum semboller	Parolada gereken minimum semboller

Maksimum hareketsizlik süresi kilidi	Zaman kilidine kadar maksimum kullanıcı hareketsizliği
Parola sona erme zaman aşımı	Oluşturur, hangi zaman aralığından sonra parolanın süresi dolar ve yeni bir parola verilmelidir
Parola geçmişi kısıtlaması	İzin verilmeyen önceden kullanılmış şifre sayısı
Maksimum başarısız parola denemesi	Tam bir cihaz silme işlemi gerçekleştirilmeden önce bir parolanın ne kadar sıklıkla yanlış girilebileceğini belirler
Biyometrik Kimlik Doğrulamaya İzin Ver	Parmak izi veya iris taraması yoluyla kimlik doğrulamayı etkinleştirir. Sadece Samsung KNOX 2.1 ve üstü için

Konteyner Şifresi

"Parola" altında bir konteyner parolası belirleyebilirsiniz, aşağıdaki ayar seçenekleri şunlardır sizin için kullanılabilir

Minimum parola uzunluğu	Bir parolanın sahip olması gereken minimum sembol sayısını belirler	
Şifre kalitesi	Belirtilmemiş	Bu politikada parola için herhangi bir gereklilik yoktur.
	Biyometrik Zayıf	Bu politika, düşük güvenlikli biyometrik tanıma teknolojisine izin vermektedir. Bu, bir bireyin kimliğini yaklaşık 3 haneli bir PIN koduna kadar tanıyabilen teknolojiler anlamına gelir (yanlış algılama 1.000'de 1'den azdır).
	Bir şey	Bu ilke, bir tür parola veya kalıp belirlenmesini gerektirir, ancak herhangi bir özel kural uygulamaz.
	Alfabetik	Kullanıcı en az alfabetik (veya diğer sembol) karakterler içeren bir parola girmiş olmalıdır.
	Alfanümerik	Kullanıcı, en az hem sayısal hem de alfabetik (veya diğer sembol) karakterleri içeren bir parola girmiş olmalıdır.
	Kompleks	Kullanıcı, varsayılan olarak en az bir harf, bir rakam ve bir özel sembol içeren bir parola girmiş olmalıdır. Bu parola kalitesiyle, parolalar en az bir büyük harf vb. gibi çeşitli karakter kümeleri içerecek şekilde kısıtlanabilir.
Minimum parola uzunluğu	Parola için gerekli karakter sayısını ayarlayın. Örneğin, PIN veya parolaların en az altı karakterden oluşmasını zorunlu tutabilirsiniz.	
Parolada gerekli minimum sayısal basamaklar	Parolada gerekli minimum sayısal basamaklar	
Parolada gereken minimum küçük harf sayısı	Parolada gereken minimum küçük harf sayısı	
Parolada gerekli minimum büyük harfler	Parolada gerekli minimum büyük harfler	
Parolada gerekli minimum harf dışı karakterler	Parolada gerekli minimum harf dışı karakterler	

Parolada gereken minimum semboller	Parolada gereken minimum semboller

Maksimum hareketsizlik süresi kilidi	Zaman kilidine kadar maksimum kullanıcı hareketsizliği
Parola sona erme zaman aşımı	Oluşturur, hangi zaman aralığından sonra parolanın süresi dolar ve yeni bir parola verilmelidir
Parola geçmişi kısıtlaması	İzin verilmeyen önceden kullanılmış şifre sayısı
Maksimum başarısız parola denemesi	Tam bir cihaz silme işlemi gerçekleştirilmeden önce bir parolanın ne kadar sıklıkla yanlış girilebileceğini belirler

AntiVirüs

Otomatik Tarama	Periyodik otomatik taramaları etkinleştirin
Tarama Aralığı	Muayene aralığı (Hızlı / Tam)
Tam Otomatik Tarama	Tam otomatik taramaları etkinleştirin
Otomatik Güncellemeler	Otomatik güncellemeleri etkinleştirin
Güncelleme Kontrol Aralığı	Uygulamanın ve veritabanının ne sıklıkla güncellenmesi gerektiği (virüsler / hasarlı kod)
Uygulama Koruması	Otomatik uygulama taramasını etkinleştirin
SD Kart Koruması	Otomatik SD Kart taramasını etkinleştirin
Yalnızca Wi-Fi Güncellemesi	Etkinleştirildiğinde, güncellemeler yalnızca cihaz bir Wi-Fi ağına başarıyla bağlandığında uygulanır

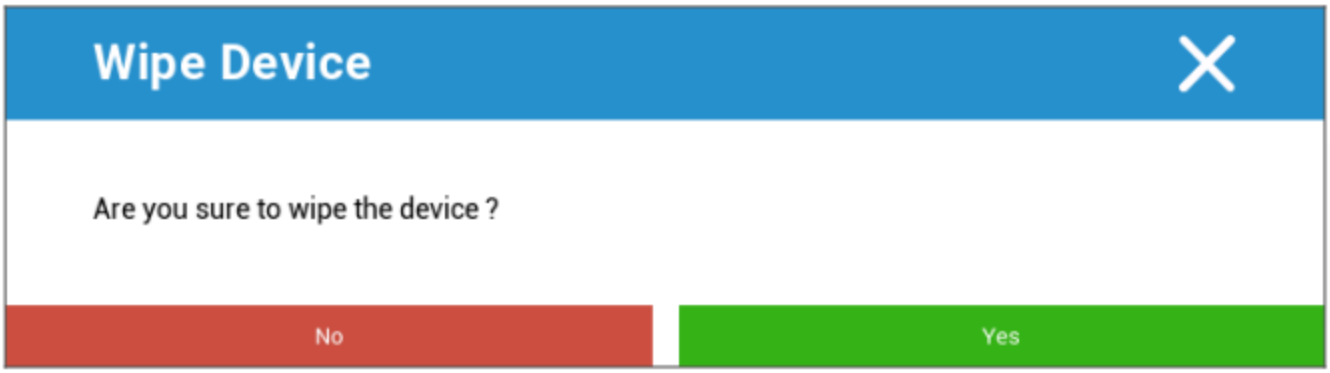
Kullanım Ömrü Sonu (yalnızca cihaz düzeyinde)

Silme (yalnızca cihaz düzeyinde)

"Sil" altında, cihazı fabrika ayarlarına geri döndürebilirsiniz (Yalnızca Gelişmiş Çalışma Profilinde).

Burada kurumsal verilerin yanı sıra özel veriler de son kullanıcı cihazında silinecektir.

"Eksi Sembolü" üzerine tıkladığınızda aşağıdaki mesajı alırsınız:



"Evet" ile silme işlemini gerçekleştirebilirsiniz.

"Silme Raporu" altında aşağıdaki öğeler görüntülenebilir

Tarafından silindi	Silme işlemini kimin yaptığına dair tarihçe
Tarih	Tarih
Durum	Durum (örn. Silme işlemi başarıyla gerçekleştirildiyse)

Kısıtlama Ayarları

Kısıtlamalar

Burada, çeşitli şeyler kısıtlanabilir ve engellenebilir.

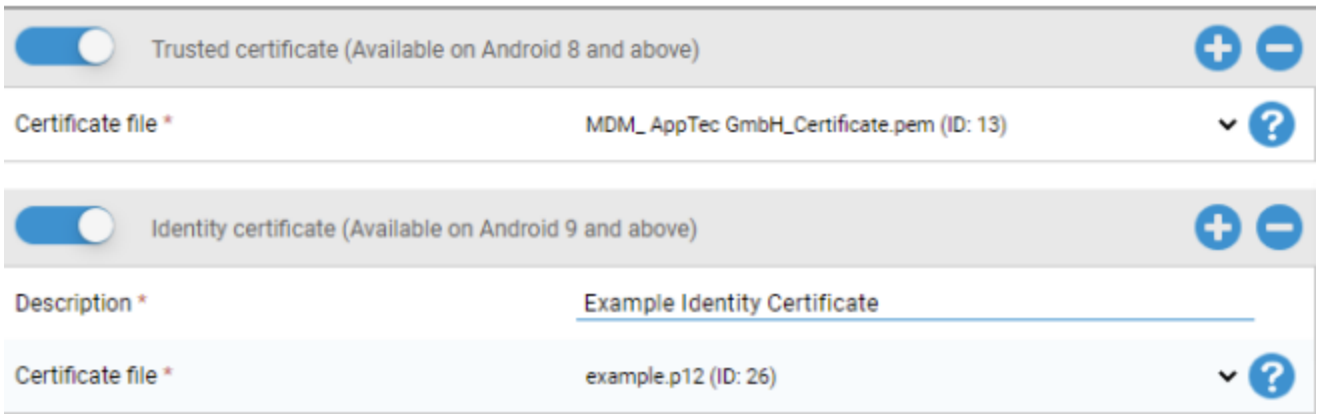
Uyum Uygulama	Mod Kullanıcıya Sor - Kullanıcıdan gerekli eylemleri yerine getirmesi istenir. Mod Kilitleme Konteyneri - Tüm gereksinimler yerine getirilene kadar tüm uygulamaları gizleyin
Çalışma Zamanı İzin Politikası	Yeni izin talepleri için kullanıcıya sor Her zaman yeni izin taleplerini kabul edin Yeni izin taleplerini her zaman reddedin Uyarı: Bunlar otomatik olarak ayarlanırsa bazı Uygulamalar izinleri tanımada sorun yaşar. İzinleri her zaman veriyorsanız ve izinlerin eksik olduğunu söyleyen uygulamalarla ilgili sorunlarla karşılaşıyorsanız, bunu "kullanıcıya sor" olarak ayarlayın ve uygulamayı yeniden yükleyin
Giden panoya izin ver	Konteynerin içinden dışına kopyalama ve yapıştırmaya izin verir
Arayan Kimliği Çözümlemesine İzin Ver	Kapsayıcıdaki kişilere bağlı olarak gelen bir aramanın adını gösterir
Kişi Arama Çözümüne İzin Ver	Arama yaparken konteyner kişilerinde isim aramaya izin verir
Bluetooth Kişi Paylaşımına İzin Ver	Arabada konteyner temasına erişim sağlar
Giden NFC Işınına İzin Verme	Konteyner için NFC'yi devre dışı bırakır
Bilinmeyen Kaynaklara İzin Ver	Etkinleştirilirse, kullanıcılar bir .apk dosyası yükleyerek Uygulamaları yandan yükleyebilir.
USB Hata Ayıklamaya İzin Ver	Etkinleştirilirse, kullanıcılar USB Hata Ayıklamayı etkinleştirebilir.
Hesap Değişikliğine İzin Verme	Kapsayıcıdaki Hesapların oluşturulmasına, silinmesine ve değiştirilmesine izin vermez Bazı uygulamaların beklendiği gibi çalışması için hesap oluşturması veya hesapları değiştirmesi gerektiğini unutmayın

İş Profili Kısıtlamaları. Yalnızca Android 11 ve üzeri cihazlarda, Geliştirilmiş Çalışma Profili ile kullanılabilir	
Kameraya İzin Verme	Çalışma profilinde kameraya izin verilip verilmediğini belirtir.
Bluetooth'a İzin Verme	Çalışma profilinde bluetooth'a izin verilmeyip verilmediğini belirtir.
Fabrika Ayarlarına Sıfırlama Korumasını Etkinleştir	Android'in Fabrika Ayarlarına Sıfırlama Korumasını "Genel Ayarlar" → "Android Yapılandırması" → "Android Enterprise" → "Fabrika Ayarlarına Sıfırlama Koruması" bölümünde tanımladığınız Google Hesabına geçersiz kılmak için bunu etkinleştirin. Bu etkinleştirilirse ve cihazı sıfırlarsanız, cihazı yeniden kurmak için yapılandırılmış Google Hesabını sağlamanız gerekecektir.
İşletim Sistemi Güncellemesini Kontrol Et	Güncelleme davranışını otomatik, pencereli veya ertelenmiş olarak ayarlamak için bunu etkinleştirin.
Güncelleme Politikası	Otomatik: Bir güncelleme mevcut olur olmaz otomatik olarak yükleyin. Pencereli: Günlük bakım penceresi içinde otomatik olarak yükleyin. Bu aynı zamanda Play uygulamalarını pencere içinde güncellenecek şekilde yapılandırır. Bu, kiosk cihazları için şiddetle tavsiye edilir çünkü ön plana kalıcı olarak sabitlenen uygulamaların Play tarafından güncellenebilmesinin tek yolu budur. Ertele: Otomatik yüklemeyi en fazla 30 güne kadar erteleyin.

Kişisel Profil Kısıtlamaları. Yalnızca Android 11 ve üzeri cihazlarda, Geliştirilmiş Çalışma Profili ile kullanılabilir	
Kameraya İzin Verme	Kameraya kişisel profilde izin verilip verilmediğini belirtir.
Bluetooth'a İzin Verme	Kişisel profilde bluetooth'a izin verilmeyip verilmediğini belirtir.
Bilinmeyen Kaynaklara İzin Ver	Etkinleştirilirse, iş profili kullanıcıları bir .apk dosyası yükleyerek Uygulamaları yandan yükleyebilir.

Sertifika Yönetimi

Burada Güvenilir Sertifikaları ve Kimlik Sertifikalarını cihazlarınıza dağıtabilirsiniz. Güvenilir Sertifikaları dağıtmak için Android 8 veya üstü, Kimlik Sertifikalarını dağıtmak için ise Android 9 veya üstü gereklidir.



"+" ile birden fazla sertifika ekleyebilirsiniz.

Güvenilir Sertifikaların PEM formatında olması gerekir.

Kimlik Sertifikalarının PKCS12 formatında olması gerekir.

Bağlantı Yönetimi

Wifi

Bu ayar için, dahili Erişime erişim için son kullanıcı cihazlarının ön yapılandırmasını gerçekleştirin Puanlar

Hizmet Seti Tanımlayıcısı (SSID)	Bağlanılacak ağ için SSID
Gizli Ağ	AP'nin SSID'yi yayınlamaması durumunda etkinleştirin

Güvenlik Türü

AP'nin güvenlik türünü belirleyin

WEP

Şifre	AP için şifre

WPA/WPA2

Şifre	AP için şifre

802.1x EAP

EAP-Metodu

PWD	Kimlik	Kimlik
	Şifre	Şifre

PEAP	Faz 2 Kimlik Doğrulama Protokolü	Hiçbiri	Ek protokol yok
		MSCHAPV2	MSCHAPV2 protokolü
		GTC	GTC protokolü
	CA Sertifikası	CA sertifikası	
	Kimlik	Kimlik	
	Anonim Kimlik	Anonim kimlik	
	Şifre	Şifre	

TTLS	Faz 2 Kimlik Doğrulama Protokolü	Hiçbiri	Ek protokol yok
		PAP	PAP protokolü
		MSCHAP	MSCHAP protokolü
		MSCHAPV2	MSCHAPV2 protokolü
		GTC	GTC protokolü
	CA Sertifikası	CA Sertifikası	
	Kimlik	Kimlik	
	Anonim Kimlik	Anonim Kimlik	
	Şifre	Şifre	

TLS	CA Sertifikası	CA sertifikası
	Kimlik	Kimlik
	Şifre	Şifre

VPN

Bağlantı Adı	VPN Bağlantısının Adı

VPN Türü

VPN

VPN İstemcisi

AppTec VPN İstemcisi	
Ağ Geçidi Yapılandırması	Ağ Geçidi VPN Yapılandırmasını seçin (Bkz. **Genel Ayarlar > Evrensel Ağ Geçidi > VPN Ayar**ları)
Her Zaman Açık VPN	Yerel Kilitlemeyi Etkinleştir
AppTec Kilitlemeyi Etkinleştir	AppTec Kilitlemeyi Etkinleştir

Dahili (Yalnızca Samsung cihazlarda mevcuttur)			
Bağlantı Türü	PPTP	Sunucu	Sunucu
		PPTP Şifrelemesini Etkinleştir	PPTP Şifrelemesini Etkinleştir
	L2TP / IPSec PSK	Sunucu	Sunucu
		IPSec Ön Paylaşımlı Anahtar	IPSec Ön Paylaşımlı Anahtar
		L2TP Sırrını Etkinleştir	L2TP Sırrını Etkinleştir
		L2TP Sırrı	L2TP Sırrı
	IPSec XAuth PSK	Sunucu	Sunucu
		IPSec Tanımlayıcı	IPSec Tanımlayıcı
		IPSec Ön Paylaşımlı Anahtar	IPSec Ön Paylaşımlı Anahtar
DNS Arama Alanları	DNS Arama Alanları		
Uzman Ayarları	DNS Sunucuları	DNS Sunucuları	
	Yönlendirme Rotaları	Yönlendirme Rotaları	

Açık VPN		
Sunucu	Sunucu	
OpenVPN Profili	OpenVPN Profili	
OpenVPN Uygulaması	Android için OpenVPN (önerilir)	
	OpenVPN Bağlantısı	
Uzman Ayarları	DNS Sunucuları	DNS Sunucuları
	Yönlendirme Rotaları	Yönlendirme Rotaları

Samsung / Güçlü Kuğu			
Bağlantı Türü	PPTP	Sunucu	Sunucu
		Kullanıcı Adı	Kullanıcı Adı
		Şifre	Şifre
		PPTP Şifrelemesini Etkinleştir	PPTP Şifrelemesini Etkinleştir
	L2TP / IPSec PSK	Sunucu	Sunucu
		IPSec Ön Paylaşımlı Anahtar	IPSec Ön Paylaşımlı Anahtar
		Kullanıcı Adı	Kullanıcı Adı
		Şifre	Şifre
		L2TP Sırrını Etkinleştir	L2TP Sırrı
	IPSec XAuth PSK	Sunucu	Sunucu
		IPSec Tanımlayıcı	IPSec Tanımlayıcı
		IPSec Ön Paylaşımlı Anahtar	IPSec Ön Paylaşımlı Anahtar
		Kullanıcı Adı	Kullanıcı Adı
		Şifre	Şifre
Uzman Ayarları	DNS Sunucuları	DNS Sunucuları	
	Yönlendirme Rotaları	Yönlendirme Rotaları	

Cisco Any Connect		
Sunucu	Sunucu	
Sertifika Modu	Engelli	Engelli
	Otomatik	Otomatik
Uzman Ayarları	DNS Sunucuları	DNS Sunucuları
	Yönlendirme Rotaları	Yönlendirme Rotaları

Uygulama Başına VPN

VPN İstemcisi

AppTec VPN İstemcisi		
Ağ Geçidi Yapılandırması	Ağ Geçidi VPN Yapılandırmasını seçin (Bkz. **Genel Ayarlar > Evrensel Ağ Geçidi > VPN Ayar**ları)	
VPN Uygulamaları	VPN Uygulamaları	
Her Zaman Açık VPN	Yerel Kilitlemeyi Etkinleştir	Her Zaman Açık VPN
AppTec Kilitlemeyi Etkinleştir	AppTec Kilitlemeyi Etkinleştir	

Samsung / Güçlü Kuğu			
Bağlantı Türü	PPTP	Sunucu	Sunucu
		VPN Uygulamaları	VPN Uygulamaları
		Kullanıcı Adı	Kullanıcı Adı
		Şifre	Şifre
		PPTP Şifrelemesini Etkinleştir	PPTP Şifrelemesini Etkinleştir
	L2TP / IPSec PSK	Sunucu	Sunucu
		VPN Uygulamaları	VPN Uygulamaları
		IPSec Ön Paylaşımlı Anahtar	IPSec Ön Paylaşımlı Anahtar
		Kullanıcı Adı	Kullanıcı Adı
		Şifre	Şifre
		L2TP Sırrını Etkinleştir	L2TP Sırrı
	IPSec XAuth PSK	Sunucu	Sunucu
		VPN Uygulamaları	VPN Uygulamaları
		IPSec Tanımlayıcı	IPSec Tanımlayıcı
		IPSec Ön Paylaşımlı Anahtar	IPSec Ön Paylaşımlı Anahtar
		Kullanıcı Adı	Kullanıcı Adı
		Şifre	Şifre
Uzman Ayarları	DNS Sunucuları	DNS Sunucuları	
	Yönlendirme Rotaları	Yönlendirme Rotaları	

Kısıtlamalar

Burada bağlantı yönetimi ile ilgili kısıtlamaları ayarlayabilirsiniz

Veri Dolaşımına İzin Ver	Dolaşımdayken mobil veriye izin ver
Veri Dolaşımını Zorla	Etkinleştirilirse, mobil veri için dolaşım kalıcı olarak etkinleştirilir (önerilmez!) Bu ayar "Veri Dolaşımına İzin Ver" ayarının üzerine yazılır!
Sistem http Proxy Sunucusu Kullanma	Sistemin ayarlar bölümünde sağlanan bir HTTP proxy sunucusunun kullanımı bağlı ağa (WiFi veya APN) bağlıdır

PIM Yönetimi

Gmail Değişimi

Bilgi: Bu Yapılandırma Gmail uygulamasına uygulanacaktır. Bu yüzden Gmail'i onaylamanız ve yüklemeniz gerekir.

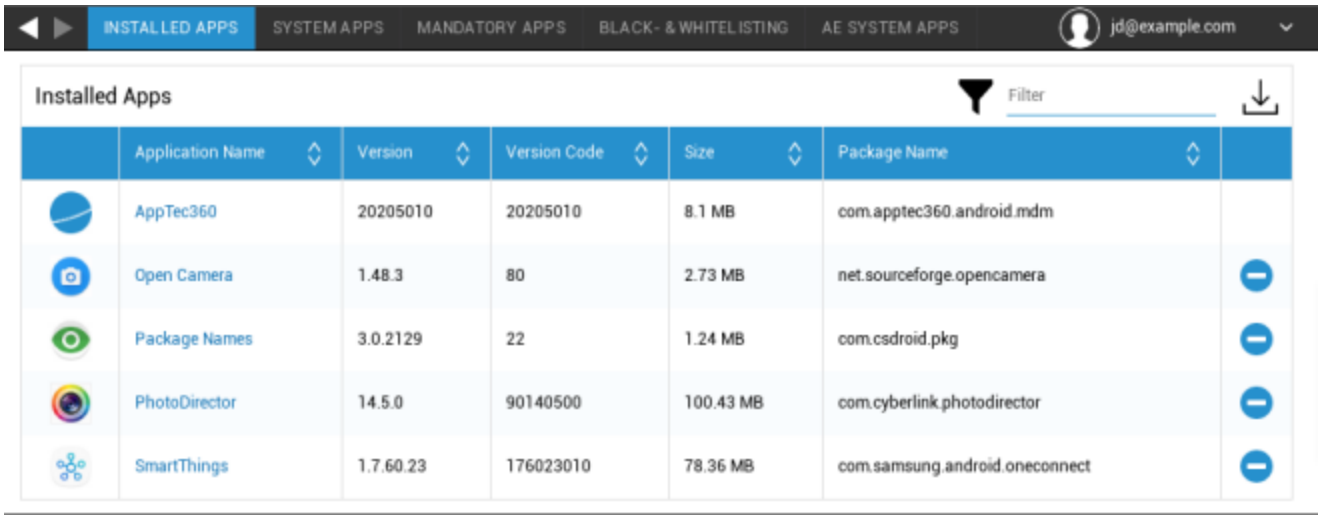
e-Posta Adresi	Sağlanan kullanıcının e-posta adresi Lütfen kimlik bilgileriyle çalışmak için kullanabileceğiniz ve her cihazda manuel olarak değişiklik yapmadığınız "Yer tutuculara" dikkat edin Bir tıklama ile bunları kendiniz için görüntüleyebilirsiniz
Sunucu Ana Bilgisayar Adı	Exchange Sunucularınızın sunucu adresi
Giriş adı	İlgili son kullanıcı cihazı için Oturum Açma Adı, lütfen "Buradaki yer tutuculara da dikkat edin
İmza	Bir imza eklenebilir (İpucu: Bazı cihazlar imza için HTML biçimlendirmesi gerektirir)
Senkronize edilecek önceki gün sayısı	E-postaların ne zaman geri senkronize edileceğini belirleyen gün sayısı
Cihaz Tanımlayıcısı	Ein String der die EAS DeviceID enthält. Bu, EAS Protokollerinin bir parçasıdır ve bazı bölgelerde kullanılabilir
Güvenli Yuva Katmanı (SSL) kullanın	SSL bağlantısı kullanın
Tüm sertifikaları kabul edin	Tüm sertifikalar kabul edilmektedir. Exchange Server'ınız kendinden imzalı bir sertifika kullanıyorsa lütfen bu seçeneği seçin
Yönetilmeyen hesaplara izin ver	Kullanıcıların, bu yönetilen yapılandırmada belirtilen hesap dışında herhangi bir Exchange hesabı eklemesine veya kaldırmasına izin verin. Bu ayar etkinleştirilirse, kullanıcıların Gmail'e başka Exchange hesapları eklemesini engelleyemezsiniz. Ayrıca diğer uygulamalar ve kullanıcılar tarafından eklenen Exchange hesapları arasında veri paylaşımını kontrol edemezsiniz. Bu ayar yalnızca kullanıcılarınızın Gmail'de birden fazla iş Exchange hesabı bulundurması gerekiyorsa etkinleştirilmelidir.
Müşteri Sertifikası	Müşteri Sertifikası. Yalnızca Posta Sunucunuz bunun mevcut olmasını bekliyorsa gereklidir.

Uygulama Yönetimi

Kurumsal Uygulama Yöneticisi

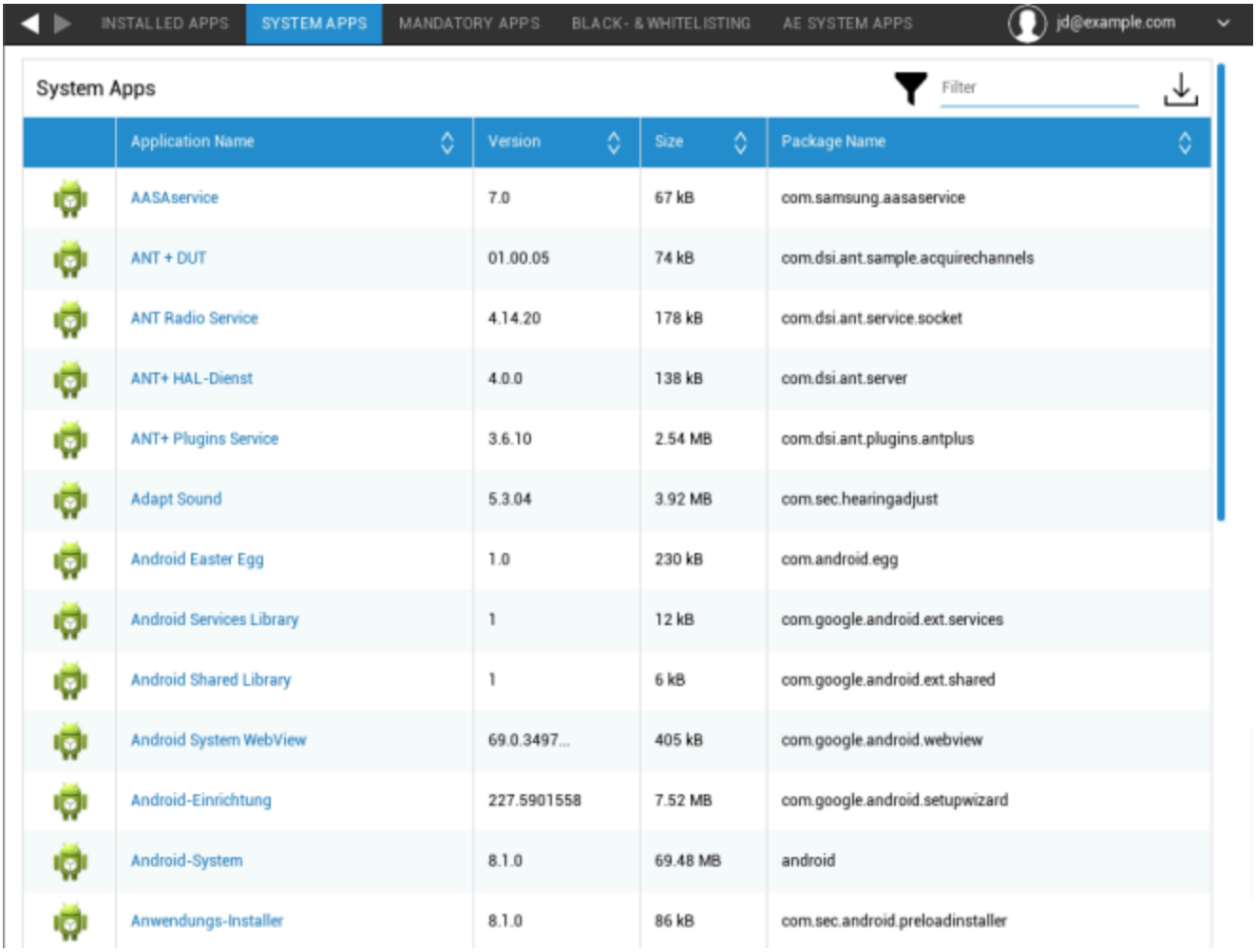
Yüklü Uygulamalar (yalnızca cihaz düzeyinde)

Burada, konteynerde o anda yüklü olan tüm Uygulamalar sizin için görüntülenecektir.



Sistem Uygulamaları (yalnızca cihaz düzeyinde)

"Sistem Uygulamaları" altında, cihaz üreticiniz tarafından son kullanıcı cihazına zaten yüklenmiş olan tüm uygulamalar ve hizmetler sizin için listelenecektir.

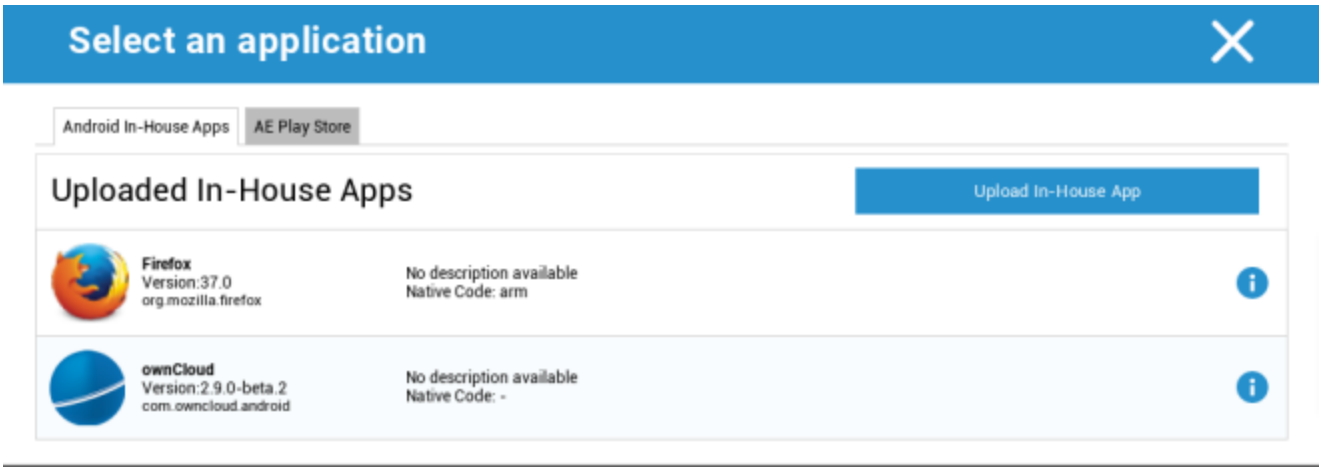


Zorunlu Uygulamalar

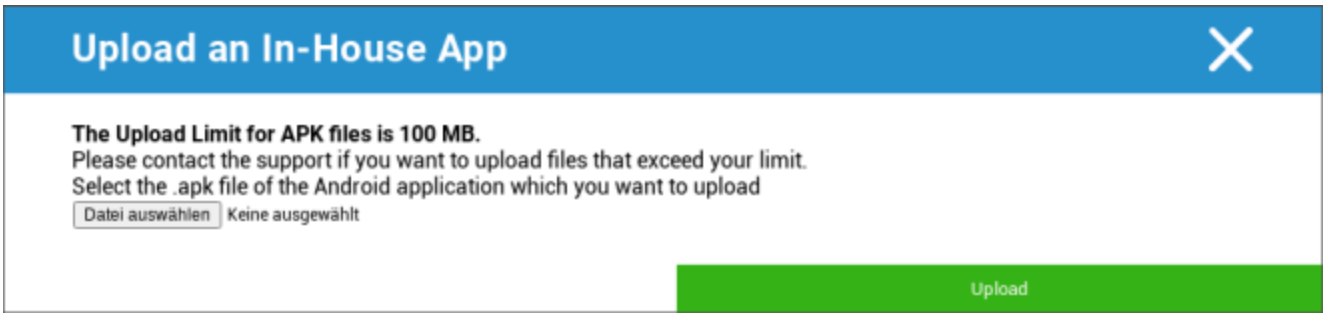
Zorunlu Uygulamalar altında, zorunlu gerekli uygulamaları belirleyebilirsiniz. Eğer bu bir Şirket İçi Uygulama ise, kullanıcıdan sürekli olarak bu belirlenmiş uygulamayı yüklemesi istenecektir. Play Store uygulamaları otomatik olarak yüklenecektir.

aracılığıyla zorunlu gerekli uygulama tanımlanabilir.

Bu, Genel Ayarlar'da yüklediğiniz "Android Şirket İçi Uygulamalar "dan bir Şirket İçi Uygulama olabilir.

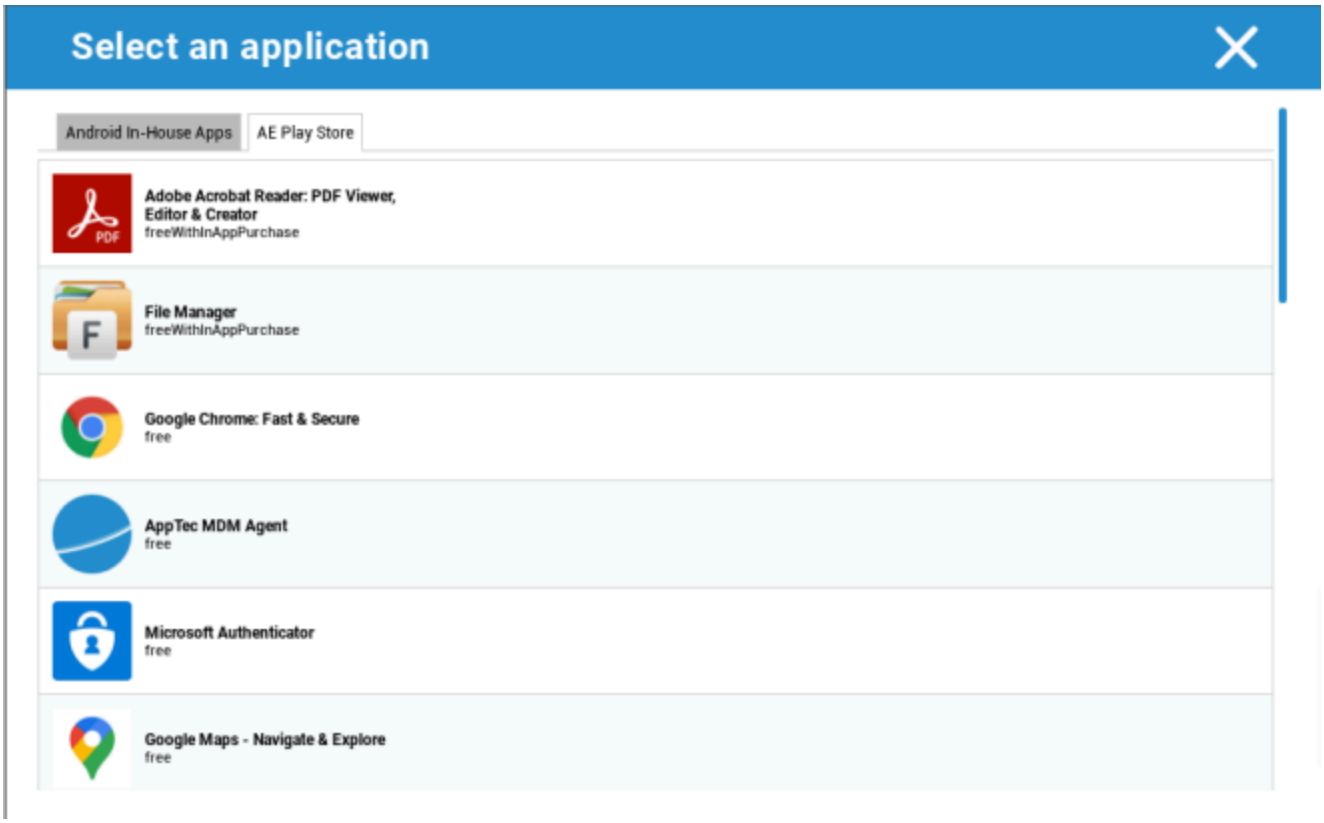


Ayrıca "Şirket İçi Uygulama Yükle" ile doğrudan bir apk dosyası seçip yükleyebilirsiniz.



Bir Şirket İçi Uygulama yüklüyorsanız, "Güncel tut" seçeneğini etkinleştirme olanağına sahip olacaksınız. Bu etkinleştirilmişse ve Şirket İçi Uygulama DB'sinde daha yeni bir sürüm tanımladıysanız, uygulama cihazda güncellenecektir.

Ya da Google Work Play Store'dan bir "AE Play Store" Uygulaması olabilir.



Bu sekmede yalnızca onaylı "AE Play Store Uygulamaları" gösterilecektir.

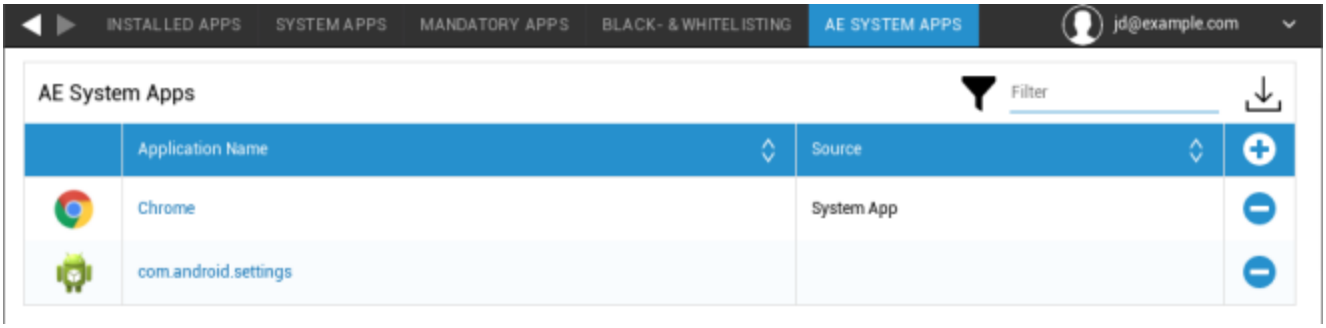
Bir "AE Play Store Uygulaması "nı onaylamak için lütfen "Genel Ayarlar" > "Uygulama Yönetimi" > "AE Play

Mağazası "na gidin ve sizi "Play Store Uygulamaları" sekmesine yönlendirecek düğme aracılığıyla bir uygulama ekleyin (veya doğrudan "Play Store Uygulamaları" sekmesine gidebilirsiniz).

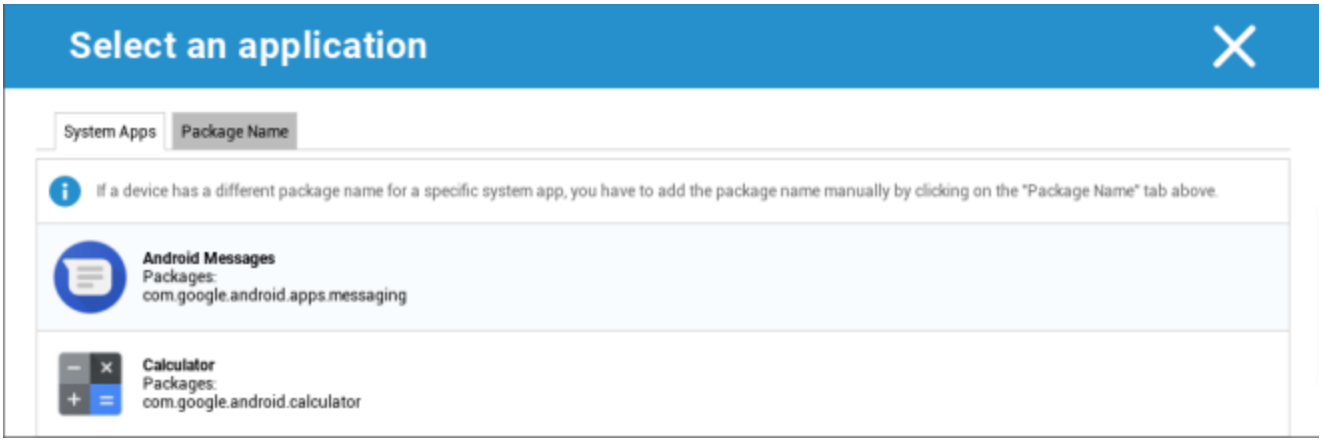
"Play Store Uygulamaları" sekmesinde uygulamaları arayabilirsiniz. Bir uygulamaya tıkladığınızda, uygulama sayfası açılır ve burada "Onayla "ya tıklayarak uygulamayı onaylayabilirsiniz.

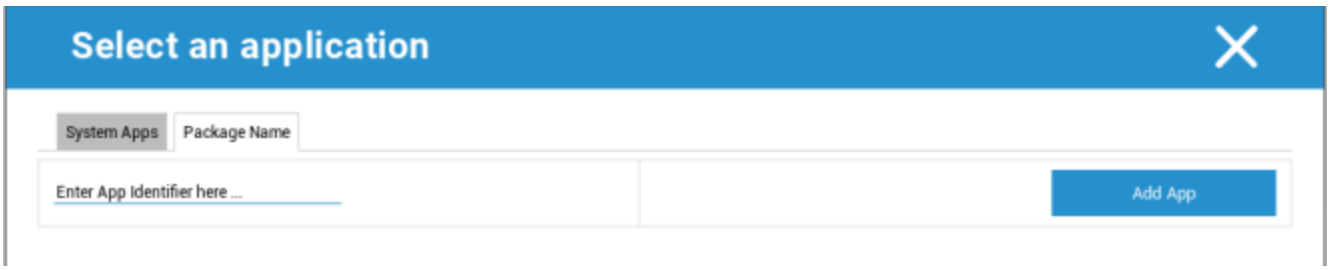
AE Sistem Uygulamaları

Burada, cihazlarda etkinleştirilmesi gereken belirli sistem uygulamalarını içeren bir liste tanımlayabilirsiniz.



Düğmeye tıklarsanız, Google tarafından sağlanan olası sistem uygulamaları listesinden seçim yapabilir veya etkinleştirilmesi gereken bir sistem uygulamasının paket adını doğrudan girebilirsiniz.





Google tarafından sağlanan listedeki sistem uygulamalarının yalnızca sistem uygulaması olabilecek uygulamalar olduğunu, ancak cihazlarınızdaki sistem uygulamaları olmak zorunda olmadığını lütfen unutmayın.

Ancak, bu liste yalnızca önceden yüklenmiş olan uygulamaları etkiler.

Cihazlarınızda önceden yüklü olmayan uygulamaları eklemek, uygulamanın Google tarafından sağlanan listeden olup olmadığına veya uygulamanın paket adının doğrudan girilip girilmediğine

bakılmaksızın cihazlarınızı etkilemeyecektir.

Kısıtlamalar ve Ayarlar

Uygulama Yönetimi Ayarları

Burada cihazın uygulama güncellemelerine ilişkin davranışını yapılandırabilirsiniz.

Güncelleme Kontrol Sıklığı	AppTec İstemcisinin uygulama güncellemelerini hangi aralıkta arayacağını belirtin. Varsayılan değer 24 saattir.
Wi-Fi Eşiği	Belirtilen boyuttan daha büyük olan uygulamalar Wi-Fi üzerinden indirilecektir. "Yalnızca Wi-Fi" seçilirse, tüm uygulamalar Wi-Fi üzerinden indirilecektir.

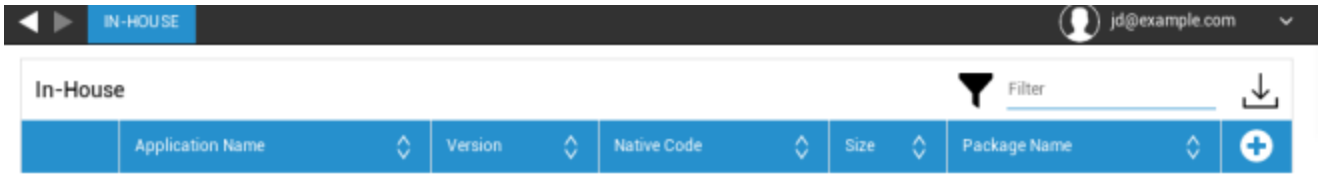
Kurumsal Uygulama Mağazası

Şirket İçi

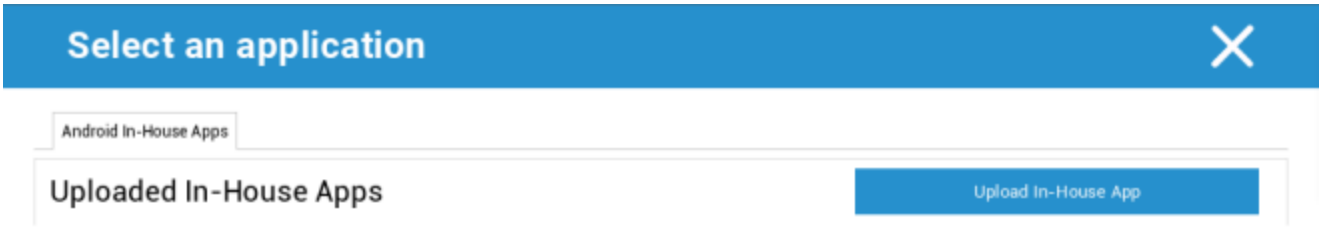
"Şirket İçi" başlığı altında, şirket içinde geliştirilen uygulamaları yükleyebilir ve dağıtabilirsiniz.

Sembol ile ek Şirket İçi Uygulamaları dağıtabilirsiniz.

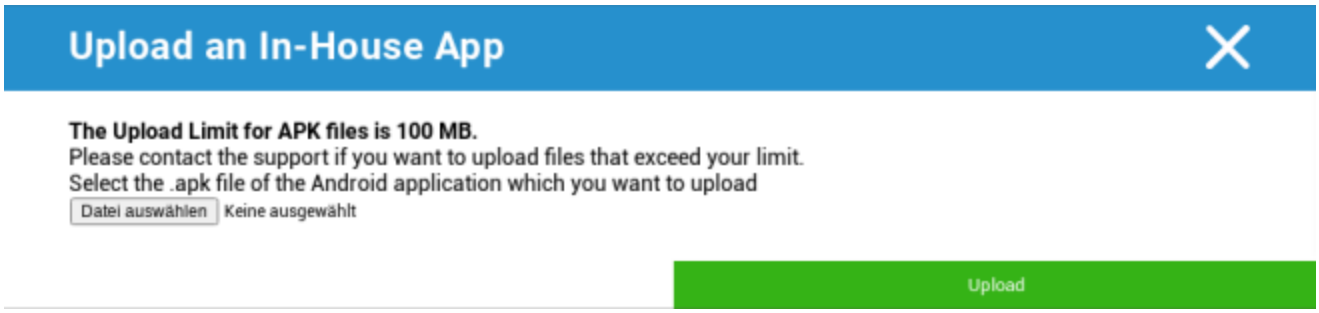
Bir Şirket İçi Uygulama yüklüyorsanız, "Güncel tut" seçeneğini etkinleştirme olanağına sahip olacaksınız. Bu etkinleştirilmişse ve Şirket İçi Uygulama DB'sinde daha yeni bir sürüm tanımladıysanız, uygulama cihazda güncellenecektir.



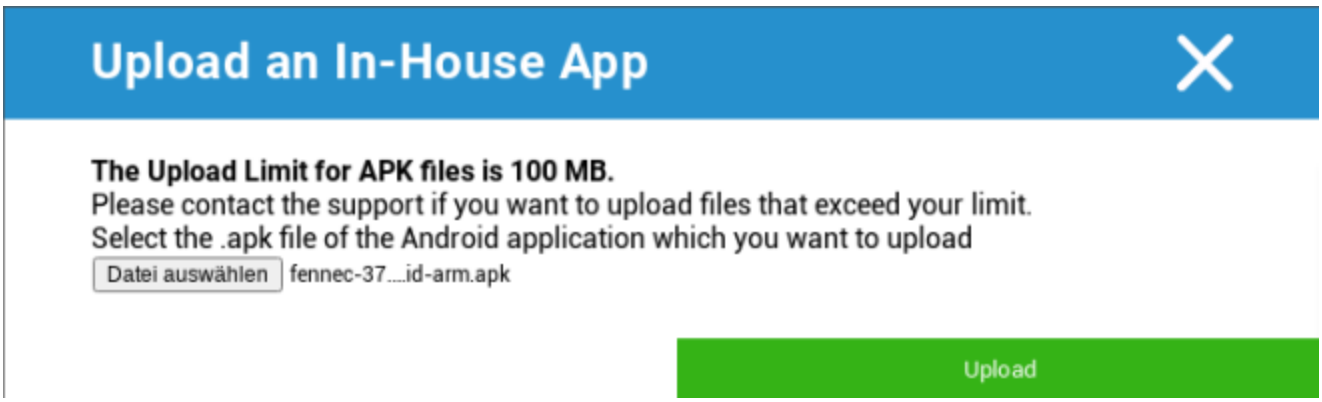
Kurum İçi Uygulamaları dağıtmadıysanız, aşağıdaki genel bakışı alacaksınız:



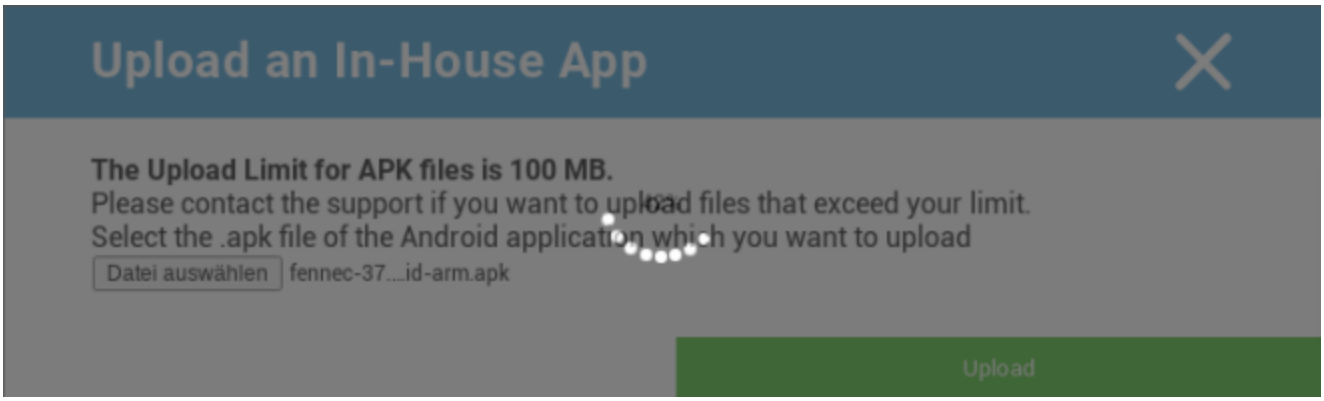
Bunun için "Şirket İçi Uygulama Yükle" seçeneğine tıklayın, ardından aşağıdaki genel bakışı alacaksınız:



Şimdi, "Ara... "yı kullanarak bir .apk dosyası seçin ve ardından "Yükle "ye tıklayın.



Uygulamanız şimdi yüklenecek, dairenin ortasında uygulamanızın ne kadarının yüklendiğini gösteren bir yüzde göstergesi göreceksiniz.



Şirket İçi Uygulamanızın yüklenmesi başarılı olursa, yüklenen uygulamayı Uygulama Kataloğunuzda bulabilirsiniz.

Kullanıcı artık bu uygulamayı son kullanıcı cihazındaki AppTec Store'da "In-House" kategorisi altında görme ve yükleme seçeneğine sahiptir.

Bunun bir Google PlayStore Uygulaması içermemesi nedeniyle, kullanıcının kendi son kullanıcı cihazında kayıtlı bir Google Kimliğine ihtiyacı yoktur.

Kurumsal Play Store

AE Play Store

Buradan Android Enterprise Playstore'a uygulama ekleyebilirsiniz. Uygulamaları ekleyebilmeniz için önce AE Yönetici Hesabınızla onaylamanız gerektiğini lütfen unutmayın.

Bir uygulamayı onaylamak için lütfen Zorunlu Uygulamalar bölümündeki talimatlara bakın.

İçerik Yönetimi

ContentBox

Burada ContentBox'ı etkinleştirebilirsiniz.

"ContentBox'ı Etkinleştir" seçeneğini "Açık" olarak değiştirdiğinizde, son kullanıcı cihazına otomatik olarak ayrı bir ContentBox Uygulaması yüklenecektir.

Güvenli Tarayıcı

Burada AppTec Secure Browser için ayarları yapılandırabilirsiniz.

"Güvenli Tarayıcı" bölümünü "Açık" olarak değiştirdiğinizde, son kullanıcı cihazına otomatik olarak ayrı bir Tarayıcı Uygulaması yüklenecektir.

Şifre Gerektir	Kullanıcının tarayıcıya erişmek için bir parola ayarlamasını ve kullanmasını gerektirir.
Gerekli minimum parola uzunluğu	Parola için gerekli karakter sayısını ayarlayın
Gerekli Şifre Kalitesi	Gerekli parola kalitesini ayarlayın
İndirmeleri Kısıtla / İçeride Aç	
Yüklemeleri Kısıtla	
Beyaz Liste Yükle	Karşıya yüklemeye her zaman izin verilecek URL'lerin bir listesi.
Kopyalamaya İzin Ver	Web sayfaları içinde metin kopyalamaya, kesmeye veya paylaşmaya izin verin.
Ekran Yakalamaya İzin Ver	Ekran görüntülerinin yakalanmasına izin verin.
Veri temizleme sıklığı	Hangi sıklıkta TÜM kullanıcı verilerinin (geçmiş, önbellek vb.) otomatik olarak kaldırılacağını seçin.
Şirket Yer İmleri	Yer İmleri, tarayıcı yer imlerindeki "Şirket yer imleri" klasöründe görünecektir. Kullanıcı tarafından düzenlenemezler.
Adres Çubuğunu Gizle	
Tarayıcı İçi Beyaz Liste (Universal Gateway olmadan)	İstemci tarafı URL beyaz listesini etkinleştirir. • Şirket Yer İmleri her zaman beyaz listeye alınır • Yalnızca 100 URL için desteklenir • Sınırsız Kara ve Beyaz Liste için lütfen Evrensel Ağ Geçidini kullanın
Beyaz Listedeki URL'ler	İzin verilen URL'lerin bir listesi.
Ağ geçidi tabanlı Kara ve Beyaz Liste	Kara listeye alma aşağıdaki gerekliliklere sahiptir: • Çalışan bir AppTec Universal Gateway ("Genel Ayarlar" → "Universal Gateway")

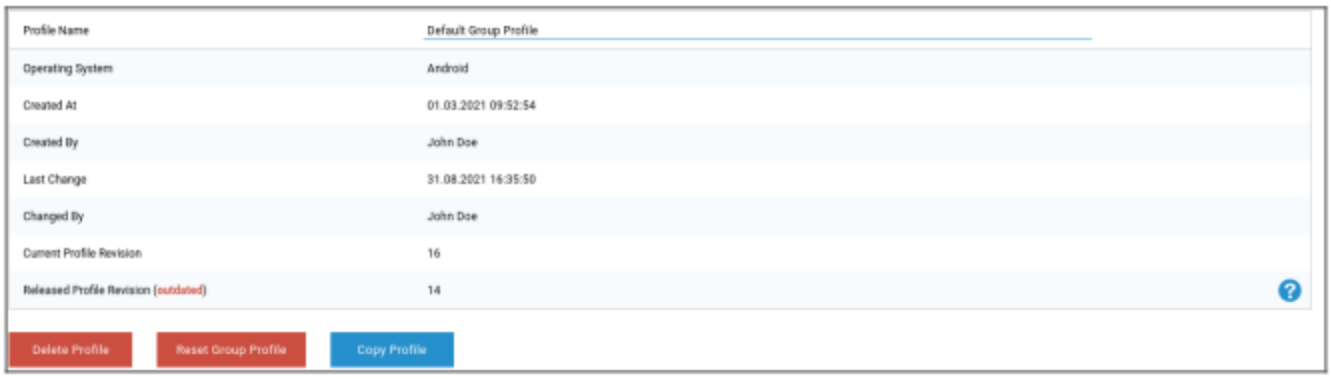
	• Belirlenmiş bir DNS sunucusu ile çalışan bir VPN yapılandırması ("Genel Ayarlar" → "Evrensel Ağ Geçidi" → "VPN Ayarları") • Bir Kara Liste yapılandırması ("Genel Ayarlar" → "Evrensel Ağ Geçidi" → "Etki Alanı Kara Listesi") • Profilde geçerli bir VPN bağlantısı ("Bağlantı Yönetimi" → "VPN")

Android Yapılandırması

Genel

Grup profiline genel bakış (yalnızca grup düzeyinde)

Bir grup profilini açtığınızda, profile hızlı bir genel bakış elde edersiniz.



Profil Adı	Profilin adı (burada değiştirilebilir)
İşletim Sistemi	Profilin ait olduğu İşletim Sistemi
Şu Adreste Oluşturuldu	Yaratılış zamanı
Tarafından Oluşturuldu	Profilin yaratıcısı
Son Değişiklik	Profilde yapılan son değişikliğin zamanı
Tarafından Değiştirildi	Son değişiklikleri yapan hesap
Güncel Profil Revizyonu	Kayıtlı profil durumunun revizyonu
Profil Revizyonu Yayınlandı	Atanmış profil revizyonu ("Şimdi ata"). Etiket metnin arkasında "(eski)" ibaresini gösteriyorsa, bu profili kaydettiğiniz ancak henüz atamadığınız anlamına gelir, bu nedenle cihazlar hala eski sürümü alacaktır.

Cihaza Genel Bakış (yalnızca cihaz düzeyinde)

Bir cihazda bulunmanız durumunda, seçilen cihazın genel bir özetini alacaksınız, burada aşağıdakiler yer almaktadır:

Cihaz Adı	Cihaz adı
Bilinen Son Konum	Bilinen son GPS koordinatları
Telefon Numarası	Telefon numarası
Atanmış Zorunlu Uygulamalar	Atanmış zorunlu uygulamaların sayısı
İşletim Sistemi Sürümü	Cihazın işletim sistemi sürümü
İşletim Sistemi	İşletim Sistemi (Android / iOS / Windows Phone)
Seri Numarası	Cihaz seri numarası
Cihaz Sahipliği	Kurumsal veya özel cihaz
Cihaz Tipi	Telefon veya Tablet
Köklü	Cihazın root edilip edilmediğini gösteren durum
Uyumlu	Kılavuza uygun
IP Adresi	IP Adresi
Son Görülme	Cihazın AppTec'e en son bağlandığı zaman noktası
Son İtiş	Sunucunun cihaza bir push gönderdiği zaman noktası
Kullanıcı Ataması	Cihazı başka bir kullanıcıya atamak için bir açılır menü

Konfigürasyon Revizyonu (sadece cihaz seviyesinde)

Burada cihaza hangi grup profilinin atandığına dair bir genel bakış elde edersiniz.

Grup profiline tıklarsanız, profile doğrudan erişirsiniz ve ayarları gerçekleştirebilirsiniz.

Sembol ile, atanan uygulamaları grup profilinin ayarlarına geri döndürebilirsiniz.

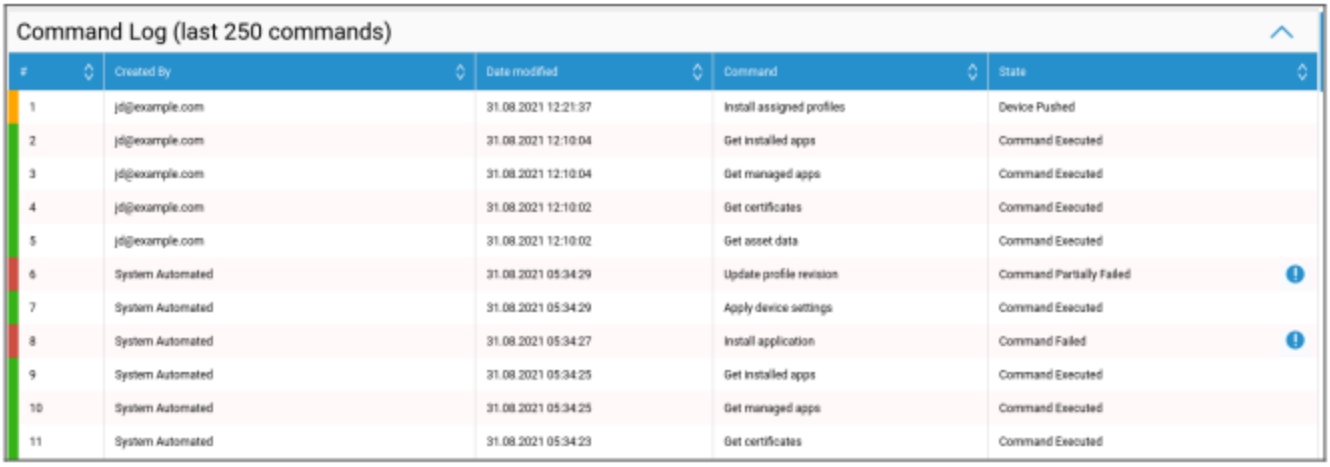
Sembol ile cihaz profilini hiçbir ayara sahip olmayacak şekilde sıfırlayabilirsiniz.

"Newer Revision available" grup profilinin değiştirildiğini ve kaydedildiğini ancak atanmadığını gösterir. Değişiklikleri cihazlara uygulamak için grup profilinin grup düzeyinde "Şimdi ata" ile atanması gerekir.

Cihaz Günlüğü (yalnızca cihaz düzeyinde)

Komut Günlüğü

Burada cihaz için hangi komutların verildiğini ve durumlarının ne olduğunu görebilirsiniz.



"System Automated" tarafından oluşturulan komutlar sistem tarafından otomatik olarak oluşturulur.

Olası komut durumları

Cihaz İtildi	Cihaza EMM sunucusuna geri bağlanmasını söylemek için push hizmetine (örn. APNS) bir push isteği gönderilmiştir.
Komut Oluşturuldu	Komut sistemde oluşturuldu.
Gönderilen Komut	Komut, sunucuya bağlandıktan sonra cihaza gönderildi.
Komut Yürütüldü	Komut başarıyla yürütüldü.
Komut Başarısız	Komut başarısız oldu. *
Komut Kısmen Başarısız	Cihazın işletim sistemine bağlı olarak bazı komutlar birlikte gruplandırılabilir. Bu komut grubunun bazı bölümleri başarısız olmuştur. *
Komut Yürütüldü, sonunda Başarısız Oldu	Komut uygulandı ama belki de uygulanmadı.
Komut Tekrar Gönderildi	Komut bir kullanıcı tarafından yeniden itildi.
Atılmış	Komut iptal edildi. Örneğin, başka bir komutun yerini aldığı için veya cihaz yeniden kaydedildiği ve eski komutlar kaldırıldığı için

*Mesajın arkasında bir ünlem işareti varsa, imlecinizi simgenin üzerine getirerek daha fazla bilgi alabilirsiniz.

Cihaz Ayarları

İstemci Yapılandırması

Burada Android cihazınızda aşağıdaki yapılandırmaları gerçekleştirebilirsiniz:

Aygıt Yönetimi devre dışı bırakıldıktan sonra uyarı mesajı	Aygıt Yönetimi devre dışı bırakıldıktan sonra oluşturulan uyarı mesajı
Uyumluluk Dışı Zaman	Cihaz uyumlu değilse, "Uyumluluk Sonrası Yaptırım Eylemi "nin gerçekleştirileceği zaman sınırı. Min. 1 dakika Max. 24 saat
Uyum zaman aşımından sonra yaptırım eylemi	Bir cihaz uyumsuz hale gelir gelmez gerçekleştirilecek eylem. • hiçbir şey yapmamak = eylem yok • Kilit Cihazı = kilit cihazı • Cihazı Sil = cihaz fabrika ayarlarına geri yüklenir
Veri Toplama Sıklığı	Cihaz/GPS bilgilerinin toplanma sıklığı
Cihaz Kalp Atışı Frekansı	Cihazın AppTec360 Sunucusu ile iletişime geçmesi gereken aralık Min. 1 dakika Max. 24 saat
Konum Güncellemelerini Etkinleştir	Etkinleştirilirse, cihaz konum güncellemelerini AppTec360 Sunucusuna gönderir
Konum Güncelleme Zamanı	Cihazın konum güncellemelerini AppTec'e hangi zaman aralıklarında göndereceğini belirler
Konum Güncellemesi için Google Konum Doğruluğunu Kullanın	Etkinleştirilirse, konum güncellemeleri için Google Konum Doğruluğu (eski adıyla ağ konumu) kullanılacaktır ("Kısıtlamalar" altında devre dışı bırakılmışsa, bu ayar hiçbir şeyi etkilemeyecektir)
Konum Güncellemesi için GPS Konumunu Kullanın	Etkinleştirilirse, konum güncellemeleri için GPS kullanılacaktır
Sahte (Fake) Konumlara İzin Ver	Üçüncü taraf uygulamalar aracılığıyla konum bilgilerinin sahtesinin yapılmasına izin verir
Kayıp Bağlantı Eylemi	Belirli sayıda kalp atışı başarısız olduktan sonra gerçekleştirilecek belirli bir eylemi ayarlamanızı sağlar

İlke Uygulama Modu	AppTec360 İstemcisinin kullanıcıdan kullanıcı girişi gerektiren belirli eylemleri gerçekleştirmesini ne kadar agresif bir şekilde isteyeceğini tanımlar. Aralık (Varsayılan) = aralıklarla sor, böylece kullanıcı bunu bir süreliğine arka plana atabilir. Uyarı Yok = gerekli herhangi bir etkileşim için açılır pencere yok. Gerekli bir eylem olup olmadığını kontrol etmek için AppTec360 İstemcisini manuel olarak açmanız gerekir Sabit Uyarı = Kullanıcı yalnızca gerekli eylemi gerçekleştirebilir. Kullanıcı bundan kaçınmaya çalışırsa AppTec360 İstemcisi kendini ön plana çıkarmaya zorlayacaktır
AppTec360 Sürüm Kilidi	İstemcinin kendini güncelleyeceği maksimum sürüm olan AppTec360 İstemcisinin bir sürümünü tanımlamanızı sağlar.

Duvar Kağıdı

Burada özel bir duvar kağıdı tanımlayabilirsiniz.

"Bir Renk Belirleyin" hex formatında bir renk tanımlamanızı sağlar (örn. #000000). Yalnızca onaltılık değerlere izin verilir.

"Resmi Duvar Kağıdı Olarak Ayarla" bir resim yüklemenizi sağlar. Lütfen farklı başlatıcılara ve işletim sistemi sürümlerine sahip farklı cihazların farklı çalıştığını unutmayın. Boyut ve oran için genel bir kılavuz çizgi yoktur, çünkü bu cihaza göre değişir.

Dosya formatı için JPG (veya JPEG) veya PNG kullanın.

Varlık Yönetimi (yalnızca cihaz düzeyinde)

Varlık Yönetimi

Cihaz Bilgisi

Model	**Cihaz model tanımı**
İşletim Sistemi	İŞLETIM SISTEMI
İşletim Sistemi Sürümü	İşletim sistemi sürümü
AE Desteği	Android Enterprise desteği (Konteyner ve tam yönetimli)
Seri Numarası	Seri numarası
Cihaz Adı	Cihaz adı
Pil Durumu	Pil durumu
Boş / Toplam Bellek	Boş / Toplam bellek
Samsung KNOX	Samsung KNOX API Seviyesi
SD Kart Mevcut	SD Kart mevcut
SD Kart Emülasyonlu	SD Kart emülasyonu
SD Kart Çıkarılabilir	SD Kart çıkarılabilir
SD Boş / Toplam Bellek	SD Boş / Toplam SD Kart belleği

Wi-Fi

IP Adresi	Cihaz IP adresi
WiFi MAC	WiFi MAC adresi

Hücresel

Durum	Durum (SIM kart takılı)
Telefon Numarası	Telefon Numarası
Dolaşım (Ses / Veri)	Ses / veri için dolaşım
Dolaşım Durumu	Mevcut dolaşım durumu
IP Adresi	IP adresi
Operatör/Taşıyıcı	Operatör/Taşıyıcı
Hücresel Teknoloji	Hücresel Teknoloji
IMEI	IMEI numarası
ICCID	Bu, SIM kartın kimliğidir, çoğu zaman bir Akıllı Kart veya Entegre Devre Kartı (ICC) da olabilir
IMSI	Uluslararası Mobil Abone Kimliği (IMSI), GSM ve UMTS mobil ağlarında ağ kullanıcılarının kesin bir şekilde tanımlanmasını sağlar IMSI en fazla 15 basamaktan oluşur ve aşağıdaki şekilde yapılandırılır: • Mobil Ülke Kodu (MCC), 3 basamaklı • Mobil Ağ Kodu (MNC), 2 veya 3 basamaklı • Mobil Abone Kimlik Numarası (MSIN), 1-10 hane
Mevcut MCC/MNC	Bkz. "SIM MCC/MNC"
SIM MCC/MNC	Mobil Ülke Kodu, E.212 uyarınca ITU tarafından belirlenen yerleşik bir ülke tanımlayıcısıdır Standart. Bu, mobil ağın tanımlanması için Mobil Ağ Kodu (MNC) ile birlikte çalışır. SIM kartın ülke/Mobil Ağ Kodu anlamına gelir. Başka bir mobil ağda dolaşım yaparsanız, mantıksal olarak "Mevcut MCC/MNC" ve "SIM MCC/MNC" farklı olacaktır.

Bluetooth

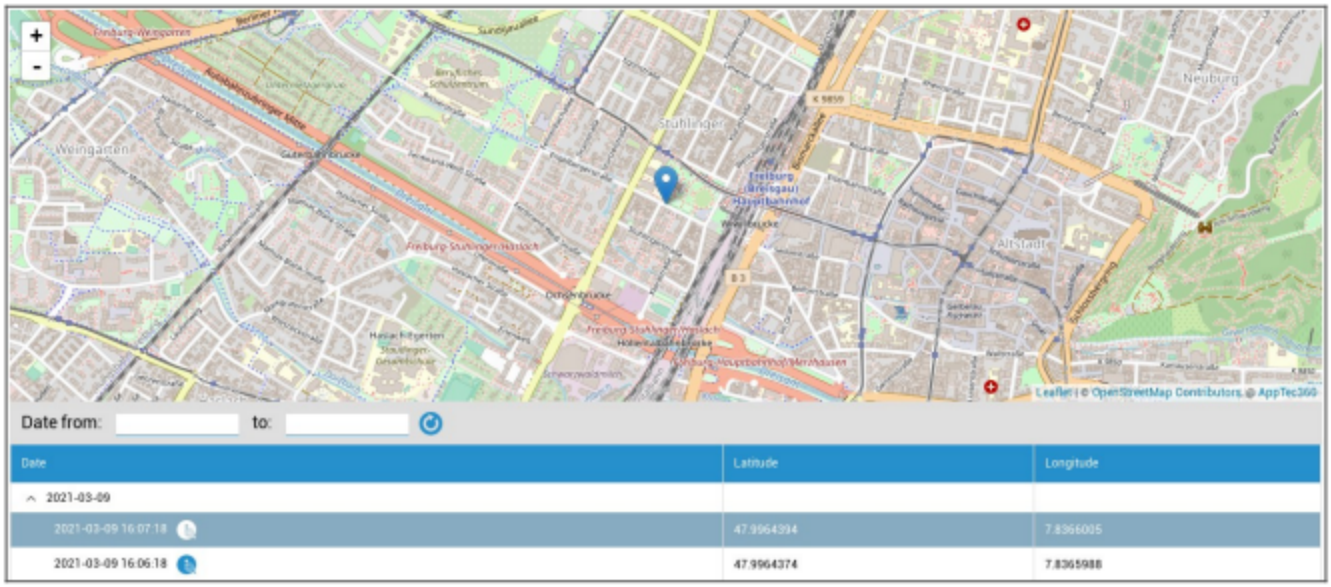
Bluetooth MAC	Bluetooth MAC adresi

Güvenlik Yönetimi

Hırsızlığa Karşı Koruma (yalnızca cihaz düzeyinde)

GPS Bilgileri (yalnızca cihaz düzeyinde)

Burada mevcut/son cihaz konumunu belirleyebilirsiniz. Yerelleştirme bir veya iki parola ile korunabilir - Bkz: Genel Ayarlar - Gizlilik - GPS Erişimi



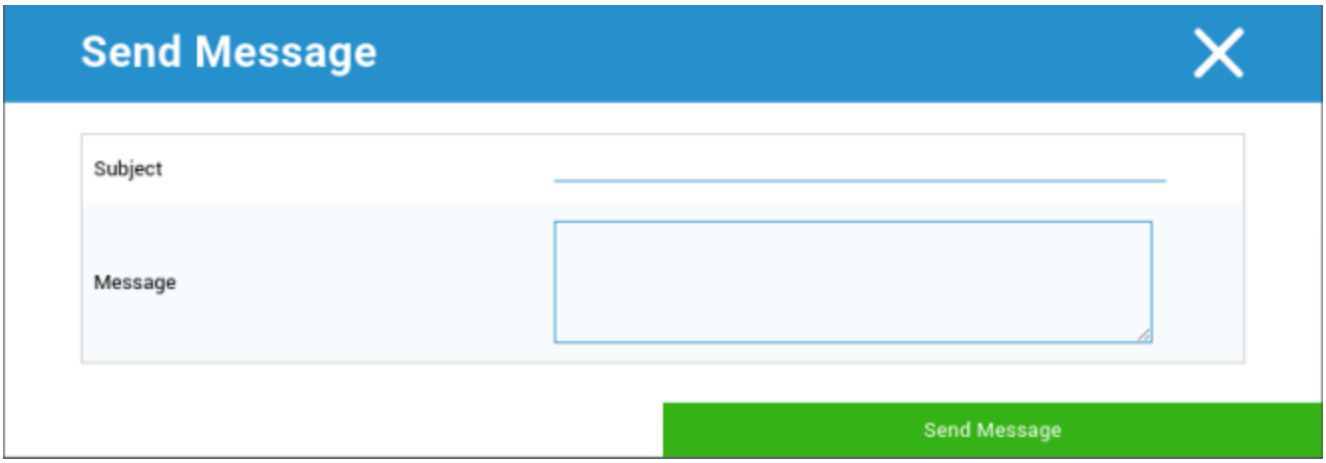
Sil ve Kilitle (yalnızca cihaz düzeyinde)

"Sil ve Kilitle" altında aşağıdaki üç eylemi gerçekleştirebilirsiniz:

Tam Silme	Cihaz fabrika ayarlarına geri döndürülür (kurumsal ve kişisel veriler silinir)
Kurumsal Silme	Son kullanıcı cihazından yalnızca kurumsal veriler kaldırılır (AppTec360 tarafından sağlanan tüm uygulamalar, veriler vb.)
Kilit Ekranı	Ekran kilidi etkinleştirildiğinde, cihazın kilidini cihaz şifresi/PIN ile açmak yeterlidir

Mesaj (yalnızca cihaz düzeyinde)

Konuyu ve mesajı doldurabilir ve bir son kullanıcı cihazına gönderebilirsiniz. Bu mesaj AppTec360 İstemcisinde görüntülenecektir.



Güvenlik Yapılandırması

Şifre

"Parola" altında bir cihaz parolası belirleyebilirsiniz, aşağıdaki ayar seçeneklerini kullanabilirsiniz

Minimum parola uzunluğu	Bir parolanın sahip olması gereken minimum sembol sayısını belirler
Şifre kalitesi	Parola gücü Belirtilmemiş = belirtilmemiş Her parola tamam = her parola kabul edilebilir en az sayısal karakter = en az sayısal karakter içermelidir en az karmaşık karakterler = en az özel karakterler içermelidir at least alphanumerical characters = en az alfanümerik karakter içermelidir at least alphabetic characters = en az alfabetik karakter içermelidir
Maksimum hareketsizlik süresi kilidi	Maksimum ekran zaman aşımı. Bu sadece kullanıcı tarafından seçilebilecek maksimum değeri yapılandırır
Parolada gereken minimum küçük harf sayısı	Parolada gereken minimum küçük harf sayısı
Parolada gerekli minimum büyük harfler	Parolada gerekli minimum büyük harfler
Parolada gerekli minimum harf dışı karakterler	Parolada gerekli minimum harf dışı karakterler
Parolada gerekli minimum sayısal basamaklar	Parolada gerekli minimum sayısal basamaklar
Parolada gereken minimum semboller	Parolada gereken minimum semboller
Parola sona erme zaman aşımı	Oluşturur, hangi zaman aralığından sonra parolanın süresi dolar ve yeni bir parola verilmelidir
Parola geçmişi kısıtlaması	İzin verilmeyen önceden kullanılmış şifre sayısı
Maksimum başarısız parola denemesi	Tam bir cihaz silme işlemi gerçekleştirilmeden önce bir parolanın ne kadar sıklıkla yanlış girilebileceğini belirler

Şifreleme

Bu noktada, dahili cihaz belleğinin yanı sıra SD kart belleğini de şifreleyebilirsiniz.

Depolama Şifrelemesi Gerektir	Bu ayar etkinleştirilirse, cihaz bu işlevi desteklediği sürece cihaz belleği şifrelenecektir. Cihaz belleği ilk kez şifrelendikten sonra artık şifrelemeyi kaldırmak mümkün değildir. Aynı şekilde, Şifre Politikası da otomatik olarak 6 alfanümerik sembole geçirilecektir
SD Kart Şifrelemesi Gerektir	Bu ayar yalnızca Samsung cihazları için geçerlidir! Bu ayar etkinleştirilirse, harici SD kart şifrelenebilir ve yalnızca son kullanıcı cihazında manuel olarak şifresi kaldırılabilir. Aynı şekilde, Şifre Politikası da otomatik olarak 6 alfanümerik sembole geçirilecektir

AntiVirüs

AntiVirus'ün etkinleştirilmesi cihazlara Ikarus'u yükleyecektir. Bunun için Genel Ayarlar → Uygulama Yönetimi → Üçüncü Taraf Uygulamaları bölümünden girilebilecek ayrı bir lisans gerektiğini lütfen unutmayın.

Otomatik Tarama	Ikarus'un otomatik olarak tarama yapıp yapmayacağını ve bu taramayı ne sıklıkla gerçekleştireceğini tanımlar "Tam Otomatik Tarama" etkinleştirildiğinde tam bir tarama gerçekleştirilir. Aksi takdirde hızlı bir tarama gerçekleştirilecektir
Otomatik Güncellemeler	Virüs veritabanının otomatik güncellemelerini etkinleştirir ve bunun ne sıklıkla yapılacağını ayarlar
Uygulama Koruması	Yalnızca Dosyaları tarayan normal Taramaya ek olarak Uygulamaların Taranmasını etkinleştirir
SD Kart Koruması	SD Kart Korumasını etkinleştirir. Bu olmadan, tarama yerel depolama alanı ile sınırlıdır
Yalnızca Wi-Fi Güncellemesi	Güncellemeyi Wi-Fi ile Sınırlar

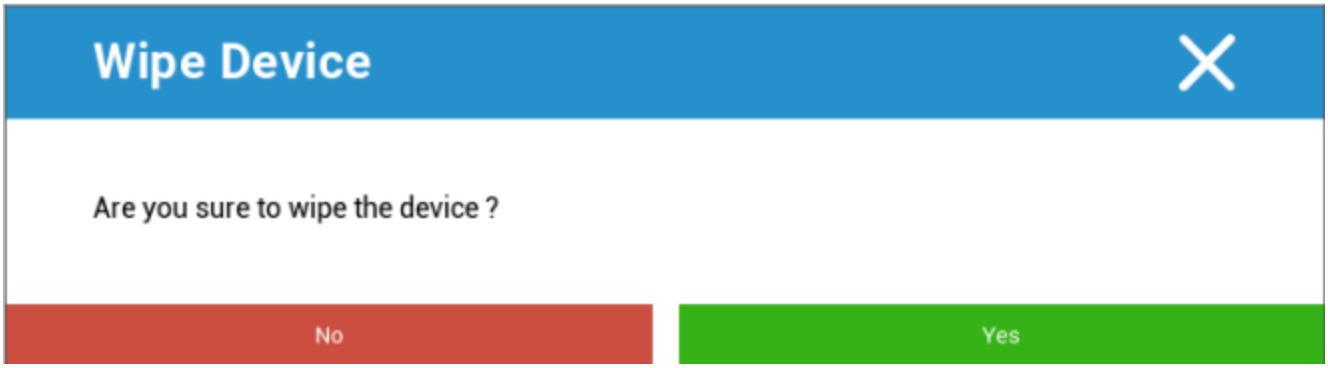
Kullanım Ömrü Sonu (yalnızca cihaz düzeyinde)

Silme (yalnızca cihaz düzeyinde)

"Sil" altında, cihazı fabrika ayarlarına geri yükleyebilirsiniz. Burada kurumsal verilerin yanı sıra özel veriler de son kullanıcı cihazında silinecektir.

"Eksi Sembolü "ne tıkladığınızda aşağıdaki mesajı almanız gerekir

SD Kartı da mı sileyim?	SD kart belleği de silinecektir



"Evet" ile silme işlemini gerçekleştirebilirsiniz.

"Silme Raporu" altında aşağıdaki öğeler görüntülenebilir

Tarafından silindi	Silme işlemini kimin yaptığına dair tarihçe
Tarih	Tarih
Durum	Durum (örn. Silme işlemi başarıyla gerçekleştirildiyse)

Kısıtlama Ayarları

Kısıtlamalar

Burada, çeşitli şeyler kısıtlanabilir ve engellenebilir.

Kamerayı Etkinleştir	Kamera kullanımına izin verin
Otomatik Senkronizasyonu Zorla	"Sync" arayüzü ile ilgilidir Açık = senkronizasyon kalıcı olarak etkinleştirilir Kapalı = senkronizasyon kalıcı olarak devre dışı bırakılır Kullanıcı seçimi = kullanıcı tarafından seçilir
Bluetooth'u Zorla	Açık = Bluetooth kalıcı olarak etkinleştirilir Kapalı = Bluetooth kalıcı olarak devre dışı bırakılır Kullanıcı seçimi = kullanıcı tarafından seçilir
Kuvvet GPS	Açık = GPS kalıcı olarak etkinleştirilir Kapalı = GPS kalıcı olarak devre dışı bırakılır Kullanıcı seçimi = kullanıcı tarafından seçilir
Google Konum Doğruluğunu Zorla	Açık = Kalıcı internet-yerelleştirme Kapalı = İnternet yerelleştirmenin kalıcı olarak devre dışı bırakılması Kullanıcı seçimi = kullanıcı tarafından seçilir

KNOX 1.0 veya daha yüksek arayüze sahip Samsung cihazları için aşağıdaki ayar seçenekleri mevcuttur.

SD Karta İzin Ver	SD Karta İzin Ver
SD Kart Yazmaya İzin Ver	SD Kart üzerinde "yazmaya" izin verin
Ekran Yakalamaya İzin Ver	Ekran yakalamaya izin ver
Panoya İzin Ver	Panoya izin ver
Ayarları ve uygulama verilerini Google Cloud'da yedekleme	Kapalı = Google Yedekleme'yi devre dışı bırak Açık = Google Yedekleme'yi etkinleştir Kullanıcı Seçimi = kullanıcı tarafından seçilir
USB Hata Ayıklamaya İzin Ver	USB Hata Ayıklamaya İzin Ver (örneğin cihaz günlüklerinin (ADB) oluşturulması için kullanılır)
Google Crash Raporuna İzin Ver	Google Crash Report'un uygulamalardan gönderilmesine izin verin
Fabrika Ayarlarına Sıfırlamaya İzin Ver	Kullanıcının cihazı fabrika ayarlarına geri yüklemesini sağlar
OTA Yükseltmesine İzin Ver	"Over-The-Air" Güncellemelere İzin Verin
USB ana bilgisayar depolamasına izin ver	Etkinleştirilirse, HD veya SD kart okuyucu biçimindeki USB bellek bağlanabilir
USB Medya Oynatıcısına İzin Ver (MTP,PTP)	USB Medya Oynatıcısına İzin Ver (MTP,PTP)
Mikrofona İzin Ver	Açık = 3. Parti Uygulamalar için mikrofona izin ver Kapalı = 3. Parti Uygulamalar için mikrofonu engelle Kullanıcı Seçimi = 3. Taraf Uygulamanın mikrofona erişimi varsa kullanıcılar seçebilir
NFC'ye (Yakın Alan İletişimi) İzin Ver	NFC'ye İzin Ver
Bilinmeyen Kaynaklara İzin Ver (APK Sideloading)	Etkinleştirilirse, Uygulamaların (APK dosyaları) yandan yüklenmesine izin verilir. Bu ayar devre dışı bırakıldıktan sonra, bilinmeyen kaynaklardan APK'ların yüklenmesine yeniden izin verdiğinizde kullanıcının bunu manuel olarak etkinleştirmesi gerekir.
Kullanıcı Oluşturmaya İzin Ver	Birden fazla kullanıcı oluşturulmasına izin verir

AE Cihaz Sahibi

(Cihazın Android Kurumsal Cihaz Sahibi Modunda olması gerekir) Cihazların "Android" cihaz olarak değil "Android Enterprise" cihaz olarak oluşturulması tavsiye edilir.

Güvenlik	
Paylaşım Konumuna İzin Verme	Bir kullanıcının konum paylaşımını açmasına izin verilmeyip verilmeyeceğini belirtir.
Güvenli Önyüklemeye İzin Verme	Kullanıcının cihazı güvenli önyükleme modunda yeniden başlatmasına izin verilmeyip verilmeyeceğini belirtir.
Ağ Sıfırlamaya İzin Verme	Bir kullanıcının Ayarlar'dan ağ ayarlarını sıfırlamasına izin verilip verilmeyeceğini belirtir.
Fabrika ayarlarına sıfırlamaya izin verme	Bir kullanıcının cihazı sıfırlamasına izin verilmeyip verilmeyeceğini belirtir.
ADB'yi Etkinleştir	ADB aracılığıyla bir PC'ye Bağlantıya İzin Verir
Keyguard'ı Devre Dışı Bırak	Keyguard'ı devre dışı bırakır
Cihaz Sahibi Kilit Ekranı Bilgisi	Kilit ekranında gösterilecek cihaz sahibi bilgilerini ayarlar.
Uyum Uygulama	Mod Kullanıcıya Sor - Kullanıcıdan gerekli eylemleri yerine getirmesi istenir. Mod Kilitleme Konteyneri - Tüm gereksinimler yerine getirilene kadar tüm uygulamaları gizleyin

Uygulama Yönetimi	
Çapraz Profil Uygulama Bağlantısına İzin Ver	Üst profildeki uygulamaların yönetilen profildeki web bağlantılarını işlemesine izin verir.
Uygulama Kontrolüne İzin Verme	Bir kullanıcının Ayarlar veya başlatıcılardaki uygulamaları değiştirmesine izin verilmeyip verilmeyeceğini belirtir.
Uygulama Yüklemesine İzin Verme	Bir kullanıcının uygulama yüklemesine izin verilmeyip verilmeyeceğini belirtir.
Kaldırma Uygulamalarına İzin Verme	Bir kullanıcının uygulamaları kaldırmasına izin verilmeyip verilmeyeceğini belirtir.
Çalışma Zamanı İzin Politikası	Uygulamalardan gelen yeni izin isteklerinin nasıl ele alınacağını belirtir.
Bilinmeyen Kaynaklara İzin Ver	Etkinleştirilirse, kullanıcılar bir .apk dosyası yükleyerek Uygulamaları yandan yükleyebilir.

Bağlanabilirlik	
Mobil Ağ Yapılandırmasına İzin Verme	Bir kullanıcının mobil ağları yapılandırmasına izin verilmeyip verilmeyeceğini belirtir.
Tethering Yapılandırmasına İzin Verme	Bir kullanıcının Tethering ve taşınabilir hotspot'ları yapılandırmasına izin verilmeyip verilmediğini belirtir.
VPN Yapılandırmasına İzin Verme	Bir kullanıcının VPN yapılandırmasına izin verilmeyip verilmeyeceğini belirtir.
Wifi Yapılandırmasına İzin Verme	Bir kullanıcının WiFi erişim noktalarını değiştirmesine izin verilmeyip verilmeyeceğini belirtir.
Giden NFC Işınına İzin Verme	Kullanıcının uygulamalardan veri ışınlamak için NFC kullanmasına izin verilmeyip verilmeyeceğini belirtir.
WiFi Yapılandırmasını Kilitle	Bu ayar, bir Cihaz Sahibi uygulaması tarafından oluşturulan WiFi yapılandırmalarının kilitli olup olmayacağını kontrol eder (yani, Ayarlar uygulaması tarafından bile değil, yalnızca Cihaz Sahibi Uygulaması tarafından düzenlenebilir veya kaldırılabilir).
Veri Dolaşımını Etkinleştir	Veri Dolaşımını Etkinleştirir

Bluetooth	
Bluetooth'a İzin Verme	Cihazda bluetooth'a izin verilip verilmediğini belirtir. Android 8.0 gerektirir
Bluetooth Paylaşımına İzin Verme	Cihazda giden bluetooth paylaşımına izin verilmeyip verilmediğini belirtir. Android 8.0 gerektirir
Bluetooth Yapılandırmasına İzin Verme	Bir kullanıcının bluetooth yapılandırmasına izin verilmeyip verilmediğini belirtir.

Hesap Yönetimi	
Yönetilen profil eklemeye izin verme	Bir kullanıcının yönetilen profiller eklemesine izin verilmeyip verilmeyeceğini belirtir. Android 8.0 gerektirir
Kullanıcı eklemeye izin verme	Bir kullanıcının yeni kullanıcı eklemesine izin verilmeyip verilmeyeceğini belirtir.
Yönetilen Profili Kaldırmaya İzin Verme	Bu kullanıcının yönetilen profillerinin, profil sahibi dışında kaldırılıp kaldırılamayacağını belirtir. Android 8.0 gerektirir
Hesap Değişikliğine İzin Verme	Authenticator tarafından programlı olarak eklenmediği sürece, bir kullanıcının hesap ekleme ve kaldırma işlemlerine izin verilmeyip verilmeyeceğini belirtir.

Telefon	
Giden Çağrılara İzin Verme	Kullanıcının giden telefon aramaları yapmasına izin verilmediğini belirtir.
SMS'e İzin Verme	Kullanıcının SMS mesajları göndermesine veya almasına izin verilmediğini belirtir.

Sistem	
Pencere Oluşturmaya İzin Verme	Uygulama pencereleri dışındaki pencerelerin oluşturulmaması gerektiğini belirtir.
Kullanıcı Simgesini ayarlamaya izin verme	Bir kullanıcının simgesini değiştirmesine izin verilmeyip verilmeyeceğini belirtir.
Duvar Kağıdı Ayarlamaya İzin Verme	Duvar kağıdı ayarlamaya izin vermemek için kullanıcı kısıtlaması.
Durum Çubuğunu Devre Dışı Bırak	Durum çubuğunun devre dışı bırakılması, tek kullanımlık bir cihazdan kaçmayı sağlayan bildirimleri, hızlı ayarları ve diğer ekran kaplamalarını engeller.
Otomatik Zamanı Etkinleştir	Saati otomatik olarak ayarlar.
Otomatik Saat Dilimini Etkinleştir	Saat dilimini otomatik olarak ayarlar.
Fişe takılıyken açık kalma	Cihaz bir güç kaynağına bağlıyken aktif kalacaktır.

Depolama	
Uygulama Doğrulamayı Devre Dışı Bırak	Bir kullanıcının uygulama doğrulamasını devre dışı bırakmasına izin verilip verilmeyeceğini belirtir.
Fiziksel Ortam Montajına İzin Verme	Bir kullanıcının fiziksel harici medyayı monte etmesine izin verilmeyip verilmeyeceğini belirtir.
Yedekleme Hizmetini Etkinleştir	Yedekleme hizmeti cihazdaki tüm yedekleme ve geri yükleme mekanizmalarını yönetir. Bunun false olarak ayarlanması verilerin yedeklenmesini veya geri yüklenmesini engeller. Yedekleme hizmeti varsayılan olarak kapalıdır. Android 8.0 gerektirir
USB Yığın Depolamayı Etkinleştir	USB Yığın Depolama kullanımını etkinleştirir.

Klavye	
Otomatik Doldurmaya İzin Verme	Bir kullanıcının Otomatik Doldurma Hizmetlerini kullanmasına izin verilip verilmediğini belirtir. Android 8.0 gerektirir
Profiller Arasında Kopyalama ve Yapıştırmaya İzin Verme	Bu profilin panosuna kopyalananların ilgili profillere yapıştırılıp yapıştırılamayacağını belirtir.

Ses	
Hacim Ayarlamasına İzin Verme	Bir kullanıcının ana ses seviyesini ayarlamasına izin verilmeyip verilmeyeceğini belirtir.
Mikrofonun Sesini Açmaya İzin Verme	Bir kullanıcının mikrofon ses düzeyini ayarlamasına izin verilmeyip verilmeyeceğini belirtir.
Sessiz Aygıt	Sessiz cihaz.

Sistem Güncelleme Politikası	
İşletim Sistemi Güncellemelerini Kontrol Etme	Güncelleme davranışını otomatik, pencereli veya ertelenmiş olarak ayarlamak için bunu etkinleştirin.

BYOD Konteyner

Android Kurumsal

Android Kurumsal

Android Enterprise'ı Etkinleştirin	Android Enterprise'ı (AE) etkinleştirin. AE, Android 5.1 ve üzeri sürümlerden beri desteklenmektedir.
Uyum Uygulama	Mod Kullanıcıya Sor - Kullanıcıdan gerekli eylemleri yerine getirmesi istenir. Mod Kilitleme Konteyneri - Tüm gereksinimler yerine getirilene kadar tüm uygulamaları gizleyin
Çalışma Zamanı İzin Politikası	Yeni izin talepleri için kullanıcıya sor Her zaman yeni izin taleplerini kabul edin Yeni izin taleplerini her zaman reddedin Uyarı: Bunlar otomatik olarak ayarlanırsa bazı Uygulamalar izinleri tanımada sorun yaşar. İzinleri her zaman veriyorsanız ve izinlerin eksik olduğunu söyleyen uygulamalarla ilgili sorunlarla karşılaşıyorsanız, bunu "kullanıcıya sor" olarak ayarlayın ve uygulamayı yeniden yükleyin
Giden panoya izin ver	Konteynerin içinden dışına kopyalama ve yapıştırmaya izin verir
Arayan Kimliği Çözümlemesine İzin Ver	Kapsayıcıdaki kişilere bağlı olarak gelen bir aramanın adını gösterir
Kişi Arama Çözümüne İzin Ver	Arama yaparken konteyner kişilerinde isim aramaya izin verir
Bluetooth Kişi Paylaşımına İzin Ver	Arabada konteyner temasına erişim sağlar
Giden NFC Işınına İzin Verme	Konteyner için NFC'yi devre dışı bırakır
Bilinmeyen Kaynaklara İzin Ver	Etkinleştirilirse, kullanıcılar bir .apk dosyası yükleyerek Uygulamaları yandan yükleyebilir.
USB Hata Ayıklamaya İzin Ver	Etkinleştirilirse, kullanıcılar USB Hata Ayıklamayı etkinleştirebilir.
Hesap Değişikliğine İzin Verme	Kapsayıcıdaki Hesapların oluşturulmasına, silinmesine ve değiştirilmesine izin vermez

	Bazı uygulamaların beklendiği gibi çalışması için hesap oluşturması veya hesapları değiştirmesi gerektiğini unutmayın

Gmail Değişimi

Kapsayıcıda Gmail'i yapılandırmanızı sağlar. Bu yapılandırmayı etkinleştirmenin uygulamayı otomatik olarak yüklemediğini lütfen unutmayın. Yine de bu uygulamayı zorunlu uygulama olarak eklemeniz gerekir.

E-posta Adresi	E-posta Adresi
Sunucu Ana Bilgisayar Adı	Sunucu Ana Bilgisayar Adı
Giriş Adı	Giriş Adı
İmza	İmza
Senkronize edilecek önceki gün sayısı	Senkronize edilecek önceki gün sayısı.
Cihaz Tanımlayıcısı	EAS Tanımlayıcı. Ortamınız bunu gerektirmiyorsa bunu boş bırakın
Güvenli Yuva Katmanı (SSL) kullanın	SSL kullanımını etkinleştirir. Bunun devre dışı bırakılması güvenliği azaltabilir
Tüm sertifikaları kabul edin	Tüm sertifikaları kabul eder. Bunu etkinleştirmek güvenliği azaltabilir
Yönetilmeyen hesaplara izin ver	Kullanıcının ek hesaplar eklemesine izin verir
Müşteri Sertifikası	Exchange sunucunuz bunu gerektiriyorsa istemci sertifikasını yükleyin

AE Sistem Uygulamaları

Burada Android Enterprise Container için Sistem Uygulamalarını etkinleştirebilirsiniz. Lütfen belirtilen uygulamanın sistemin depolama alanında olması gerektiğini unutmayın, aksi takdirde hiçbir şey olmaz.

Konteyner Şifresi

Yalnızca Android 7.0 veya üstü için

Konteyner için belirli bir parola gereksinimi belirlemenizi sağlar.

Minimum parola uzunluğu	Bir parolanın sahip olması gereken minimum sembol sayısını belirler
Şifre kalitesi	Parola gücü Belirtilmemiş = belirtilmemiş Her parola tamam = her parola kabul edilebilir en az sayısal karakter = en az sayısal karakter içermelidir en az karmaşık karakterler = en az özel karakterler içermelidir at least alphanumerical characters = en az alfanümerik karakter içermelidir at least alphabetic characters = en az alfabetik karakter içermelidir
Maksimum hareketsizlik süresi kilidi	Konteyner kilitlenene kadar geçen Maksimum Süre. Bu sadece kullanıcı tarafından seçilebilecek maksimum değeri yapılandırır
Parolada gereken minimum küçük harf sayısı	Parolada gereken minimum küçük harf sayısı
Parolada gerekli minimum büyük harfler	Parolada gerekli minimum büyük harfler
Parolada gerekli minimum harf dışı karakterler	Parolada gerekli minimum harf dışı karakterler
Parolada gerekli minimum sayısal basamaklar	Parolada gerekli minimum sayısal basamaklar
Parolada gereken minimum semboller	Parolada gereken minimum semboller
Parola sona erme zaman aşımı	Oluşturur, hangi zaman aralığından sonra parolanın süresi dolar ve yeni bir parola verilmelidir
Parola geçmişi kısıtlaması	İzin verilmeyen önceden kullanılmış şifre sayısı
Maksimum başarısız parola denemesi	Konteyner silinmeden önce bir parolanın ne kadar sıklıkla yanlış girilebileceğini belirler

Samsung KNOX

Aktivasyon

Burada Samsung KNOX Konteynerini etkinleştirebilirsiniz. Lütfen bunun artık Android 10 veya üzeri sürümlerde Samsung tarafından desteklenmediğini unutmayın. Android Enterprise Container'ı Android 10 veya üzerinde kullanın

Knox Parolası

Cihaz şifresinin ayarlarıyla ilgili yönergeleri belirleyin

Minimum parola uzunluğu	Parolanın kaç sembol içermesi gerektiğini belirler
Şifre kalitesi	Parola gücü Her parola tamam = Her parola tamam En az sayısal karakter = En az sayısal karakter bulunmalıdır En az karmaşık karakterler = Minimum özel karakterler bulunmalıdır En az alfanümerik karakter = En az alfanümerik karakter bulunmalıdır En az alfabetik karakter = En az alfabetik karakter bulunmalıdır
Gerekli minimum karmaşık karakterler	Minimum karmaşık karakterler mevcut olmalıdır
Maksimum Hareketsizlik Zaman Aşımı	Klavye kilidinden önce maksimum kullanıcı hareketsizlik zaman aşımı
Parmak İzi Kimlik Doğrulamasına İzin Ver	Parmak izi kimlik doğrulamasına izin ver
İris Kimlik Doğrulamasına İzin Ver	İris tanıma kimlik doğrulamasına izin verin
Maksimum Şifre Yaşı	Parolanın süresinin ne zaman dolacağını ve yeni bir parola verilmesi gerektiğini belirler
Saklanan Parola Geçmişi	İzin verilmeyen eski parola sayısı
Maksimum başarısız parola denemesi	Tam bir cihaz silme işlemi gerçekleşmeden önce parolanın ne kadar sıklıkla yanlış girilebileceğini belirler

Knox Güvenlik

Belirli cihaz işlevlerini sınırlandırın

Kamerayı Etkinleştir	Kamera kullanımına izin verin
Samsung KNOX Uygulama Mağazasına İzin Ver	Samsung KNOX App Store'un kullanımına izin verin
Google Play Hizmetlerine İzin Ver	Google Play Hizmetlerine İzin Ver
Tarayıcıya İzin Ver	Yerel tarayıcının kullanılmasına izin verin
Ekran Görüntülerine İzin Ver	Ekran Görüntülerinin oluşturulmasına izin verin
Kişi İçe Aktarmaya İzin Ver	Etkinleştirilirse, KNOX Konteynerinden cihaz kontaklarına erişime izin verilir

Kişi Dışa Aktarımına İzin Ver	Etkinleştirilirse, KNOX kontaklarına cihazdan erişime izin verilir
Takvim İçe Aktarmaya İzin Ver	Etkinleştirilirse, KNOX Konteynerinden cihaz takvimine erişime izin verilir
Takvim Dışa Aktarımına İzin Ver	Etkinleştirilirse, cihazdan KNOX takvimine erişime izin verilir
Güvenli Olmayan Tuş Takımına İzin Ver	Güvenli Olmayan Tuş Takımının Kullanımına İzin Verin
Dosya İçe Aktarmayı Etkinleştir	KNOX Konteynerine Dosya Aktarımını Etkinleştirme
Dosya Dışa Aktarmayı Etkinleştir	KNOX Konteynerinden Dosya Dışa Aktarımını Etkinleştirme

Knox Exchange

Burada KNOX Konteyneri için Exchange-Profilini yapılandırabilirsiniz

e-Posta Adresi	Sağlanan kullanıcının e-posta adresi Lütfen kimlik bilgileriyle çalışmak için kullanabileceğiniz ve her cihazda manuel olarak değişiklik yapmadığınız "Yer tutuculara" dikkat edin **Yer Tutucuları Göster** 'e tıklayarak bunları kendiniz görüntüleyebilirsiniz
Sunucu Ana Bilgisayar Adı	Exchange Sunucularınızın sunucu adresi
Giriş adı	İlgili son kullanıcı cihazının Oturum Açma Adı, lütfen buradaki "Yer Tutuculara" da dikkat edin
Etki Alanı	Etki alanı adresi
Şifre (yalnızca cihaz düzeyinde)	İsteğe bağlı olarak her bir cihaza bir parola verilebilir, bu parolanın boş kalması durumunda kullanıcıdan Exchange Parolasını girmesi istenecektir
Senkronize edilecek önceki gün sayısı	E-postaların ne zaman geri senkronize edileceğini belirleyen gün sayısı
İmza	Bir imza eklenebilir
Varsayılan Hesap	Bu e-posta hesabının standart hesap olduğunu belirler
Güvenli Yuva Katmanı (SSL) kullanın	SSL bağlantısı kullanın
Aktarım Katmanı Güvenliği (TLS) kullanın	TLS bağlantısı kullanın
Tüm sertifikaları kabul edin	Tüm sertifikalar kabul edilmektedir. Exchange Server'ınız kendinden imzalı bir sertifika kullanıyorsa lütfen bu seçeneği seçin

Knox e-Posta

e-Posta Adresi	Sağlanan kullanıcının e-posta adresi Lütfen kimlik bilgileriyle çalışmak için kullanabileceğiniz ve her cihazda manuel olarak değişiklik yapmadığınız "Yer tutuculara" dikkat edin **Yer Tutucuları Göster** 'e tıklayarak bunları kendiniz görüntüleyebilirsiniz
Gelen sunucu protokolü	Gelen sunucu protokolü IMAP veya POP
Gelen sunucu adresi	Gelen sunucu adresi
Gelen sunucu bağlantı noktası	Gelen sunucu bağlantı noktası
Gelen sunucu oturum açma/kullanıcı adı	Gelen sunucu oturum açma/kullanıcı adı
Gelen sunucu şifresi	Gelen sunucu şifresi
Gelen sunucu SSL kullanır	Gelen sunucu SSL kullanır
Gelen sunucu TLS kullanır	Gelen sunucu TLS kullanır
Gelen sunucu tüm sertifikaları kabul eder	Gelen sunucu tüm sertifika türlerini kabul eder
Giden sunucu protokolü	Giden sunucu protokolü SMTP
Giden sunucu bağlantı noktası	Giden sunucu bağlantı noktası
Giden Sunucu ekstra kimlik bilgileri kullanır	Giden Sunucu için ek kimlik bilgileri. Bu "kapalı" olarak ayarlanırsa, gelen sunucu ayarları kullanılacaktır
Giden sunucu oturum açma adı/kullanıcı adı	Giden sunucu oturum açma adı/kullanıcı adı
Giden sunucu parolası	Giden sunucu parolası
Giden sunucu SSL kullanır	Giden sunucu SSL kullanır
Giden sunucu TLS kullanır	Giden sunucu TLS kullanır
Giden sunucu tüm sertifikaları kabul eder	Giden sunucu tüm sertifika türlerini kabul eder
İmza	Burada bir imza eklenebilir
Yeni e-posta aldığında kullanıcıyı bilgilendir	Yeni e-posta aldığında kullanıcıyı bilgilendir

Knox Uygulamaları

Son kullanıcı cihazlarına dağıtmak istediğiniz uygulamaları burada oluşturun. Bunlar daha sonra KNOX-Konteynerinde mevcut olacaktır. Bir uygulama eklemek için lütfen Zorunlu Uygulamalar menüsünde yaptığınız gibi devam edin

Uygulama Adı	Uygulama Adı
O zamandan beri zorunlu	Uygulamanın eklendiği zaman noktası
Kaynak	Uygulamanın kaynağı (Play Store | Şirket içi)

Sembolü tıklayarak ilgili uygulama tekrar kaldırılabilir

Bağlantı Yönetimi

Wifi

Bu ayar için, dahili Erişim Noktalarına erişim için son kullanıcı cihazlarının ön yapılandırmasını gerçekleştirin

Hizmet Seti Tanımlayıcısı (SSID)	Bağlanılacak ağ için SSID
Gizli Ağ	AP'nin SSID'yi yayınlamaması durumunda etkinleştirin
Güvenlik Türü	AP'nin güvenlik türünü belirleyin

Güvenlik Türü

WEP

Şifre	AP için şifre

WPA/WPA2

Şifre	AP için şifre

802.1x EAP

EAP-Metodu	

PWD	Kimlik	Kimlik

	Şifre	Şifre

PEAP	Faz 2 Kimlik Doğrulama Protokolü	Hiçbiri	Ek protokol yok
		MSCHAPV2	MSCHAPV2 protokolü
		GTC	GTC protokolü
	CA Sertifikası	CA sertifikası	
	Kimlik	Kimlik	
	Anonim Kimlik	Anonim kimlik	
	Şifre	Şifre	

EAP-Metodu	

TTLS	Faz 2 Kimlik Doğrulama Protokolü	Hiçbiri	Ek protokol yok
		PAP	PAP protokolü
		MSCHAP	MSCHAP protokolü
		MSCHAPV2	MSCHAPV2 protokolü
		GTC	GTC protokolü
	CA Sertifikası	CA sertifikası	
	Kimlik	Kimlik	
	Anonim Kimlik	Anonim Kimlik	
	Şifre	Şifre	

TLS	CA Sertifikası	CA sertifikası
	Kimlik	Kimlik
	Şifre	Şifre

VPN

Bağlantı Türü	**VPN bağlantı türü oluştur**

VPN Türü olarak "Uygulama Başına VPN" seçerseniz, mevcut VPN İstemcileri değişecektir. Uygulama Başına VPN, VPN'i belirli uygulamalarla sınırlar ve belirli bir uygulama başlatıldığında VPN bağlantısını otomatik olarak başlatır.

AppTec360 VPN İstemcisi	AppTec360 VPN İstemcisini Evrensel Ağ Geçidi ile birlikte kullanır
Bağlantı Adı	VPN bağlantı adı
Ağ Geçidi Yapılandırması	Evrensel Ağ Geçidinin VPN Yapılandırmasını seçin
Her zaman açık VPN	VPN'i her zaman etkin olmaya zorlar, böylece tüm trafik VPN üzerinden geçer.
Yerel Kilitlemeyi Etkinleştir	Cihaz VPN'e bağlı değilken tüm ağ bağlantılarını engeller. Doğru yapılandırılmadığı takdirde bağlantının tamamen kopmasına neden olabileceğinden bunu dikkatli kullanın. Yalnızca Android 7 veya üzeri sürümlerde Android Enterprise için
AppTec360 Kilitlemeyi Etkinleştir	VPN bağlantısı başlatılana kadar tüm Uygulamaların kullanımını engeller

Cisco AnyConnect	
Bağlantı Adı	VPN bağlantı adı
Sunucu	Sunucu adresi
Sertifika Modu	Devre dışı = devre dışı bırakıldı Otomatik = otomatik

L2TP (Yalnızca KNOX)	Yalnızca Samsung cihazlarda kullanılabilir
Bağlantı Adı	Bağlantı adı
Sunucu	Sunucu adresi
L2TP Sırrını Etkinleştir	
DNS Arama Alanları	DNS arama etki alanları

Bağlantı Türü	**VPN bağlantı türü oluştur**

PPTP (Yalnızca KNOX)	Yalnızca Samsung cihazlarda kullanılabilir
Bağlantı Adı	VPN bağlantı adı
Sunucu	Sunucu adresi
Şifrelemeyi Etkinleştir	Şifrelemeyi etkinleştir
DNS Arama Alanları	DNS arama etki alanları

L2TP / IPSec PSK (Yalnızca KNOX)	Yalnızca Samsung cihazlarda kullanılabilir
Bağlantı Adı	VPN bağlantı adı
Sunucu	Sunucu adresi
IPSec Ön Paylaşımlı Anahtar	Kimlik doğrulama için önceden paylaşılan anahtar
L2TP Sırrını Etkinleştir	
L2TP Sırrı	
DNS Arama Alanları	DNS arama etki alanları

IPSec XAuth PSK (Yalnızca KNOX)	Yalnızca Samsung cihazlarda kullanılabilir
Bağlantı Adı	VPN bağlantı adı
Sunucu	Sunucu adresi
IPSec Tanımlayıcı	Bağlantı için kullanıcı adı
IPSec Ön Paylaşımlı Anahtar	Bağlantı için şifre
DNS Arama Alanları	DNS arama etki alanları

OpenVPN	
Bağlantı Adı	Bağlantı adı

OpenVPN Profili	.ovpn dosyasının içeriği buraya kopyalanacak
OpenVPN Uygulaması	OpenVPN kullanımı için iki farklı uygulama vardır "Android için OpenVPN" uygulamasını öneriyoruz. Ancak alternatif olarak, "OpenVPN Connect" uygulaması kullanılabilir

Kısıtlamalar

Burada bağlantı yönetimi ile ilgili kısıtlamaları ayarlayabilirsiniz.

Veri Dolaşımına İzin Ver	Dolaşımdayken mobil veriye izin ver
Veri Dolaşımını Zorla	Etkinleştirilirse, mobil veri için dolaşım kalıcı olarak etkinleştirilir (önerilmez!) Bu ayar "Veri Dolaşımına İzin Ver" ayarının üzerine yazılır!
Aşağıdaki ayarlar yalnızca Samsung KNOX 2.0 veya üzeri sürümlerde kullanılabilir	
Yalnızca Acil Durum Çağrılarına İzin Ver	Yalnızca Acil Durum Çağrılarına İzin Ver
WiFi'a İzin Ver	WiFi'a İzin Ver
WiFi Ağı Minimum Güvenlik Seviyesi	WiFi ağı minimum güvenlik seviyesi Açık = her türlü WiFi'a izin verilir
Kullanıcının WiFi ağları eklemesini yasaklayın	Kullanıcı kendisi bir WiFi ağı ekleyemez Bu ayar yalnızca "Bağlantı Yönetimi" altında bir WiFi profili tanımlanmışsa mümkündür
SMS ve MMS'e İzin Ver	Tümü = Tüm SMS ve MMS trafiğine izin verilir Yalnızca Gelen SMS = Yalnızca gelen SMS mesajlarına izin verilir Yalnızca Giden SMS = Yalnızca giden SMS mesajlarına izin verilir Yok = SMS / MMS trafiğine izin verilmez
Dolaşım Sırasında Senkronizasyona İzin Ver	Dolaşım Sırasında Senkronizasyona İzin Ver Açık = etkinleştirildi Kapalı = devre dışı Kullanıcı seçimi = kullanıcının seçimi
Ses Dolaşımına İzin Ver	Ses Dolaşımına İzin Ver Açık = etkinleştirildi Kapalı = devre dışı Kullanıcı Seçimi = kullanıcının seçimi
Sistem http Proxy Sunucusu Kullanma	Sistemin ayarlar bölümünde sağlanan bir HTTP proxy sunucusunun kullanımı bağlı ağa (WiFi veya APN) bağlıdır

APN

Aşağıdaki ayarlar yalnızca Samsung SAFE 2.0 veya üzeri sürümlerde kullanılabilir!

APN Görünen Adı	APN Görünen Adı	
Erişim Noktası Adı	APN'nin Adı	
Giden sunucu protokolü	Ayarlanmamış	
	Hiçbiri	
	PAP	PAP protokolü
	CHAP	CHAP protokolü
	PAP veya CHAP	PAP veya CHAP protokolü
MCC - Mobil Ülke Kodu	MCC buraya girilir, takılı SIM kartın MCC'sinin kullanılması gerekiyorsa bu alanı boş bırakın	
MNC - Mobil Ağ Kodu	MNC buraya girilir, takılı SIM kartın MCC'sinin kullanılması gerekiyorsa bu alanı boş bırakın	
Sunucu adresi	Sunucu adresi	
Sunucu bağlantı noktası numarası	Sunucu bağlantı noktası numarası	
Sunucu proxy adresi	Sunucu proxy adresi	
MMS sunucu adresi	MMS sunucu adresi, Standart için lütfen boş bırakın	
MMS bağlantı noktası numarası	MMS bağlantı noktası numarası	
MMS proxy adresi	MMS proxy adresi	
Kullanıcı adı	Kullanıcı adı	
Şifre	Şifre	
Erişim Noktası Tipi	İzin verilen türler şunlardır: "default", "mms", "supl" Bu alan boş bırakılırsa, "default,supl,mms" kullanılacaktır	
Tercih Edilen APN	APN tercih sebebidir	

Bluetooth

Burada, çeşitli Bluetooth ayarları gerçekleştirilebilir.

Aşağıdaki ayarlar yalnızca Samsung KNOX 1.0 veya üzeri sürümlerde kullanılabilir!

Bluetooth aracılığıyla Cihaz keşfine izin ver	Bluetooth aracılığıyla cihaz keşfine izin ver
Bluetooth Eşleştirmesine İzin Ver	Bluetooth eşleştirmesine izin ver
Bluetooth Kulaklık cihazlarına izin ver	Bluetooth Kulaklık cihazlarına izin ver
Bluetooth Eller Serbest cihazlarına izin ver	Bluetooth Eller Serbest cihazlarına izin ver
Bluetooth A2DP cihazlarına izin ver	Cihazlar arasında Bluetooth A2DP ses akışına izin ver
Giden Aramalara İzin Ver	BT üzerinden giden aramalara izin ver
Bluetooth ile Veri Aktarımına İzin Ver	Bluetooth üzerinden veri aktarımına izin ver
Bluetooth Tethering'e İzin Ver	Cihazın modem olarak kullanılmasını sağlar (Bluetooth internet bağlantısı)
Bluetooth ile Bilgisayar bağlantısına izin ver	Bluetooth ile Bilgisayar bağlantısına izin ver

PIM Yönetimi

Değişim

Yalnızca Samsung KNOX 1.0 veya üstü için kullanılabilir!

e-Posta Adresi	Sağlanan kullanıcının e-posta adresi Lütfen kimlik bilgileriyle çalışmak için kullanabileceğiniz ve her cihazda manuel olarak değişiklik yapmadığınız "Yer tutuculara" dikkat edin **Yer Tutucuları Göster** 'e tıklayarak bunları kendiniz görüntüleyebilirsiniz
Sunucu Ana Bilgisayar Adı	Exchange Sunucularınızın sunucu adresi
Giriş adı	İlgili son kullanıcı cihazı için Oturum Açma Adı, lütfen "Buradaki yer tutuculara da dikkat edin
Etki Alanı	Etki alanı adresi
Şifre (yalnızca cihaz düzeyinde)	İsteğe bağlı olarak, bireysel bir cihaza bir parola verilebilir; bu parolanın boş kalması durumunda, kullanıcıdan Exchange Parolasını girmesi istenecektir
Senkronize edilecek önceki gün sayısı	E-postaların ne zaman geri senkronize edileceğini belirleyen gün sayısı
İmza	Bir imza eklenebilir (İpucu: Bazı cihazlar imza için HTML biçimlendirmesi gerektirir)
Varsayılan Hesap	Bu posta hesabının standart hesap olduğunu belirler
Güvenli Yuva Katmanı (SSL) kullanın	SSL bağlantısı kullanın
Aktarım Katmanı Güvenliği (TLS) kullanın	TLS bağlantısı kullanın
Tüm sertifikaları kabul edin	Tüm sertifikalar kabul edilmektedir. Exchange Server'ınız kendinden imzalı bir sertifika kullanıyorsa lütfen bu seçeneği seçin

e-Posta

Burada, IMAP ve POP hesaplarını ilgili son kullanıcı cihazlarına dağıtabilirsiniz.

Aşağıdaki ayarlar yalnızca Samsung KNOX 1.0 veya üzeri sürümlerde kullanılabilir!		
e-Posta Adresi	Sağlanan kullanıcının e-posta adresi Lütfen kimlik bilgileriyle çalışmak için kullanabileceğiniz ve her cihazda manuel olarak değişiklik yapmadığınız "Yer tutuculara" dikkat edin **Yer Tutucuları Göster** 'e tıklayarak bunları kendiniz görüntüleyebilirsiniz	
Gelen sunucu protokolü	Gelen sunucu protokolü	IMAP oder POP
Gelen sunucu adresi	Gelen sunucu adresi	
Gelen sunucu bağlantı noktası	Gelen sunucu bağlantı noktası	
Gelen sunucu oturum açma/kullanıcı adı	Gelen sunucu oturum açma/kullanıcı adı	
Gelen sunucu şifresi (yalnızca cihaz düzeyinde)	Gelen sunucu şifresi (yalnızca cihaz düzeyinde)	
Gelen sunucu SSL kullanır	Gelen sunucu SSL kullanır	
Gelen sunucu TLS kullanır	Gelen sunucu TLS kullanır	
Gelen sunucu tüm sertifikaları kabul eder	Gelen sunucu tüm sertifika türlerini kabul eder	
Giden sunucu protokolü	Giden sunucu protokolü	SMTP
Giden sunucu bağlantı noktası	Giden sunucu bağlantı noktası	
Giden Sunucu ekstra kimlik bilgileri kullanır	Giden sunucu için ek kimlik bilgileri. Bu "kapalı" olarak ayarlanırsa, gelen sunucu ayarları kullanılacaktır	
Giden sunucu oturum açma adı/kullanıcı adı	Giden sunucu oturum açma adı/kullanıcı adı	
Giden sunucu şifresi (yalnızca cihaz düzeyinde)	Giden sunucu parolası	
Giden sunucu SSL kullanır	Giden sunucu SSL kullanır	
Giden sunucu TLS kullanır	Giden sunucu TLS kullanır	

Giden sunucu tüm sertifikaları kabul eder	Giden sunucu tüm sertifika türlerini kabul eder
İmza	Buraya bir imza eklenebilir (İpucu: Bazı cihazlar imza için HTML biçimlendirmesi gerektirir)
Yeni e-posta aldığında kullanıcıyı bilgilendir	Yeni e-posta aldığında kullanıcıyı bilgilendirir

AE Gmail Değişimi

Bilgi: Bu Yapılandırma Gmail uygulamasına uygulanacaktır. Bu yüzden Gmail'i onaylamanız ve yüklemeniz gerekir.

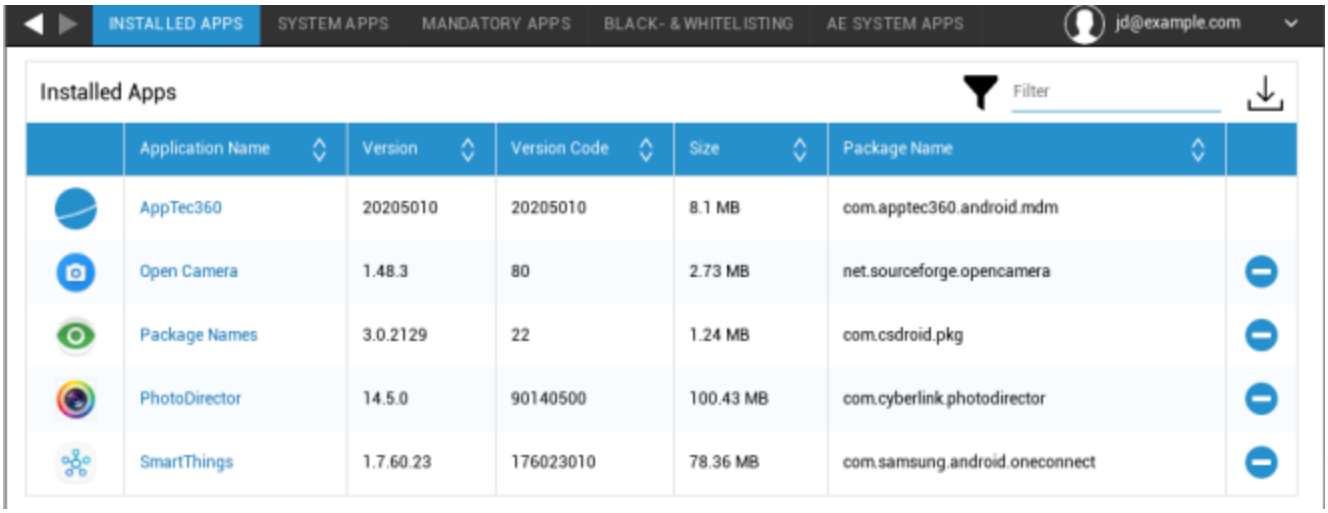
e-Posta Adresi	Sağlanan kullanıcının e-posta adresi Lütfen kimlik bilgileriyle çalışmak için kullanabileceğiniz ve her cihazda manuel olarak değişiklik yapmadığınız "Yer tutuculara" dikkat edin Yer Tutucuları Göster'e tıklayarak bunları kendiniz görüntüleyebilirsiniz
Sunucu Ana Bilgisayar Adı	Exchange Sunucularınızın sunucu adresi
Giriş adı	İlgili son kullanıcı cihazı için Oturum Açma Adı, lütfen "Buradaki yer tutuculara da dikkat edin
İmza	Bir imza eklenebilir (İpucu: Bazı cihazlar imza için HTML biçimlendirmesi gerektirir)
Senkronize edilecek önceki gün sayısı	E-postaların ne zaman geri senkronize edileceğini belirleyen gün sayısı
Cihaz Tanımlayıcısı	EAS Tanımlayıcı. Ortamınız bunu gerektirmiyorsa bunu boş bırakın
Güvenli Yuva Katmanı (SSL) kullanın	SSL bağlantısı kullanın
Tüm sertifikaları kabul edin	Tüm sertifikalar kabul edilmektedir. Exchange Server'ınız kendinden imzalı bir sertifika kullanıyorsa lütfen bu seçeneği seçin
Yönetilmeyen hesaplara izin ver	Kullanıcının ek hesaplar eklemesine izin verir
Müşteri Sertifikası	Exchange sunucunuz bunu gerektiriyorsa istemci sertifikasını yükleyin

Uygulama Yönetimi

Kurumsal Uygulama Yöneticisi

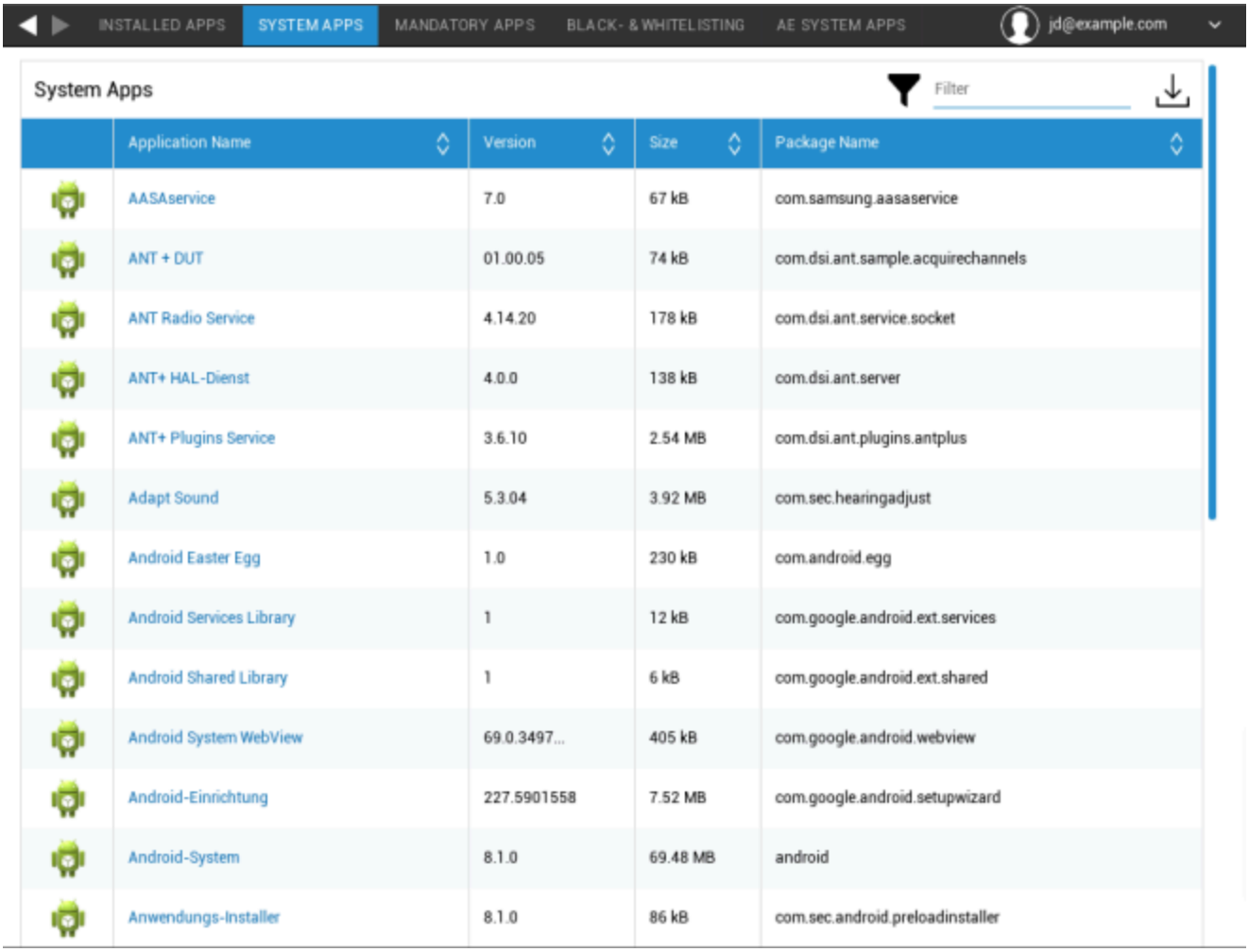
Yüklü Uygulamalar (yalnızca cihaz düzeyinde)

Burada, son kullanıcı cihazında o anda yüklü olan tüm Uygulamalar sizin için görüntülenecektir.


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

Sistem Uygulamaları (yalnızca cihaz düzeyinde)

"Sistem Uygulamaları" altında, önceden yüklenmiş tüm sistemler paket adları ve sürümleriyle birlikte listelenecektir.



Zorunlu Uygulamalar

Zorunlu Uygulamalar bölümünde hangi uygulamaların cihaza yüklenmesi gerektiğini tanımlayabilirsiniz. Yapılandırmanıza ve cihazınıza bağlı olarak uygulama otomatik olarak yüklenecek veya kullanıcıdan yüklemesi istenecektir.

Kolay uygulama yönetimi için Android Enterprise kullanmanızın tavsiye edildiğini lütfen unutmayın.

Senaryolar aşağıda listelenmiştir:

Normal Play Store Uygulamaları

Playstore Uygulama Yüklemeleri her zaman bir kullanıcı etkileşimine ihtiyaç duyar. Ayrıca cihazda bir Google Hesabı yapılandırılmalıdır.

Şirket İçi Uygulama Kurulumu

Samsung Cihazlarda bu uygulamalar sessizce yüklenecektir. Bunun tek istisnası, kullanıcının kurulumu onaylaması gereken konteynerdir.

Başka herhangi bir senaryoda, kullanıcının uygulama yüklemesini onaylaması gerekir.

Android Kurumsal Play Store Uygulamaları

Bu Uygulamalar her zaman kullanıcı etkileşimi olmadan sessizce yüklenecektir.

Zorunlu bir uygulama eklemek için "+" işaretine tıklayın ve listeden istediğiniz uygulamayı seçin. Cihaz Android Enterprise ile tam yönetimli veya konteyner olarak yapılandırılmışsa, "Google Play Store" Sekmesinden uygulama yükleyemeyeceğinizi lütfen unutmayın.

Android Enterprise kullanıyorsanız, "AE Play Store" bölümünden uygulamaları seçin. Uygulamaları burada kullanılabilir hale getirmek için, Genel Ayarlar → AE Play Store → Play Store Uygulamaları bölümüne giderek Google Enterprise Play mağazasında onaylayın.

Zorunlu bir uygulama kaldırıldığında, cihazdan da kaldırılacaktır.

Zorunlu uygulama listesinde bir uygulamanın adına tıklayabilir ve bir uygulamayı yapılandırmak için "yapılandırma" sekmesine gidebilirsiniz. Bu, Android Enterprise kullanımını gerektirir ve uygulamanın bunu desteklemesi gerekir. Bu nedenle mevcut seçenekler seçilen uygulamaya bağlıdır.

AE Sistem Uygulamaları

Burada Android Kurumsal cihazlar için Sistem Uygulamalarını etkinleştirebilirsiniz. Lütfen belirtilen uygulamanın sistemin depolama alanında olması gerektiğini unutmayın, aksi takdirde hiçbir şey olmaz. 296

Kısıtlamalar ve Ayarlar

Kara ve Beyaz Liste

Burada bir kara veya beyaz liste tanımlayabilirsiniz. Kara listedeki tüm uygulamalar engellenecektir. Beyaz listede olmayan tüm uygulamalar engellenecektir. Boş bir kara liste hiçbir şeyi engellemezken, boş bir beyaz liste her şeyi engeller*

**Kurumsal App Store'daki tüm zorunlu uygulamalar ve uygulamalar otomatik olarak beyaz listeye alınacaktır. Bunları manuel olarak eklemenize gerek yok*

"+" işaretine tıkladığınızda, kara veya beyaz listenize eklemek istediğiniz bir uygulamayı arayabilir veya manuel olarak bir paket adı girebilirsiniz.

Sistem Uygulama Kısıtlamaları

"Sys App Restrictions" altında, diğer şeylerin yanı sıra, önceden yüklenmiş uygulamaları ve hizmetleri istediğiniz gibi engelleyebilirsiniz.

Tarayıcıyı Devre Dışı Bırak	Standart tarayıcıyı devre dışı bırak
Takvimi Devre Dışı Bırak	Yerel takvimi devre dışı bırakma
Hesap Makinesini Devre Dışı Bırak	Hesap makinesini devre dışı bırak
Chrome Tarayıcıyı Devre Dışı Bırak	Chrome tarayıcıyı devre dışı bırak
Saati Devre Dışı Bırak	Saati devre dışı bırak
Kişileri Devre Dışı Bırak	Kişileri Devre Dışı Bırak
Çeviriciyi Devre Dışı Bırak	Yerel çeviriciyi devre dışı bırak
E-postayı Devre Dışı Bırak	E-postayı devre dışı bırak
Değişimi Devre Dışı Bırak	Exchange hesaplarını devre dışı bırakma
Facebook'u Devre Dışı Bırak	Facebook uygulamasını devre dışı bırakın
Galeriyi Devre Dışı Bırak	Yerel galeri uygulamasını devre dışı bırakın
Gmail'i devre dışı bırakın	Gmail'i devre dışı bırakın
Google Kitaplar'ı devre dışı bırakın	Google Kitaplar'ı devre dışı bırakın
Google Play Kiosk'u devre dışı bırakma	Google Play Kiosk'u devre dışı bırakma
Google Haritalar'ı devre dışı bırakın	Google Haritalar'ı devre dışı bırakın
Google Music'i devre dışı bırakma	Google Music'i devre dışı bırakma
Google Movies'i devre dışı bırakın	Google Movies'i devre dışı bırakın
Google Play Store'u devre dışı bırakma	Google Play Store'u (genel App Store) devre dışı bırakın
Google Plus'ı devre dışı bırakın	Google Plus'ı devre dışı bırakın
Google Aramayı Devre Dışı Bırak	Google Aramayı Devre Dışı Bırak
Google Talk / Google Hangouts'u devre dışı bırakma	Google Talk / Google Hangouts'u devre dışı bırakma
Müzik Çaları Devre Dışı Bırak	Yerel müzik çalar uygulamasını devre dışı bırakın
Ayarları Devre Dışı Bırak	Cihaz ayarlarını devre dışı bırakma
Sim Araç Takımını Devre Dışı Bırak	Sim Toolkit hizmetlerini devre dışı bırakın
SMS / MMS'i Devre Dışı Bırak	SMS / MMS'i Devre Dışı Bırak
Sokak Görünümünü Devre Dışı Bırak	Street View hizmetlerini devre dışı bırakın
Youtube'u Devre Dışı Bırak	Youtube'u Devre Dışı Bırak

Samsung Uygulamaları

"Samsung Uygulamaları" altında, Samsung cihazları için ek ayarlar ve/veya kısıtlamalar tanımlayabilirsiniz.

AllShare Play / Samsung Link'i devre dışı bırakma	AllShare Play / Samsung Link'i devre dışı bırakma
ChatON'u devre dışı bırak	ChatON'u devre dışı bırak
Oyun Merkezini Devre Dışı Bırak	Oyun Merkezini Devre Dışı Bırak
Grup Oyununu Devre Dışı Bırak	Grup Oyununu Devre Dışı Bırak
Yardımı Devre Dışı Bırak	Samsung Yardım'ı devre dışı bırakma
KNOX'u devre dışı bırak	Samsung KNOX Konteynerini Devre Dışı Bırak
Memo'yu Devre Dışı Bırak	Sesli Notu Devre Dışı Bırak
Dosyalarımı Devre Dışı Bırak	Dosyalarımı Devre Dışı Bırak
Optik Okuyucuyu Devre Dışı Bırak	Optik Okuyucuyu Devre Dışı Bırak
Polaris Office'i devre dışı bırakın	Polaris Office'i devre dışı bırakın
Readers Hub / Samsung Books'u devre dışı bırak	Readers Hub / Samsung Books'u devre dışı bırak
S Memo'yu Devre Dışı Bırak	Samsung Memo uygulamasını devre dışı bırakma
S Çeviriciyi Devre Dışı Bırak	Samsung Translator uygulamasını devre dışı bırakın
S Voice'u Devre Dışı Bırak	S Voice asistanını devre dışı bırakma
Samsung Uygulamalarını Devre Dışı Bırak	Samsung App Store'u devre dışı bırakma
Samsung Hub'ı devre dışı bırak	Samsung Eğlence Mağazalarını Devre Dışı Bırak
Video Oynatıcıyı Devre Dışı Bırak	Video Oynatıcıyı Devre Dışı Bırak
Ses Kaydediciyi Devre Dışı Bırak	Ses Kaydediciyi Devre Dışı Bırak
WatchON'u devre dışı bırak	WatchON'u devre dışı bırak (uzaktan kumandayı simüle eder)

Huawei Uygulamaları

"Huawei Uygulamaları" altında, Huawei cihazında ek ayarlar ve/veya kısıtlamalar tanımlayabilirsiniz.

DLNA'yı devre dışı bırak	DLNA'yı devre dışı bırak
Uygulama Yükleyiciyi Devre Dışı Bırak	Uygulama Yükleyiciyi Devre Dışı Bırak
Dosya Yöneticisini Devre Dışı Bırak	Dosya Yöneticisini Devre Dışı Bırak
Yedekleme Yöneticisini Devre Dışı Bırak	Yedekleme Yöneticisini Devre Dışı Bırak
Sistem Güncelleyicisini Devre Dışı Bırak	Sistem Güncelleyicisini Devre Dışı Bırak
Araç Kutusunu Devre Dışı Bırak	Araç Kutusunu Devre Dışı Bırak
Hava Durumunu Devre Dışı Bırak	Hava Durumunu Devre Dışı Bırak
FM Radyoyu Devre Dışı Bırak	FM Radyoyu Devre Dışı Bırak

Uygulama Yönetimi Ayarları

Burada InHouse Uygulamalarının güncelleme davranışını tanımlayabilirsiniz.

Güncelleme Kontrol Sıklığı, AppTec360 Uygulamasının Şirket içi uygulamalar için güncellemeleri ne sıklıkta arayacağını tanımlar. Yeni bir sürüm tespit edildiğinde indirilecek ve yüklenecektir.

Wi-Fi Eşiği, Uygulama yapılandırdığınız Eşikten büyükse indirmenin Wi-Fi bağlantılarıyla sınırlandırılıp sınırlandırılmayacağını tanımlar. Daha küçükse veya bir eşik tanımlamazsanız, uygulama Wi-Fi'de ve hücresel bir ağda indirilir.

Kurumsal Uygulama Mağazası

Lütfen uygulamaların buraya (Enterprise App Store) eklenmesinin cihaz(lar)a otomatik olarak yüklenmesini SAĞLAMAYACAĞINI unutmayın. Kullanıcının cihazda Enterprise App Store'u açması ve uygulamayı manuel olarak yüklemesi gerekir.

Uygulamaları cihaza otomatik olarak yüklemek istiyorsanız, lütfen "Uygulama Yönetimi" → "Kurumsal Uygulama Yöneticisi" → "Zorunlu Uygulamalar" bölümüne gidin ve istediğiniz uygulamaları buraya ekleyin.

Bu nokta altında, kullanıcılarınıza isteğe bağlı Uygulamalar dağıtabilirsiniz.

Playstore

Mağazaya bir Play Store uygulaması eklemek için "+" işaretine tıklayın. Android Enterprise kullanıyorsanız lütfen "Uygulama Yönetimi Enterprise Play Store "a gidin. Ayrıca, burada tanımlanan uygulamaları yüklemek için cihazda bir Google Hesabının yapılandırılması gerektiğini unutmayın.

Şirket İçi

"Şirket İçi" başlığı altında, şirket içinde geliştirilen uygulamaları yükleyebilir ve dağıtabilirsiniz.

Daha sonra kullanıcı tarafından yüklenebilecek bir InHouse uygulamasını kurumsal uygulama mağazasına eklemek için "+" işaretine tıklayın. Bu diyalogda yeni bir InHouse uygulaması da yükleyebilirsiniz.

Kurumsal Play Store

Lütfen uygulamaların buraya (Enterprise Play Store) eklenmesinin cihaz(lar)a otomatik olarak yüklenmesini SAĞLAMAYACAĞINI unutmayın. Kullanıcının cihazda Play Store'u açması ve uygulamayı manuel olarak yüklemesi gerekir.

Uygulamaları cihaza otomatik olarak yüklemek istiyorsanız, lütfen "Uygulama Yönetimi" → "Kurumsal Uygulama Yöneticisi" → "Zorunlu Uygulamalar" bölümüne gidin ve istediğiniz uygulamaları buraya ekleyin.

Bu nokta altında, kullanıcılarınıza isteğe bağlı Uygulamalar dağıtabilirsiniz.

Buradan Android Enterprise Playstore'a uygulama ekleyebilirsiniz. Uygulamaları Genel Ayarlar → AE Play Store → Play Store Uygulamaları bölümünden onaylamanız gerektiğini lütfen unutmayın. Bu Uygulamalar normal Google Play Store'a eklenecektir.

Ayrıca, öncelikle Genel Ayarlar → Uygulama Yönetimi → AE Play Store → Mağaza Düzeni bölümünde Uygulamalar ile bir Düzen tanımlamanız gerektiğini unutmayın.

Uygulamaları mağazaya başarılı bir şekilde ekleyebilmeniz için önce bir Düzen içinde olmaları gerekir.

Kiosk Modu ve Başlatıcı

Kiosk Modu

Kiosk Modu, bir uygulamayı veya URL'yi önceden tanımlamanıza olanak tanır. O zaman sadece bu uygulamayı ve / veya URL'yi çalıştırmak / ziyaret etmek mümkün olacaktır.

Aynı şekilde, çeşitli donanım düğmeleri Kiosk Modu çeşitliliğinde devre dışı bırakılabilir.

Otomatik Başlatma	Profil son kullanıcı cihazına ulaşır ulaşmaz Kiosk Modunu otomatik olarak başlatır
Zamanlanmış Kiosk Modu?	Kiosk Modu için bir zaman planlayabilirsiniz, bu daha sonra sizin belirlediğiniz bir zamanda otomatik olarak başlayacak ve bitecektir
Başlangıç Zamanı	Başlangıç zamanı
Dakika cinsinden zaman	Kiosk Modunun tekrar sona ermesi gereken dakika cinsinden süre

Uygulama Türü

Tek Uygulama	Uygulamayı Kiosk Modunda başlatmak istiyorsanız, "Uygulama Türü" altında "Paket" seçeneğini seçin
Kiosk Uygulaması	Kiosk Modunda başlatılması gereken bir uygulama seçmek için buraya tıklayın Her zamanki Uygulama Yönetimine genel bakışı bulacaksınız "Google Play Store", "Android Şirket İçi Uygulamalar" ve "Paket Adı" arasında seçim yapabilirsiniz

Uygulama Türü

URL	Kiosk Modunda bir URL başlatmak istiyorsanız, "Uygulama Türü" altında "URL "yi seçin Ardından istediğiniz URL adresini tanımlayın
Hareketsizlikten sonra tarayıcıyı temizle	Burada, Kiosk Modunun yeniden başlatılması gereken zaman aralığını dakika cinsinden tanımlayabilirsiniz
Web Önbelleğini ve Çerezleri Temizle	Bu işlevi etkinleştirirseniz, Kiosk Modu yeniden başlatıldıktan sonra Web Önbelleği (çerezler ve önbelleğe alınmış resimler) silinecektir
Aynı Menşe Politikası	Bu işlev etkinse, kullanıcı yalnızca tanımlanmış bir URL'nin alt sayfalarında gezinebilir Örneğin, aşağıdaki URL'yi tanımladınız:www.mypage.com Ardından, kullanıcı şu adreste gezinebilir: www.mypage.com/subpage
Beyaz Listedeki URL'ler	Burada bir Beyaz Liste tutabilirsiniz, tüm bu URL'lere izin verilir Satır başına en fazla 1 URL Bir URL http:/ veya https:// ile başlamalıdır
Kara Listeye Alınan URL'ler	Burada bir Kara Liste tutabilirsiniz, tüm bu URL'lere izin verilmez Satır başına en fazla 1 URL Bir URL http:/ veya https:// ile başlamalıdır
Ekran Yönü	Bu ayar ekran ayarlarıyla ilgilidir Otomatik = otomatik Portre = dikey format Landscape = manzara modu

Çoklu Uygulama	"Çoklu Uygulama" Kiosk Modunu seçerseniz, AppTec360 Launcher'ın kullanımı zorunlu olacaktır.
Uygulamalar	Uygulama: Kiosk Uygulaması olarak bir Playstore veya Şirket İçi Uygulama seçin. Bir paket adı girmek de mümkündür. Seçilen Kiosk Uygulaması cihazda yüklü olmalıdır. Kiosk Uygulamasını zorunlu olarak ayarlamayı unutmayın. Ana Ekranda Kısayol: "Açık" olarak ayarlanırsa ana ekranda bir kısayol oluşturulacaktır. "Kapalı" olarak ayarlanırsa Uygulama, Uygulama Listesinde görünmeye devam edecektir.

Çıkış Şifresi Etkin	Bu işlevi etkinleştirirseniz, kullanıcının Kiosk Modunu sizin tarafınızdan önceden tanımlanmış bir parola ile sonlandırması mümkündür
Çıkış Şifresi	Bu, sizin tarafınızdan önceden tanımlanmış olan paroladır
Durum Çubuğunu Otomatik Daralt	Etkinleştirilirse, Durum Çubuğu otomatik olarak harmanlanır. Bu seçenekle kullanıcılar Durum Çubuğundaki bilgileri görebilir, ancak işlevlerine erişemez
Durum Çubuğunu Devre Dışı Bırak	Durum Çubuğu Bildirimler, Kısayollar ve Bilgiler içerir. Yalnızca KNOX 1.0 veya üzeri sürümlere sahip Samsung cihazları için kullanılabilir.
Ses Tuşlarını Devre Dışı Bırak	Ses tuşlarını devre dışı bırakma (yalnızca KNOX 1.0 veya üzeri Samsung cihazlarında kullanılabilir)
Açma / Kapama Anahtarını Devre Dışı Bırak	Açma / Kapama düğmesini devre dışı bırakma (yalnızca KNOX 1.0 veya üzeri Samsung cihazlarında kullanılabilir)
Ana Ekran Düğmesini Devre Dışı Bırak	Ana Ekran düğmesini devre dışı bırakın. Bu işlev etkinleştirildiyse, Kiosk Modu yalnızca AppTec360 Konsolunda sonlandırılabilir (yalnızca KNOX 1.0 veya üzeri Samsung cihazlarında kullanılabilir)
Gezinti Çubuğunu Devre Dışı Bırak	Bununla Gezinti Çubuğunu (Geri / Menü) devre dışı bırakabilirsiniz Bu işlev etkinleştirildiyse, Kiosk Modu yalnızca AppTec360 Konsolunda sonlandırılabilir (yalnızca KNOX 1.0 veya üzeri Samsung cihazlarında kullanılabilir)

Uygulama Güncelleme Ayarları	
Uygulama Güncellemelerine İzin Ver	Kiosk Modu etkin olsa bile kullanıcılardan uygulama güncellemeleri yapmaları istenecektir. Samsung KNOX'a sahip cihazlarda uygulamalar sessizce güncellenecektir.
Güncelleme Penceresi	Kullanıcılardan uygulama güncellemelerini yüklemelerinin isteneceği bir aralık belirleyin.

TeamViewer	
Katılımsız Erişimi Etkinleştir	Etkinleştirilirse, yöneticiler kullanıcı etkileşimi olmadan cihazı uzaktan kontrol edebilir. TeamViewer Host uygulamasının cihaza yüklenmesi gerekir.

AppTec360 Başlatıcı

AppTec360 Başlatıcıyı Etkinleştir	Açık: AppTec360 Başlatıcıyı etkinleştirir. Kullanıcının bunu bir kez varsayılan Başlatıcı olarak ayarlaması gerekir. Not: Kiosk Modu etkinleştirilirse ve Kiosk Modu "Çoklu Uygulama" olarak ayarlanırsa, AppTec360 başlatıcısının kullanımı zorunlu olacaktır.
Büyük Simgeler	Açık: Başlatıcıda Uygulama Simgelerinin daha büyük bir Sürümünü gösterir
AppTec360 Uygulama Simgesini Gizle	Açık: AppTec360 Uygulamasını tamamen gizler
AppTec360 Mağaza Simgesini Gizle	Açık: AppTec360 Enterprise AppStore'u tamamen gizler

AppTec360 Ayarları

AppTec360 Ayarlar Uygulamasını Etkinleştir	AppTec360 Ayarlar Uygulaması WiFi ve Bluetooth bağlantıları üzerinde kontrol sağlar
Çoklu Uygulamada Ayarları Etkinleştir Kiosk Modu	Etkinleştirilirse, kullanıcılar Çoklu Uygulama Kiosk Modu etkinken AppTec360 Ayarlar Uygulamasına erişebilir

Uzaktan Kumanda

Splashtop

Splashtop Kurulumunun mevcut durumunu gösterir. Burada, Splashtop aracılığıyla cihaza uzaktan erişmek için gerçekleştirmeniz gereken adımları göreceksiniz. Burada ayrıca Splashtop web sitesinden alabileceğiniz dağıtım kodunuzu da girmeniz gerekir. Cihaza bağlanmak için dağıtım kodu gereklidir.

Teamviewer

Teamviewer Kurulumunun mevcut durumunu gösterir. Burada, Teamviewer aracılığıyla cihaza uzaktan erişmek için gerçekleştirmeniz gereken adımları göreceksiniz.

İçerik Yönetimi

İçerik kutusu

Burada bu cihaz için Contentbox'ı etkinleştirebilirsiniz. Etkinleştirildikten sonra Contentbox Uygulaması cihaza yüklenecektir.

Güvenli Tarayıcı

Burada bu cihaz için Güvenli Tarayıcıyı etkinleştirebilirsiniz. Etkinleştirildikten sonra, Secure Browser Uygulaması cihaza yüklenecektir. Bu Tarayıcı, cihazda ihtiyaçlarınızla sınırlı bir Web Tarayıcısı sunacak şekilde yapılandırılabilir.

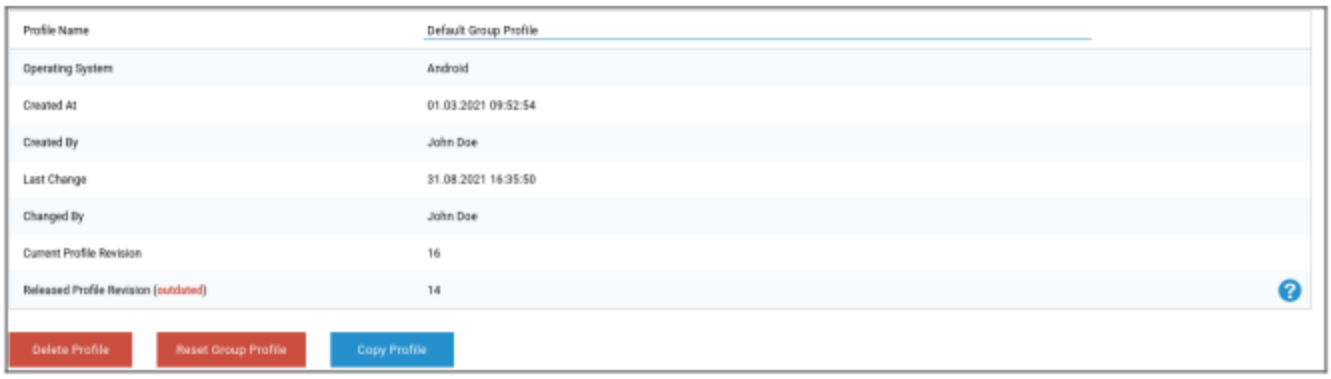
Şifre Gerektir	Kullanıcının tarayıcıya erişmek için bir parola ayarlamasını ve kullanmasını gerektirir.
İndirmeleri Kısıtla / İçeride Aç	Web Sitelerinden İndirmeleri Engeller
Yüklemeleri Kısıtla	Yüklemeleri belirli URL'lerle kısıtlar. Yüklemeyi tamamen engellemek için URL sağlamayın
Kopyalamaya İzin Ver	Web sayfaları içinde metin kopyalamaya, kesmeye veya paylaşmaya izin verin.
Ekran Yakalamaya İzin Ver	Ekran görüntülerinin yakalanmasına izin verin.
Veri temizleme sıklığı	Hangi sıklıkta TÜM kullanıcı verilerinin (geçmiş, önbellek vb.) otomatik olarak kaldırılacağını seçin.
Şirket Yer İmleri	Yer İmleri, tarayıcı yer imlerindeki "Şirket yer imleri" klasöründe görünecektir. Kullanıcı tarafından düzenlenemezler.
Adres Çubuğunu Gizle	Kullanıcının ziyaret ettiği URL'yi görmemesi için Adres Çubuğunu gizler
Tarayıcı İçi Beyaz Liste (Universal Gateway olmadan)	İstemci tarafı URL beyaz listesini etkinleştirir. - Şirket Yer İmleri her zaman beyaz listeye alınır - Yalnızca 100 URL için desteklenir - Sınırsız Kara ve Beyaz Liste için lütfen Evrensel Ağ Geçidini kullanın
Ağ geçidi tabanlı Kara ve Beyaz Liste	Kara listeye alma aşağıdaki gereksinimlere sahiptir: - Çalışan bir AppTec360 Universal Gateway ("Genel Ayarlar" → "Universal Gateway") - Belirtilen bir DNS sunucusuyla çalışan bir VPN yapılandırması ("Genel Ayarlar" → "Universal Gateway" → "VPN Ayarları") - Bir Kara Liste yapılandırması ("Genel Ayarlar" → "Universal Gateway" → "Etki Alanı Kara Listesi") - Profilde geçerli bir VPN bağlantısı ("Bağlantı Yönetimi" → "VPN")

Yapılandırma Windows 10 PC

Genel

Grup profiline genel bakış (yalnızca grup düzeyinde)

Bir grup profilini açtığınızda, profile hızlı bir genel bakış elde edersiniz.



Profil Adı	Profilin adı (burada değiştirilebilir)
İşletim Sistemi	Profilin ait olduğu İşletim Sistemi
Şu Adreste Oluşturuldu	Yaratılış zamanı
Tarafından Oluşturuldu	Profilin yaratıcısı
Son Değişiklik	Profilde yapılan son değişikliğin zamanı
Tarafından Değiştirildi	Son değişiklikleri yapan hesap
Güncel Profil Revizyonu	Kayıtlı profil durumunun revizyonu
Profil Revizyonu Yayınlandı	Atanmış profil revizyonu ("Şimdi ata"). Etiket metnin arkasında "(eski)" ibaresini gösteriyorsa, bu profili kaydettiğiniz ancak henüz atamadığınız anlamına gelir, bu nedenle cihazlar hala eski sürümü alacaktır.

Cihaza Genel Bakış (yalnızca cihaz düzeyinde)

Aşağıdakileri içeren cihazın özetlenmiş genel görünümü:

Bilgisayar Adı	Bilgisayarın adı
Müşteri	Windows tipi cihazlar
Bilinen Son Konum	Cihazların bilinen son konumunun enlem ve boylamı
Atanmış Zorunlu Uygulamalar	Cihaza atanan Zorunlu Uygulama Sayısı
PC UID	Bilgisayarın UID'si
İşletim Sistemi Sürümü	Windows Sürümünüzü gösterir
İşletim Sistemi Sürümü	Şu anda yüklü Windows Sürümü
İşletim Sistemi Yapısı	Geçerli Windows Yapısı
İşletim Sistemi	Şu anda kurulu İşletim Sistemi
Seri Numarası	Cihazın Seri Numarası
Cihaz Sahipliği	Yapılandırılmış Sahiplik Türü
Cihaz Tipi	Cihazın Türü
Köklü	Cihazın köklü olup olmadığını gösterir
Uyumlu	Cihazın uyumlu olup olmadığını gösterir
Son Görülme	Profil üzerinde değişikliklerin yapıldığı tarih ve saat
Kullanıcı Ataması	Bu cihazın o anda atandığı kullanıcı veya grubu görüntüler. Açılır listeden farklı bir kullanıcı veya grup seçerek cihazı taşıyabilirsiniz.

Ayarlar

Otomatik Güncellemeye İzin Ver	Otomatik sistem güncellemelerine izin verin veya izin vermeyin.

Konfigürasyon Revizyonu (sadece cihaz seviyesinde)

Burada cihaza hangi grup profilinin atandığına dair bir genel bakış elde edersiniz.

Grup profiline tıklarsanız, profile doğrudan erişirsiniz ve ayarları gerçekleştirebilirsiniz.

Sembol ile, atanan uygulamaları grup profilinin ayarlarına geri döndürebilirsiniz.

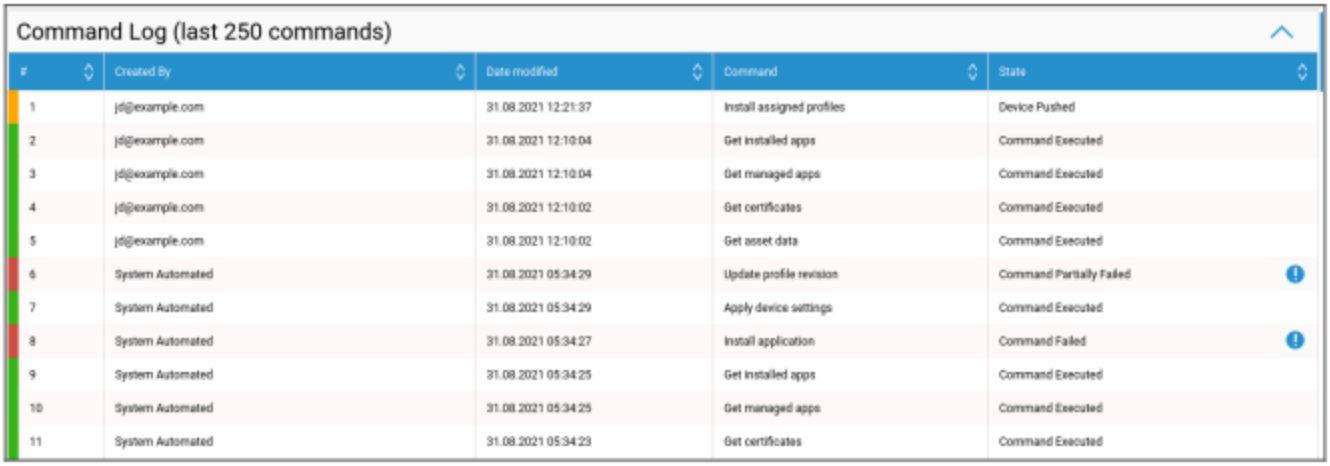
Sembol ile cihaz profilini hiçbir ayara sahip olmayacak şekilde sıfırlayabilirsiniz.

"Newer Revision available" grup profilinin değiştirildiğini ve kaydedildiğini ancak atanmadığını gösterir. Değişiklikleri cihazlara uygulamak için grup profilinin grup düzeyinde "Şimdi ata" ile atanması gerekir.

Cihaz Günlüğü (yalnızca cihaz düzeyinde)

Komut Günlüğü

Burada cihaz için hangi komutların verildiğini ve durumlarının ne olduğunu görebilirsiniz.



"System Automated" tarafından oluşturulan komutlar sistem tarafından otomatik olarak oluşturulur.

Olası komut durumları

Cihaz İtildi	Cihaza EMM sunucusuna geri bağlanmasını söylemek için push hizmetine (örn. APNS) bir push isteği gönderilmiştir.
Komut Oluşturuldu	Komut sistemde oluşturuldu.
Gönderilen Komut	Komut, sunucuya bağlandıktan sonra cihaza gönderildi.
Komut Yürütüldü	Komut başarıyla yürütüldü.
Komut Başarısız	Komut başarısız oldu. *
Komut Kısmen Başarısız	Cihazın işletim sistemine bağlı olarak bazı komutlar birlikte gruplandırılabilir. Bu komut grubunun bazı bölümleri başarısız olmuştur. *
Komut Yürütüldü, sonunda Başarısız Oldu	Komut uygulandı ama belki de uygulanmadı.
Komut Tekrar Gönderildi	Komut bir kullanıcı tarafından yeniden itildi.
Atılmış	Komut iptal edildi. Örneğin, başka bir komutun yerini aldığı için veya cihaz yeniden kaydedildiği ve eski komutlar kaldırıldığı için

*Mesajın arkasında bir ünlem işareti varsa, imlecinizi simgenin üzerine getirerek daha fazla bilgi alabilirsiniz.

Varlık Yönetimi (yalnızca cihaz düzeyinde)

Cihaz Bilgisi

Üretici firma	Cihaz üreticisi
Model	Cihaz modeli
Model Numarası	Model Numarası
İşletim Sistemi	İşletim sistemi
İşletim Sistemi Sürümü	İşletim sistemi sürümü
Seri Numarası	Seri Numarası
ExchangeID	ExchangeID
Toplam RAM	Toplam RAM
Ekran Çözünürlüğü	Ekran çözünürlüğü
Telefon Dili	Cihaz dili
Ürün Yazılımı Sürümü	Ürün yazılımı sürümü
DM İstemci Sürümü	Cihaz Yönetimi İstemcisi sürümü
Donanım Sürümü	Cihaz donanım sürümü
CPU Mimarisi	CPU Mimarisi (işlemci tipi)

Hücresel

SIM Taşıyıcı Ağ	Taşıyıcı ağ
Telefon Numarası	Telefon Numarası
Dolaşım Durumu	Dolaşım Durumu
IMEI	IMEI
IMSI	IMSI
Modem Ürün Yazılımı	Modem Ürün Yazılımı

Senkronizasyon Bilgisi

Anında DM Bağlantısı	Cihaz hemen AppTec ile bir bağlantı oluşturmalıdır
İlk Yeniden Deneme Süresi	Bu ilk bağlantı için ilk yeniden deneme süresi
Bağlantı Yeniden Denemeleri	Bağlantı Yöneticisi bağlantısının kesilmesinden veya WinInet düzeyinde bir hatadan sonra yeni bağlantı yeniden deneme sayısı
Maksimum Uyku Süresi	Paket gönderme hatasından sonra maksimum uyku süresi
İlk Senkronizasyon Yeniden Denemeleri	Kayıttan sonraki ilk aşama için zaman
İlk Yeniden Deneme Aralığı	Kayıttan sonraki ilk aşama için zaman
İkinci Senkronizasyon Yeniden Denemeleri	Kayıttan sonraki ikinci aşama için zaman
İkinci Yeniden Deneme Aralığı	Kayıttan sonraki ikinci aşama için zaman
Düzenli Senkronizasyon Yeniden Denemeleri	Kayıttan sonraki ek aşamalar için zaman
Düzenli Yeniden Deneme Aralığı	Kayıttan sonraki ek aşamalar için zaman

Güvenlik Yönetimi

Hırsızlığa Karşı Koruma (yalnızca cihaz düzeyinde)

GPS Bilgileri (yalnızca cihaz düzeyinde)

Burada mevcut/son cihaz konumunu belirleyebilirsiniz. Yerelleştirme bir veya iki parola ile korunabilir - Bkz: "Genel Ayarlar" > "Gizlilik" > "GPS Erişimi"

GPS Ayarları

GPS İzlemeyi Etkinleştirin	GPS bilgilerinin düzenli senkronizasyonunu etkinleştirin.
İzleme Aralığı	GPS bilgi senkronizasyon aralığını ayarlayın.

Güvenlik Yapılandırması

Şifre

Minimum Parola Uzunluğu	Minimum parola uzunluğu	
Şifre Oluşturma	Parolanın içermesi gereken belirli karakter sayısını belirtir Bunlar büyük harfler, küçük harfler, sayılar ve özel sembollerden oluşur	
Şifre Kalitesi	Burada şifre kalitesini ayarlayabilirsiniz	
	Alfanümerik	Sadece sayılar ve harfler
	Sayısal	Sadece sayılar
	Sayısal veya Alfanümerik	Sayılar veya sayılar ve harfler
Maksimum Hareketsizlik Süresi Kilidi	Cihazın kilitleneceği, cihazda kullanıcının hareketsiz kaldığı dakika sayısı. Kullanıcı bu süreden sonra cihaz şifresini girerek cihazın kilidini açmalıdır.	
Şifre Sona Erme	Yeni bir parola belirlenene kadar geçecek süreyi ayarlayın	
Parola Geçmişi Kısıtlaması	İzin verilmeyen önceden kullanılmış parola sayısı	
Maksimum Başarısız Parola Denemeleri	Cihazın tamamen silinmesinden önce parolanın yanlış girilme sayısı	

Antivirüs

Antivirüs ayarları - Tarama yapılandırmasını ayarla	
Tarama türü	Hızlı tarama mı yoksa tam tarama mı yapılacağını seçer
Tarama başlangıcını ayarla	Windows Defender'ın taramayı başlatacağı günün saatini seçer
Tarama frekansı	Windows Defender taramasının çalışması gereken günü seçer
İmza güncelleme sıklığı	İmzaları kontrol etmek için kullanılacak saat aralığını belirtir

Tarama için dosya türünü yapılandırma	
Arşiv dosyalarının taranmasına izin ver	Erişildiğinde arşivlerin (.zip gibi) taranmasına izin verin veya izin vermeyin.
Komut dosyalarının taranmasına izin ver	Windows Defender Komut Dosyası Tarama işlevine izin verir veya vermez.
E-postaların taranmasına izin ver	E-postaların taranmasına izin verin veya izin vermeyin.
Ağ dosyalarının taranmasına izin ver	Ağ dosyalarının taranmasına izin verin veya vermeyin.
Eşlenen ağ sürücülerinin tam taranmasına izin ver	Eşlenen ağ sürücülerinin taranmasına izin verin veya izin vermeyin (yalnızca tam tarama etkinleştirildiğinde etkinleştirilir).
Çift yönlü taramayı kontrol edin	Hangi dosya kümelerinin izlenmesi gerektiğini kontrol eder.
Çıkarılabilir sürücülerin tam taranmasına izin ver	Çıkarılabilir sürücülerin tam taranmasına izin verin veya izin vermeyin. Yalnızca tam tarama sırasında başlatılır.

Tarama dışında tutulacak dosya türleri	
Tarama için dosya türlerini yoksay	Bir dizi dosya türü uzantısı tanımlayın. Her bir alan için her bir dosya uzantısı.
Dizin yollarını yoksay	Taramamak için bir dizi dizin yolu tanımlayın. Her alan için bir yol. Örnekler: "C:\Example", "C:\Windows" veya "C:\Users".
Süreçleri taramadan hariç tutma	Belirli işlemler tarafından açılmış dosyaları Microsoft Defender Antivirus taramalarından hariç tutun. . Her alan için bir yol. Örnekler: "C:\myFile.exe", "C:\Windows\myProcess.exe", "C:\myScript.bat

Ekstra Ayarlar	
Gerçek Zamanlı İzlemeye İzin Ver	Windows Defender Gerçek Zamanlı İzleme işlevine izin verme veya vermeme
Davranış izlemeye izin ver	Windows Davranış İzleme işlevine izin verme veya vermeme
Bulut Korumasına İzin Ver	Windows Defender'ın bulduğu herhangi bir sorun hakkında Microsoft'a bilgi göndermesine izin verin veya izin vermeyin. Microsoft bu bilgileri analiz edecek, cihazı etkileyen sorun hakkında daha fazla bilgi edinecek ve gelişmiş çözümler sunacaktır
	Numune gönderme davranışı
Windows Defender IOAV korumasına izin ver	Windows Defender IOAV korumasına izin verme veya vermeme
Defenders "Erişim korumasında" kullanıcı arayüzüne erişime izin verin	
Ortalama CPU yük faktörü	Windows Defender taraması için ortalama CPU yük faktörünü temsil eder (yüzde olarak)

Kötü amaçlı yazılım işleme	
Düşük şiddette	Her önem düzeyi için cihazın kötü amaçlı yazılımları nasıl ele alacağını tanımlayabilirsiniz. Mevcut seçenekler şunlardır: • Temiz • Karantina • Kaldırmak • İzin ver • Kullanıcı tanımlı • Blok
Orta şiddette	
Yüksek ciddiyet	
Şiddet derecesi	
Temizlenmiş Kötü Amaçlı Yazılımın saklanması için günler	Karantina dosyalarının/öğelerinin sistemde saklanacağı gün cinsinden süre. Varsayılan değer 0'dır; bu değer öğeleri karantinada tutar ve otomatik olarak kaldırmaz. Maksimum değer 90'dır.

Güvenlik Merkezi

Windows Güvenlik Merkezi - Windows Güvenlik Ayarları	
Virüs ve tehdit koruması kullanıcı arayüzünü devre dışı bırakın	
Fidye Yazılımı Veri Kurtarma Arayüzünü Gizle	
Hesap koruma kullanıcı arayüzünü devre dışı bırak	
Güvenlik Duvarı ve Ağ koruması kullanıcı arayüzünü devre dışı bırakın	
Uygulama ve Tarayıcı kontrol kullanıcı arayüzünü devre dışı bırakın	
Exploit korumasında değişikliklere izin verme	Kullanıcının Exploit koruma ayarlarında değişiklik yapmasına izin verme
Cihaz güvenliği kullanıcı arayüzünü devre dışı bırak	
TPM sorun gidermeyi gizle	TPM sorun giderme ayarlarını gizle
TPM'yi Temizle düğmesini devre dışı bırak	
Cihaz performansını ve sağlık kullanıcı arayüzünü devre dışı bırakma	
Aile seçenekleri kullanıcı arayüzünü devre dışı bırak	

Tostları Özelleştirin	
Özelleştirilmiş destek bilgilerini etkinleştirin	Güvenlik merkezi uygulamasının sağ alt kısmında şirketiniz için özelleştirilmiş destek iletişim bilgilerini görüntülemeyi etkinleştirin.
E-Posta adresi	Şirketin e-posta adresini ayarlayın
Şirket adı	Şirket adını belirleyin
Şirket telefonu	Şirketin telefonunu ayarlayın
Yardım URL'si	Şirketin yardım URL'sini ayarlayın

Ekstra Ayarlar	
Bildirimleri devre dışı bırak	Windows Defender Güvenlik Merkezi Bildirimleri'nin görüntülenmesini devre dışı bırakın.
TPM ürün yazılımı güncelleme önerilerini gizle	Güvenlik açığı bulunan bir ürün yazılımı tespit edildiğinde TPM Ürün Yazılımını güncelleme önerisini gizleyin.
Şirket adını ve iletişim seçeneklerini görüntüleme	Şirketinizin adını ve iletişim seçeneklerini Windows Defender Güvenlik Merkezi'nde açılan bir iletişim kartında görüntüleyin.
Güvenli Önyüklemeyi Gizle	Güvenlik Önyükleme alanını gizle.
Güvenlik bildirim alanı kontrolünü gizle	Windows Güvenlik bildirim alanı denetimini gizle.

Güvenlik Duvarı Yapılandırması

Güvenlik duvarı yapılandırması - Genel ayarlar	
Kimlik doğrulama ayarını yoksay	Kümede belirtilen tüm kimlik doğrulama paketlerini desteklemiyorlarsa tüm kimlik doğrulama kümesini yoksay
Paket kuyruklama türü	IPsec tünel ağ geçidi senaryosu için alıcı taraftaki yazılım için ölçeklendirmenin hem şifreli alma hem de iletme yolunu temizleme için nasıl etkinleştirileceğini belirtir.
Durum bilgisi içeren FTP filtrelemeyi devre dışı bırak	Devre dışı bırakılırsa, ikincil bağlantılara izin vermek için durum bilgisi içeren Dosya Aktarım Protokolü (FTP) filtrelemesi gerçekleştirmez
Güvenlik birliği boşta kalma süresi	Bu alan, güvenlik ilişkisi boşta kalma süresini saniye cinsinden yapılandırır. Güvenlik ilişkilendirmeleri, belirtilen süre boyunca ağ trafiği görülmediğinde silinir.
Önceden paylaşılan anahtar kodlaması	Önceden paylaşılan anahtar kodlamasını ayarlama
IPSec İstisnaları	İnternet Protokolü özel durumlarını yapılandırma
Sertifika iptal listesi kontrolü	

Güvenlik Duvarı Profilleri (Etki Alanı Profili / Özel Profil / Genel Profil)	
Bu profil için Güvenlik Duvarını Etkinleştir	
Bildirimleri devre dışı bırak	Bir uygulamanın bir bağlantı noktasını dinlemesi engellendiğinde kullanıcıya bildirim gösterilmesini devre dışı bırakın.
Çok noktaya yayın yayınlarına tek noktaya yayın yanıtlarını engelleme	
Yetkili uygulama güvenlik duvarı kurallarını uygulayın	Zorlanmazsa, yerel depodaki yetkili uygulama güvenlik duvarı kuralları yok sayılır ve zorlanmaz
Genel bağlantı noktası güvenlik duvarı kurallarını uygulayın	Zorlanmazsa, yerel depodaki genel bağlantı noktası güvenlik duvarı kuralları yok sayılır ve zorlanmaz. Ayar yalnızca Grup İlkesi deposunda ayarlanmış veya numaralandırılmışsa ya da GroupPolicyRSoPStore'dan numaralandırılmışsa anlamlıdır
Güvenlik duvarı kurallarını uygulayın	Zorlanmazsa, yerel depodaki güvenlik duvarı kuralları yok sayılır ve uygulanmaz
Bağlantı güvenliği kurallarını uygulayın	Uygulanmazsa, yerel depodaki bağlantı güvenliği kuralları yok sayılır ve uygulanmaz
Varsayılan giden eylem	Güvenlik duvarının giden bağlantılarda varsayılan olarak gerçekleştirdiği eylem
Varsayılan gelen eylem	Güvenlik duvarının gelen bağlantılarda varsayılan olarak gerçekleştirdiği eylem
Gizli modu devre dışı bırak	Gizli mod, Windows Güvenlik Duvarı'nda kötü niyetli kullanıcıların ağ bilgisayarları ve çalıştırdıkları hizmetler hakkındaki bilgileri keşfetmesini önlemeye yardımcı olan bir mekanizmadır.
İstenmeyen trafiğe yanıt vermeyi engellemeyi devre dışı bırakma	Devre dışı bırakılırsa, güvenlik duvarının gizli mod kuralları, trafik IPsec ile güvence altına alınmışsa ana bilgisayarın istenmeyen ağ trafiğine yanıt vermesini engellememelidir

Güvenlik Duvarı Kuralları

Güvenlik Duvarı Kuralları	
İsim	Kuralın adı
Açıklama	Kuralın açıklaması
Eylem	Bu kuralın trafiği engelleyeceğini veya trafiğe izin vereceğini belirtin. Lütfen Engelle seçeneğinin MDM sunucusu ile Cihaz arasındaki trafiği de (yapılandırmanın geri kalanına bağlı olarak) engelleyebileceğini göz önünde bulundurun
Yön	
Kenar geçişini etkinleştir (Yalnızca **Yön gelen trafik** olarak ayarlandığında kullanılabilir)	Belirli gelen trafiğin Teredo tünelleme teknolojisini kullanarak NAT'lar ve diğer uç cihazlar boyunca tünellemesine izin verildiğini gösterir.

Programlar ve hizmetler	
Uygulamaları tanımlayın, aksi takdirde	Etkinleştirilmezse, tüm başvuruları dikkate alacaktır
Paket Aile Adı	Kuralın uygulanacağı Paket Aile Adı.
Uygulamanın dosya yolu	Kuralın uygulanacağı C:\Windows\System\Notepad.exe gibi tam uygulama
Tam Nitelikli İkili Ad	Kuralın uygulanacağı Tam Nitelikli İkili Ad. Bir FQBN aşağıdaki formda bir dizedir: {Yayıncı\Ürün\Dosya adı,Sürüm}
Hizmet Adı	Bir Hizmetin adını girin (örneğin "EventLog"). Powershell üzerinde "Get-Service" komutunu çalıştırarak Servis Adlarının bir listesini alabilirsiniz.

Protokoller ve bağlantı noktaları				
Protokol	Kural tarafından kullanılan protokol.			
	Mevcut değerler: - Herhangi bir - Özel - HOPORT - ICMPv4 - IGMP - TCP - UDP - IPv6 - IPv6-Route - IPv6-Frag - GRE - ICMPv6 - IPv6-NoNxt - IPv6-Opts - VRRP - PGM - L2TP	Özel olarak ayarlandığında	0 ile 255 arasında bir protokol numarası girin	Protokol numarası
		TCP veya UDP olarak ayarlandığında	Yerel portları belirtin, aksi takdirde tümü kullanılacaktır	Kuralın kullanacağı yerel portlar, aralık portlarına da izin verilir
			Yerel Liman	Tek bağlantı noktası veya bir dizi bağlantı noktası. Örneğin 100-120,200,300-320.
			Uzak bağlantı noktalarını belirtin, aksi takdirde tümü kullanılacaktır	Kuralın kullanacağı uzak portlar, aralık portlarına da izin verilir
			Uzak Bağlantı Noktası	Tek bağlantı noktası veya bir dizi bağlantı noktası. Örneğin 100-120,200,300-320.

Kapsam	
Yerel IP'leri belirtin, aksi takdirde herhangi bir IP	Yerel IP'ler kümesi, - ile ayrılmış bir IP aralığı da olabilir.
Yerel IP adresi	ile ayrılmış tek bir IP kümesi veya IP aralığı
Uzak IP'leri belirtin, aksi takdirde herhangi bir uzak IP	Bir uzak IP kümesi belirtin, "-" ile ayrılmış bir IP aralığı da olabilir.
Uzak IP adresi	Tek IP'ler veya bir IP aralığı belirtin
Jetonlar	Uzak Adresler ile birlikte ayarlanabilen belirteçler. Tokens Intranet, RmtIntranet ve Ply2Renders, Windows 10, sürüm 1809 ve sonraki sürümlerde desteklenmektedir.

Gelişmiş Ayarlar	
Profilleri belirtin, aksi takdirde hepsi kullanılacaktır	Devre dışı bırakılırsa tüm profiller kullanılır
Etki Alanı	Etki Alanı Profili
Özel	Özel Profil
Kamu	Genel Profil
Arayüzleri belirtin, aksi takdirde hepsi kullanılacaktır	Devre dışı bırakılırsa tüm arayüzler kullanılır
Yerel Alan Ağı	Yerel Alan Ağı arayüzü
Uzaktan Erişim	Uzaktan Erişim arayüzü
Kablosuz	Kablosuz arayüz

Yerel Müdürler	
Yetkili yerel kullanıcılar ekleme	Bu kuralı kullanacak yerel kullanıcıların bir listesini eklemeye izin ver
Yetkili kullanıcılar	Bu kural için yetkili yerel kullanıcıların listesi. Kullanıcı, Güvenlik Tanımlama Dili (SDDL) biçiminde olmalıdır, örneğin PC_NAME\USERNAME. Bu kuralı kullanmak için bir hizmet adı ayarlanmışsa bu alan doldurulmamalıdır

Kısıtlama Ayarları

Cihaz İşlevselliği

SD Karta İzin Ver	SD kart kullanımına izin verin
Kameraya İzin Ver	Kamera kullanımına izin verin
Konum Hizmetine İzin Ver	Cihaz konum hizmetine izin ver
Uygulama Yan Yüklemeye İzin Ver	Bilinmeyen kaynaklardan gelen uygulamaların yüklenmesine izin ver
Geliştirici Moduna İzin Ver	Geliştirici moduna izin verir
Hücresel Veri Dolaşımına İzin Ver	Hücresel veri dolaşımına izin ver
Cortana'ya izin ver	Sesli asistan Cortana'ya izin ver
Aramanın Konumu Kullanmasına İzin Ver	Aramanın konumu kullanmasına izin ver
Microsoft Dışı E-posta Hesabı Eklemeye İzin Ver	Kullanıcının MSA dışı e-posta hesapları eklemesine izin verilip verilmediğini belirtin.
Microsoft Hesap Bağlantısına İzin Ver	E-posta ile ilgili olmayan bağlantı kimlik doğrulaması ve hizmetleri için MSA hesabının kullanılmasına izin verilip verilmeyeceğini belirtin.
Ayarlarımı Senkronize Etmeye İzin Ver	Ayarların tüm cihaz boyunca senkronize edilmesini sağlar
Kurumsal Korumalı Alan Adları	";" ile ayrılmış kurumsal alan adlarını belirtir.
Kullanıcının Sistem Geri Yükleme'yi devre dışı bırakmasına izin ver	Kullanıcının Sistem Geri Yükleme'yi devre dışı bırakmasını sağlar. **UYARI!** Bu özellik yalnızca kurumsal şirket veya kuruluş tarafından sahip olunan veya sağlanan cihazlarda veya kullanıcının cihazın tamamen kurumsal şirket tarafından yönetilmesine izin verdiği kullanıcıya ait bir cihazda kullanılmalıdır. Bu ilke ayarını devre dışı bırakırsanız, Sistem Geri Yükleme kapatılır ve Sistem Geri Yükleme Sihirbazı'na erişilemez. Sistem Geri Yükleme'yi yapılandırma

	veya Sistem Koruması aracılığıyla bir geri yükleme noktası oluşturma seçeneği de devre dışı bırakılmıştır.
Kullanıcı Kaydının Silinmesine İzin Ver	Kullanıcının kurumsal parçayı cihazdan çıkarmasına ve böylece AppTec360 Sunucuları ile bağlantıyı kesmesine olanak tanır. Böyle bir durumda, cihazı yönetmek artık mümkün olmayacaktır **UYARI!** Bu özellik yalnızca kurumsal şirket veya kuruluş tarafından sahip olunan veya sağlanan cihazlarda veya kullanıcının cihazın tamamen kurumsal şirket tarafından yönetilmesine izin verdiği kullanıcıya ait bir cihazda kullanılmalıdır. Bu ilke ayarını devre dışı bırakırsanız, kullanıcılar MDM kayıtlarını kaldıramaz. Kullanıcının işyeri kontrol paneli aracılığıyla işyeri hesabını silmesine izin verilip verilmediğini belirtin. MDM sunucusu hesabı her zaman uzaktan silebilir.

BitLocker

BitLocker Yapılandırması

Genel Ayarlar	
Cihaz şifrelemesi gerektir	Windows sürümüne ve sistem yapılandırmasına bağlı olarak, kullanıcılardan cihaz şifrelemesini etkinleştirmeleri istenebilir: - Başka bir sağlayıcıdan şifrelemenin etkinleştirilmediğini doğrulamak için. - BitLocker Sürücü Şifrelemesini kapatmak ve ardından BitLocker'ı tekrar açmak için.
Şifreleme yöntemleri	
İşletim sistemi sürücüleri için şifreleme yöntemi	
Sabit veri sürücüleri için şifreleme yöntemi	
Çıkarılabilir veri sürücüleri için şifreleme yöntemi	
Üçüncü taraf disk şifrelemesiyle ilgili uyarıyı devre dışı bırakma	Cihazda kullanılan bir üçüncü taraf disk şifreleme hizmeti hakkındaki uyarı istemini devre dışı bırakın. Windows 10, sürüm 1803'ten itibaren bu ayar yalnızca Azure Active Directory'ye katılmış cihazlar için desteklenir.
Yönetici olmayan kullanıcı oturum açmışken şifrelemenin çalıştırılmasına izin ver	Yalnızca Azure Active Directory'ye katılmış cihazlar için desteklenir

AppTec360 Uzantıları	
Sessiz şifreleme	"Cihaz şifrelemesi gerektir" ile birlikte seçilirse, AppTec360 Yönetim Hizmeti cihaz sürücülerinin otomatik sessiz şifrelemesini çalıştıracaktır.
Kullanıcı kimlik bilgilerini otomatik olarak oluşturun	Şifrelenmiş işletim sistemi sürücüsü otomatik olarak oluşturulan kullanıcı kimlik bilgileriyle korunacaktır. Bir TPM mevcutsa TPM PIN kodu veya 6 haneli bir metin parolası. Oluşturulan kimlik bilgileri, verilen cihaz için kayıtlı e-posta adresine gönderilir. Bu seçenek kapatılırsa, sessiz şifreleme için mümkün olan tek koruma TPM kullanmaktır. Bu durumda, TPM'si olmayan cihazlar için sessiz şifreleme başarısız olacaktır.
Sabit sürücüleri şifreleyin	Mevcut tüm sabit veri sürücüleri de şifrelenecek ve işletim sistemi sürücüsünde saklanan bir anahtar kullanılarak "Otomatik Kilit Açma" ile korunacaktır.

İşletim Sistemi Sürücü Ayarları

Başlangıçta ek kimlik doğrulama gerektir	Bu ayar, BitLocker'ın bilgisayar her başlatıldığında bir kimlik doğrulaması gerektirip gerektirmediğini yapılandırmanıza olanak tanır. Bu ayar BitLocker kurulumu sırasında uygulanır. Bu ayarı etkinleştirirseniz, kullanıcılar BitLocker kurulum sihirbazında gelişmiş başlatma seçeneklerini yapılandırabilir.
Uyumlu bir TPM olmadan BitLocker'ı engelleme	
Yalnızca TPM	
TPM ve PIN	
TPM ve anahtar	
TPM, anahtar ve PIN	PIN ve USB flash sürücü (anahtar) kullanımını zorunlu kılmak istiyorsanız, kullanıcı BitLocker Sürücü Şifreleme kurulum sihirbazı yerine "manage-bde" komut satırı aracını kullanarak BitLocker'ı kurmalıdır.

Minimum PIN uzunluğu gerektir	
	Minimum karakterler

Önyükleme öncesi kurtarma mesajını ve URL'sini yapılandırma	Kurtarma mesajının tamamını yapılandırın veya işletim sistemi sürücüsü kilitlendiğinde önyükleme öncesi anahtar kurtarma ekranında görüntülenen mevcut URL'yi değiştirin. Not: Tüm karakterler ve diller önyüklemede desteklenmez. Kullandığınız karakterlerin önyükleme öncesi kurtarma ekranında doğru göründüğünü test etmeniz önemle tavsiye edilir.
	Önyükleme öncesi kurtarma mesajı seçeneği
	Özel kurtarma mesajı
	Özel kurtarma URL'si

İşletim sistemi sürücüsü kurtarma seçenekleri		Bu ayar, BitLocker korumalı işletim sistemi sürücülerinin gerekli kimlik bilgileri olmadığında nasıl kurtarılacağını kontrol etmenizi sağlar. Bu ayar BitLocker kurulumu sırasında uygulanır. Varsayılan olarak Sertifika tabanlı bir veri kurtarma aracısına izin verilir, kurtarma seçenekleri kurtarma parolası ve kurtarma anahtarı dahil olmak üzere kullanıcı tarafından belirlenebilir ve kurtarma bilgileri AD DS'ye yedeklenmez.
	Blok Sertifika tabanlı veri kurtarma aracısı	BitLocker korumalı işletim sistemi sürücüleriyle bir veri kurtarma aracısının kullanılıp kullanılamayacağını belirtin. Bir veri kurtarma aracısı kullanılmadan önce, Grup İlkesi Yönetim Konsolu veya Yerel Grup İlkesi Düzenleyicisi'ndeki Ortak Anahtar İlkeleri öğesinden eklenmelidir. Veri kurtarma aracıları ekleme hakkında daha fazla bilgi için Microsoft TechNet'teki BitLocker Sürücü Şifreleme Dağıtım Kılavuzu'na başvurun.
	BitLocker kurtarma parolası ayarları	
	BitLocker kurtarma anahtarı ayarları	
	BitLocker kurtarma bilgilerini Active Directory Etki Alanı Hizmetleri'ne kaydetme	
	AD DS BitLocker kurtarma depolama yapılandırması	Anahtar paketinin saklanması, fiziksel olarak bozulmuş bir sürücüden verilerin kurtarılmasını destekler.
	Kurtarma verilerinin AD DS'de depolanmasını gerektirme	Bilgisayar etki alanına bağlı olmadığı sürece kullanıcıların BitLocker'ı etkinleştirmesini engelleyin ve

Sabit Sürücü Ayarları	
Sabit sürücü kurtarma seçenekleri	Bu ayar, BitLocker korumalı sabit sürücülerin gerekli kimlik bilgileri olmadığında nasıl kurtarılacağını kontrol etmenizi sağlar. Bu ayar BitLocker kurulumu sırasında uygulanır. Varsayılan olarak Sertifika tabanlı bir veri kurtarma aracısına izin verilir, kurtarma seçenekleri kurtarma parolası ve kurtarma anahtarı dahil olmak üzere kullanıcı tarafından belirlenebilir ve kurtarma bilgileri AD DS'ye yedeklenmez.
Blok Sertifika tabanlı veri kurtarma aracısı	
BitLocker kurtarma parolası ayarları	
BitLocker kurtarma anahtarı ayarları	
BitLocker kurtarma bilgilerini Active Directory Etki Alanı Hizmetleri'ne kaydetme	
AD DS BitLocker kurtarma depolama yapılandırması	Anahtar paketinin saklanması, fiziksel olarak bozulmuş bir sürücüden verilerin kurtarılmasını destekler.
Kurtarma verilerinin AD DS'de depolanmasını gerektirme	Bilgisayar etki alanına bağlı olmadığı ve BitLocker kurtarma bilgilerinin AD DS'ye yedeklenmesi başarılı olmadığı sürece kullanıcıların BitLocker'ı etkinleştirmesini engelleyin. Not: Kurtarma parolası otomatik olarak oluşturulur.
Korumasız sabit sürücülere yazma erişimini reddetme	

Çıkarılabilir Sürücü Ayarları	
Korumasız çıkarılabilir sürücülere yazma erişimini reddetme	Bitlocker tarafından korunmayan çıkarılabilir veri sürücülerine yazma erişimini reddedin. Not: Grup ilkesinde "Çıkarılabilir Diskler: Yazma erişimini reddet" grup ilkesinde etkinleştirilmişse, bu ilke ayarı yok sayılır.
Başka bir kuruluşta yapılandırılmış cihazlara yazma erişimini reddetme	Yalnızca kimlik alanları bilgisayarın kimlik alanlarıyla eşleşen sürücülere yazma erişimi verilecektir. Bu alanlar "Kuruluşunuz için benzersiz tanımlayıcılar sağlayın" grup ilkesi ayarı tarafından tanımlanır.

BitLocker Durumu

Burada BitLocker şifreli sürücülerin mevcut durumunu görebilirsiniz

C [OS Drive]
Şifreleme Durumu
Şifrelenmiş (%)
Koruma Durumu
Şifreleme Yöntemi
Anahtar Koruyucular
Kurtarma Şifresi

"Kurtarma parolasını döndür" düğmesine tıklayarak BitLocker kurtarma parolasını döndürebilirsiniz.

Sertifika Yönetimi

Sertifika Listesi

Burada, görüntülenen cihazda yüklü olan sertifikaların bir listesi bulunmaktadır.

Sertifika Yapılandırması

Burada sertifikaları ve bunların cihaza nasıl yükleneceğini yapılandırabilirsiniz.

Güvenilir sertifika	
Açıklama	Sertifika açıklaması
Kapsam	Sertifika dağıtım kapsamı: Mevcut Kullanıcı vs Cihaz
Sertifika deposu	"Güvenilmeyen Sertifikalar" yalnızca Windows 10, sürüm 1803'ten itibaren kullanılabilir
Sertifika dosyası	Bir PKCS#1 dosyası yükleyin

<table>
<tr><td colspan="4">Kimlik belgesi</td></tr>
<tr><td>Açıklama</td><td colspan="3">Sertifika açıklaması</td></tr>
<tr><td>Kapsam</td><td colspan="3">Sertifika dağıtım kapsamı: Mevcut Kullanıcı vs Cihaz</td></tr>
<tr><td rowspan="5">Anahtar konum</td><td colspan="3">Özel anahtarın yükleneceği Anahtar Depolama Sağlayıcısı.</td></tr>
<tr><td></td><td colspan="2">TPM. TPM yoksa başarısız</td></tr>
<tr><td colspan="3">TPM. TPM yoksa, Yazılım KSP'ye geri dönülür</td></tr>
<tr><td colspan="2">Yazılım Anahtarı Depolama Sağlayıcısı</td><td>Özel anahtarı dışa aktarılabilir olarak işaretleme</td></tr>
<tr><td rowspan="2">İşletmeler için Windows Hello</td><td>Konteyner adı</td><td>Windows Hello for Business (eski adıyla Microsoft Passport for Work) kapsayıcı adını belirtir.</td></tr>
<tr><td>PIN istemi metni</td><td>Sertifika kaydı sırasında Windows Hello for Business PIN isteminde gösterilecek özel metni belirtir.</td></tr>
<tr><td>Kimlik Bilgileri</td><td colspan="3">PKCS#12 Dosyası Yükleme</td></tr>
</table>

SCEP

Açıklama	SCEP Sunucusu açıklaması		
Dağıtım Kapsamı	Sertifika dağıtım kapsamı: Mevcut Cihaz vs Kullanıcı		
SCEP Sunucu URL'leri	SCEP aracılığıyla sertifika veren bir veya daha fazla sunucu		
Konu	Bir X.500 adının gösterimi. Örneğin "C=US, O=Microsoft Corporation, CN=foo, 1.2.5.3=bar"		
Konu alternatif isimleri	Tip	E-posta adresi	
		DNS	
		URI	
		Kullanıcı Asıl Adı (UPN)	
CA Parmak İzi	Sertifika Yetkilisi sertifikasının SHA1 parmak izi. E.g. 31:8F:1E:78:5C:D5:12:9F:7E:3B:AD:F3:1C:C0:19:03:96:43:A9:E5		
Geçerlilik süresi birimleri	Günler, Aylar veya Yıllar		
Geçerlilik süresi			
Meydan Okuma	Otomatik kayıt için önceden paylaşılan gizli bilgi olarak kullanılır		
Yeniden Denemeler	Sunucu bir BEKLEMEDE yanıtı gönderirse cihazın yeniden deneme sayısı. Varsayılan değer 5'tir. Maksimum değer 30'dur.		
Yeniden deneme gecikmesi	Yeniden denemeden önce beklenecek dakika sayısı. Varsayılan değer 5'tir. Minimum değer 1'dir.		
Anahtar boyutu	Bit cinsinden anahtar boyutu		
Hash algoritması	Karma algoritma ailesi		
Anahtar kullanımı	Anahtar kullanım uzantısı, sertifikada bulunan anahtarın amacını (örn. şifreleme, imza) tanımlar. "Dijital imza" veya "Anahtar şifreleme" seçeneklerinden en az birinin seçilmesi gerekir.		
Genişletilmiş anahtar	Genişletilmiş anahtar kullanımlarını belirtir.SCEP sunucu yapılandırmasına tabidir. İlgili OID'lerin listesini belirtin, örn. 1.3.6.1.5.5.7.3.2 (İstemci Kimlik Doğrulaması)		

kullanımı			
Anahtar konum	Özel anahtarın yükleneceği Anahtar Depolama Sağlayıcısı.		
		TPM. TPM yoksa başarısız	
	TPM. TPM yoksa, Yazılım KSP'ye geri dönülür		
	Yazılım Anahtarı Depolama Sağlayıcısı		
	İşletmeler için Windows Hello	Konteyner adı	Windows Hello for Business (eski adıyla Microsoft Passport for Work) kapsayıcı adını belirtir.
		PIN istemi metni	Sertifika kaydı sırasında Windows Hello for Business PIN isteminde gösterilecek özel metni belirtir.

Bağlantı Yönetimi

Wifi

Bu ayarda, dahili Erişim Noktalarına erişim için son kullanıcı cihazlarının ön yapılandırmasını gerçekleştirin

Hizmet Kümesi Tanımlayıcısı (SSID)	Bağlantının kurulacağı ağın SSID'si
Otomatik Katıl	Ağa otomatik katılımı etkinleştirin
Gizli Ağ	AP'nin SSID'yi yayınlamaması durumunda etkinleştirin

Güvenlik Türü

AP güvenlik türünü belirleme

WEP Açık Sistem	
Şifre	AP için şifre

WPA PSK	
Şifre	AP için şifre

WPA EAP	
Kimlik Doğrulama Türü	Kimlik doğrulama türü, yalnızca "PEAP-MSCAHPv2" ile mümkündür
Hızlı Yeniden Bağlanma	Cihazlar, tekrar kimlik doğrulaması yapmak zorunda kalmadan Erişim Noktaları arasında geçiş yapabilir
Misafir Erişimi	Kullanıcının bir hesabı yoktur ve bu nedenle misafir olarak kaydolmalıdır
Karantina Kontrolleri	İstemci NAP (Ağ Erişim Koruması) Kontrolleri gerçekleştirmeli ve sonuçları sistemle paylaşmalıdır, sistem daha sonra istemcinin bağlanıp bağlanamayacağına karar verir
Kripto Bağlama Gerektir	Kimlik doğrulama yalnızca Crypto Binding aracılığıyla mümkündür
Sunucu Doğrulama	İstemci, sunucu sertifikasının geçerli olup olmadığını kontrol eder. Bu durumda, bir bağlantı kurulacaktır
Sertifikalar için İstem	Kullanıcının güvenilir olmayan sertifikaları kabul etmesine izin verir
Sunucu Adları	Ağ kimlik doğrulaması ve yetkilendirmesi sunan RADIUS-Sunucusunun adını görüntüleme seçeneği sunar

WPA2-PSK	
Şifre	AP şifresi

WPA2 EAP	
Kimlik Doğrulama Türü	Kimlik Doğrulama Türü, yalnızca "PEAP-MSCAHPv2" ile mümkündür
Hızlı Yeniden Bağlanma	
Misafir Erişimi	
Karantina Kontrolleri	Ağ erişim korumasını etkinleştirir NAP
Kripto Bağlama Gerektir	Kimlik doğrulama yalnızca Crypto Binding aracılığıyla mümkündür
Sunucu Doğrulama	
Sertifikalar için İstem	Doğrulanmış bir sunucu sertifikası, adı veya Kök sertifika kimlik doğrulaması (CA) ister
Sunucu Adları	Cihazlar tarafından güvenilmesi gereken sunucuların listelenmesi
Hiçbiri	Yerleşik güvenlik yok
Proxy Sunucusu Kullan	Proxy sunucu kullanımı
Sunucu Adresi	Proxy sunucu adresi
Sunucu Bağlantı Noktası	Proxy Sunucusunun Sunucu Bağlantı Noktası

Proxy Sunucusu Kullan

Proxy sunucu kullanımını etkinleştirin.

Sunucu Adresi	Bu ağ tarafından kullanılan proxy sunucu adresi.
Sunucu Bağlantı Noktası	Bu ağ tarafından kullanılan proxy sunucu bağlantı noktası.

Wifi Kısıtlamaları

Burada çeşitli Wifi kısıtlamaları tanımlayabilirsiniz.

WiFi'a İzin Ver	WiFi'a izin ver/reddet
İnternet Paylaşımına İzin Ver	Hotspot kullanımına izin ver
WiFi Sense Etkin Noktalarına Otomatik Bağlanmaya İzin Ver	WiFi Sense Etkin Noktalarına Otomatik Bağlanmaya İzin Ver
Manuel WiFi Yapılandırmasına İzin Ver	Kullanıcının AppTec tarafından tanımlanmamış WiFi ağlarına bağlanmasına izin verin
WLAN Tarama Frekansı	WLAN-Tarama aralığını belirler. Burada, daha yüksek bir değer WIFI ağlarını tanıma yeteneğini artırır.

VPN

VPN bağlantılarını yapılandırmak için burada uygun ayarları yapın

Bağlantı Adı	Belirtilen bağlantı adı		
VPN türü	Belirli Uygulamaların trafiğini güvence altına almak için Uygulama Başına VPN bağlantısı kullanılır.		
	VPN	Her Zaman Açık	Bu, oturum açma sırasında VPN'i otomatik olarak bağlayacak ve kullanıcı manuel olarak bağlantıyı kesene kadar bağlı kalacaktır.
	Uygulama Başına VPN	VPN Uygulamaları	Bu VPN Bağlantısını kullanan Uygulamaları Tanımlama
		Uygulama Başına Kilitleme	Uygulama Başına Kilitleme, seçilen uygulamaların yalnızca bu VPN bağlantısı üzerinden bağlantıya sahip olmasını sağlar. Bu özellik Windows Defender Güvenlik Duvarı'na bağlıdır.
	WIP profili	Bu bağlantı için WIP alanı	Bu VPN profilini bir Windows Bilgi Koruması (WIP) ilkesine bağlamak için gerekli olan Kurumsal Kimlik

Bağlantı türü

AppTec360 VPN	
"AppTec360 VPN" için uygulama yan yüklemesine izin verilmesi gerekir. Lütfen "Güvenlik Yönetimi" → "Kısıtlama Ayarları" → "Cihaz İşlevselliği" bölümünden "Uygulama Yan Yüklemeye İzin Ver" seçeneğini etkinleştirin.	
Ağ Geçidi Yapılandırması	VPN bağlantısını kara listeye alarak yapılandırmak için lütfen belirli bir DNS sunucusuna sahip bir VPN yapılandırması seçin. Bir VPN yapılandırmasını "Genel Ayarlar" → "Universal Gateway" → "VPN Ayarları" altında kurabilirsiniz.

IKEv2		
Sunucular	VPN sunucularının listesi	
Cihaz Tüneli	Kullanıcı oturum açmadan önce bağlantıyı etkinleştirin.	
Kimlik doğrulama yöntemi	EAP	EAP XML
	Makine Sertifikaları	
Şifreleme algoritması		
Bütünlük kontrol algoritması		
Diffie-Hellman grubu		
Şifre dönüştürme algoritması		
Kimlik doğrulama dönüşüm algoritması		
Mükemmel ileri gizlilik (PFS) grubu		

PPTP		
Sunucular	VPN sunucularının listesi	
Kimlik doğrulama yöntemi	EAP	EAP XML

L2TP		
Sunucular	VPN sunucularının listesi	
Kimlik doğrulama yöntemi	EAP	EAP XML
Şifreleme algoritması		
Bütünlük kontrol algoritması		
Diffie-Hellman grubu		
Şifre dönüştürme algoritması		
Kimlik doğrulama dönüşüm algoritması		
Mükemmel ileri gizlilik (PFS) grubu		

Otomatik		
Sunucular	VPN sunucularının listesi	
Kimlik doğrulama yöntemi	EAP	EAP XML

Genel VPN Yapılandırmaları

Her oturum açmada kimlik bilgilerini hatırlayın	
IP adreslerini dahili DNS'e kaydetme	
Ağ trafiği filtreleme kuralları	VPN bağlantısını tanımlanan kurallar kümesiyle sınırlayın.
DNS sonek arama listesi	Kısa adları yönlendirmek için DNS arama listesine eklenecek DNS sonekleri.
Ad Çözümleme İlkesi Tablosu (NRPT) kuralları	Ad Çözümleme İlkesi tablosu (NRPT) kuralları, VPN'e bağlanıldığında DNS'in adları nasıl çözümleyeceğini tanımlar.
Güvenilir ağ algılama	Güvenilen ağı tanımlamak için DNS soneklerinin listesi.
Bölünmüş tünelleme	Bölünmüş tünelleme, trafiğin ağ yığını tarafından belirlenen herhangi bir arayüz üzerinden gidebileceği anlamına gelir.
Bölünmüş tünelleme rotaları	VPN arabirimi için yönlendirme tablosuna eklenecek yolların listesi.
Proxy kurulumu	Bu ağ ile kullanılan Proxy'yi yapılandırır
Proxy Adresi	Tam nitelikli ana bilgisayar adı veya IP adresi olarak proxy sunucu adresi.
Liman	Proxy sunucu bağlantı noktası.
Proxy Otomatik Yapılandırma URL'si	Proxy ayarlarını otomatik olarak almak için URL.

VPN Kısıtlamaları

Burada çeşitli VPN kısıtlamaları tanımlayabilirsiniz.

VPN Ayarlarına İzin Ver	Bu kılavuz, kullanıcının VPN ayarlarını devre dışı bırakmasına ve değiştirmesine izin verir/yasaklar
Hücresel Üzerinden VPN'e İzin Ver	Cihaz mobil veri kullanıyorsa, cihazın VPN bağlantısı kurmasına izin verir/vermez
Hücresel Üzerinden VPN Dolaşımına İzin Ver	Cihaz dolaşımdaysa, cihazın VPN bağlantısı kurmasına izin verir/engeller

Bluetooth

Burada Bluetooth'a izin verilip verilmeyeceğini belirleyebilirsiniz.

Bluetooth'a İzin Ver	Bluetooth'u etkinleştirme/devre dışı bırakma

PIM Yönetimi

Exchange Active Sync

Son kullanıcı cihazında ActiveSync hesabının kurulması

Hesap Adı	E-posta hesabı adı
Sunucu Ana Bilgisayar Adı	Sunucu adresi/FQDN
Alan Adı	Sunucu etki alanı
E-posta Adresi	E-posta adresi
Kullanıcı Adı	Kullanıcı adı
Kullanıcı Şifresi	İsteğe bağlı olarak, burada kullanıcıya zaten bir parola ekleyebilirsiniz
SSL kullanın	SSL bağlantısı kullan
Senkronizasyon Aralığı	Burada senkronizasyon aralığı belirlenebilir Manuel senkronizasyon = Kullanıcı e-postalarını indirmeli ve manuel senkronizasyon gerçekleştirmelidir
Posta Yaşı Filtresi	E-postalar senkronize edilene kadar geçmesi gereken süre Filtre yok = sınırsız
Günlük Seviyesi	ActiveSync trafiği için günlük tutma seviyelerinin oluşturulması
E-posta Senkronizasyonu	Etkinleştirildi = e-postalar senkronize edildi
Kişileri Senkronize Et	Etkinleştirildi = kişiler senkronize edildi
Takvimi Senkronize Et	Etkinleştirildi = takvim senkronize edildi
Görevleri Senkronize Et	Etkinleştirildi = görevler senkronize edildi

e-Posta

Son kullanıcı cihazında POP3/IMAP4 hesaplarının oluşturulması.

Hesap Açıklaması	E-posta hesabı adı
Gönderen Adı	Görüntülenen gönderen adı
Alan Adı	E-posta hesabı için alan adı
E-posta Adresi	Kullanıcı e-posta adresi
Kullanıcı Adı	Kullanıcı adı
Kullanıcı Şifresi	İsteğe bağlı olarak, burada kullanıcıya zaten bir parola ekleyebilirsiniz
Alternatif Giden Sunucu Kimlik Bilgileri	Giden sunucu için başka kimlik bilgileri gerekiyorsa burada tanımlanabilir
Giden Alan Adı	Giden alan adı
Giden Sunucu Kullanıcı Adı	Giden sunucu kullanıcı adı
Giden Sunucu Parolası	Giden sunucu parolası
E-posta Protokolü	POP3 veya IMAP4, protokol olarak kullanılabilir
Gelen Posta Sunucusu Ana Bilgisayar Adı	Gelen posta sunucusu ana bilgisayar adı
Gelen Postalar için SSL Kullanın	Gelen e-postalar için SSL kullanın
Giden Posta Sunucusu Ana Bilgisayar Adı	Giden posta sunucusu ana bilgisayar adı
Giden Postalar için SSL Kullanın	Giden e-postalar için SSL kullanın
Giden Sunucu Kimlik Doğrulaması	Giden sunucu kimlik doğrulaması gereklidir
Senkronizasyon Aralığı	Burada senkronizasyon aralığı belirlenebilir Manuel senkronizasyon = Kullanıcı e-postalarını indirmeli ve manuel senkronizasyon gerçekleştirmelidir
Posta Yaşı Filtresi	E-postalar senkronize edilene kadar geçmesi gereken süre Filtre yok = sınırsız

Uygulama Yönetimi

Kurumsal Uygulama Yöneticisi

Yüklü Uygulamalar

Burada, görüntülenen cihazda o anda yüklü olan uygulamaların bir listesi bulunmaktadır.

Zorunlu Uygulamalar

Burada, cihazda zorunlu olan uygulamaların bir listesini yapılandırabilirsiniz.

Bu liste, cihaz MDM'ye her bağlandığında kontrol edilecek ve uygulamanın kaldırılmış olmasına veya daha önce hiç yüklenmemiş olmasına bakılmaksızın, bu listedeki cihazda yüklü olmayan tüm uygulamaları yükleyecektir.

Windows 10 Şirket İçi Uygulamaları yükleyebilir ve ardından bu listeye ekleyebilir veya "Genel Ayarlar" > "Uygulama Yönetimi" > "Microsoft Office" bölümünde önceden yapılandırılması gereken Microsoft Office yapılandırmalarını ekleyebilirsiniz.

Sistem Uygulama Kısıtlamaları

Gelen Kutusu Uygulamaları
Alarmlara ve Saate İzin Ver
Hesaplayıcıya İzin Ver
Kameraya İzin Ver
İletişim Desteğine İzin Ver
Cortana'ya izin ver
Dosya Gezgini'ne İzin Ver
Başlamanıza İzin Verin
Allow Groove Music
Haritalara İzin Ver
Mesajlaşmaya İzin Ver
Microsoft Edge'e izin ver
Filmlere ve TV'ye İzin Ver
Paraya İzin Ver
Haberlere İzin Verin
OneDrive'a izin ver
OneNote'a İzin Ver
Outlook Takvim ve Posta'ya İzin Ver
İnsanlara İzin Verin
Telefona İzin Ver
Fotoğraflara İzin Ver
Powerpoint'e İzin Ver
Ayarlara İzin Ver
Skype'a izin ver
Spora İzin Ver
Mağazaya İzin Ver
Ses Kaydediciye İzin Ver
Cüzdana İzin Ver
Hava Durumuna İzin Ver

Windows Geri Bildirim Merkezi'ne İzin Ver
Word'e İzin Ver
Xbox'a izin ver

Sayfaları Ayarlama
Hesaplara İzin Ver İşyeri
Gelişmiş Bilgilere İzin Ver
Uygulamalar Köşesine İzin Ver
Engellemeye ve Filtrelemeye İzin Ver
Renk Profiline İzin Ver
Sürüş Moduna İzin Ver
E-posta ve Hesaplara İzin Ver
Ekolayzıra İzin Ver
Klavyeye İzin Ver
Gezinti Çubuğuna İzin Ver
Ağ Uçak Moduna İzin Ver
Ağ İnternet Paylaşımına İzin Ver
Ağ Hizmetlerine İzin Ver
Ağ Wi-Fi'sine İzin Ver
PC Sistem Bluetooth'una İzin Ver
Cihazınızı Değerlendirmeye İzin Verin
Güncellemeyi Geri Yüklemeye İzin Ver
Paylaşıma İzin Ver
Başlatmaya İzin Ver
Zaman Dilimine İzin Ver
Zaman Bölgesine İzin Ver
Windows Varsayılan Kilit Ekranına İzin Ver
İş veya Okul Hesabına İzin Ver

Kara ve Beyaz Liste

"Kara ve Beyaz Liste" altında, "Beyaz Liste" Modu ile "Kara Liste" Modu arasında seçim yapabilirsiniz.

Beyaz Liste	Yalnızca listeye eklenen uygulamalar ve hizmetler son kullanıcı cihazına yüklenebilir. Bunlar son kullanıcı cihazına önceden yüklenmişse, kullanıcının bunları çalıştırabilmesi için etkinleştirilecek ve ayarlanacaktır.
	Listeye eklenmeyen diğer tüm uygulamalar son kullanıcı cihazına yüklenemez. Bunlar son kullanıcı cihazına önceden yüklenmişse, devre dışı bırakılacak ve kullanıcının bunları çalıştıramayacağı şekilde ayarlanacaktır.
Kara Liste	Listeye eklenen uygulamalar ve hizmetler son kullanıcı cihazına yüklenemez. Bunlar son kullanıcı cihazına önceden yüklenmişse, devre dışı bırakılacak ve kullanıcının bunları çalıştıramayacağı şekilde ayarlanacaktır.
	Listeye eklenmeyen diğer tüm uygulamalar son kullanıcı cihazına yüklenebilir. Bunlar son kullanıcı cihazına önceden yüklenmişse, kullanıcının bunları çalıştırabilmesi için etkinleştirilecek ve ayarlanacaktır.

ile o anda kullanılanlar listesine ek uygulamalar veya hizmetler ekleyebilirsiniz.

ile o anda etkin olmayan listeye ek uygulamalar veya hizmetler ekleyebilirsiniz.

"Windows App Store "dan bir uygulama ekleyebilir ya da kara veya beyaz listeye eklemek için doğrudan bir "Uygulama Tanımlayıcısı" girebilirsiniz.

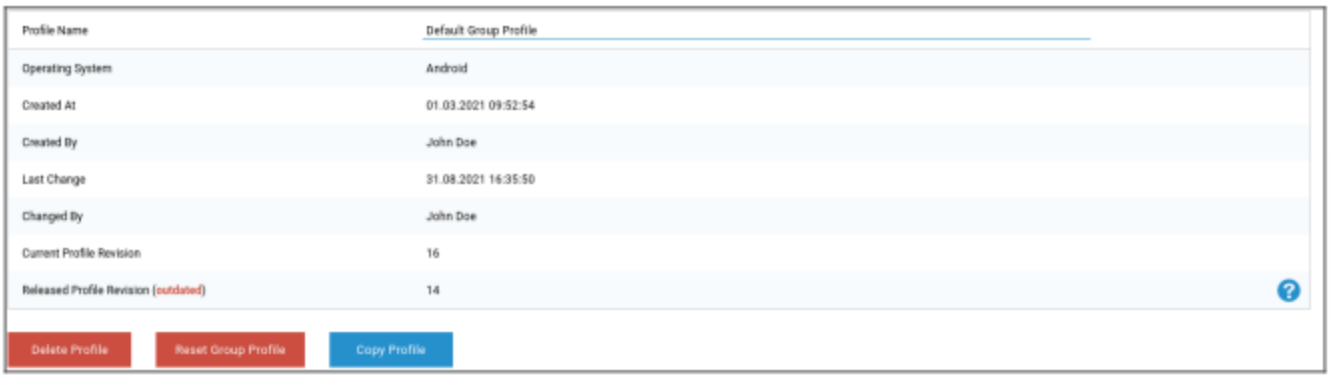
MacOS Yapılandırması

Bir profil veya cihaz seçmiş olmanıza bağlı olarak, ekran ve alt noktaları farklıdır - lütfen buna dikkat edin!

Genel

Grup profiline genel bakış (yalnızca grup düzeyinde)

Bir grup profilini açtığınızda, profile hızlı bir genel bakış elde edersiniz.



Profil Adı	Profilin adı (burada değiştirilebilir)
İşletim Sistemi	Profilin ait olduğu İşletim Sistemi
Şu Adreste Oluşturuldu	Yaratılış zamanı
Tarafından Oluşturuldu	Profilin yaratıcısı
Son Değişiklik	Profilde yapılan son değişikliğin zamanı
Tarafından Değiştirildi	Son değişiklikleri yapan hesap
Güncel Profil Revizyonu	Kayıtlı profil durumunun revizyonu
Profil Revizyonu Yayınlandı	Atanmış profil revizyonu ("Şimdi ata"). Etiket metnin arkasında "(eski)" ibaresini gösteriyorsa, bu profili kaydettiğiniz ancak henüz atamadığınız anlamına gelir, bu nedenle cihazlar hala eski sürümü alacaktır.

Cihaza Genel Bakış (yalnızca cihaz düzeyinde)

Cihazın özetlenmiş genel görünümü.

Cihaz Adı	Cihaz adı
Model	Model
İşletim Sistemi	İşletim Sistemi
Seri Numarası	Cihazın seri numarası
Cihaz Sahipliği	Yapılandırılmış Sahiplik Türü
Cihaz Tipi	Cihazın Türü
Uyumlu	Cihazın uyumlu olup olmadığını gösterir
IP Adresi	Cihazın sunucuya bağlandığı IP Adresi
Son Görülme	Cihazdan yapılan son bağlantının zamanı
Son İtiş	Cihaza gönderilen son itmenin zamanı
Görevlendirme	Burada cihazı başka bir kullanıcıya veya gruba taşıyabilirsiniz

Konfigürasyon Revizyonu (sadece cihaz seviyesinde)

Burada cihaza hangi grup profilinin atandığına dair bir genel bakış elde edersiniz.

Grup profiline tıklarsanız, profile doğrudan erişirsiniz ve ayarları gerçekleştirebilirsiniz.

Sembol ile, atanan uygulamaları grup profilinin ayarlarına geri döndürebilirsiniz.

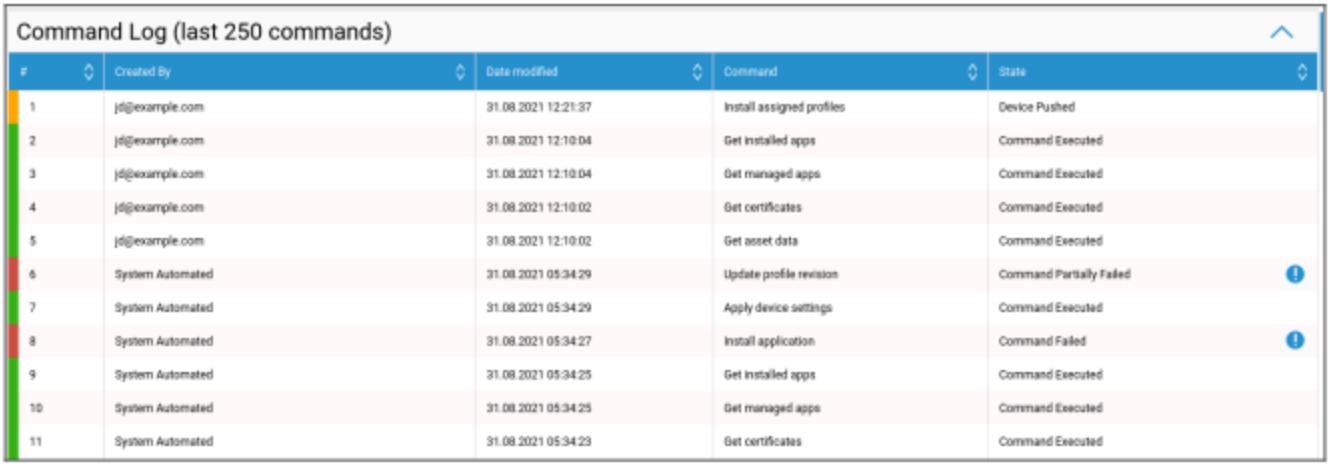
Sembol ile cihaz profilini hiçbir ayara sahip olmayacak şekilde sıfırlayabilirsiniz.

"Newer Revision available" grup profilinin değiştirildiğini ve kaydedildiğini ancak atanmadığını gösterir. Değişiklikleri cihazlara uygulamak için grup profilinin grup düzeyinde "Şimdi ata" ile atanması gerekir.

Cihaz Günlüğü (yalnızca cihaz düzeyinde)

Komut Günlüğü

Burada cihaz için hangi komutların verildiğini ve durumlarının ne olduğunu görebilirsiniz.



"System Automated" tarafından oluşturulan komutlar sistem tarafından otomatik olarak oluşturulur.

Olası komut durumları

Cihaz İtildi	Cihaza EMM sunucusuna geri bağlanmasını söylemek için push hizmetine (örn. APNS) bir push isteği gönderilmiştir.
Komut Oluşturuldu	Komut sistemde oluşturuldu.
Gönderilen Komut	Komut, sunucuya bağlandıktan sonra cihaza gönderildi.
Komut Yürütüldü	Komut başarıyla yürütüldü.
Komut Başarısız	Komut başarısız oldu. *
Komut Kısmen Başarısız	Cihazın işletim sistemine bağlı olarak bazı komutlar birlikte gruplandırılabilir. Bu komut grubunun bazı bölümleri başarısız olmuştur. *
Komut Yürütüldü, sonunda Başarısız Oldu	Komut uygulandı ama belki de uygulanmadı.
Komut Tekrar Gönderildi	Komut bir kullanıcı tarafından yeniden itildi.
Atılmış	Komut iptal edildi. Örneğin, başka bir komutun yerini aldığı için veya cihaz yeniden kaydedildiği ve eski komutlar kaldırıldığı için

*Mesajın arkasında bir ünlem işareti varsa, imlecinizi simgenin üzerine getirerek daha fazla bilgi alabilirsiniz.

Varlık Yönetimi (yalnızca cihaz düzeyinde)

Cihaz Bilgisi

Model Numarası	Model Numarası
Ana bilgisayar adı	Ana bilgisayar adı
Yerel Ana Bilgisayar Adı	Yerel Ana Bilgisayar Adı
İşletim Sistemi	İşletim sistemi
İşletim Sistemi Sürümü	İşletim sistemi sürümü
UDID	UDID
Boş / Toplam Bellek	Boş / Toplam Bellek

WiFi

IP Adresi	IP Adresi
WiFi MAC	WiFi MAC

Hücresel

Telefon Numarası	Telefon Numarası
Dolaşım Durumu	Dolaşım Durumu
Dolaşım (Ses / Veri)	Dolaşım (Ses / Veri)
IP Adresi	IP Adresi
Operatör/Taşıyıcı	Operatör/Taşıyıcı
SIM Taşıyıcı Ağ	Taşıyıcı ağ
Taşıyıcı Versiyonu	Taşıyıcı Versiyonu
ICCID	ICCID
Mevcut MCC/MNC	Mevcut MCC/MNC
SIM MCC/MNC	SIM MCC/MNC

Bluetooth

Bluetooth MAC	Bluetooth MAC

Güncelleme Yönetimi (yalnızca cihaz düzeyinde)

Güncelleme Bilgileri

Bu sekme, cihazdaki sistem güncelleme ayarları hakkında bilgi gösterir.

Otomatik kontrol etkin	Sistem güncellemeyi otomatik olarak kontrol ediyorsa.
Otomatik Uygulama Güncellemesi etkin	Sistem uygulama güncellemelerini otomatik olarak yükleyecekse.
Otomatik İşletim Sistemi Güncellemeleri etkin	Sistem işletim sistemi güncellemelerini otomatik olarak yükleyecekse.
Otomatik Güvenlik Güncellemeleri etkin	Sistem güvenlik güncellemelerini otomatik olarak yükleyecekse.
Uygulama Güncelleme Arka Plan-İndirme etkin	Sistem uygulama güncellemelerini arka planda indirecekse.
Katalog URL'si	İstemcinin kullandığı yazılım güncelleme kataloğunun URL'si.
Varsayılan katalog	"Evet" ise, Katalog varsayılan katalogdur.
Periyodik kontrol gerçekleştirin	"Evet" ise, yeni bir tarama başlatın.
Önceki tarama tarihi	Son yazılım güncelleme taramasının tarihi.
Önceki tarama sonucu	Son yazılım güncelleme taramasının sonuç kodu.

Güvenlik Yönetimi

Hırsızlığa Karşı

Sil ve Kilitle

Tam Silme	Cihazı fabrika ayarlarına sıfırlamak için bir komut gönderin
Kurumsal Silme	MDM'yi cihazdan kaldırın ve tüm MDM Verilerini (ör. Hesaplar, Uygulamalar) kaldırın
Kilit Ekranı	Cihazın kilit ekranına dönmesini sağlayın

Güvenlik Yapılandırması

Şifre

Kod devre dışı bırakmaya izin verildi	Kullanıcının bir PIN ayarlamaya zorlanıp zorlanmayacağını belirler. Sadece bu değeri ayarlamak (ve diğerlerini ayarlamamak), kullanıcıyı bir uzunluk veya kalite dayatmadan bir parola girmeye zorlar.
Basit değere izin ver	Kullanıcının aynı, artan ve azalan sayı dizilerini kullanmasına izin verin (örn. 1234, 1111)
Alfanümerik değer gerektir	Parolalar en az bir harf içermelidir
Minimum şifre uzunluğu	Minimum parola uzunluğu
Minimum karmaşık karakter sayısı	Paroladaki minimum alfanümerik sembol sayısı
Maksimum şifre yaşı	Parolanın değiştirilmesi gereken gün sayısı
Maksimum Otomatik Kilit	Cihazın kilitleneceği maksimum süre
Cihaz kilidi için maksimum ödemesiz süre	Kilit açıldığında parola sorulmadan cihazın kilitlenebileceği süre
Maksimum parola yaşı (1-730 gün veya hiç)	Parolanın değiştirilmesi gereken günler
Parola geçmişi (1-50 parola veya hiçbiri)	Yeniden kullanımdan önce benzersiz şifre sayısı

Sertifika

PKCS#1	
Açıklama	Sertifika için bir Açıklama Girin
Kimlik Bilgileri	Bir pkcs1 Dosyası Yükleyin

PKCS#12	
Açıklama	Sertifika için bir Açıklama Girin
Kimlik Bilgileri	Bir pkcs12 Dosyası Yükleyin

Kısıtlama Ayarları

Cihaz İşlevselliği

Kameraya İzin Ver	Kamera kullanımına izin verin
Oyun Merkezine İzin Ver	Yanlış olduğunda, Game Center devre dışı bırakılır ve simgesi Ana ekrandan kaldırılır.
Çok oyunculu oyunlara izin ver	Yanlış olduğunda, çok oyunculu oyun oynamayı yasaklar.
Game Center arkadaş eklemeye izin ver	Yanlış olduğunda, Game Center'a arkadaş eklemeyi yasaklar.
iCloud Fotoğraf Arşivi'ne izin ver	Yanlış olarak ayarlanırsa iCloud Fotoğraf Arşivi devre dışı bırakılır. iCloud Fotoğraf Arşivi'nden aygıta tam olarak indirilmeyen tüm fotoğraflar yerel depolama alanından kaldırılacaktır.
Touch ID'ye İzin Ver	Yanlışsa, Touch ID'nin bir cihazın kilidini açmasını engeller.

iCloud

iCloud eşleştirme sırasında belirli işlevleri engelleme

Belge senkronizasyonuna izin ver	Belge senkronizasyonuna izin ver
iCloud Anahtar Zinciri Eşzamanlamasına İzin Ver	iCloud Anahtar Zinciri Eşzamanlamasına İzin Ver
iCloud Notlarına İzin Ver	Yanlış olduğunda, MacOS iCloud Notes hizmetlerini devre dışı bırakır
iCloud BTMM'ye izin ver	Yanlış olduğunda, MacOS Back to My Mac iCloud hizmetini devre dışı bırakır.
iCloud FMM'ye izin ver	Yanlış olduğunda, MacOS Mac'imi Bul iCloud hizmetini devre dışı bırakır.
iCloud Yer İmlerine İzin Ver	Yanlış olduğunda, MacOS iCloud Bookmark senkronizasyonuna izin vermez.
iCloud Mail'e İzin Ver	Yanlış olduğunda, MacOS Mail iCloud hizmetlerini devre dışı bırakır.
iCloud Takvim'e izin ver	Yanlış olduğunda, MacOS Cloud iCloud hizmetlerini devre dışı bırakır.

iCloud Anımsatıcılarına İzin Ver	Yanlış olduğunda, iCloud Anımsatıcı hizmetlerini devre dışı bırakır.
iCloud Adres Defterine İzin Ver	Yanlış olduğunda, MacOS iCloud Adres Defteri hizmetlerini devre dışı bırakır.

Medya Yönetimi

Oturumu Kapatırken Çıkar	Oturumu Kapatırken tüm çıkarılabilir medyayı çıkar
Ağa İzin Ver	Ağ medyası için erişime izin ver
Dahili Diske İzin Ver	Dahili disk için erişime izin ver.
Kimlik Doğrulama Gerektir	Bu ortamın kullanımı için Kimlik Doğrulama Gerektir
Sadece Okunur	Kullanıcı yalnızca medyadan veri okuyabilir
Harici Diske İzin Ver	Harici disk için erişime izin ver.
Kimlik Doğrulama Gerektir	Bu ortamın kullanımı için Kimlik Doğrulama Gerektir
Sadece Okunur	Kullanıcı yalnızca medyadan veri okuyabilir
Disk Görüntülerinin kullanımına izin ver	Görüntüler için erişime izin verin.
Kimlik Doğrulama Gerektir	Bu ortamın kullanımı için Kimlik Doğrulama Gerektir
Sadece Okunur	Kullanıcı yalnızca medyadan veri okuyabilir
DVD-RAM'lerin kullanımına izin ver	DVD-RAM diski için erişime izin ver.
Kimlik Doğrulama Gerektir	Bu ortamın kullanımı için Kimlik Doğrulama Gerektir
Sadece Okunur	Kullanıcı yalnızca medyadan veri okuyabilir
DVD kullanımına izin verin	DVD disk için erişime izin ver.
Kimlik Doğrulama Gerektir	Bu ortamın kullanımı için Kimlik Doğrulama Gerektir
CD'lerin kullanımına izin verin	CD disk için erişime izin ver.
Kimlik Doğrulama Gerektir	Bu ortamın kullanımı için Kimlik Doğrulama Gerektir

Bağlantı Yönetimi

Wi-Fi

Burada Wi-Fi bağlantıları ekleyebilir ve yapılandırabilirsiniz

Hizmet Kümesi Tanımlayıcısı (SSID)	Bağlantının kurulacağı ağın SSID'si
Otomatik Katıl	Ağ için otomatik katılımı etkinleştirin
Gizli Ağ	AP'nin SSID'yi yayınlamaması durumunda etkinleştir
Proxy Kurulumu	Her Erişim Noktası için bir Proxy Yapılandırılması
Hiçbiri	Proxy Sunucusu Kullanmayın
Manuel	Manuel bir Proxy oluşturun
Proxy Sunucu URL'si	Proxy Ayarlarına erişim için adres
Liman	Proxy için bağlantı noktası belirleme
Kimlik Doğrulama	Proxy'de kimlik doğrulama için kullanıcı adı
Şifre	Proxy'de kimlik doğrulama için şifre
Otomatik	Otomatik olarak bir Proxy oluşturun
Proxy Sunucu URL'si	Proxy ayarları dosyası için URL
Güvenlik Türü	AP için Güvenlik Türü Oluşturma
WEP	
Şifre	AP için şifre
WPA/WPA2	
Şifre	AP için şifre
WEP Kurumsal - WPA / WPA2 Kurumsal / Herhangi Bir İşletme	Tablo Hatasına bakınız: Referans kaynağı aşağıda bulunamadı
Hiçbiri	Hiçbir güvenlik oluşturmayın
MAC adresi rastgeleleştirmeyi devre dışı bırakma	Ağ ile ilişkiliyken söz konusu Wi-Fi ağı için MAC adresi rastgeleleştirmesini devre dışı bırakır. Bu aynı zamanda Ayarlar'da ağın gizlilik korumalarını azalttığını belirten bir gizlilik uyarısı gösterir.

Kurumsal Wi-Fi Yapılandırması

Not: Yalnızca "Güvenlik Türü" bir Kurumsal Tür olarak ayarlandığında kullanılabilir.

Protokoller	Hedef ağda desteklenen kimlik doğrulama protokolü
TLS	Kullanımı Etkinleştir / Devre Dışı Bırak
TTLS	Kullanımı Etkinleştir / Devre Dışı Bırak
İç Kimlik Doğrulamaları	Kullanılması gereken kimlik doğrulama protokolü: PAP, CHAP, MSCHAP, MSCHAPv2
LEAP	Kullanımı Etkinleştir / Devre Dışı Bırak
PEAP	Kullanımı Etkinleştir / Devre Dışı Bırak
EAP-FAST	Kullanımı Etkinleştir / Devre Dışı Bırak
EAP-SIM	Kullanımı Etkinleştir / Devre Dışı Bırak
PAC kullanın	PAC (Korumalı Erişim Kontrolü) Kullanımı
Provizyon PAC	Provision PAC Yapılandırması
Anonim Olarak PAC Sağlama	Anonim PAC Temini
Kimlik Doğrulama	
Kullanıcı Adı	Kimlik doğrulama kullanıcı adı
Kullanmayın Bağlantı Başına Şifre	Bağlantı Başına Parola kullanmayın
Şifre	Kullanılacak şifre
Kimlik Belgesi	Kimlik doğrulama sertifikası yükleme/seçme
Dış Kimlik	Dışarıdan görülebilen kimlik
Güven	
Güvenilir Sertifika 1	İlk güvenilir sertifikayı yükleme
Güvenilir Sertifika 2	İkinci güvenilir sertifikayı yükleme
Güvenilir Sertifika 3	Üçüncü güvenilir sertifikayı yükleme
Güvenilir Sunucu Sertifika İsimleri	Beklenen sunucu sertifikalarının adları (virgülle ayrılmış bir listede)

VPN

Seçilen Bağlantı Türüne bağlı olarak, farklı alanlar görünür olabilir.

Bağlantı Adı	VPN-Profilinin Adı
VPN Türü	
VPN	Tüm cihaz ağ trafiği bir VPN bağlantısı üzerinden yönlendirilecektir.
Bağlantı Türü	VPN bağlantı türü oluştur
IPsec (cisco)	Cisco tarafından IPsec protokolü
L2TP	L2TP protokolü
Özel SSL	Özel SSL ile Bağlantı
IKEv2	IKEv2 protokolü
Proxy Kurulumu	VPN bağlantısı için bir Proxy'nin yapılandırılması
Hiçbiri	Vekil Oluşturma
Manuel	Manuel olarak Proxy oluşturma
Proxy Sunucu URL'si	Proxy Ayarlarına erişim için adres
Liman	Proxy için bağlantı noktası belirleme
Kimlik Doğrulama	Proxy'de kimlik doğrulama için kullanıcı adı
Şifre	Proxy'de kimlik doğrulama için şifre
Otomatik	Otomatik olarak bir Proxy oluşturun
Proxy Sunucu URL'si	Proxy ayarlarına erişim için URL

HTTP Proxy

Proxy Türü	
Manuel	Manuel olarak bir Proxy oluşturun
Proxy Sunucu URL'si	Proxy Ayarlarına erişim için adres
Liman	Proxy bağlantı noktası oluştur
Kimlik Doğrulama	Proxy'de kimlik doğrulama için kullanıcı adı
Şifre	Proxy'de kimlik doğrulama için şifre
Otomatik	Otomatik olarak bir Proxy oluşturun
Proxy PAC URL'si	Proxy PAC URL'si
PAC'ye erişilemiyorsa doğrudan bağlantıya izin ver	PAC'ye erişilemiyorsa doğrudan bağlantıya izin ver (VPN olmadan)
Tutsak ağlara erişmek için proxy'yi atlamaya izin verin	Tutsak iç ağlara erişmek için proxy'yi atlamaya izin verin

AirPrint

IP Adresi	Yazıcı IP adresi
Kaynak Yolu	AirPrint cihazına giden kesin yol

AirPlay

Cihaz Adı	Cihaz adı
Şifre	Eşleştirme şifresi
Beyaz Liste	Cihazın yalnızca kendisini eşleştirebileceği cihazların bir listesini tanımlayın

PIM Yönetimi

Exchange Active Sync

Hesap Adı	Hesabın adı.
e-Posta Adresi	Hesabın adresi (örn. max@company.com)
Sunucu Ana Bilgisayar Adı	Dahili Ana Bilgisayar Adı
Giriş Adı	Cihazın kullanıcı istemesi için "Domain" ve "Login Name" boş olmalıdır.
Etki Alanı	Cihazın kullanıcı istemesi için "Domain" ve "Login Name" boş olmalıdır. Bir ACL Ağ Geçidi Yapılandırması etkinleştirilmişse ve Etki Alanı alanı boş değilse, AppTec360 Universal Gateway cihazın kimliğini aşağıdaki adla doğrulayacaktır "Etki Alanı\Login Adı"
Şifre	Hesap için parola (örn. secretUserPassword)
Mail to Sync'in Geçmiş Günleri	Senkronize edilecek geçmiş posta günü sayısı
SSL kullanın	Dahili Exchange Ana Bilgisayarı için SSL Kullanın
Gelişmiş Seçenek	Gelişmiş Seçenekleri Göster
Sunucu Bağlantı Noktası	Dahili Bağlantı Noktası
Sunucu Yolu	Dahili Yol
Harici Ana Bilgisayar Adı	Harici Ana Bilgisayar
Harici Bağlantı Noktası	Harici Bağlantı Noktası
Harici Yol	Harici Yol
Harici için SSL kullanın Değişim Ana Bilgisayarı	Harici Exchange Ana Bilgisayarı için SSL Kullanın

e-Posta

Son kullanıcı cihazında POP3 / IMAP hesaplarının kurulması

Hesap Açıklaması	İsim des E-posta Hesapları
Hesap Türü	
IMAP	
Yol Öneki	Özel klasörler için Yol Öneki
POP	
Kullanıcı Ekran Adı	Kullanıcı ekran adı
E-posta Adresi	Kullanıcı e-posta adresi

Gelen Posta	Gelen sunucu ayarları
Posta Sunucusu Adresi	Posta Sunucusu adresi
Posta Sunucusu Bağlantı Noktası	Posta Sunucusu bağlantı noktası
Kullanıcı Adı	İlgili kullanıcı adı
Kimlik Doğrulama Türü	Kimlik Doğrulama Türü
Hiçbiri	Kimlik Doğrulama Türü Yok
Şifre (yalnızca cihaz düzeyinde)	Parola istemi
MDM Mücadelesi-Yanıt	
NTLM	NTLM-Kimlik Doğrulama
HTTP MD5 Özeti	
SSL kullanın	Gerekirse SSL kullanın

Giden Posta	Giden sunucu ayarları
Posta Sunucusu Adresi	Posta Sunucusu Adresi
Posta Sunucusu Bağlantı Noktası	Posta Sunucusu Bağlantı Noktası
Kullanıcı Adı	İlgili Kullanıcı Adı
Kimlik Doğrulama Türü	
Hiçbiri	Kimlik doğrulama yöntemi yok
Şifre (yalnızca cihaz düzeyinde)	Parola istemi
MDM Mücadelesi-Yanıt	
NTLM	NTLM-Kimlik Doğrulama
HTTP MD5 Özeti	
SSL kullanın	Gerekirse SSL kullanın
Giden şifre gelen ile aynı	Giden şifre gelen ile aynı
Sadece postada kullanın	Tüm giden e-postalar Mail-App aracılığıyla gönderilecekse etkinleştirin

CalDav

Bir CalDav Hesabının kurulumunu ve dağıtımını yapılandırma

Hesap Açıklaması	Hesabın görünen adı
Ana bilgisayar adı	Ana bilgisayar adı ve/veya IP adresi
Liman	CalDav Hesabının Bağlantı Noktası
Ana URL	Hesabın Ana URL'si
Kullanıcı Adı	İlgili CalDav kullanıcı adı
Şifre (yalnızca cihaz düzeyinde)	İlgili CalDav şifresi
SSL kullanın	Gerekirse SSL kullanın

CardDav

Bir CardDav Hesabının kurulumunu ve dağıtımını yapılandırma

Hesap Açıklaması	Hesabın görünen adı
Ana bilgisayar adı	Ana bilgisayar adı ve/veya IP adresi
Liman	CardDav Hesabının Bağlantı Noktası
Ana URL	Hesabın Ana URL'si
Kullanıcı Adı	İlgili CardDav kullanıcı adı
Şifre (yalnızca cihaz düzeyinde)	İlgili CardDav şifresi
SSL kullanın	Gerekirse SSL kullanın

LDAP

Bu alanda, son kullanıcı cihazı ile Active Directory arasında dinamik bir sertifika alışverişine izin vermek için bir LDAP bağlantısı kurun.

Lütfen seçilen kullanıcının ilgili okuma iznine sahip olması gerektiğini unutmayın.

Hesap Açıklaması	Hesap Açıklaması
Hesap Kullanıcı Adı	LDAP erişimi için kullanıcı
Hesap Şifresi	LDAP erişimi için parola
Hesap Ana Bilgisayar Adı	LDAP Sunucusu Ana bilgisayar adı/IP adresi
SSL kullanın	Gerekirse SSL kullanın

İkinci bölümde, LDAP kayıt defterinde arama yapmak için ayrı ayrı filtreler tanımlayabilirsiniz.

Açıklama	Kapsam	Arama Tabanı
Filtre açıklaması	LDAP kayıt defterinde arama düzeyi	Bireysel filtreyi tanımlama

Gösterge Tablosu ve Raporlama

Gösterge Tablosu Ayarları

Burada hangi gösterge tablolarının mevcut olduğunu görebilir, bunları düzenleyebilir veya yenilerini oluşturabilirsiniz. Her Gösterge Tablosunun gösterilecek kendi veri seti ve grafik yapılandırması vardır.

Gösterge Tablosu Ayarları Kontrolü

Kamu	Gösterge Tablosunu herkese açık olarak ayarlar, böylece diğer kullanıcılar Gösterge Tablosunu görebilir. Kullanıcılar elbette oturum açabilmeli ve Gösterge Tablolarını görüntüleyebilmelidir. "Herkese Açık" etkinleştirilmezse, yalnızca oluşturan kişi görebilir.
Varsayılan	Gösterge Tablosunu varsayılan olarak ayarlar, böylece Gösterge Tablosu Görünümüne bir sonraki erişiminizde otomatik olarak açılır.
	Gösterge Tablosunu ve grafiklerini gösterin
	Gösterge Tablosunu Silme
	Gösterge Tablosu Adını ve Ayarlarını Düzenleme
	Gösterge Tablosunun bir kopyasını oluşturun
	Tamamen yeni bir Gösterge Tablosu ekleyin

Gösterge Tablosu Görünümü

Bu, seçilen Gösterge Tablosunun Verilerini ve Grafiklerini gösterir ve ayrıca bunları değiştirmenize olanak tanır.

Gösterge Paneli Kontrolü

	Gösterge Tablosunda hangi verilerin gösterileceğini, gösterilecek veri miktarını ve bu verilerin hangi boyutta gösterileceğini tanımlamanızı sağlar
	Sizi Gösterge Tablosuna Genel Bakış'a geri götürür
	O anda açık olan Gösterge Tablosunu varsayılan haline sıfırlar
	O anda açık olan Gösterge Tablosunda yaptığınız tüm değişiklikleri kaydeder (örneğin hangi verilerin gösterileceği)
	Grafik türünü sütun grafiği olarak değiştirme
	Grafik türünü pasta grafik olarak değiştirme
	Grafik türünü donut grafiği olarak değiştirme
	Grafik türünü kutupsal alan grafiği olarak değiştirme
	Sıralama düzenini değiştirme

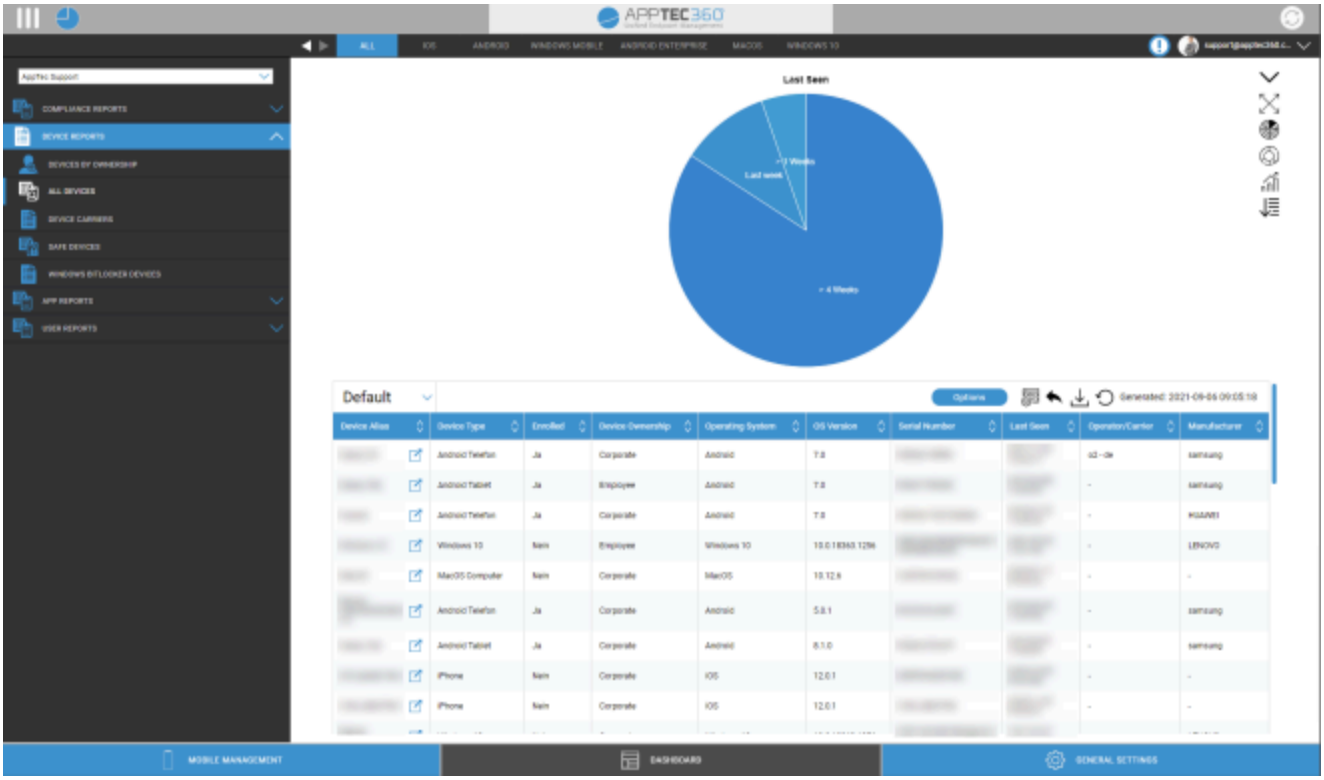
Genişletilmiş Raporlama

"Genişletilmiş Raporlama", cihaz ve kullanıcı bilgileri hakkında ayrıntılı genel bakışlar ve grafikler sunar.

Birkaç varsayılan Rapor vardır, ancak gösterilecek verileri eklemek veya kaldırmak için hepsi manuel olarak değiştirilebilir.

Lütfen hangi verilerin gösterileceğini yalnızca manuel olarak değiştirebileceğinizi unutmayın. Seçilen rapor kategorisi bunun dayandığı verileri tanımlar. Örneğin, Cihaz Raporları Tüm Cihazlar iOS'ta iOS raporunda Android cihazları asla göremezsiniz

Sol üstte, raporlama verilerini belirli bir grupla (ve tüm alt gruplarıyla) sınırlayabilirsiniz. Varsayılan olarak bu kök düğümünüze ayarlanmıştır, bu nedenle TÜM cihazları ve kullanıcıları dikkate alır.



Genişletilmiş Raporlama Kontrolü

Her bir genel bakışta, raporu istediğiniz şekilde değiştirmek için aşağıdaki işlevleri kullanabilirsiniz:

	Grafiği gizle (Grafik gösteriliyorsa)
	Grafiği göster (Grafik gizliyse)
	Grafiği genişletin (Grafik daraltılmışsa)
	Grafiği daralt (Grafik genişletilmişse)
	Grafik türünü sütun grafiği olarak değiştirme
	Grafik türünü pasta grafik olarak değiştirme
	Grafik türünü donut grafiği olarak değiştirme
	Grafik türünü kutupsal alan grafiği olarak değiştirme
	Sıralama düzenini değiştirme
	Görüntülenen genel bakışla ilgili aşağıdaki kısımları değiştirin: • Sütun ekleme/kaldırma • Sütunların gösterilme sırasını belirtin • Tablonun üzerindeki grafiği Göster/Gizle • Grafik için kullanılan sütunu seçin • Tablonuzun verilerini filtreleme
	Farklı raporları kaydetmek ve yüklemek için kurulum yöneticisini açın
	O anda açık olan Raporu varsayılana sıfırlar
	Geçerli raporu .csv dosyası olarak dışa aktarma
	Verileri yeniden oluşturun ve geçerli raporu yeniden yükleyin

Sonraki sayfalarda tüm varsayılan raporların bir listesini bulabilirsiniz.

Uyum Raporları

Köklü Cihazlar

Root/jailbreak yapılmış cihazlara genel bakış.

Bu raporun varsayılan sütunları:

Cihaz Takma Adı
Cihaz Sahibi
E-Posta
İşletim Sistemi
Telefon Numarası
Son Görülme
Üretici firma

Dolaşım Cihazları

Dolaşımda olan tüm cihazlara genel bakış

Bu raporun varsayılan sütunları:

Cihaz Takma Adı
Cihaz Sahibi
E-Posta
Cihaz Tipi
İşletim Sistemi
Telefon Numarası
Son Görülme

Dolaşım Etkin Cihazlar

Dolaşımı etkinleştirmiş ancak şu anda dolaşımda olması gerekmeyen tüm cihazlara genel bakış.

Bu raporun varsayılan sütunları:

Cihaz Takma Adı
Cihaz Sahibi
E-Posta
Cihaz Tipi
İşletim Sistemi
Telefon Numarası
Son Görülme

Denetlenen Cihazlar

Denetimli modda denetlenen tüm cihazlara genel bakış (yalnızca iOS)

Bu raporun varsayılan sütunları:

Cihaz Takma Adı
Cihaz Sahibi
E-Posta
Cihaz Tipi
Son Görülme

Etkin Olmayan Cihazlar

Son 7 gün içinde sunucuya bağlanmamış tüm cihazlara genel bakış

Bu raporun varsayılan sütunları:

Cihaz Takma Adı
Cihaz Sahibi
E-Posta
Cihaz Tipi
İşletim Sistemi
Son Görülme

Cihaz Raporları

Sahipliğe Göre Cihazlar

Burada şu anda kaç cihazın kurumsal (kurumsal cihazlar) ve çalışan (özel cihazlar) cihazı olarak dağıtıldığını görebilirsiniz.

Bu raporun varsayılan sütunları:

Cihaz Takma Adı
Cihaz Sahibi
Cihaz Tipi
Cihaz Sahipliği
İşletim Sistemi

Tüm Cihazlar

Burada en önemli bilgilerle birlikte tüm cihazlara genel bir bakış görebilirsiniz.

Bu raporun varsayılan sütunları:

Cihaz Takma Adı
Cihaz Tipi
Kayıtlı
Cihaz Sahipliği
İşletim Sistemi
İşletim Sistemi Sürümü
Seri Numarası
Son Görülme
Operatör/Taşıyıcı
Üretici firma

Cihaz Taşıyıcıları

Burada taşıyıcıya (hücresel sağlayıcı) ilişkin bir genel bakış görebilirsiniz.

Bu raporun varsayılan sütunları:

Cihaz Takma Adı
Cihaz Sahibi
E-Posta
İşletim Sistemi
İşletim Sistemi Sürümü
Operatör/Taşıyıcı

SAFE Cihazları

Burada hangi cihazların SAFE Sürümünü kullandığına dair genel bir bakış görebilirsiniz.

Genel bakış ve/veya SAFE yalnızca Samsung cihazları için mevcut olduğundan, bu noktanın altında normal sekmeleri göremezsiniz.

Bu raporun varsayılan sütunları:

Cihaz Takma Adı
Cihaz Sahibi
E-Posta
Cihaz Tipi
Son Görülme
GÜVENLİ Sürüm

Windows BitLocker Aygıtları

Burada BitLocker kullanan Windows cihazlarına genel bir bakış görebilirsiniz.

Bu raporun varsayılan sütunları:

Cihaz Takma Adı
Cihaz Sahibi
E-Posta

BitLocker Durumu

Uygulama Raporları

Burada uygulamalarla ilgili çeşitli genel bakışlar elde edersiniz. Tüm bu raporlarda, cihazlarda hangi sürümlerin ne sıklıkla yüklü olduğunu görmek için bir girdiye tıklayabilirsiniz. Bu görünümde, hangi cihazlarda bu belirli sürümün yüklü olduğunu görmek için belirli bir sürüme tekrar tıklayabilirsiniz.

Not: Sistemin cihazdan güncel bilgileri alması biraz zaman alabilir. Ayrıca raporlar her dakika güncellenmemektedir. Yeni bir uygulama veya sürüm atadıysanız mevcut durumu görmek için sabırlı olmanız gerekebilir. Raporu manuel olarak yeniden yüklemek, raporu mevcut en güncel verileri göstermeye zorlayacaktır

Yüklü Uygulamalar

Burada yüklü tüm uygulamalara genel bir bakış elde edersiniz.

Bu raporun varsayılan sütunları:

İsim	İlgili uygulamanın ve/veya hizmetin adı
Tanımlayıcı	Belirli uygulama/hizmet kimliği
Toplam Sayı	Bu uygulamanın / hizmetin son kullanıcı cihazlarına ne sıklıkla yüklendiği

En Çok Yüklenen Uygulamalar

Burada en çok yüklenen uygulamalara genel bir bakış elde edersiniz.

Bu raporun varsayılan sütunları:

İsim	İlgili uygulamanın ve/veya hizmetin adı
Tanımlayıcı	Belirli uygulama/hizmet kimliği
Toplam Sayı	Bu uygulamanın / hizmetin son kullanıcı cihazlarına ne sıklıkla yüklendiği

Zorunlu Uygulamalar

Burada zorunlu (zorunlu gerekli) uygulamalara genel bir bakış elde edersiniz.

Bu raporun varsayılan sütunları:

İsim	İlgili uygulamanın ve/veya hizmetin adı
Tanımlayıcı	Belirli uygulama/hizmet kimliği
Uygulama Kaynağı	Hangi AppStore'un dahil olduğu: • Google PlayStore (Android) • iTunes AppStore (iOS)
İŞLETIM SISTEMI	İşletim Sistemi

Kara Listeye Alınan Uygulamalar

Burada, tanımlanmış tüm kara listeye alınmış uygulamalara genel bir bakış elde edersiniz.

Bu raporun varsayılan sütunları:

İsim	İlgili uygulamanın ve/veya hizmetin adı
Tanımlayıcı	Belirli uygulama/hizmet kimliği
Uygulama Kaynağı	Hangi AppStore'un dahil olduğu: • Google PlayStore (Android) • iTunes AppStore (iOS)
İŞLETIM SISTEMI	İşletim Sistemi

Kullanıcı Raporları

Tarife

Burada kullanıcılarınızın telefon tarifelerine ve SIM kartlarına genel bir bakış elde edersiniz.

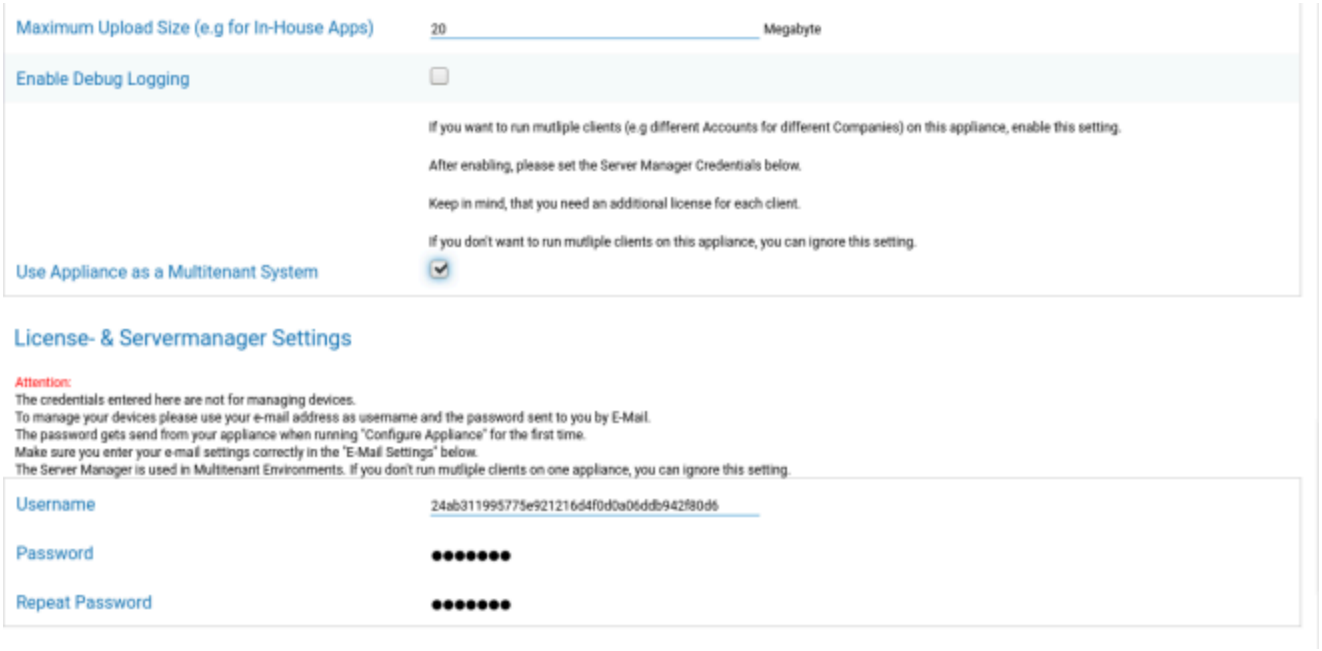
Bu raporun varsayılan sütunları:

E-Posta
İsim
telefonNumarası
taşıyıcı
tarife
seçenek
fiyat
sözleşmeİptal Edildi
sözleşmeBaşlangıç
duringTime
mobileAndData
dataVolume
multiSIM
tip
simCardSerial1
simCardSerial2
simCardSerial3
pin1
pin2
puk1
puk2
Not

Çok Kiracılı Yönetim

AppTec360 EMM, her biri kendi kullanıcıları ve grupları, izinleri ve genel ayarları olan birden fazla ayrı kiracıyı barındırabilir.

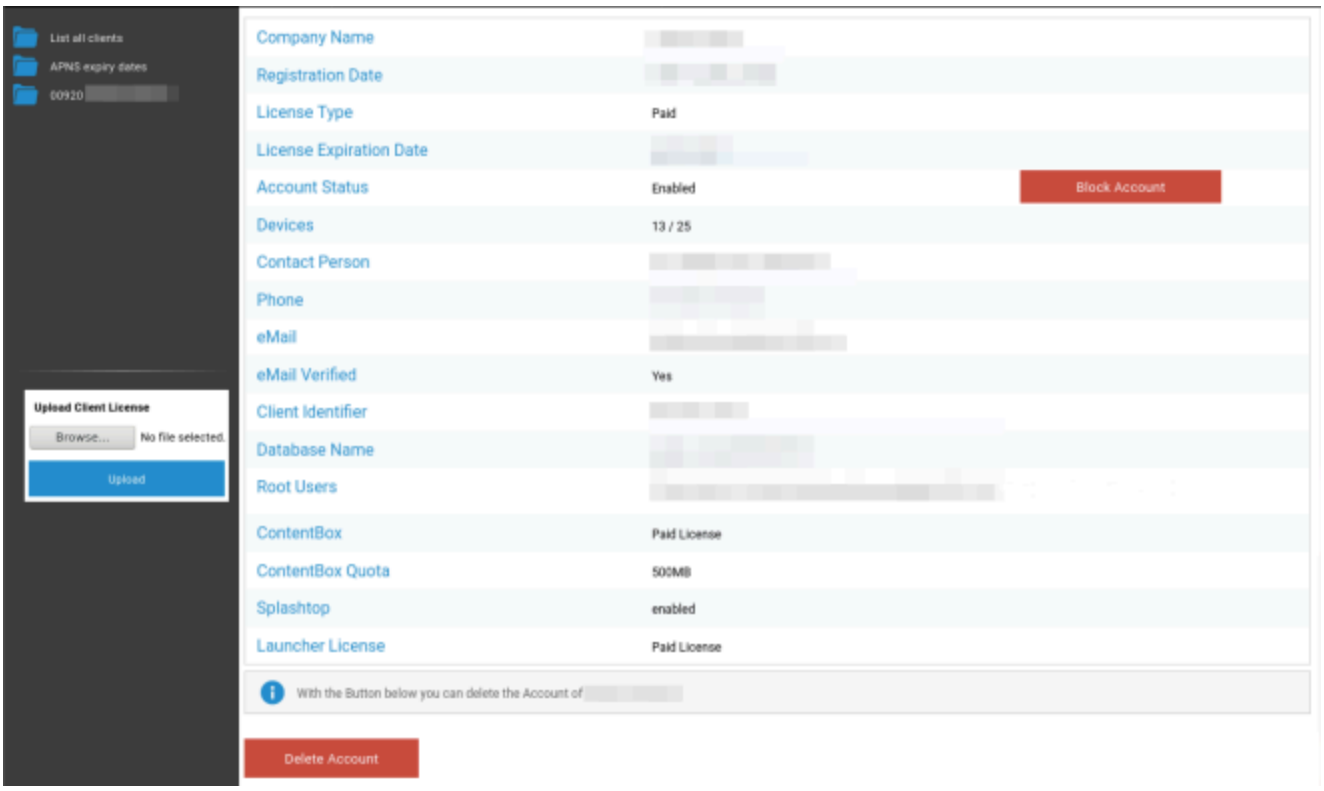
Multitenant özelliklerini etkinleştirmek için, "Üçüncü Adım - Sunucu Ayarları" bölümünde Uygulamanın yapılandırma arayüzünde etkinleştirmeniz gerekir.



Yeni menüde Servermanager için bir kullanıcı adı ve şifre belirleyin. Ayarları kaydedin ve ayarı uygulamak için "Beşinci Adım - Lisans Sözleşmesi "nde "Configure Appliance "ı çalıştırın.

Yapılandırma tamamlandığında, artık normal Mobil Yönetim arayüzü üzerinden ayarlanan kimlik bilgileriyle oturum açabilirsiniz.

Giriş yaptıktan sonra aşağıdaki görünümü görebilirsiniz.



Sol tarafta tüm kiracıları (bu durumda yalnızca 920 kimlikli bir kiracı) ve sağ tarafta bu müşteriyle ilgili bilgileri görebilirsiniz. Ayrıca hesaba erişimi engelleme ve istemciyi silme seçeneğiniz de vardır (DİKKAT: Bu, söz konusu istemciyle ilgili tüm verileri kaldıracaktır).

Sol tarafta yeni bir müşteri lisansı yükleyebilirsiniz; bu, mevcut bir müşteri için lisans güncellemesi veya otomatik olarak yeni bir müşteri oluşturan yeni bir lisans olabilir. Yeni bir müşteri oluşturulduğunda, oturum açma şifresini içeren bir e-posta otomatik olarak lisansın verildiği e-posta adresine gönderilir.

Yeni veya güncellenmiş bir istemci lisansı almak için (örneğin daha fazla cihaz lisansına ihtiyaç duyduğunuzda) satış temsilcinizle iletişime geçin.

Ek görünümler

Tüm müşterileri listeleyin

Sistemdeki tüm istemciler hakkında genel bir bakış gösterir.

Müşteri Kimliği	Müşteri Kimliği
Tanımlayıcı	Müşteri Tanımlayıcı
Veritabanı	Veritabanı
Şirket Adı	Şirket adı
e-Posta	İlgili kişi e-Posta
Doğrulandı	İlgili kişinin e-postasının doğrulanıp doğrulanmadığı
Ülke	Ülke
Cihazlar	Kayıtlı cihaz sayısı
Kayıt Tarihi	Lisans atamasının yapıldığı zaman noktası
Son Giriş	Son yönetici hesabı girişi
Lisans	Lisans türü göstergesi (Ücretsiz|Ücretli)
CB Lisansı	ContentBox lisans türü (Free|Paid)
Durum	Mevcut AppTec-Client durumu
Süresi doldu	Lisansın süresi dolmuşsa görüntüler
iOS	iOS Cihaz Sayısı
Android	Android Cihaz Sayısı
Windows Mobile	Windows Mobile Cihaz Sayısı
MacOS	MacOS Cihaz Sayısı
Windows 10	Windows 10 Cihaz Sayısı
Android Kurumsal	Android Kurumsal Cihaz Sayısı
IOS BYOD (Kullanıcı Kaydı)	IOS BYOD (Kullanıcı Kaydı) Cihazlarının Sayısı
IoT	IoT Cihazlarının Sayısı

APNS son kullanma tarihleri

Tüm istemcilerin tüm APNS sertifika sona erme tarihlerine genel bir bakış gösterir.

Müşteri Kimliği	Müşteri Kimliği
Şirket Adı	Şirket Adı
Son Kullanma Tarihi	Apple APNS sertifikası için son kullanma tarihi
Bilgi	Son kullanma tarihi hakkında bilgi

İletişim

Başka sorunuz var mı? Bizimle iletişime geçmeniz yeterlidir:

Genel teknik sorular için

support@apptec360.com

+41 61 511 3210

Bir sanal cihazın kurulumuyla ilgili sorular için

consulting@apptec360.com

+41 61 511 3214

Sorumluluk Reddi