AppTec360 Enterprise Mobile Manager & ContentBox

Příručka pro správu | Verze 5.0 (202110)

Obsah

- Zabezpečení SecurePIM
- Prohlížeč SecurePIM
- Výměna

Správa připojení

- Wi-Fi
  - Nastavení serveru proxy
  - Typ zabezpečení
- VPN
  - Typ VPN
    - VPN
    - VPN pro jednotlivé aplikace
  - Nastavení serveru proxy
- APN
- Cellular
- Proxy server HTTP
- AirPrint
- AirPlay

Správa PIM

- Exchange Active Sync
- eMail
  - Příchozí pošta
  - Odchozí pošta
- CalDav
- Přihlášené kalendáře
- LDAP

Správa webu

- Webové klipy
- Filtr webového obsahu

Správa aplikací

- Správce podnikových aplikací
  - Nainstalované aplikace (pouze na úrovni zařízení)
  - Povinné aplikace
    - Možnosti instalace
  - Webové aplikace

- Omezení a nastavení
  - Aplikace na černé / bílé listině
  - Omezení aplikace SysApp
  - App-VPN
  - Nastavení aplikace
- Obchod s podnikovými aplikacemi
  - Aplikace iTunes
  - In-House
- Režim kiosku
  - Typ aplikace
    - Balíček
    - ADRESA URL
  - Nastavení režimu kiosku

Android Enterprise – plně spravovaná konfigurace zařízení

Obecné

- Přehled profilu skupiny (pouze na úrovni skupiny)
- Přehled zařízení (pouze na úrovni zařízení)
- Revize konfigurace (pouze na úrovni zařízení)
- Protokol zařízení (pouze na úrovni zařízení)
  - Protokol příkazů
  - Možné stavy příkazů
- Nastavení zařízení
  - Konfigurace klienta
  - Tapety

Správa aktiv (pouze na úrovni zařízení)

- Informace o zařízení
  - Wi-Fi
- Cellular
- Bluetooth

Správa zabezpečení

- Ochrana proti krádeži (pouze na úrovni zařízení)
  - Informace GPS (pouze na úrovni zařízení)
  - Vymazání a uzamčení (pouze na úrovni zařízení)
  - Zpráva (pouze na úrovni zařízení)

- Konfigurace zabezpečení
  - Přístupový kód zařízení
  - AntiVirus
- Konec životnosti (pouze na úrovni zařízení)
  - Vymazat (pouze na úrovni zařízení)
- Nastavení omezení
  - Omezení
- Správa certifikátů

Správa připojení

- Wifi
  - Typ zabezpečení
    - WEP
    - WPA/WPA2
    - 802.1x EAP
- VPN
  - Typ VPN
    - VPN
    - VPN pro jednotlivé aplikace
- Omezení

Správa PIM

- Výměna Gmail

Správa aplikací

- Správce podnikových aplikací
  - Nainstalované aplikace (pouze na úrovni zařízení)
  - Systémové aplikace (pouze na úrovni zařízení)
  - Povinné aplikace
  - Černá a bílá listina
  - Systémové aplikace AE
- Omezení a nastavení
  - Nastavení správy aplikací
- Obchod s podnikovými aplikacemi
  - In-House
- Obchod Play pro podniky
  - Obchod AE Play
- Režim kiosku a spouštěč

- Tapety

Správa aktiv (pouze na úrovni zařízení)

- Informace o zařízení
  - Wi-Fi
- Cellular
- Bluetooth

Správa zabezpečení

- Ochrana proti krádeži (pouze na úrovni zařízení)
  - Informace GPS (pouze na úrovni zařízení)
  - Vymazání a uzamčení (pouze na úrovni zařízení)
  - Zpráva (pouze na úrovni zařízení)
- Konfigurace zabezpečení
  - Přístupový kód zařízení
  - Přístupový kód kontejneru
  - AntiVirus
- Konec životnosti (pouze na úrovni zařízení)
  - Vymazat (pouze na úrovni zařízení)
- Nastavení omezení
  - Omezení
- Správa certifikátů

Správa připojení

- Wifi
  - Typ zabezpečení
    - WEP
    - WPA/WPA2
    - 802.1x EAP
- VPN
  - Typ VPN
    - VPN
    - VPN pro jednotlivé aplikace
- Omezení

Správa PIM

- Výměna Gmail

Správa aplikací

- Správce podnikových aplikací

- Zpráva (pouze na úrovni zařízení)
- Konfigurace zabezpečení
  - Přístupový kód
  - Šifrování
  - AntiVirus
- Konec životnosti (pouze na úrovni zařízení)
  - Vymazat (pouze na úrovni zařízení)
- Nastavení omezení
  - Omezení
  - Vlastník zařízení AE

Kontejner BYOD

- Android Enterprise
  - Android Enterprise
  - Výměna Gmail
  - Systémové aplikace AE
  - Přístupový kód kontejneru
- Samsung KNOX
  - Aktivace
  - Přístupový kód Knox
  - Knox Security
  - Knox Exchange
  - Knox eMail
  - Knox Apps

Správa připojení

- Wifi
  - Typ zabezpečení
    - WEP
    - WPA/WPA2
    - 802.1x EAP
- VPN
- Omezení
- APN
- Bluetooth

Správa PIM

- Výměna

- eMail
- AE Gmail Exchange

Správa aplikací

- Správce podnikových aplikací
  - Nainstalované aplikace (pouze na úrovni zařízení)
  - Systémové aplikace (pouze na úrovni zařízení)
  - Povinné aplikace
  - Systémové aplikace AE
- Omezení a nastavení
  - Černá a bílá listina
  - Omezení aplikací systému
    - Aplikace Samsung
    - Aplikace Huawei
  - Nastavení správy aplikací
- Obchod s podnikovými aplikacemi
  - Obchod Playstore
  - In-House
- Obchod Play pro podniky
- Režim kiosku a spouštěč
  - Režim kiosku
  - Spouštěč AppTec360
  - Nastavení AppTec360

Dálkové ovládání

- Splashtop
- Teamviewer

Správa obsahu

- Obsahové pole
- Zabezpečený prohlížeč

Konfigurace počítače se systémem Windows 10

Obecné

- Přehled profilu skupiny (pouze na úrovni skupiny)
- Přehled zařízení (pouze na úrovni zařízení)
- Nastavení
- Revize konfigurace (pouze na úrovni zařízení)

- Wi-Fi
  - Konfigurace podnikové sítě Wi-Fi
- VPN
- Proxy server HTTP
- AirPrint
- AirPlay

Správa PIM

- Exchange Active Sync
- eMail
- CalDav
- CardDav
- LDAP

Dashboard & Reporting

Nastavení ovládacího panelu

Zobrazení přístrojové desky

Rozšířené hlášení

- Zprávy o dodržování předpisů
  - Zakořeněná zařízení
  - Roamingová zařízení
  - Zařízení s povoleným roamingem
  - Zařízení pod dohledem
  - Neaktivní zařízení
- Zprávy o zařízení
  - Zařízení podle vlastnictví
  - Všechna zařízení
  - Nosiče zařízení
  - Zařízení SAFE
  - Zařízení se systémem Windows BitLocker
- Zprávy o aplikacích
  - Nainstalované aplikace
  - Nejčastěji instalované aplikace
  - Povinné aplikace
  - Aplikace na černé listině
- Uživatelské zprávy

Obecný přehled

Úvod do AppTec360

Řešení AppTec Enterprise-Mobile-Management-Solution nabízí možnost správy a konfigurace všech mobilních zařízení pomocí intuitivní konzole pro správu. V tomto případě může být server EMM spuštěn buď ve vašem vlastním prostředí, nebo můžete využít naše cloudové řešení.

Pokud jde o centrální instalaci podnikových aplikací do chytrých telefonů, jste na správném místě. Pomocí nástroje Enterprise Mobile Manager můžete během několika sekund distribuovat firemní aplikace a dokumenty do zařízení nebo blokovat nežádoucí aplikace pomocí bílé/černé listiny.

Používání soukromých zařízení ve firmách představuje novou výzvu pro zabezpečení chytrých telefonů a tabletů. Vzhledem k tomu, že zaměstnanci chtějí stále více používat své chytré telefony, musí správci IT chránit velké množství různých typů zařízení. Pomůžeme vám se zabezpečením všech zařízení a citlivých dat, která jsou na nich uložena, a jejich správou z intuitivní konzole.

Podporované operační systémy zařízení

AppTec360 nabízí podporu pro zařízení se systémy iOS, Android a Windows. Upozorňujeme, že kapacita funkcí uvedených platforem se může v jednotlivých operačních systémech lišit.

- Apple iOS 11.0 nebo vyšší*
- Apple macOS 10.11 nebo vyšší
- Google Android 4.4 nebo vyšší** v cloudové verzi
- Systém Google Android 4.1 nebo vyšší** ve verzi OnPrem
- MS Windows 10 nebo vyšší*** (stolní počítač, notebook a tablet)

**Upozorňujeme, že zařízení se systémem iOS 10 nebo starším nelze zaregistrovat kvůli drastickým změnám, které společnost Apple provedla v procesu registrace.*

***Zařízení lze připojit a nakonfigurovat, i když používají verzi, která již není podporována výrobcem. Upozorňujeme, že některé funkce mohou vyžadovat určitou verzi systému Android. V případech podpory se řídíme oficiální podporou výrobce. V případě problémů nebo chyb způsobených zastaralou verzí, která již není podporována výrobcem, si vyhrazujeme právo nabídnout pouze omezenou podporu.*

****Domácí verze systému Windows nejsou podporovány z důvodu omezení operačního systému. Důrazně doporučujeme používat verzi operačního systému, která je stále podporována výrobcem. Nejen kvůli kompatibilitě, ale také z bezpečnostních důvodů. Proto doporučujeme iOS 12 nebo vyšší a Android 9 nebo vyšší.*

Podporované adresáře LDAP

- Služba Microsoft Active Directory
- Otevřít LDAP

Aktuální informace o "Podporovaných operačních systémech zařízení" a "Podporovaných adresářích LDAP" naleznete zde:

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

Vysvětlení „režimu pod dohledem“ v zařízeních Apple

Režim Supervised představuje rozšířené rozhraní pro zařízení iOS.

Na příslušně nakonfigurovaném zařízení lze uplatnit další omezení, která se týkají funkčnosti zařízení koncového uživatele. Ty jsou rovněž obsaženy v příručce pro správu a jsou označeny bannerem.

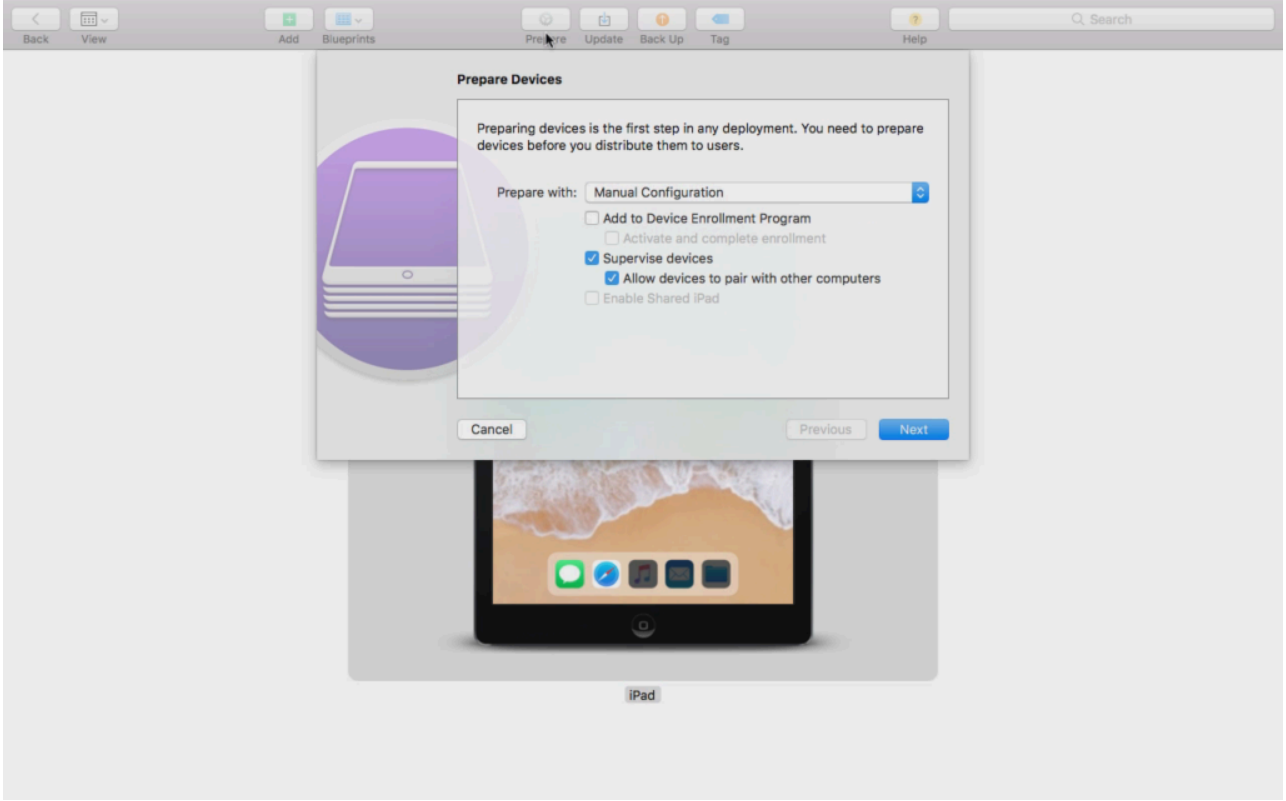
K dispozici v režimu Supervised

Režim "Supervised-Mode" lze aktivovat pomocí programu "Apple Configurator". Apple Configurator může nastavit výchozí nastavení nových zařízení iOS jako konfigurační nástroj (přes rozhraní USB).

Nástroj umí instalovat nejen konfigurační profily, ale také aplikace. Je zdarma, ale vyžaduje počítač Mac.

Aktivace režimu pod dohledem

1. Otevření nástroje Apple Configurator



2. Klikněte na zařízení a vyberte možnost "Připravit".
3. Zvolte "Ruční konfigurace" a "Dohled nad zařízeními".
4. Klikněte na "Další".
5. (volitelně) Nyní můžete přidat server MDM, na kterém bude zařízení zapsáno. Odkaz na něj najdete v části "Obecná nastavení - Konfigurace iOS - Konfigurátor a adresa URL" Vyberte svou organizaci nebo vytvořte novou.
6. Vyberte si svou organizaci nebo vytvořte novou
7. Zvolte, které kroky úvodního nastavení mají být přeskočeny, a klikněte na "Další" (POZOR: Pokračování povede ke smazání zařízení!).

Nyní bude vaše zařízení přepnuto do režimu pod dohledem. To může trvat několik minut. Po dokončení se zařízení restartuje.

Nyní je vaše zařízení pod dohledem!

Přidání zařízení do DEP

Zařízení můžete do programu DEP (Device Enrollment Programm) přidat také pomocí nástroje Apple Configurator, pokud máte zařízení se systémem iOS 11 nebo vyšším.

Více informací o DEP: https: //www.apple.com/business/dep/

Postupujte stejně jako při dohledu nad zařízením a navíc zaškrtněte políčko "Add to Device Enrollment Programm". Budete požádáni o přihlašovací údaje do programu DEP, pokud jste se do něj ještě nikdy nepřihlásili pomocí nástroje Apple Configurator.

Po dokončení procesu lze zařízení najít na serveru DEP "Devices Added by Apple Configurator 2". Nyní můžete tento server použít a připojit jej ke konzole pro správu nebo zařízení přenést na již existující server.

Nyní jste úspěšně přidali zařízení do DEP!

Vysvětlení systému Android Enterprise

Co je Android Enterprise?

Android Enterprise nabízí lepší kontrolu nad pracovními zařízeními, která jsou spravována pomocí MDM. Správci tak mohou mít buď plnou kontrolu nad zařízeními s Androidem, nebo oddělit firemní data od soukromých dat v kontejnerových zařízeních. Android Enterprise navíc umožňuje snadnější registraci zařízení a snadnou distribuci aplikací.

Jaké jsou požadavky na používání systému Android Enterprise?.

Aplikaci Android Enterprise může používat každý zdarma. K aktivaci všech funkcí Android Enterprise stačí k MDM připojit účet Google. Více informací o tom najdete v části Android Enterprise.

Systém Android Enterprise lze používat na zařízeních se systémem Android 5.1 nebo vyšším, s výjimkou rozšířeného pracovního profilu (viz níže). Doporučujeme alespoň Android 7 nebo vyšší pro snazší zápis nebo Android 11 pro využití všech dostupných funkcí.

Jaké jsou dostupné režimy systému Android Enterprise?

Při používání systému Android Enterprise můžete používat 3 různé režimy.

AE Plně spravované zařízení (Work Managed): Plně spravované zařízení, které se používá pouze k práci. To umožňuje správci plnou kontrolu nad zařízením. To neumožňuje soukromé používání zařízení. Pro registraci zařízení v tomto režimu je třeba zařízení resetovat a zaregistrovat pomocí QR kódu (viz Registrace AE) nebo zaregistrovat pomocí funkce Knox Enrollment nebo Zero Touch.

AE BYOD Container: Kontejner BYOD (bring your own device) umožňuje uživatelům přístup k firemním datům na jejich soukromém telefonu v samostatném kontejneru. V tomto režimu nemohou soukromé aplikace vidět firemní data a aplikace a naopak. Pro registraci zařízení v tomto režimu je třeba stáhnout aplikaci AppTec a naskenovat QR kód. Vytvořte zařízení v konzoli a jako typ zařízení vyberte "AE Container (BYOD & Enahnced Work Profile)". Kliknutím na QR kód na nově vytvořeném zařízení získáte QR kód a nastavíte první přepínač na "Legacy & BYOD".

Rozšířený pracovní profil AE: (vyžaduje Android 11 nebo vyšší) Zatímco výše zmíněný kontejner BYOD přináší firemní data na soukromé zařízení, rozšířený pracovní profil dělá totéž, ale pro zařízení ve vlastnictví společnosti. Vytváří stejný kontejner, ale dává správci o něco větší kontrolu nad zařízením, takže uživatel nemůže jednoduše odebrat MDM ze zařízení. Vytvořte zařízení v konzole a jako typ zařízení vyberte "AE Container (BYOD & Enahnced Work Profile)". Kliknutím na QR kód na nově vytvořeném zařízení získáte QR kód a nastavíte první přepínač na "Enhanced Work Profile". Tento QR kód lze naskenovat po resetování zařízení a šestinásobném klepnutí na obrazovku, jak je vysvětleno v metodě 1 v části Registrace AE.

Jak mohu přiřadit aplikace k zařízením Android Enterprise?

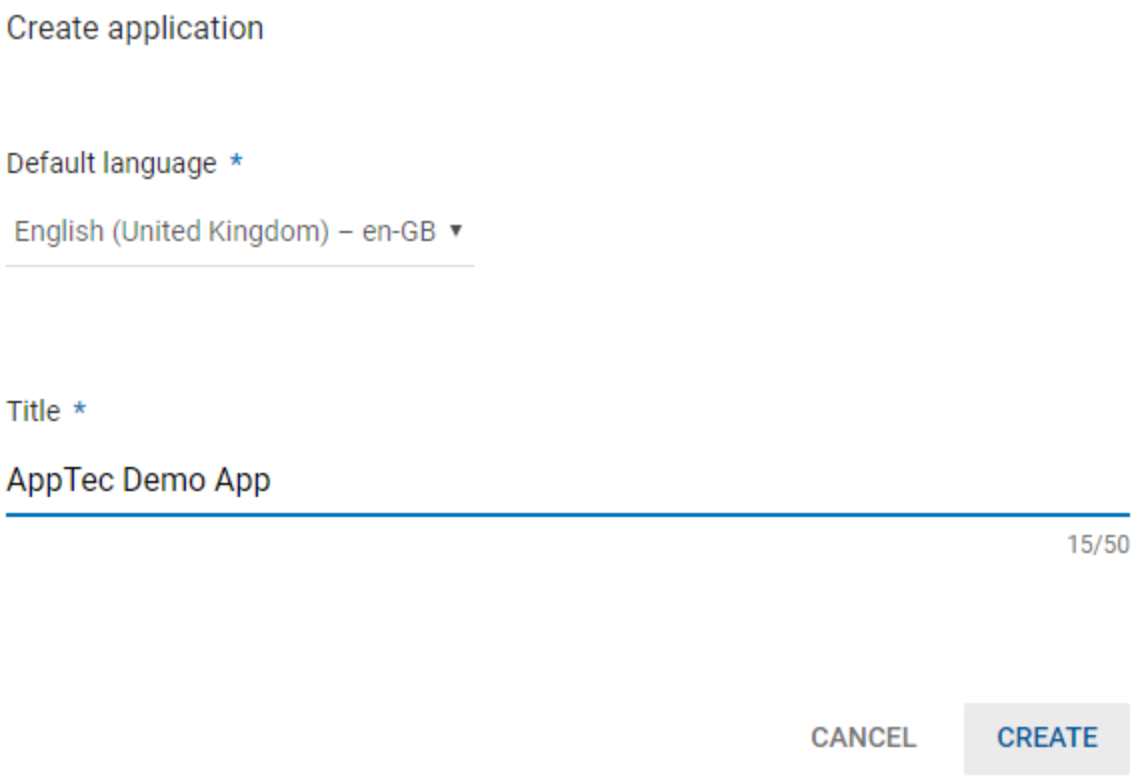
Nejprve musíte schválit aplikace, které chcete používat, v části Obecná nastavení → Správa aplikací → AE Play Store → Aplikace Play Store. Po schválení aplikace je můžete přiřadit do seznamu povinných aplikací → svého profilu kliknutím na "+" a výběrem aplikace na kartě "AE Play Store". Tím se aplikace automaticky stáhne a nainstaluje. V zařízení není vyžadován žádný účet Google a uživatel to nemusí potvrzovat ani povolovat.

Nahrávání vlastních aplikací do obchodu Google Play

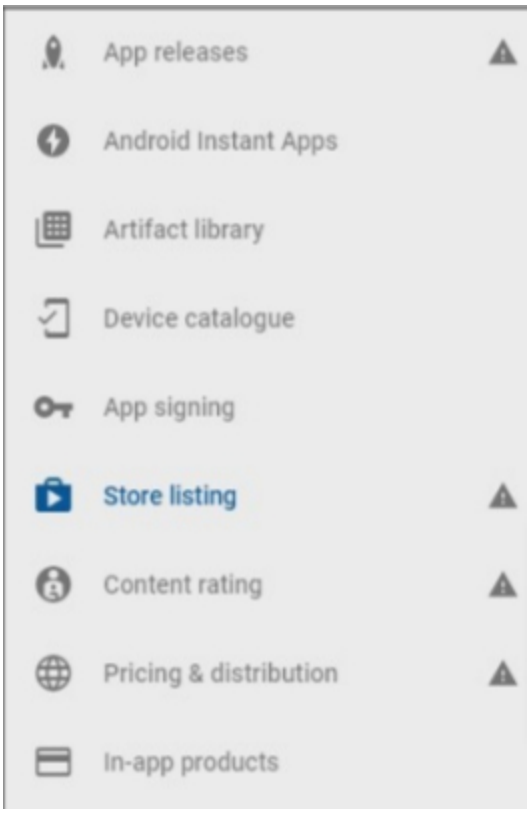
Do obchodu Google Play je možné nahrát vlastní aplikace. Tímto způsobem můžete využívat různé výhody, jako je mechanismus aktualizací Obchodu Play.

K tomu potřebujete vývojářský účet Google. Přihlaste se pomocí Konzoly Google Play(https://play.google.com/apps/publish).

Klikněte na možnost "Vytvořit aplikaci". Zvolte výchozí jazyk a název aplikace.



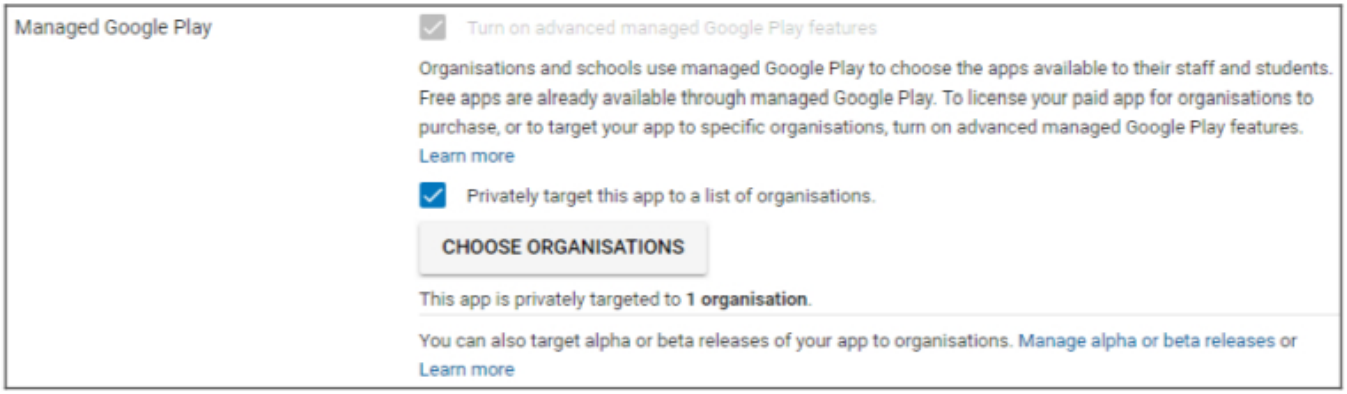
Na následující stránce budete vyzváni k zadání různých údajů o vaší aplikaci.



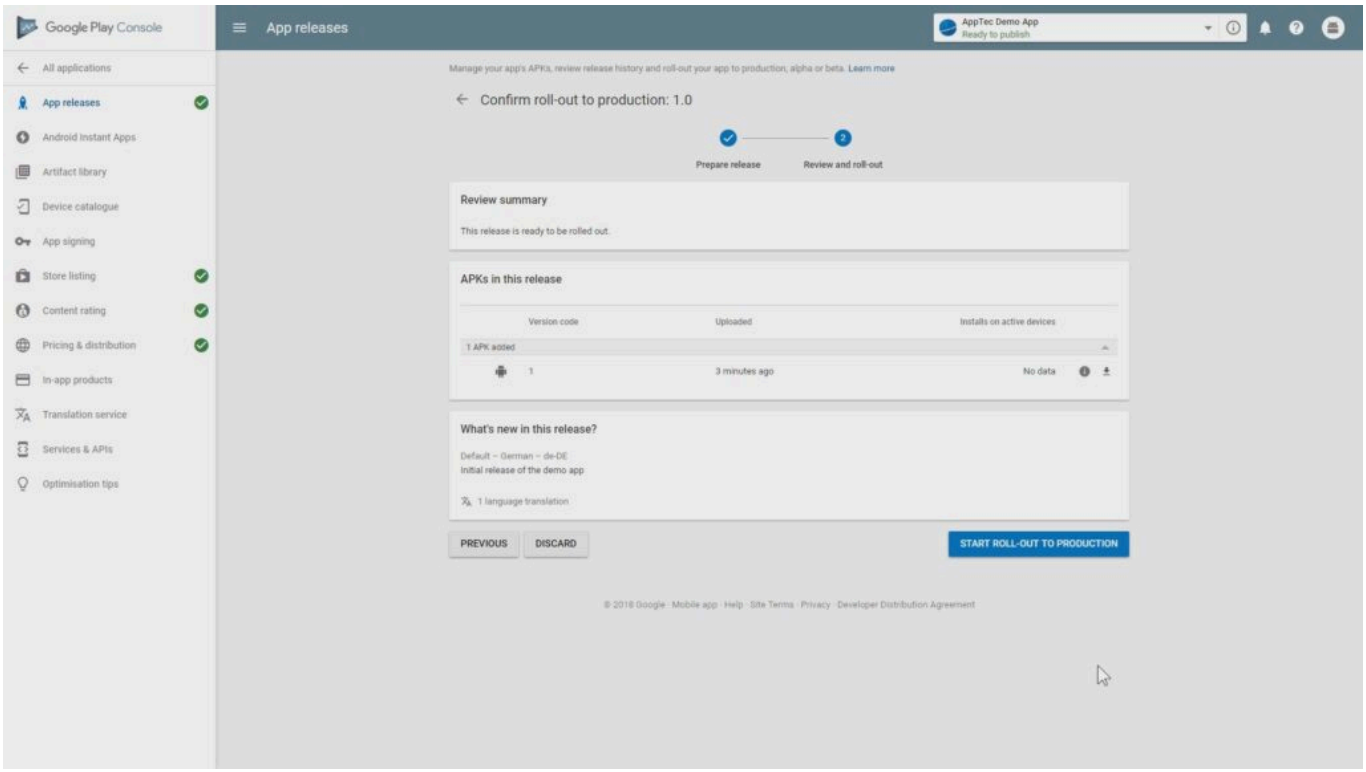
Po zadání všech údajů se na levé straně zobrazí různé symboly nápovědy.

Najeďte na ně, abyste viděli, které kroky zbývají, a postupujte podle nich v libovolném pořadí.

Poznámka: Ujistěte se, že jste zaškrtli dvě políčka u položky "Managed Google Play" v části "Pricing & Distribution". Jinak bude aplikace veřejná a bude k ní mít přístup každý. Ujistěte se také, že jste vybrali zemi pro distribuci.



Po dokončení všech kroků můžete přejít na "Vydání aplikace". Kliknutím na "Review" a "Start Roll-Out to Production" dokončíte návrh a aplikaci zveřejníte.



Nějakou dobu potrvá, než bude aplikace k dispozici v Obchodě Play. Po dokončení procesu můžete aplikaci vyhledat v obchodě Play for Work a schválit ji. Poté můžete aplikaci jednoduše přiřadit k zařízením pomocí konzoly EMM stejně jako u jiných aplikací.

Požadavky a instalace

Požadavky

Systémové požadavky

Virtuální zařízení je k dispozici ve formátu Open Virtualization Format (VMWare, VirtualBox, Citrix Xen Server) a jako komprimovaný soubor .vhdx (Hyper-V)*.

*Poznámka: Při použití technologie Hyper-V musí být počítač vytvořen s generací 1.

Virtuální disk má cílovou velikost 20 GB a počítač vyžaduje 4 GB paměti RAM.

Zařízení je založeno na Debianu 9 64bit.

Upgradujte importovaný počítač na nejnovější kompatibilitu (např. ve VMWare) a zkontrolujte, zda je typ operačního systému počítače správně nastaven v hypervizoru.

Licenční klíč

K úspěšné aktivaci a instalaci serveru potřebujete platný licenční soubor. Ten můžete získat přímo od AppTec360 a/nebo od příslušného prodejce.

Řešení IP adres a DNS

Zařízení AppTec360 musí být dosažitelné zařízením používajícím název hostitele, pro který je licence vydána.

Chcete-li zaregistrovat zařízení se systémem Windows 10, musíte také nastavit další subdoménu ve tvaru "enterpriseenrollment.", která bude směřovat na zařízení.

Certifikát SSL

Protože všechna připojení k zařízení a ze zařízení musí být zabezpečena pomocí protokolu SSL, potřebujete pro název hostitele platný certifikát vydaný certifikační autoritou, které zařízení důvěřuje. Soukromý klíč k certifikátu musí být nahrán bez ochrany heslem. Ve většině případů je vyžadován zprostředkující certifikát certifikační autority, aby zařízení rozpoznala certifikát serveru.

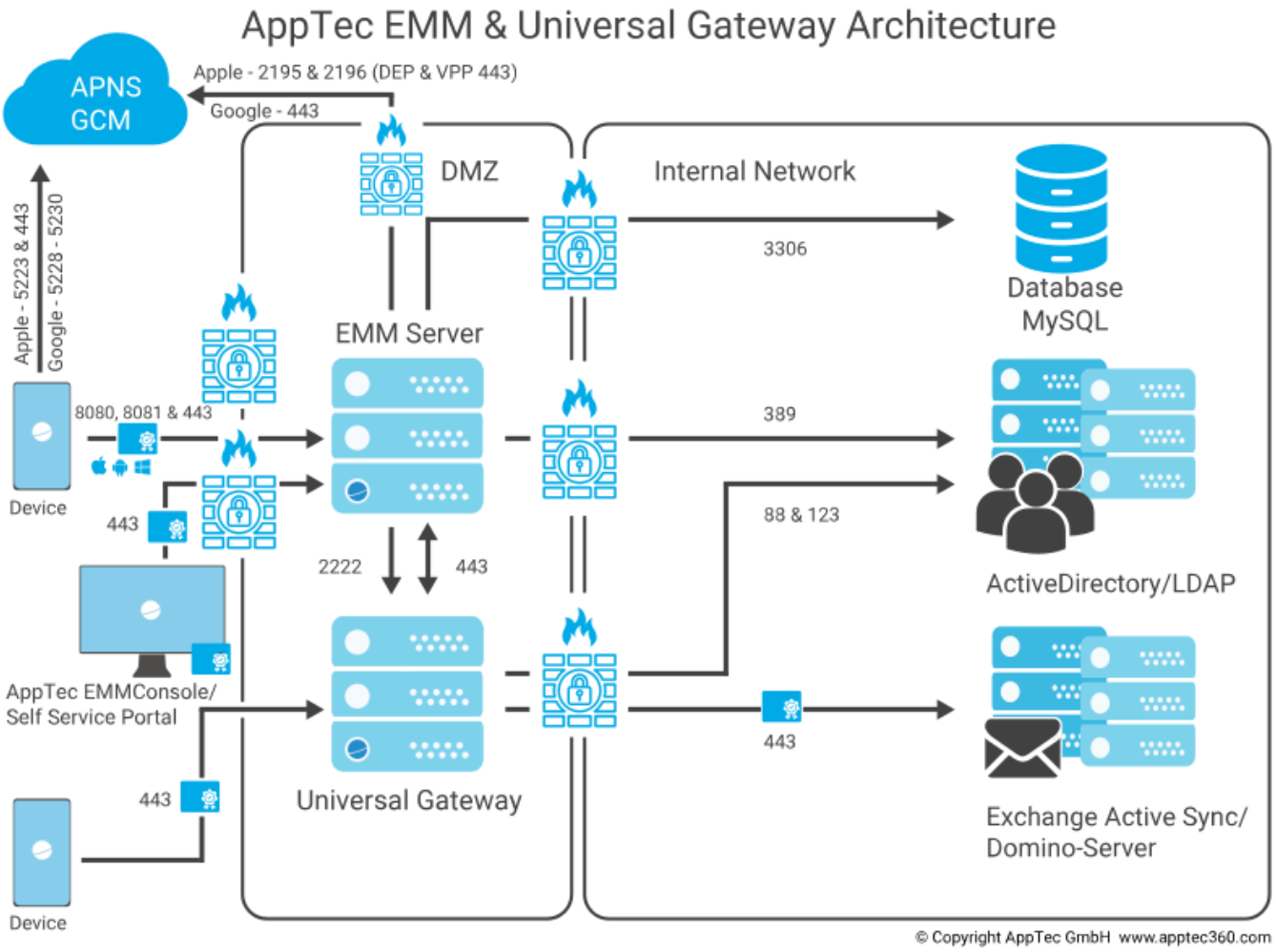
Zařízení se systémem Windows 10 budou vyžadovat specifický certifikát pro subdoménu enterpriseenrollment.

Od verze zařízení 202104 můžete také používat certifikáty Let's Encrypt, které se generují automaticky (popsáno v druhém kroku - certifikát SSL).

Server SMTP

Aby mohl AppTec360 EMM odesílat e-maily (např. pro registraci zařízení a ověření účtu), je zapotřebí e-mailový server a/nebo e-mailová přenosová linka.

Pravidla brány firewall



Toto schéma ukazuje, které připojení je nutné v závislosti na tom, jaké služby chcete používat.

Podrobnější popis najdete v tabulce na následující straně.

Jakékoli (externí/zařízení)	→	**AppTec360 Appliance / emmconsole.com**
Porty	443	Správa, podnikový AppStore a komunikace se systémem Windows Phone
	8080	Komunikace se systémem Android a iOS
	80	První nastavení aplikace Let´s Encrypt. Poté používá 443.
Jakékoli (zařízení)	→	**Jakýkoli (externí)**
Porty	5223, 443	Služba Apple Push Service, musí být dostupná bez proxy serveru, 443 jako Fallback, viz https://support.apple.com/en-us/HT203609.
	5228-5230	Služba Android Push Service (FCM), musí být dostupná bez proxy serveru.
Zařízení AppTec360	→	**Řadič domény**
Porty	389, (LDAPS 636)	Synchronizace uživatelů s LDAP
Zařízení AppTec360	→	**Jakýkoli**
Přístav	443	Používá se pro službu Android Push Service (GCM) Vyhledávání v AppStore / Obchodě Play
Zařízení AppTec360	→	**emmconsole.com**
Porty	443	Aktualizace zařízení AppTec360, generování certifikátu APNS
Zařízení AppTec360	→	**Síť Apple (17.0.0.0/8)**
Porty	2195, 2196	Služba Apple Push Service a služba zpětné vazby
	443	DEP A VPP

Aktualizace zabezpečení

Operační systém Debian je třeba pravidelně aktualizovat, abyste získali nejnovější bezpečnostní opravy. Ujistěte se však, že neprovádíte upgrade na novější hlavní verzi Debianu ručně. Až bude AppTec360 EMM kompatibilní s novější hlavní verzí, přidáme způsob upgradu v aktualizaci zařízení.

Výchozí hesla virtuálního zařízení

Přihlášení uživatele (Přihlášení roota je zakázáno. Pro administrátorské úlohy použijte "sudo")

apptec

Přihlašovací heslo

apptec

Kořenový uživatel MySQL

root

Kořenové heslo MySQL

apptec

Výchozí uživatel MySQL

AppTec

Výchozí uživatelské heslo MySQL

AppTec

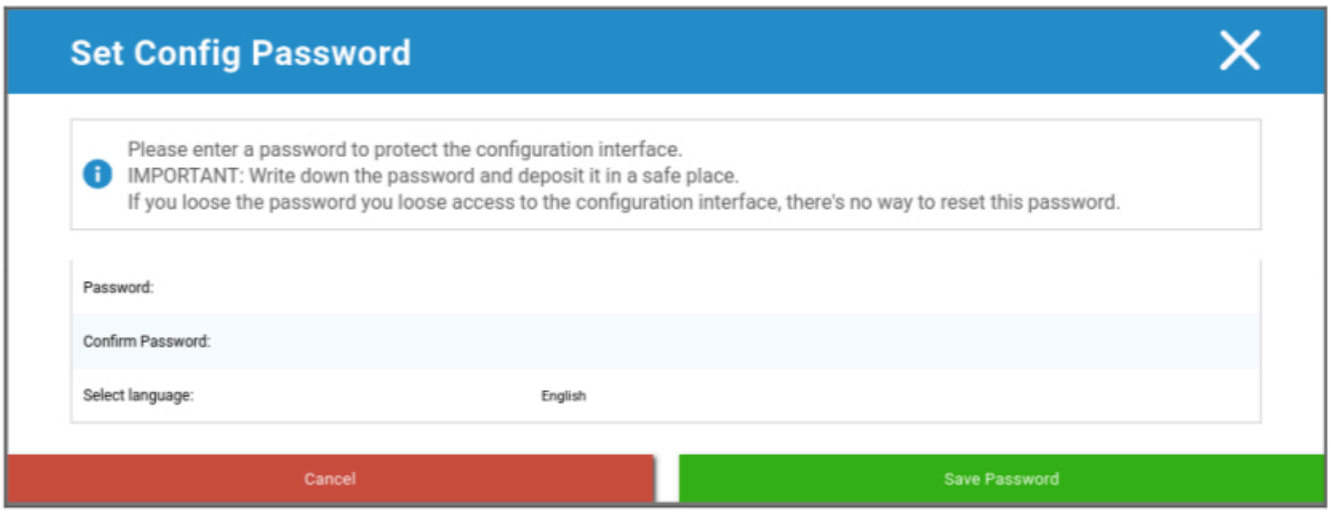
Konfigurace virtuálního zařízení

Důležité: Před zahájením konfigurace virtuálního zařízení by mělo být rozlišení displeje nastaveno alespoň na 1280 x 800 pixelů.

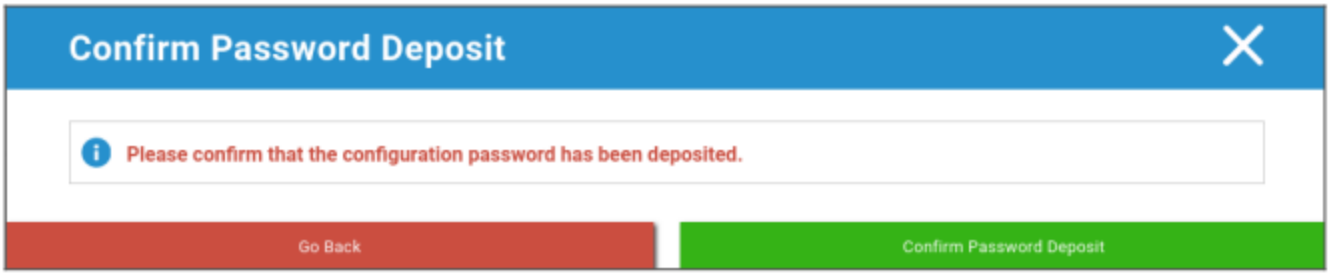
Po dlouhém přihlášení ke spotřebiči by se měl Firefox automaticky spustit a zobrazit konfigurační rozhraní.

Příprava

Nejprve je třeba zadat heslo pro konfigurační rozhraní. Toto heslo se používá k šifrování všech informací a souborů zadávaných v konfiguračním rozhraní. Zde můžete také nastavit jazyk, ve kterém se má rozhraní zobrazovat (lze změnit později).

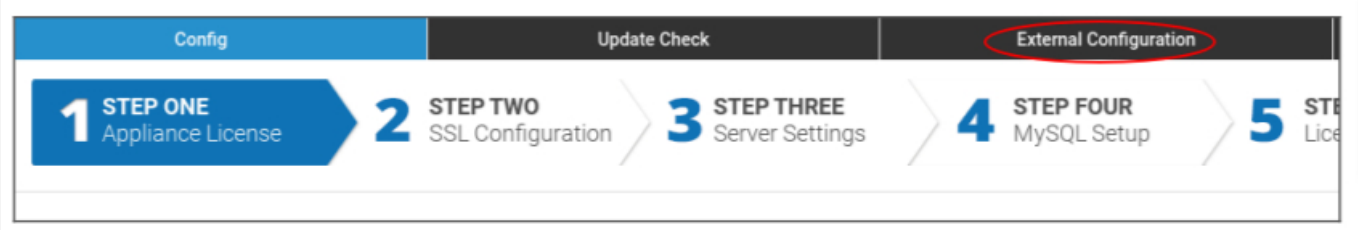


Heslo může resetovat pouze podpora AppTec360, takže si ho uložte na bezpečné místo a potvrďte nadcházející vyskakovací okno.



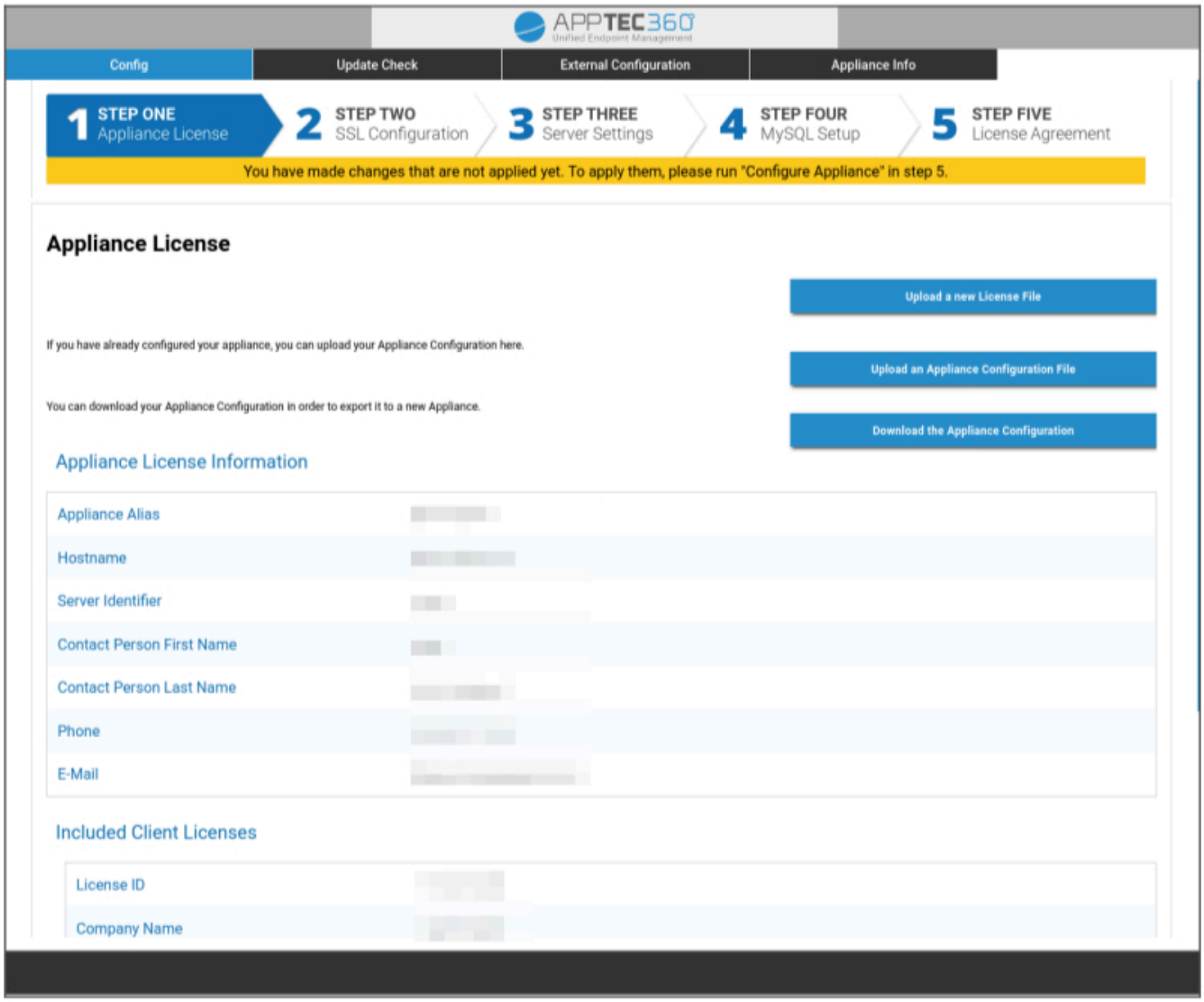
Konfigurace z externího hostitele

Chcete-li usnadnit proces nastavení, můžete konfigurační stránku zpřístupnit ze vzdáleného přístupu. Postupujte podle pokynů v části "Konfigurace z externího hostitele".



První krok – Licence spotřebiče

1. Nahrajte prosím licenční soubor, který jste obdrželi od společnosti AppTec.
2. Pokud byl licenční soubor úspěšně nahrán, zobrazí se informace o licenci spotřebiče jako na obrázku níže.



Druhý krok – certifikát SSL

Můžete použít automatické nastavení certifikátu pomocí služby Let's Encrypt nebo si certifikáty zajistit sami (více informací naleznete v části SSL-Certifikát).

Automatické

Certifikát bude automaticky vygenerován pomocí služby Let's Encrypt.

AppTec360 EMM používá pro ověření domény výzvu HTTP-01, což znamená, že pro první žádost o certifikát musí být otevřen port HTTP z internetu. Následné žádosti o obnovení mohou být ověřovány prostřednictvím protokolu HTTPS.

Přepněte přepínače na možnost "Automaticky (Let's Encrypt)" a stiskněte tlačítko "ULOŽIT HODNOTY". Certifikát bude automaticky vyžádán při použití konfigurace v pátém kroku - Licenční smlouva. Certifikát bude v případě potřeby automaticky obnoven a pokud se blíží vypršení platnosti certifikátu (což znamená, že se obnovení mohlo nezdařit), obdržíte e-mail.

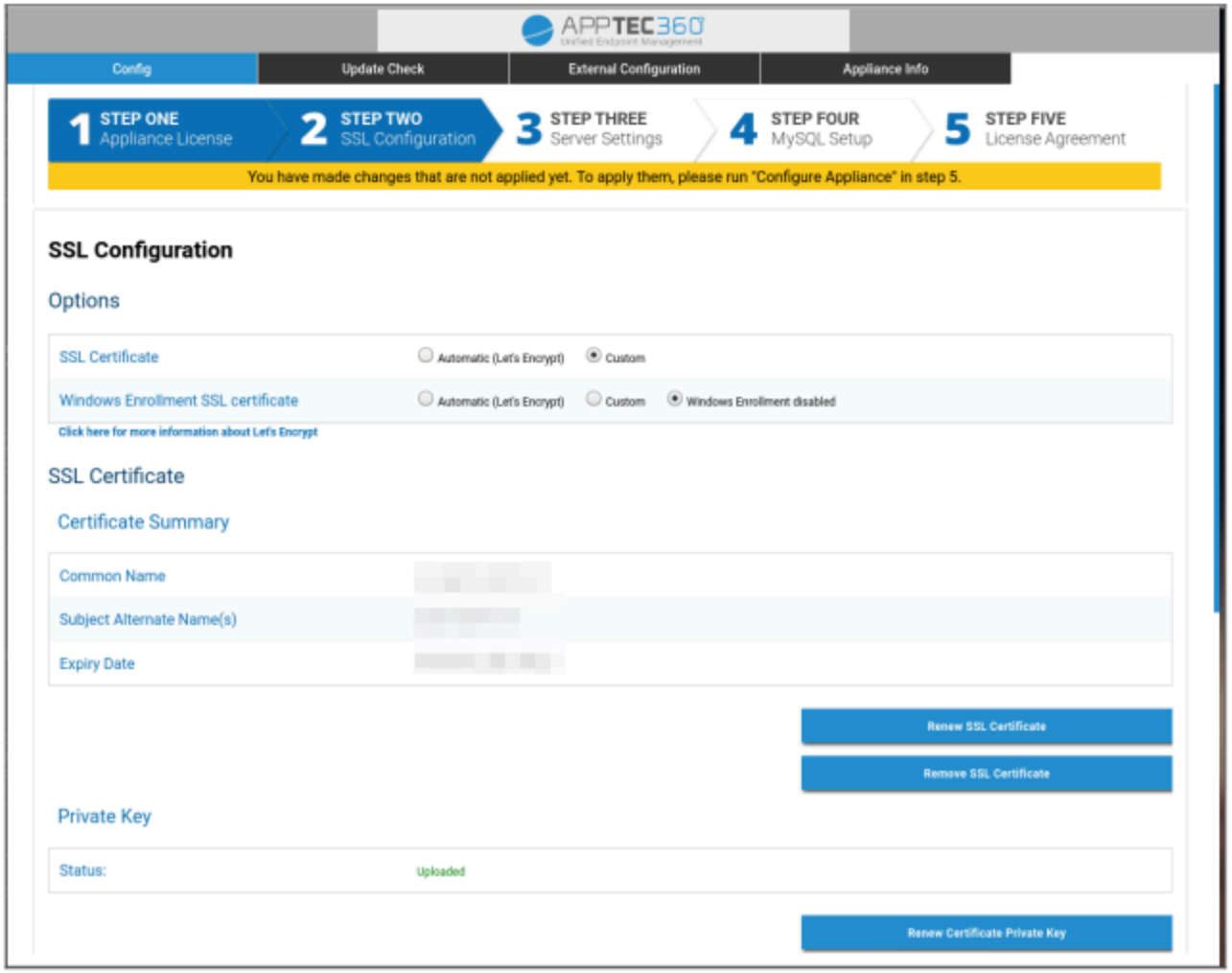
Vlastní

1. Nahrajte certifikát SSL pro licencovaný název hostitele. Hostitelský název můžete zobrazit v prvním kroku - Licence spotřebiče.

2. Nahrajte také soukromý klíč k certifikátu a v případě potřeby i zprostředkující certifikát.

Důležité: Klíč nesmí být chráněn heslem. Pokud ano, před odesláním heslo odstraňte.

Tip: Pokud chcete používat také zařízení se systémem Windows 10, musíte povolit "Certifikát SSL pro zápis do systému Windows" a nahrát certifikát, soukromý klíč a zprostředkující certifikát pro subdoménu (popsáno v části Nahrání adresy IP a rozlišení DNS) v dolní části stránky.



Třetí krok – Nastavení serveru

1. Zadejte prosím globální e-mailovou adresu podpory. Tato adresa bude použita v e-mailech zasílaných uživatelům, aby věděli, na koho se obrátit v případě jakýchkoli problémů s jejich zařízením.
2. Zadejte nastavení e-mailu, které bude systém používat k odesílání e-mailů. Nastavení bude použito k odesílání e-mailů uživateli a také k odesílání hlášení o chybách a požadavků na funkce na adresu"support@apptec360.com". Po uložení nastavení e-mailu je třeba je ověřit kliknutím na "Test E-Mail Configuration" a následováním pokynů.

Čtvrtý krok – Nastavení MySQL

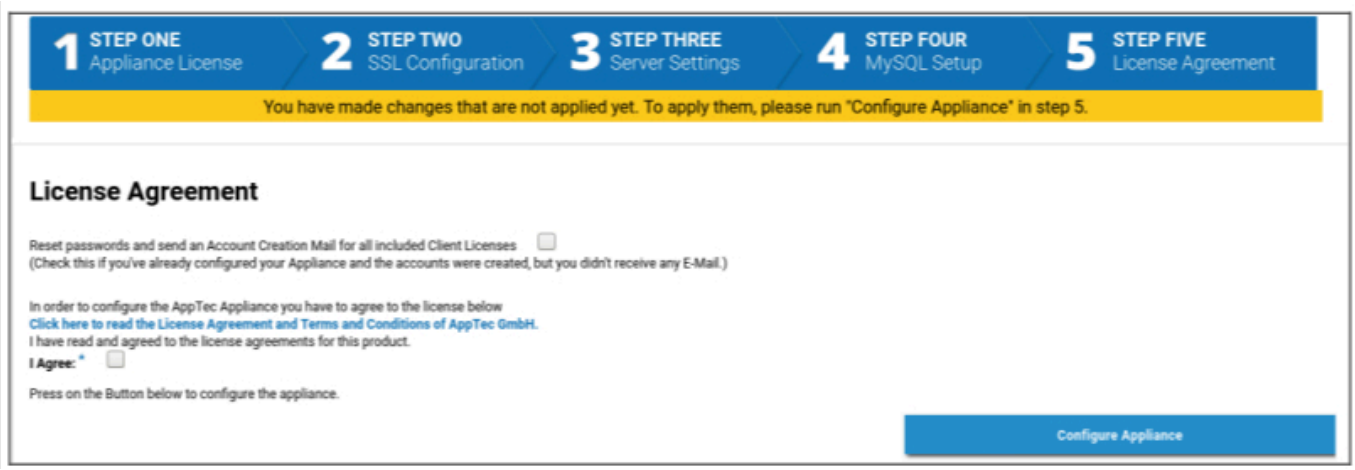
1. Pokud chcete používat interní databázi, můžete tento krok přeskočit. V opačném případě můžete zadat informace o připojení k externímu databázovému serveru.


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)

Pátý krok – Licenční smlouva

1. Přečtěte si licenční smlouvu.
2. Zaškrtněte políčko "I Agree" (Souhlasím) a stiskněte tlačítko "Configure Appliance" (Konfigurace spotřebiče), čímž provedete nastavení.

Tip: Při každé změně nastavení v 5 krocích je třeba spustit "Konfiguraci zařízení", aby se nastavení použilo.



Gratulujeme!

Dokončili jste konfiguraci virtuálního zařízení.

Na adresu, kterou jste zadali pro získání licence (viditelnou v části "Zahrnuté klientské licence" v prvním kroku - Licence spotřebiče), byl odeslán e-mail s heslem.

Nyní se můžete přihlásit do konzoly pomocí tohoto hesla a e-mailové adresy, na kterou jste ho obdrželi.

Chcete-li se přihlásit do konzoly, zadejte do adresního řádku prohlížeče název hostitele konzoly.

Název hostitele vašeho spotřebiče najdete v části První krok - Licence spotřebiče.

Řešení problémů

1. Při konfiguraci spotřebiče v pátém kroku - Licenční smlouva - jste neobdrželi e-mail:

Ujistěte se, že nastavení e-mailu ve třetím kroku - Nastavení serveru je správné. Pro opětovné zaslání hesla zaškrtněte "Resetovat hesla a odeslat mail pro vytvoření účtu pro všechny zahrnuté klientské licence" v kroku pět - Licenční smlouva před opětovným spuštěním "Konfigurace zařízení".

2. Během konfigurace v pátém kroku - Licenční smlouva - jste obdrželi chybu týkající se služby Let's Encrypt:

Ujistěte se, že je spotřebič dosažitelný pomocí názvu domény na portu 80. Let's encrypt také zapisuje log do "/var/log/letsencrypt", což může pomoci při dalším řešení problémů.

Bezpečnostní doporučení

Pro zabezpečení zařízení AppTec360 se doporučuje provést následující kroky.

Nejedná se o úplný soubor pokynů, ale pouze o doporučení pro základní konfiguraci.

- Změna hesla uživatele AppTec360
- Změňte heslo pro uživatele MySQL "root" a "AppTec" a aktualizujte čtvrtý krok - Nastavení MySQL podle toho.
- Změna výchozího portu serveru SSH
- Zablokujte port 80 v konzoli a zakažte příchozí provoz HTTP, používejte pouze HTTPS. Po konfiguraci je možná i externí konfigurace přes HTTPS.
- Omezení přístupu k rozhraní pro správu pouze na určité IPS v dolní části třetího kroku - Nastavení serveru.
- Konfigurace brány firewall

Obecná nastavení

Přehled účtů

Informace o účtu

Přehled

Zde si můžete prohlédnout přehled svého účtu AppTec360.

Název společnosti	Název vaší společnosti
Datum vytvoření	Datum vytvoření účtu
Typ licence	Paid = placená licence Zdarma = neplacená licence Poznámka: Účty na zařízení OnPremise se z technických důvodů vždy zobrazují jako zaplacené.
Identifikátor klienta	Identifikátor vašeho účtu (NEjedná se o vaše zákaznické číslo)
Datum vypršení platnosti licence	Datum vypršení platnosti licence AppTec360
Licence ContentBox	Zdarma = bezplatná licence pro 25 zařízení Placená = placená licence pro x zařízení
Spouštěcí zařízení	Zobrazuje, zda můžete použít vlastní spouštěč pro systém Android.
Zařízení	Počet aktuálně používaných / celkový počet licencí
Kontaktní osoba	Poskytnutá kontaktní osoba
Telefon	Poskytnuté telefonní číslo
eMail*	Poskytnutá e-mailová adresa
Kořenový uživatel	Kořenoví uživatelé, kteří se mohou přihlásit
Verze softwaru	Aktuální verze softwaru

**Poznámka: Zde uvedená e-mailová adresa je ta, kterou jste zadali při registraci účtu. Na jejím základě se ve stromu uživatelů/zařízení vytvoří uživatel, kterého lze upravit. Úpravou tohoto uživatele se změní e-mailová adresa, kterou musíte použít pro přihlášení, ale nezmění se informace v přehledu účtů. .*

Hlášení chyb

Hlášení o chybě lze odeslat přímo na podporu a nahlásit v něm problémy nebo chyby a obsahuje informace a protokoly o vašem účtu a nastavení.

Předmět	Předmět hlášení chyby. Pokud chcete přidat tuto hlášku k existující hlášce podpory, uveďte číslo hlášky.
Očekávané chování	Podrobně popište, co jste udělali a co jste očekávali, že se stane.
Skutečné chování	Podrobně popište, co se přesně stalo. Chybové hlášení uveďte PŘESNĚ. Pomůže také, když do přílohy přidáte snímky obrazovky.
V jakém čase se problém vyskytl?	Uveďte prosím přesný čas, kdy jste obdrželi konkrétní chybovou zprávu/problém. V nejlepším případě uveďte i sekundy, např. 18:55:27.
Lze problém opakovat? Pokud ano, jak (podrobně)?	Podrobně popište, jak můžete problém reprodukovat.
Fungovala tato funkce dříve podle vašich představ? Pokud ano, do kdy?	Pokud nevíte, nechte prázdné.
Byly v systému provedeny nějaké konkrétní změny, než se tento problém objevil? Pokud ano, jaké změny (podrobně)?	Vždy uveďte, jaká byla vaše poslední změna nebo akce předtím, než se problém objevil, i když si myslíte, že je to irelevantní.
V případě potřeby: Kterých modelů zařízení a verzí operačního systému se to týká?	Vždy uvádějte přesný název verze operačního systému (např. iOS 14.7.1 nebo Android 11).
V případě potřeby: Jaká je veřejná IP adresa a/nebo sériové číslo zařízení?	Uveďte alespoň jedno, i když se to týká všech zařízení.
Zahrnout soubory protokolu	Zaškrtnutím této možnosti odešlete soubor protokolu s hlášením chyby. Doporučujeme to udělat.
Získání aktuálního stavu VPP od společnosti Apple a zahrnutí do hlášení o chybě	Obsahuje informace o přidělování licencí VPP. Aktivujte ji pouze v případě, že vás o to požádá podpora nebo pokud se váš problém týká VPP.
Příloha	Přiložte jakýkoli soubor, který by mohl být užitečný (např. snímky obrazovky s chybovou zprávou).

Požadavek na funkci

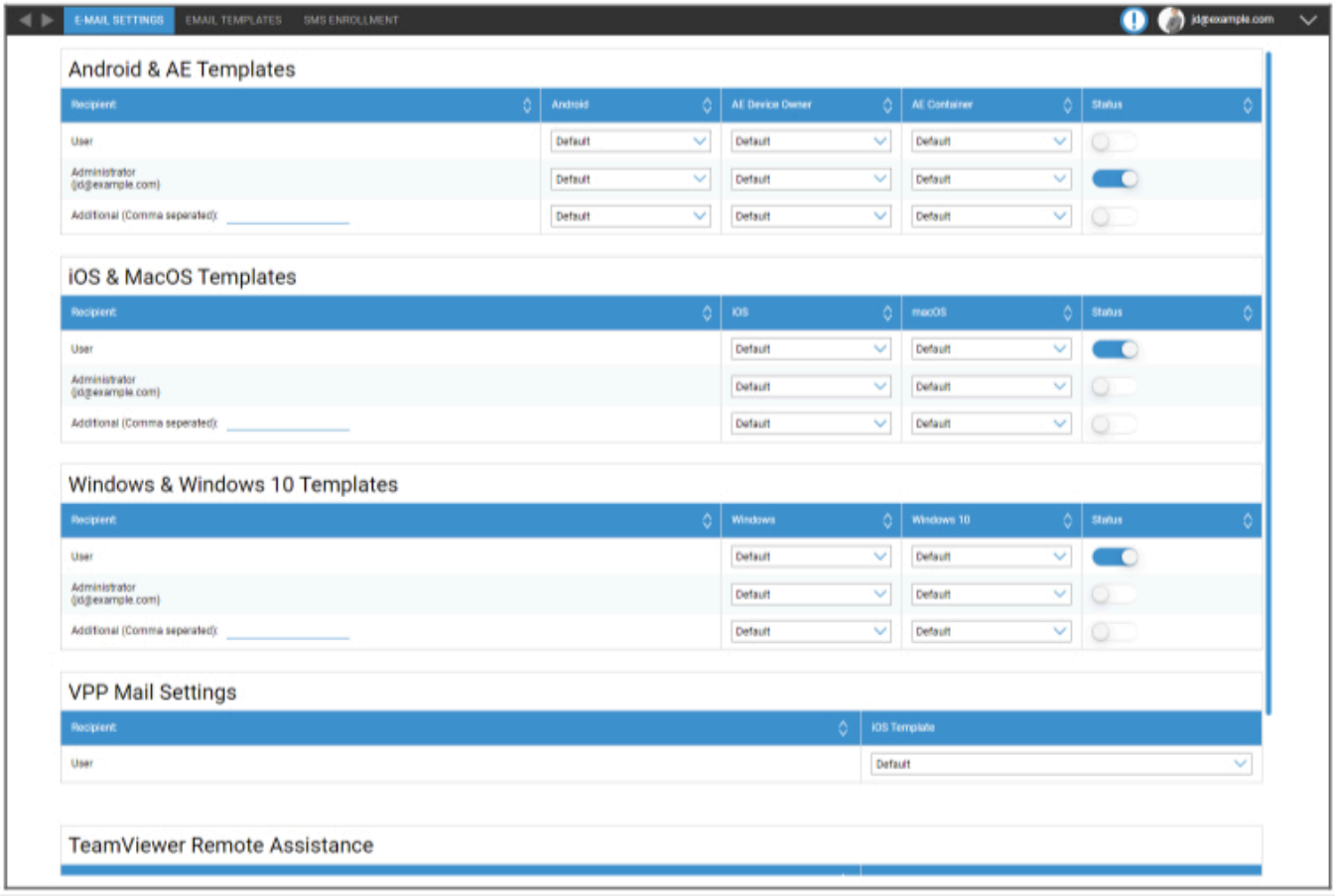
Požadavek na funkci lze zaslat přímo na podporu. Může obsahovat požadavek na konkrétní funkci nebo vylepšení pro

Souhrn	Stručné shrnutí vašeho problému
Popis	Podrobný popis vašeho problému, buďte co nejkonkrétnější.
Příloha	Připojení souborů k hlášení chyby

Globální konfigurace

Nastavení elektronické pošty

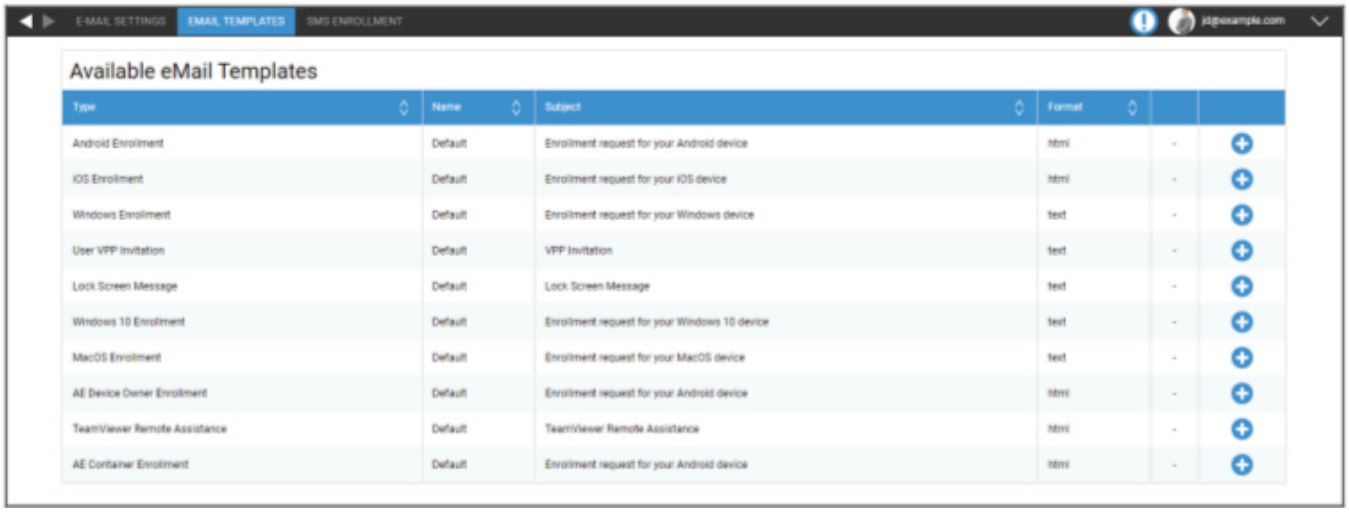
Zde můžete definovat, komu bude zaslán e-mail při generování žádosti o zápis a jaká textová šablona bude pro tento e-mail použita.



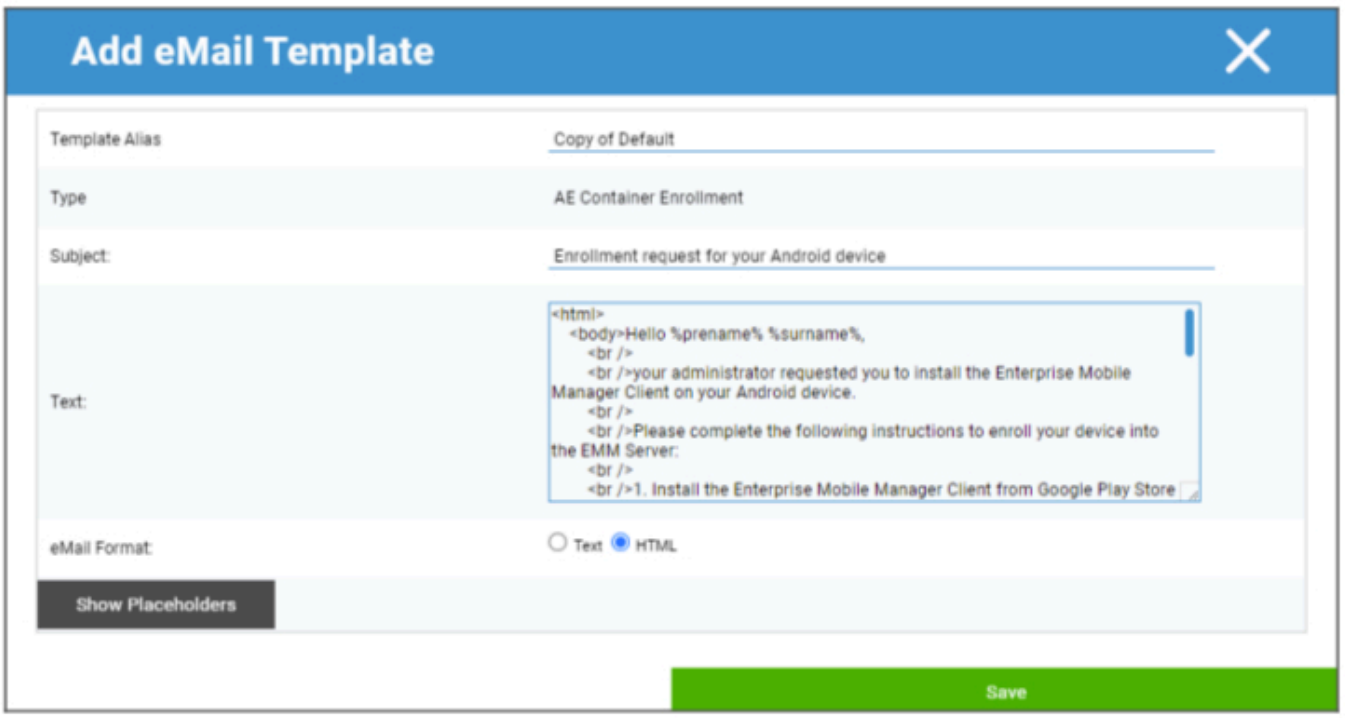
Šablony elektronické pošty

Zde můžete vytvářet a upravovat šablony pro různé scénáře. Ty mohou být v normální textové podobě nebo ve formátu HTML. V HTML můžete lépe kontrolovat formátování textu.

Výchozí šablony nelze upravovat ani mazat.



Můžete také použít zástupné znaky jako proměnnou, která bude automaticky nahrazena. Při úpravách klikněte na "Zobrazit zástupné symboly", abyste viděli dostupné zástupné symboly. Různé kategorie mají různé Zástupné symboly.



Zápis SMS

Zde můžete zadat/aktivovat proces registrace SMS.

(Výchozí: deaktivováno)

Zobrazí se také informace o tom, kolik kreditů SMS je ještě k dispozici.

SMS kredity je třeba zakoupit samostatně.

Ochrana osobních údajů

Přístup k GPS

Zde můžete chránit zobrazení GPS pro každé zařízení pomocí 1 nebo 2 hesel (princip čtyř očí). Při každém pokusu o přístup k poloze zařízení budete vyzváni k zadání hesla (hesel).

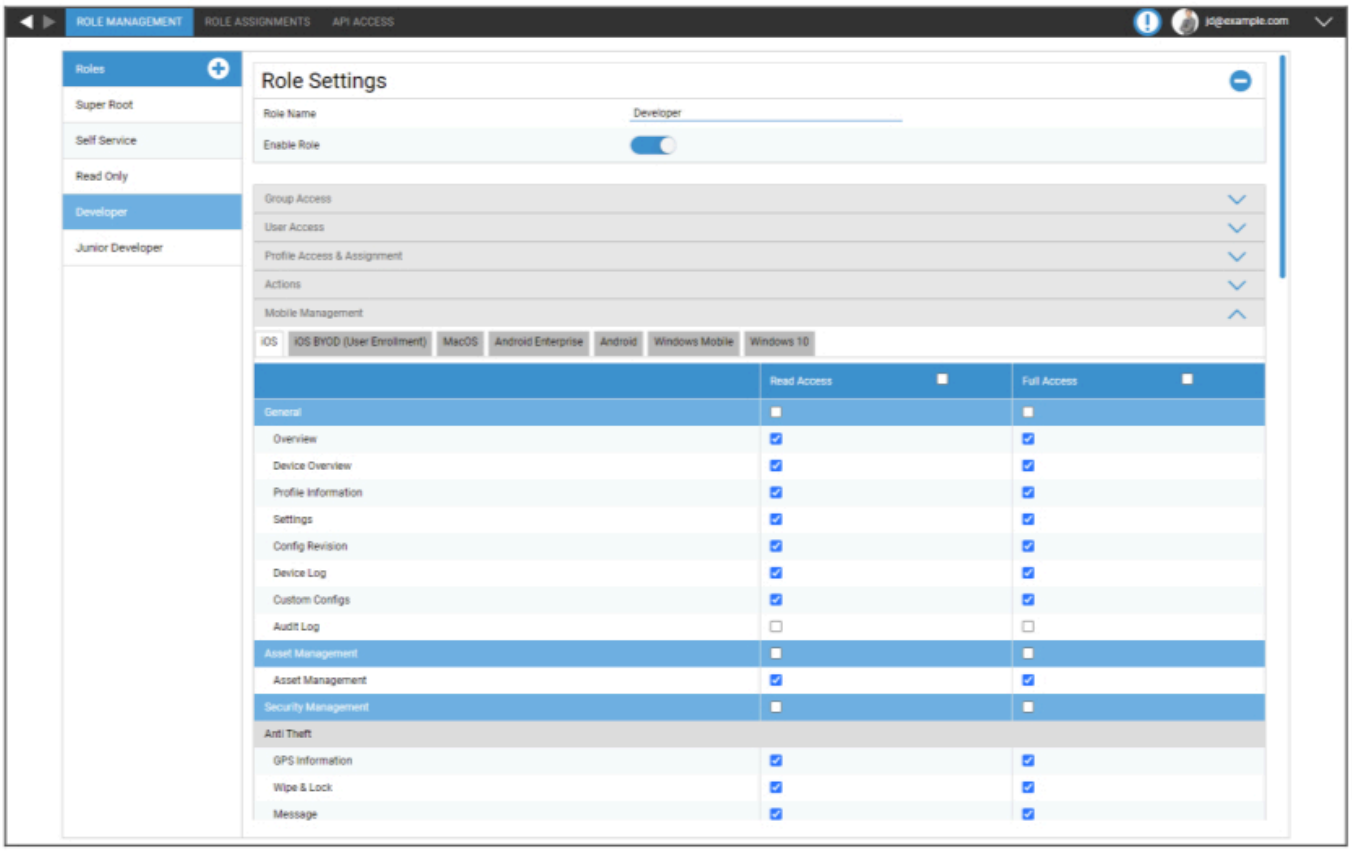
Omezení přístupu k nastavení GPS	Vypnuto = funkce je vypnutá a pro lokalizaci není vyžadováno heslo.
	Zapnuto = funkce je zapnutá a pro lokalizaci je vyžadováno heslo.
Metoda ochrany	Použít jedno heslo = použít jedno heslo pro lokalizaci
	Použít dvě hesla = použít dvě hesla pro lokalizaci
Zadejte heslo (1)	Zadejte zvolené heslo
Opakování hesla (1)	Opětovné zadání zvoleného hesla
volitelně: Zadejte heslo 2	Zadejte 2. zvolené heslo
volitelně: Opakujte heslo 2	Znovu zadejte 2. zvolené heslo

Poznámka: Po nastavení přístupového kódu (kódů) jej musíte zadat ještě jednou, než bude zcela povolen.

Přístup založený na rolích

Správa rolí

Role definují, co může uživatel vidět a dělat, když se přihlásí do konzoly pro správu. To vám umožní vytvořit uživatele, kteří se mohou přihlásit, ale mají omezené funkce.



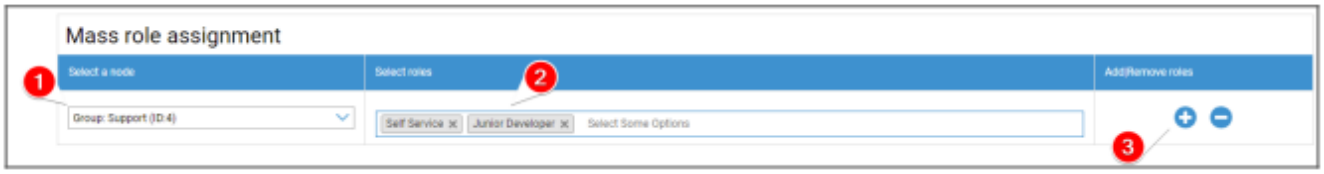
Role Super Root je výchozí rolí, která má vždy možnost vše zobrazit a změnit. Nelze ji změnit ani odstranit. Samoobslužná role vidí pouze své vlastní uživatele a zařízení. Můžete kombinovat samoobsluhu a vlastní roli a např. umožnit uživatelům přihlašovat se a registrovat zařízení samostatně a pouze pro svého uživatele.

Vlastní role lze ručně povolit nebo zakázat. Nové role jsou ve výchozím nastavení zakázány. Uživatelé s vypnutou rolí pracují, jako by tuto roli neměli. To umožňuje např. dočasně omezit dané roli její akce.

Všechna oprávnění jsou rozdělena na "Přístup ke čtení" a "Plný přístup". Přidělení Přístupu ke čtení roli umožňuje zobrazit konkrétní část konzoly. Přidělení Plného přístupu umožňuje Roli vidět a měnit konkrétní část konzoly.

Přiřazení rolí

Zde získáte přehled o všech uživatelích, kteří mají určitou roli, a uvidíte, jakou mají roli. Můžete zde také přiřadit roli uživatelům nebo celým skupinám:

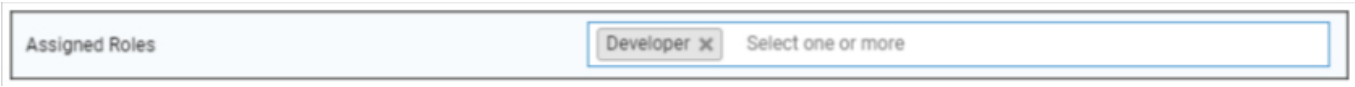


1. Vyberte, pro kterou skupinu nebo uživatele chcete přidat nebo odebrat role. Můžete vybrat buď jednoho uživatele, nebo skupinu. Při výběru skupiny se vaše změna dotkne všech uživatelů v rámci této skupiny a všech uživatelů podskupin ve vybrané skupině.
2. Vyberte roli, kterou chcete přidat nebo odebrat. Můžete vybrat jednu nebo více rolí.
3. . Select what operation you want to perform. Clicking the “+” adds the selected roles if the user(s) did not have them already. Clicking the “-” removes the selected roles from the user(s). If you add roles to a user which did not yet have any role, it will automatically enable “Can Login” for the user.
4. Uložením proces dokončíte. Uživatelé, kteří dříve neměli žádnou roli a měli zakázáno "Může se přihlásit", automaticky obdrží e-mail s odkazem pro nastavení hesla.

Pod přiřazením hromadné role najdete přehled přiřazených rolí. Můžete zde také ručně změnit role pro konkrétní uživatele.

Přiřazení role

Chcete-li uživateli přiřadit roli, musíte přejít do Správy mobilních zařízení, kde najdete strom skupin, uživatelů a zařízení. Upravte uživatele a přiřaďte mu roli. Případně můžete výše uvedený způsob použít i pouze pro jednotlivé uživatele.



Přístup k rozhraní API

Přístup k API REST AppTec360

Rozhraní AppTec360 REST API vyžaduje autentizační token (klíč API) a soukromý klíč, které je třeba vygenerovat v konzoli pro správu.

Za tímto účelem se přihlaste do systému AppTec360 EMM a přejděte na stránku

Obecná nastavení → Přístup na základě rolí → Přístup k rozhraní API a přidejte nový klíč.

Je třeba vybrat uživatele, jehož oprávnění se budou vztahovat na klíč API.

Soukromý klíč lze stáhnout pouze jednou. Po zahájení stahování se klíč vymaže a tlačítko "Stáhnout" zmizí.

Pokud ztratíte soukromý klíč, musíte si vygenerovat nový klíč API.

Obecná pravidla

- Rozhraní REST API je k dispozici pod základní adresou URL:

/public/external/api

- Všechny požadavky musí být odeslány prostřednictvím POST.
- Rozhraní REST API podporuje pouze požadavky přes protokol HTTPS.
- Žádosti musí obsahovat následující záhlaví:

Název záhlaví	Hodnota záhlaví	Popis
Typ obsahu	application/json	pevný
auth	123...xyz	Klíč API na kartě "Přístup k rozhraní API"
podpis	Podpis v kódování Base64	Podpis užitečného zatížení generovaného pomocí soukromý klíč na kartě "Přístup k rozhraní API"

- Tělo požadavku musí být kódovaný objekt json, který musí obsahovat následující hodnoty:

Pole	Příklad pole Hodnota	Popis
api	v2/device/listdevices	Název rozhraní API
čas	1529662725	Časové razítko Unix (UTC) klientského počítače. Maximální povolený časový rozdíl mezi klientem a serverem je 30 minut.

- V případě úspěchu vrátí rozhraní API požadovaná data (viz dotazy níže) a stavový kód HTTP 200.
- Pokud dojde k chybě, bude stavový kód HTTP v závislosti na chybě mezi 4xx a 5xx a objekt odpovědi bude obsahovat pole s klíčem "errors", které obsahuje seznam chybových zpráv, které lze přečíst.
- Pokud pro zařízení neexistují žádná odpovídající data, vrátí se prázdné pole.
- Pokud ID zařízení neexistuje, budou jeho návratová data nulová.

Příklad žádosti

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]}}

Dotazy

Seznam všech zařízení

Funkčnost:
API URI: v2/device/listdevices
Povinné parametry: žádné
Nepovinné parametry: žádné

Příklad těla požadavku

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

Příklad těla odpovědi

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

Získání seznamu poloh (GPS)

Funkčnost:
API URI: v2/device/listposition
Povinné parametry: "ids" - pole ID zařízení
Nepovinné parametry: žádné

Příklad těla požadavku


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


Příklad těla odpovědi


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

Získat mapu aktiv

Funkčnost:
Vrátí seznam všech uložených možných aktiv, která mají být vyžádána pomocí funkce Get any asset data.
Pro vyžádání dat můžete použít buď lidsky čitelný formulář, nebo značku aktiva.
URI API: v2/device/getassetmap
Povinné parametry: žádné
Nepovinné parametry: žádné

Příklad těla požadavku

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

Příklad těla odpovědi

Tato odpověď byla zkrácena pro lepší srozumitelnost.

{
"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": []
}

Získání jakýchkoli údajů o majetku

Funkčnost:
URI API: v2/device/getassetdata
Povinné parametry:
"Nepovinné parametry:
"assetkeys" - Klíče dat aktiv, které se mají vrátit. Pokud není zadáno, budou vrácena všechna dostupná data aktiv
. Seznam klíčů aktiv můžete získat pomocí funkce Get asset map.

Příklad těla požadavku


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


Příklad těla odpovědi


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

Příklad kódu v jazyce Python3

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

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

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

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

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

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

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

Konfigurace Apple

Certifikát APNS

Zde můžete nahrát certifikát APNS. Ten je nutný pro správu zařízení se systémy iOS a MacOS.

Poznámka: Certifikát APNS je platný pouze jeden rok. Před vypršením jeho platnosti je třeba jej obnovit. Proces obnovení je totožný s procesem vytvoření (viz níže) a trvá jen několik krátkých minut.

Pokud zapomenete obnovit tuto registraci včas, nemůžete provádět změny v již zaregistrovaných zařízeních. **a budete muset všechna zařízení zaregistrovat znovu.**.

Krok 1

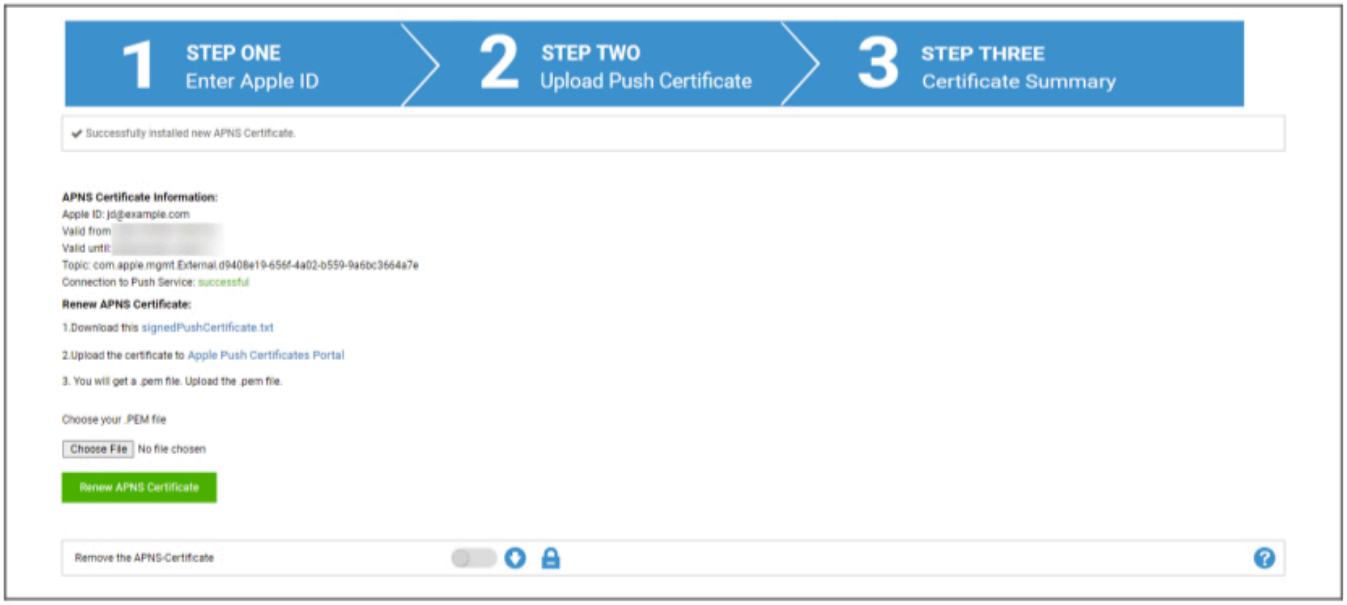
- Nejprve zadejte své Apple ID, které chcete použít k vytvoření certifikátu APNS.

Poznámka: Toto Apple ID se používá pouze pro vytvoření certifikátu APNS. Toto Apple ID nemá se zařízeními nic společného a zařízení o něm nebudou vědět. Kromě toho potřebujete přístup k tomuto Apple ID také k obnovení certifikátu APNS. Proto se doporučuje použít nějaké obecné Apple ID a přihlašovací údaje zdokumentovat. Před vypršením platnosti certifikátu APNS se na použitou poštovní adresu Apple ID odešle připomenutí.

- Klikněte na "Další krok" a pokračujte.
- (volitelné) Pokud jste omylem smazali dříve odstraněný certifikát APNS, můžete jej také obnovit.

Krok 2

- Stáhněte si soubor signedPushCertificate.txt
- Přejděte na [stránku https://identity.apple.com/pushcert/](https://identity.apple.com/pushcert/) a přihlaste se pomocí Apple ID z kroku 1.
- Klikněte na "Vytvořit certifikát"
- (nepovinné) zadejte poznámku. To může být užitečné, pokud spravujete více nájemců, abyste je mohli snadno identifikovat.
- Klikněte na "Choose File" a vyberte dříve stažený soubor signedPushCertificate.txt.
- Klikněte na "Nahrát".
- Nyní se zobrazí potvrzení o vytvoření certifikátu APNS.
- Klikněte na "Stáhnout" a uložte jej.
- Vraťte se do konzoly pro správu.
- Klikněte na "Choose File" a vyberte certifikát APNS, který chcete nahrát.
- Klikněte na "Nahrát"



Krok 3

Nyní jste úspěšně nastavili certifikát APNS a můžete spravovat zařízení se systémy iOS a MacOS.

V kroku 3 se zobrazí přehled aktuálně používaných certifikátů APNS.

Také máte možnost obnovit certifikát APNS podle kroků zobrazených na obrazovce. Nezapomeňte jej obnovit před vypršením jeho platnosti.

Při obnovování certifikátu APNS nezapomeňte na to, že se musíte přihlásit pomocí Apple ID uvedeného v kroku 3, a také na to, že musíte obnovit dříve použitý certifikát a NE vytvářet nový. "Téma" certifikátu APNS se zobrazí v kroku 3 a po kliknutí na "i" na portálu Apple Push Certificate. Jedná se o jedinečné ID, které identifikuje certifikát. To vám pomůže identifikovat správný a obnovit správný.

Když se zobrazí zpráva "Chyba: Push certifikát má jiné téma!", znamená to, že jste obnovili jiný certifikát nebo vytvořili nový.

Pokud chcete nahrát nový certifikát, např. pokud již nemáte přístup k dříve používanému Apple ID, musíte nejprve odstranit aktuálně nahraný certifikát.

Každopádně odstranění certifikátu APNS znamená, že již nelze provádět změny pro aktuálně zapsaná zařízení, dokud je znovu nezapíšete. Proto se ujistěte, že jste na to připraveni, a odstraňte certifikát pouze tehdy, pokud není jiná možnost.

Spravovaný přístup

Zde můžete povolit funkci Registrace uživatele pro zařízení se systémem iOS a Sdílený iPad pro zařízení se systémem iOS.

Registrace uživatelů

"Registrace uživatele" umožňuje speciální režim pro zařízení BYOD.

Pro každého uživatele musí být na portálu Apple Business Portal vytvořeno spravované Apple-ID.

Během procesu registrace budou uživatelé požádáni o zadání pověření Apple-ID.

"Registrace uživatele" zaručuje maximální bezpečnost uživatele, protože umožňuje pouze omezenou sadu nastavení a omezení, která může MDM nakonfigurovat.

Spravovaná doména:

Doména použitá k mapování e-mailové adresy uživatele na jeho spravované Apple-ID (musí být ve formátu: "@appleid.company.com").Např. john.doe@example.com bude mapována na john.doe@appleid.company.com.

V aplikaci Apple Business Manager si můžete prohlédnout spravovanou doménu.

Sdílený iPad

Sdílený iPad je zařízení DEP nakonfigurované se speciálním profilem DEP.

To umožňuje přihlášení více uživatelů k zařízení pomocí jejich spravovaného Apple-ID.

Spravované Apple-ID musí být vytvořeno v Apple Business Portal nebo Apple School Manageru.

Uživatelé, kteří se přihlašují ke sdílenému iPadu, jsou požádáni o zadání spravovaných pověření Apple-ID.

Spravovaná doména:

Doména použitá k mapování e-mailové adresy uživatele na jeho spravované Apple-ID (musí být ve formátu: "@appleid.company.com").Např. john.doe@example.com bude mapována na john.doe@appleid.company.com.

V aplikaci Apple Business Manager si můžete prohlédnout spravovanou doménu.

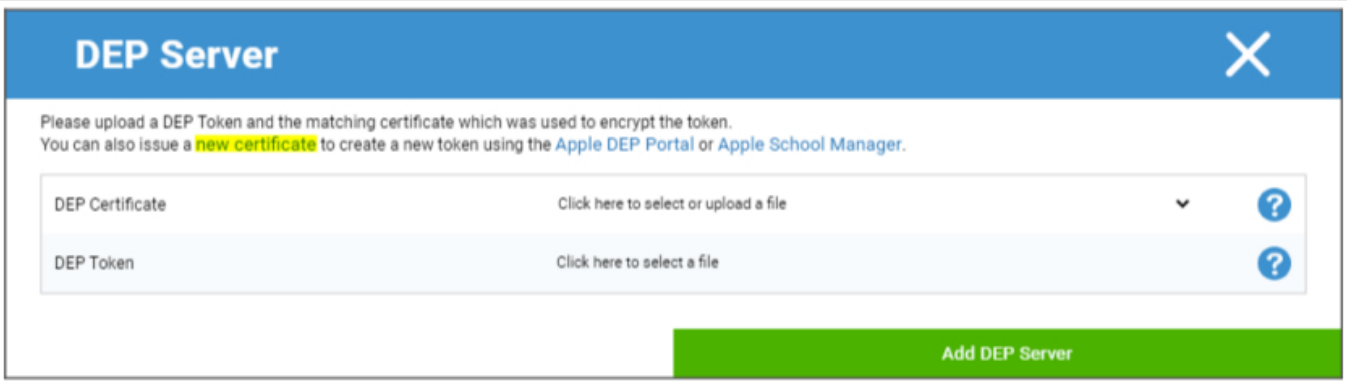
DEP

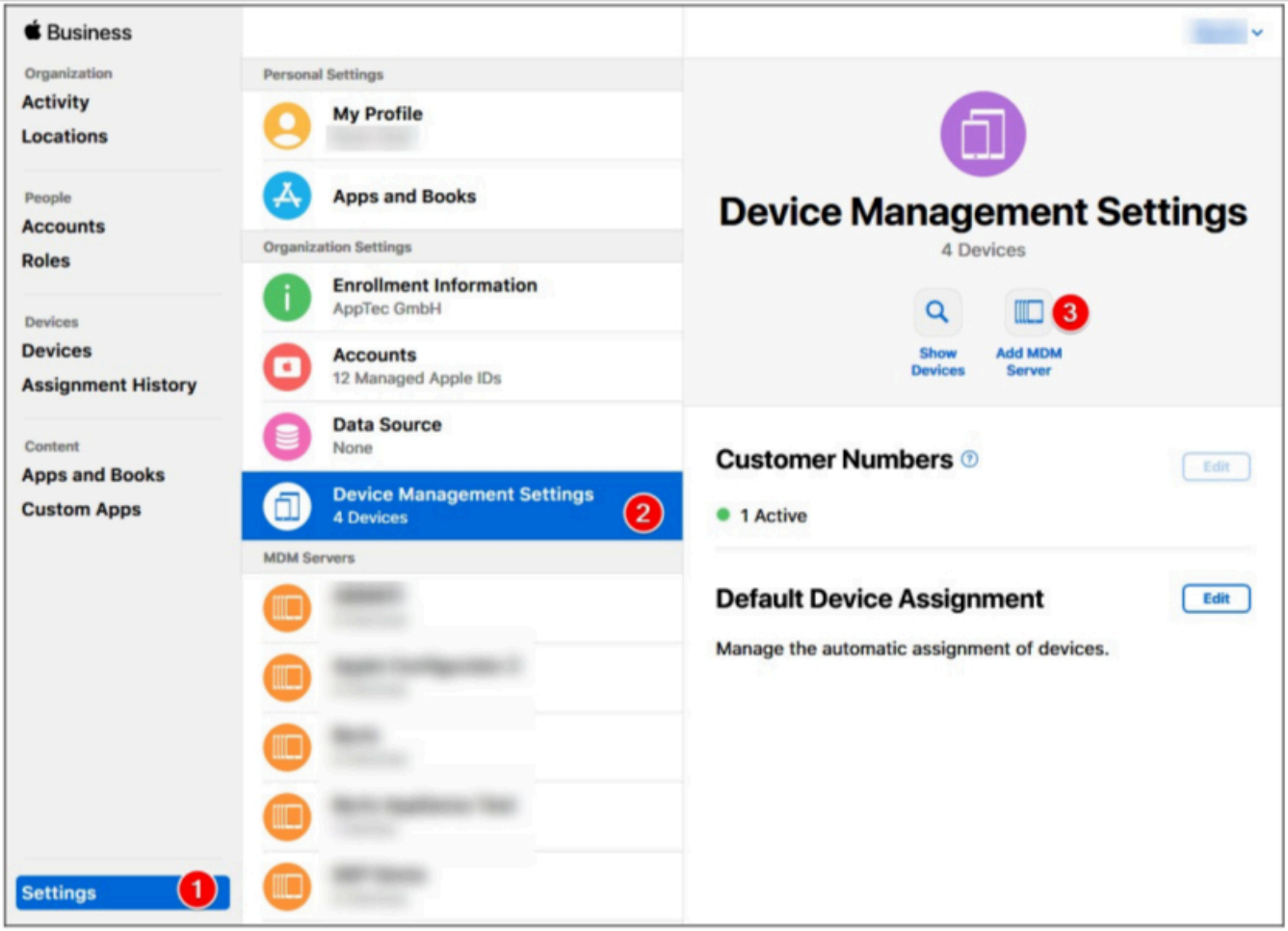
DEP (Device Enrollment Program) umožňuje snadnou registraci zařízení do MDM. Při použití DEP budou zařízení automaticky připojena k MDM při nastavení zařízení. Můžete také přeskočit téměř všechny kroky nastavení, které jsou v systému iOS obvykle povinné.

Mějte na paměti, že zařízení musíte zakoupit u prodejce, který podporuje DEP. Další informace získáte u prodejce nebo ve společnosti Apple.

Více informací o DEP: https: //www.apple.com/business/dep/

Kliknutím na "+" přidáte token DEP. Ve vyskakovacím okně klikněte na "new certificate" v textu (na obrázku níže označen žlutě). Tím se vygeneruje a stáhne certifikát DEP. Poté přejděte do aplikace Apple Business Manager(https://business.apple.com/) nebo Apple School Manager(https://school.apple.com/).

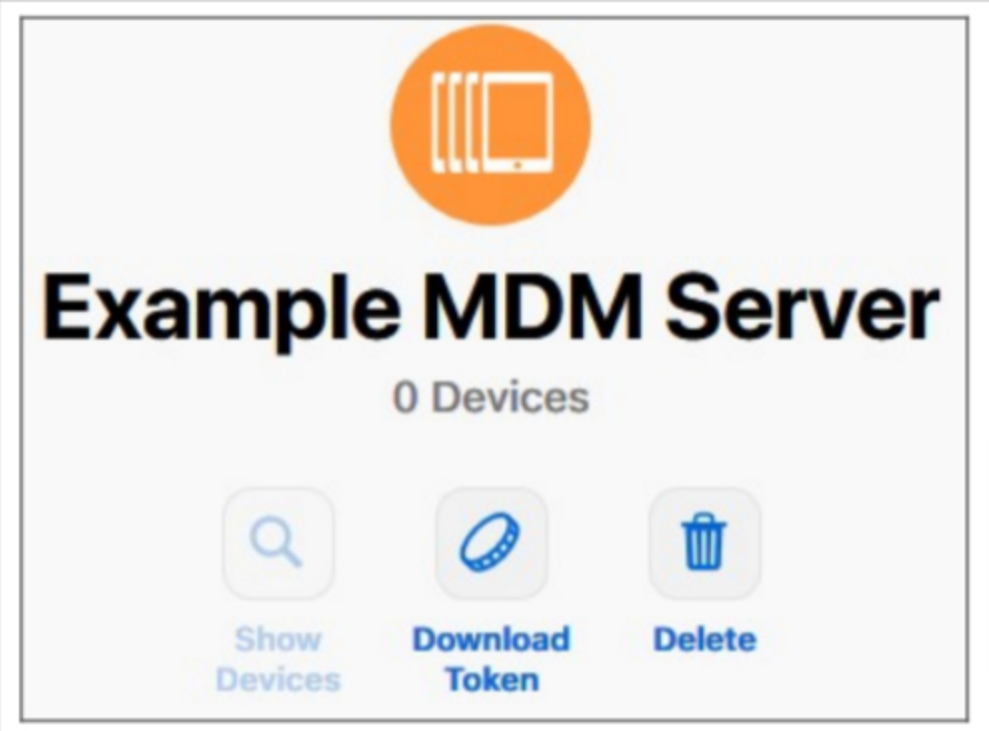




V aplikaci Apple Business Manager postupujte podle obrázku výše. Nastavení → Nastavení správy zařízení → Přidat server MDM.

Server libovolně pojmenujte a nahrajte dříve stažený certifikát DEP v části Nastavení serveru MDM → Nahrát veřejný klíč a klikněte na tlačítko "Uložit".

Nyní se zobrazí možnost "Stáhnout token". Klikněte na ni a uložte ji. Token je platný pouze 1 rok. Stačí však znovu kliknout na "Download Token" a získáte nový token, díky čemuž je jeho obnovení velmi snadné.



Nyní se můžete vrátit do MDM, odkud jste předtím stáhli certifikát DEP. Pokud jste kartu nezavřeli, mělo by být vyskakovací okno pro přidání serveru DEP stále otevřeno a certifikát DEP by již měl být vybrán. Nyní můžete nahrát svůj token do pole "DEP Token" a kliknout na DEP Server.

Ve sloupci "**Devices**" se zobrazí počet zařízení, která jsou přiřazena k tomuto DEP Serveru. Zařízení přidaná k tomuto DEP serveru budou automaticky vytvořena v DEP poolu ve správě mobilních zařízení.

Kliknutím na toto číslo získáte přehled o všech svých zařízeních DEP a jejich stavu.

Poznámka: V závislosti na pracovním postupu nebo konfiguraci v Business Manageru je možné, že budete muset tato zařízení přiřadit k DEP Serveru ručně. V Apple Business Manageru můžete také nastavit výchozí DEP Server pro nová zařízení.

Ve sloupci "**Profily**" vidíte počet profilů DEP, které máte. Kliknutím na toto číslo můžete také zobrazit podrobnosti o svých DEP profilech a můžete zde odstranit staré/nepoužívané profily. V současné době je není možné měnit. Pokud chcete provést změnu, musíte vytvořit nový.

Ve sloupci "**Poslední synchronizace**" můžete ručně synchronizovat server DEP (např. pokud jste právě přidali nové zařízení do DEP) a zobrazit datum poslední úspěšné synchronizace.

Ve sloupci "**Automatický profil**" můžete nastavit profil DEP jako automatický výchozí profil. Tento profil bude automaticky přiřazen novým zařízením. Pokud automatický profil nenastavíte, musíte profil novým zařízením pokaždé přiřadit ručně.

Ve sloupci "**Přidat profil**" můžete přidat nový profil DEP. Zařízení jej obdrží na začátku nastavení zařízení. Profil DEP určuje, jak se zařízení nastaví a které kroky nastavení budou přeskočeny.

Poznámka: po registraci zařízení lze tato nastavení změnit pouze obnovením továrního nastavení a registrací zařízení s novým profilem. To se týká zejména položek "**Removable**" a "**Allow pairing**". V případě "**Allow pairing" (Povolit párování**) doporučujeme tuto funkci zapnout, protože ji lze zakázat prostřednictvím omezení MDM, ale nelze ji znovu povolit, pokud je zakázána v profilu DEP.

Ve sloupci "**Upravit**" můžete nahrát nový token, např. při obnově tokenu.

Konfigurátor a adresa URL

URL adresy pro zápis do bazénu

Zde můžete vytvořit adresu URL pro zápis a QR kód pro zápis, který je platný po stanovenou dobu zápisu a do stanoveného data. To umožňuje zapsat více zařízení, která pouze jeden odkaz nebo QR kód.

Zařízení zaregistrovaná pomocí této adresy URL nebo kódu QR budou ve skupině ve správě mobilních zařízení a je třeba je následně ručně přiřadit ke skupině nebo uživateli.

Poznámka: toto platí pouze pro ruční zápis. Tuto adresu URL nepoužívejte, pokud zařízení registrujete prostřednictvím nástroje Apple Configurator.

Profil MDM – Konfigurátor Apple

Zde můžete získat adresu URL, kterou potřebujete při registraci zařízení prostřednictvím nástroje Apple Configurator. Při přípravě zařízení pomocí nástroje Apple Configurator můžete ve stejném procesu přidat zařízení do MDM. Nástroj Apple Configurator k tomu vyžaduje tuto adresu URL.

Zařízení přidaná prostřednictvím nástroje Apple Configurator budou ve skupině ve Správě mobilních zařízení a následně je musíte ručně přiřadit ke skupině nebo uživateli.

Najdete zde také soubor .mobileconfig, který lze použít k registraci zařízení prostřednictvím nástroje Apple Configurator. Každopádně doporučujeme použít adresu URL.

Konfigurace systému Android

Konfigurace systému Android

Odinstalování ochrany	Pokud je tato funkce aktivována, uživatel nemůže správce zařízení deaktivovat, aniž by zadal heslo nastavené správcem MDM. Heslo je nastaveno při registraci, takže pro aktualizaci hesla je třeba zařízení znovu zaregistrovat. Existují dvě možnosti odebrání správců zařízení: 1. Ručně v zařízení ◦ Otevření aplikace EMM v zařízení ◦ Přepnutí na kartu Stav ◦ Klepněte na možnost "Odinstalovat ochranu". ◦ Zadejte heslo Správné heslo můžete získat pomocí Revize z "Historie hesel" v konzoli. ◦ Přejděte dolů a klepněte na nově přidaný bod, "Klepnutím odinstalujete aplikaci AppTec360 MDM" (na provedení tohoto úkolu máte 20 sekund). ◦ Dialog "Odinstalovat aplikaci AppTec360 MDM" potvrďte tlačítkem "ok". Tím se zařízení odhlásí z konzoly. ◦ Pro odstranění aplikace ze zařízení potvrďte dialog "AppTec360 MDM bude odinstalován" volbou "UNINSTALL". 2. automatický (konzola) ◦ Vyberte zařízení v konzole ◦ Klikněte na modrou ikonu ozubeného kola a vyberte možnost "Enterprise Wipe". Poznámka: K dispozici pouze ve verzích systému Android 4.x a nižších nebo v zařízeních s rozhraním KNOX API (zařízení Samsung).
Odinstalovat heslo (revize x)	Nastavené heslo, pomocí kterého může uživatel odebrat správce zařízení.

	Revize x = počítadlo, jak často již bylo heslo změněno Je důležité, jaké heslo uživatel potřebuje, protože je možné, že zařízení nekomunikuje se serverem AppTec360, a proto ještě nebylo přeneseno nejnovější heslo.
Historie hesel	Po kliknutí na modré tlačítko ("Zobrazit historii") si můžete prohlédnout dříve zadaná hesla.
Rozšířená ochrana při odinstalaci	Tato možnost nabízí ochranu proti zařízením, která nejsou součástí systému SAFE. Pokud je toto nastavení aktivováno, není možné správce zařízení snadno deaktivovat.
Vyzvat uživatele k odinstalaci blokovaných aplikací?	Pokud je to možné, zablokované aplikace budou nejen zablokovány, ale také automaticky odinstalovány. Pokud automatické odinstalování není možné, bude uživatel vyzván k odinstalování blokovaných Aplikací.
Blokování aplikací inteligentního systému	Pokud je povolen whitelisting, klient Android MDM zablokuje všechny aplikace nainstalované uživatelem. Povolením tohoto nastavení zablokujete všechny spustitelné systémové aplikace v režimu Whitelisting.

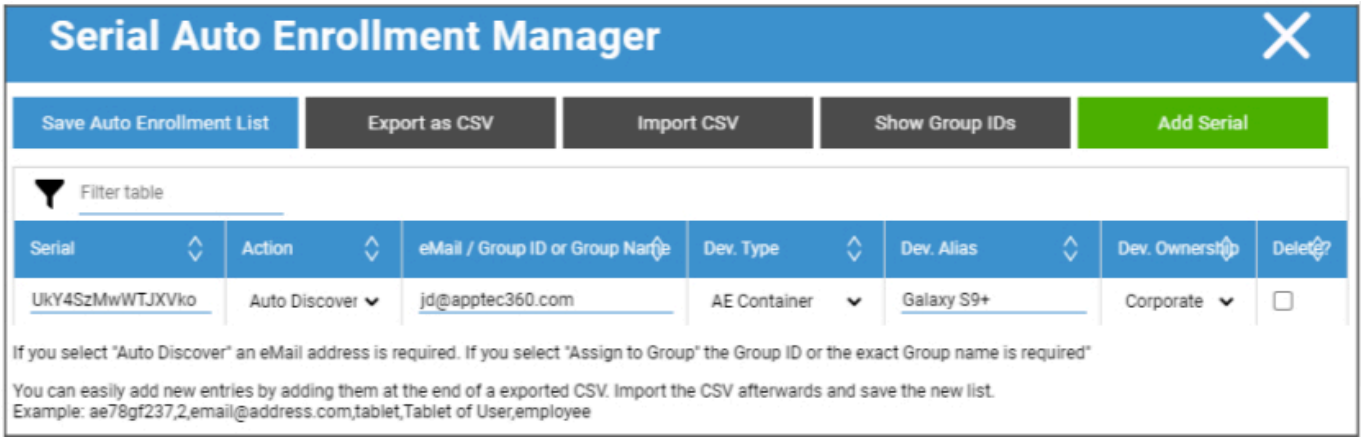
Automatický zápis

Zde můžete povolit funkci automatické registrace, aby se zařízení automaticky zaregistrovala po otevření klienta AppTec360 MDM na zařízení.

Důležité: Tato metoda zápisu je zastaralá a v systému Android 10 nebo novějším již nefunguje. Každopádně při použití systému Android 7 nebo vyššího byste měli zařízení stejně zaregistrovat jako plně spravované zařízení Android Enterprise. Pokud chcete používat kontejner Android Enterprise BYOD a používáte systém Android 10 nebo vyšší, musíte zařízení zaregistrovat ručně pomocí pověření, kódu QR nebo SMS. Každopádně seznam automatických zápisů se stále používá k automatizaci procesu zápisu např. pro zápis AE, zápis Knox atd.

Seznam automatických zápisů se stále používá k automatizaci procesu zápisu, např. pro zápis AE, zápis Knox atd.

Kliknutím na položku "Serial Manager" nebo "IMEI Manager" můžete přidat sériové nebo IMEI zařízení. Není nutné provádět pro vaše zařízení obě, stačí pouze jedno.



Akce určuje, zda budou zařízení zapsána do fondu, uživatele nebo skupiny.

Můžete také exportovat a importovat soubor .csv a filtrovat záznamy podle klíčových slov.

Android Enterprise

Zde můžete nastavit systém Android Enterprise. To je nezbytné pro používání všech funkcí Android Enterprise.

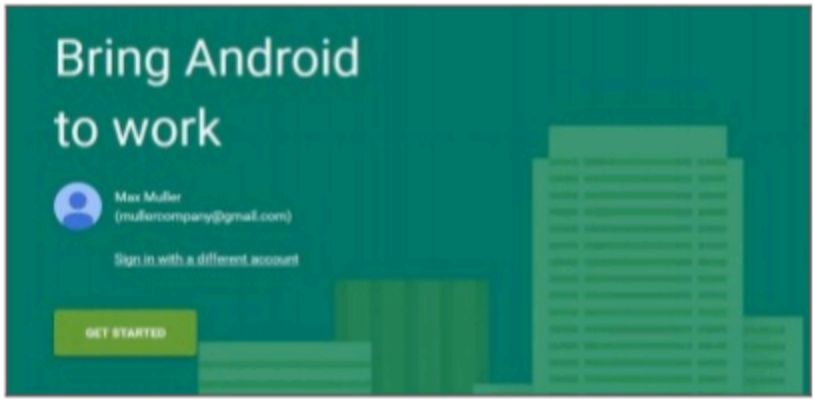
První metoda: Podnikový účet Android (účet Google)

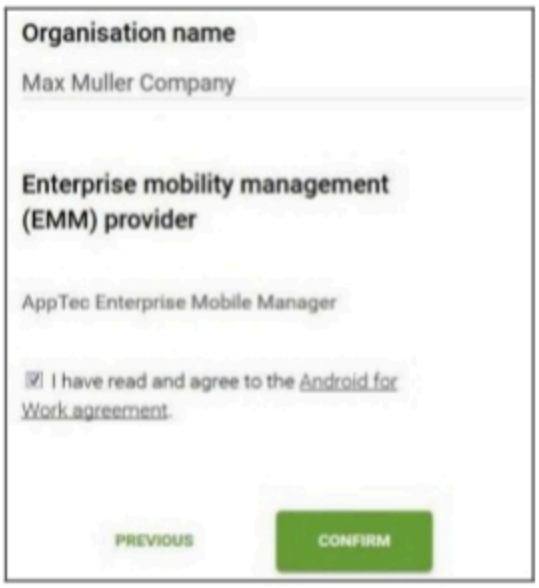
Nejprve stiskněte tlačítko "Prepare Setup" a po chvíli by se mělo objevit tlačítko "Start Setup".

Tím se dostanete na stránku nastavení systému Android Enterprise společnosti Google.

Pokud ještě nejste přihlášeni, přihlaste se pomocí účtu Google, který chcete používat, a stiskněte tlačítko "Začít".

Nyní můžete zadat název své společnosti. Poté zaškrtněte políčko a stiskněte tlačítko "Potvrdit".





V posledním kroku můžete dokončit registraci a měli byste se vrátit do konzoly. Pokud vše fungovalo, mělo by to vypadat takto:

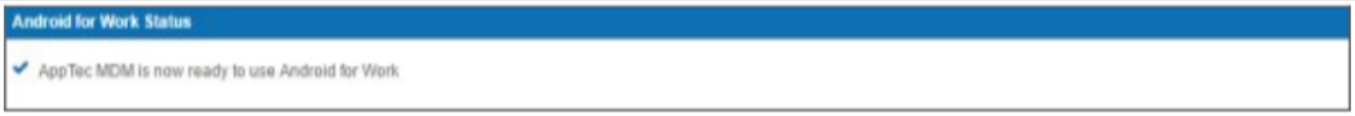
Nyní můžete začít konfigurovat kontejner Android Enterprise Container.

Druhá metoda: Účet G-Suite

Stiskněte tlačítko "Use G-Suite" a přihlaste se ke svému účtu správce Google. Tam přejděte na "Zabezpečení" -> "Zobrazit více" -> "Správa poskytovatele EMM pro Android" a vygenerujte token. Poznámka: Pokud ve svém účtu G-Suite nevidíte podnikové nastavení pro Android, musíte přejít na "Získat další aplikace a služby" a přidat správu zařízení Android. Nyní zadejte Token a svou primární doménu v naší konzoli a klikněte na "Uložit změny". Po dokončení klikněte na "Use Android Enterprise Account".

Nyní by se mělo zobrazit tlačítko "Vytvořit servisní účet". Klikněte na něj. Tento proces může trvat několik okamžiků.

Pokud vše fungovalo, mělo by to vypadat takto:



Nyní můžete začít konfigurovat kontejner Android Enterprise Container.

Ochrana před obnovením továrního nastavení

Pomocí ochrany proti obnovení továrního nastavení můžete zařízení svázat s účtem Google podle vlastního výběru, což také přepíše jakékoli stávající svázání s účtem Google. Chcete-li ochranu před obnovením továrního nastavení používat, musíte ji nejprve nastavit zde a poté ji aktivovat ve svých profilech.

Chcete-li nastavit ochranu proti obnovení továrního nastavení, klikněte na "FRP Setup" a postupujte podle pokynů na obrazovce.

POZNÁMKA: Pečlivě si přečtěte a proveďte následující kroky. Doporučujeme postupovat v novém okně prohlížeče inkognito, abyste se vyhnuli automatickému přihlášení do nesprávného účtu Google. Pokud byste zadali špatné ID nebo ztratili přístup k používanému účtu Google, můžete se ze zařízení zcela vyřadit!

Zápis do AE

Zde můžete aktivovat Android Enterprise Ernollment. Použitím této metody se vaše zařízení zapíší do režimu vlastníka zařízení Android Enterprise. V tomto režimu budete mít nad zařízením plnou kontrolu.

Povolit zápis AE	Aktivuje funkci AE Enrollment Caution: Pokud deaktivujete funkci AE Enrollment, přestanou fungovat stávající kódy QR a již nakonfigurovaná programovací zařízení NFC. Pokud AE Enrollment znovu povolíte, budete muset znovu odeslat konfiguraci NFC push / vygenerovat nové QR kódy.
Povolení automatického zjišťování	Když se zařízení samo zaregistruje prostřednictvím funkce "AE Enrollment", systém se pokusí přiřadit jej k uživateli na základě informací nastavených v bílé listině sériového čísla / IMEI ("General Settings" > "Android Configuration" > "Auto Enrollment").
Blokování neznámých zařízení	Zapsat se mohou pouze zařízení, která byla zařazena na bílou listinu sériových čísel / IMEI ("Obecná nastavení" > "Konfigurace systému Android" > "Automatický zápis").

Poznámka k metodě 1 a 2: "Uvítací obrazovka" je první obrazovka, která se zobrazí po obnovení továrního nastavení. Ta může vypadat různě v závislosti na verzi systému Android a/nebo modelu zařízení, které používáte.

Metoda 1: Zápis pomocí kódu QR

(vyžaduje systém Android 7.0 nebo vyšší) Pokud používáte systém Android 7 nebo vyšší, doporučujeme vždy použít tuto metodu.

1. Obnovení továrního nastavení zařízení
2. Vygenerujte kód QR pro zápis pomocí jedné ze dvou následujících metod:
    - Klikněte v "Obecná nastavení -> Konfigurace Androidu -> Zápis AE" na "Generovat QR kód". Zvolte, zda chcete přeskočit šifrování úložiště a/nebo zda mají být odstraněny všechny systémové aplikace.
    - (případně) Vyberte existující Zařízení. V "Přehledu zařízení" klikněte na zobrazený QR kód. Zvolte, zda chcete přeskočit šifrování úložiště a/nebo zda mají být odstraněny všechny systémové aplikace.
3. Nyní klepněte šestkrát na uvítací obrazovku zařízení. Tím se spustí režim zápisu QR.
4. Nyní se připojte k bezdrátové síti a krátce počkejte, než se nainstaluje čtečka QR kódů.
5. Nyní naskenujte kód QR
6. To je vše. Vaše zařízení je nyní zaregistrováno v režimu zařízení Android Enterprise.
    - a. Pokud jste v "Obecných nastaveních" použili QR kód, můžete své zařízení najít v "Bazénu -> Zařízení vlastníka AE". (Tip: Je možné, že budete muset znovu načíst stránku,

abyste zařízení viděli). Pokud jste zaškrtli políčko "Enable Auto Discover" (Povolit automatické zjišťování), najdete jej v rámci uživatele automatického zjišťování.

- Pokud jste použili QR kód existujícího profilu zařízení, bude zařízení do tohoto profilu zapsáno.

Metoda 2: Zápis NFC

(vyžaduje NFC a systém Android 6.0 nebo vyšší)

Příprava: Zadejte informace o své WiFi v "Obecná nastavení -> Konfigurace Androidu -> Zápis AE -> Údaje pro zajištění NFC". Nyní pomocí "NFC Device" vyhledejte zařízení, které se stane programátorem. Toto zařízení bude sloužit k odesílání informací o zápisu do ostatních zařízení prostřednictvím NFC.

1. Obnovení továrního nastavení zařízení
2. Otevřete na programátoru aplikaci pro párování NFC z AppTec360.
3. Zvolte, zda chcete šifrování úložiště přeskočit a/nebo zda mají být odstraněny všechny systémové aplikace.
4. Držte obě zařízení zády k sobě
5. Nyní by měl Android Enterprise Enrollment výrazně
6. Nyní najdete své zařízení v konzole
    - a. Pokud jste v poolu nenakonfigurovali funkci Automatické zjišťování.
    - b. V rámci uživatele, který jste nakonfigurovali pro funkci Automatické zjišťování
    - c. Tip: Je možné, že budete muset znovu načíst stránku, abyste viděli zařízení.

Metoda 3: Účet Google

(vyžaduje systém Android 5.1 nebo vyšší)

(Poznámka: Pokud používáte tuto metodu, zařízení nebude automaticky zaregistrováno. Místo toho jej musíte zapsat ručně nebo proces zautomatizovat pomocí funkce Automatický zápis.)

1. Obnovení továrního nastavení zařízení
2. Projděte kroky nastavení, dokud se nebudete moci přihlásit pomocí účtu Google.
3. Jako uživatelské jméno/mail zadejte "afw#apptec".
4. Klepněte na "Další".
5. Vaše zařízení je nyní zařízením Android Enterprise

Zápis do společnosti KNOX

Zde můžete aktivovat registraci KNOX a najít informace potřebné k vytvoření registračního profilu KNOX na portálu pro nasazení KNOX. Ke konfiguraci a používání potřebujete účet na portálu KNOX Deployment Portal.

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

Povolení zápisu do systému KNOX	Aktivuje funkci KNOX Enrollment. Upozornění: Pokud zakážete funkci KNOX Enrollment, stávající profily MDM přestanou fungovat. Pokud funkci KNOX Enrollment znovu povolíte, budete muset aktualizovat pole "Custom JSON Data" ve svém profilu MDM.
Povolení automatického zjišťování	Když se zařízení samo zaregistruje prostřednictvím funkce "KNOX Enrollment", systém se jej pokusí přiřadit k uživateli na základě informací nastavených v bílé listině sériových čísel / IMEI ("General Settings" > "Android Configuration" > "Auto Enrollment").

1. Přihlaste se na portál Samsung KNOX Mobile Enrollment Portal https://eukme.samsungknox.com/itadmin.
2. Přejděte na "Profily MDM"
3. Klikněte na "Přidat"
4. Vyberte možnost "Server URI není pro můj MDM vyžadován" a klikněte na "Další".
5. Nyní vytvořte profil s informacemi zobrazenými v konzole pro správu.

Pokud zařízení získáte přímo od společnosti Samsung, může být tento profil pro registraci KNOX nainstalován přímo do zařízení.

Případně si můžete stáhnout aplikaci KNOX Deployment App, přihlásit se pomocí účtu KNOX Deployment Account a odeslat profil KNOX Enrollment Profile prostřednictvím NFC do jiných zařízení.

Pokud má zařízení nainstalovaný profil pro registraci KNOX, stáhne si naši aplikaci a zaregistruje zařízení, pokud má funkční připojení k internetu.

Zápis zařízení prostřednictvím služby KNOX Enrollment naleznete v části "Pool -> KNOX Enrollment" nebo v rámci uživatele, kterého jste zadali v nástroji Auto Discover.

Zero-Touch

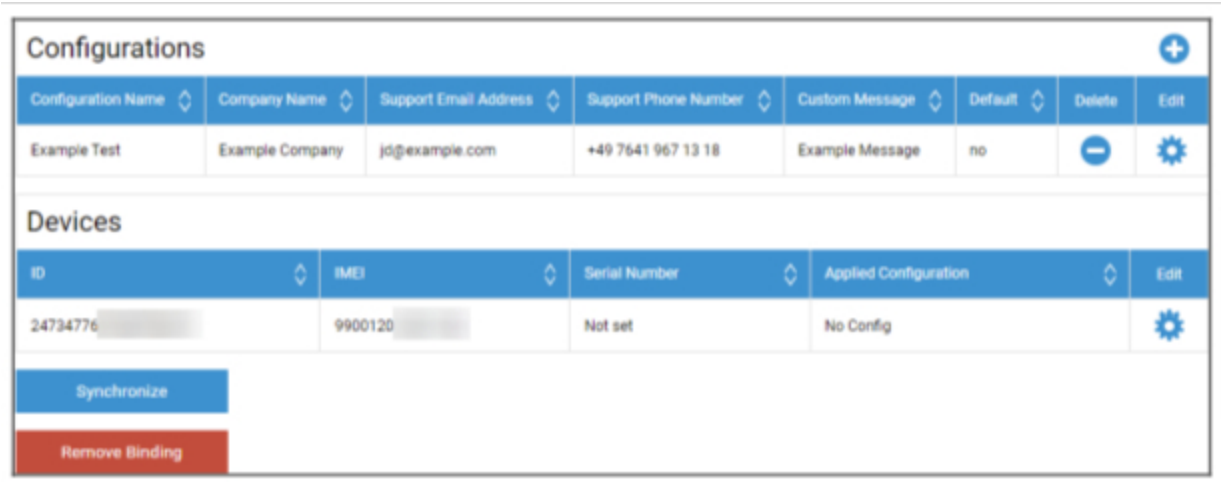
Pomocí funkce Zero-Touch můžete snadno zaregistrovat svá zařízení, aniž byste se jich museli dotýkat nebo cokoli konfigurovat na samotném zařízení. Stačí jej zapnout, projít běžnou konfigurací a zařízení zcela automaticky obdrží všechny informace o tom, jak se má nastavit a připojit k MDM.

Chcete-li používat Zero-Touch, musíte si zařízení zakoupit u prodejce, který Zero-Touch podporuje. Stejný prodejce vám také vytvoří účet na portálu Zero-Touch. Pro více informací o postupu nebo v případě problémů při přístupu na portál Zero-Touch se obraťte na svého prodejce.

Kliknutím na "Start Setup" spustíte nastavení. Budete přesměrováni na přihlašovací stránku, kde musíte vybrat svůj účet Google, který má přístup k portálu Zero-Touch.

POZNÁMKA: Je možné vybrat JAKÝKOLIV účet. V tomto kroku tedy nezapomeňte vybrat správný Účet. Pokud se vaše zařízení/konfigurace nezobrazí, je vysoce pravděpodobné, že jste použili nesprávný Účet.

Po dokončení přihlášení bude vypadat takto:



Kliknutím na tlačítko "+" přidejte konfiguraci a vyplňte pole, která jsou zobrazena na obrazovce. Pokud Konfiguraci povolíte jako výchozí Konfiguraci, bude automaticky přiřazena novým zařízením. Vytvoření nebo nastavení výchozí Konfigurace ji nepřiřadí k již existujícím zařízením.

Pokud zařízení nemá přiřazenou žádnou konfiguraci, nastaví se jako běžné zařízení a nepřipojí se k modulu MDM. Ujistěte se proto, že zařízení mají přiřazenou konfiguraci.

Po připojení účtu, zobrazení zařízení a přiřazení konfigurace k nim můžete začít nastavovat zařízení.

Zařízení můžete přidat do seznamu automatického zápisu, aby se automaticky zapsala do určité skupiny nebo k určitému uživateli. Pokud jste v seznamu Automatický zápis nic nenakonfigurovali, budou zařízení zapsána do skupiny.

Konfigurace systému Windows

Konfigurace systému Windows

Zde máte možnost povolit následující konfigurace v počítači s Windows 10:

Okamžité připojení k DM	
Počáteční doba opakování	naváže první pokus o připojení k zařízení, tato hodnota se exponenciálně zvyšuje.
Opakování připojení	Udává, kolik pokusů o připojení má klient DM provést při chybě připojení.
Maximální doba spánku	Udává maximální dobu spánku po chybě připojení.
První opakování synchronizace	Intervaly, ve kterých má zařízení komunikovat se serverem po prvním připojení.
Interval prvního opakování	Vztahuje se k položce "První opakování synchronizace". Zde jsou časy uvedeny v minutách Například v položce "First Sync Retries" (První opakování synchronizace) je uvedena hodnota "2" a v položce "First Retry Interval" (Interval prvního opakování) je uvedena hodnota "4 Minutes" (4 minuty), takže zařízení komunikuje dvakrát každé 4 minuty po prvním spojení.
Druhé opakování synchronizace	Intervaly, ve kterých má zařízení komunikovat se serverem po dokončení "Prvních opakovaných synchronizací".
Druhý interval opakování	Stejný princip jako u "First Retry Interval" - jen zde platí pro "Second Sync Retries".
Pravidelné opakování synchronizace	Intervaly, jak často má zařízení v budoucnu komunikovat se serverem. Výchozí hodnota: "Infinite" Doporučujeme tuto hodnotu neměnit, protože pokud zadáte "10", zařízení bude se serverem komunikovat 10x a pak přestane Proto se komunikace se serverem AppTec360 přeruší!
Pravidelný interval opakování	Stejný princip jako u "First/Second Retry Interval" - jen zde platí nastavení pro budoucnost.
Pravidelný interval opakování	Stejný princip jako u "First/Second Retry Interval" - jen zde platí nastavení pro budoucnost.

ContentBox

Konfigurace

Zde můžete nakonfigurovat pole ContentBox. Do ContentBoxu můžete umístit soubory pro skupiny, ke kterým lze přistupovat pomocí aplikace ContentBox v zařízení.

Povolení pole ContentBox	Povolení pole ContentBox. Vypnutím této funkce, pokud ContentBox nepoužíváte, můžete ušetřit prostředky na počítačích OnPremise.
Použití externí instalace modulu ContentBox	ContentBox lze provozovat také s vlastním systémem Nextcloud.
ADRESA URL	Úplná adresa URL subjektu Nextcloud
Kořenový uživatel	Kořenový uživatel účtu Nextcloud
Kořenové heslo	Kořenové heslo účtu Nextcloud
Výchozí oprávnění složek skupiny	Výchozí oprávnění skupinových složek, které lze individuálně upravit podle skupiny (ve Správě mobilních zařízení).
Sdílení složky skupiny s podskupinami	Pokud je aktivní, může každá podskupina číst všechny složky hlavní skupiny, lze je také individuálně konfigurovat pro každou skupinu (Správa mobilních zařízení).
Oprávnění pro podskupiny	Oprávnění pro podskupiny lze nakonfigurovat pro každou skupinu zvlášť (Správa mobilních zařízení).
Povolit sdílení	Umožňuje uživateli sdílet obsah prostřednictvím odkazů, lze konfigurovat individuálně pro každou skupinu.
Maximální velikost nahraného souboru v MB	Maximální velikost souboru Standardní: 512 MB Maximální konfigurace: 2048
Pověření WebDAV	
Adresa URL WebDAV	ContentBox můžete otevřít také pomocí WebDAV. V žádném případě nemažte následující složky: /apptecgroups /apptecgroups/AppTecGroup-X.
Kořenový uživatel	Název kořenových uživatelů
Heslo	Heslo kořenových uživatelů

Synchronizace s okénkem ContentBox probíhá automaticky. Můžete však provést ruční synchronizaci pomocí "Synchronize ContentBox".

Kromě toho zde můžete aktivovat/deaktivovat ContentBox v jednotlivých zařízeních.

To je relevantní pouze v případě, že jste si ContentBox dodatečně nelicencovali, pak máte stále přístup k 25 zařízením, se kterými můžete ContentBox testovat - zde jej můžete aktivovat pro příslušná zařízení.

Konfigurace LDAP

Přehled protokolu LDAP

Zde můžete navázat spojení se službou Active Directory prostřednictvím protokolu LDAP a hromadně importovat uživatele a skupiny. Synchronizaci je třeba provést ručně. Můžete nakonfigurovat více připojení LDAP k různým systémům nebo s různými konfiguracemi/filtry.

Název serveru	Zobrazovaný název serveru
Typ	V současné době jsou podporovány pouze adresáře Active Directories, které podporují LDAP.
Doména LDAP	Primární doména LDAP (např. example.com)
Hostitel LDAP	Nutné pouze v případě, že hostitel LDAP není dosažitelný pod danou doménou LDAP.
Přístav	Pro použití standardního portu (389 nebo 636 pro SSL) nechte prázdné.
Uživatelské jméno	Např. CN=John,OU=Users,DC=EXAMPLE,DC=COM Poznámka: Většina systémů vyžaduje uživatelské jméno v tomto formátu a neakceptuje "John" jako uživatelské jméno.
Heslo	
Potvrzení hesla	
Zabezpečení připojení	Poznámka: při použití protokolu SSL nebo TLS se kontroluje certifikát služby Active Directory. Pokud je podepsán vlastním podpisem, musíte přidat kořenovou certifikační autoritu do úložiště důvěryhodnosti počítače OnPremise. Pokud jste v cloudu, musí služba Active Directory poskytnout důvěryhodný certifikát, jinak bude připojení fungovat pouze bez šifrování.
Automatická synchronizace.	Povolí automatickou synchronizaci adresáře LDAP v časovém intervalu zadaném v obecných nastaveních LDAP.
Základní DN	Pokud nechcete synchronizovat celý adresář, můžete zde zadat organizační jednotku.Např. OU=AndroidUsers,OU=Users,DC=EXAMPLE,DC=COM.
Člen	Všichni importovaní uživatelé budou přidáni do vybrané skupiny.
Pouze aktivovaní uživatelé?	Pokud je povolen, bude se brát v úvahu atribut userAccountControl, uživatelé bez tohoto atributu nebudou importováni.
Filtr LDAP	Pomocí filtru LDAP můžete filtrovat, kteří uživatelé budou importováni.
Filtr Regex	Pomocí filtru Regex můžete filtrovat, kteří uživatelé budou importováni.

Testovací připojení	Testuje připojení při ukládání konfigurace
Obnovení adresářové struktury při synchronizaci?	Pokud je to pravda, budou všechny položky LDAP přesunuty zpět na své původní místo ve stromu LDAP. Doporučuje se povolit.
Znovu importovat smazané uživatele a skupiny?	Pokud je tato možnost povolena, budou odstranění uživatelé a skupiny znovu vytvořeni. Doporučuje se povolit.
Synchronizace smazání?	Pokud je tato možnost povolena, budou skupiny a uživatelé odstraněni při jejich odstranění na serveru LDAP. Odstraní se také zařízení odstraněných uživatelů.

Pod seznamem Konfigurace LDAP můžete definovat období, ve kterém se systém automaticky synchronizuje. Pro automatickou synchronizaci se používají pouze Konfigurace LDAP, které mají aktivovanou příslušnou volbu.

Správa aplikací

Vlastní aplikace DB

Android

Zde můžete nahrát aplikace pro Android, které vaše společnost vyvinula, a později je distribuovat v aplikaci Mobile Management v profilech zařízení nebo skupin.

Upozorňujeme, že tímto způsobem doporučujeme distribuovat pouze aplikace, které nejsou dostupné v obchodě Google Play.

Kliknutím na "+" nahrajte soubor APK aplikace, kterou chcete nahrát. V současné době je podporován pouze formát APK.

Limit nahrávání u zařízení OnPremise lze zvýšit v kroku 3 konfigurace zařízení. Pokud chcete zvýšit limit nahrávání v cloudu, obraťte se na podporu a získejte další informace.

Uvědomte si, že soubory APK jsou obvykle o něco menší než jejich obsah. Je možné, že se kvůli tomu nahrávání nezdaří, protože APK je v průběhu procesu rozbalován. Např. je možné, že se 95MB APK nepodaří nahrát při limitu 100 MB. V takovém případě zvyšte limit nahrávání, jak je uvedeno výše.

Doporučujeme také nejprve ručně přenést soubor APK do jednoho testovacího zařízení (např. přes USB) a zkusit jej nainstalovat ručně pomocí aplikace Soubory v zařízení. Pokud to z nějakého důvodu nepůjde, nepůjde to ani přes MDM.

Cíl aktualizace

Pomocí funkce "Cíl aktualizace" můžete zvolit, která verze aplikace má být nainstalována nebo na kterou verzi má být aplikace aktualizována, pokud jste u aplikace aktivovali funkci "Aktualizovat".

Pokud jste nevybrali cíl aktualizace, bude použita nejvyšší verze.

Mějte na paměti, že systém Android neumožňuje downgrade aplikací. Uvědomte si také, že "kód verze" určuje, zda je verze vyšší, nižší nebo stejná. Proto se při vytváření aktualizace ujistěte, že jste tuto verzi v aplikaci správně zvýšili.

iOS

Zde můžete nahrát aplikace pro iOS, které jste vyvinuli, a později je distribuovat ve Správě mobilních zařízení v profilu zařízení nebo skupiny.

Kliknutím na "+" nahrajte IPA aplikace, kterou chcete nahrát. Zatím je podporován pouze formát IPA.

Limit nahrávání u zařízení OnPremise lze zvýšit v kroku 3 konfigurace zařízení. Pokud chcete zvýšit limit nahrávání v cloudu, obraťte se na podporu a získejte další informace.

Cíl aktualizace

Pomocí funkce "Cíl aktualizace" můžete zvolit, která verze aplikace má být nainstalována nebo na kterou verzi má být aplikace aktualizována, pokud jste u aplikace aktivovali funkci "Aktualizovat".

Pokud jste nevybrali cíl aktualizace, bude použita nejvyšší verze.

MacOS

Zde můžete nahrát aplikace pro MacOS, které jste vyvinuli, a později je distribuovat ve Správě mobilních zařízení v profilu zařízení nebo skupiny.

Kliknutím na "+" nahrajte PKG aplikace, kterou chcete nahrát. Zatím je podporován pouze formát PKG.

Limit nahrávání u zařízení OnPremise lze zvýšit v kroku 3 konfigurace zařízení. Pokud chcete zvýšit limit nahrávání v cloudu, obraťte se na podporu a získejte další informace.

Cíl aktualizace

Pomocí funkce "Update Target" můžete zvolit, která verze aplikace se má nainstalovat nebo na kterou verzi se má aplikace aktualizovat, pokud jste u aplikace aktivovali funkci "Keep up to date".

Pokud jste nevybrali cíl aktualizace, bude použita nejvyšší verze.

Windows 10

Zde můžete nahrát aplikace pro Windows 10 a později je distribuovat ve Správě mobilních zařízení v profilu zařízení nebo skupiny.

Kliknutím na "+" nahrajte APPX, APPXBUNDLE nebo MSI aplikace, kterou chcete nahrát. Zatím je podporován pouze formát APPX, APPXBUNDLE nebo MSI.

Můžete také nahrát a definovat Závislosti pro aplikaci, které budou automaticky distribuovány a nainstalovány před instalací požadované aplikace.

Limit nahrávání u zařízení OnPremise lze zvýšit v kroku 3 konfigurace zařízení. Pokud chcete zvýšit limit nahrávání v cloudu, obraťte se na podporu a získejte další informace.

Cíl aktualizace

Pomocí funkce "Update Target" můžete zvolit, která verze aplikace se má nainstalovat nebo na kterou verzi se má aplikace aktualizovat, pokud jste u aplikace aktivovali funkci "Keep up to date".

Pokud jste nevybrali cíl aktualizace, bude použita nejvyšší verze.

Balíček Win32 (.exe)

Do zařízení můžete také distribuovat soubory .exe/instalační programy.

Název balíčku	Název, který se zobrazí v MDM
Popis	Popis uvedený v MDM
Soubor balíčku	Povoleny jsou pouze soubory .zip. Do tohoto souboru zip umístěte soubory, které chcete nasadit.
Kontext nasazení	**Systém**: Instalační příkaz se spouští se systémovými právy, která jsou vyšší než "User". Při použití "System" také proces nemá uživatelské rozhraní, takže bude tichý a uživatelský profil, např. proměnné prostředí jako %AppDat%, není přístupný. **Uživatel**: Instalační příkaz má přístup k uživatelskému profilu a v případě potřeby může zobrazit uživatelské rozhraní. Poznámka: Některé procesy mohou pracovat pouze v jednom kontextu. Např. pokud se software instaluje do AppData, bude fungovat pouze při výběru "User" (Uživatel).
Instalační příkaz	Příkaz použitý k instalaci programu. Například instalační příkaz pro soubor zip obsahující v kořenovém adresáři soubor "setup.exe", který podporuje parametr "/s" pro tichou instalaci, by byl příkaz Install "setup.exe /s". Uvědomte si, že různé programy mohou mít různé parametry.
Příkaz k odinstalaci	Příkaz, který se spustí pro odinstalování softwaru prostřednictvím MDM. Obvykle ukazuje na odinstalační program. Například "C:\Program Files\ExampleSoftware\uninstall.exe".
Požadavky	
Poznámka: Aby se software nainstaloval, musí být splněny všechny stanovené požadavky. V opačném případě se nenainstaluje. Některá pole mohou být povinná. Pokud není pro požadavek nastavena žádná hodnota, bude požadavek ignorován.	
Architektura operačního systému	Architektura operačního systému
Minimální verze operačního systému	Minimální verze operačního systému
Min. volné místo na disku (MB)	Min. volné místo na disku (MB)

Min. fyzická paměť (MB)	Min. fyzická paměť (MB)
Minimální počet logických procesorů	Minimální počet logických procesorů
Minimální rychlost procesoru (MHz)	Minimální rychlost procesoru (MHz)
Další požadavky	Pokud chcete, můžete zde také ručně definovat pravidla nebo nahrát skript, který provede další kontroly požadavků.
Pravidla detekce	
Metoda detekce	Zde můžete definovat způsob zjišťování, zda je aplikace v zařízení nainstalována. Příkazy pro instalaci se spustí pouze tehdy, když tato pravidla zjistí, že aplikace NENÍ nainstalována. Příkazy pro odinstalování se spustí pouze tehdy, když tato pravidla zjistí, že aplikace není nainstalována. **Ruční definice pravidel**: Umožňuje ručně definovat jedno nebo více pravidel, která například kontrolují přítomnost určitého souboru, složky, klíče MSI nebo klíče registru. Pokud jsou všechna zadaná detekční pravidla pravdivá, bude aplikace považována za přítomnou. **Použít skript**: Nahrát vlastní skript s vlastními kontrolami. Pokud skript vrátí hodnotu "$TRUE", bude aplikace považována za přítomnou.
Pravidla detekce	

Nastavení aplikace

Nastavení aplikace iOS

Zde můžete definovat výchozí nastavení pro přidání aplikace do povinného obchodu s aplikacemi nebo do podnikového obchodu s aplikacemi.

Poznámka: Nastavuje se pouze to, co je ve výchozím nastavení vybráno při přidávání aplikací. NEMĚNÍ se tím stávající nastavení aplikací, které jsou již přidány v povinných aplikacích nebo v podnikovém obchodě s aplikacemi.

Udržujte aktuální stav	Automaticky udržuje aplikaci aktuální. Upozorňujeme, že po vydání aktualizace může trvat až 7 dní, než se aplikace aktualizuje.
Předbíhání, pokud není řízeno	Pokud je aplikace již nainstalována jako nespravovaná (uživatelem), bude převzata a spravována službou MDM.
Odstranění aplikace při odebrání profilu MDM	Odinstaluje aplikaci při odebrání MDM.
Zabránění zálohování dat aplikace	Zabraňuje zálohování dat aplikace.

Nastavení aplikace Android

Zde můžete definovat výchozí nastavení pro přidání aplikace do povinného obchodu s aplikacemi nebo do podnikového obchodu s aplikacemi.

Poznámka: Nastaví se pouze to, co je při přidávání vybráno jako výchozí. NEMĚNÍ se tím nastavení aplikací, které jsou již přidány v povinných aplikacích nebo v podnikovém obchodě s aplikacemi.

Udržujte aktuální stav	Automaticky udržuje aplikaci aktuální. K dispozici pouze pro aplikace InHouse Apps.
Řízená aktualizace klienta EMM AppTec360	Pokud je tato možnost povolena, mohou správci určit cíl aktualizace pro klienta AppTec360 EMM. Seznam všech dostupných verzí klienta AppTec360 EMM Client se zobrazí v části "Obecná nastavení" → "Správa aplikací" → "In-House App DB" → "Android".

Aplikace třetích stran

Android

Zde můžete nastavit aktivační kód pro Ikarus.

Nastavte tuto možnost na "Použít aktivační kód" a zadejte zde svůj aktivační kód.

Poznámka: Po zadání kódu a uložení se kód ještě nepřidá do profilu, který se odešle do zařízení. Aby byl kód přidán do profilu, musíte provést jakoukoli změnu v profilu. Např. změňte libovolný přepínač v profilu z vypnuto → zapnuto → vypnuto - Uložit → Přiřadit nyní.

iOS

Zde můžete zadat svou licenci SecurePIM. Po zadání licence stiskněte tlačítko "Uložit změny" a můžete používat možnosti SecurePIM.

VPP / KNOX Premium

Program Apples Volume Purchase Program (VPP) umožňuje snadno distribuovat placené i bezplatné aplikace do zařízení. Tento způsob je velmi doporučován, protože v zařízeních nepotřebujete Apple ID, uživatelé nemusí potvrzovat instalaci (pod dohledem), uživatelé nebudou muset zadávat heslo Apple ID a můžete snadno distribuovat placené Aplikace, aniž byste je museli znovu kupovat na každém Zařízení.

Chcete-li používat VPP, musíte se zaregistrovat v aplikaci Apple Business Manager.

Licence VPP

Zde získáte přehled o svých aplikacích VPP, o tom, kolik licencí je použito a kolik jich je k dispozici.

Po kliknutí na kolečko se zobrazí, kterým zařízením je licence přiřazena a jaký je stav tohoto přiřazení.

Kliknutím na tlačítko se obnoví mezipaměť VPP, která porovná licence přidělené v MDM s licencemi přidělenými na straně Applu. To může v některých případech vyřešit problémy s licencemi.

Token VPP

Zde můžete nahrát svůj VPP Token, který najdete v Apple Business Manageru v Nastavení → Aplikace a knihy. Můžete nahrát více tokenů VPP.

Token můžete obnovit jednoduše tak, že si v aplikaci Apple Business Manager stáhnete nový, kliknete na kolečko "Upravit" a nahrajete nový.

"Režim VPP" rozhoduje o tom, jak bude přiřazení licence zpracováno. V závislosti na scénáři je třeba použít různé režimy:

Při registraci zařízení pomocí QR kódu, odkazu, nástroje Apple Configurator nebo DEP je třeba použít "Device based".

"Na základě uživatele" je vyžadováno, pokud jsou zařízení zaregistrována s přihlášením uživatele nebo jako sdílený iPad.

Pokud povolíte funkci "Automatizovaná správa licencí", budou uživatelům přesunutým z jedné skupiny do druhé automaticky přiřazeny licence Apple VPP na základě profilu skupiny, do které byli přesunuti.

Stávající licence Apple VPP ze skupiny, ze které byly přesunuty, nebudou zrušeny.

Novým uživatelům přidaným do skupiny budou automaticky přiřazeny licence Apple VPP na základě příslušného profilu skupiny.

Klíč KNOX Premium

Zde můžete zadat svůj klíč KNOX Premium Key pro používání kontejneru Samsung KNOX.

Upozorňujeme, že tato funkce již není od systému Android 10 podporována. Místo toho použijte kontejner Android Enterprise.

Nastavení obchodu App Store

Oblast a jazyk

Zde můžete nastavit výchozí jazyk a oblast pro vyhledávání aplikací ve správě aplikací.

Uvědomte si, že nastavení iTunes určuje také způsob, jakým systém získává informace o určitých aplikacích. Pokud se v seznamech setkáte s aplikacemi, které se zobrazují podivným způsobem (např. chybějící ikona), možná jste nastavili oblast, kde konkrétní aplikace není dostupná.

Obchod AE Play

Zde najdete všechny možnosti Obchodu Play pro podniková zařízení se systémem Android pro schvalování aplikací, nahrávání vlastních aplikací do Obchodu Play nebo vytváření vlastních webových aplikací.

Schválené aplikace

Zde můžete získat přehled o všech schválených aplikacích.

Aplikace v Obchodě Play

Tím se načte iFrame zobrazující Obchod Play. Vyhledejte libovolnou aplikaci, klikněte na ni a schválte ji. Při schvalování aplikace můžete také definovat, že schválení bude odvoláno, pokud se změní požadovaná oprávnění. Doporučujeme ponechat tato nastavení při schvalování Aplikací ve výchozím nastavení.

Po schválení aplikace ji můžete přidat do svých profilů.

Tlačítko "Schválit" se po schválení změní na "Odvolat schválení", takže aplikace můžete kdykoli odstranit, pokud je již nepotřebujete.

Soukromé aplikace

Zde můžete do obchodu Google Play nahrát vlastní aplikaci jako soukromou aplikaci. To vám umožní distribuovat aplikaci prostřednictvím služeb Googlu a aktualizovat ji jejich prostřednictvím. To má také tu výhodu, že vaše vlastní Aplikace lze instalovat bez potvrzení uživatelem, které je obvykle nutné.

Webové aplikace

Zde můžete vytvářet webové aplikace, což jsou odkazy na určité webové stránky, které lze přiřadit jako aplikace.

Můžete mu také přidělit vlastní ikonu a dále definovat, jak přesně se má zobrazovat.

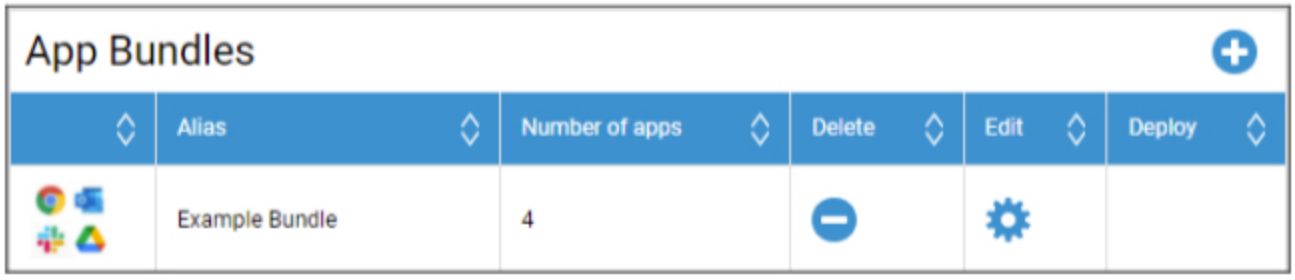
Rozložení obchodu

Rozložení obchodu určuje, jak se aplikace v Obchodě Play zobrazují, nebo zda se vůbec zobrazují.

Pokud chcete zobrazit aplikace v Obchodě Play, které si uživatel může ručně nainstalovat, je třeba je přidat sem do rozvržení. **A .** v profilu do podnikového obchodu Play. Pokud přidáte aplikaci pouze do jednoho z nich, nebude se zobrazovat.

Balíček aplikací

Pomocí balíčků aplikací můžete definovat skupiny aplikací, které lze jedním kliknutím přiřadit k profilům zařízení nebo skupinám.



Kliknutím na "+" vytvoříte nový Svazek aplikací. Po vytvoření balíčku aplikací můžete kliknutím na "Edit" přidat do balíčku aplikace z různých zdrojů.

Svazek lze přidávat do profilů jako všechny ostatní aplikace. Při přidávání aplikací se vám zobrazí další karta s názvem "Svazky aplikací", kde máte své Svazky.

Pokud provedete jakoukoli změnu ve svazku aplikací, zobrazí se tlačítko ve sloupci "Deploy". To vám umožní odeslat tyto změny do všech profilů obsahujících tento Svazek. Mějte tedy na paměti, že po přidání nebo odebrání aplikací ve svazku Bundle je nutné toto provést ručně.

Dálkové ovládání

TeamViewer

Konektor TeamViewer

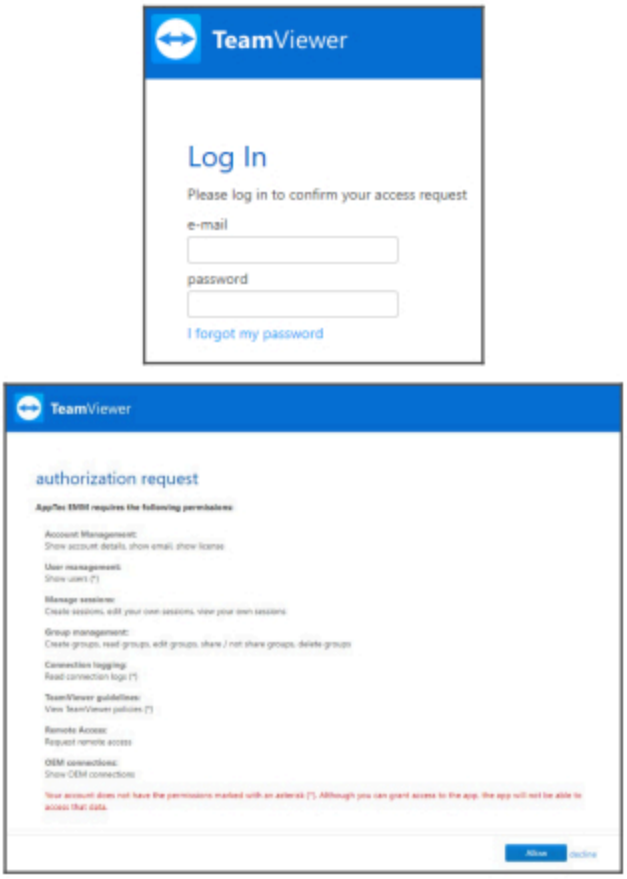
Poznámka: V bezplatné zkušební verzi naší cloudové verze nemůžete připojit svůj účet TeamViewer. Místo toho se automaticky připojí bezplatný demo účet.

Přejděte do Obecná nastavení -> Vzdálené ovládání -> TeamViewer. Zde můžete propojit svůj účet TeamViewer s konzolí nebo zobrazit informace o aktuálně připojeném účtu. Také si můžete prohlédnout všechny aktuálně aktivní relace, pokud přejdete do části "Aktivní relace".

Pro propojení účtu klikněte na "Start Setup".

Tím se dostanete na novou stránku, kde se musíte přihlásit pomocí svého účtu TeamViewer.

Po přihlášení musíte AppTec360 MDM autorizovat k používání tohoto účtu. Po potvrzení je třeba počkat několik sekund a účet je připojen.


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

Instalace nástroje TeamViewer QuickSupport

Přidejte aplikaci "TeamViewer QuickSupport" do povinných aplikací profilu vašeho zařízení nebo profilu skupiny a klikněte na "Přiřadit nyní". Počkejte, až bude aplikace v zařízení nainstalována.

Pokud se pokusíte o přístup k zařízení, ve kterém aplikace není nainstalována, bude v závislosti na konfiguraci zařízení nainstalována nebo bude vyzvána k její instalaci.

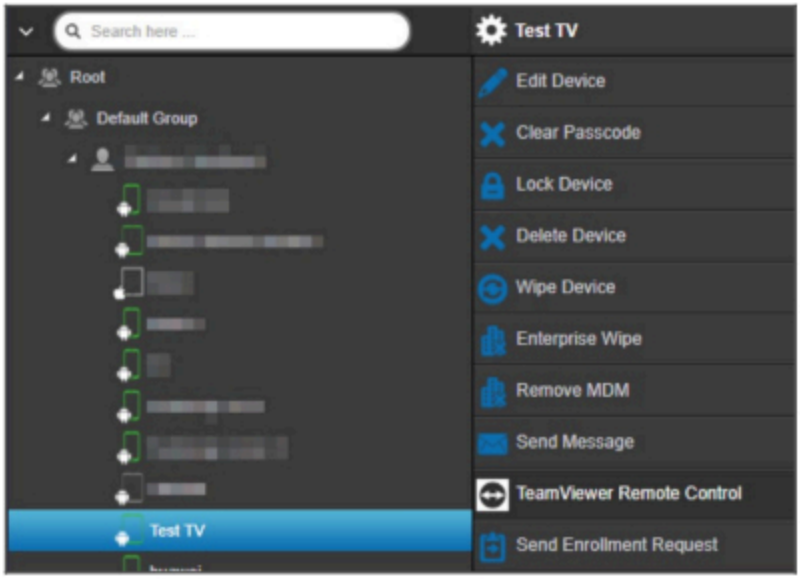
Dálkové ovládání zařízení

Chcete-li vzdáleně ovládat zařízení, vyberte zařízení, klikněte na kolečko a vyberte možnost "TeamViewer Remote Control".

Pokud již existuje aktivní relace, můžete použít starou relaci nebo vytvořit novou.

Potvrďte, že chcete vytvořit novou relaci TeamViewer.

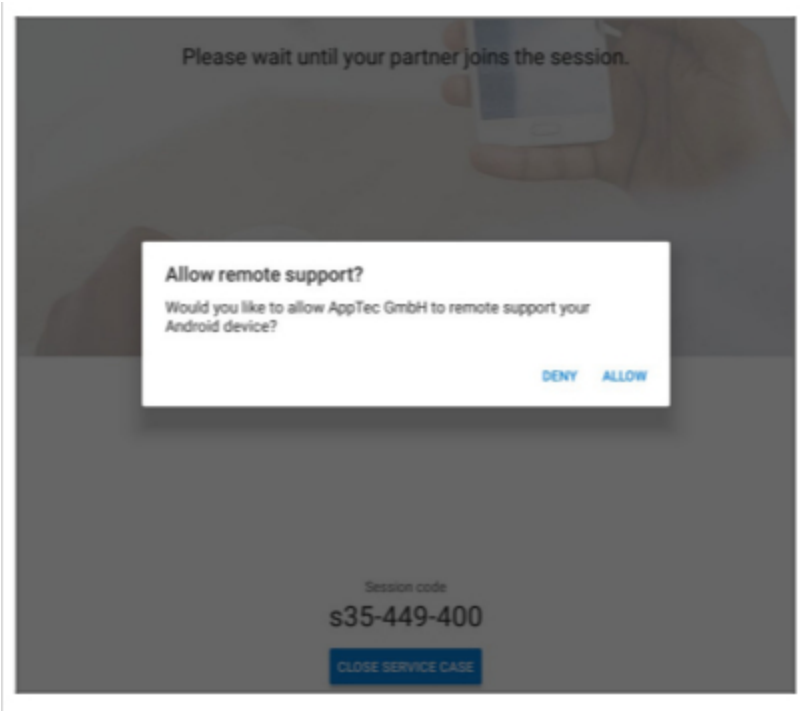
Po několika sekundách se zobrazí odkaz na relaci TeamViewer. Kliknutím na "Start" otevřete tento odkaz v novém okně.


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

Tento odkaz otevře nainstalovaný program TeamViewer a připojí vás k zařízení.

Nyní musíte potvrdit připojení na samotném zařízení, abyste jej mohli dálkově ovládat.

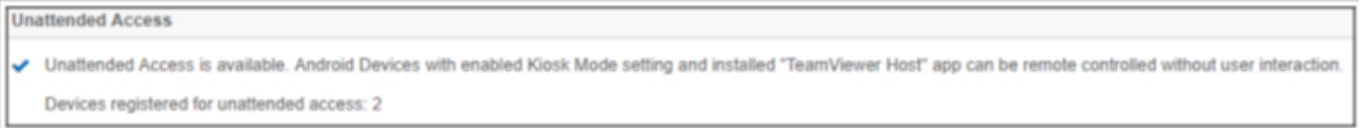


Pokud používáte iOS, zobrazí se v klientovi AppTec360 MDM zpráva. Pomocí tohoto odkazu se zařízení připojí ke vzdálené relaci. V závislosti na nastavení oznámení v zařízení je možné, že oznámení neobdržíte a budete muset AppTec360 MDM Client otevřít ručně.

Na některých zařízeních se systémem Android (např. Samsung) je nutné nainstalovat další aplikaci jako doplněk. Aplikace TeamViewer v zařízení vás o tom bude informovat, pokud je to ve vašem zařízení nutné.

Bezobslužný přístup

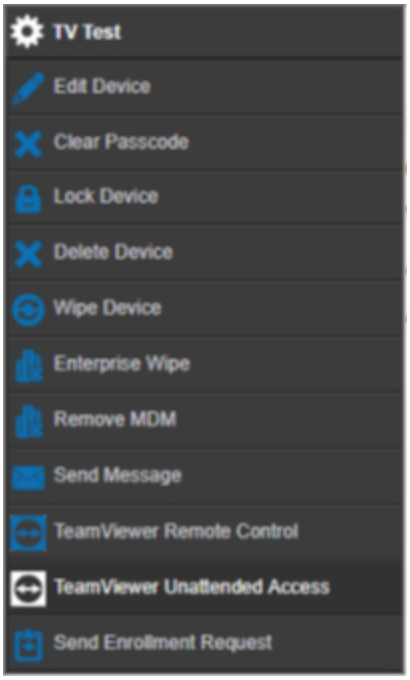
Poznámka: Bezobslužný přístup je možný pouze na zařízeních se systémem Android.



K zařízením se můžete připojit bez přijetí připojení na zařízení pouze v případě, že váš účet TeamViewer používá licenci "Tensor" nebo "Corporate".

Po propojení účtu to můžete zkontrolovat v části "Obecná nastavení".

Chcete-li používat bezobslužný přístup, musíte si nainstalovat aplikaci "TeamViewer Host" a aktivovat "Enable Unattended Access" v části "Kiosk Mode & Launcher" ve svém profilu. Upozorňujeme, že to je možné pouze v případě, že používáte režim Kiosk Mode.



Nyní můžete zvolit bezobslužný přístup, pokud vyberete zařízení a kliknete na kolečko. Tím se připojíte k zařízení bez nutnosti potvrzení na samotném zařízení. Upozorňujeme, že může chvíli trvat, než se zobrazí Odkaz pro přístup k zařízení.

Splashtop

Pokud povolíte možnost Splashtop, zobrazí se v profilech možnosti konfigurace Splashtop.

Chcete-li používat službu Splashtop, musíte ve svém profilu nastavit streamer Splashtop (com.splashtop.streamer.csrs) jako povinnou aplikaci. Poté můžete povolit konfiguraci Splashtop ve svém profilu v části "Vzdálené ovládání". Povolením této funkce se nakonfiguruje aplikace Splashtop Streamer. Pokud používáte aplikaci Splashtop Streamer, ale ne v kombinaci s MDM, měli byste tuto funkci ponechat vypnutou.

Ve svém profilu v části "Dálkové ovládání" musíte také nastavit kód nasazení. Přejděte na stránku https://my.splashtop.com a přihlaste se ke svému účtu Splashtop. Klikněte na "Add Computer" (Přidat počítač) a zkopírujte 12místný deploy kód z výsledné stránky.

Bez kódu Deploy Code není vzdálené ovládání možné.

Poté můžete kliknout pravým tlačítkem myši na zařízení a spustit vzdálenou relaci kliknutím na "Splashtop Remote Control".

Správa karet Sim

Hromadný import CSV

Zobrazí se přehled přidělených SIM karet a všechny informace o nich. To vám pomůže mít všechny informace nejen o vašich zařízeních, ale také o vašich SIM kartách v jednom systému.

POZNÁMKA: Jedná se o ruční správu/dokumentaci. Tato data není možné získat ze zařízení automaticky z důvodu ochrany soukromí/bezpečnostních mechanismů operačních systémů.

Tento seznam můžete také ex- a importovat jako CSV.

Dopravce a tarif

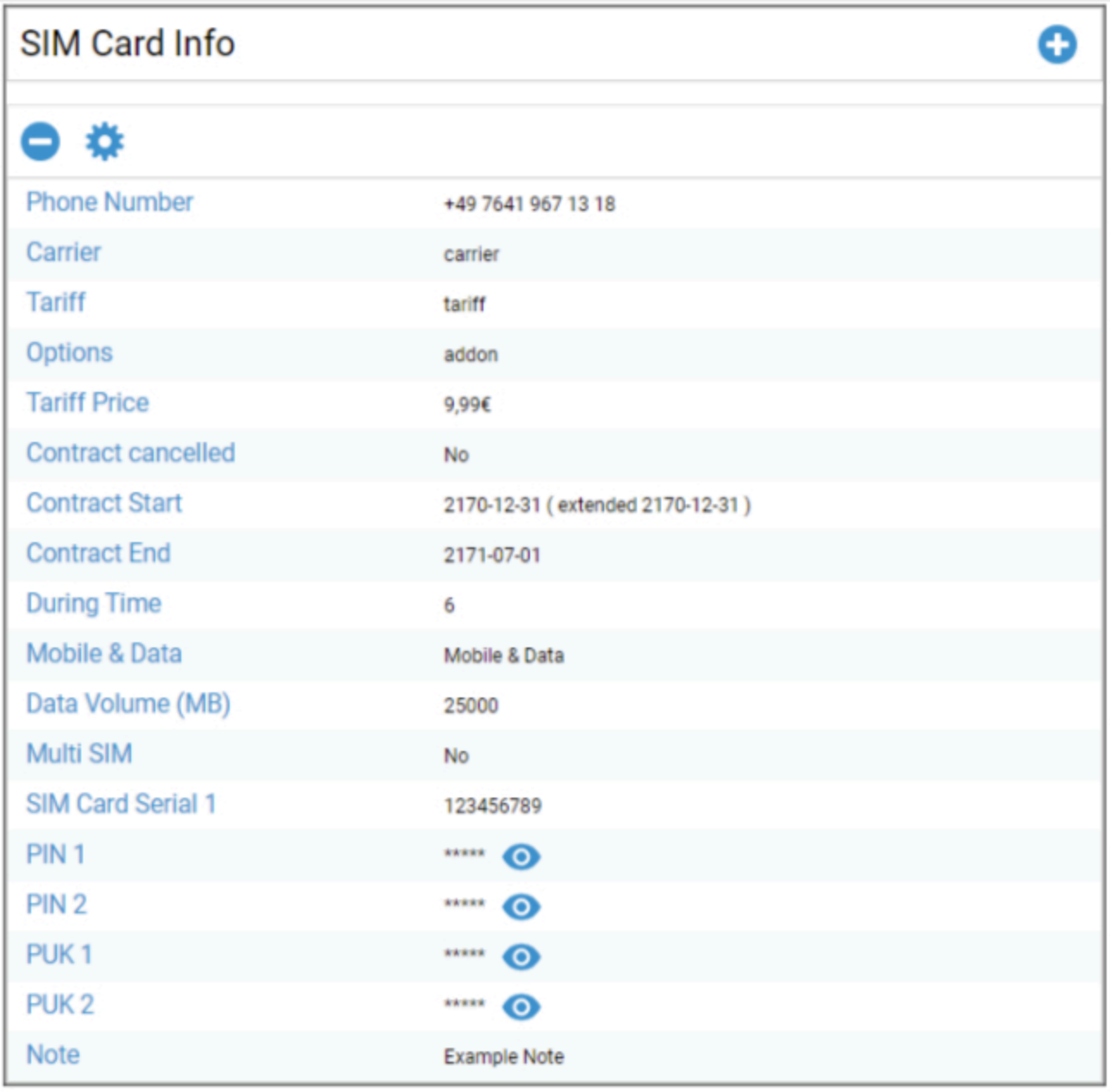
Chcete-li přidat SIM kartu, klikněte nejprve na tlačítko pro přidání jednoho nebo více operátorů.

Poté klikněte na tlačítko "+" v části "Informace o tarifu" a přidejte tarif k dopravci.

Volitelně můžete přidat volitelné doplňky níže, pokud máte něco takového.

Připraveno je vše, co potřebujete k přidání skutečné karty Sim. Karty Sim jsou v současné době přiřazeny k uživateli. Přejděte proto do Správy mobilních telefonů, vyberte Uživatele a přejděte na "Přehled sim karet.

Zde vidíte SIM karty těchto uživatelů. Pokud zde nějaká je, můžete ji upravit nebo odebrat. Uživatelé mohou mít více SIM karet.

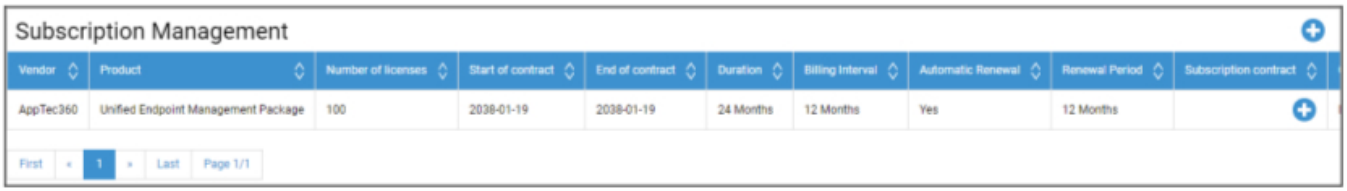


Klepnutím na "+" přidejte SIM kartu a přidejte všechny potřebné informace. Tyto Sim karty budou také uvedeny v seznamu všech vašich Sim karet v části Obecná nastavení → Správa Sim karet.

Správa předplatného

Správa předplatného

Zde můžete dokumentovat probíhající předplatné, jeho podrobnosti a také ukládat různé soubory, např. podepsanou smlouvu, výpověď smlouvy atd. Můžete si také nastavit upomínky, které vám před ukončením předplatného připomenou per mail a možná se automaticky prodlouží.



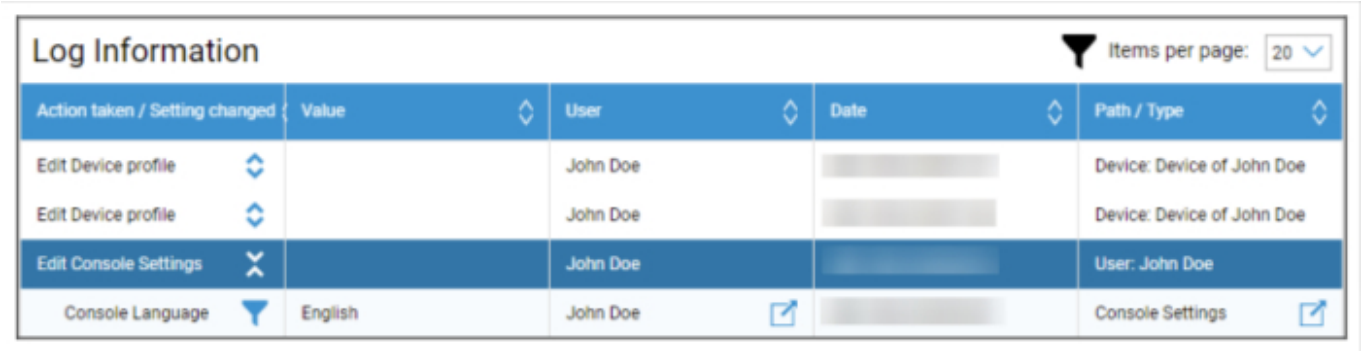
Chcete-li přidat odběr, klikněte na tlačítko "+" v horní části. Můžete přidat libovolný počet odběrů.

Chcete-li nahrát soubory týkající se tohoto předplatného, klikněte na "+" v různých polích. Technicky můžete nahrát jakýkoli typ souboru, ale mějte na paměti, že ne každý typ souboru lze zobrazit v prohlížeči.

Obecný protokol auditu

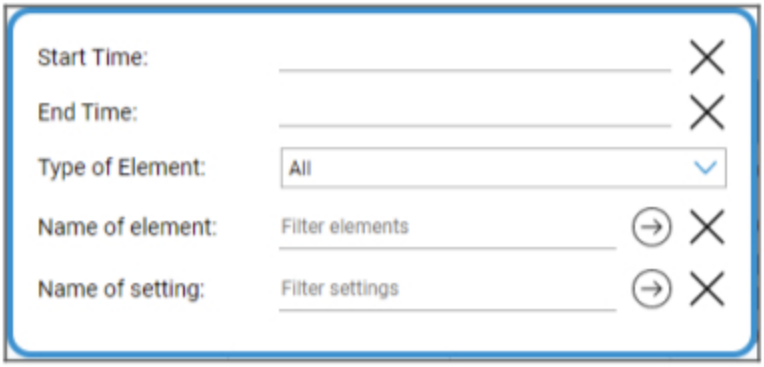
Protokol o auditu

Zde je k dispozici obecný protokol auditu, který zobrazuje všechny provedené změny. Zatímco v protokolu auditu u uživatele nebo skupiny se zobrazují pouze změny podle tohoto uživatele nebo skupiny, zde se zobrazuje KAŽDÁ změna provedená kdekoli v konzoli.



Můžete se podívat, co, kdo, kdy a kde změnil. V některých případech můžete záznam rozšířit a zobrazit další podrobnosti.

Kliknutím na uživatele nebo na položku v části "Cesta / Typ" se dostanete do umístění, kde byla změna provedena.



Vpravo nahoře můžete také definovat filtr, který může pomoci najít určité změny v prostředí, kde dochází k mnoha změnám.

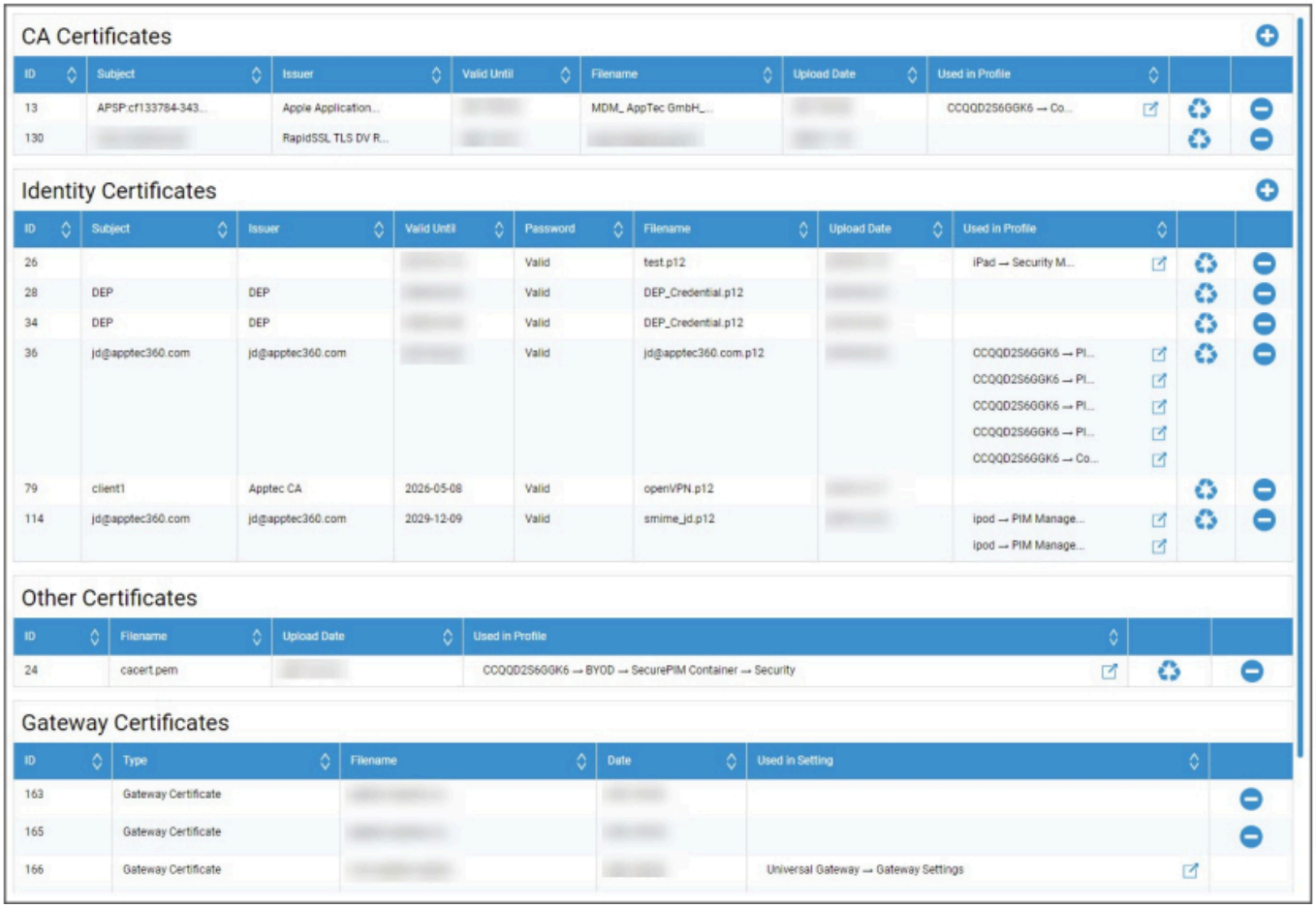
Nastavení protokolu auditu

"Doba uchovávání protokolů o auditu" definuje, jak dlouho by měly být protokoly o auditu uchovávány před jejich smazáním.

Správa certifikátů

Zde získáte přehled o všech certifikátech nahraných a použitých v konzole. Jedná se pouze o přehled. Skutečná konfigurace např. certifikátů Wi-Fi se stále provádí v profilu na příslušném místě.

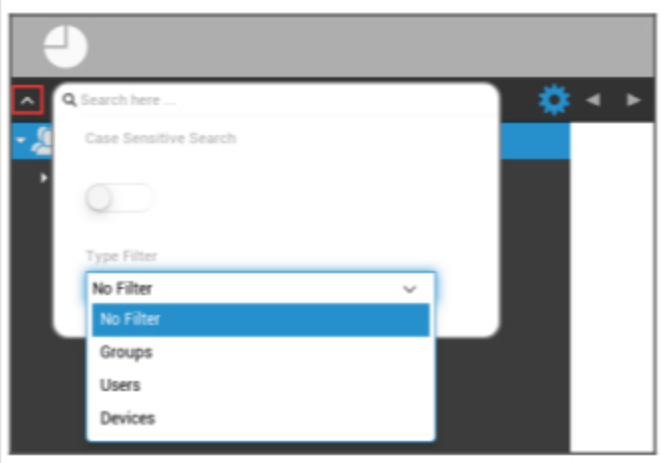
Zde můžete také odebrat nebo aktualizovat certifikáty, což se automaticky projeví v dotčených profilech. Kliknutím na informace v části "Použité v profilu" zjistíte, kde přesně je který certifikát ještě přiřazen.



Správa mobilních zařízení

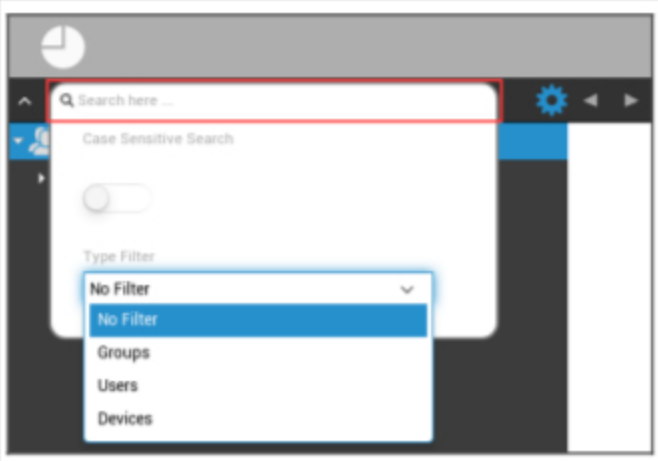
Obrazovka pro správu mobilních zařízení

Filtr zařízení



Kliknutím v levém horním rohu obrazovky najdete řadu filtrů pro zobrazení zařízení.

Vyhledávací okno



Okno vyhledávání umožňuje vyhledávat všechna zařízení a/nebo uživatele s určitým klíčovým slovem.

Volitelná výbava

Po kliknutí na příslušný symbol se zobrazí seznam možností, které máte k dispozici.

Ty se mění s každým aktuálním oknem a jsou vysvětleny v příslušných kapitolách.

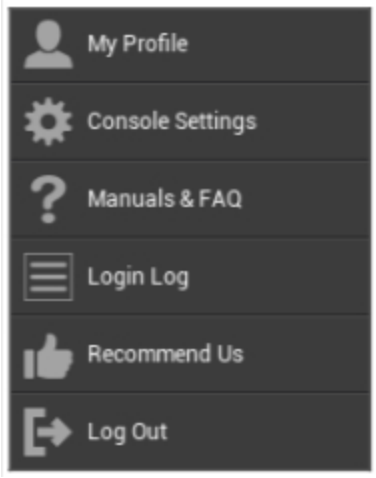
Navigační šipky

Kliknutím na šipku vlevo se dostanete na předchozí stránku.

Poté se kliknutím na šipku vpravo dostanete na stránku, kterou jste právě opustili.

Nastavení účtu pro správu

Kliknutím na e-mailovou adresu, jak je vidět výše, se zobrazí následující nabídka:



Můj profil	Úprava údajů o účtu správce
Nastavení konzoly	Konfigurace nastavení konzoly pro účet Admins
Příručky a nejčastější dotazy	Zobrazení stránky "Manuály a nejčastější dotazy" v části "Obecná nastavení".
Přihlašovací protokol	Přístup k "Přihlašovacímu protokolu"
Doporučte nás	Zobrazení stránky "Doporučit nás" v části "Obecná nastavení"
Odhlášení	Odhlášení z konzoly MDM

Informace pro uživatele

Zde můžete upravit údaje o účtu aktuálně přihlášeného správce.

Uživatelské jméno	Uživatelské jméno a/nebo e-mailová adresa účtu
Název	Křestní jméno správců
Příjmení	Příjmení správců
Přihlašovací jméno	Přihlašovací jméno správců
E-mailová adresa	E-mailová adresa správců
Alternativní e-mailová adresa	Náhradní e-mailová adresa správců
Obrázek	Profilový obrázek
Telefonní číslo	Telefonní číslo správců
Číslo mobilního telefonu	Číslo mobilního telefonu správce
Prodloužení telefonu	Prodloužení telefonu
Umístění	Umístění
Pozice	Pozice ve společnosti
Skupina uživatelů	Vyberte, do které skupiny uživatelů chcete přiřadit účet správce.
Komentář:	Zadejte komentář
Zadejte nové heslo	Zadejte heslo pro změnu hesla
Opakování nového hesla	Zopakujte nové heslo pro potvrzení

Vezměte prosím na vědomí, že administrátorský přístup může být ve struktuře hierarchie podán také jako místní uživatelský účet. Bez založení dalšího správce by tento neměl být odstraněn!

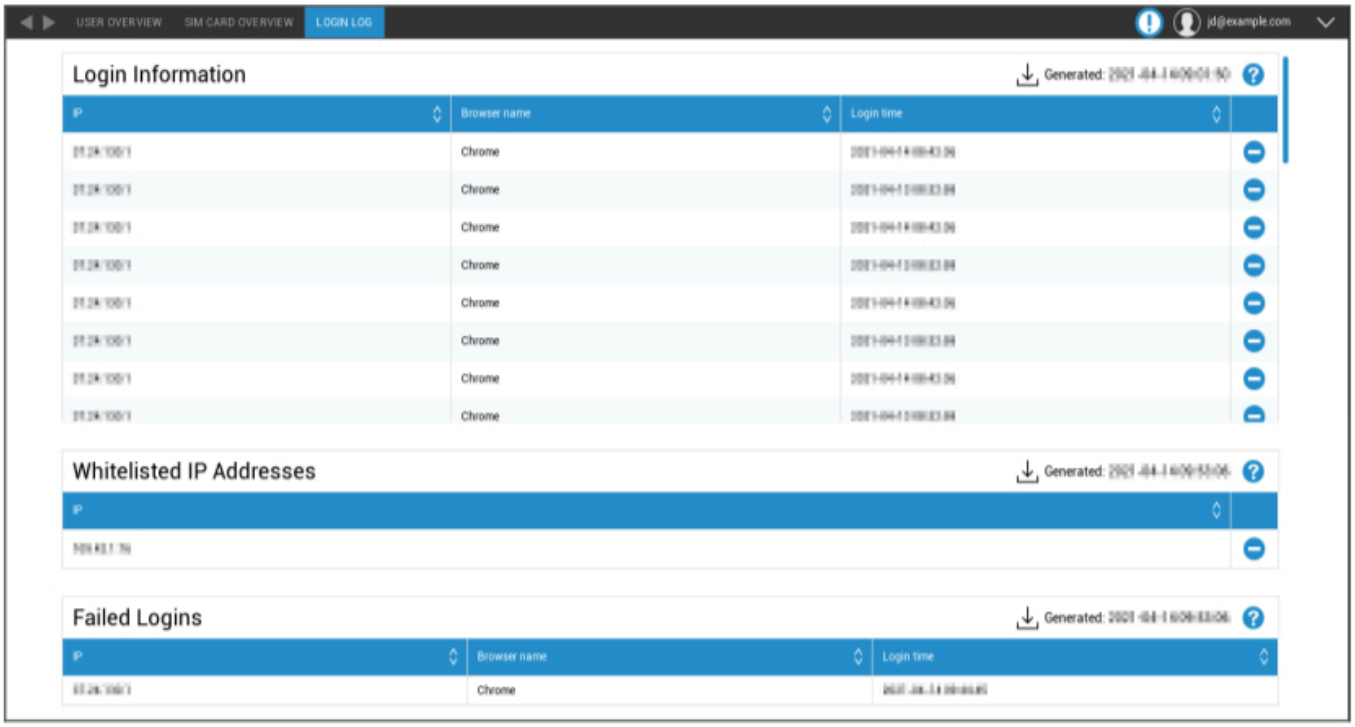
Nastavení konzoly

Zde můžete nakonfigurovat následující nastavení konzoly pro účet Admins:

Možnosti zobrazení uživatele adresáře	Definujte, jak mají být uživatelé ve stromu označeni.
Možnosti zobrazení adresářového zařízení	Definujte, jak mají být zařízení ve stromu označena.
Časový limit relace	Pokud uživatel v zadaném čase nic neudělá, bude odhlášen. Výchozí hodnota je 60 minut. Po změně tohoto nastavení se odhlaste a znovu přihlaste.
Časové pásmo	Výběr používaného časového pásma
Časový formát	Zvolte, jak se mají zobrazovat časová razítka
Jazyk konzoly	Vyberte jazyk, ve kterém se má konzola zobrazit. K dispozici je angličtina a němčina.
Hlavní barva	Můžete nastavit barvu, která bude použita jako základ pro barevné schéma konzoly. Můžete použít nástroj pro výběr barvy nebo zadat barvu v zápisu HTML HEX. Fungují i formátory RGB jako "růžová", "žlutá".
Uložit příkaz	Kombinace kláves pro spuštění ukládání bez stisknutí tlačítka "Uložit".
Použití dvoufaktorového ověřování	Povolte používání dvoufaktorového ověřování při přihlašování. Po přihlášení obdržíte e-mail s kódem, který musíte zadat pro přihlášení.
Časový limit dvoufaktorového ověřování	Nastavte dobu, po kterou nebudete po úspěšném ověření žádáni o dvoufaktorové ověření.
Odeslat ověřovací kód prostřednictvím	Ověřovací kód bude zaslán na vybrané možnosti. Zpráva o zařízení se zobrazí v aplikaci AppTec360 MDM na všech zařízeních se systémem Android a iOS, která vám patří.
Odeslání přihlašovací zprávy po přihlášení	Pokud je tato možnost povolena, bude při každém přihlášení z ip adresy, která není na bílé listině, odeslán e-mail. E-mail obsahuje informace o přihlášení (např. IP, prohlížeč).

Přihlašovací protokol

Zde můžete zobrazit informace o přihlášeních aktuálně přihlášeného účtu správce.



Přihlašovací údaje	Seznam obsahující přihlášení aktuálně přihlášeného účtu správce, která byla zaznamenána konzolou. Tento seznam zobrazuje všechna vaše úspěšná přihlášení za posledních 30 dní.
IP adresy na bílé listině	Toto je seznam všech vašich IP adres na bílé listině. Pokud se přihlásíte z IP adresy, která je zde uvedena, zpráva o přihlášení se nezobrazí. IP adresu můžete do tohoto seznamu přidat kliknutím na tlačítko vedle položky ve výše uvedeném seznamu "Přihlašovací údaje". IP adresu můžete z tohoto seznamu odstranit kliknutím na tlačítko vedle položky v tomto seznamu nebo v seznamu "Přihlašovací údaje" výše.
Neúspěšná přihlášení	Toto je seznam všech neúspěšných pokusů o přihlášení za posledních 30 dní. Pokud se vám nepodařilo zadat správné heslo alespoň třikrát během 20 minut, objeví se v tomto seznamu položka. O neúspěšných pokusech o přihlášení budete informováni také e-mailem.

Podniková správa (kořenový uzel) v mobilní správě

Po dosažení kořenového uzlu (první skupiny) můžete provést řadu nastavení pro vaši společnost, pokud jde o správu mobilních zařízení.

Vytvoření podskupiny	Vytvoření podskupiny
Přejmenování kořenového uzlu	Přejmenování kořenového uzlu (např. název vaší společnosti)
Hromadný zápis	Registrace více zařízení / uživatelů najednou
Hromadné přiřazení	Přiřazení profilu pro příslušné skupiny s jedním pohledem
Rychlá správa aplikací	Odesílání požadavků na (ne)instalaci aplikace příslušným skupinám zařízení.
Import uživatelů CSV	Import uživatelů z CSV do příslušné skupiny

Vytvoření podskupiny

Pomocí funkce "Vytvořit podskupinu" můžete vytvořit další podskupinu.

Můžete určit, do které skupiny má být podskupina zařazena.

(Ve výchozím nastavení je vytvořena nová skupina, která je přiřazena jako podskupina v kořenovém uzlu).

Přejmenování kořenového uzlu

Zde můžete přejmenovat svůj kořenový název. Je běžné, že se v tomto případě používá název společnosti.

Hromadný zápis

Pomocí funkce "Hromadný zápis" můžete zapsat více zařízení a uživatelů.

Můžete přímo zvolit, jakým způsobem má uživatel obdržet zápis (eMail; alternativní eMail; SMS).

V závislosti na tom, jaké zařízení uživatel obdrží (iOS, Android, Windows Phone), jej zde můžete přímo označit.

Zde lze také nastavit, zda se jedná o chytrý telefon nebo tablet, což je třeba správně zaškrtnout.

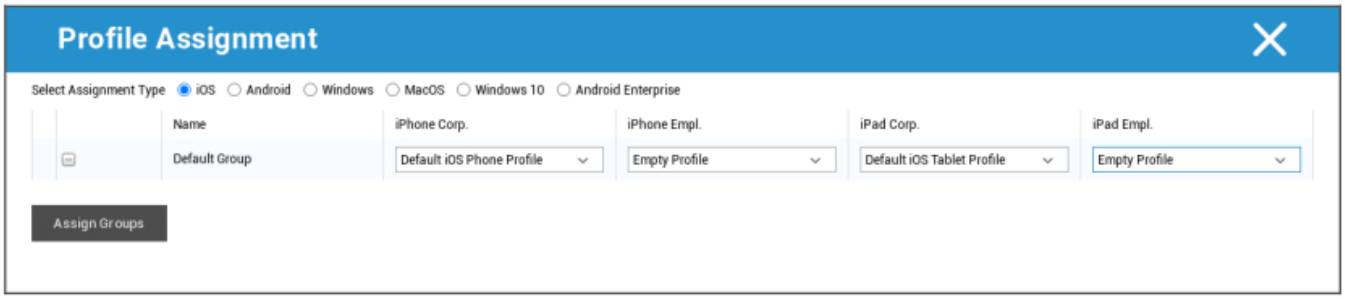
V posledním kroku můžete zjistit, zda je příslušné zařízení firemní nebo soukromé (BYOD).

Pomocí možnosti "Exportovat jako CSV" můžete exportovat informace jako datový soubor CSV. Na oplátku můžete také importovat datový soubor CSV pomocí "Import CSV", soubor by měl vypadat jako v příkladu níže:

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

Hromadné přiřazení

V části Hromadné přiřazení můžete přiřadit profil všem skupinám, které jsou rozděleny na iOS - Android - Windows - MacOS - Windows 10 - Android Enterprise.

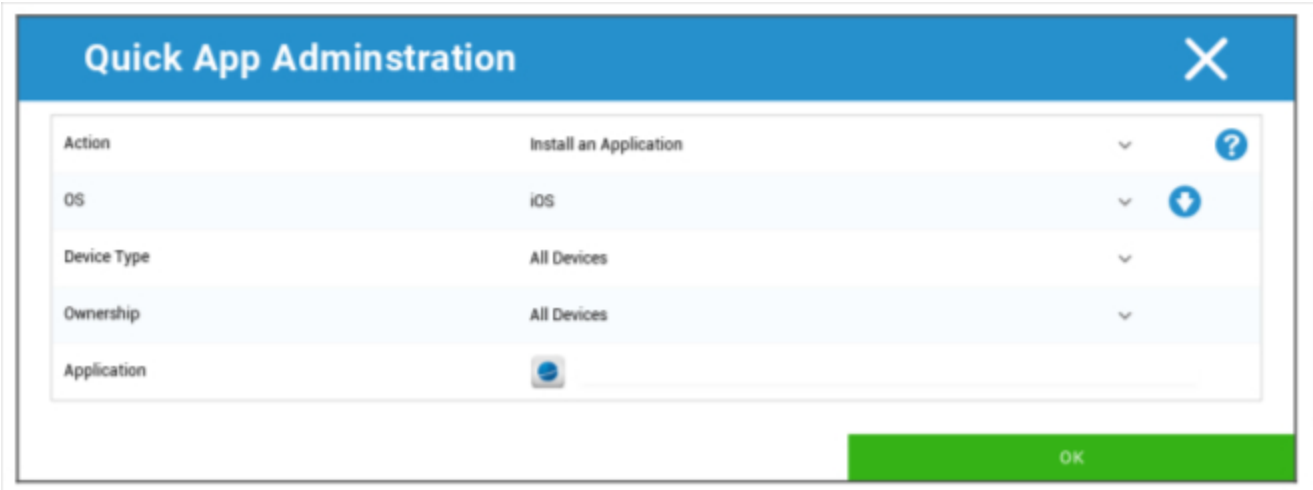


Windows - MacOS - Windows 10 - Android Enterprise

Rychlá správa aplikací

V části Rychlá správa aplikací můžete odesílat požadavky na instalaci nebo odinstalaci zadané aplikace do vybraného operačního systému.

Můžete také definovat, zda má být požadavek odeslán na všechny typy zařízení vybraného operačního systému, nebo pouze na konkrétní typ zařízení.



Import uživatelů CSV

Importovat uživatele z CSV do příslušné skupiny.

Pomocí funkce "Stáhnout šablonu CSV" můžete exportovat soubor šablony CSV, který lze vyplnit (nebo jej lze použít jako referenci).

Volby "Show Role Ids" a "Show Group Ids" můžete také použít jako odkaz pro vytvoření vlastního souboru CSV.

Soubor CSV lze do MDM nahrát pomocí "Nahrát CSV".

V posledním kroku můžete spustit import kliknutím na "Start Import".

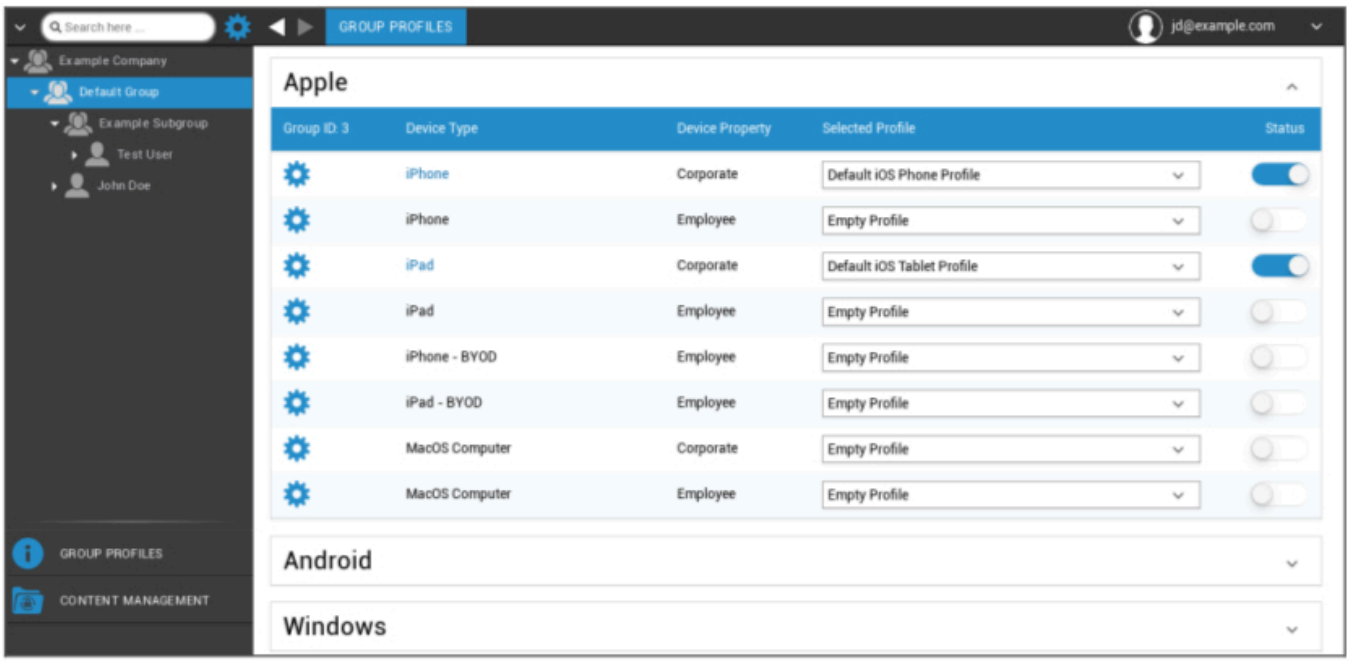
Správa skupiny v mobilní správě

Jedním kliknutím na přehled se zobrazí různé konfigurační profily pro příslušné platformy.

Jeden profil obsahuje všechny možnosti nastavení, které lze pomocí AppTec360 předem nastavit v zařízení koncového uživatele. Na každé platformě můžete vytvořit profily pro firemní zařízení (Corporate) nebo zařízení Bring-Your-Own-Device (Employee).

Pro odlišení konfigurací skupin zařízení, například podle umístění nebo funkce, se doporučuje vytvořit několik podskupin.

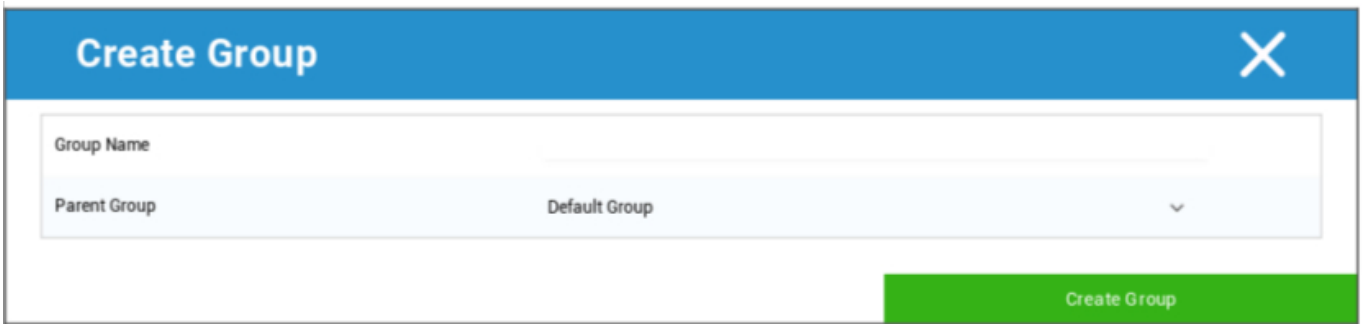
Vezměte prosím na vědomí správu profilů v mobilní správě



V nabídce převodovky můžete nastavit různá nastavení pro příslušnou (pod)skupinu.

Vytvoření podskupiny	Vytvoření podskupiny pro příslušnou (pod)skupinu
Upravit vybranou skupinu	Upravit vybranou skupinu
Odstranění vybrané skupiny	Odstranění vybrané skupiny
Hromadný zápis	Registrace mnoha zařízení / uživatelů najednou pro vybraný profil
Hromadné přiřazení	Přiřazení profilů do aktuálně vybrané skupiny
Vytvoření podskupiny	Vytvoření podskupiny pro příslušnou (pod)skupinu
Vytvoření uživatele	Vytvoření uživatele pro příslušnou (pod)skupinu

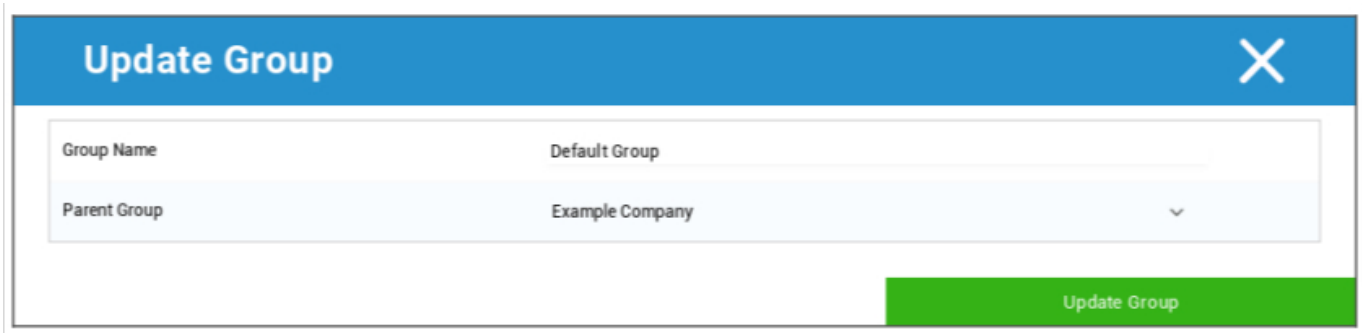
Vytvoření podskupiny



Pomocí funkce "Vytvořit podskupinu" můžete vytvořit další podskupinu.

Můžete určit, pod kterou skupinu má být podskupina přiřazena (ve výchozím nastavení je podskupina přiřazena pod skupinu, která je aktuálně vybrána).

Upravit vybranou skupinu



Zde můžete profil upravit - jsou zde možná následující nastavení:

- Název skupiny lze změnit
- Rodičovskou skupinu lze změnit

Odstranění vybrané skupiny

V části "odstranit vybranou skupinu" se zobrazí seznam všech uživatelů a zařízení, kteří jsou v příslušné skupině. Zde máte možnost je odstranit.

Pro jednoho uživatele můžete provést následující příkazy k odstranění:

Odstranit uživatele	Uživatel je smazán
Přesunout uživatele do skupiny:	Uživatele můžete přesunout do jiné skupiny (následující sloupec, např. "Admins).

Pro jedno zařízení můžete provést následující příkazy k odstranění:

Vymazání a odstranění	Vymazání a odstranění zařízení
Odstranit ze systému	Odstranění zařízení pouze z AppTec

Odkaz: Hromadný zápis

Odkaz: Hromadné přidělení

Vytvoření uživatele

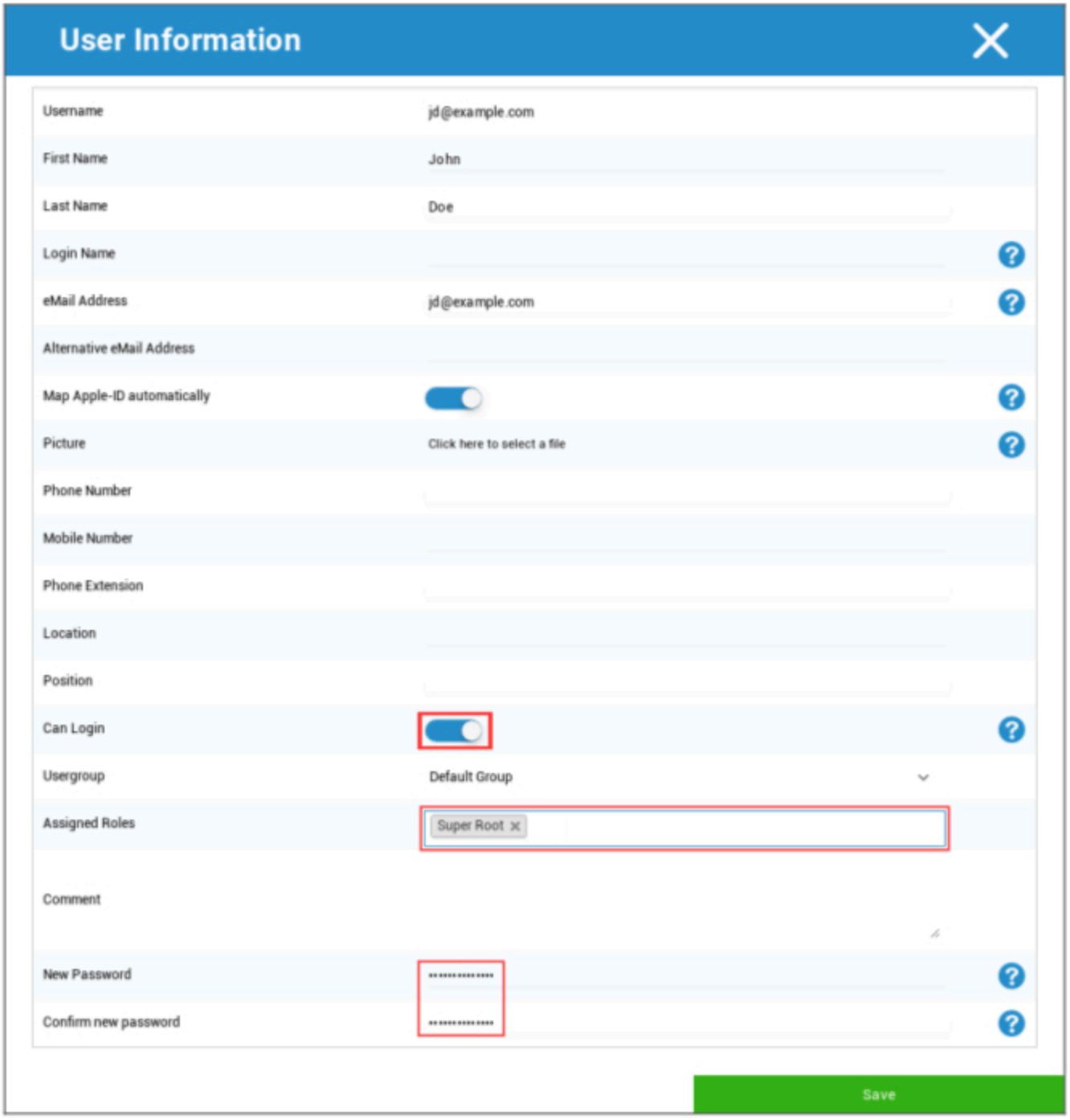
Pomocí funkce "Vytvořit uživatele" můžete přidat nového uživatele.

Vytvoření nového správce-uživatele

Uživatele můžete nastavit jako uživatele Admin-User. Tím mu dáte oprávnění přihlašovat se do konzoly a také měnit uživatele/skupiny/zařízení.

Vytvořte normálního uživatele nebo použijte stávajícího uživatele. Vyberte Uživatele, kterému chcete udělit oprávnění správce, klikněte na kolečko a vyberte možnost "Upravit uživatele":

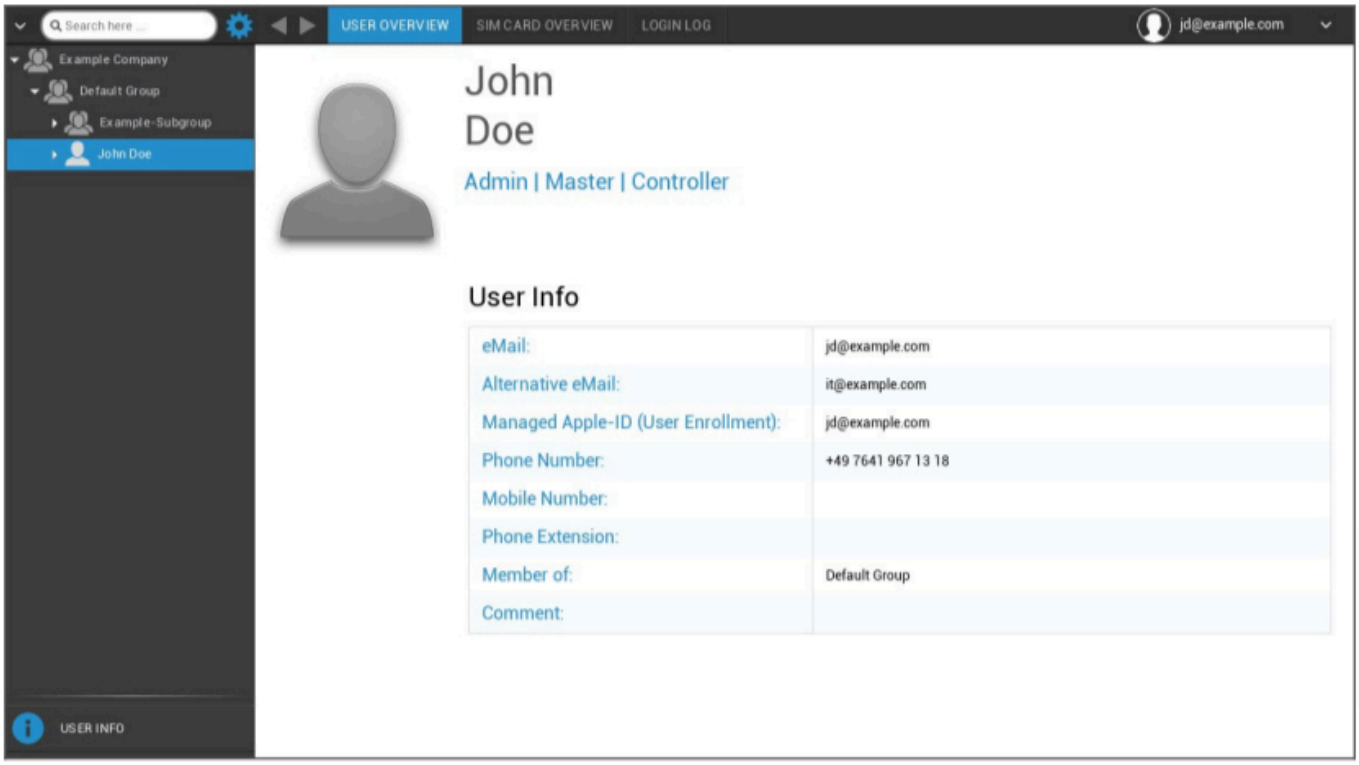
Aktivujte přepínač "Can Login", přiřaďte uživateli roli "Super-Root" a nastavte heslo.



Uložíte jej a uživatel se nyní může přihlásit pomocí uživatelského jména a hesla.

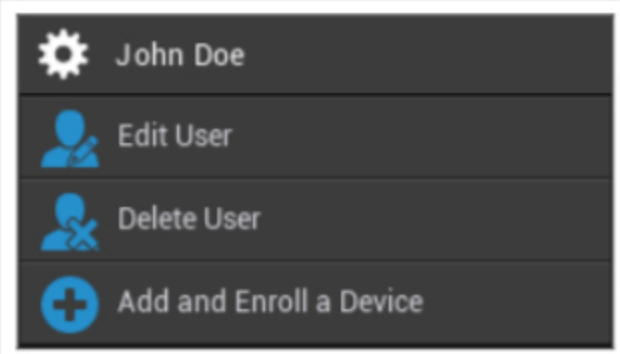
Správa uživatelů v mobilní správě

Po výběru určitého uživatele se zobrazí následující přehled:



Zobrazí se vám přehled všech informací, které jste zadali v části "Vytvořit uživatele".

S převodovkou, která je nainstalována nahoře, můžete provést následující konfigurace:



Uživatelské jméno	Uživatelské jméno vybraného uživatele
Upravit uživatele	Úprava informací o uživateli
Odstranění uživatele	Odstranění uživatele • Odstranit ze systému = zařízení bude odstraněno z AppTecu.

	• Wipe & Delete = zařízení bude obnoveno do továrního nastavení a odstraněno z AppTecu.
Přidání a registrace zařízení	Zapsat zařízení pro vybraného uživatele

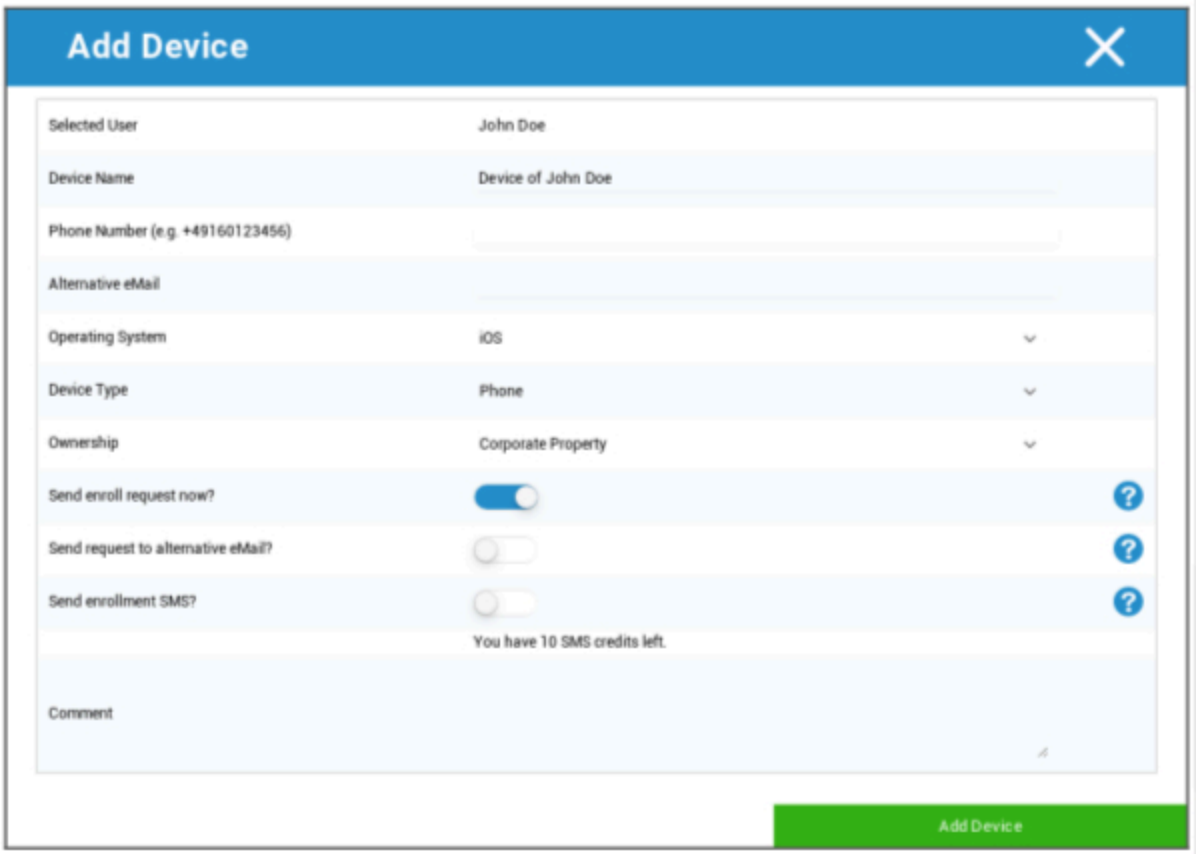
Vezměte prosím na vědomí, že administrátorský přístup může být ve struktuře hierarchie podán také jako místní uživatelský účet. Bez založení dalšího správce by tento neměl být odstraněn!

Přidání a registrace zařízení

Zde můžete vybrat zařízení pro vybrané použití.

Případně můžete zařízení do skupiny zapsat přímo. To provedete tak, že kliknete na skupinu, kliknete na kolečko a vyberete možnost "Přidat a zapsat zařízení".

Měl by se zobrazit následující přehled:



V závislosti na typu zařízení, které chcete zaregistrovat, je třeba provést následující konfigurace:

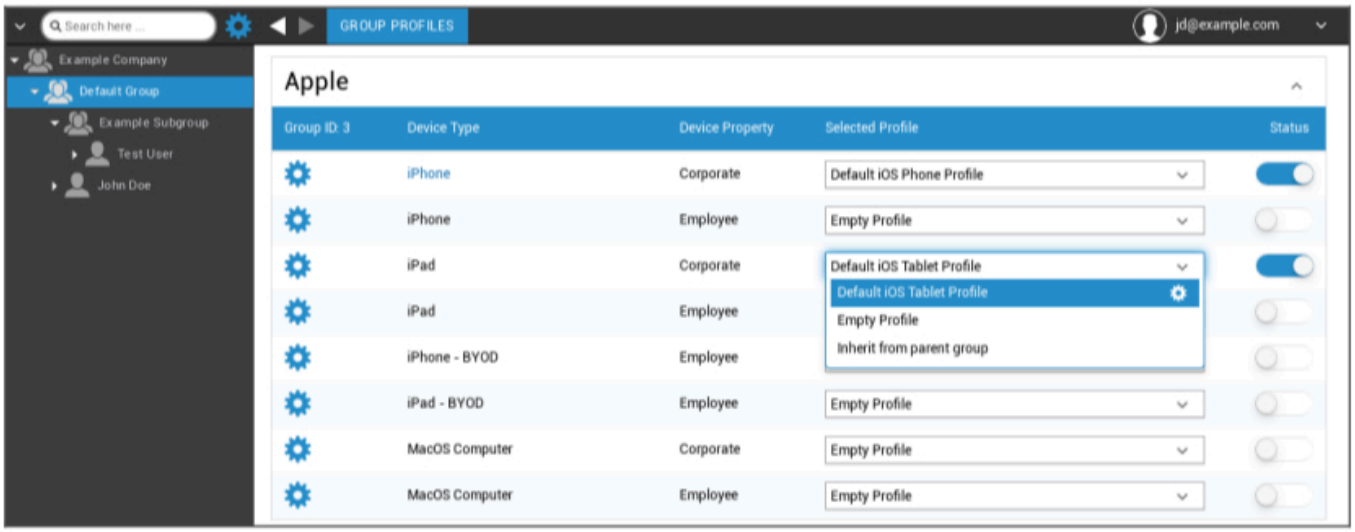
Vybraný uživatel	Vybraný uživatel (vyplní se automaticky)
Název zařízení	Vyplní se automaticky (zařízení pro "jméno uživatele") - lze však změnit.
Telefonní číslo	Telefonní číslo se vyplní automaticky (pokud bylo uživatelem zadáno) - zde jej však lze doplnit nebo změnit.
Alternativní e-mail	Alternativní e-mail, vyplní se automaticky (pokud jej uživatel zadal) - zde jej však lze přidat nebo změnit.
Vlastník zařízení	Firemní majetek = firemní zařízení Majetek zaměstnance = zařízení BYOD
Zvolte operační systém	Zde si můžete vybrat z následujících operačních systémů: • iOS • iOS BYOD (registrace uživatelů) • MacOS • Android Enterprise • Android • Windows Mobile • Windows 10
Odeslat žádost o zápis?	E-mail je okamžitě odeslán na hlavní e-mailovou adresu a uživatel je vyzván k připojení svého zařízení.
Odeslat žádost na alternativní e-mail?	Odeslání e-mailu dodatečně nebo výhradně (v případě, že byla možnost "Odeslat žádost o zápis?" deaktivována) na alternativní e-mailovou adresu (e-mail se liší od "normálního" e-mailu s žádostí o zápis).
Odeslat registrační SMS?	Odeslání žádosti o registraci prostřednictvím SMS (je třeba zadat "telefonní číslo").

Po odeslání žádosti o registraci se zařízení ihned zobrazí (označeno červeně).

Jakmile je zařízení úspěšně připojeno, krátce poté se označí zeleně, a je tak připraveno přijímat omezení, aplikace atd.

Správa profilů v mobilní správě

Po kliknutí na skupinu se zobrazí přehled všech platforem zařízení, které mají být nakonfigurovány, a přiřazených profilů.



	Provedení konfigurace vybraného profilu
Typ zařízení	Typ a/nebo model zařízení
Vlastnost zařízení	Vlastník zařízení (Corporate = firemní majetek, Employee = soukromé zařízení zaměstnance)
Vybraný profil	Vybraný profil (ozubené kolečko otevře dialog konfigurace profilu)
Stav	Zapnuto/vypnuto (profil je aktivován/deaktivován)

Po výběru převodovky se zobrazí následující možnosti:

Vytvoření profilu

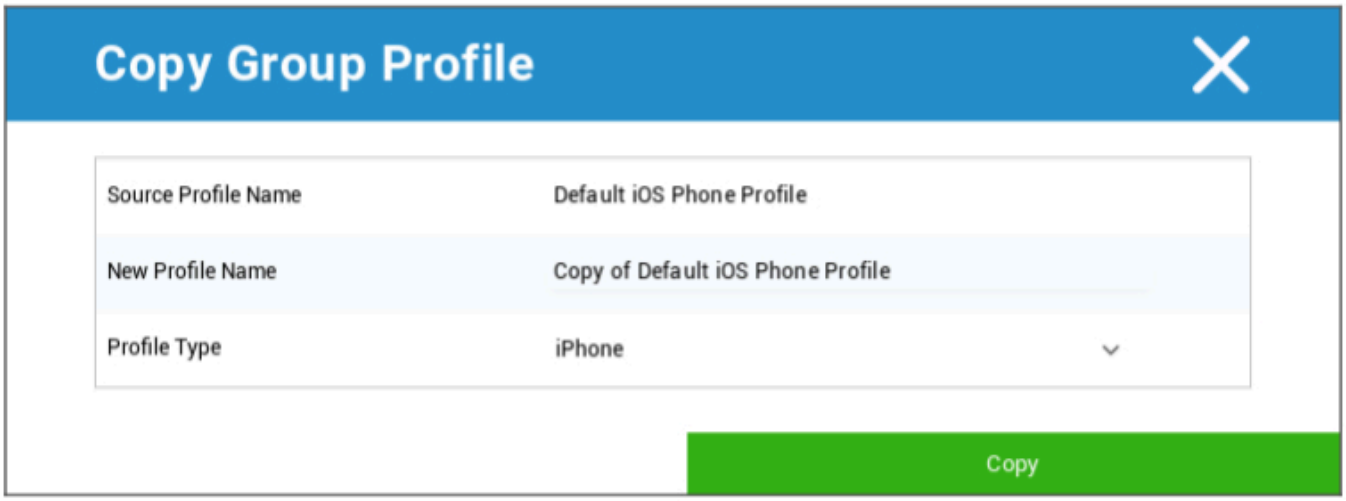
Pro každou položku a/nebo platformu můžete vytvořit a nakonfigurovat nový profil. Po kliknutí na tento dílčí bod se profil ihned vytvoří a vy můžete ihned začít s konfigurací pro iOS, Android a Windows Phone.

Upravit profil

Po kliknutí na "Upravit profil" se zobrazí konfigurace příslušného profilu, kde můžete nastavit konfigurace.

Kopírovat profil

Pomocí funkce "Kopírovat profil" můžete zkopírovat nastavení/konfigurace z již existujícího profilu a přidat je do nového profilu.

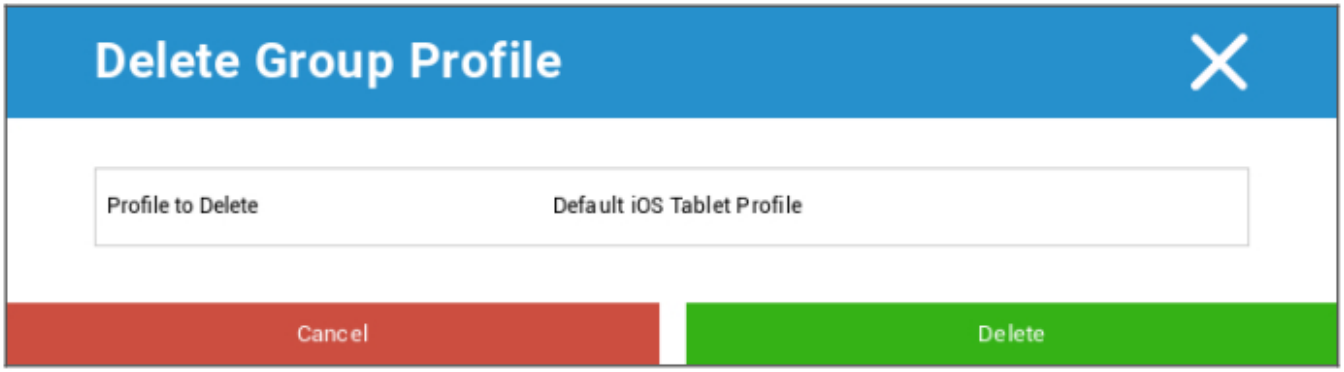


Název profilu zdroje	Název profilu, který má být zkopírován
Nový název profilu	Název nového profilu
Typ profilu	Typ profilu (Telefon/Tablet)

Po kliknutí na tlačítko "Kopírovat" se profil vytvoří a nyní jej lze přiřadit ke skupině.

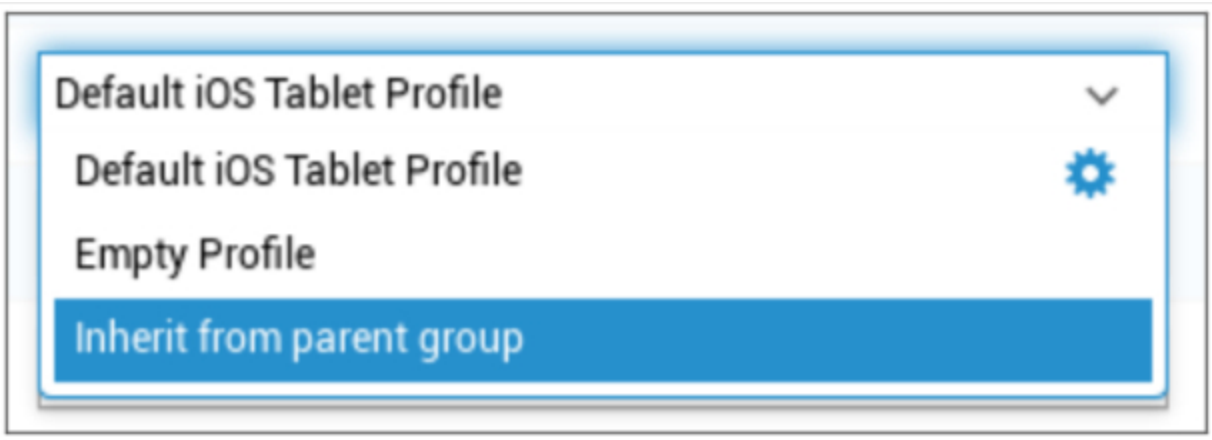
Smazat profil

Zde můžete profil trvale odstranit. Upozorňujeme, že během procesu mazání a následujícího procesu "Assign Now" pro profil zmizí konfigurace na příslušných zařízeních dotčené skupiny a nelze ji obnovit!


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

Dědictví profilů

Při výběru profilů je k dispozici možnost "Zdědit z nadřazené skupiny".



Pokud je profil aktivován, použije se pro vybrané zařízení (a příslušný typ zařízení) profil nadřazené skupiny. Mějte také na paměti, že změny tohoto profilu mohou případně ovlivnit řadu skupin.

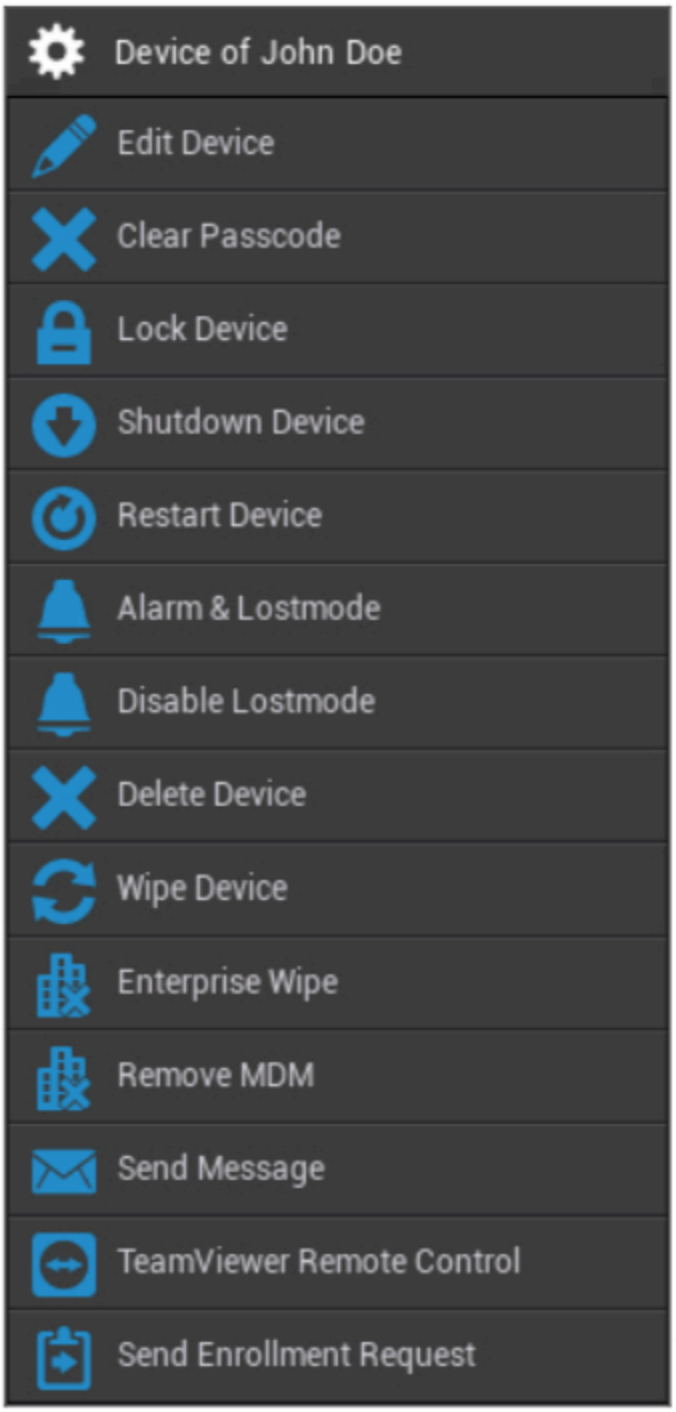
Tato konfigurace je při vytvoření nové podskupiny nastavena jako výchozí hodnota.

K dispozici je také konfigurace "Prázdný profil", která odpovídá prázdnému profilu, což znamená, že na zařízení koncového uživatele nebudou nakonec provedeny žádné nové konfigurace.

Správa zařízení v mobilní správě

Když vyberete zařízení, můžete pomocí ozubeného kola provádět různé úkoly. Ty se liší v závislosti na platformě operačního systému (iOS, Android Enterprise, Android, Windows Mobile, Windows 10).

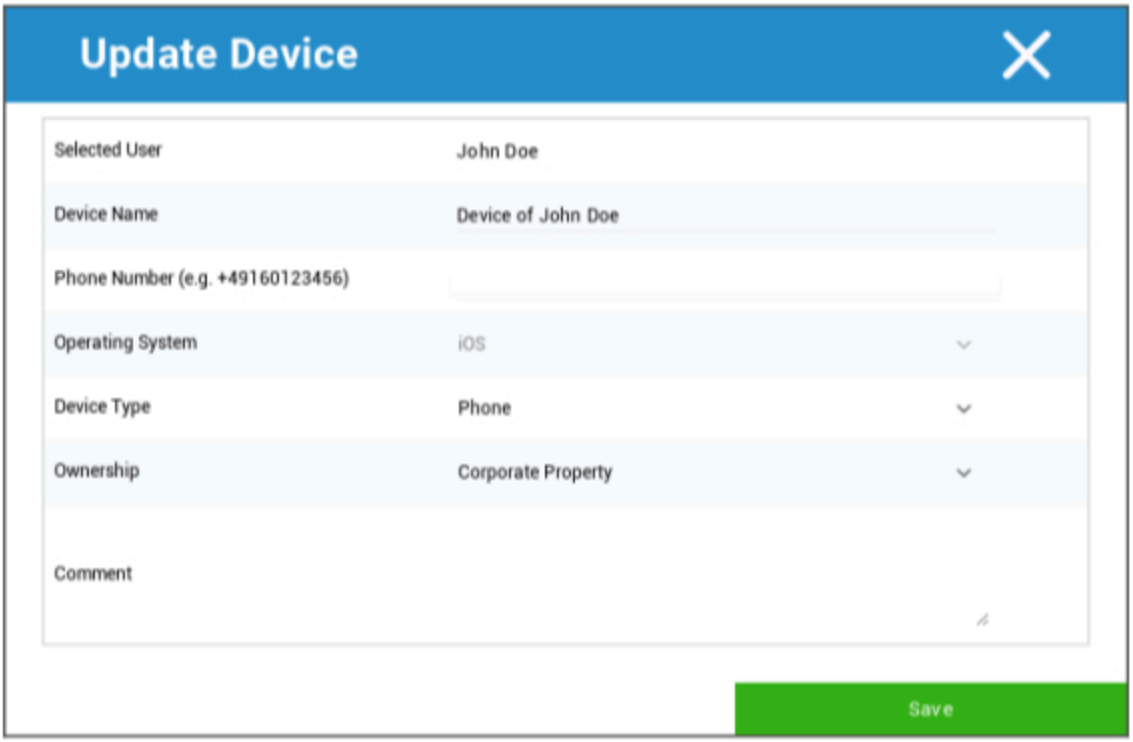
IOS



Upravit zařízení	Upravit zařízení
Vymazání přístupového kódu	Přístupový kód zařízení je vymazán
Zámek zařízení	Uzamčení zařízení (zamykací obrazovka)
Zařízení pro vypnutí	Vypínací zařízení

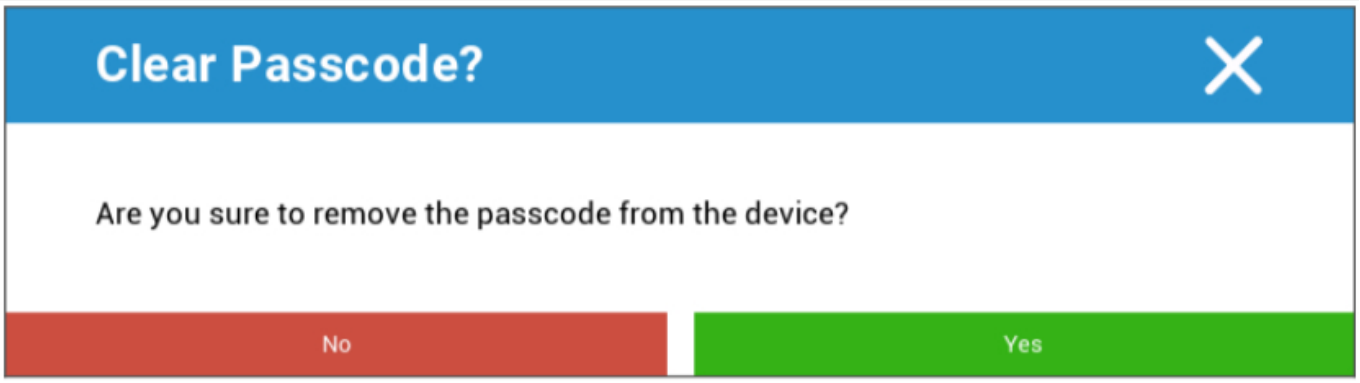
Restartování zařízení	Restartování zařízení
Alarm & Lostmode	Spuštění alarmu a ztrátového režimu
Zakázat Lostmode	Zakázat Lostmode
Odstranit zařízení	Odstranění zařízení z AppTec
Zařízení na stírání	Obnovení továrního nastavení zařízení
Podnikové utírání	Informace, aplikace a profily poskytnuté AppTec360 jsou smazány (zařízení je odděleno od MDM).
Odstranění MDM	
Odeslat zprávu	Odesílání oznámení Push do zařízení Zpráva se zobrazí v aplikaci AppTec360 (záložka Zpráva).
Vzdálené ovládání TeamViewer	Spuštění relace vzdáleného ovládání pomocí aplikace TeamViewer
Odeslat žádost o zápis	Odeslání (opakované) žádosti o zápis

Upravit zařízení



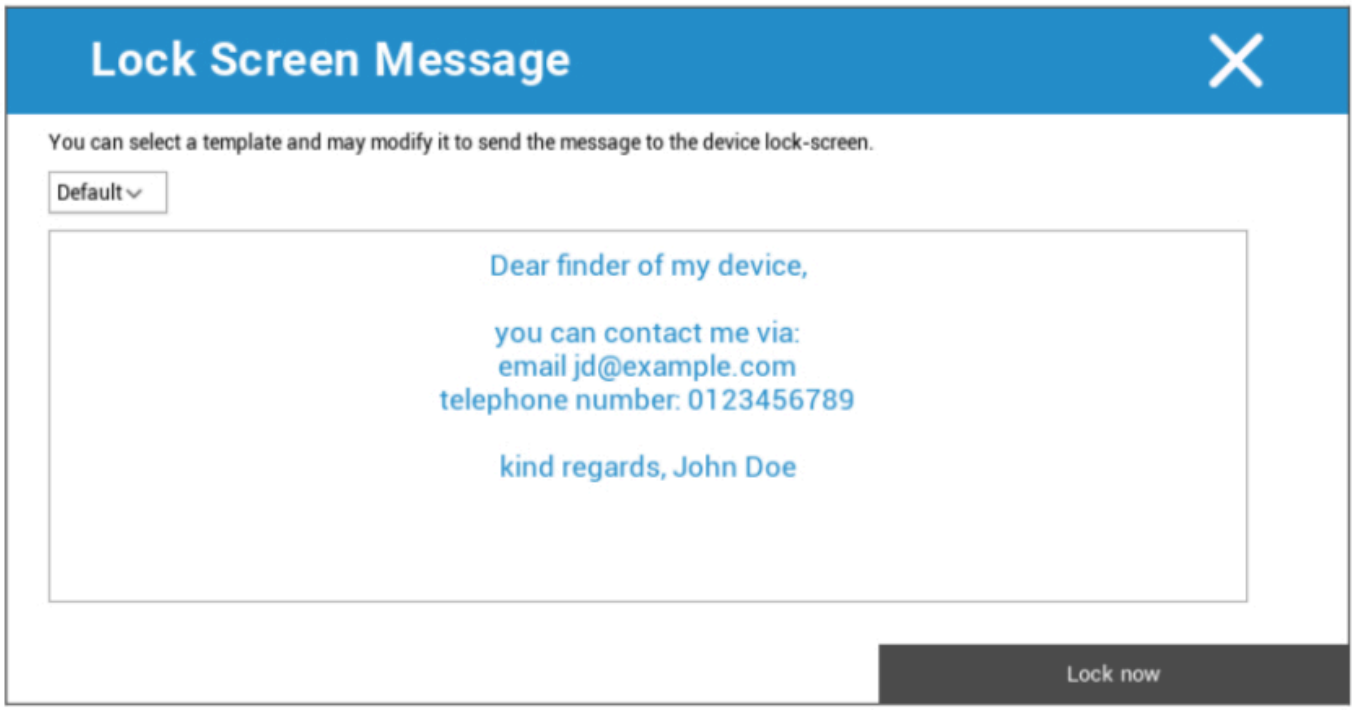
Zde můžete aktualizovat řadu informací o zařízení.

Vymazání přístupového kódu



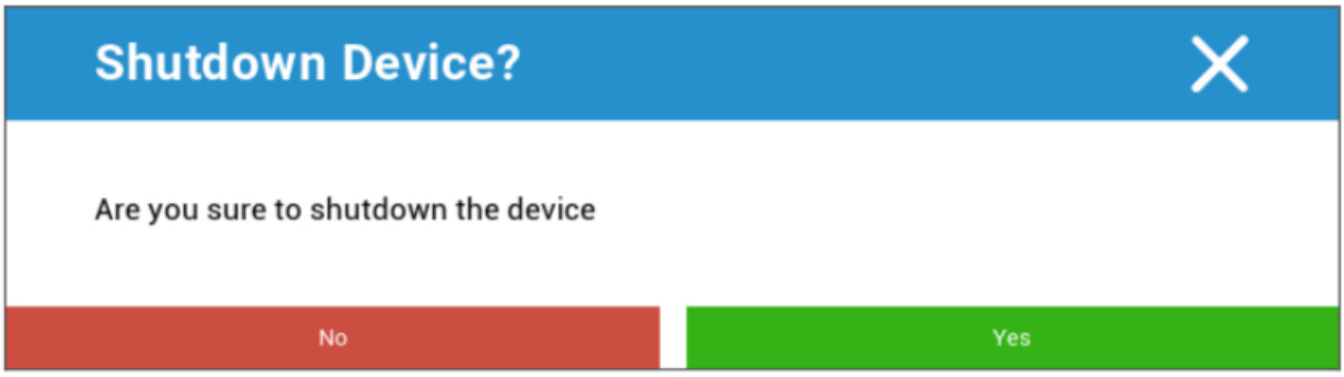
V části "Vymazat přístupový kód" můžete vzdáleně odstranit přístupový kód ze zařízení. Následně bude uživatel vyzván k zadání nového hesla (v závislosti na pokynech pro zadávání přístupových kódů).

Zámek zařízení



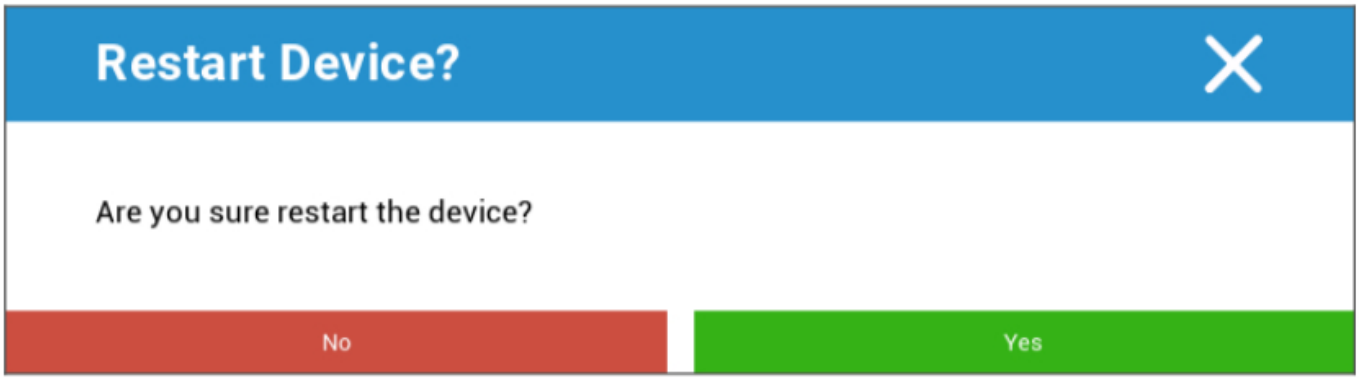
Zde je do zařízení koncového uživatele odeslán příkaz k uzamčení (zamykací obrazovka).

Vypínací zařízení



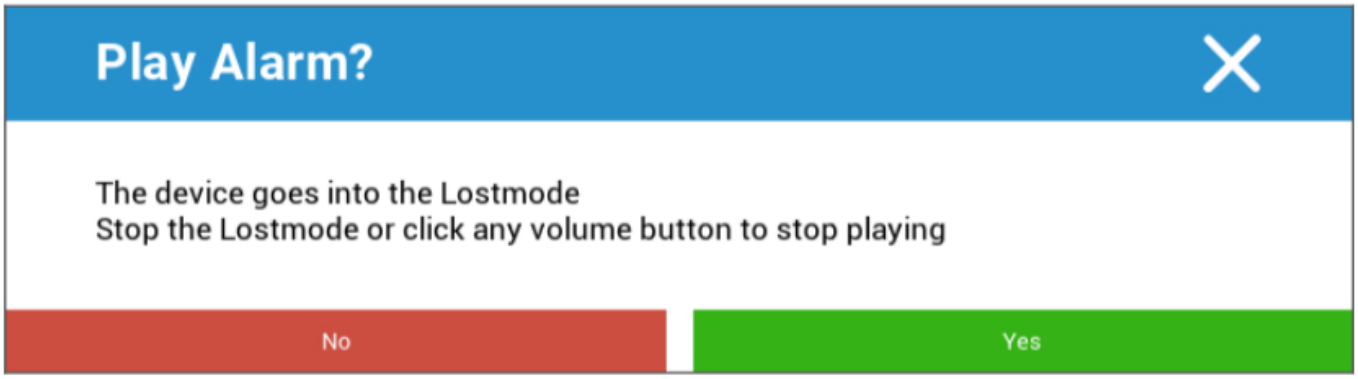
Zde je do zařízení koncového uživatele odeslán příkaz k vypnutí.

Restartování zařízení

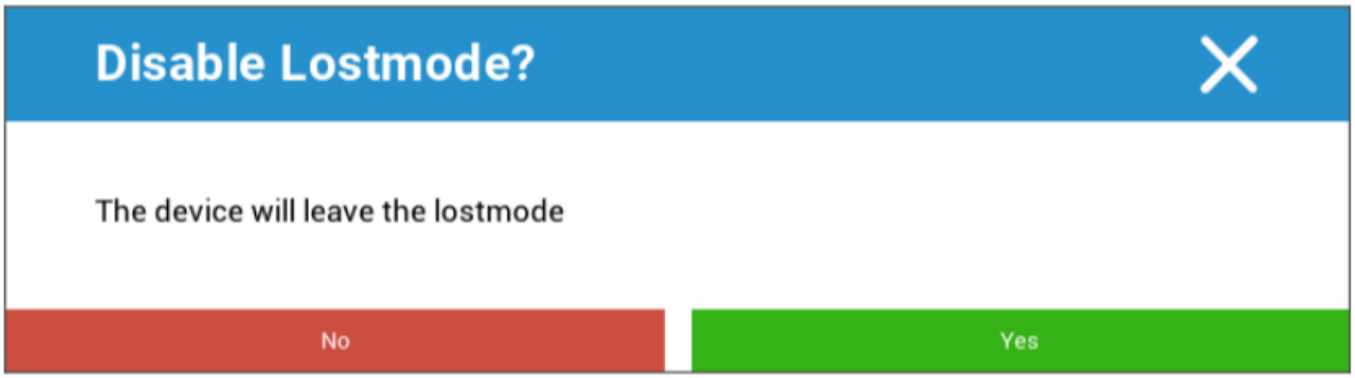


Zde je do koncového uživatelského zařízení odeslán příkaz k restartu.

Alarm a ztrátový režim | Zakázat ztrátový režim



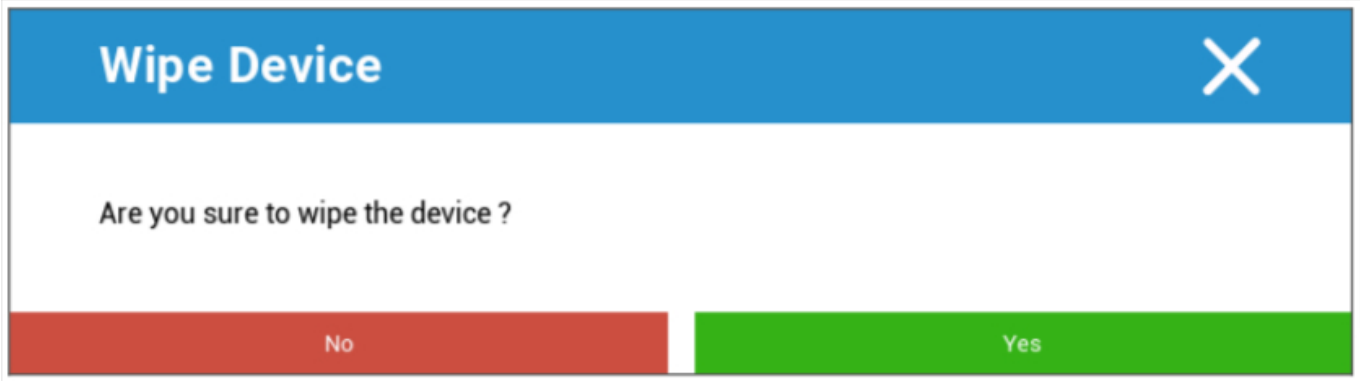
Zde lze zařízení nastavit do režimu Lostmode, který nastaví zařízení tak, aby neustále přehrávalo zvuk budíku. Režim Lostmode lze zastavit stisknutím libovolného tlačítka hlasitosti zařízení nebo vzdáleně kliknutím na "Disable Lostmode" (Zakázat režim Lostmode):



Odstranit zařízení

Zde lze provést příkaz k odstranění. Opět se můžete rozhodnout, zda má být zařízení odstraněno pouze z AppTec360 ("Delete from System"), nebo zda má být zařízení odstraněno z AppTec360 a zároveň obnoveno do továrního nastavení ("Wipe & Delete").

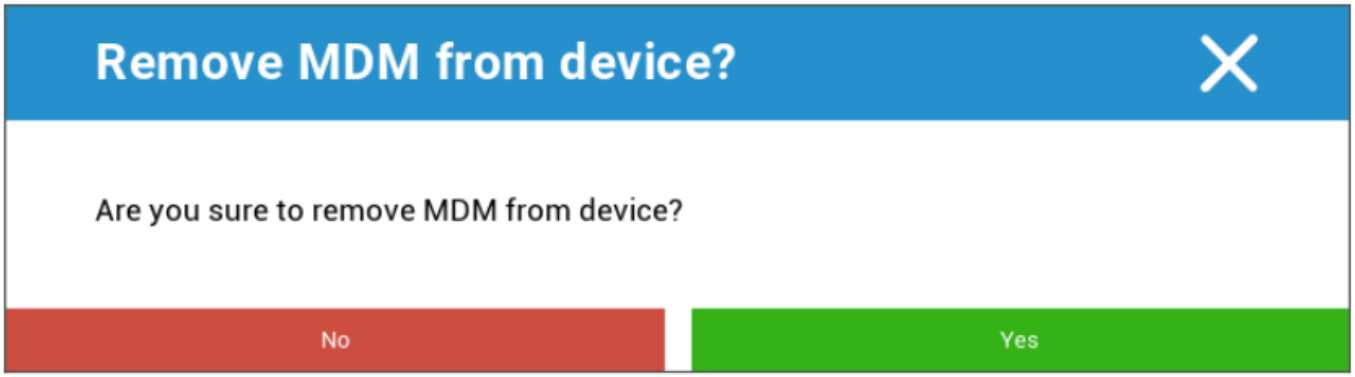
Zařízení na stírání



V části "Wipe Device" (Vymazat zařízení) můžete provést úplné vymazání zařízení. Zařízení bude obnoveno do továrního nastavení.

Enterprise Wipe | Odebrat MDM

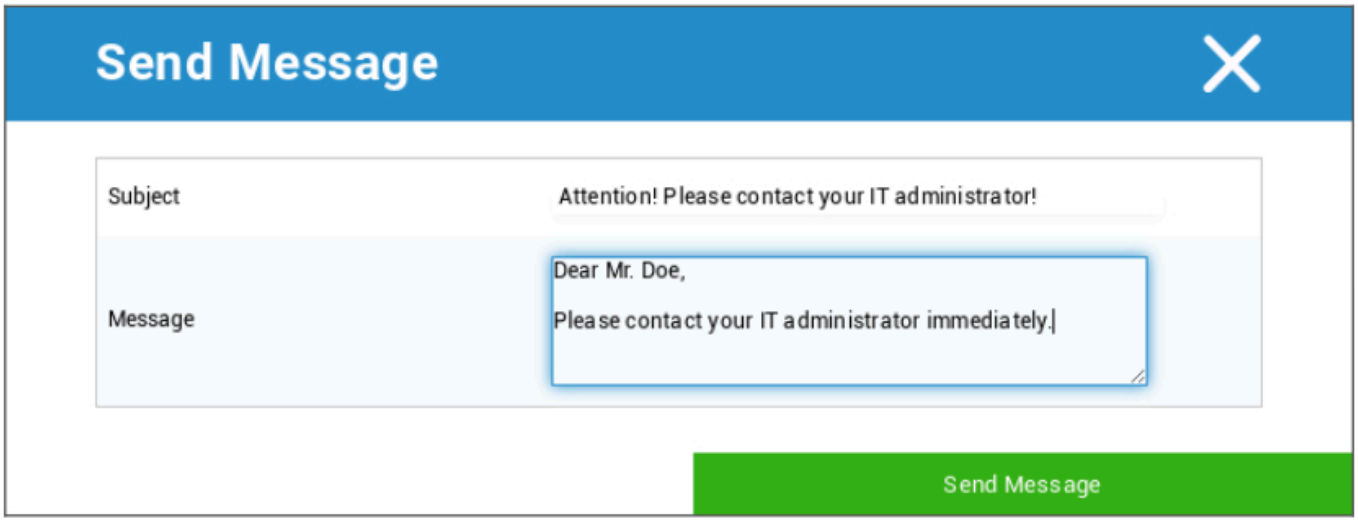
Vymazány jsou pouze informace, aplikace a profily poskytnuté společností AppTec360. Tímto způsobem již nebudou firemní data v zařízení koncového uživatele dostupná. Soukromá oblast není ovlivněna a zůstává i nadále v zařízení koncového uživatele.



Pomocí funkce "Remove MDM" můžete odebrat profil MDM na zařízení koncového uživatele a všechny ostatní položky poskytované společností AppTec.

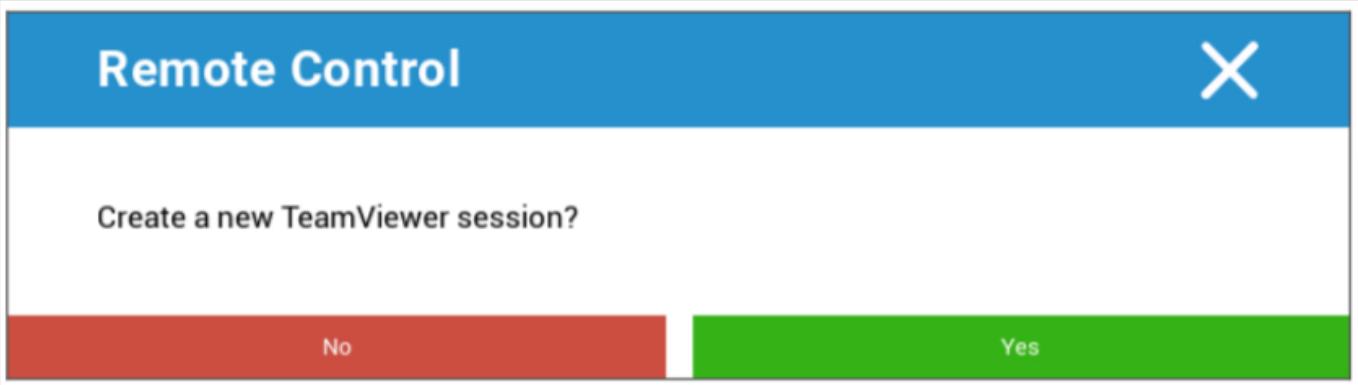
Tento příkaz provede stejnou akci jako příkaz "Enterprise Wipe".

Odeslat zprávu



Zde můžete odeslat oznámení Push do příslušného zařízení.

Vzdálené ovládání TeamViewer



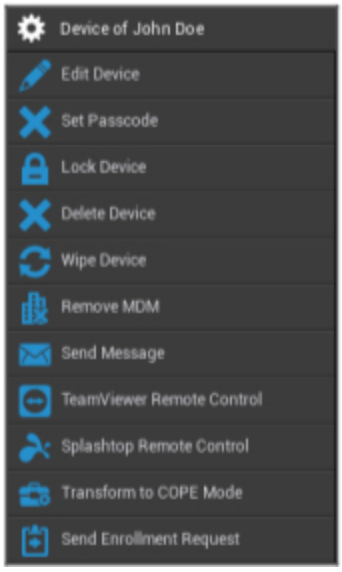
Zde lze spustit relaci vzdáleného ovládání Teamviewer.

Odeslat žádost o zápis

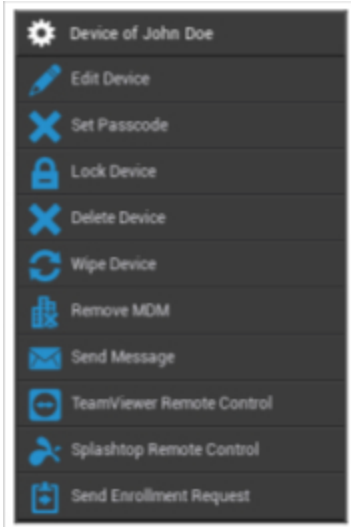
Pomocí možnosti "Odeslat žádost o zápis" můžete příslušnému uživateli (opět) odeslat žádost o zápis.

Android

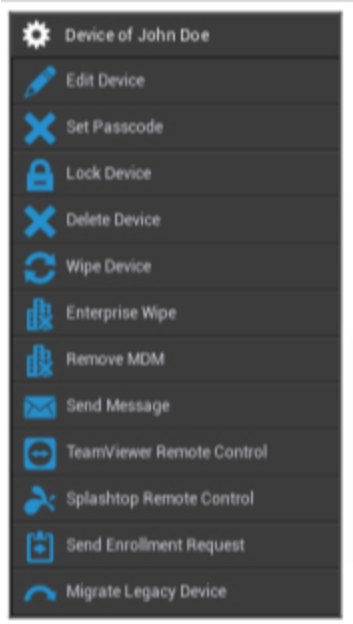
Plně spravované zařízení AE (Work Managed)



Pracovní profil AE (kontejner)



Telefon se systémem Android | Tablet

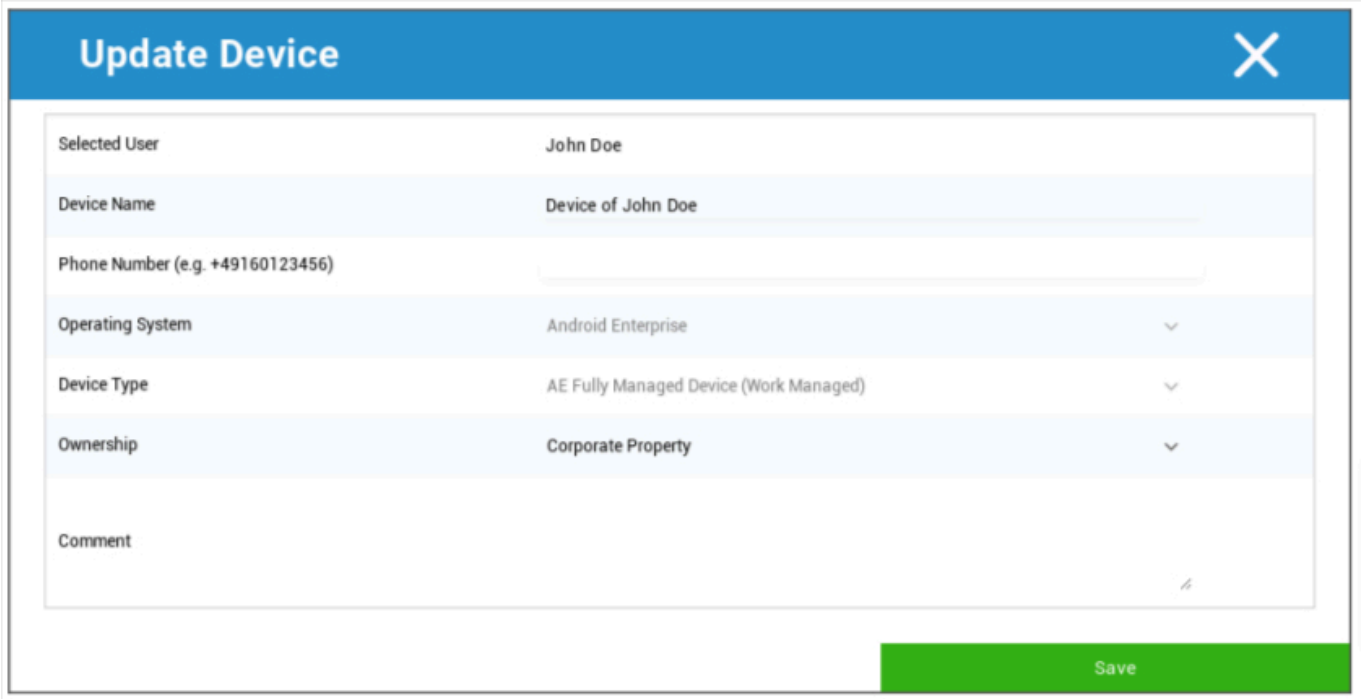


Upravit zařízení	Úprava informací o zařízení
Nastavení přístupového kódu	Nastavení přístupového kódu zařízení
Zámek zařízení	Uzamčení zařízení (zamykací obrazovka)
Odstranit zařízení	Odstranění zařízení z AppTec
Zařízení na stírání	Obnovení továrního nastavení zařízení
Podnikové utírání	Informace, aplikace a profily, které poskytuje AppTec360, jsou smazány (zařízení bude odděleno od MDM).
Odstranění MDM	
Odeslat zprávu	Odesílání oznámení Push do zařízení Zpráva se zobrazí v aplikaci AppTec360 (záložka Zpráva).
Vzdálené ovládání TeamViewer	Spuštění relace vzdáleného ovládání pro toto zařízení pomocí aplikace TeamViewer
Dálkové ovládání Splashtop	Spuštění relace vzdáleného ovládání pro toto zařízení pomocí aplikace Splashtop
Transformace do režimu COPE (pouze u plně spravovaného zařízení AE (Work Managed))	Vytvoření pracovního profilu na tomto plně spravovaném (pracovně spravovaném) zařízení AE
Odeslat žádost o zápis	Odeslání (opakované) žádosti o zápis
Migrace staršího zařízení (pouze v telefonu / tabletu se systémem Android, pokud je zaregistrován pomocí	Migrace profilu telefonu / tabletu se systémem Android na profil plně

funkce Device Owner Mode Provisioning)	spravovaného zařízení AE (spravovaný prací)

Upravit zařízení

Zde můžete aktualizovat různé informace o zařízení.



Vybraný uživatel	Uživatel zařízení
Název zařízení	Název zařízení
Telefonní číslo	Telefonní číslo zařízení
Operační systém	Android Enterprise Android
Typ zařízení	Android Enterprise: • Plně spravované zařízení AE (Work Managed) • Režim pracovního profilu AE (pouze kontejner) • Plně spravované zařízení AE s pracovním profilem (COPE) Android: • Telefon • Tablet
Vlastnictví	Corporate = majetek společnosti

	Employee = vlastnost zaměstnance
Komentář:	Další popisy zařízení

Vymazání přístupového kódu

Zde můžete odebrat přístupový kód zařízení na vybraném zařízení. Ve výchozím nastavení systému Android je přístupový kód nastaven na hodnotu "123456" - tuto hodnotu může a měl by uživatel dodatečně změnit.

Zámek zařízení

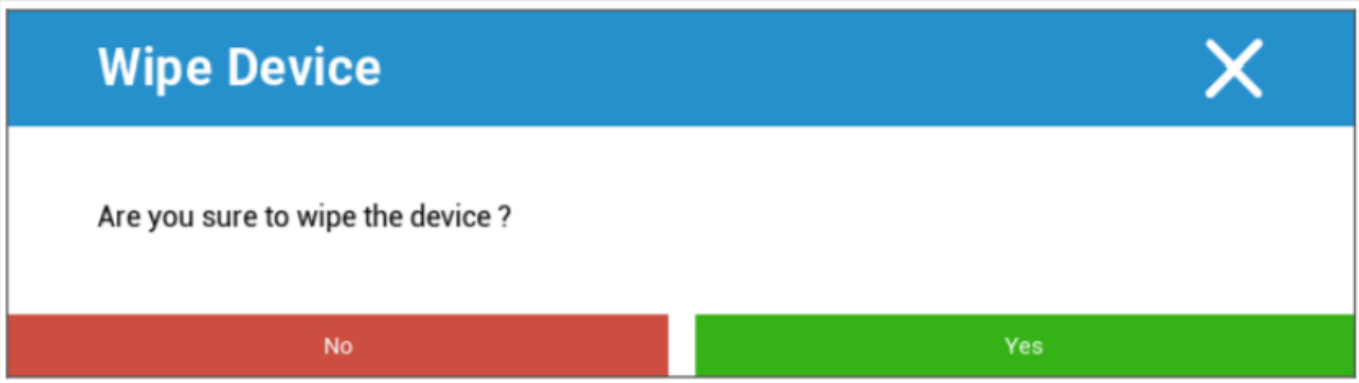
Zde se do zařízení odešle příkaz k uzamčení zařízení (uzamčení obrazovky).

Odstranit zařízení

Zde lze provést příkaz k odstranění. Opět se můžete rozhodnout, zda má být zařízení odstraněno pouze z AppTec360 ("Delete from System"), nebo zda má být zařízení odstraněno z AppTec360 a navíc obnoveno do továrního nastavení ("Wipe & Delete").

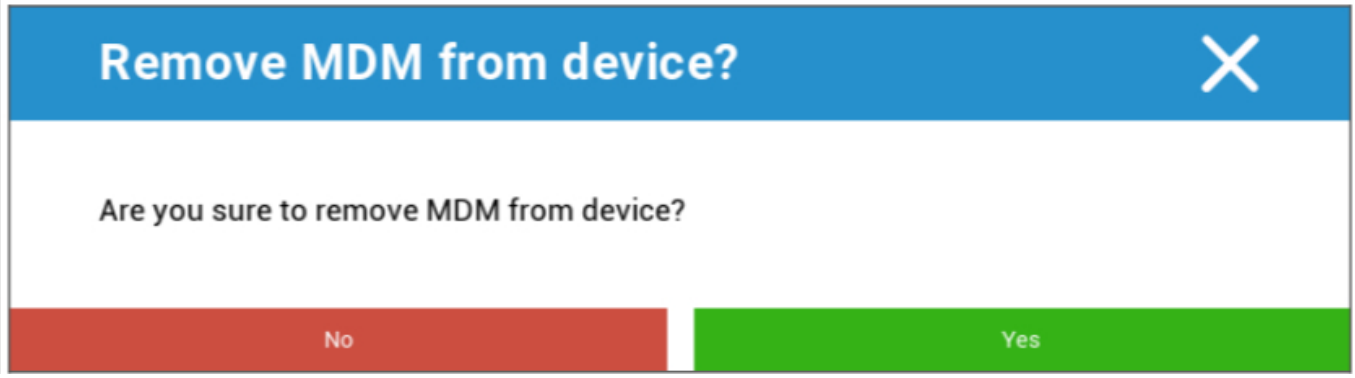
Zařízení na stírání

V části "Wipe Device" (Vymazat zařízení) můžete provést úplné vymazání zařízení. Zařízení bude poté obnoveno do továrního nastavení.



Pokud zařízení obsahuje kartu SD, můžete ji navíc vymazat. Toho můžete dosáhnout nastavením možnosti "Wipe SD Card too? " na "Zapnuto".

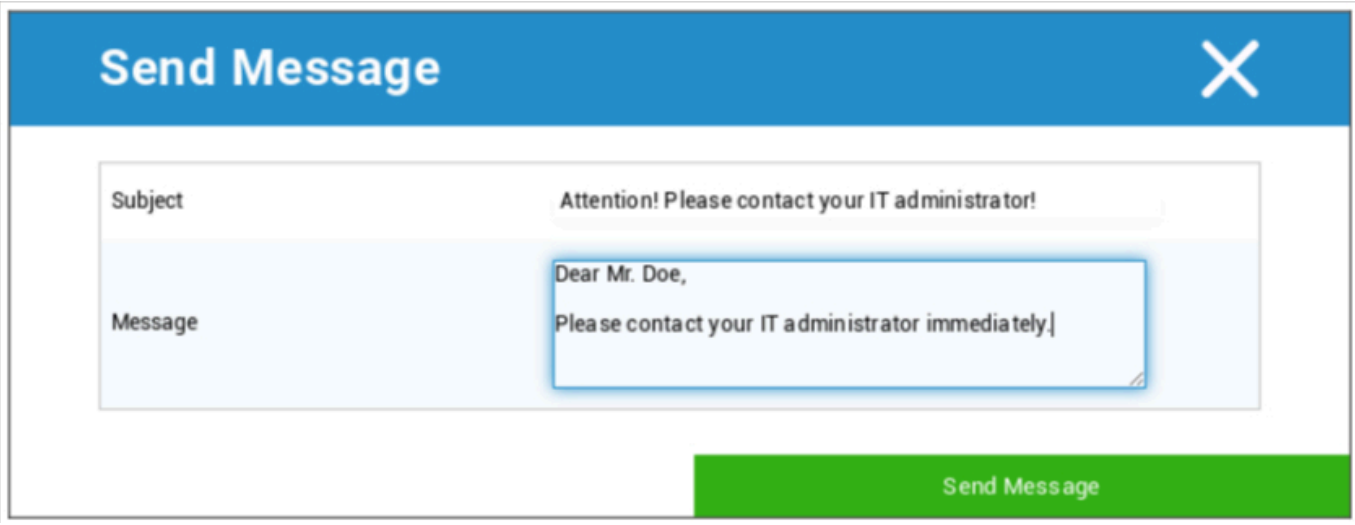
Odstranění MDM



Jedná se o doporučenou metodu pro vytvoření oddělení od MDM.

Vymazány jsou pouze informace, aplikace a profily poskytnuté společností AppTec360, což znamená, že všechna firemní data již nebudou v zařízení koncového uživatele k dispozici. Soukromé sféry se to však netýká a zůstávají v zařízení koncového uživatele i nadále.

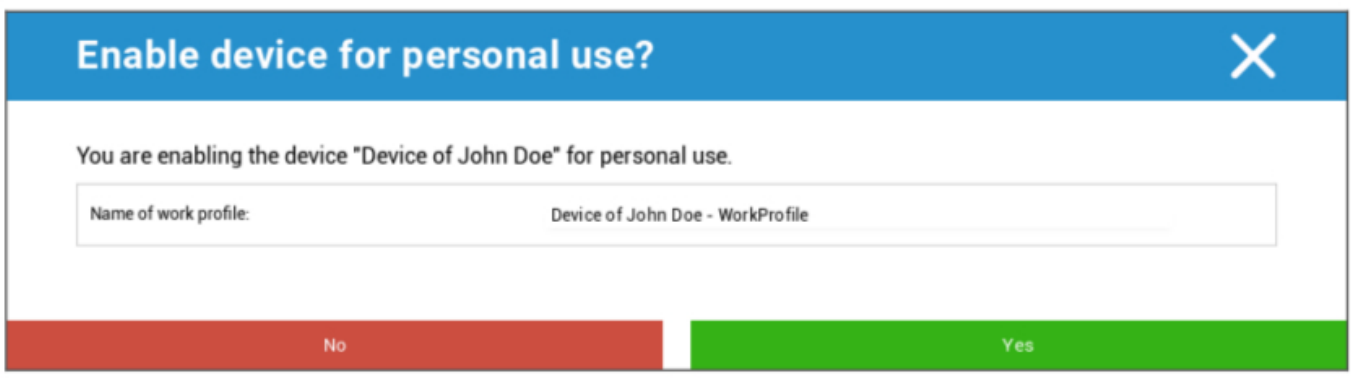
Odeslat zprávu



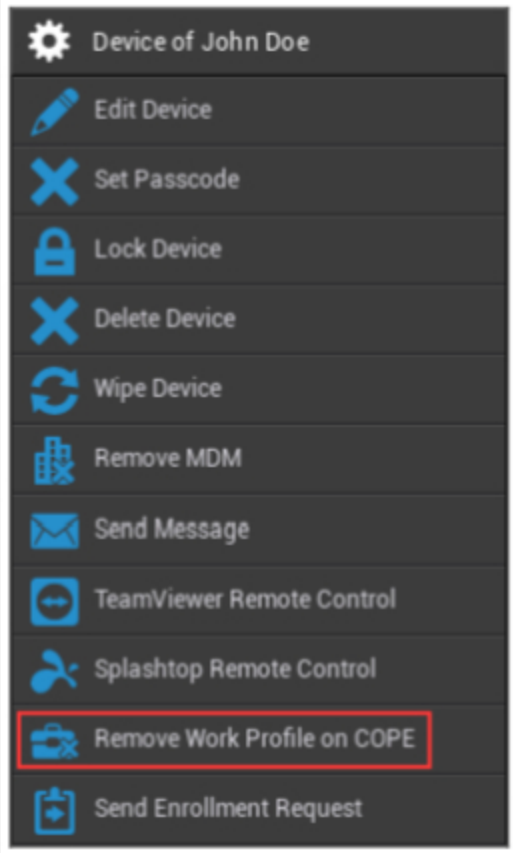
Zde můžete odeslat oznámení Push do příslušného zařízení koncového uživatele.

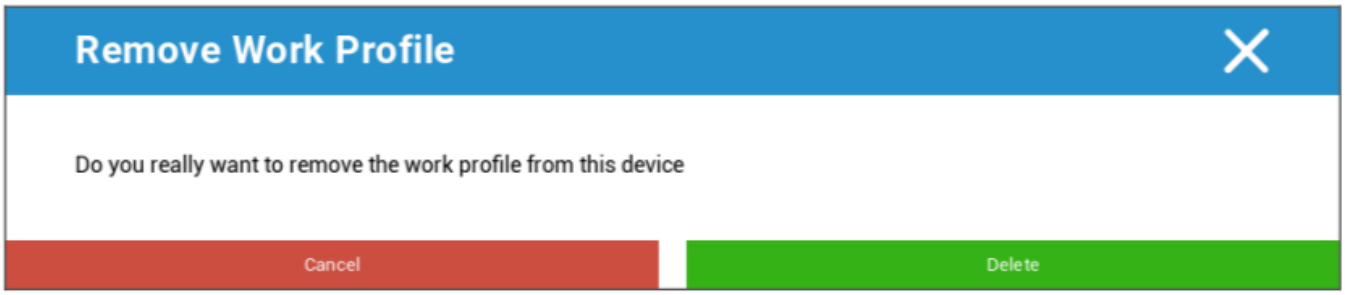
Transformace do režimu COPE

Vytvoření pracovního profilu na tomto plně spravovaném (pracovně spravovaném) zařízení AE



Po převedení zařízení do režimu COPE můžete pracovní profil odebrat kliknutím na ozubené kolečko **Odstranit pracovní profil na COPE:**




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

Odeslat žádost o zápis

Pomocí funkce "Odeslat žádost o zápis" můžete příslušnému uživateli (opět) odeslat žádost o zápis.

Upozorňujeme, že platný je pouze nejnovější zápis - žádost.

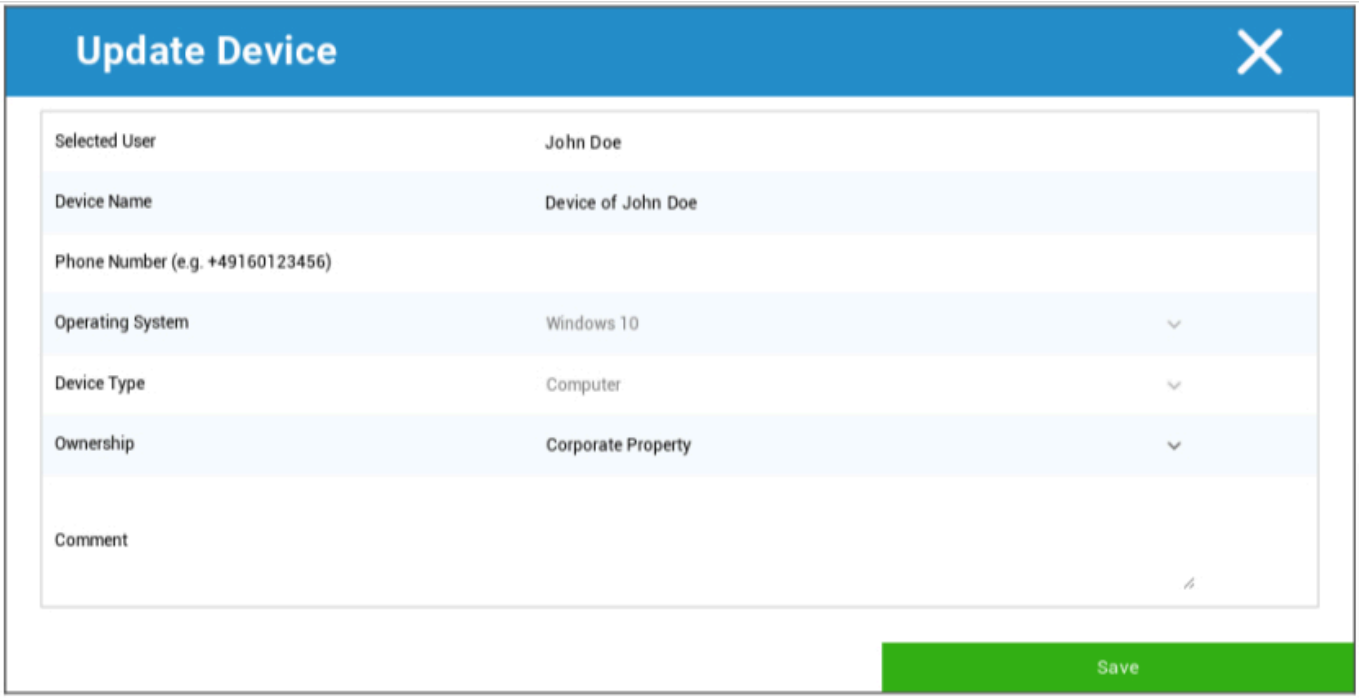
Migrace staršího zařízení

Migrace profilu telefonu / tabletu se systémem Android na profil plně spravovaného zařízení AE (spravovaný prací)

Windows

Název zařízení	Název vybraného zařízení
Upravit zařízení	Upravit zařízení
Odstranit zařízení	Odstranění zařízení z AppTec
Podnikové utírání	Informace, aplikace a profily poskytnuté společností AppTec360 jsou smazány.
Odstranění MDM	
Vzdálené ovládání TeamViewer	Vzdálené ovládání zařízení pomocí aplikace TeamViewer
Odeslat žádost o zápis	Odeslání žádosti o registraci (znovu)

Upravit zařízení

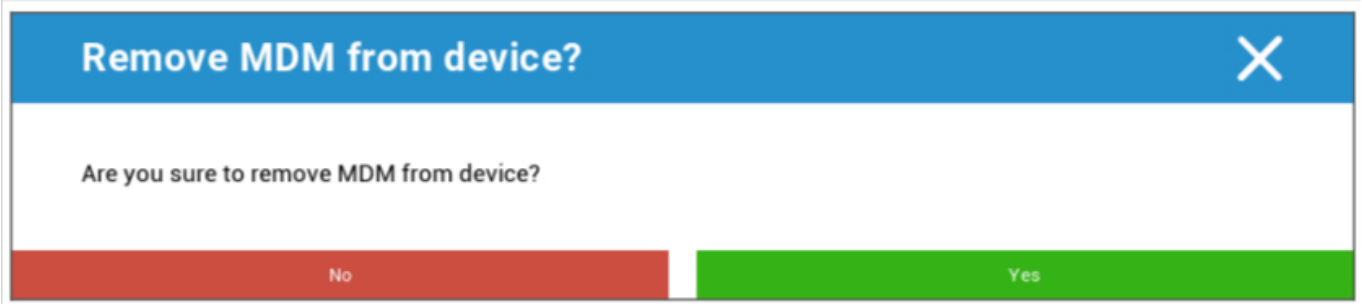


Zde můžete aktualizovat řadu informací o zařízení.

Odstranit zařízení

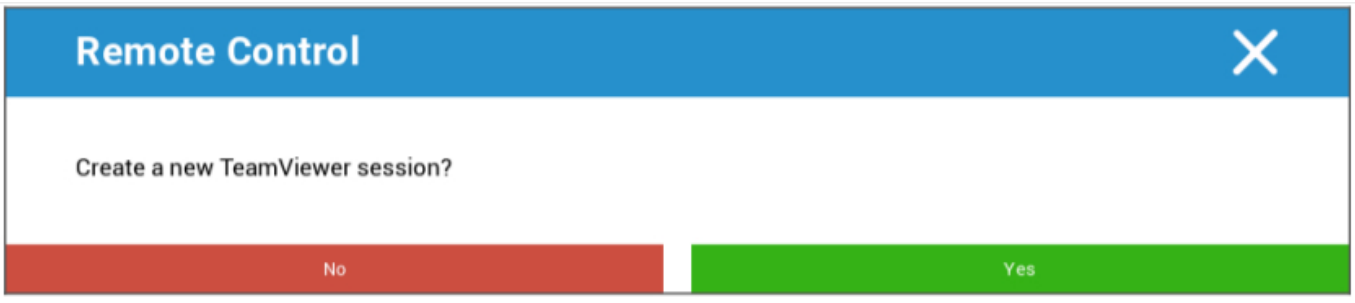
Zde lze provést příkaz delete, který pouze odstraní zařízení z AppTec360.

Enterprise Wipe | Odebrat MDM



Vymazány jsou pouze informace, aplikace a profily poskytnuté společností AppTec360. Tímto způsobem již nebudou firemní data v zařízení koncového uživatele dostupná. Soukromá oblast není ovlivněna a zůstává i nadále v zařízení koncového uživatele.

Vzdálené ovládání TeamViewer



Zde můžete spustit relaci vzdáleného ovládání TeamViewer pro toto zařízení.

Odeslat žádost o zápis

Pomocí možnosti "Odeslat žádost o zápis" můžete příslušnému uživateli (opět) odeslat žádost o zápis.

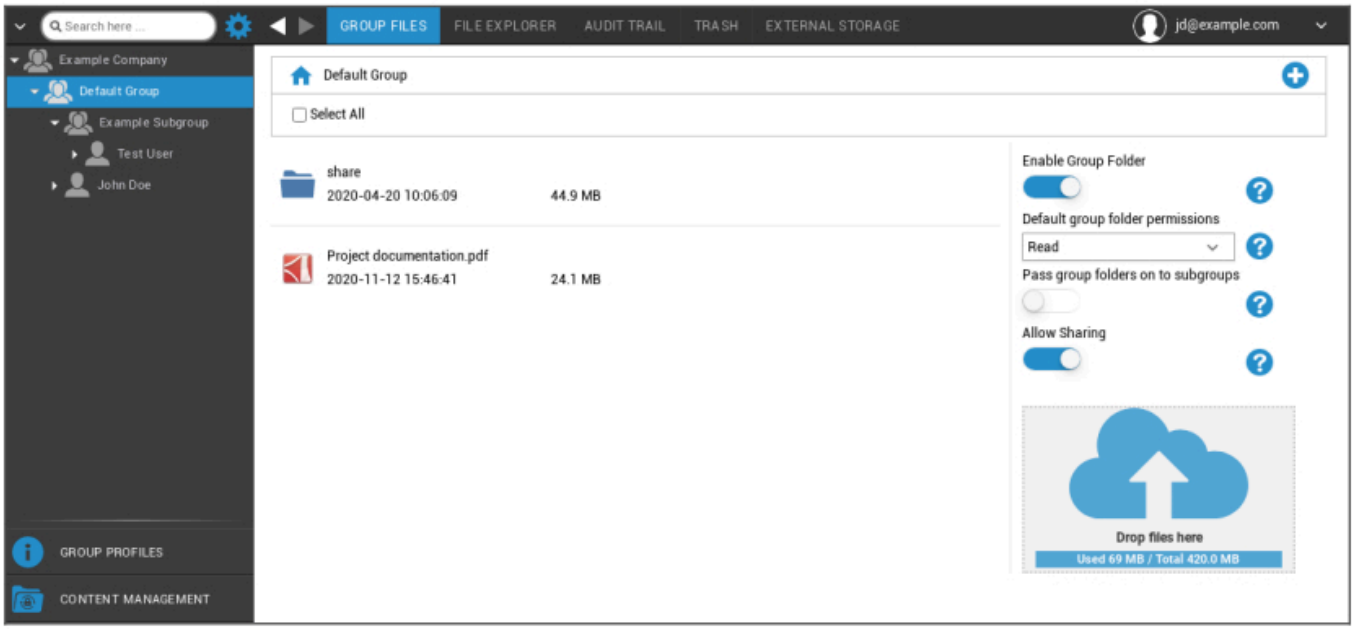
Správa obsahu

Pokud jste ve skupině, můžete spravovat AppTec ContentBox pomocí "Správy obsahu".

Pomocí Content Boxu můžete bezpečně distribuovat dokumenty a další firemní data do zařízení koncových uživatelů.

Skupinové soubory

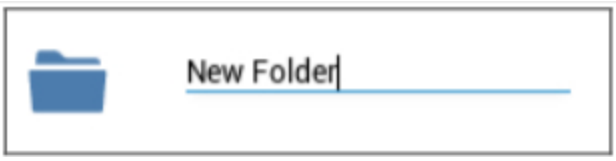
"Skupinové soubory" představují základní část ContentBox. Zde můžete provádět nastavení, nahrávat dokumenty, vytvářet nové složky atd.



Pomocí symbolu v pravém horním rohu můžete vytvářet nové složky, které jsou přiřazeny k příslušné skupině pomocí "Přidat složku".

Pomocí symbolu v pravém horním rohu můžete vytvořit novou složku pomocí "Přidat složku", která by měla být přiřazena k příslušné skupině.

Složku můžete pojmenovat libovolně.



Prostřednictvím "Nahrát soubory" můžete nahrát data. Zde se otevře váš Standard-Explorer. Tyto dvě akce můžete samozřejmě provádět v každé (dílčí) složce.

Pomocí symbolu v levém horním rohu se můžete vrátit do hlavní nabídky.

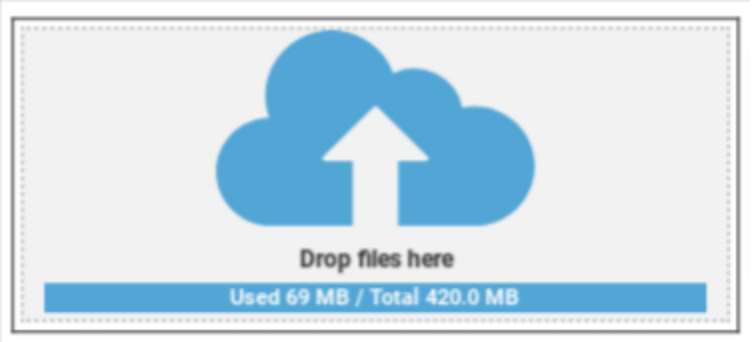
Můžete vybrat několik složek a souborů a stáhnout je pomocí "Download" nebo je můžete vymazat kliknutím na "Delete".

Můžete také vybrat všechny soubory a složky a provést příkazy "Stáhnout" a "Odstranit".

Po najetí myší na složku nebo soubor se zobrazí následující přehled:

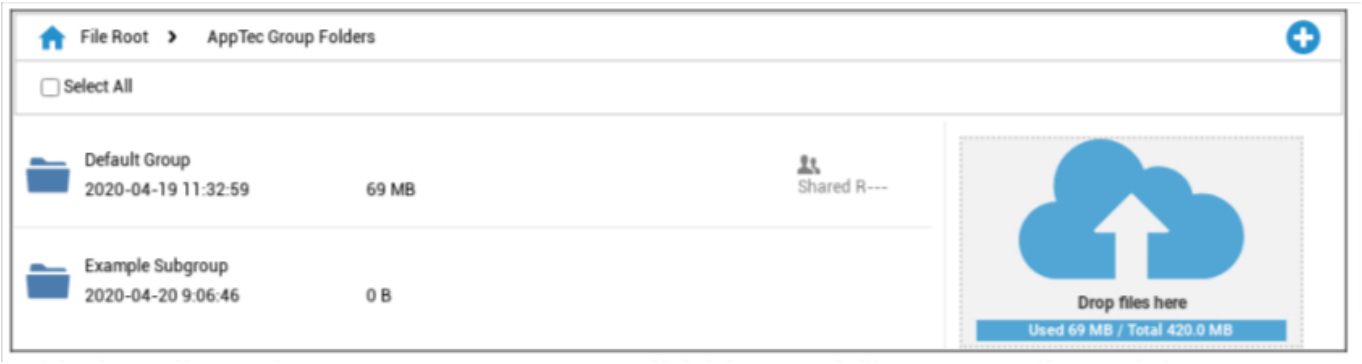
- Pomocí funkce "Přejmenovat" můžete složku/soubor přejmenovat.
- Pomocí možnosti "Stáhnout" můžete stáhnout složku/soubor.
- Pomocí "Delete" můžete složku/soubor smazat.

Povolení složky skupiny	Pokud je aktivována, mají všichni členové skupiny přístup do příslušné složky.
Výchozí oprávnění složek skupiny	Oprávnění uživatelů ve vybrané skupině: Read = oprávnění pouze pro čtení Aktualizace = oprávnění k aktualizaci Vytvořit = oprávnění k vytvoření Odstranit = oprávnění k odstranění
Předávání skupinových složek podskupinám	Pokud je aktivována, mohou mít příslušné podskupiny přístup k nadřazeným datovým souborům.
Oprávnění pro podskupiny	Oprávnění uživatelů ve vybrané podskupině: Read = oprávnění pouze pro čtení Aktualizace = oprávnění k aktualizaci Vytvořit = oprávnění k vytvoření Odstranit = oprávnění k odstranění
Povolit sdílení	Pokud je aktivována, může uživatel sdílet soubory prostřednictvím odkazu.



Pro nahrávání souborů můžete toto pole použít tak, že do tohoto okna přetáhnete soubor pomocí funkce Drag & Drop. Na toto pole můžete také kliknout, abyste vybrali a nahráli soubor pomocí aplikace Internet Explorer.

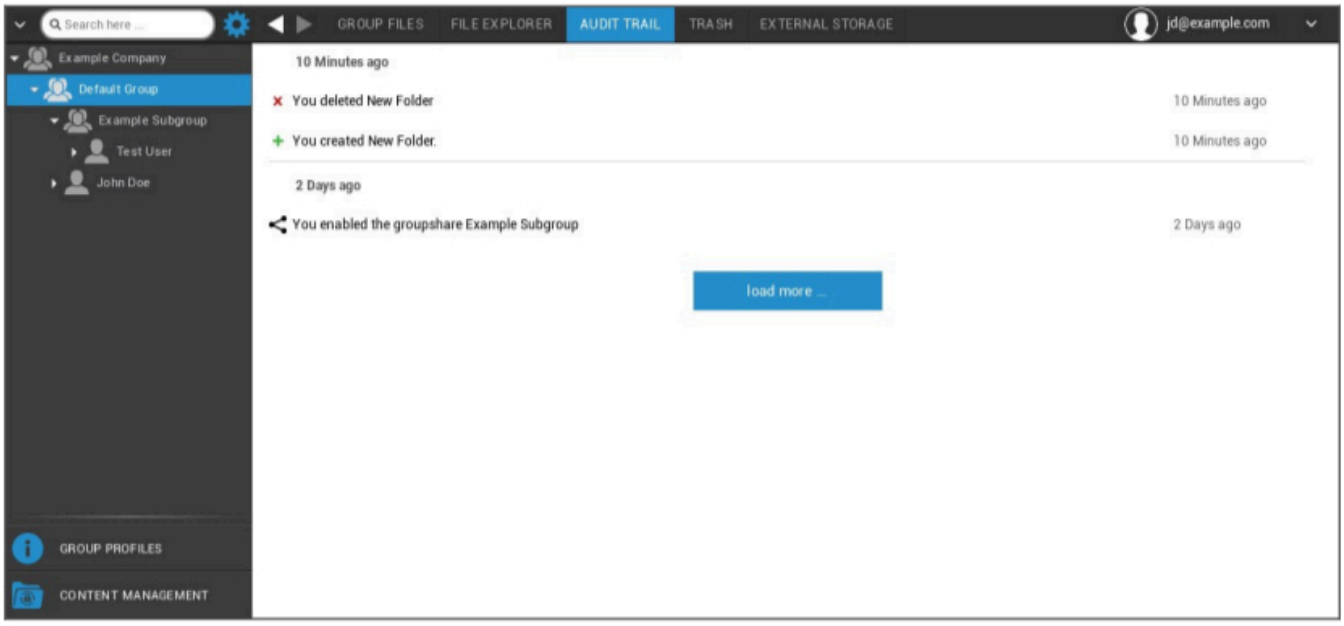
Průzkumník souborů



Pomocí Průzkumníka souborů můžete spravovat všechny složky a soubory - bez ohledu na skupinu, ve které jsou uloženy.

Najdete zde také nastavení a tlačítka, o kterých jste se dozvěděli v části "Skupinové soubory".

Auditní stopa



V části "Audit Trail" můžete z historie zjistit, který uživatel co vytvořil, smazal nebo sdílel. Kdykoli tak můžete zjistit, co bylo s firemními daty provedeno.

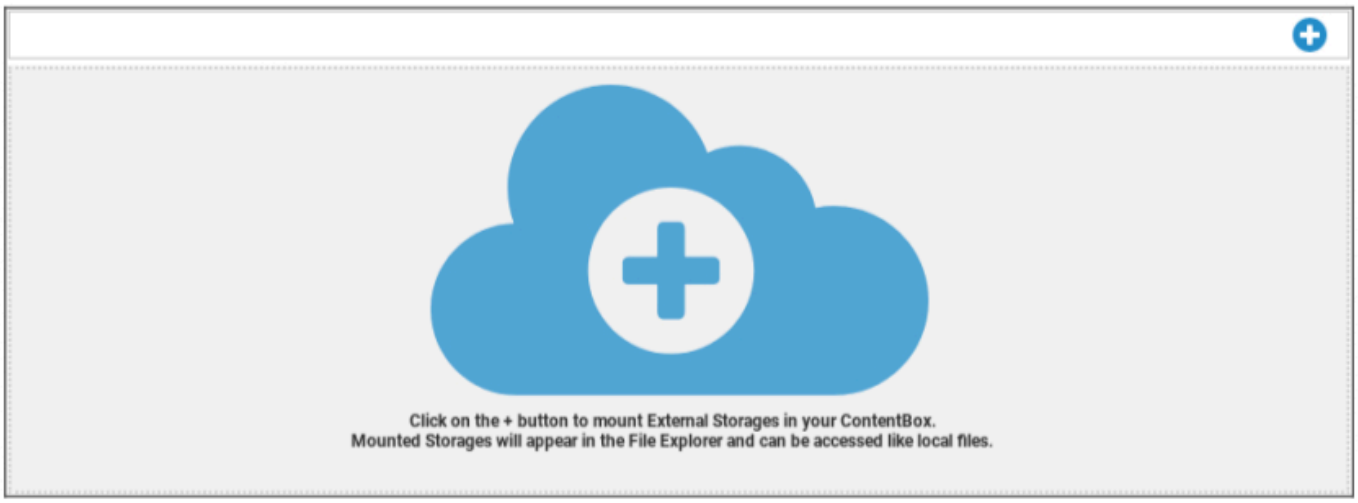
Odpadkový koš

Pokud jste něco smazali (omylem), můžete si složky a soubory zobrazit v části "Koš" a obnovit je podle svého přání.

- Pomocí funkce "Undelete" můžete data/složku obnovit.
- Příkazem "Delete" můžete data/složku trvale odstranit - příkaz dele musíte ještě jednou potvrdit.

Vezměte prosím na vědomí, že kapacita úložiště, která je využívána v koši, snižuje "celkový dostupný prostor" - jedná se o požadavek služby ownCloud.

Externí úložiště



V části "Externí úložiště" můžete připojit externí úložiště.

Pomocí symbolu lze přidat (další) úložiště.

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

Amazon S3	
Zobrazení názvu	Zobrazení názvu
Přístupový klíč	Přístupový klíč
Tajný klíč	Bezpečnostní klíč
Kbelík	Určitá identita podsložky, která vám byla přidělena.
Název hostitele (nepovinné)	Název hostitele (nepovinné)
Port (volitelný)	Port (volitelný)
Region	Oblast (nepovinné)
Povolení protokolu SSL	Povolení protokolu SSL
Povolit styl cesty	Vymazat adresu cesty, která vám byla přidělena

FTP	
Zobrazení názvu	Zobrazení názvu
Hostitel	Adresa hostitele
Uživatelské jméno	Uživatelské jméno
Heslo	Heslo
Kořen	Hlavní menu
Zabezpečení ftps://	

SFTP	
Zobrazení názvu	Zobrazení názvu
Hostitel	Adresa hostitele
Uživatelské jméno	Uživatelské jméno
Heslo	Heslo
Kořen	Hlavní menu

ownCloud	
Zobrazení názvu	Zobrazení názvu
ADRESA URL	Adresa URL služby ownCloud
Uživatelské jméno	Uživatelské jméno
Heslo	Heslo
Vzdálená podsložka	Standardní složka
Zabezpečení https://	

WebDAV	
Zobrazení názvu	Zobrazení názvu
ADRESA URL	Adresa URL WebDAV
Uživatelské jméno	Uživatelské jméno
Heslo	Heslo
Kořen	Hlavní menu
Zabezpečení https://	
Sdílení systému Windows	Podpora pro Windows Share bude k dispozici brzy
SharePoint	Podpora pro Microsoft SharePoint bude brzy k dispozici

Protokol o auditu

Zde najdete protokol, který zaznamenává informace o akcích prováděných v konzole MDM.

Pomocí ikony filtru můžete na zobrazený seznam použít filtry.

Pomocí rozevírací nabídky **Položky na stránku**: můžete vybrat počet položek, které se mají zobrazit na jedné stránce seznamu.

Přijatá opatření / změna nastavení	Akce, která byla provedena / Nastavení, které bylo změněno
Hodnota	Hodnota provedené akce / změněného nastavení
Uživatel	Jméno uživatele, který provedl akci / změnil nastavení.
Datum	Časové razítko, kdy byla tato akce provedena / toto nastavení změněno.
Cesta / typ	Cesta k místu, kde byla tato akce provedena / toto nastavení změněno

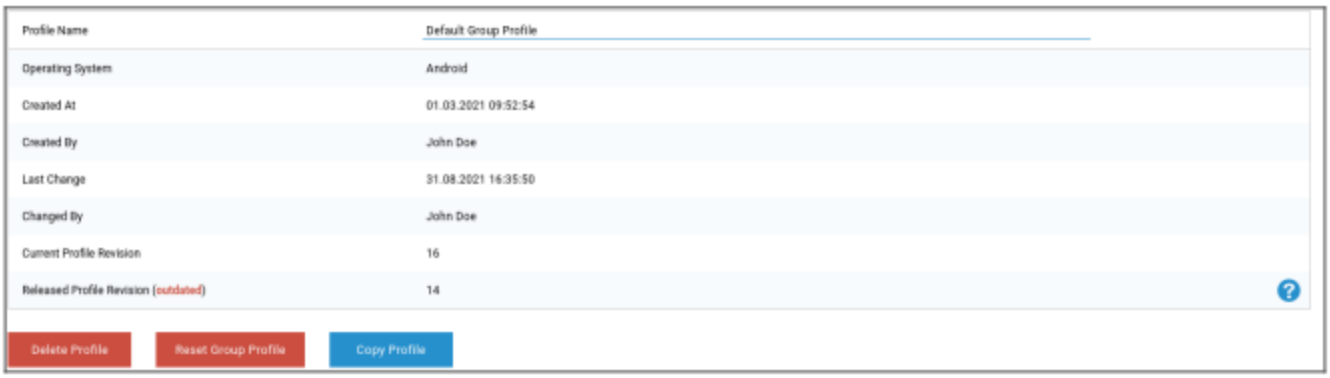
Konfigurace iOS

Obecné

V závislosti na tom, zda jste aktuálně vybrali skupinu nebo zařízení, se zobrazení a jeho dílčí body liší - věnujte tomu prosím zvýšenou pozornost!

Přehled profilu skupiny (pouze na úrovni skupiny)

Při otevření profilu skupiny se zobrazí rychlý přehled profilu.



Název profilu	Název profilu (zde lze změnit)
Operační systém	Operační systém, pro který je profil určen
Vytvořeno v	Čas vytvoření
Vytvořil	Tvůrce profilu
Poslední změna	Čas poslední změny profilu
Změněno podle	Účet, který provedl poslední změny
Aktuální revize profilu	Revize uloženého stavu profilu
Vydaná revize profilu	Přiřazená revize profilu ("Assign now"). Pokud se za textem na štítku zobrazí " (zastaralý)", znamená to, že jste profil uložili, ale ještě jste ho nepřiřadili, takže zařízení budou stále dostávat starší verzi.

Obecné informace

Pokud se nacházíte přímo v zařízení, zobrazí se stručný přehled vybraného zařízení.

Název zařízení	Název zařízení
Telefonní číslo	Telefonní číslo zařízení
Model	Číslo modelu
Operační systém	OS
Sériové číslo	Sériové číslo zařízení
Vlastnictví zařízení	Firemní nebo soukromé zařízení Corporate = firemní zařízení Zaměstnanec = soukromé zařízení
Typ zařízení	Typ zařízení (tablet nebo telefon)
Jailbroken	Pokud je v zařízení útěk z vězení
Pod dohledem	Označuje, zda se jedná o zařízení pod dohledem
V souladu s předpisy	Pokud byly porušeny nějaké pokyny
Naposledy viděno	Stav, kdy zařízení naposledy komunikovalo se serverem AppTec360.

Nastavení

Tato nastavení obsahují název zařízení a předdefinované pozadí.

Název zařízení na název systému	Název, který bude uveden v konzole AppTec360 (v levé hierarchické struktuře), bude stejný jako na příslušném zařízení koncového uživatele (lze zobrazit v nastavení zařízení).
Použití vlastní tapety (pouze zařízení pod dohledem)	Zde můžete předem definovat pozadí, které se má zobrazit na zařízení koncového uživatele (např. pro typ firemní značky zařízení). Je k dispozici pouze v režimu pod dohledem!
Automatické aktualizace operačního systému	Vynutí aktualizace operačního systému, pokud jsou k dispozici. Pouze pro zařízení DEP v režimu pod dohledem.
Vlastní písma	Zde můžete přidat vlastní písma.
Název	Volitelně. Uživatelsky viditelný název písma. Toto pole je po instalaci nahrazeno skutečným názvem písma.
Písmo	Nahrajte soubor písma (.otf nebo .ttf).

Revize konfigurace

Zde získáte přehled o tom, který skupinový profil je pro zařízení určen.

Pokud kliknete na profil skupiny, dostanete se přímo do profilu a můžete provést nastavení.

Pomocí symbolu můžete vrátit přiřazené aplikace do nastavení skupinového profilu.

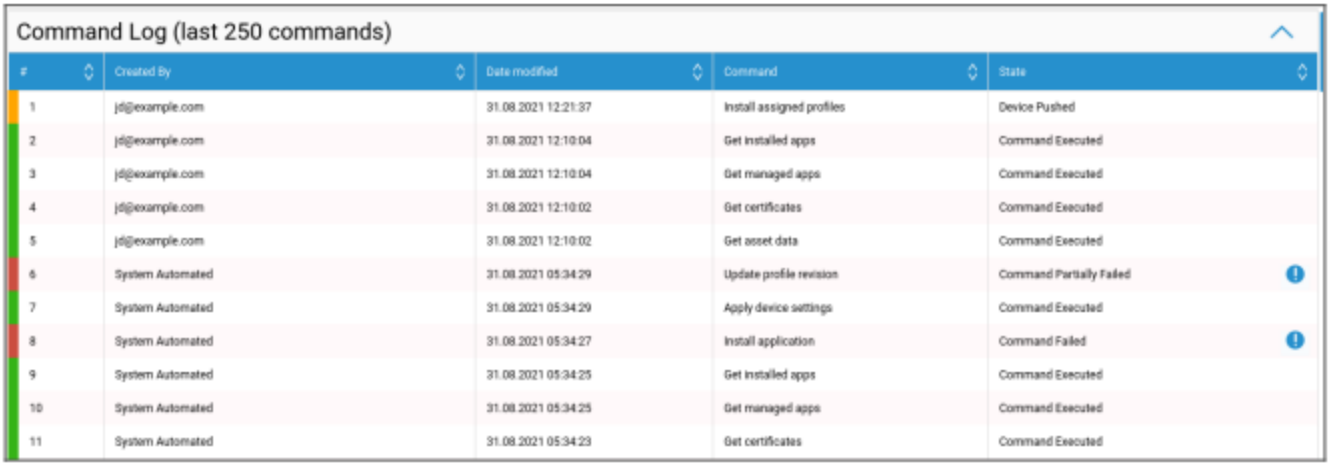
Pomocí symbolu můžete obnovit profil zařízení tak, aby neměl žádné nastavení.

"K dispozici je novější revize" znamená, že profil skupiny byl změněn a uložen, ale nebyl přiřazen. Profil skupiny je třeba přiřadit pomocí "Přiřadit nyní" na úrovni skupiny, aby se změny uplatnily na zařízení.

Protokol zařízení (pouze na úrovni zařízení)

Protokol příkazů

Zde můžete zjistit, které příkazy byly pro zařízení vydány a jaký je jejich stav.



Příkazy vytvořené pomocí "System Automated" jsou automaticky vytvořeny systémem.

Možné stavy příkazů

Stlačené zařízení	Službě push (např. APNS) byl odeslán požadavek na připojení, aby se zařízení připojilo zpět k serveru EMM.
Vytvořený příkaz	Příkaz byl vytvořen v systému.
Odeslaný příkaz	Příkaz byl odeslán do zařízení po jeho připojení k serveru.
Spuštěný příkaz	Příkaz byl úspěšně proveden.
Příkaz se nezdařil	Příkaz se nezdařil. *
Příkaz částečně selhal	V závislosti na operačním systému zařízení mohou být některé příkazy seskupeny. V tomto některé části této skupiny příkazů selhaly. *
Příkaz proveden, případně neúspěšný	Příkaz byl proveden, ale možná nebyl.
Přesunutí příkazu	Příkaz byl znovu odeslán uživatelem.
Vyřazené	Příkaz byl vyřazen. Například proto, že byl nahrazen jiným příkazem nebo že zařízení bylo znovu zapsáno a staré příkazy byly odstraněny.

Pokud je za zprávou vykřičník, můžete získat další informace, když na ikonu najedete kurzorem.

Správa aktiv (pouze na úrovni zařízení)

Správa aktiv (pouze na úrovni zařízení)

Informace o zařízení

Model	Číslo modelu zařízení
Operační systém	OS
Verze operačního systému	Verze operačního systému
Sériové číslo	Sériové číslo
UDID	UDID zařízení
Název zařízení	Název zařízení
Pod dohledem	Zobrazí, zda je zařízení pod dohledem
Stav baterie	Stav baterie

Wi-Fi

IP adresa	Adresa IP zařízení
WiFi MAC	Adresa MAC WiFi

Cellular

Stav	Stav (přítomnost karty SIM)
Telefonní číslo	Telefonní číslo
Stav roamingu	Aktuální stav roamingu
Roaming (hlas/ data)	Stav roamingu pro hlasové/datové služby
IP adresa	IP adresa
IMEI	Číslo IMEI
Provozovatel/přepravce	Poskytovatel mobilních služeb
Síť operátora SIM	Síť operátora SIM
Verze pro nosiče	Verze pro nosiče
Firmware modemu	Firmware modemu
Současné MCC/MNC	Viz "SIM MCC/MNC"
SIM MCC/MNC	Kód mobilní sítě je identifikace země stanovená ITU podle normy E.212, která se ve spojení s kódem mobilní sítě (MNC) používá k identifikaci mobilní sítě (=kód země). Když přejdete do jiné mobilní sítě, "Current MCC/MNC" a "SIM MCC/MNC" se proto liší.

Bluetooth

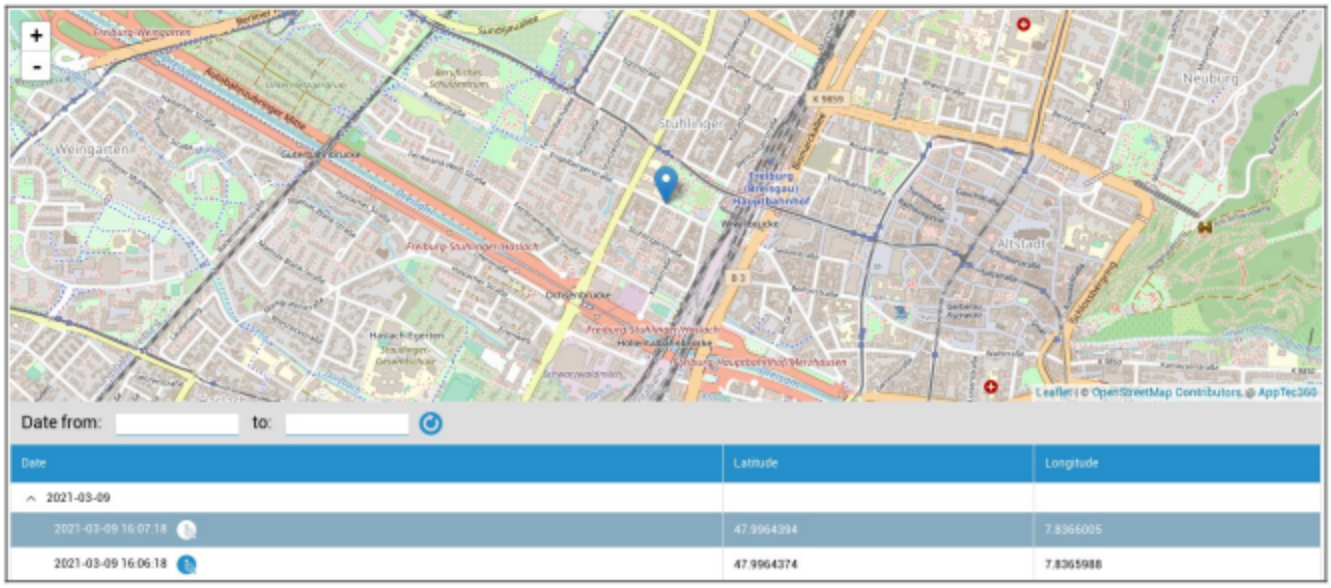
Bluetooth MAC	Adresa MAC Bluetooth

Správa zabezpečení

Ochrana proti krádeži (pouze na úrovni zařízení)

Informace GPS (pouze na úrovni zařízení)

Zde můžete vyhodnotit aktuální/poslední polohu zařízení. Lokalizaci lze chránit buď jedním, nebo dokonce dvěma hesly - viz: Přístup k GPS můžete nastavit podle následujících možností: Obecná nastavení - Soukromí - Přístup k GPS



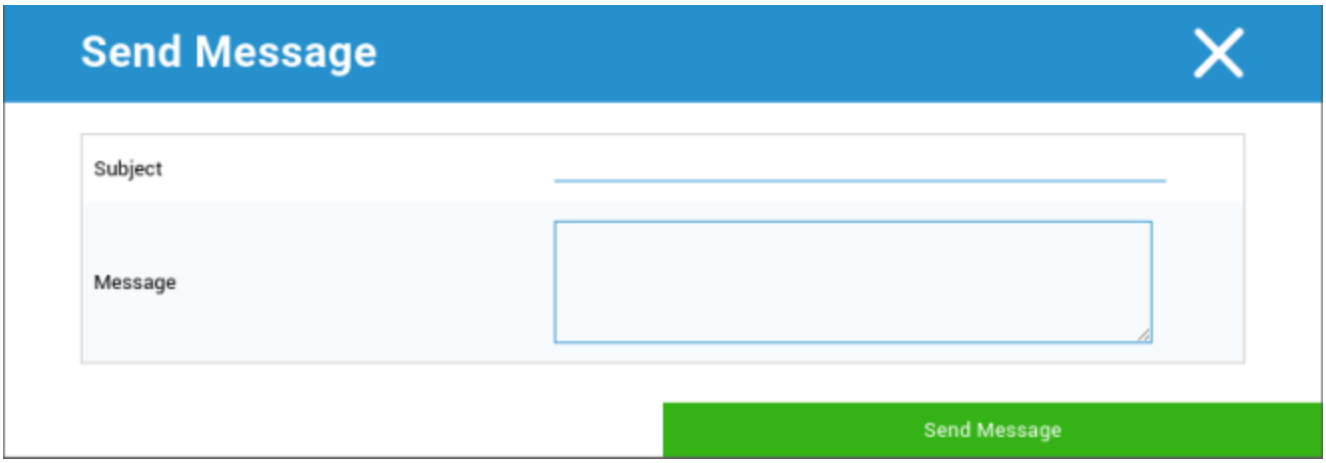
Vymazání a uzamčení (pouze na úrovni zařízení)

V části "Wipe & Lock" můžete provést následující tři akce:

Úplné otření	Zařízení je obnoveno do továrního nastavení (firemní i osobní údaje jsou smazány).
Podnikové utírání	Ze zařízení koncového uživatele jsou odstraněna pouze firemní data (všechny aplikace, data atd., které poskytla společnost AppTec).
Zamykací obrazovka	Zámek obrazovky je aktivován, stačí zařízení odemknout pomocí hesla zařízení/PIN kódu.
Forenzní uzamčení (pouze dozorovaná zařízení)	Pokud je tato funkce aktivována pomocí symbolu  , zařízení se uzamkne zobrazením zprávy, kterou nelze zavřít. Zaměstnanec rovněž nemůže zařízení odemknout. Zařízení může odemknout pouze správce v konzole pomocí symbolu odemknutí  .
Povolit aktivační zámek (pouze dozorovaná zařízení)	Pokud je tato funkce aktivována , zařízení se uzamkne, jakmile je v nastavení iCloudu aktivována funkce "Najít můj iPhone".

Zpráva (pouze na úrovni zařízení)

V následujícím okně můžete vyplnit předmět a zprávu a odeslat ji na zařízení koncového uživatele:



Konfigurace zabezpečení

Přístupový kód

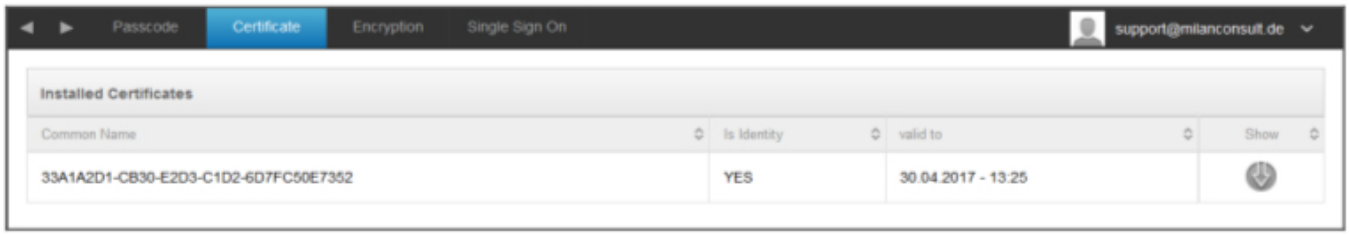
Zde se nastavuje heslo zařízení.

Povolená deaktivace kódu	Pokud je toto nastavení aktivováno, nezobrazuje se výzva k zadání hesla. Jakmile je heslo zavedeno, nelze jej deaktivovat.
Povolit jednoduchou hodnotu	Umožnit uživateli používat stejné, eskalující a redukující číselné řetězce (např. 1234, 1111).
Vyžadovat alfanumerickou hodnotu	Hesla musí obsahovat alespoň jedno písmeno
Minimální délka přístupového kódu	Minimální délka hesla
Minimální počet složených znaků	Minimální počet alfanumerických symbolů v hesle
Maximální věk přístupového kódu	Počet dní, po kterých je třeba heslo změnit.
Maximální automatické zamykání	Maximální doba, po kterou je zařízení uzamčeno
Maximální doba odkladu pro uzamčení zařízení	čas, po kterém zařízení přejde do uzamčeného režimu Stand-By.
Maximální počet neúspěšných pokusů	Stanovuje, jak často může být heslo zadáno nesprávně, než dojde k úplnému vymazání zařízení.
Maximální stáří přístupového kódu (1-730 dní)	Maximální věk hesla
Historie přístupových kódů (1-50 přístupových kódů)	Po tomto čísle je povoleno používat staré heslo.

Kliknutím na koš se otevře dialogové okno Obnovení hesla, ve kterém lze vymazat zapomenuté heslo zařízení.

Certifikát (pouze na úrovni zařízení)

Zobrazí certifikáty, které jsou v zařízení k dispozici.


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

Šifrování

Požadavek na šifrování úložiště	Aktivace funkce šifrování nainstalovaného zařízení

Jednotné přihlášení

V bodě "Single Sign-On" můžete nakonfigurovat ověřování Kerberos.

Zde nastavíte přístupové údaje a příslušné adresy URL / aplikace, které mohou používat tokeny Kerberos.

K dispozici v režimu s dohledem	
Název účtu	Název účtu
Jméno ředitele	Jedinečná identita, na kterou lze distribuovat vstupenky Kerberos.
Realm	Vaše sféra Kerberos, která má být použita (např. vaše doména).

Pomocí symbolu můžete vytvořit další adresy URL.

Vzor URL použitý k omezení tohoto účtu	Určí se adresy URL, na které lze distribuovat lístky Kerberos.

Pomocí symbolu můžete vytvořit další aplikace.

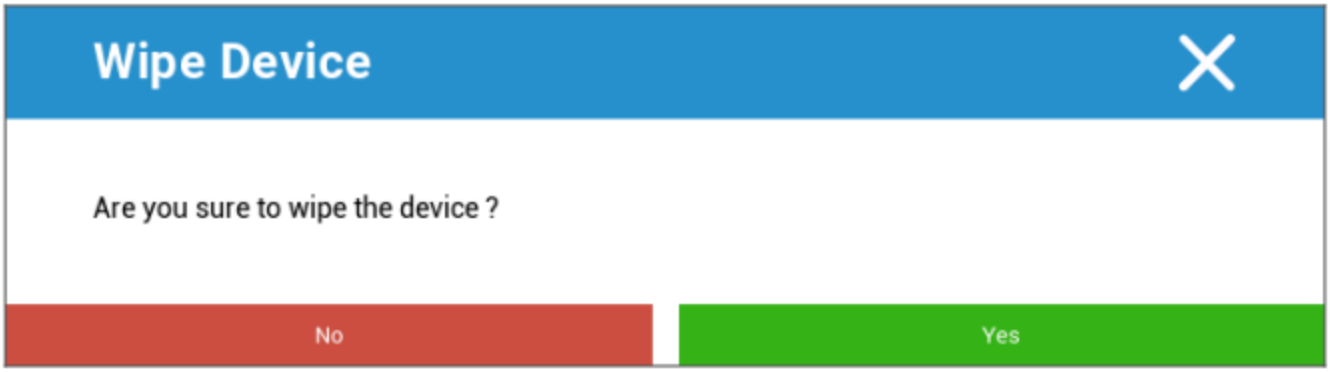
Aplikace pro omezení tohoto účtu	Bude určeno Aplikace, kterým lze distribuovat vstupenky Kerberos

Konec životnosti (pouze na úrovni zařízení)

Vymazat (pouze na úrovni zařízení)

V části "Wipe" můžete obnovit tovární nastavení zařízení. Zde budou vymazána firemní i soukromá data v zařízení koncového uživatele.

Po kliknutí na symbol "Minus" by se měla zobrazit následující zpráva.



Pokud zvolíte "Ano", můžete provést vymazání.

V části "Wipe Report" lze zobrazit následující položky.

Setřeno	Historie toho, kdo stírání provedl
Datum	Datum
Stav	Stav (např. zda bylo vymazání provedeno úspěšně)

Nastavení omezení

Funkčnost zařízení

Zde můžete blokovat jednotlivé funkce zařízení koncového uživatele.

Povolení instalace aplikací	Povolení instalace aplikací
Povolit kameru	Povolení používání fotoaparátu
Povolit FaceTime	Povolit FaceTime
Povolit snímání obrazovky	Povolit snímání obrazovky
Povolení automatické synchronizace při roamingu	Povolení automatické synchronizace při roamingu
Povolit Siri	Povolit Siri
Povolení hlasového vytáčení	Povolení hlasového vytáčení
Povolení nákupu v aplikaci	Povolení nákupu v aplikaci
Vyžadování hesla iTunes Store pro všechny nákupy	Vyžadování hesla iTunes Store pro všechny nákupy
Povolit hraní pro více hráčů	Povolit hraní pro více hráčů
Povolení přidávání přátel do služby Game Center	Povolení přidávání přátel do služby Game Center
Povolení otevření ze spravovaného do nespravovaného	Povolení otevírání obsahu spravovaných aplikací v nespravovaných aplikacích
Povolit otevření z neřízeného na řízený	Povolení otevírání obsahu nespravovaných aplikací ve spravovaných aplikacích
Povolení zobrazení dneška na uzamčené obrazovce	Když je toto nastavení aktivní, zobrazí se v oznamovacím centru na zamykací obrazovce zobrazení "Dnes".
Povolení ovládacího centra na zamykací obrazovce	Povolení Ovládacího centra na uzamčené obrazovce
Povolit TouchID	Povolit TouchID
Povolení aktualizací PKI over-the-air	Povolení aktualizací PKI over-the-air
Povolit zamčenou vkladní knížku	Povolení passbooku při zamknutém zařízení

Omezení sledování reklam	Tato funkce deaktivuje sledování reklam (např. inzerenti nemohou používat sledování reklam k šíření personalizovaných reklam).
Povolit předávání	Povolit předávání
Povolení výsledků internetu v záři reflektorů	Povolení internetových výsledků v záři reflektorů (např. Bing nebo Wikipedia)
Vyžadování přístupového kódu při prvním párování AirPlay	Vyžadování přístupového kódu při prvním párování AirPlay
Ochrana zápěstí hodinek Force Watch	Pokud je aktivována, jsou hodinky Apple Watch nuceny používat funkci "Ochrana zápěstí" (rozpoznávání zápěstí).
Povolení knihovny fotografií iCloud	Umožňuje používat knihovnu iCloud Photo Library. Pokud není povoleno, budou všechny obrázky, které nebyly zcela staženy z iCloudu, vymazány z místního úložiště.
K dispozici v režimu Supervised	
Povolit změnu účtu	Povolení úprav "pošta, kontakty, kalendář"
Povolení služby AirDrop	Povolení služby AirDrop
Povolení modifikace aplikace Cellular	Toto nastavení blokuje nastavení, které aplikace mohou používat mobilní data. Toto nastavení lze například nastavit ručně na zařízení koncového uživatele a poté toto omezení aktivovat.
Povolení dotazování Siri na obsah vytvořený uživatelem z webu	Webové vyhledávání na některých webových stránkách je blokováno, např. na Wikipedii, protože každý může provádět změny podle svého uvážení.
Povolení filtru nadávek Siri	Profanace namířená proti Siri je cenzurována.
Povolení obchodu iBook Store	Povolení obchodu iBook Store
Povolit iBook Store Erotika	Povolit iBook Store Erotika
Povolení úpravy nastavení služby Najít mé přátele	Povolení úpravy nastavení služby Najít mé přátele
Povolit Game Center	Povolit Game Center
Povolit párování hostitelů	Párování řídicího počítače
Povolení instalace konfiguračních profilů	Povolení instalace konfiguračních profilů
Povolit odebrání aplikace	Odstranění řídicích aplikací

Povolení iMessage	Povolení iMessage
Povolit vymazání veškerého obsahu a nastavení	Povolení vymazání veškerého obsahu a nastavení
Povolení konfigurace omezení	Povolení konfigurace omezení
Povolit podcast	Povolit podcast
Povolit vyhledávání definic	Povolit vyhledávání definic
Povolení prediktivní klávesnice	Povolit prediktivní klávesnici
Povolit automatickou opravu	Povolit automatickou korekci
Povolení instalace aplikací uživatelského rozhraní	Pokud je deaktivován, nelze z veřejného obchodu AppStore instalovat žádné aplikace (ikona se již nezobrazuje). Aplikace však lze stále instalovat prostřednictvím iTunes a Konfigurátoru.
Povolení klávesových zkratek	Povolit klávesové zkratky, pokud je zařízení připojeno k fyzické klávesnici.
Povolení párování s hodinkami Apple Watch	Zakáže párování mezi zařízením a hodinkami Apple Watch, stávající spojení budou ukončena.
Povolit změnu přístupového kódu	Pokud není povoleno, nelze přidat, změnit ani odebrat žádné heslo zařízení.
Povolit změnu názvu zařízení	Pokyn pro určení, zda lze název zařízení změnit
Povolit úpravu tapety	Pokyny pro určení, zda lze tapetu změnit
Povolení automatického stahování aplikací	Pokud je zakoupená aplikace deaktivována, nebude se automaticky instalovat do jiných zařízení. Nevztahuje se na aktualizace stávajících aplikací
Povolit Novinky	Povolení zpráv v zařízení iOS
Povolení důvěryhodnosti aplikací Enterprise	Pokud je nastavena na hodnotu false, zabrání důvěryhodným podnikovým aplikacím.

iCloud

Blokování určitých funkcí při párování iCloudu

Povolit zálohování	Povolit zálohování
Povolení synchronizace dokumentů	Povolení synchronizace dokumentů
Povolit proud fotografií	Povolit proud fotografií
Povolit sdílený proud fotografií	Povolit sdílený proud fotografií
Povolení synchronizace s cloudovou klíčenkou	Povolení synchronizace s cloudovou klíčenkou
Povolení spravovaným aplikacím ukládat data	Povolení spravovaným aplikacím ukládat data
Povolení synchronizace poznámek a zvýraznění pro podnikové knihy	Povolení synchronizace poznámek a zvýraznění pro podnikové knihy
Umožnit zálohování podnikových knih	Umožnit zálohování podnikových knih

Zabezpečení a ochrana osobních údajů

Blokování těchto funkcí spojených s diagnostickými údaji

Povolení odesílání diagnostických dat do společnosti Apple	Povolení odesílání diagnostických dat do společnosti Apple
Povolit uživateli přijímat nedůvěryhodné certifikáty TLS	Povolit uživateli přijímat nedůvěryhodné certifikáty TLS
Vynucení šifrovaných záloh	Vynucení šifrovaných záloh

BYOD

Vestavěné zabezpečení iOS (kontejner)

iOS vždy dokázal rozlišovat mezi spravovaným (business) a nespravovaným (private). Vše, co pochází ze systému MDM, je považováno za spravované. Pokud například nainstalujete aplikaci prostřednictvím MDM oder nakonfigurujete účet Exchange, bude to systém iOS považovat za spravované.

Vše ostatní, co se v zařízení nakonfiguruje/instaluje ručně, bude považováno za nespravované. Například pokud si uživatel sám nainstaluje aplikaci WhatsApp nebo pokud přidává účet Exchange. Toto oddělení však nikdy neovlivnilo kontakty. Od verze iOS 11.3 (a vyšší) však bylo toto oddělení přidáno i pro kontakty.

Protože se jedná o základní funkci operačního systému, nemusíte nic instalovat ani nastavovat speciální kontejner.

Aktivujte vestavěnou funkci pro oddělení soukromých a pracovních aplikací/informací/souborů. Toto nastavení také zakáže některé další funkce, které by jinak mohly omylem vypnout části tohoto oddělení.

Aktivace

Aktivace kontejnerových řešení podporovaných aplikací AppTec360

Povolení kontejneru Google Divide	Povolení kontejneru Google Divide
Povolení kontejneru SecurePIM	Povolení kontejneru SecurePIM

Pokud jste kontejner SecurePIM aktivovali, najdete v části "Aktivace" také následující bod. Kromě toho se hned otevřou další čtyři záložky, které jsou popsány níže.

E-mailová adresa podpory	E-mailová adresa podpory, na kterou se uživatel může obrátit s problémy.

Heslo SecurePIM

V části "SecurePIM Password" můžete nastavit pokyny pro sílu zabezpečení hesla.

Časový limit relace	Zde můžete nastavit, po kolika minutách je třeba znovu zadat nové heslo, jakmile SecurePIM běží na pozadí.
Délka hesla	Délka hesla pro přístup do kontejneru SecurePIM
Velká písmena	Minimální počet velkých písmen
Znaky malých písmen	Minimální počet malých písmen
Speciální znaky	Minimální počet speciálních znaků
Číslice	Minimální počet číslic
Aplikace Wipe	Kolikrát lze heslo zadat nesprávně, než se obsah SecurePIM vymaže. (Aplikace však stále zůstává v zařízení koncového uživatele).

Zabezpečení SecurePIM

V části "Zabezpečení SecurePIM" můžete nastavit různá nastavení zabezpečení.

Detekce zařízení s jailbreakem	Pokud je toto nastavení aktivováno, bude přístup ke kontejneru SecurePIM zablokován, jakmile bude zařízení detekováno jako jailbreaknuté.
Zabezpečená textová pole	Obsah polí pro odeslání bude zašifrován, do operačního systému (iOS) se nedostanou žádné informace. Poznámka: Pokud je toto nastavení aktivní, automatická oprava již není k dispozici.
Export kontaktních údajů do zařízení	Pokud je toto nastavení aktivováno, může uživatel exportovat kontakty Exchange do svého místního zařízení. Poznámka: Exportuje se pouze jméno a telefonní číslo.
Zobrazit místo události	Pokud je toto nastavení aktivováno, zobrazí se umístění nadcházejících událostí v oznamovací liště.
Zobrazit název události	Pokud je toto nastavení aktivováno, zobrazí se v oznamovací liště umístění názvu nadcházející události.

Prohlížeč SecurePIM

Zde můžete nakonfigurovat prohlížeč SecurePIM.

Pomocí symbolu můžete definovat novou adresu URL.

Pomocí symbolu můžete definovanou adresu URL opět odebrat.

"Adresy URL na bílé listině" jsou adresy URL, které lze načíst.

"Adresy URL na černé listině" jsou adresy URL, které nelze načíst, a proto jsou blokovány.

Upozorňujeme, že položky bílé listiny mají vyšší prioritu než položky černé listiny. V části "Bookmark Title" (Název záložky) můžete zadat název. Pomocí položky "Bookmark URL" můžete k názvu záložky přiřadit URL adresu - tímto způsobem můžete příslušným uživatelům distribuovat individualizované záložky.

Výměna

V části "Exchange" můžete nakonfigurovat účet Exchange.

E-mailová adresa ActiveSync	E-mailová adresa Exchange (všimněte si "zástupných symbolů").
Přihlášení k Exchange ActiveSync	Výměna uživatelských jmen (všimněte si "zástupných symbolů")
Server Exchange ActiveSync	Adresa serveru Exchange (FQDN)
Doména Exchange ActiveSync	Adresa domény Exchange
Certifikát uživatele	Certifikát uživatele
Ověřování na základě certifikátu	Uživatel se ověří pomocí certifikátu
Povolit šifrování S/MIME	Umožňuje uživateli šifrovat poštu
Povolení podepisování S/MIME	Umožňuje uživateli podepsat svou poštu
Kontrola CRL	Pokud je aktivní, bude soukromý certifikát porovnán se seznamem odvolaných certifikátů (CRL).

Správa připojení

Wi-Fi

Identifikátor sady služeb (SSID)	SSID sítě, která má být připojena.
Automatické připojení	Aktivace automatického připojení při připojení k síti
Skrytá síť	Aktivovat v případě, že přístupový bod nevysílá SSID.

Nastavení serveru proxy

Konfigurace proxy serveru pro každý přístupový bod

Žádné	Nezavést žádnou proxy
Manuální	Vytvoření ručního zástupce
Adresa URL proxy serveru	Adresa pro přístup k nastavení proxy serveru
Přístav	Nastavení portu pro proxy server
Ověřování	Uživatelské jméno pro ověřování na serveru Proxy
Heslo	Heslo pro ověřování na serveru Proxy
Automatické	Automatické vytvoření proxy serveru
Adresa URL proxy serveru	Adresa URL pro přístup k nastavení proxy serveru

Typ zabezpečení

Nastavení typu zabezpečení pro přístupový bod

WEP	
Heslo	Heslo pro přístupový bod

WPA/WPA2	
Heslo	Heslo pro přístupový bod

WEP Enterprise - WPA / WPA2 Enterprise - Any Enterprise			
	Protokoly		
	TLS	Aktivace/deaktivace	
	TTLS	Aktivace/deaktivace	
	LEAP	Aktivace/deaktivace	
	PEAP	Aktivace/deaktivace	
	EAP-FAST	Aktivace/deaktivace	
	EAP-SIM	Aktivace/deaktivace	
	Použití PAC		Použití PAC (Protected Access Controll)
	Ustanovení PAC	Konfigurace systému Provision PAC	
	Anonymní poskytování PAC	Anonymní poskytování PAC	
	Vnitřní ověřování	Ověřovací protokol, který by měl být použit: PAP, CHAP, MSCHAP, MSCHAPv2	
	Uživatelské jméno	Ověřování uživatelského jména	
	Nepoužívejte heslo pro připojení	Nepoužívejte heslo pro připojení	
	Certifikát totožnosti	Nahrání/vybrání ověřovacího certifikátu	
	Vnější identita	Identita viditelná zvenčí	
	Trust		
	Důvěryhodný certifikát 1	Nahrání prvního důvěryhodného certifikátu	
	Důvěryhodný certifikát 2	Nahrání druhého důvěryhodného certifikátu	
	Důvěryhodný certifikát 3	Nahrání třetího důvěryhodného certifikátu	
	Názvy certifikátů důvěryhodných serverů	Názvy očekávaných certifikátů serverů (v seznamu odděleném čárkou)	

Žádné	Nezavádět žádné zabezpečení

VPN

Název připojení	Název profilu VPN

Typ VPN

VPN

Veškerý síťový provoz zařízení bude směrován prostřednictvím připojení VPN.

Typ připojení	Vytvoření typu připojení VPN
IPsec (cisco)	Protokol IPsec od společnosti cisco
PPTP	Protokol PPTP
L2TP	Protokol L2TP
Cisco AnyConnect	Protokol AnyConnect
Juniper SSL	Protokol Juniper SSL
F5 SSL	Protokol F5 SSL
SonicWall mConnect	SonicWall mobile Connect
Aruba VIA	Protokol Aruba VIA
Vlastní protokol SSL	Připojení přes vlastní protokol SSL
OpenVPN	Protokol OpenVPN

VPN pro jednotlivé aplikace

Při otevření určité aplikace se vytvoří připojení VPN.

Automatické spuštění připojení VPN pro jednotlivé aplikace		Automatické spuštění připojení VPN pro jednotlivé aplikace
Typ připojení		Vytvoření typu připojení VPN
	Cisco AnyConnect	Protokol AnyConnect
	Juniper SSL	Protokol Juniper SSL
	F5 SSL	Protokol F5 SSL
	SonicWall mConnect	SonicWall mobile Connect
	Aruba VIA	Protokol Aruba VIA
	Vlastní protokol SSL	Připojení přes vlastní protokol SSL
	OpenVPN	Protokol OpenVPN

Nastavení serveru proxy

Konfigurace proxy serveru pro připojení VPN

Žádné	Nezavést žádnou proxy
Manuální	Ruční vytvoření proxy serveru
Adresa URL proxy serveru	Adresa pro přístup k nastavení proxy serveru
Přístav	Nastavení portu pro proxy server
Ověřování	Uživatelské jméno pro ověřování na serveru Proxy
Heslo	Heslo pro ověřování na serveru Proxy
Automatické	Automatické vytvoření proxy serveru
Adresa URL proxy serveru	Adresa URL pro přístup k nastavení proxy serveru

Zobrazit zástupné symboly	Zobrazí všechny dostupné uživatelské proměnné, které může AppTec360 použít.

APN

Název přístupového bodu	Název přístupového bodu
Uživatelské jméno přístupového bodu	Uživatelské jméno přístupového bodu
Heslo přístupového bodu	Heslo přístupového bodu
Proxy server	Adresa proxy serveru
Přístav	Příslušný port proxy serveru

Cellular

Povolení datového roamingu	Povolení datového roamingu
Povolení hlasového roamingu	Povolení hlasového roamingu
Povolení hotspotu	Povolení hotspotu

Proxy server HTTP

Typ proxy serveru	
Manuální	Vytvoření proxy serveru ručně
Adresa URL proxy serveru	Adresa pro přístup k nastavení proxy serveru
Přístav	Vytvoření portu proxy serveru
Ověřování	Uživatelské jméno pro ověřování na serveru Proxy
Heslo	Heslo pro ověřování na serveru Proxy
Automatické	Automatické vytvoření proxy serveru
Adresa URL proxy serveru PAC	Adresa URL proxy serveru PAC
Povolit přímé připojení, pokud je PAC nedostupný	Povolit přímé připojení (bez VPN), pokud je PAC nedostupný.
Povolení obcházení proxy serveru pro přístup k chráněným sítím	Povolení obcházení proxy serveru pro přístup k interním sítím v režimu captive

AirPrint

IP adresa	IP adresa tiskárny
Cesta ke zdroji	Určitá cesta k zařízení AirPrint

AirPlay

Název zařízení	Název zařízení
Heslo	Heslo pro párování
Bílá listina	Definujte seznam zařízení, se kterými se zařízení může výhradně spárovat.

Správa PIM

Exchange Active Sync

Název účtu	Název e-mailového účtu
Hostitel služby Exchange ActiveSync	Adresa/FQDN serveru
Povolit přesun	Povolit přesouvání e-mailů
Používejte pouze v poště	Interakce mohou probíhat pouze v nativní aplikaci Mail.
Použití protokolu SSL	Použití šifrování SSL
Doména	Doména serveru
Uživatel	Uživatelské jméno
E-mailová adresa	e-mailová adresa (pouze na úrovni zařízení)
Heslo (pouze na úrovni zařízení)	Heslo uživatele
Certifikát totožnosti	Vyberte příslušný certifikát pro ověřování na serveru.
Minulé dny služby Mail to Sync	Počet dní, do kdy mají být e-maily synchronizovány zpět. Bez omezení = neomezeně
Povolení S/MIME	Povolení šifrování S/MIME
Podpisový certifikát	Nahrání příslušného podpisového certifikátu
Šifrovací certifikát	Nahrání příslušného šifrovacího certifikátu

eMail

Nastavení účtů POP3 / IMAP v zařízení koncového uživatele

Popis účtu		Název des E-mailové účty		
Typ účtu		IMAP	Předpona cesty	Předpona cesty pro speciální složky
		POP		
Zobrazované jméno uživatele		Zobrazované jméno uživatele		
E-mailová adresa		E-mailová adresa uživatele		
Povolit přesun		Povolit přesouvání e-mailů		
Povolení S/MIME		Povolení šifrování S/MIME		
	Podpisový certifikát	Nahrání příslušného podpisového certifikátu		
	Šifrovací certifikát	Nahrání příslušného šifrovacího certifikátu		

Příchozí pošta

Nastavení příchozího serveru

Adresa poštovního serveru	Adresa poštovního serveru
Port poštovního serveru	Port poštovního serveru
Uživatelské jméno	Příslušné uživatelské jméno
Typ ověření	Typ ověření
Žádné	Ne Typ ověření
Heslo (pouze na úrovni zařízení)	Výzva k zadání hesla
MDM Challenge-Response	
NTLM	Ověřování NTLM
Digest HTTP MD5	
Použití protokolu SSL	V případě potřeby použijte protokol SSL

Odchozí pošta

Nastavení odchozího serveru

Adresa poštovního serveru	Adresa poštovního serveru
Port poštovního serveru	Port poštovního serveru
Uživatelské jméno	Příslušné uživatelské jméno
Typ ověření	
Žádné	Žádná metoda ověřování
Heslo (pouze na úrovni zařízení)	Výzva k zadání hesla
MDM Challenge-Response	
NTLM	Ověřování NTLM
Digest HTTP MD5	
Použití protokolu SSL	V případě potřeby použijte protokol SSL
Odchozí heslo stejné jako příchozí	Odchozí heslo stejné jako příchozí
Používejte pouze v poště	Aktivujte, pokud mají být všechny odchozí e-maily odesílány prostřednictvím aplikace Mail-App.

CalDav

Konfigurace nastavení a distribuce účtu CalDav

Popis účtu	Zobrazovaný název účtu
Hostitelské jméno	Název hostitele a/nebo IP adresa
Přístav	Přístav účtu CalDav
Hlavní adresa URL	Hlavní adresa URL účtu
Uživatelské jméno	Příslušné uživatelské jméno CalDav
Heslo (pouze na úrovni zařízení)	Příslušné heslo CalDav
Použití protokolu SSL	V případě potřeby použijte protokol SSL

Přihlášené kalendáře

Nastavení a distribuce přihlášených kalendářů

Popis	Zobrazovaný název účtu
ADRESA URL	Adresa URL databáze kalendáře
Uživatelské jméno	Uživatelské jméno předplatného kalendáře
Heslo (pouze na úrovni zařízení)	Heslo předplatného kalendáře
Použití protokolu SSL	V případě potřeby použijte protokol SSL

LDAP

V této oblasti nastavte připojení LDAP, abyste umožnili dynamickou výměnu certifikátů mezi zařízením koncového uživatele a službou Active Directory.

Upozorňujeme, že vybraný uživatel vyžaduje příslušné oprávnění ke čtení.

Popis účtu	Popis účtu
Uživatelské jméno účtu	Uživatel pro přístup k LDAP
Heslo k účtu	Heslo pro přístup do LDAP
Název hostitele účtu	Název hostitele/IP adresa serveru LDAP
Použití protokolu SSL	V případě potřeby použijte protokol SSL

Ve druhé části můžete definovat jednotlivé filtry pro vyhledávání v registru LDAP.

Popis	Oblast působnosti	Základna pro vyhledávání
Popis filtru	Úroveň vyhledávání v registru LDAP	Definice jednotlivých filtrů

Správa webu

Webové klipy

V tomto umístění definujte záložky s odkazy na webové stránky, intranetové portály atd., které budou viditelné jako aplikace v zařízení koncového uživatele.

Štítek	Název připojení v zařízení koncového uživatele
ADRESA URL	Odkaz na příslušné webové stránky
Odnímatelný	Pokud je aktivován, může uživatel webový klip odstranit.
Ikona	V tomto dialogu nahrajte logo připojení: Rozměry 180x180, formát png
Předkomponovaná ikona	Pokud je aktivována, nezobrazí se na ikoně žádné další efekty (stín, odraz).
Přes celou obrazovku	Při otevírání webových klipů se prohlížeč otevírá v režimu celé obrazovky.

Filtr webového obsahu

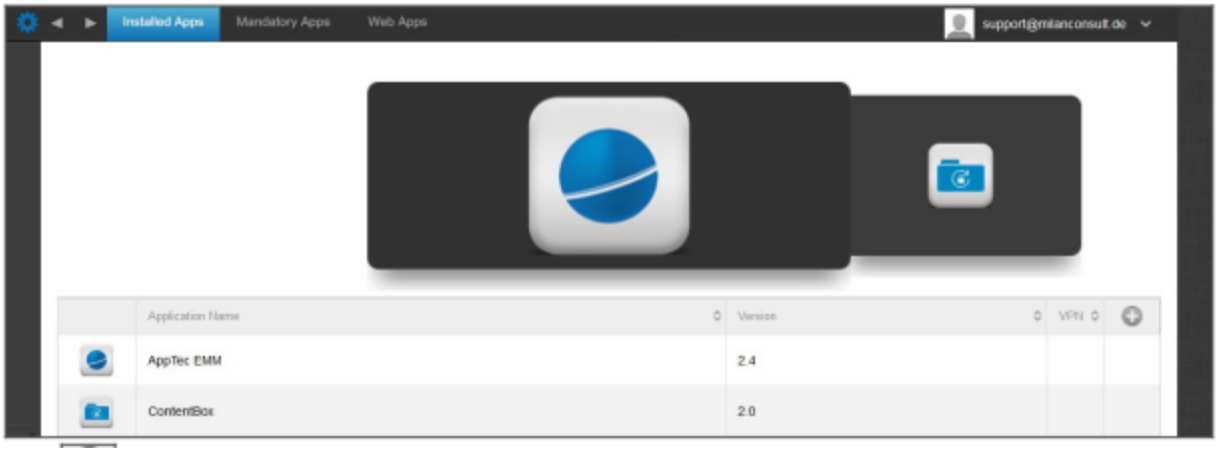
Filtr webového obsahu umožňuje omezit přístup k určitým internetovým stránkám.

Povolené webové stránky	
Omezení obsahu pro dospělé	Webový filtr se automaticky použije na obsah pro dospělé
Povolené adresy URL	Pomocí symbolu + přidejte povolené stránky
Adresy URL na černé listině	Pomocí symbolu + přidejte blokované stránky
Pouze konkrétní webové stránky	Zobrazit lze pouze určitý obsah, který můžete přidat pomocí symbolu +.

Správa aplikací

Správce podnikových aplikací

Nainstalované aplikace (pouze na úrovni zařízení)



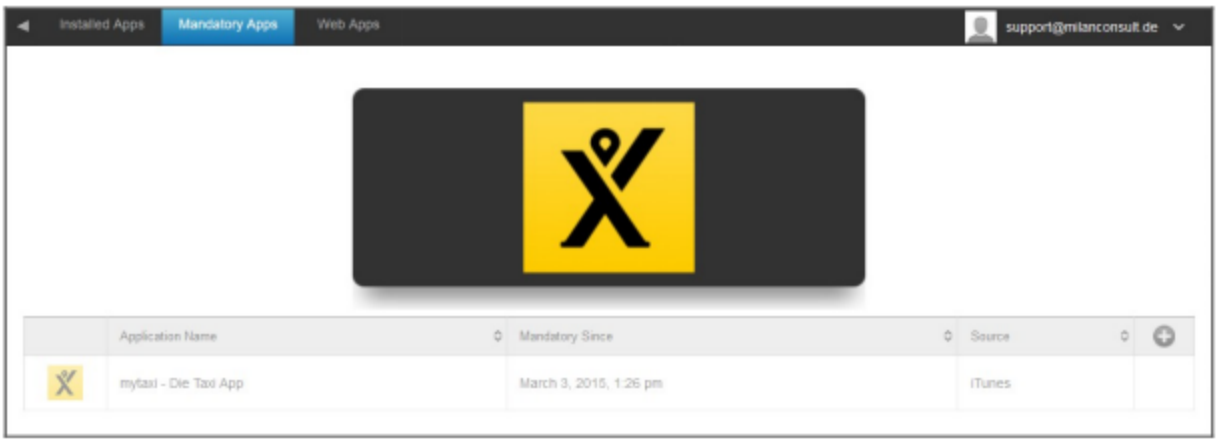
Zde můžete zobrazit aplikace, které jsou v zařízení aktuálně nainstalovány.

Povinné aplikace

V části Povinné aplikace můžete nařídit potřebné aplikace.

Uživatel bude neustále upozorňován na nutnost instalace této aplikace.

Prostřednictvím , lze definovat povinnou aplikaci.



Může se jednat o aplikaci z obchodu Apple App Store, ale také o interní aplikaci.

Pokud se jedná o zařízení pod dohledem, aplikace se nainstaluje automaticky.

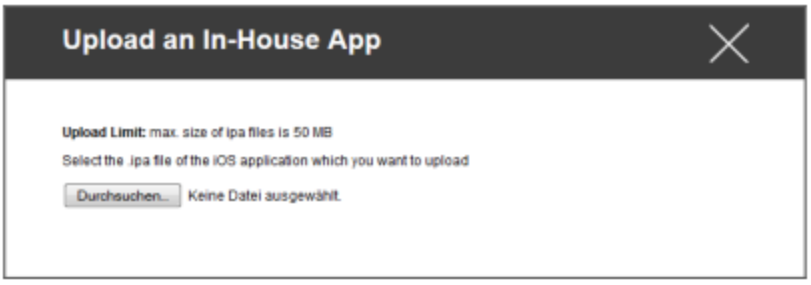
Do zařízení můžete nahrát aplikaci z veřejného obchodu Apple AppStore i interně vyvinutou aplikaci.

Nebo si můžete vybrat z kategorie "iOS In-House Apps" a vybrat vlastní aplikaci, kterou jste nahráli v části Obecná nastavení.

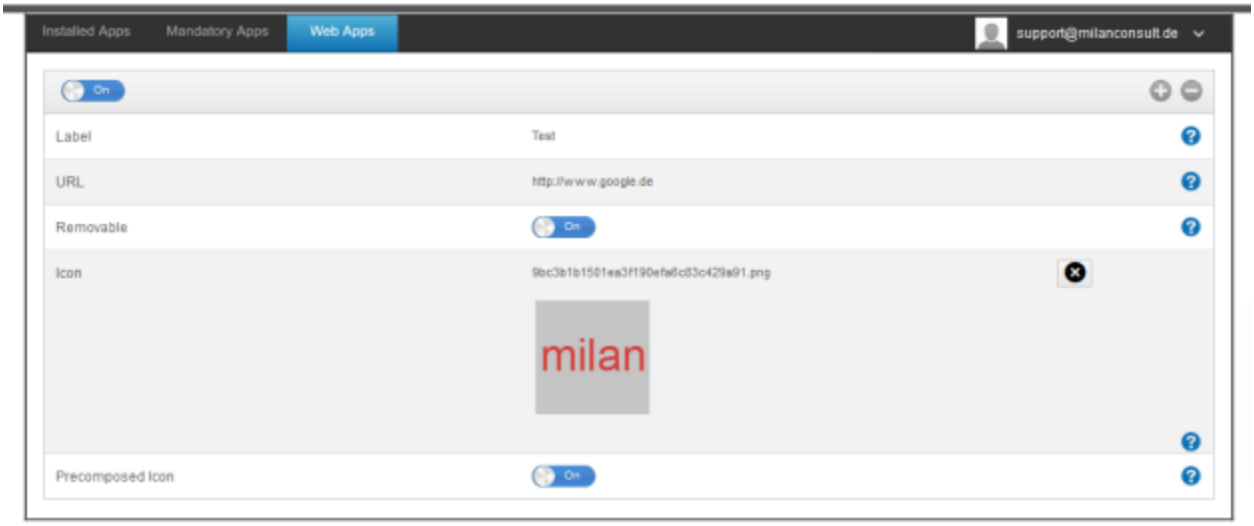
Možnosti instalace

Aktualizovat (podporováno pouze pro VPP na zařízení)	Jednou týdně se zjistí, zda je k dispozici aktualizace aplikace. Pokud ano, bude tato aktualizace nainstalována U vlastních aplikací se pro proces aktualizace použije cíl aktualizace, který jste nakonfigurovali v obecných nastaveních.
Předbíhání, pokud není řízeno	Pokud je aplikace již nainstalována, MDM ji převezme a bude ji spravovat.
Odstranění aplikace při odebrání profilu MDM	V případě odebrání správy zařízení bude aplikace odinstalována.
Zabránění zálohování dat aplikace	Záloha dat specifických pro aplikaci nebude vytvořena.
Nastavení aplikace	V části "Nastavení aplikace" můžete aplikaci přiřadit určité hodnoty do popředí (pokud to aplikace podporuje, v případě potřeby se zeptejte vývojáře aplikace).

Soubor ipa můžete také přímo vybrat a nahrát pomocí funkce "Nahrát vlastní aplikaci".



Webové aplikace



Pod bodem "Web Apps" můžete, podobně jako u "Web Clips", posílat internetové stránky nebo intranetové portály jako aplikaci do zařízení koncového uživatele v oblasti správy webu. Ve výchozím nastavení se Web Apps zobrazí v celoobrazovkovém režimu, který lze nakonfigurovat v části Webclips.

Štítek	Název připojení v zařízení koncového uživatele
ADRESA URL	Odkaz na příslušné webové stránky
Odnímatelný	Pokud je aktivován, může uživatel webový klip odstranit.
Ikona	V tomto dialogu nahrajte logo připojení: Rozměry 180x180, formát png
Předkomponovaná ikona	Pokud je aktivována, nezobrazí se na ikoně žádné další efekty (stín, odraz).

Omezení a nastavení

Aplikace na černé / bílé listině

Zde můžete nastavit aplikace, které jsou blokovány (nebo povoleny) v závislosti na nastavení v části "Obecná nastavení". Po kliknutí se zobrazí vyhledávání známých aplikací. Zde můžete vyhledat aplikace, které chcete přidat.

Všimněte si, že pro tuto funkci je nutné monitorované zařízení.

Omezení aplikace SysApp

Blokování konkrétních aplikací nebo funkcí zařízení

Povolení používání služby YouTube	Povolení používání služby YouTube
Povolení používání obchodu iTunes Store	Povolení používání obchodu iTunes Store
Povolení používání prohlížeče Safari	Povolení používání prohlížeče Safari
Povolení automatického vyplňování	Umožňuje automatické vyplňování
Varování před podvody	Vynutí si upozornění na podvod
Povolení jazyka JavScript	Umožňuje použití jazyka JavaScript
Blokování vyskakovacích oken	Blokuje všechny druhy štěňat
Povolit soubory cookie	Volba, kdy bude Safari přijímat soubory cookie

App-VPN

Prostřednictvím tohoto symbolu můžete definovat aplikace, které budou při spuštění automaticky spouštět vybrané připojení VPN.

Nastavení aplikace

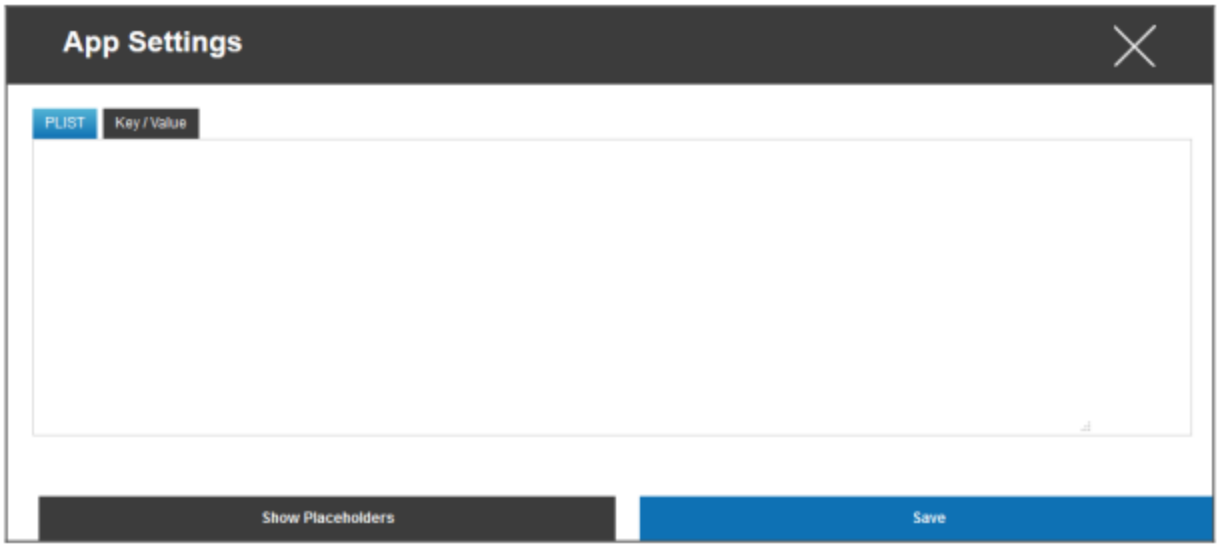
V části "Nastavení aplikace" můžete aplikaci přiřadit určité hodnoty do popředí (pokud to aplikace podporuje, v případě potřeby se zeptejte vývojáře aplikace).

Prostřednictvím symbolu přidáte (další) aplikaci. Opět zde najdete známé zobrazení AppTec360 App-Import.

Zde vyhledejte aplikaci, kterou chcete nakonfigurovat, a vyberte ji. Nastavení se bude týkat pouze spravovaných aplikací.

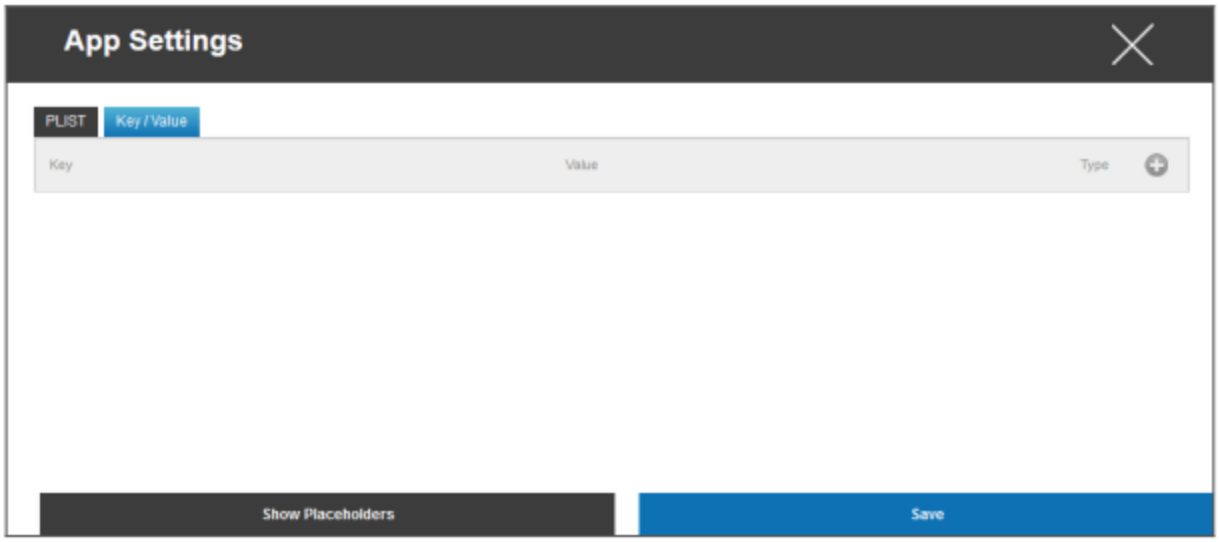
Pokud by import proběhl úspěšně, zobrazí se následující zobrazení:

Nyní můžete kliknutím na tlačítko , provádět různé konfigurace. Poté se zobrazí následující přehled:

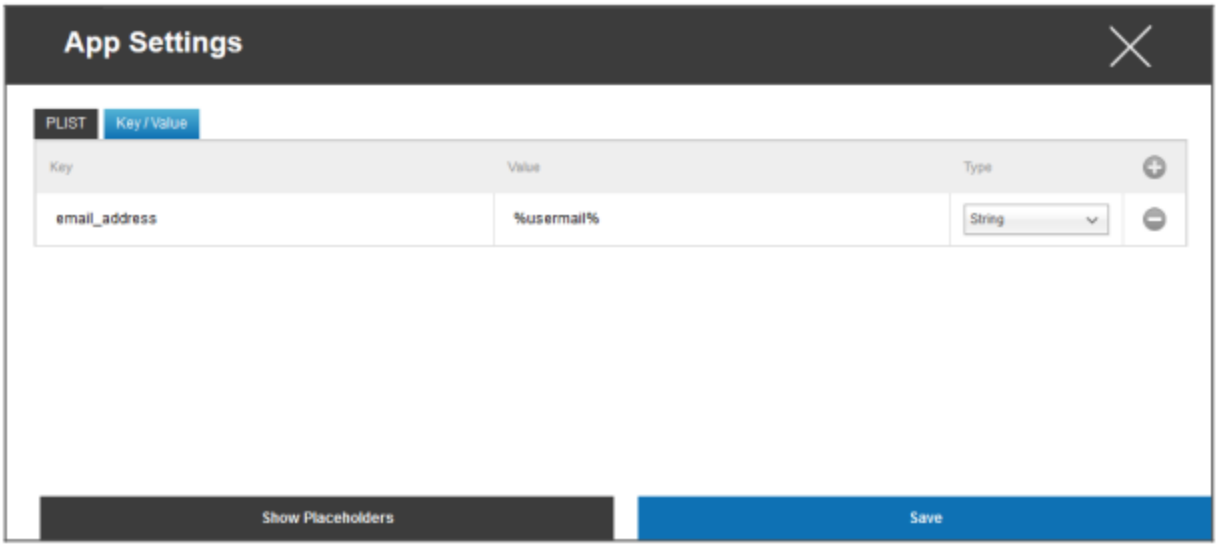


Pokud již máte PLIST (zdrojový text konfigurace), můžete jej zde přidat a vše uložit pomocí "Uložit".

V části "Klíč / hodnota" můžete k aplikaci připojit konkrétní konfigurace.



Zde můžete vytvořit nový klíč a jeho hodnotu pomocí symbolu.



Samozřejmě máte k dispozici všechny zástupné symboly AppTec.

Vysvětlení "Type":

Řetězec	Text
Boolean	Pravda/nepravda
Číslo	Číslo

Pomocí symbolu můžete aplikaci opět odebrat.

Obchod s podnikovými aplikacemi

Aplikace iTunes

V tomto bodě můžete distribuovat volitelné aplikace pro uživatele.

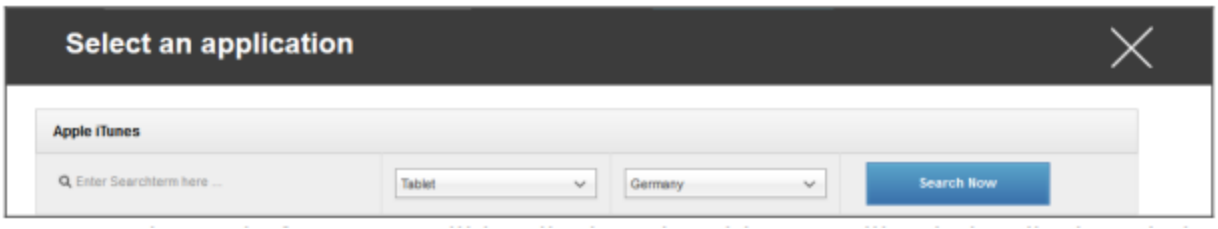
Pokud se zde nachází aplikace, bude automaticky nainstalována do zařízení koncového uživatele AppTec360 Store.

Jedná se pouze o odkazy na oficiální Apple App Store. Z tohoto důvodu musí být každé zařízení koncového uživatele vybaveno Apple ID.

V tuto chvíli doporučujeme, aby měl každý uživatel své vlastní Apple ID.

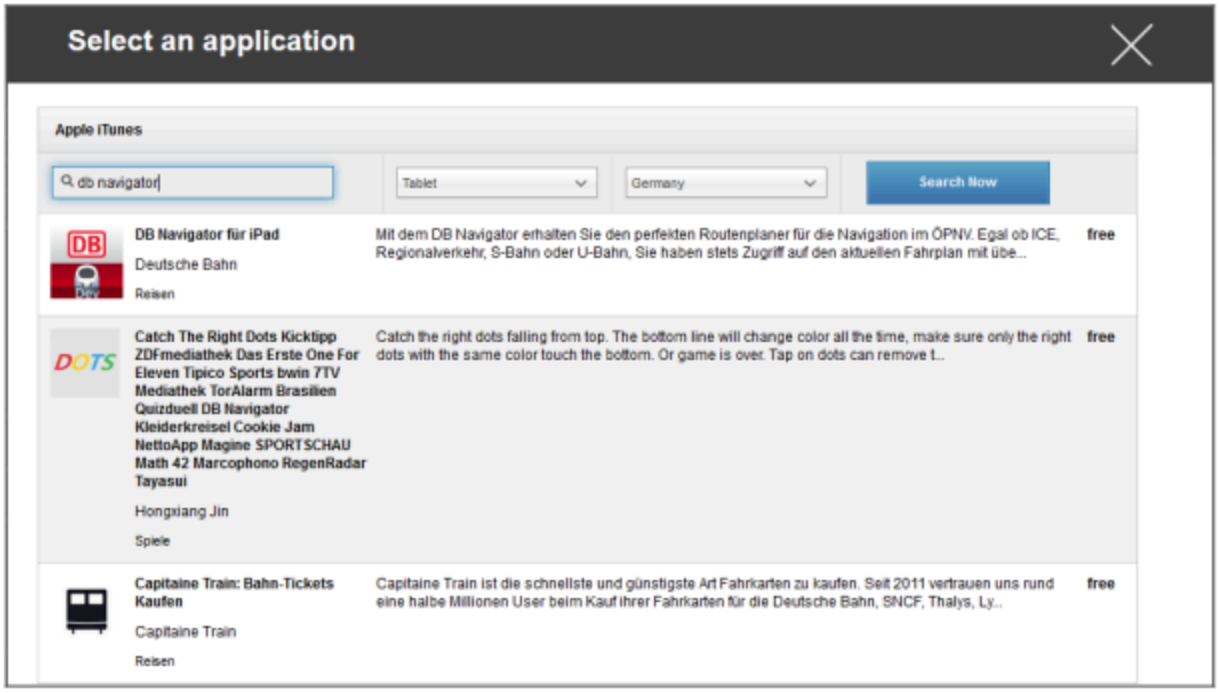
Pomocí symbolu můžete přidávat další aplikace.

Poté by se mělo otevřít okno s následujícím přehledem.



Upozorňujeme, že se zobrazí pouze bezplatné aplikace, placené aplikace se zobrazí pouze prostřednictvím sítě VPN.

V části "Zadejte zde hledaný výraz..." můžete vyhledat aplikaci, která je v obchodě Apple App Store.



Po kliknutí na ikonu nebo na název aplikace budete znovu vyzváni k provedení dalších konfigurací.

Udržujte aktuální stav	Jednou týdně se zjistí, zda je k dispozici aktualizace aplikace. Pokud ano, bude tato aktualizace nainstalována
Odstranění aplikace při odebrání profilu MDM	V případě odebrání správy zařízení bude aplikace odinstalována.
Zabránění zálohování dat aplikace	Záloha dat specifických pro aplikaci nebude vytvořena.
App-VPN	Vyberte připojení VPN, které se spustí po otevření aplikace.

Po kliknutí na tlačítko "Instalovat" se aplikace přidá do podnikového obchodu s aplikacemi a poté ji lze nainstalovat do zařízení koncového uživatele prostřednictvím AppTec360 AppStore.

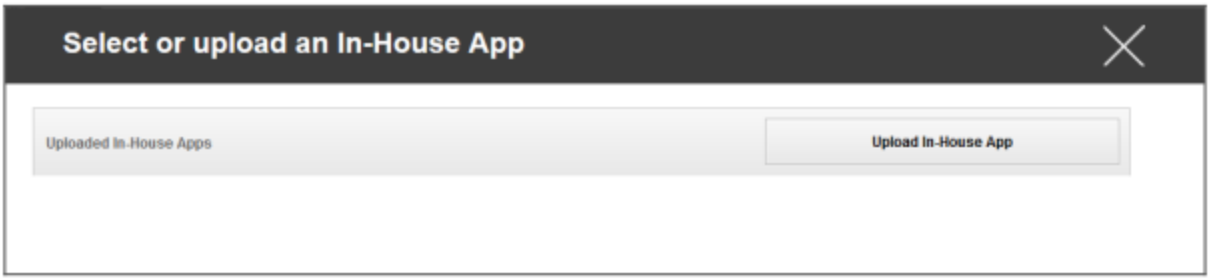
Pokud import do App-Store proběhl úspěšně, zobrazí se následující přehled:

In-House

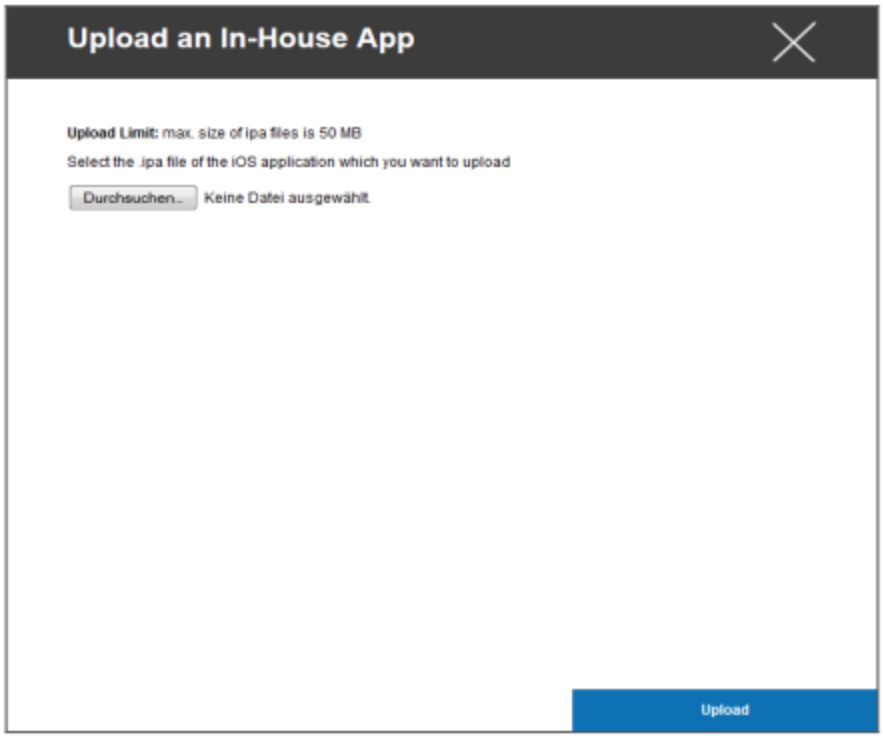
V bodě "In-House" můžete nahrát interně vyvinuté aplikace a distribuovat je.

Pomocí tohoto symbolu můžete distribuovat další aplikace In-House.

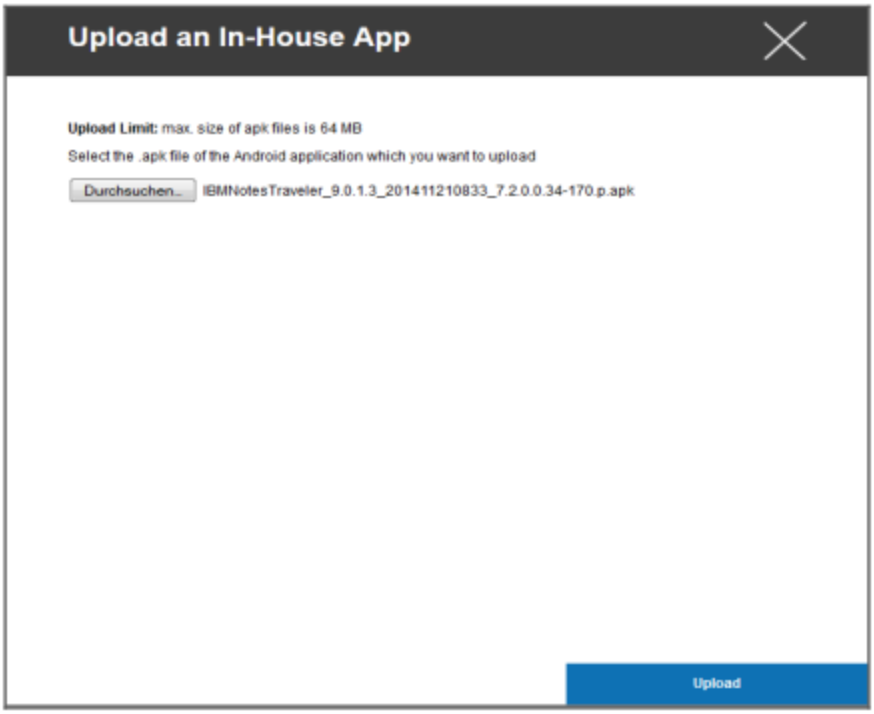
Pokud jste aplikaci In-House nikdy nedistribuovali, obdržíte následující přehled:



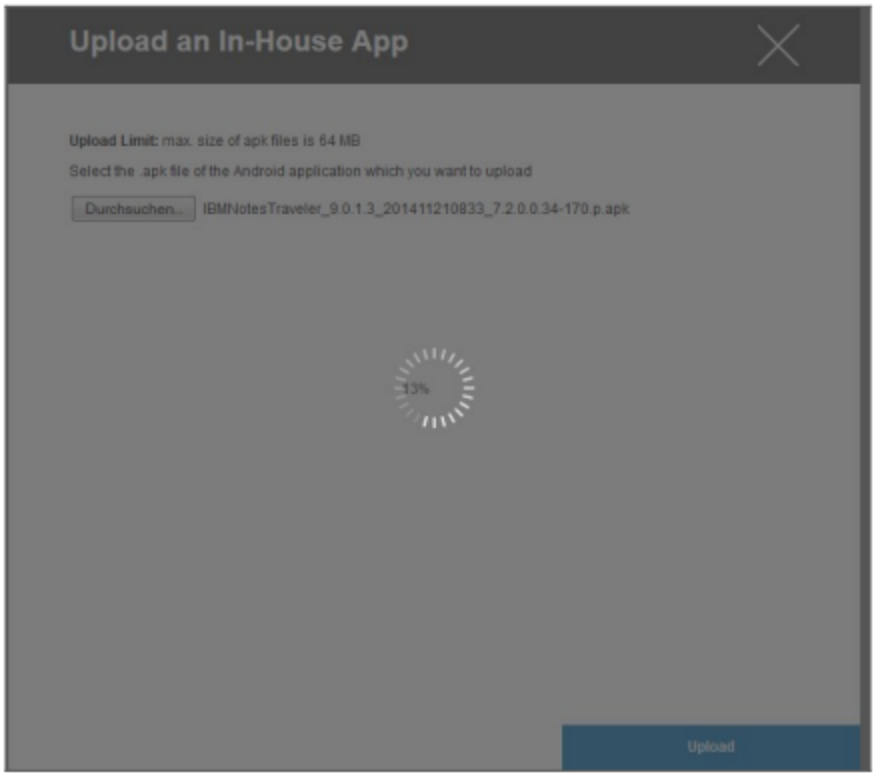
Za tímto účelem klikněte na tlačítko "Nahrát interní aplikaci" a zobrazí se následující přehled:



Nyní vyberte pomocí "Search..." soubor .ipa a klikněte na "Upload".



Vaše aplikace se nyní nahraje. Uprostřed kruhu vidíte procentuální vyjádření toho, jak velká část vaší aplikace již byla nahrána.



Pokud proběhne nahrávání interní aplikace úspěšně, zobrazí se nově nahraná aplikace v katalogu aplikací.

Uživatel má nyní možnost zobrazit a nainstalovat tuto aplikaci v AppTec360 Store na zařízení koncového uživatele v kategorii "In-House".

Vzhledem k tomu, že se nejedná o veřejnou aplikaci Apple AppStore, nepotřebuje uživatel v koncovém zařízení uložené Apple ID.

Režim kiosku

Režim iOS Kiosk je k dispozici pouze v režimu pod dohledem

Režim Kiosek umožňuje předem definovat aplikaci nebo adresu URL tak, aby bylo možné spouštět/navštěvovat výhradně tuto aplikaci/URL.

Kromě toho můžete v režimu kiosku deaktivovat různá hardwarová tlačítka.

Typ aplikace

Balíček

Pokud chcete aplikaci spustit v režimu kiosku, vyberte v části "Typ aplikace" možnost "Balíček".

Aplikace kiosku	Klikněte sem a vyberte aplikaci, která se má spustit v režimu kiosku. Aktuální přehled správy aplikací naleznete zde Můžete si vybrat mezi "Apple iTunes Apps" a "iOS In-House Apps".

ADRESA URL

Chcete-li v režimu kiosku spustit adresu URL, vyberte v části "Typ aplikace" možnost "URL".

ADRESA URL	Nyní definujte požadovanou adresu URL
Zásady stejného původu	Pokud je tato funkce aktivní, může uživatel surfovat pouze na podstránkách předdefinované adresy URL. Pokud jste například definovali následující adresu URL: www.mypage.com, pak může uživatel surfovat na stránkách www.mypage.com/subpage.
Adresy URL na bílé listině	Zde můžete udržovat bílou listinu, všechny tyto adresy URL jsou povoleny. Maximálně 1 adresa URL na řádek Adresa URL musí začínat http:/ nebo https://.
Adresy URL na černé listině	Zde můžete udržovat černou listinu, všechny tyto adresy URL jsou zakázány. Maximálně 1 adresa URL na řádek Adresa URL musí začínat http:/ nebo https://.
Vymazání prohlížeče po nečinnosti	Po nečinnosti se mezipaměť prohlížeče vyprázdní.
Heslo pro ukončení povoleno	Pokud tuto funkci aktivujete, uživatel má možnost ukončit režim kiosku pomocí hesla, které jste předem definovali.
Heslo pro ukončení	Jedná se o vámi předdefinované heslo.

Nastavení režimu kiosku

Plánovaný režim kiosku	Na základě denní doby můžete nastavit režim kiosku tak, aby se režim automaticky spustil a ukončil v předem stanovený čas.
Čas zahájení	Čas zahájení
Čas v minutách	Doba v minutách, po které by měl být režim kiosku opět ukončen.
Zakázat dotyk	Pokud je aktivován, dotykový displej je deaktivován.
Zakázat otáčení zařízení	Pokud je aktivována, je automatické přizpůsobení obrazovky deaktivováno.
Vypnutí přepínače vyzvánění	Pokud je aktivován, přepínač vyzvánění se deaktivuje. Od této chvíle je chování závislé na dříve nastavené funkci.
Zakázat tlačítka hlasitosti	Pokud je aktivována, tlačítka hlasitosti se deaktivují.
Zakázat tlačítko probuzení ve spánku	Pokud je aktivován, vypínač se deaktivuje.
Zakázat automatické zamykání	Pokud je aktivován, zařízení se nepřepne do pohotovostního režimu.
Povolení funkce Voice Over	Pokud je aktivován, aktivuje se hlasový asistent.
Povolení zvětšení	Pokud je aktivován, aktivuje se zoom.
Povolit invertování barev	Pokud je aktivován, aktivuje se režim inverzního zobrazení.
Povolení asistovaného dotyku	Pokud je aktivována, aktivuje se funkce AssistiveTouch.
Povolení volby mluvení	Pokud je aktivována, aktivuje se volba mluvit.
Povolení monofonního zvuku	Pokud je aktivována, aktivuje se funkce Mono Audio.
VoiceOver	Pokud je aktivována, může uživatel povolit funkci VoiceOver.
Zoom	Pokud je aktivována, může uživatel povolit funkci Zoom
Invertování barev	Pokud je aktivována, může uživatel povolit invertované barvy.
Asistivní dotyk	Pokud je aktivován, může uživatel povolit asistovaný dotyk.

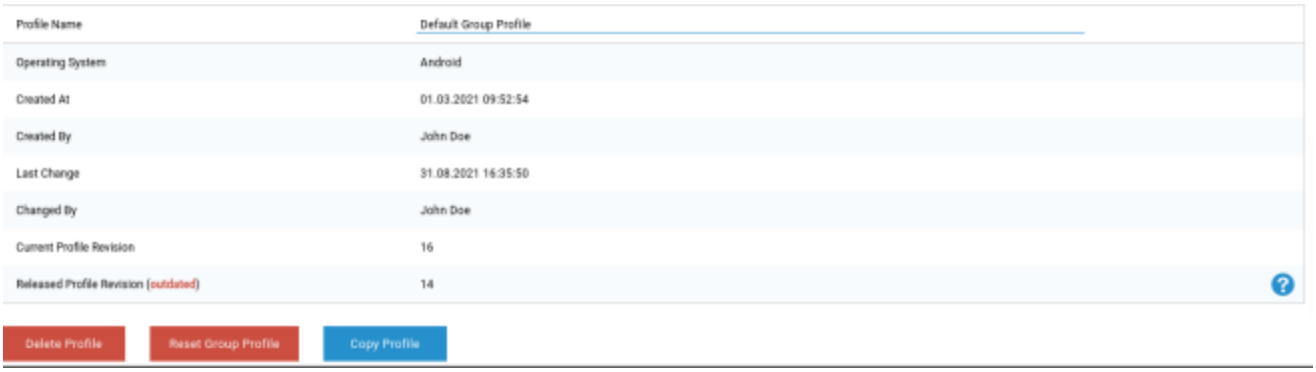
Android Enterprise – plně spravovaná konfigurace zařízení

V závislosti na tom, zda jste aktuálně vybrali profil skupiny nebo zařízení, se přehled a jeho dílčí body liší - věnujte tomu prosím pozornost!

Obecné

Přehled profilu skupiny (pouze na úrovni skupiny)

Po otevření profilu skupiny se zobrazí rychlý přehled profilu.



Název profilu	Název profilu (zde lze změnit)
Operační systém	Operační systém, pro který je profil určen
Vytvořeno v	Čas vytvoření
Vytvořil	Tvůrce profilu
Poslední změna	Čas poslední změny profilu
Změněno podle	Účet, který provedl poslední změny
Aktuální revize profilu	Revize uloženého stavu profilu
Vydaná revize profilu	Přiřazená revize profilu ("Assign now"). Pokud se za textem na štítku zobrazí " (zastaralý)", znamená to, že jste profil uložili, ale ještě jste ho nepřiřadili, takže zařízení budou stále dostávat starší verzi.

Přehled zařízení (pouze na úrovni zařízení)

Pokud se nacházíte na zařízení, zobrazí se přehledová rekapitulace vybraného zařízení, která obsahuje následující informace:

Název zařízení	Název zařízení
Umístění	Souřadnice polohy
Telefonní číslo	Telefonní číslo
Přiřazené povinné aplikace	Počet přidělených povinných aplikací
Verze operačního systému	Verze operačního systému zařízení
Operační systém	Operační systém (Android Enterprise)
Sériové číslo	Sériové číslo zařízení
Vlastnictví zařízení	Firemní nebo soukromé zařízení
Typ zařízení	Spravované zařízení AE Work
Zakořeněný	Stav, který udává, zda bylo zařízení rootnuto.
V souladu s předpisy	V souladu s pokyny
IP adresa	IP adresa zařízení
Naposledy viděno	Časový okamžik, kdy se zařízení naposledy připojilo k AppTec.
Poslední impuls	Časový okamžik, kdy byl do zařízení odeslán poslední push.
Režim vlastníka zařízení AE	Ano
Přiřazení uživatele	Uživatel nebo skupina, ke které je toto zařízení přiřazeno

Revize konfigurace (pouze na úrovni zařízení)

Zde získáte přehled o tom, který skupinový profil je k zařízení přiřazen.

Pokud kliknete na profil skupiny, získáte přímý přístup k tomuto profilu a můžete provádět nastavení.

Pomocí tohoto symbolu můžete vrátit distribuované aplikace do nastavení profilu skupiny.

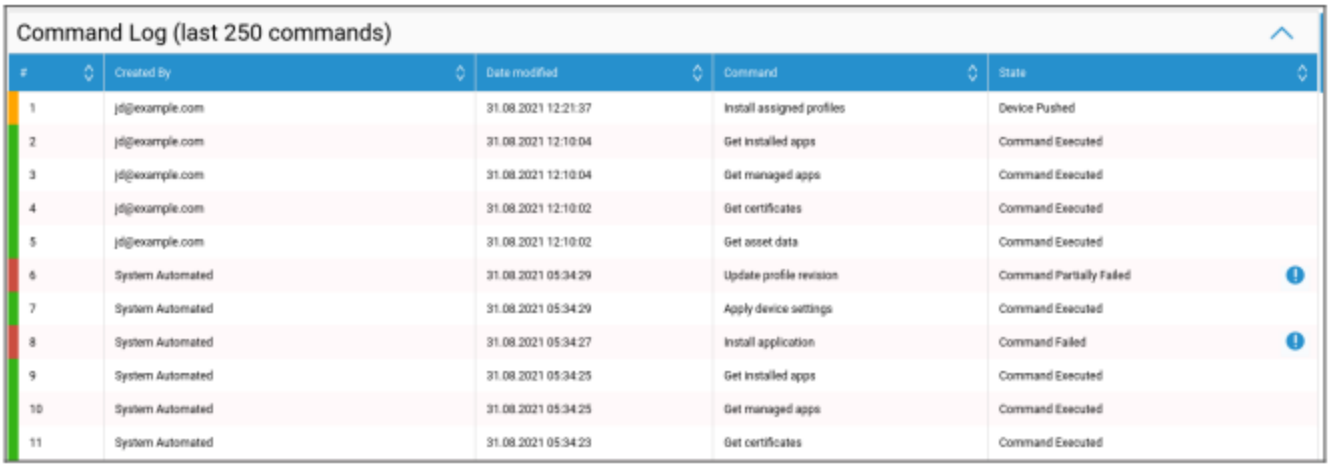
Pomocí tohoto symbolu můžete vrátit všechny používané aplikace do nastavení skupinového profilu.

"K dispozici je novější revize" znamená, že profil skupiny byl změněn a uložen, ale nebyl přiřazen. Profil skupiny je třeba přiřadit pomocí "Přiřadit nyní" na úrovni skupiny, aby se změny uplatnily na zařízení.

Protokol zařízení (pouze na úrovni zařízení)

Protokol příkazů

Zde můžete zjistit, které příkazy byly pro zařízení vydány a jaký je jejich stav.



Příkazy vytvořené pomocí "System Automated" jsou automaticky vytvořeny systémem.

Možné stavy příkazů

Stlačené zařízení	Službě push (např. APNS) byl odeslán požadavek na připojení, aby se zařízení připojilo zpět k serveru EMM.
Vytvořený příkaz	Příkaz byl vytvořen v systému.
Odeslaný příkaz	Příkaz byl odeslán do zařízení po jeho připojení k serveru.
Spuštěný příkaz	Příkaz byl úspěšně proveden.
Příkaz se nezdařil	Příkaz se nezdařil. *
Příkaz částečně selhal	V závislosti na operačním systému zařízení mohou být některé příkazy seskupeny. V tomto některé části této skupiny příkazů selhaly. *
Příkaz proveden, případně neúspěšný	Příkaz byl proveden, ale možná nebyl.
Přesunutí příkazu	Příkaz byl znovu odeslán uživatelem.
Vyřazené	Příkaz byl vyřazen. Například proto, že byl nahrazen jiným příkazem nebo že zařízení bylo znovu zapsáno a staré příkazy byly odstraněny.

Pokud je za zprávou vykřičník, můžete získat další informace, když na ikonu najedete kurzorem.

Nastavení zařízení

Konfigurace klienta

Zde můžete provést následující konfigurace zařízení se systémem Android:

Čas mimo soulad	Časový limit odezvy uživatele, po jehož uplynutí se použije akce vynucení.
Donucovací opatření po uplynutí lhůty pro splnění požadavků	vynucovací akce, pokud uživatel neprovede akce, které vedou ke stavu zařízení, které je v souladu s předpisy.
Frekvence sběru dat	Četnost shromažďování informací o zařízení/GPS
Frekvence srdečního tepu zařízení	Interval, ve kterém má zařízení kontaktovat server AppTec360. Min. 1 minuta Max. 24 hodin
Povolení aktualizací polohy	Pokud je aktivováno, zařízení odesílá aktualizace polohy na server AppTec360.
Čas aktualizace umístění	Určuje, v jakých časových intervalech zařízení odesílá aktualizace polohy do AppTec360.
Použití služby Google Location Accuracy pro aktualizaci polohy	Pokud je aktivováno, bude se pro aktualizace polohy používat poloha v síti (pokud bylo toto nastavení deaktivováno v části "Omezení", pak toto nastavení nic neovlivní).
Použití polohy GPS pro aktualizaci polohy	Pokud je aktivována, bude se pro aktualizaci polohy používat GPS.
Povolení falešných umístění	Umožňuje falšování informací o poloze prostřednictvím aplikací třetích stran.
Akce při ztrátě spojení	Pokud je tato možnost povolena, můžete zadat akci pro případ, že zařízení nezíská připojení k serveru MDM v intervalu heartbeat. Například pokud má zařízení interval srdečního rytmu 5 minut, připojí se k serveru v 10:35. Poté zařízení opustí dosah sítě Wi-Fi. Další srdeční tep v 10:40 se nezdaří a provede se zadaná akce.
Akce	Opatření, která je třeba přijmout, jakmile se zařízení stane nevyhovujícím. • Zámek zařízení = zámek zařízení • Vymazat zařízení = zařízení bude obnoveno do továrního nastavení.

	• Vymazání zařízení a karty SD = zařízení bude obnoveno do továrního nastavení a úložiště karty SD bude vymazáno.
Prahová hodnota	Můžete zadat prahový počet chybných srdečních tepů, které jsou nutné pro spuštění zadané akce.

Režim vynucování zásad	Výchozí nastavení:	Uživatelé budou pravidelně vyzýváni k provedení zbývajících akcí.
	Líné vynucování zásad:	Uživatelé nebudou nikdy vyzváni k provedení zbývajících akcí. Všechny otevřené akce se zobrazí v klientovi AppTec360.
	Agresivní prosazování zásad:	Uživatelé budou nepřetržitě vyzýváni k provedení zbývajících akcí.
Zámek verze AppTec360	Pokud je tato možnost povolena, lze zadat kód verze klienta AppTec360 MDM. Klient AppTec360 se aktualizuje pouze na zadanou verzi. Novější verze budou ignorovány. Downgrade NENÍ možný.	
Kód verze	Kód verze klienta AppTec360 MDM, který má být uzamčen.	
Zakázat oznámení AppTec360	Pokud je zakázáno, klient AppTec360 nezobrazí oznámení v oznamovacím panelu. Uživatelé tak mohou klienta AppTec360 zavřít prostřednictvím správce úloh. Pokud je klient AppTec360 zavřený, nebude správně fungovat několik funkcí včetně režimu Kiosk Mode a App Black/Whitelisting. Zařízení Samsung nabízejí ochranný mechanismus pro klienta AppTec360. Na zařízeních Samsung, která podporují rozhraní KNOX API, je oznámení ve výchozím nastavení vypnuto. Upozornění by nemělo být zakázáno na zařízeních se systémem Android 8.0 nebo vyšším.	

Tapety

Nastavení vlastní tapety	Povolení/zakázání vlastní tapety
Tapety	Nastavení režimu tapety na použití barevného kódu nebo obrázku
Zadejte barvu	Zadejte barvu pozadí jako hexadecimální hodnotu, např. #000000 pro černou nebo #ffffff pro bílou.
Nastavení obrázku jako tapety	Nahrání souboru s obrázkem, který chcete použít jako tapetu

Správa aktiv (pouze na úrovni zařízení)

Informace o zařízení

Model	Označení modelu zařízení
Operační systém	OS
Verze operačního systému	Verze operačního systému
Sériové číslo	Sériové číslo
Název zařízení	Název zařízení
Stav baterie	Stav baterie
Volná / celková paměť	Volná / celková paměť
Samsung Safe	Rozhraní Samsung SAFE, potřebné pro různé možnosti nastavení
K dispozici je karta SD	K dispozici je karta SD
Emulace karty SD	Emulovaná karta SD
Vyměnitelná karta SD	Vyjímatelná karta SD
SD Volná / Celková paměť	Volná paměť SD / Celková paměť karty SD

Wi-Fi

IP adresa	IP adresa zařízení
WiFi MAC	Adresa MAC WiFi

Cellular

Stav	Stav (nainstalovaná karta SIM)
Telefonní číslo	Telefonní číslo
Roaming (hlas / data)	Roaming pro hlas / data
Stav roamingu	Aktuální stav roamingu
IP adresa	IP adresa
Provozovatel/přepravce	Provozovatel/přepravce
Mobilní technologie	Mobilní technologie
IMEI	Číslo IMEI
ICCID	Jedná se o ID karty SIM, často také karty Smartcard nebo karty s integrovanými obvody (ICC).
IMSI	Mezinárodní identifikace mobilního účastníka (IMSI) umožňuje v mobilních sítích GSM a UMTS jednoznačnou identifikaci uživatelů sítě. IMSI se skládá z maximálně 15 číslic a konfiguruje se následujícím způsobem: • Kód země mobilního telefonu (MCC), 3 číslice • Kód mobilní sítě (MNC), 2 nebo 3 číslice • Identifikační číslo mobilního účastníka (MSIN), 1-10 číslic
Současné MCC/MNC	Viz "SIM MCC/MNC"
SIM MCC/MNC	Kód mobilní země je zavedený identifikátor země stanovený ITU podle normy E.212. Funguje ve spojení s kódem mobilní sítě (MNC) pro identifikaci mobilní sítě. Znamená kód země/mobilní sítě karty SIM. Pokud jste v roamingu v jiné mobilní síti, pak se logicky budou údaje "Current MCC/MNC" a "SIM MCC/MNC" lišit.

Bluetooth

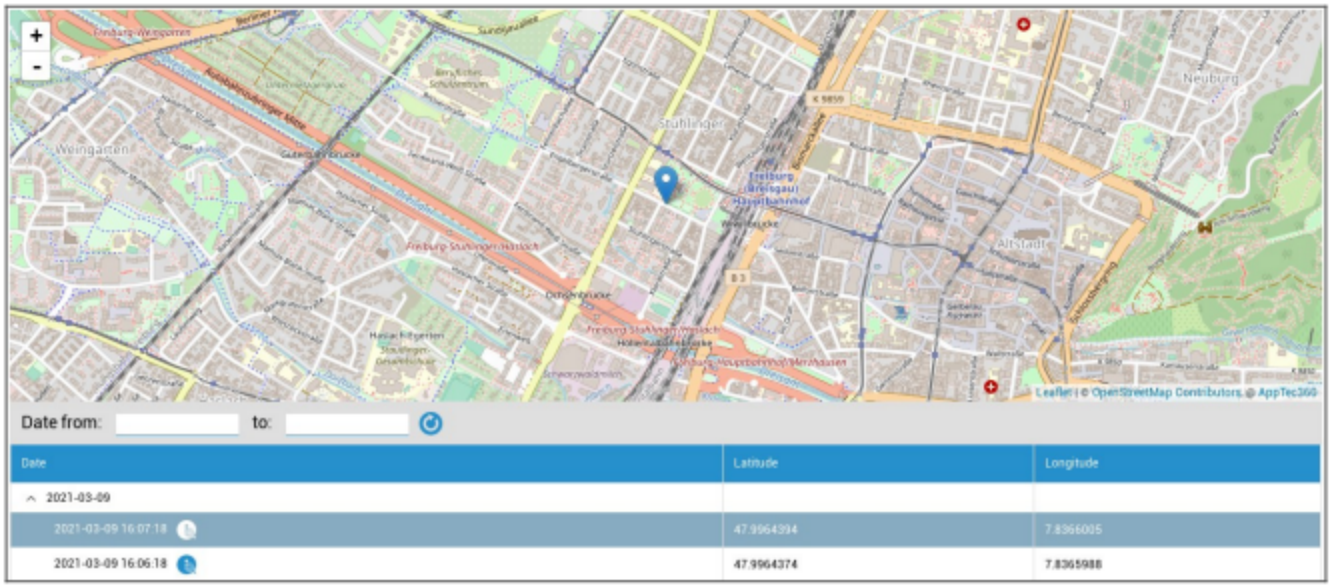
Bluetooth MAC	Adresa MAC Bluetooth

Správa zabezpečení

Ochrana proti krádeži (pouze na úrovni zařízení)

Informace GPS (pouze na úrovni zařízení)

Zde můžete zjistit aktuální/poslední umístění zařízení. Lokalizaci lze chránit jedním nebo dokonce dvěma hesly - viz: Přístup k GPS: - Obecná nastavení - Soukromí - Přístup k GPS



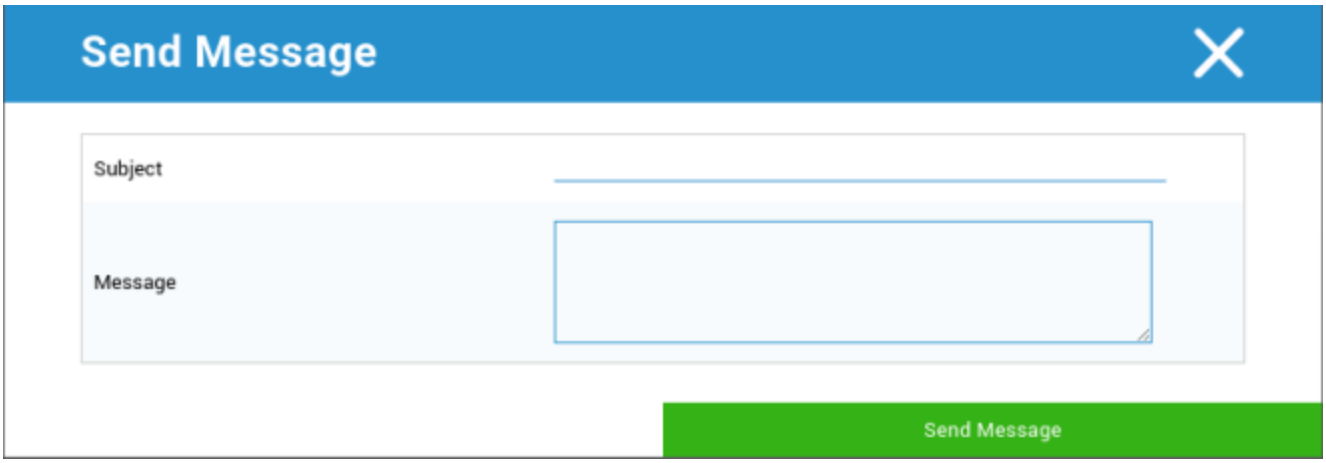
Vymazání a uzamčení (pouze na úrovni zařízení)

V části "Wipe & Lock" můžete provést následující tři akce:

Úplné otření	Zařízení je obnoveno do továrního nastavení (firemní i osobní údaje jsou smazány).
Podnikové utírání	Ze zařízení koncového uživatele jsou odstraněna pouze firemní data (všechny aplikace, data atd., které poskytla společnost AppTec360).
Zamykací obrazovka	Zámek obrazovky je aktivován, stačí zařízení odemknout pomocí hesla zařízení/PIN kódu.

Zpráva (pouze na úrovni zařízení)

Zde můžete vyplnit předmět a zprávu a odeslat ji na zařízení koncového uživatele.



Konfigurace zabezpečení

Přístupový kód zařízení

V části "Přístupový kód" můžete zadat heslo zařízení, k dispozici jsou následující možnosti nastavení.

Minimální délka hesla	stanovuje minimální počet symbolů, které musí heslo obsahovat.	
Kvalita hesla	Nespecifikováno	Tato zásada neobsahuje žádné požadavky na heslo.
	Biometrické Slabé	Tato politika umožňuje použití biometrické rozpoznávací technologie s nízkým stupněm zabezpečení. To znamená technologie, které dokáží rozpoznat identitu jednotlivce přibližně do třímístného PIN kódu (falešná detekce je menší než 1 z 1000).
	Něco	Tato zásada vyžaduje nastavení nějakého hesla nebo vzoru, ale nevynucuje žádná konkrétní pravidla.
	Abecední	Uživatel musí zadat heslo obsahující alespoň znaky abecedy (nebo jiný symbol).
	Alfanumerické	Uživatel musí zadat heslo, které obsahuje alespoň číselné a abecední (nebo jiné znaky).
	Komplexní	Uživatel musí zadat heslo, které standardně obsahuje alespoň písmeno, číslici a speciální symbol. Díky této kvalitě hesla lze omezit, aby hesla obsahovala různé sady znaků, například alespoň jedno velké písmeno atd.
Minimální délka hesla	Nastavte požadovaný počet znaků pro heslo. Můžete například požadovat, aby PIN nebo hesla měla alespoň šest znaků.	
Minimální počet číslic požadovaných v hesle	Minimální počet číslic požadovaných v hesle	
Minimální počet malých písmen v hesle	Minimální počet malých písmen v hesle	
Minimální počet velkých písmen v hesle	Minimální počet velkých písmen v hesle	
Minimální počet nepísmenných znaků požadovaných v hesle	Minimální počet nepísmenných znaků požadovaných v hesle	
Minimální požadované symboly v hesle	Minimální požadované symboly v hesle	

Zámek maximální doby nečinnosti	Maximální nečinnost uživatele do časového zámku
Časový limit vypršení platnosti hesla	stanoví, po uplynutí jakého časového intervalu heslo vyprší a musí být vydáno nové heslo.
Omezení historie hesel	Počet dříve použitých hesel, která nejsou povolena
Maximální počet neúspěšných pokusů o zadání hesla	Stanovuje, jak často může být heslo zadáno nesprávně, než dojde k úplnému vymazání zařízení.
Povolení biometrického ověřování	Umožňuje ověřování pomocí otisku prstu nebo skenu oční duhovky. Pouze pro Samsung KNOX 2.1 a vyšší.

AntiVirus

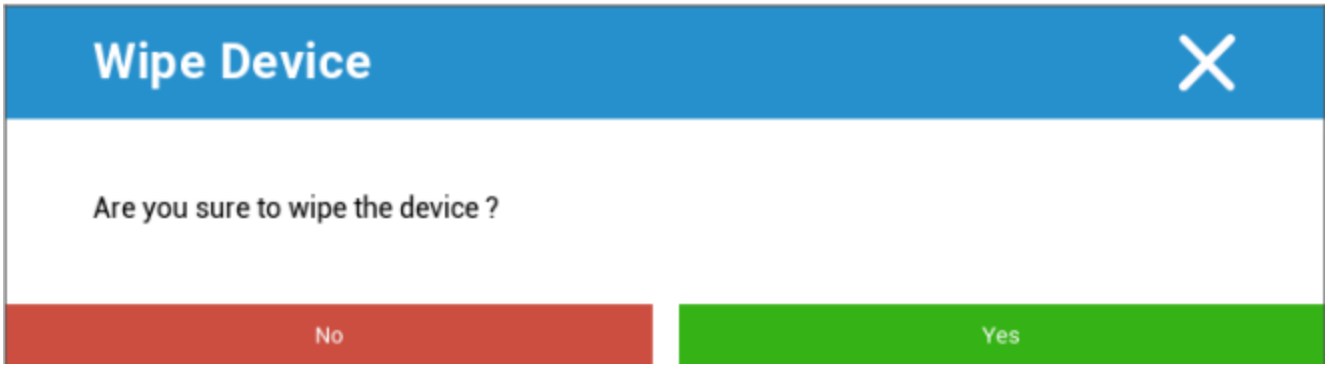
Automatické skenování	Povolení pravidelného automatického skenování
Interval skenování	Interval pro vyšetření (rychlé / úplné)
Plně automatické skenování	Povolení úplného automatického skenování
Automatické aktualizace	Povolení automatických aktualizací
Interval kontroly aktualizace	Jak často by měla být aplikace a její databáze aktualizována (viry / poškozený kód).
Ochrana aplikací	Povolení automatického skenování aplikací
Ochrana karty SD	Povolení automatického skenování karty SD
Aktualizace pouze pro Wi-Fi	Pokud je tato možnost povolena, aktualizace se použijí pouze v případě, že je zařízení úspěšně připojeno k síti Wi-Fi.

Konec životnosti (pouze na úrovni zařízení)

Vymazat (pouze na úrovni zařízení)

V části "Wipe" můžete obnovit tovární nastavení zařízení. Zde budou vymazána firemní i soukromá data v zařízení koncového uživatele.

Po kliknutí na symbol mínus se zobrazí následující zpráva:



Pokud zvolíte "Ano", můžete provést vymazání.

V části "Wipe Report" lze zobrazit následující položky.

Setřeno	Historie toho, kdo stírání provedl
Datum	Datum
Stav	Stav (např. zda bylo vymazání provedeno úspěšně)

Nastavení omezení

Omezení

Zde lze omezit a zablokovat celou řadu věcí.

Povolit kameru	Povolení použití kamery	
Vynutit automatickou synchronizaci	Na adrese	Synchronizace je trvale aktivována
	Vypnuto	Synchronizace je trvale deaktivována
	Volba uživatele	Vybrané uživatelem
Vynucení Bluetooth	Na adrese	Bluetooth je trvale aktivováno
	Vypnuto	Bluetooth je trvale deaktivováno
	Volba uživatele	Vybrané uživatelem
Force GPS	Na adrese	GPS je trvale aktivována
	Vypnuto	Systém GPS je trvale deaktivován
	Volba uživatele	Vybrané uživatelem
Umístění sítě Force	Na adrese	Trvalá lokalizace na internetu
	Vypnuto	Trvalá deaktivace lokalizace na internetu
	Volba uživatele	Vybrané uživatelem

Zabezpečení		
Zakázat sdílení umístění	Určuje, zda je uživateli zakázáno zapnout sdílení polohy.	
Zakázat nouzové spouštění	Určuje, zda uživatel nesmí restartovat zařízení do nouzového režimu spouštění.	
Zakázat resetování sítě	Určuje, zda je uživateli zakázáno resetovat nastavení sítě z Nastavení.	
Zakázat obnovení továrního nastavení	Určuje, zda je uživateli zakázáno resetovat zařízení.	
Povolení ADB	Umožňuje připojení k počítači přes ADB	
Zakázat funkci Keyguard	Zakáže funkci Keyguard	
Informace o uzamčené obrazovce vlastníka zařízení	Nastaví informace o vlastníkovi zařízení, které se mají zobrazovat na zamykací obrazovce.	
Prosazování shody	Režim Výzva Uživatel	Uživatel bude vyzván k provedení potřebných akcí.
	Kontejner pro uzamčení režimu	Skrýt všechny aplikace, dokud nejsou splněny všechny požadavky.

Správa aplikací	
Povolení propojení aplikací napříč profily	Umožňuje aplikacím v nadřazeném profilu zpracovávat webové odkazy ze spravovaného profilu.
Zakázat ovládání aplikací	Určuje, zda je uživateli zakázáno upravovat aplikace v Nastavení nebo spouštěčích.
Zakázat instalaci aplikací	Určuje, zda je uživateli zakázáno instalovat aplikace.
Zakázat odinstalování aplikací	Určuje, zda je uživateli zakázáno odinstalovávat aplikace.
Zásady oprávnění v době běhu	Určuje, jak budou zpracovávány nové požadavky na oprávnění od aplikací.
Povolit neznámé zdroje	Pokud je tato možnost povolena, mohou uživatelé načítat aplikace ze strany instalací souboru .apk.

Připojení	
Zakázat konfiguraci mobilní sítě	Určuje, zda je uživateli zakázáno konfigurovat mobilní sítě.
Zakázat konfiguraci tetheringu	Určuje, zda je uživateli zakázáno konfigurovat Tethering a přenosné hotspoty.
Zakázat konfiguraci VPN	Určuje, zda je uživateli zakázáno konfigurovat síť VPN.
Zakázat konfiguraci Wifi	Určuje, zda je uživateli zakázáno měnit přístupové body WiFi.
Zakázat odchozí paprsek NFC	Určuje, zda uživatel nesmí používat NFC k přenosu dat z aplikací.
Konfigurace uzamčení WiFi	Toto nastavení určuje, zda mají být konfigurace WiFi vytvořené aplikací Vlastník zařízení uzamčeny (tj. zda je může upravovat nebo odebírat pouze aplikace Vlastník zařízení, nikoli i aplikace Nastavení).
Povolení datového roamingu	Aktivace datového roamingu

Bluetooth	
Zakázat Bluetooth	Určuje, zda je v zařízení zakázáno připojení Bluetooth. Vyžaduje systém Android 8.0
Zakázat sdílení Bluetooth	Určuje, zda je v zařízení zakázáno odchozí sdílení Bluetooth. Vyžaduje systém Android 8.0
Zakázat konfiguraci Bluetooth	Určuje, zda je uživateli zakázáno konfigurovat bluetooth.

Správa účtů	
Zakázat přidání spravovaného profilu	Určuje, zda je uživateli zakázáno přidávat spravované profily. Vyžaduje Android 8.0
Zakázat přidávání uživatelů	Určuje, zda je uživateli zakázáno přidávat nové uživatele.
Zakázat odebrání spravovaného profilu	Určuje, zda lze spravované profily tohoto uživatele odstranit jinak než vlastníkem profilu. Vyžaduje Android 8.0
Zakázat změnu účtu	Určuje, zda je uživateli zakázáno přidávat a odebírat účty, pokud nejsou přidány programově nástrojem Authenticator.

Telefonování	
Zakázat odchozí hovory	Určuje, že uživatel nemá povoleno uskutečňovat odchozí telefonní hovory.
Zakázat SMS	Určuje, že uživatel nesmí odesílat ani přijímat zprávy SMS.

Systém	
Zakázat vytváření oken	Určuje, že kromě oken aplikace nemají být vytvářena jiná okna.
Zakázat nastavit ikonu uživatele	Určuje, zda uživatel nesmí měnit svou ikonu.
Zakázat nastavení tapety	Omezení uživatele, které zakáže nastavení tapety.
Zakázat stavový řádek	Vypnutím stavového řádku zablokujete oznámení, rychlá nastavení a další překryvy obrazovky, které umožňují útěk ze zařízení na jedno použití.
Povolení automatického času	Automaticky nastaví čas.
Povolení automatického časového pásma	Automaticky nastaví časové pásmo.
Zůstat zapnutý, když je připojen k síti	Zařízení zůstane aktivní, i když je připojeno ke zdroji napájení.

Úložiště	
Zakázat zakázat ověřování aplikací	Určuje, zda je uživateli zakázáno zakázat ověřování aplikací.
Zakázat připojení fyzických médií	Určuje, zda je uživateli zakázáno připojovat fyzická externí média.
Povolení služby zálohování	Služba zálohování spravuje všechny mechanismy zálohování a obnovení v zařízení. Nastavení této hodnoty na false zabrání zálohování nebo obnovení dat. Služba zálohování je ve výchozím nastavení vypnutá. Vyžaduje systém Android 8.0
Povolení velkokapacitního úložiště USB	Povoluje použití velkokapacitního úložiště USB.

Klávesnice	
Zakázat automatické vyplňování	Určuje, zda uživatel nesmí používat služby automatického vyplňování. Vyžaduje Android 8.0
Zakázat kopírování a vkládání mezi profily	Určuje, zda to, co je zkopírováno do schránky tohoto profilu, lze vložit do souvisejících profilů.

Zvuk	
Zakázat úpravu objemu	Určuje, zda je uživateli zakázáno upravovat hlavní hlasitost.
Zakázat vypnutí mikrofonu	Určuje, zda je uživateli zakázáno upravovat hlasitost mikrofonu.
Ztlumení zařízení	Ztlumení zařízení.

Správa certifikátů

Zde můžete distribuovat důvěryhodné certifikáty a certifikáty totožnosti do svých zařízení.

Pro distribuci důvěryhodných certifikátů je vyžadován systém Android 8 nebo vyšší a pro distribuci certifikátů identity je vyžadován systém Android 9 nebo vyšší.

Pomocí tlačítka "+" můžete přidat více certifikátů.

Důvěryhodné certifikáty musí být ve formátu PEM.

Certifikáty totožnosti musí být ve formátu PKCS12.

Správa připojení

Wifi

Pro toto nastavení proveďte předběžnou konfiguraci zařízení koncového uživatele pro přístup k interním přístupovým bodům

.

Identifikátor sady služeb (SSID)	SSID sítě, která má být připojena.
Skrytá síť	Aktivovat v případě, že přístupový bod nevysílá SSID.

Typ zabezpečení

Stanovení typu zabezpečení přístupového bodu

WEP

Heslo	Heslo pro přístupový bod

WPA/WPA2

Heslo	Heslo pro přístupový bod

802.1x EAP

Metoda EAP

PWD	Identita	Identita
	Heslo	Heslo

PEAP	Protokol ověřování fáze 2	žádné	Žádný další protokol
		MSCHAPV2	Protokol MSCHAPV2
		GTC	Protokol GTC
	Certifikát certifikační autority	Certifikát certifikační autority	
	Identita	Identita	
	Anonymní identita	Anonymní identita	
	Heslo	Heslo	

TTLS	Protokol ověřování fáze 2	žádné	Žádný další protokol
		PAP	Protokol PAP
		MSCHAP	Protokol MSCHAP
		MSCHAPV2	Protokol MSCHAPV2
		GTC	Protokol GTC
	Certifikát certifikační autority	Certifikát certifikační autority	
	Identita	Identita	
	Anonymní identita	Anonymní identita	
	Heslo	Heslo	

TLS	Certifikát certifikační autority	Certifikát certifikační autority
	Identita	Identita
	Heslo	Heslo

VPN

Název připojení	Název připojení VPN

Typ VPN

VPN

Klient VPN

Klient VPN AppTec360	
Konfigurace brány	Vyberte konfiguraci brány VPN (viz **Obecná nastavení > Univerzální brána > Nastavení VPN**).
Vždy zapnutá síť VPN	Povolení nativního uzamčení
Povolení uzamčení AppTec360	Povolení uzamčení AppTec360

Vestavěný (k dispozici pouze v zařízeních Samsung)			
Typ připojení	PPTP	Server	Server
		Povolení šifrování PPTP	Povolení šifrování PPTP
	L2TP / IPSec PSK	Server	Server
		Předsdílený klíč IPSec	Předsdílený klíč IPSec
		Povolení protokolu L2TP Secret	Povolení protokolu L2TP Secret
		Tajemství protokolu L2TP	Tajemství protokolu L2TP
	IPSec XAuth PSK	Server	Server
		Identifikátor IPSec	Identifikátor IPSec
		Předsdílený klíč IPSec	Předsdílený klíč IPSec
Vyhledávání domén DNS	Vyhledávání domén DNS		
Expertní nastavení	Servery DNS	Servery DNS	
	Trasy předávání	Trasy předávání	

Otevřená síť VPN		
Server	Server	
Profil OpenVPN	Profil OpenVPN	
Aplikace OpenVPN	OpenVPN pro Android (doporučeno)	
	Připojení k síti OpenVPN	
Expertní nastavení	Servery DNS	Servery DNS
	Trasy předávání	Trasy předávání

Samsung / Strong Swan			
Typ připojení	PPTP	Server	Server
		Uživatelské jméno	Uživatelské jméno
		Heslo	Heslo
		Povolení šifrování PPTP	Povolení šifrování PPTP
	L2TP / IPSec PSK	Server	Server
		Předsdílený klíč IPSec	Předsdílený klíč IPSec
		Uživatelské jméno	Uživatelské jméno
		Heslo	Heslo
		Povolení protokolu L2TP Secret	Tajemství protokolu L2TP
	IPSec XAuth PSK	Server	Server
		Identifikátor IPSec	Identifikátor IPSec
		Předsdílený klíč IPSec	Předsdílený klíč IPSec
		Uživatelské jméno	Uživatelské jméno
		Heslo	Heslo
Expertní nastavení	Servery DNS	Servery DNS	
	Trasy předávání	Trasy předávání	

Cisco Any Connect		
Server	Server	
Režim certifikátu	Bezbariérový	Bezbariérový
	Automatické	Automatické
Expertní nastavení	Servery DNS	Servery DNS
	Trasy předávání	Trasy předávání

VPN pro jednotlivé aplikace

Klient VPN

Klient VPN AppTec360		
Konfigurace brány	Vyberte konfiguraci brány VPN (viz **Obecná nastavení > Univerzální brána > Nastavení VPN**).	
Aplikace VPN	Aplikace VPN	
Vždy zapnutá síť VPN	Povolení nativního uzamčení	Vždy zapnutá síť VPN
Povolení uzamčení AppTec360	Povolení uzamčení AppTec360	

Samsung / Strong Swan			
Typ připojení	PPTP	Server	Server
		Aplikace VPN	Aplikace VPN
		Uživatelské jméno	Uživatelské jméno
		Heslo	Heslo
		Povolení šifrování PPTP	Povolení šifrování PPTP
	L2TP / IPSec PSK	Server	Server
		Aplikace VPN	Aplikace VPN
		Předsdílený klíč IPSec	Předsdílený klíč IPSec
		Uživatelské jméno	Uživatelské jméno
		Heslo	Heslo
		Povolení protokolu L2TP Secret	Tajemství protokolu L2TP
	IPSec XAuth PSK	Server	Server
		Aplikace VPN	Aplikace VPN
		Identifikátor IPSec	Identifikátor IPSec
		Předsdílený klíč IPSec	Předsdílený klíč IPSec
		Uživatelské jméno	Uživatelské jméno
		Heslo	Heslo
Expertní nastavení	Servery DNS	Servery DNS	
	Trasy předávání	Trasy předávání	

Omezení

Zde můžete nastavit omezení týkající se správy připojení.

Povolení datového roamingu	Povolení mobilních dat při roamingu
Vynucení datového roamingu	Pokud je aktivován, je roaming pro mobilní data trvale aktivován (nedoporučuje se!). Toto nastavení přepíše nastavení "Povolit datový roaming"!
Následující nastavení jsou k dispozici pouze v systému SAFE 2.x nebo vyšším.	
Povolit pouze tísňová volání	Povolit pouze tísňová volání
Povolit Wi-Fi	Povolit Wi-Fi
Minimální úroveň zabezpečení sítě WiFi	Minimální úroveň zabezpečení sítě WiFi Otevřený = všechny typy WiFi jsou povoleny
Zakázat uživateli přidávat sítě WiFi	Uživatel nesmí sám přidat síť WiFi Toto nastavení je možné pouze v případě, že byl profil WiFi definován v části "Správa připojení".
Povolení SMS a MMS	All = Veškerý provoz SMS a MMS je povolen. Pouze příchozí SMS = povoleny jsou pouze příchozí SMS zprávy. Pouze odchozí SMS = povoleny jsou pouze odchozí SMS zprávy. Žádný = není povolen žádný provoz SMS / MMS.
Povolit synchronizaci během roamingu	Povolit synchronizaci během roamingu Zapnuto = aktivováno Vypnuto = deaktivováno Volba uživatele = volba uživatele
Povolení hlasového roamingu	Povolení hlasového roamingu Zapnuto = aktivováno Vypnuto = deaktivováno Volba uživatele = volba uživatele
Použití systémového serveru http Proxy	Použití proxy serveru HTTP, který je k dispozici v nastavení systému, závisí na připojené síti (WiFi nebo APN).

Správa PIM

Výměna Gmail

Informace: Tato konfigurace se použije pro aplikaci Gmail. Musíte tedy schválit a nainstalovat aplikaci Gmail.

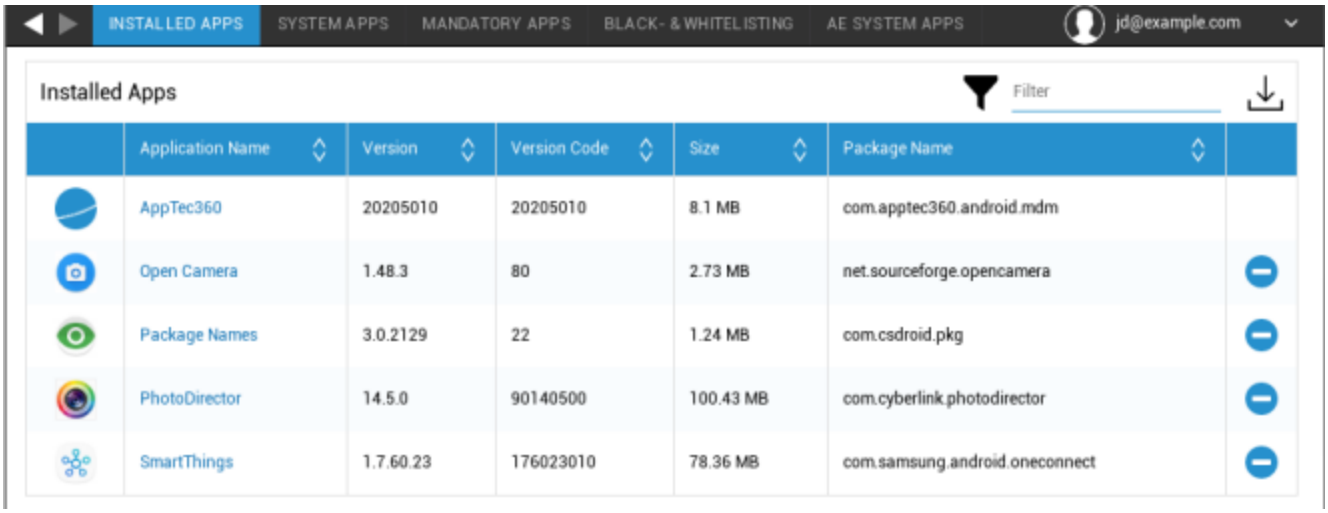
E-mailová adresa	Poskytnutá e-mailová adresa uživatele Všimněte si "zástupných symbolů", které můžete použít pro práci s pověřeními a neprovádíte změny ručně na každém zařízení. Jedním kliknutím si je můžete sami zobrazit.
Název hostitele serveru	Adresa serveru serverů Exchange
Přihlašovací jméno	Přihlašovací jméno pro příslušné zařízení koncového uživatele, všimněte si prosím také "Placeholders here".
Podpis	Lze připojit podpis (Tip: některá zařízení vyžadují formátování podpisu v HTML).
Počet předchozích dnů k synchronizaci	Počet dní, které určují, kdy se e-maily synchronizují zpět.
Identifikátor zařízení	Ein String der die EAS DeviceID enthält. Dies ist Teil des EAS Protokols und wird in einigen Umgebungen benötigt
Použití protokolu SSL (Secure Sockets Layer)	Použití připojení SSL
Přijmout všechny certifikáty	Přijímají se všechny certifikáty. Tuto možnost vyberte, pokud váš Exchange Server používá certifikát s vlastním podpisem.

Správa aplikací

Správce podnikových aplikací

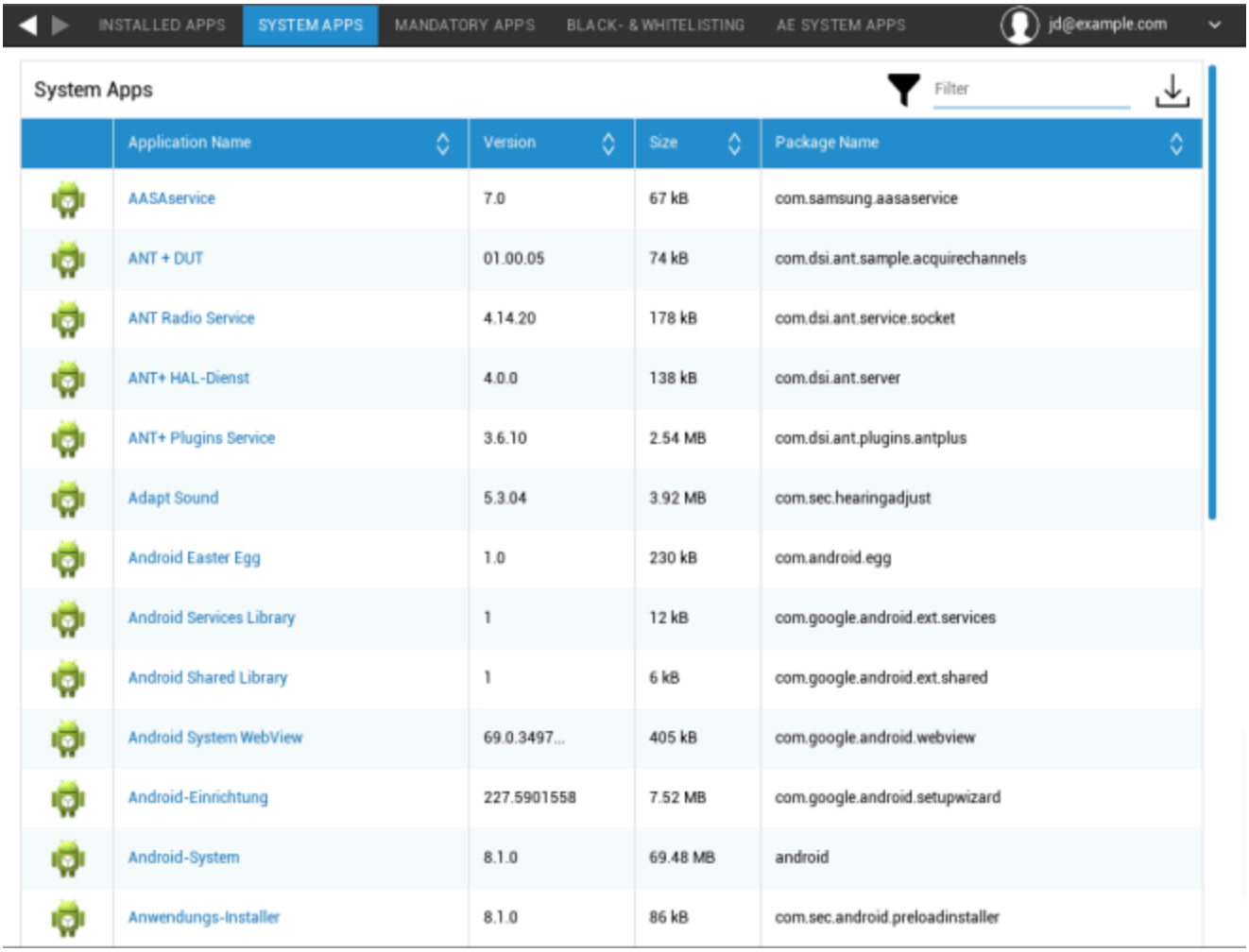
Nainstalované aplikace (pouze na úrovni zařízení)

Zde se zobrazí všechny aplikace, které jsou aktuálně nainstalovány v zařízení koncového uživatele.



Systémové aplikace (pouze na úrovni zařízení)

V části "Systémové aplikace" se zobrazí seznam všech aplikací a služeb, které již byly do koncového zařízení uživatele nainstalovány výrobcem zařízení.

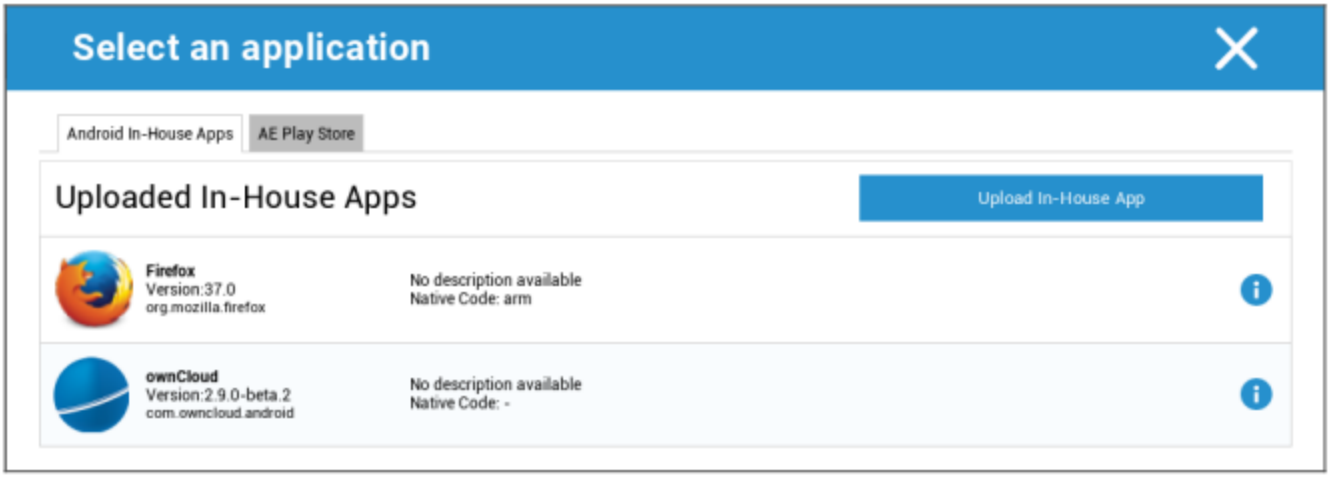


Povinné aplikace

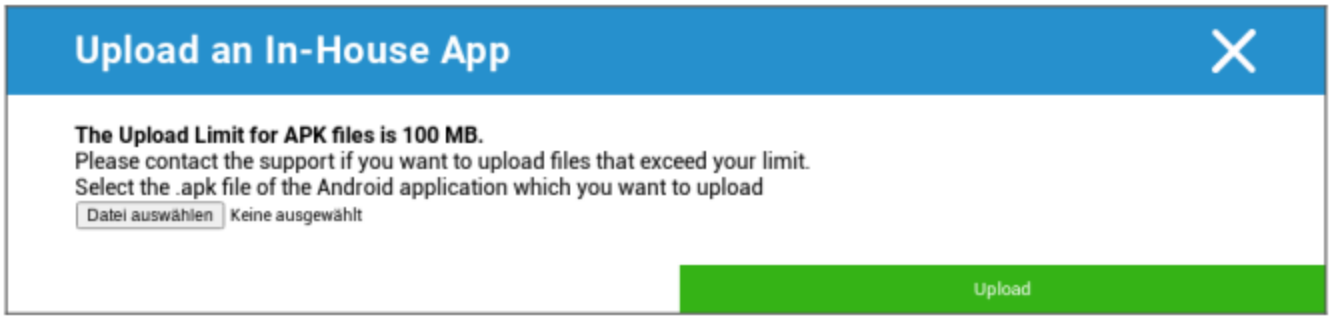
V části Povinné aplikace můžete nastavit povinné aplikace. Uživatel bude průběžně vyzýván k instalaci této určené aplikace.

Prostřednictvím , lze definovat povinnou požadovanou aplikaci.

Může se jednat o interní aplikaci z nabídky "Interní aplikace pro Android", kterou jste nahráli v obecných nastaveních.

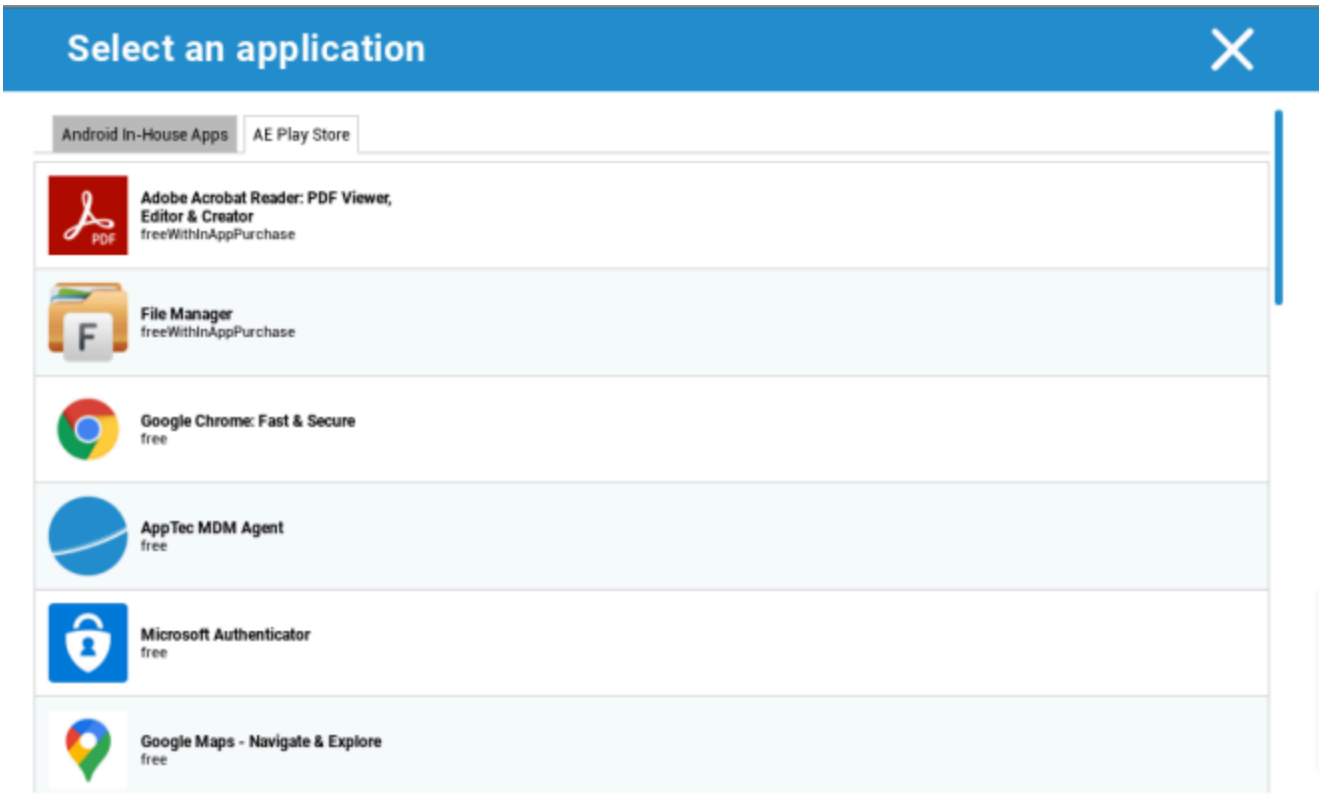


Soubor apk můžete také přímo vybrat a nahrát pomocí funkce "Upload In-House App".



Pokud instalujete aplikaci In-House, máte možnost aktivovat funkci "Keep up to date". Pokud je tato funkce aktivována a v databázi In-House App DB jste definovali novější verzi, aplikace se v zařízení aktualizuje.

Nebo to může být aplikace "AE Play Store" z pracovního obchodu Google Play.



Na této kartě se zobrazí pouze schválené aplikace "AE Play Store Apps".

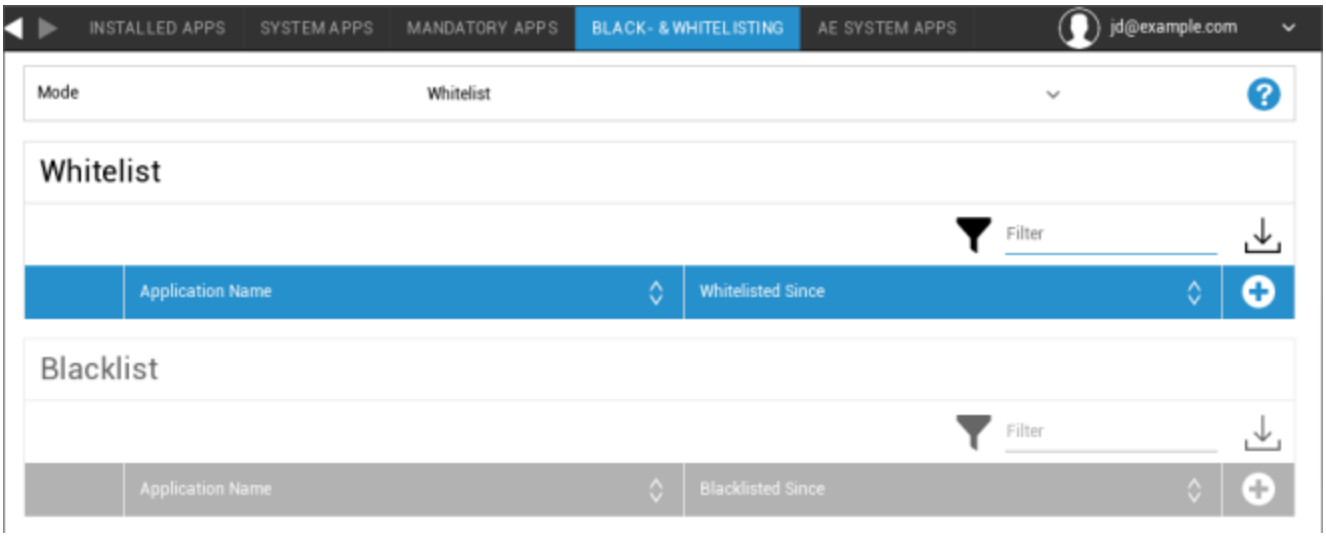
Chcete-li schválit aplikaci "AE Play Store", přejděte do "Obecná nastavení" > "Správa aplikací" > "AE Play".

Store" a přidejte aplikaci pomocí tlačítka, které vás přesměruje na kartu "Play Store Apps" (nebo můžete
přímo přejít na kartu "Play Store Apps").

Na kartě "Aplikace v Obchodě Play" můžete vyhledávat aplikace. Po kliknutí na aplikaci se otevře stránka aplikace
a zde můžete aplikaci schválit kliknutím na "Approve".

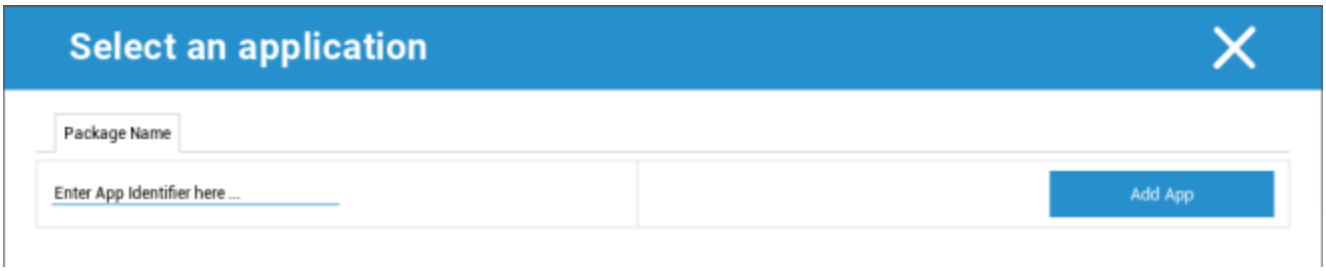
Černá a bílá listina

V části "Black- & Whitelisting" si můžete vybrat mezi režimem "Whitelist" a režimem "Blacklist".



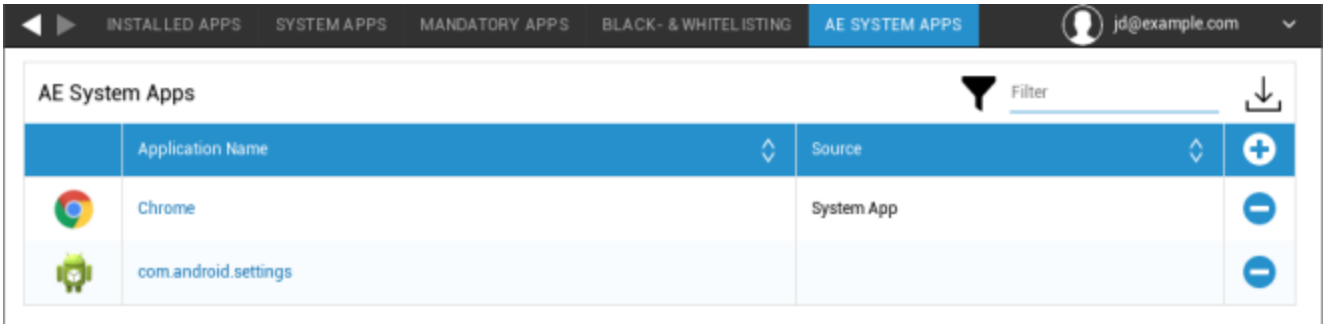
Bílá listina	Do zařízení koncového uživatele lze nainstalovat pouze aplikace a služby, které jsou přidány do seznamu. Pokud jsou již v zařízení koncového uživatele předinstalovány, budou aktivovány a nastaveny tak, aby je uživatel mohl spustit.
	Všechny ostatní aplikace, které nejsou přidány do seznamu, nelze do zařízení koncového uživatele nainstalovat. Pokud jsou již v zařízení koncového uživatele předinstalovány, budou deaktivovány a nastaveny tak, aby je uživatel nemohl spustit.
Černá listina	Aplikace a služby přidané do seznamu nelze nainstalovat do zařízení koncového uživatele. Pokud jsou v zařízení koncového uživatele již předinstalovány, budou deaktivovány a nastaveny tak, aby je uživatel nemohl spustit.
	Všechny ostatní aplikace, které nejsou přidány do seznamu, lze nainstalovat do zařízení koncového uživatele. Pokud jsou již v zařízení koncového uživatele předinstalovány, budou aktivovány a nastaveny tak, aby je uživatel mohl spustit.

Prostřednictvím , přidáváte další aplikace nebo služby do aktuálně používaného seznamu.
Prostřednictvím , přidáváte další aplikace nebo služby do aktuálně neaktivního seznamu.
Můžete definovat "Packagename":

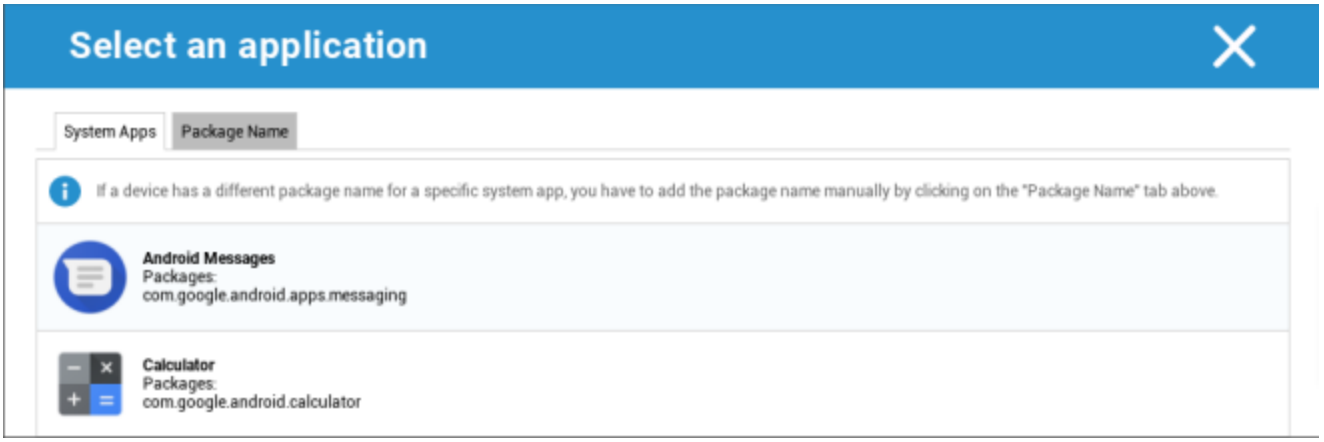

Select an application
Package Name
Enter App Identifier here ...
Add App

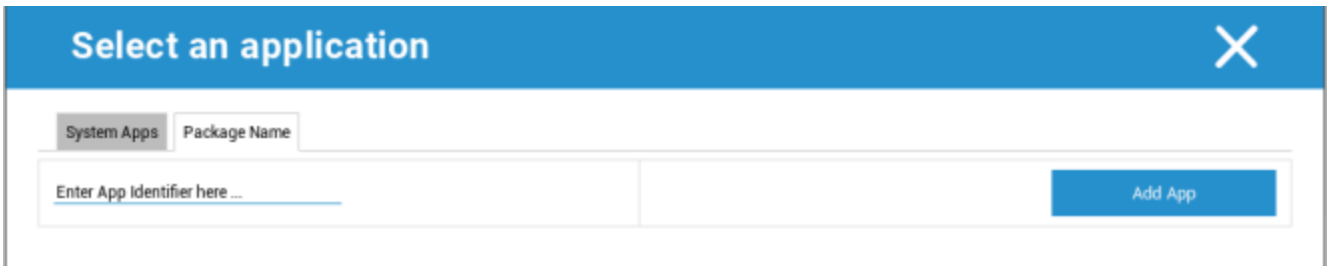
Systémové aplikace AE

Zde můžete definovat seznam obsahující konkrétní systémové aplikace, které mají být v zařízeních aktivovány.



Po kliknutí na tlačítko můžete vybrat ze seznamu možných systémových aplikací poskytnutých společností Google nebo přímo zadat název balíčku systémové aplikace, která má být aktivována.





Mějte na paměti, že systémové aplikace v seznamu poskytnutém společností Google jsou pouze aplikace, které mohou být systémovými aplikacemi, ale nemusí být nutně systémovými aplikacemi ve vašich zařízeních.

Tento seznam se však týká pouze již předinstalovaných aplikací.

Přidání aplikací, které nejsou v zařízeních předinstalovány, nebude mít na zařízení vliv bez ohledu na to, zda je aplikace ze seznamu poskytnutého společností Google, nebo je zadán přímo název balíčku

aplikace.

Omezení a nastavení

Nastavení správy aplikací

Zde můžete nastavit chování zařízení, pokud jde o aktualizace aplikací.

Frekvence kontroly aktualizací	Zadejte, v jakém intervalu bude klient AppTec360 vyhledávat aktualizace aplikací. Výchozí hodnota je 24 hodin.
Prahová hodnota Wi-Fi	Aplikace, které jsou větší než zadaná velikost, budou staženy přes Wi-Fi. Pokud je vybrána možnost "Pouze Wi-Fi", budou všechny aplikace stahovány přes Wi-Fi.

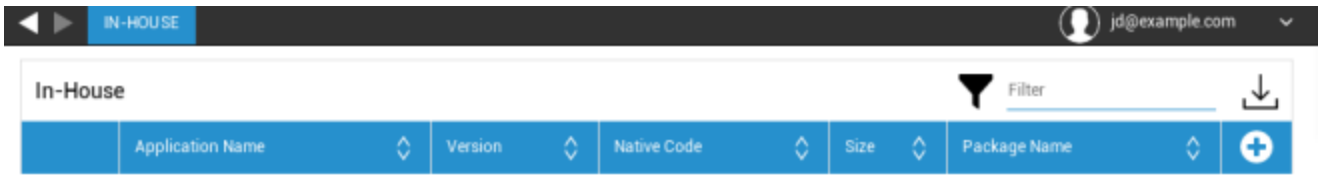
Obchod s podnikovými aplikacemi

In-House

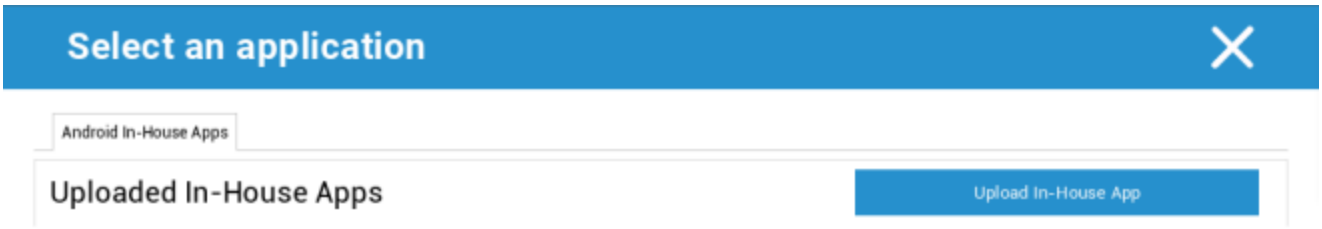
V bodě "In-House" můžete nahrávat a distribuovat interně vyvinuté aplikace.

Pomocí tohoto symbolu můžete distribuovat další aplikace In-House.

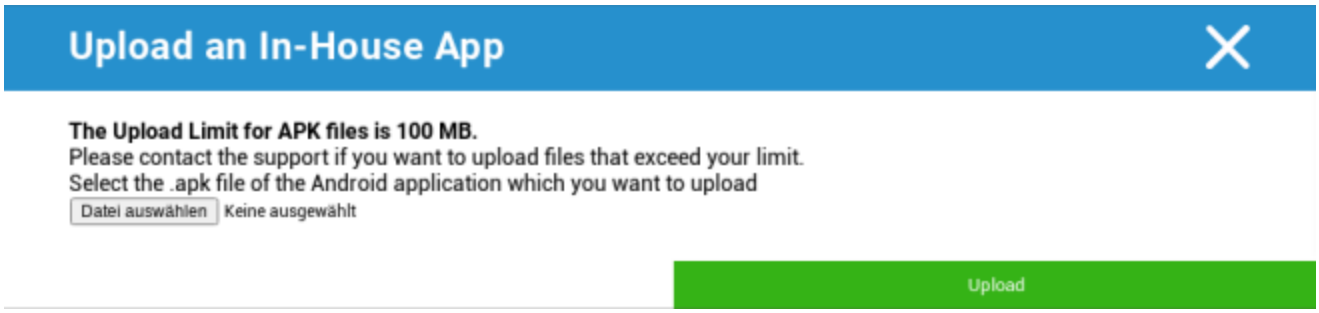
Pokud instalujete aplikaci In-House, máte možnost aktivovat funkci "Keep up to date". Pokud je tato funkce aktivována na adrese
a v databázi In-House App DB jste definovali novější verzi, bude aplikace v zařízení aktualizována na adrese
.



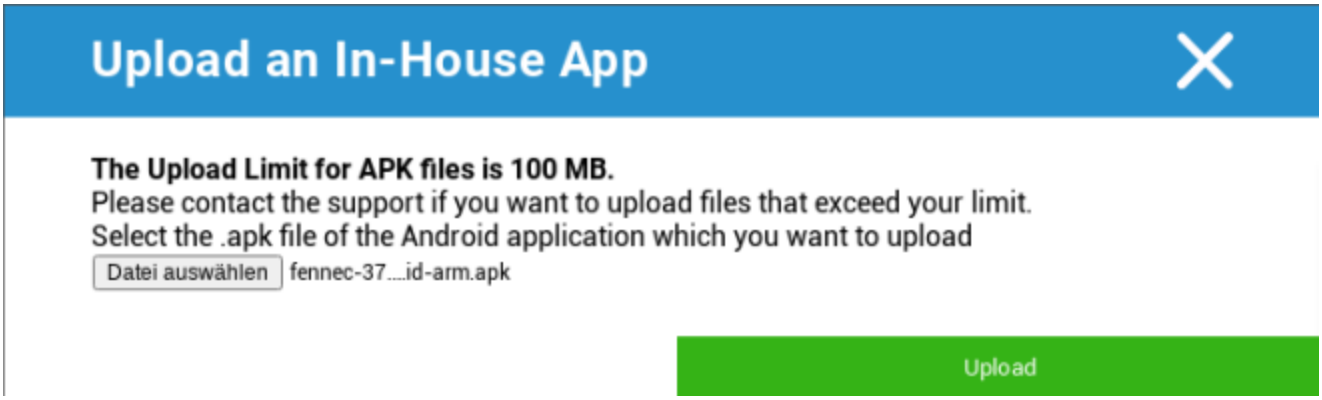
Pokud nemáte distribuované aplikace In-House Apps, obdržíte následující přehled:



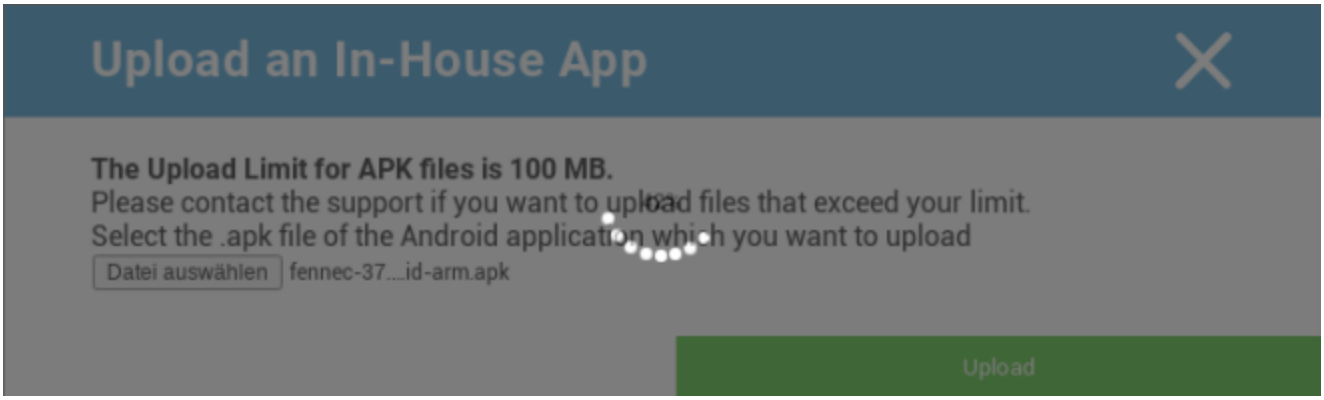
Za tímto účelem klikněte na "Nahrát interní aplikaci" a zobrazí se následující přehled:



Nyní vyberte pomocí "Search..." soubor .apk a klikněte na "Upload".



Vaše aplikace se nyní nahraje a uprostřed kruhu se zobrazí procentuální ukazatel , který ukazuje, jak velká část aplikace již byla nahrána.



Pokud bylo nahrání vaší interní aplikace úspěšné, najdete nahranou aplikaci na adrese
ve svém katalogu aplikací.

Uživatel má nyní možnost zobrazit a nainstalovat tuto aplikaci v obchodě AppTec360 na zařízení koncového uživatele
v kategorii "In-House".

Vzhledem k tomu, že se nejedná o aplikaci Google PlayStore, uživatel nepotřebuje mít v příslušném koncovém zařízení uložené Google
ID.

Obchod Play pro podniky

Obchod AE Play

Zde můžete přidávat aplikace do obchodu Android Enterprise Playstore. Vezměte prosím na vědomí, že před přidáním aplikací musíte schválit
Apps pomocí účtu správce AE.

Pokyny ke schválení aplikace naleznete v části Povinné aplikace.

Režim kiosku a spouštěč

Režim kiosku

Režim Kiosek umožňuje předem definovat aplikaci nebo adresu URL. Poté bude možné tuto aplikaci nebo adresu URL spustit nebo navštívit výhradně na adrese

.

Stejně tak lze různá hardwarová tlačítka deaktivovat v režimu Kiosk Mode.

Automatické spuštění	Automatické spuštění režimu Kiosk, jakmile profil dorazí do zařízení koncového uživatele.
Plánovaný režim kiosku?	Můžete naplánovat čas pro režim kiosku, který se pak automaticky spustí a ukončí ve vámi nastavený čas.
Čas zahájení	Čas zahájení
Čas v minutách	Doba v minutách, po které by měl být režim kiosku opět ukončen.

Typ aplikace

Jednotlivá aplikace	Pokud chcete aplikaci spustit v režimu kiosku, vyberte možnost "Package" v části "Application Type".
Aplikace kiosku	Klikněte sem a vyberte aplikaci, která má být spuštěna v režimu kiosku. Najdete zde obvyklý přehled správy aplikací. Můžete si vybrat mezi "Google Play Store", "Android In-House Apps" a "Packagename".

Typ aplikace

ADRESA URL	Chcete-li v režimu kiosku spustit adresu URL, vyberte v části "Typ aplikace" možnost "URL". Pak definujte požadovanou adresu URL
Vymazání prohlížeče po nečinnosti	Zde můžete definovat časový interval v minutách, po kterém se má režim kiosku znovu spustit.
Vymazání webové mezipaměti a souborů cookie	Pokud tuto funkci aktivujete, po restartu režimu Kiosek se vymaže webová mezipaměť (soubory cookie a obrázky v mezipaměti).
Zásady stejného původu	Pokud je tato funkce aktivní, může uživatel procházet pouze podstránky definované adresy URL. Například jste definovali následující adresu URL:www.mypage.com Uživatel pak může surfovat na adrese: www.mypage.com/subpage.
Adresy URL na bílé listině	Zde můžete udržovat bílou listinu, všechny tyto adresy URL jsou povoleny. Maximálně 1 adresa URL na řádek Adresa URL musí začínat http:/ nebo https://.
Adresy URL na černé listině	Zde můžete udržovat černou listinu, všechny tyto adresy URL nejsou povoleny. Maximálně 1 adresa URL na řádek Adresa URL musí začínat http:/ nebo https://.
Orientace obrazovky	Toto nastavení se týká úprav obrazovky Automatic = automatický Portrét = vertikální formát Krajina = režim na šířku

Aplikace Multi App	Pokud vyberete režim kiosku "Multi App", bude vynuceno použití spouštěče AppTec360.
Aplikace	Použití: Jako aplikaci pro kiosek vyberte aplikaci z obchodu Playstore nebo vlastní aplikaci. Je také možné zadat název balíčku. Vybraná Kiosková aplikace musí být v zařízení nainstalována. Nezapomeňte nastavit Kioskovou aplikaci jako povinnou. Zkratka na domovské obrazovce: Pokud je nastaveno na "Zapnuto", vytvoří se zástupce na domovské obrazovce. Pokud je nastaveno na "Vypnuto", aplikace se bude stále zobrazovat v seznamu aplikací.

Heslo pro ukončení povoleno	Pokud tuto funkci aktivujete, je možné, aby uživatel ukončil režim kiosku pomocí vámi předem definovaného hesla.
Heslo pro ukončení	Toto je heslo, které jste předem definovali.
Automatické sbalení stavového řádku	Pokud je tato možnost povolena, stavový řádek se automaticky podbarví. S touto možností mohou uživatelé vidět informace na stavovém řádku, ale nemají přístup k jeho funkcím.
Zakázat stavový řádek	Stavový řádek obsahuje Oznámení, Zkratky a Informace. K dispozici pouze pro zařízení Samsung s verzí SAFE 4.0 nebo vyšší.
Zakázat klávesy hlasitosti	Zakázat tlačítka hlasitosti (dostupné pouze v zařízeních Samsung s verzí SAFE 3.0 nebo vyšší)
Vypnutí vypínače	Vypnutí přepínače zapnuto/vypnuto (k dispozici pouze u zařízení Samsung s verzí SAFE 3.0 nebo vyšší)
Zakázat tlačítko Domů	Zakázat tlačítko Domů. Pokud je tato funkce aktivována, lze režim kiosku ukončit pouze v konzoli AppTec360. (k dispozici pouze v zařízeních Samsung s verzí SAFE 3.0 nebo vyšší)
Zakázat navigační panel	Pomocí této funkce můžete vypnout navigační panel (Zpět / Menu). Pokud je tato funkce aktivována, lze režim kiosku ukončit pouze v konzoli AppTec360. (k dispozici pouze v zařízeních Samsung s verzí SAFE 3.0 nebo vyšší)

Spouštěč AppTec360

Povolení spouštěče AppTec360	Na: AppTec360 Launcher se zapne. Uživatel jej musí jednorázově nastavit jako výchozí spouštěč. Poznámka: Pokud je povolen režim kiosku a režim kiosku je nastaven na "Multi App", bude vynuceno použití spouštěče AppTec360.
Velké ikony	Na: Zobrazí větší verzi ikon aplikací v Launcheru.
Skrýt ikonu aplikace AppTec360	Na: Zcela skryje aplikaci AppTec360
Skrytí ikony obchodu AppTec360	Na: Úplně skryje AppTec360 Enterprise AppStore.

Nastavení AppTec360

Povolení aplikace AppTec360 Settings	Aplikace AppTec360 Settings umožňuje ovládat připojení WiFi a Bluetooth.
Povolení nastavení v aplikaci Multi App Režim kiosku	Pokud je tato možnost povolena, mohou uživatelé přistupovat k aplikaci AppTec360 Settings, když je aktivní režim Multi App Kiosk Mode.

Dálkové ovládání

Splashtop

Chcete-li spustit relaci vzdáleného ovládání zařízení, je třeba do zařízení nainstalovat aplikaci "Splashtop Streamer" přidáním aplikace do **Správa aplikací** → **Správce podnikových aplikací** → **Povinné aplikace**.

Poté nakonfigurujte následující nastavení pro Splashtop:

Povolení funkce Splashtop	Pokud je tato možnost povolena, AppTec360 nakonfiguruje aplikaci Splashtop tak, aby umožňovala vzdálené ovládání.
Nasazení kódu	Přejděte na stránku https://my.splashtop.com a přihlaste se ke svému účtu Splashtop. Klikněte na "Add Computer" a zkopírujte 12místný kód nasazení z výsledné stránky.
Nastavení vlastní brány nasazení?	Nasazení brány
Nasazení domény brány / hostitele	Nasazení brány
Ověření certifikátu	Ověření certifikátu

Poté můžete pomocí možnosti Splashtop Remote Control v kontextové nabídce (ozubené kolečko vedle vyhledávacího řádku, když je zařízení vybráno, nebo kliknutím pravým tlačítkem myši na zařízení ve stromu) spustit relaci vzdáleného ovládání.

TeamViewer

Abyste mohli spustit relaci vzdáleného ovládání zařízení, je třeba do zařízení nainstalovat aplikaci "TeamViewer QuickSupport" přidáním aplikace do **Správa aplikací** → **Správce podnikových aplikací** → **Povinné aplikace**.

Poté můžete pomocí možnosti **TeamViewer Remote Control** v kontextové nabídce (ozubené kolečko vedle vyhledávacího řádku, když je zařízení vybráno, nebo kliknutí pravým tlačítkem myši na zařízení ve stromu) spustit relaci vzdáleného ovládání.

Správa obsahu

ContentBox

Zde můžete aktivovat pole ContentBox.

Jakmile přepnete možnost "Povolit ContentBox" na "Zapnuto", do zařízení koncového uživatele se automaticky nainstaluje samostatná aplikace ContentBox

.

Zabezpečený prohlížeč

Zde můžete nakonfigurovat nastavení pro AppTec360 Secure Browser.

Jakmile přepnete sekci "Zabezpečený prohlížeč" do polohy "Zapnuto", do zařízení koncového uživatele se automaticky nainstaluje samostatná aplikace prohlížeče
.

Vyžadovat heslo	Požadovat, aby si uživatel nastavil a používal heslo pro přístup k prohlížeči.
Minimální požadovaná délka hesla	Nastavení požadovaného počtu znaků pro heslo
Požadovaná kvalita hesla	Nastavení požadované kvality hesla
Omezit stahování / Otevřít v	
Omezení nahrávání	
Nahrání bílé listiny	Seznam adres URL, pro které bude vždy povoleno nahrávání.
Povolit kopírování	Povolení kopírování, vyřezávání nebo sdílení textu uvnitř webových stránek.
Povolit snímání obrazovky	Umožňuje pořizování snímků obrazovky.
Frekvence čištění dat	Zvolte, s jakou frekvencí se mají automaticky odstraňovat VŠECHNA uživatelská data (historie, mezipaměť atd.).
Záložky společnosti	Záložky se zobrazí ve složce "Firemní záložky" v záložkách prohlížeče. Uživatel je nemůže upravovat.
Skrytí adresního řádku	
Whitelisting v prohlížeči (bez univerzální brány)	Povoluje whitelisting adres URL na straně klienta. • Firemní záložky jsou vždy na bílé listině • Podporováno pouze pro 100 adres URL • Pro neomezený black- a whitelisting používejte univerzální bránu.
Adresy URL na bílé listině	Seznam povolených adres URL.
Černá a bílá listina založená na bráně	Černá listina má následující požadavky:

	• Fungující univerzální brána AppTec360 ("Obecná nastavení" → "Univerzální brána"). • Fungující konfigurace VPN se zadaným serverem DNS ("Obecná nastavení" → "Univerzální brána" → "Nastavení VPN"). • Konfigurace černé listiny ("Obecná nastavení" → "Univerzální brána" → "Černá listina domén") • Platné připojení VPN v profilu ("Správa připojení" → "VPN").

Další rozhraní API

Samsung KNOX

Omezení

Povolení karty SD	
Povolit zápis na kartu SD	
Povolit snímání obrazovky	
Povolit schránku	
Zálohování nastavení a dat aplikací ve službě Google Cloud	
Obnovení nastavení z Google Cloud při přeinstalování aplikace	
Povolení ladění USB	
Povolit Google Crash Report	
Povolit obnovení továrního nastavení	
Povolení aktualizace OTA	
Povolení hostitelského úložiště USB	Pokud je tato funkce povolena, může uživatel připojit libovolnou jednotku typu pen (přenosné úložiště USB), externí pevný disk nebo čtečku karet Secure Digital (SD), která se v zařízení připojí jako úložná jednotka.
Povolení přehrávače médií USB (MTP,PTP)	
Povolit mikrofon	Zakázání mikrofonu pro aplikace třetích stran
Povolení NFC (Near Field Communication)	
Povolit neznámé zdroje (APK Sideloading)	Pokud je povoleno, je povoleno boční načítání aplikací (souborů APK). Jakmile je toto nastavení zakázáno, musí jej uživatel povolit ručně, když znovu povolíte instalaci souborů APK z neznámých zdrojů.

Povolit vytváření uživatelů	Pokud je tato možnost povolena, může uživatel v zařízení vytvořit více účtů, např. účty pro hosty.

E-mail

E-mailová adresa	
Protokol příchozího serveru	
Adresa příchozího serveru	
Příchozí port serveru	
Přihlašovací jméno/uživatelské jméno příchozího serveru	
Heslo příchozího serveru	
Příchozí server používá protokol SSL	
Příchozí server používá TLS	
Příchozí server přijímá všechny certifikáty	
Protokol odchozího serveru	
Adresa odchozího serveru	
Port odchozího serveru	
Odchozí server používá další pověření	Pokud je zakázáno, systém použije příchozí pověření i pro odchozí server.
Přihlašovací jméno/uživatelské jméno odchozího serveru	
Heslo odchozího serveru	
Odchozí server používá protokol SSL	
Odchozí server používá TLS	
Odchozí server přijímá všechny certifikáty	
Nastavit podpis	
Podpis	Poznámka: U některých zařízení musí být podpis zadán ve formátu HTML.
Upozornit uživatele na přijetí nového e-mailu	

Výměna

E-mailová adresa	
Název hostitele serveru	Název hostitele serveru Exchange
Přihlašovací jméno	Uživatelské jméno, které se používá k přihlášení k serveru Exchange Server.
Doména	Pokud je povolena konfigurace brány ACL a pole Doména není prázdné, bude univerzální brána AppTec360 ověřovat zařízení pod následujícím názvem "Doména\Přihlašovací jméno".
Heslo	
Počet předchozích dnů k synchronizaci	
Frekvence synchronizace elektronické pošty	
Synchronizace při roamingu	
Nastavit podpis	
Podpis	Poznámka: U některých zařízení musí být podpis zadán ve formátu HTML.
Výchozí účet	
Použití protokolu SSL (Secure Sockets Layer)	
Použití protokolu TLS (Transport Layer Security)	
Přijmout všechny certifikáty	

APN

Zobrazovaný název APN	
Název přístupového bodu	Název APN
Protokol odchozího serveru	
MCC - Kód země mobilního telefonu	Ponechte prázdné, chcete-li použít mmc nainstalované SIM karty
MNC - Kód mobilní sítě	Ponechte prázdné, chcete-li použít mnc nainstalované SIM karty
Adresa serveru	
Číslo portu serveru	
Adresa proxy serveru	
Adresa serveru MMS	Pro výchozí nastavení ponechte prázdné
Číslo portu MMS	Pro výchozí nastavení ponechte prázdné
Adresa proxy serveru MMS	Pro výchozí nastavení ponechte prázdné
Uživatelské jméno	
Heslo	
Typ přístupového bodu	Akceptované typy jsou "default", "mms", "supl".
	Pokud je předána hodnota null nebo prázdná, použije se ve výchozím nastavení hodnota "default,supl,mms".
	Pro výchozí nastavení ponechte prázdné.
Preferované APN	

Bluetooth

Povolit zjišťování zařízení přes Bluetooth	
Povolení párování Bluetooth	
Povolení zařízení Bluetooth Headset	
Povolení zařízení Bluetooth Hands-free	
Povolení zařízení Bluetooth A2DP	A2DP, Advanced Audio Distribution Profile, umožňuje streamování zvuku mezi zařízeními.
Povolení odchozích hovorů	
Povolení přenosu dat přes Bluetooth	
Povolení tetheringu Bluetooth	
Povolení připojení k počítači přes Bluetooth	

Připojení

Povolit pouze tísňová voláníPovolit Wi-Fi	
Minimální úroveň zabezpečení sítě Wi-Fi	
Zakázat uživateli přidávat sítě Wi-Fi	Toto omezení lze aktivovat pouze v případě, že je v části Správa připojení definován alespoň jeden aktivní profil Wi-Fi.
Povolení SMS a MMS	
Povolit synchronizaci během roamingu	
Povolení hlasového roamingu	

Android Enterprise – Plně spravované zařízení s pracovním profilem (COPE)

Obecné vysvětlení COPE

COPE je zkratka pro **Corporate Owned Personally Enabled**, tedy " **osobně vlastněná**společnost".

Režim COPE umožňuje zapsat zařízení se systémem Android jako **zařízení Android Enterprise - plně spravované zařízení s** integrovaným profilem **Android Enterprise - kontejner**.

Může se jednat buď o zařízení se systémem Android, které je již zaregistrováno jako **zařízení Android Enterprise - plně spravované zařízení** a na kterém je navíc nastaven **kontejner Android Enterprise - Container**, nebo o nově zaregistrované zařízení se systémem Android, které je přímo zaregistrováno jako **zařízení Android Enterprise - plně spravované zařízení** spolu s **kontejnerem Android Enterprise - Container** na něm.

Režim COPE je k dispozici pouze pro zařízení se systémem Android 8, 9 a 10.

Konfigurace profilů pro zařízení COPE

Protože pro samotný režim COPE neexistuje žádný konfigurační profil, je konfigurace **systému Android Enterprise - plně spravované zařízení** a **systému Android Enterprise - kontejner** rozdělena do dvou profilů v rámci profilu COPE. Mezi těmito dvěma profily je možné přepínat konfiguraci každého z nich kliknutím na příslušné tlačítko na levé straně konzoly:

Oba profily lze nakonfigurovat podle popisu pro jednotlivé profily:

Android Enterprise - Plně spravované zařízení

Android Enterprise - Kontejner

Návrat k plně spravovanému zařízení AE

Profil **Android Enterprise - Container** lze odebrat podle popisu v části **Správa mobilních zařízení**.

Odstraněním profilu Container se profil COPE změní na profil **Android Enterprise - plně spravované zařízení**.

Android Enterprise – Konfigurace kontejneru

V závislosti na tom, zda jste aktuálně vybrali profil skupiny nebo zařízení, se přehled a jeho dílčí body liší - věnujte tomu prosím pozornost!

Obecné

Přehled profilů (pouze na úrovni profilu)

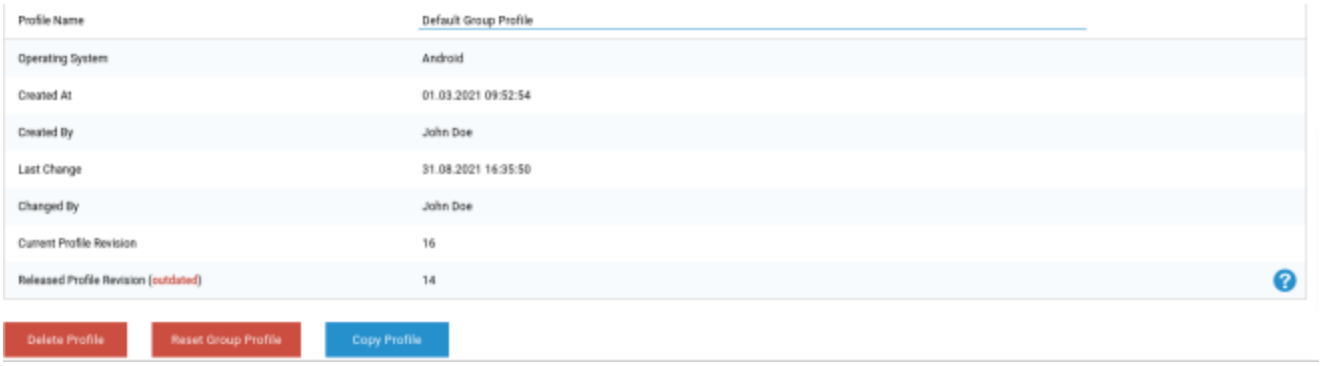
Pokud se nacházíte v profilu, zobrazí se vám stručný přehled profilu, pokud jde o název, operační systém, datum vytvoření, autora atd.

Název profilu	Název profilu - zde lze přímo přejmenovat
Operační systém	Platný operační systém pro profil
Vytvořeno v	Datum vytvoření
Vytvořil	Vytvořil
Poslední změna	Datum poslední změny
Změněno podle	Uživatel, který provedl poslední změny v tomto profilu.
Aktuální revize profilu	Počet aktualizací profilu
Vydaná revize profilu	Počet případů, kdy byl profil již aktualizován a byla mu přiřazena zařízení.

Smazat profil	Smazat profil
Obnovení profilu skupiny	Obnovení profilu skupiny
Kopírovat profil	Kopírovat profil

Přehled profilu skupiny (pouze na úrovni skupiny)

Po otevření profilu skupiny se zobrazí rychlý přehled profilu.



Název profilu	Název profilu (zde lze změnit)
Operační systém	Operační systém, pro který je profil určen
Vytvořeno v	Čas vytvoření
Vytvořil	Tvůrce profilu
Poslední změna	Čas poslední změny profilu
Změněno podle	Účet, který provedl poslední změny
Aktuální revize profilu	Revize uloženého stavu profilu
Vydaná revize profilu	Přiřazená revize profilu ("Assign now"). Pokud se za textem na štítku zobrazí " (zastaralý)", znamená to, že jste profil uložili, ale ještě jste ho nepřiřadili, takže zařízení budou stále dostávat starší verzi.

Přehled zařízení (pouze na úrovni zařízení)

Pokud se nacházíte na zařízení, zobrazí se přehledová rekapitulace vybraného zařízení, která obsahuje následující informace:

Název zařízení	Název zařízení
Umístění	Souřadnice polohy
Telefonní číslo	Telefonní číslo
Přiřazené povinné aplikace	Počet přidělených povinných aplikací
Verze operačního systému	Verze operačního systému zařízení
Operační systém	Operační systém (Android Enterprise)
Sériové číslo	Sériové číslo zařízení
Vlastnictví zařízení	Firemní nebo soukromé zařízení
Typ zařízení	Spravované zařízení AE Work
Zakořeněný	Stav, který udává, zda bylo zařízení rootnuto.
V souladu s předpisy	V souladu s pokyny
IP adresa	IP adresa zařízení
Naposledy viděno	Časový okamžik, kdy se zařízení naposledy připojilo k AppTec.
Poslední impuls	Časový okamžik, kdy byl do zařízení odeslán poslední push.
Přiřazení uživatele	Uživatel nebo skupina, ke které je toto zařízení přiřazeno

Revize konfigurace

Zde získáte přehled o tom, který skupinový profil je k zařízení přiřazen.

Pokud kliknete na profil skupiny, získáte přímý přístup k tomuto profilu a můžete provádět nastavení.

Pomocí tohoto symbolu můžete vrátit distribuované aplikace do nastavení profilu skupiny.

Pomocí tohoto symbolu můžete vrátit všechny používané aplikace do nastavení skupinového profilu.

"K dispozici je novější revize" znamená, že profil skupiny byl změněn a uložen, ale nebyl přiřazen. Profil skupiny je třeba přiřadit pomocí "Přiřadit nyní" na úrovni skupiny, aby se změny uplatnily na

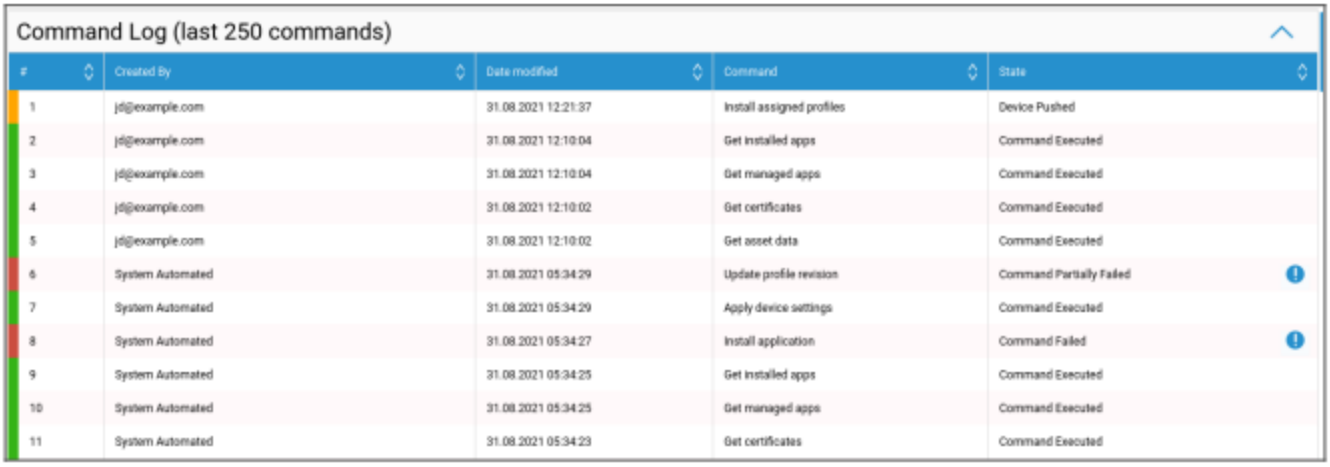
zařízení.

Protokol zařízení (pouze na úrovni zařízení)

Zde se zobrazí různé protokoly zařízení. V případě potřeby zde můžete přímo zjistit příčinu chyby.

Protokol příkazů

Zde můžete zjistit, které příkazy byly pro zařízení vydány a jaký je jejich stav.


Command Log (last 250 commands)

#	Created By	Date modified	Command	State
1	jd@example.com	31.08.2021 12:21:37	Install assigned profiles	Device Pushed
2	jd@example.com	31.08.2021 12:10:04	Get installed apps	Command Executed
3	jd@example.com	31.08.2021 12:10:04	Get managed apps	Command Executed
4	jd@example.com	31.08.2021 12:10:02	Get certificates	Command Executed
5	jd@example.com	31.08.2021 12:10:02	Get asset data	Command Executed
6	System Automated	31.08.2021 05:34:29	Update profile revision	Command Partially Failed
7	System Automated	31.08.2021 05:34:29	Apply device settings	Command Executed
8	System Automated	31.08.2021 05:34:27	Install application	Command Failed
9	System Automated	31.08.2021 05:34:25	Get installed apps	Command Executed
10	System Automated	31.08.2021 05:34:25	Get managed apps	Command Executed
11	System Automated	31.08.2021 05:34:23	Get certificates	Command Executed

Možné stavy příkazů

Stlačené zařízení	Službě push (např. APNS) byl odeslán požadavek na připojení, aby se zařízení připojilo zpět k serveru EMM.
Vytvořený příkaz	Příkaz byl vytvořen v systému.
Odeslaný příkaz	Příkaz byl odeslán do zařízení po jeho připojení k serveru.
Spuštěný příkaz	Příkaz byl úspěšně proveden.
Příkaz se nezdařil	Příkaz se nezdařil. *
Příkaz částečně selhal	V závislosti na operačním systému zařízení mohou být některé příkazy seskupeny. V tomto některé části této skupiny příkazů selhaly. *
Příkaz proveden, případně neúspěšný	Příkaz byl proveden, ale možná nebyl.
Přesunutí příkazu	Příkaz byl znovu odeslán uživatelem.
Vyřazené	Příkaz byl vyřazen. Například proto, že byl nahrazen jiným příkazem nebo že zařízení bylo znovu zapsáno a staré příkazy byly odstraněny.

*Pokud je za zprávou vykřičník, můžete získat další informace, když na ikonu najedete kurzorem.

Nastavení zařízení

Konfigurace klienta

Zde můžete provést následující konfigurace zařízení se systémem Android:

Čas mimo soulad	Časový limit odezvy uživatele, po jehož uplynutí se použije akce vynucení.
Donucovací opatření po uplynutí lhůty pro splnění požadavků	vynucovací akce, pokud uživatel neprovede akce, které vedou ke stavu zařízení, které je v souladu s předpisy.
Frekvence sběru dat	Četnost shromažďování informací o zařízení/GPS
Frekvence srdečního tepu zařízení	Interval, ve kterém má zařízení kontaktovat AppTec Server Min. 1 minuta Max. 24 hodin
Povolení aktualizací polohy	Pokud je aktivováno, zařízení odesílá aktualizace polohy na server AppTec Server.
Čas aktualizace umístění	Určuje, v jakých časových intervalech zařízení odesílá aktualizace polohy do systému AppTec.
Použití služby Google Location Accuracy pro aktualizaci polohy	Pokud je aktivováno, bude se pro aktualizace polohy používat poloha v síti (pokud bylo toto nastavení deaktivováno v části "Omezení", pak toto nastavení nic neovlivní).
Použití polohy GPS pro aktualizaci polohy	Pokud je aktivována, bude se pro aktualizaci polohy používat GPS.
Povolení falešných umístění	Umožňuje falšování informací o poloze prostřednictvím aplikací třetích stran.
Akce při ztrátě spojení	Pokud je tato možnost povolena, můžete zadat akci pro případ, že zařízení nezíská připojení k serveru MDM v intervalu heartbeat. Například pokud má zařízení interval srdečního rytmu 5 minut, připojí se k serveru v 10:35. Poté zařízení opustí dosah sítě Wi-Fi. Další srdeční tep v 10:40 se nezdaří a provede se zadaná akce.
Akce	Opatření, která je třeba přijmout, jakmile se zařízení stane nevyhovujícím. • Lock Zařízení = zámek zařízení • Vymazat zařízení = zařízení bude obnoveno do továrního nastavení. • Vymazání zařízení a karty SD = zařízení bude obnoveno do továrního nastavení a úložiště karty SD bude vymazáno.

Prahová hodnota	Můžete zadat prahovou hodnotu neúspěšných srdečních tepů, která je nutná pro spuštění zadané akce.

Režim vynucování zásad	Výchozí nastavení:	Uživatelé budou pravidelně vyzýváni k provedení zbývajících akcí.
	Líné vynucování zásad:	Uživatelé nebudou nikdy vyzváni k provedení zbývajících akcí. Všechny otevřené akce se zobrazí v aplikaci AppTec Client.
	Agresivní prosazování zásad:	Uživatelé budou nepřetržitě vyzýváni k provedení zbývajících akcí.
Zámek verze AppTec	Pokud je tato možnost povolena, lze zadat kód verze aplikace AppTec. Klient AppTec bude aktualizovat pouze na zadanou verzi. Novější verze budou ignorovány. Aktualizace na nižší verzi NENÍ možná.	
Kód verze	Kód verze aplikace AppTec, která má být uzamčena.	
Zakázat oznámení AppTec	Pokud je zakázáno, nezobrazí se oznámení v oznamovacím panelu klienta AppTec. Uživatelé tak mohou klienta AppTec zavřít prostřednictvím správce úloh. Pokud je klient AppTec zavřený, nebude správně fungovat několik funkcí včetně režimu Kiosk Mode a App Black/Whitelisting. Zařízení Samsung nabízejí ochranný mechanismus pro klienta AppTec. V zařízeních Samsung, která podporují rozhraní KNOX API, je oznámení ve výchozím nastavení vypnuto. Upozornění by nemělo být zakázáno na zařízeních se systémem Android 8.0 nebo vyšším.	

Tapety

Nastavení vlastní tapety	Povolení/zakázání vlastní tapety
Tapety	Nastavení režimu tapety na použití barevného kódu nebo obrázku
Zadejte barvu	Zadejte barvu pozadí jako hexadecimální hodnotu, např. #000000 jako černou nebo #ffffff jako bílou.
Nastavení obrázku jako tapety	Nahrání souboru s obrázkem, který chcete použít jako tapetu

Správa aktiv (pouze na úrovni zařízení)

Informace o zařízení

Model	Označení modelu zařízení
Operační systém	OS
Verze operačního systému	Verze operačního systému
Sériové číslo	Sériové číslo
Název zařízení	Název zařízení
Stav baterie	Stav baterie
Volná / celková paměť	Volná / celková paměť
Samsung Safe	Rozhraní Samsung SAFE, potřebné pro různé možnosti nastavení
K dispozici je karta SD	K dispozici je karta SD
Emulace karty SD	Emulovaná karta SD
Vyměnitelná karta SD	Vyjímatelná karta SD
SD Volná / Celková paměť	Volná paměť SD / Celková paměť karty SD

Wi-Fi

IP adresa	IP adresa zařízení
WiFi MAC	Adresa MAC WiFi

Cellular

Stav	Stav (nainstalovaná karta SIM)
Telefonní číslo	Telefonní číslo
Roaming (hlas / data)	Roaming pro hlas / data
Stav roamingu	Aktuální stav roamingu
IP adresa	IP adresa
Provozovatel/přepravce	Provozovatel/přepravce
Mobilní technologie	Mobilní technologie
IMEI	Číslo IMEI
ICCID	Jedná se o ID karty SIM, často také karty Smartcard nebo karty s integrovanými obvody (ICC).
IMSI	Mezinárodní identifikace mobilního účastníka (IMSI) umožňuje v mobilních sítích GSM a UMTS jednoznačnou identifikaci uživatelů sítě. IMSI se skládá z maximálně 15 číslic a konfiguruje se následujícím způsobem: • Kód země mobilního telefonu (MCC), 3 číslice • Kód mobilní sítě (MNC), 2 nebo 3 číslice • Identifikační číslo mobilního účastníka (MSIN), 1-10 číslic
Současné MCC/MNC	Viz "SIM MCC/MNC"
SIM MCC/MNC	Kód mobilní země je zavedený identifikátor země stanovený ITU podle normy E.212. Funguje ve spojení s kódem mobilní sítě (MNC) pro identifikaci mobilní sítě. Znamená kód země/mobilní sítě karty SIM. Pokud jste v roamingu v jiné mobilní síti, pak se logicky budou údaje "Current MCC/MNC" a "SIM MCC/MNC" lišit.

Bluetooth

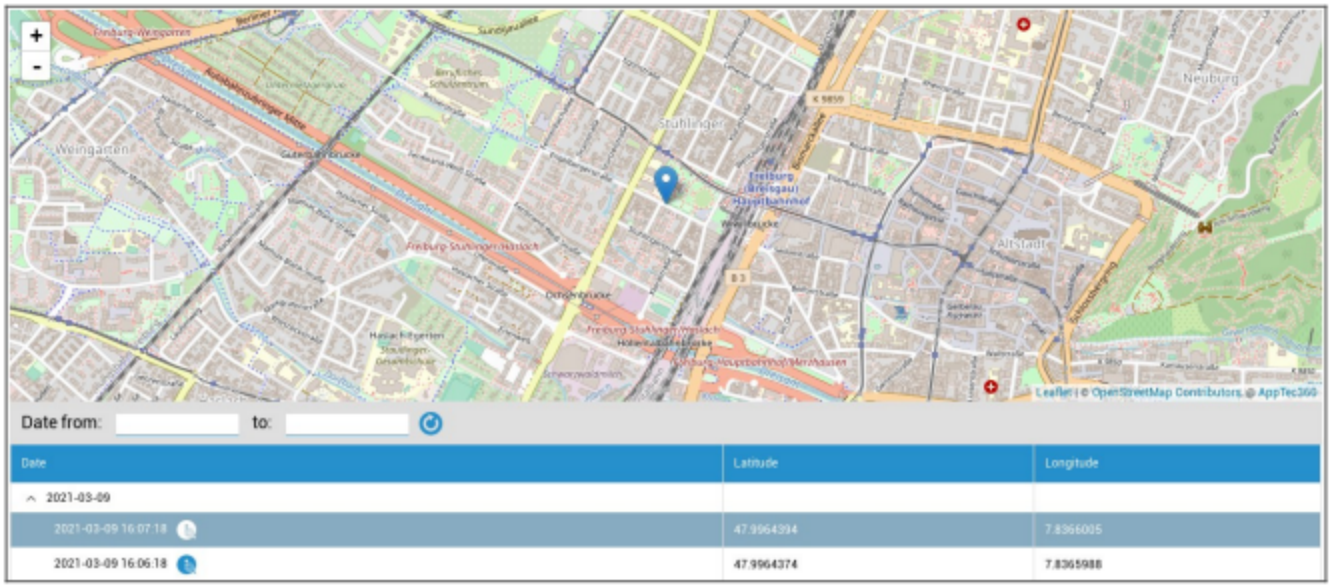
Bluetooth MAC	Adresa MAC Bluetooth

Správa zabezpečení

Ochrana proti krádeži (pouze na úrovni zařízení)

Informace GPS (pouze na úrovni zařízení)

Zde můžete zjistit aktuální/poslední umístění zařízení. Lokalizaci lze chránit jedním nebo dokonce dvěma hesly - viz: Přístup k GPS: - Obecná nastavení - Soukromí - Přístup k GPS



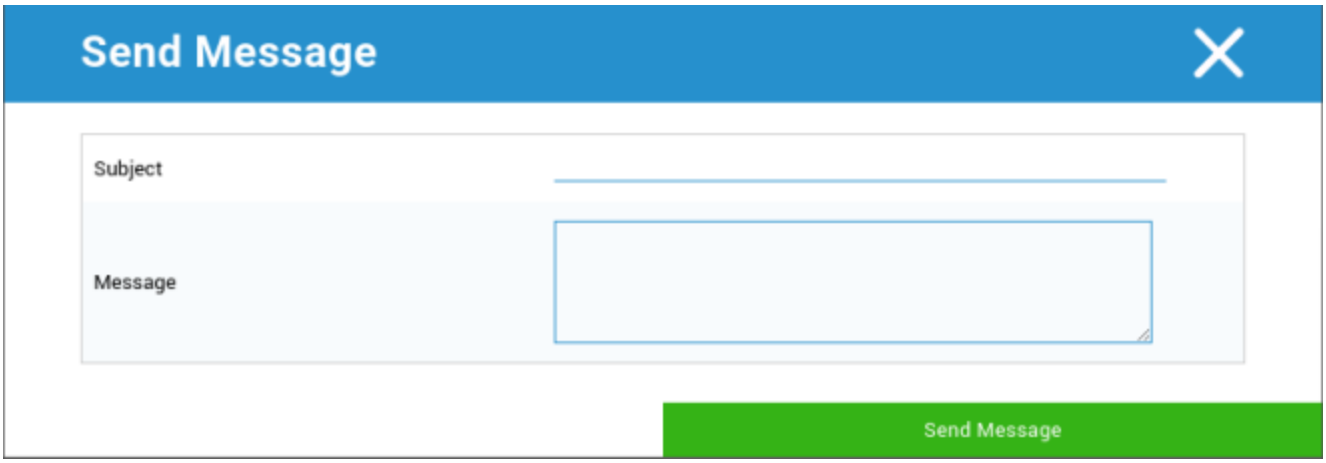
Vymazání a uzamčení (pouze na úrovni zařízení)

V části "Wipe & Lock" můžete provést následující tři akce:

Úplné otření	Zařízení je obnoveno do továrního nastavení (firemní i osobní údaje jsou odstraněny). Funguje pouze pro rozšířený pracovní profil
Podnikové utírání	Ze zařízení koncového uživatele jsou odstraněna pouze firemní data (všechny aplikace, data atd., které poskytla společnost AppTec).
Zamykací obrazovka	Zámek obrazovky je aktivován, stačí zařízení odemknout pomocí hesla zařízení/PIN kódu.

Zpráva (pouze na úrovni zařízení)

Zde můžete vyplnit předmět a zprávu a odeslat ji koncovému zařízení uživatele.



Konfigurace zabezpečení

Přístupový kód zařízení

V části "Přístupový kód" můžete zadat heslo zařízení, k dispozici jsou následující možnosti nastavení.

Minimální délka hesla	stanovuje minimální počet symbolů, které musí heslo obsahovat.	
Kvalita hesla	Nespecifikováno	Tato zásada neobsahuje žádné požadavky na heslo.
	Biometrické Slabé	Tato politika umožňuje použití biometrické rozpoznávací technologie s nízkým stupněm zabezpečení. To znamená technologie, které dokáží rozpoznat identitu jednotlivce přibližně do třímístného PIN kódu (falešná detekce je menší než 1 z 1000).
	Něco	Tato zásada vyžaduje nastavení nějakého hesla nebo vzoru, ale nevynucuje žádná konkrétní pravidla.
	Abecední	Uživatel musí zadat heslo obsahující alespoň znaky abecedy (nebo jiný symbol).
	Alfanumerické	Uživatel musí zadat heslo, které obsahuje alespoň číselné a abecední (nebo jiné znaky).
	Komplexní	Uživatel musí zadat heslo, které standardně obsahuje alespoň písmeno, číslici a speciální symbol. Díky této kvalitě hesla lze omezit, aby hesla obsahovala různé sady znaků, například alespoň jedno velké písmeno atd.
Minimální délka hesla	Nastavte požadovaný počet znaků pro heslo. Můžete například požadovat, aby PIN nebo hesla měla alespoň šest znaků.	
Minimální počet číslic požadovaných v hesle	Minimální počet číslic požadovaných v hesle	
Minimální počet malých písmen v hesle	Minimální počet malých písmen v hesle	
Minimální počet velkých písmen v hesle	Minimální počet velkých písmen v hesle	
Minimální počet nepísmenných znaků požadovaných v hesle	Minimální počet nepísmenných znaků požadovaných v hesle	
Minimální požadované symboly v hesle	Minimální požadované symboly v hesle	

Zámek maximální doby nečinnosti	Maximální nečinnost uživatele do časového zámku
Časový limit vypršení platnosti hesla	stanoví, po uplynutí jakého časového intervalu heslo vyprší a musí být vydáno nové heslo.
Omezení historie hesel	Počet dříve použitých hesel, která nejsou povolena
Maximální počet neúspěšných pokusů o zadání hesla	Stanovuje, jak často může být heslo zadáno nesprávně, než dojde k úplnému vymazání zařízení.
Povolení biometrického ověřování	Umožňuje ověřování pomocí otisku prstu nebo skenu oční duhovky. Pouze pro Samsung KNOX 2.1 a vyšší.

Přístupový kód kontejneru

V části "Přístupový kód" můžete zadat heslo kontejneru, k dispozici jsou následující možnosti nastavení

.

Minimální délka hesla	stanovuje minimální počet symbolů, které musí heslo obsahovat.	
Kvalita hesla	Nespecifikováno	Tato zásada neobsahuje žádné požadavky na heslo.
	Biometrické Slabé	Tato politika umožňuje použití biometrické rozpoznávací technologie s nízkým stupněm zabezpečení. To znamená technologie, které dokáží rozpoznat identitu jednotlivce přibližně do třímístného PIN kódu (falešná detekce je menší než 1 z 1000).
	Něco	Tato zásada vyžaduje nastavení nějakého hesla nebo vzoru, ale nevynucuje žádná konkrétní pravidla.
	Abecední	Uživatel musí zadat heslo obsahující alespoň znaky abecedy (nebo jiný symbol).
	Alfanumerické	Uživatel musí zadat heslo, které obsahuje alespoň číselné a abecední (nebo jiné znaky).
	Komplexní	Uživatel musí zadat heslo, které standardně obsahuje alespoň písmeno, číslici a speciální symbol. Díky této kvalitě hesla lze omezit, aby hesla obsahovala různé sady znaků, například alespoň jedno velké písmeno atd.
Minimální délka hesla	Nastavte požadovaný počet znaků pro heslo. Můžete například požadovat, aby PIN nebo hesla měla alespoň šest znaků.	
Minimální počet číslic požadovaných v hesle	Minimální počet číslic požadovaných v hesle	
Minimální počet malých písmen v hesle	Minimální počet malých písmen v hesle	
Minimální počet velkých písmen v hesle	Minimální počet velkých písmen v hesle	
Minimální počet nepísmenných znaků požadovaných v hesle	Minimální počet nepísmenných znaků požadovaných v hesle	
Minimální požadované symboly v hesle	Minimální požadované symboly v hesle	

Zámek maximální doby nečinnosti	Maximální nečinnost uživatele do časového zámku
Časový limit vypršení platnosti hesla	stanoví, po uplynutí jakého časového intervalu heslo vyprší a musí být vydáno nové heslo.
Omezení historie hesel	Počet dříve použitých hesel, která nejsou povolena
Maximální počet neúspěšných pokusů o zadání hesla	Stanovuje, jak často může být heslo zadáno nesprávně, než dojde k úplnému vymazání zařízení.

AntiVirus

Automatické skenování	Povolení pravidelného automatického skenování
Interval skenování	Interval pro vyšetření (rychlé / úplné)
Plně automatické skenování	Povolení úplného automatického skenování
Automatické aktualizace	Povolení automatických aktualizací
Interval kontroly aktualizace	Jak často by měla být aplikace a její databáze aktualizována (viry / poškozený kód).
Ochrana aplikací	Povolení automatického skenování aplikací
Ochrana karty SD	Povolení automatického skenování karty SD
Aktualizace pouze pro Wi-Fi	Pokud je tato možnost povolena, aktualizace se použijí pouze v případě, že je zařízení úspěšně připojeno k síti Wi-Fi.

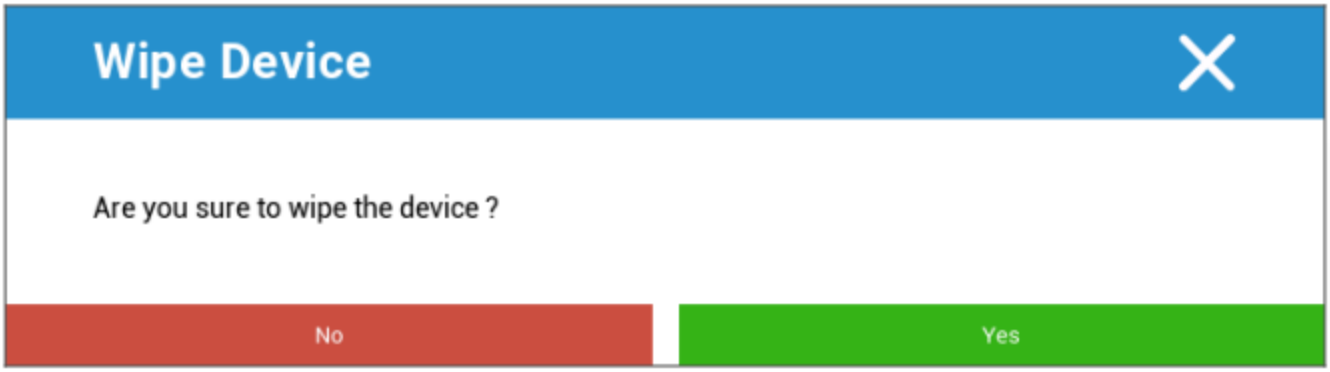
Konec životnosti (pouze na úrovni zařízení)

Vymazat (pouze na úrovni zařízení)

V části "Wipe" (Vymazat) můžete obnovit tovární nastavení zařízení (pouze v rozšířeném pracovním profilu).

V tomto případě budou v zařízení koncového uživatele smazána firemní i soukromá data.

Po kliknutí na symbol mínus se zobrazí následující zpráva:



Pokud zvolíte "Ano", můžete provést vymazání.

V části "Wipe Report" lze zobrazit následující položky.

Setřeno	Historie toho, kdo stírání provedl
Datum	Datum
Stav	Stav (např. zda bylo vymazání provedeno úspěšně)

Nastavení omezení

Omezení

Zde lze omezit a zablokovat celou řadu věcí.

Prosazování shody	Režim Výzva uživateli - Uživatel bude vyzván k provedení potřebných akcí. Kontejner s uzamčeným režimem - Skrytí všech aplikací, dokud nejsou splněny všechny požadavky.
Zásady oprávnění v době běhu	Výzva uživateli k zadání nových požadavků na oprávnění Vždy vyhovět novým žádostem o povolení Vždy odmítnout nové žádosti o povolení Varování: Některé aplikace mají problémy s rozpoznáním oprávnění, pokud jsou nastavena automaticky. Pokud vždy udělujete oprávnění a narazíte na problémy s aplikacemi, které tvrdí, že oprávnění chybí, nastavte tuto možnost na "vyzvat uživatele" a aplikaci znovu nainstalujte.
Povolit odchozí schránku	Umožňuje kopírování a vkládání z vnitřku kontejneru na vnější stranu.
Povolení rozlišení ID volajícího	Zobrazí jméno příchozího hovoru na základě kontaktů v kontejneru.
Povolit rozlišení vyhledávání kontaktů	Umožňuje vyhledávat jména v kontejneru kontaktů při volání.
Povolení sdílení kontaktů Bluetooth	Umožňuje přístup ke kontaktu kontejneru v autě
Zakázat odchozí paprsek NFC	Zakázání funkce NFC pro kontejner
Povolit neznámé zdroje	Pokud je tato možnost povolena, mohou uživatelé načítat aplikace ze strany instalací souboru .apk.
Povolení ladění USB	Pokud je povoleno, mohou uživatelé povolit ladění USB.
Zakázat změnu účtu	Zakáže vytváření, mazání a úpravy účtů v kontejneru. Mějte na paměti, že některé aplikace potřebují vytvořit nebo upravit účty, aby fungovaly podle očekávání.

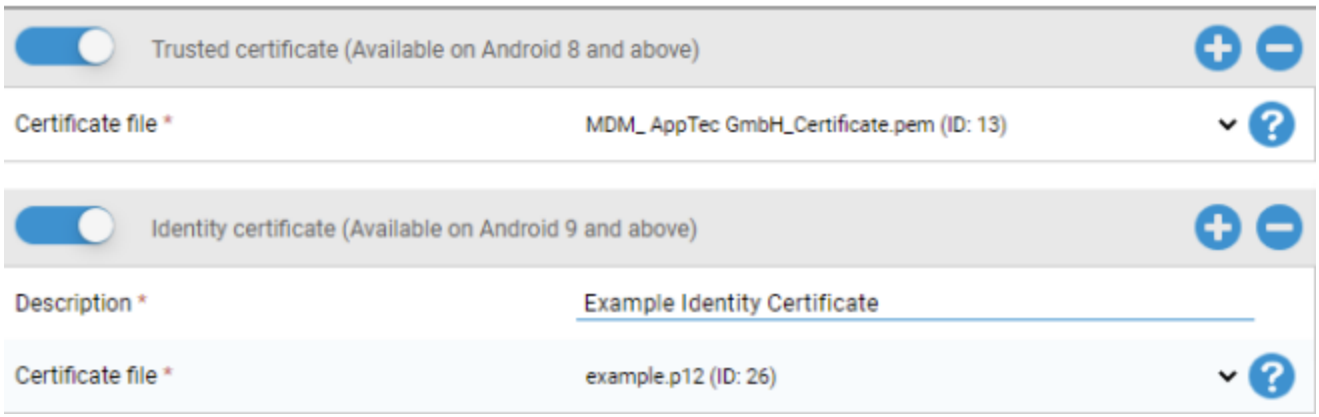
Omezení pracovního profilu. K dispozici pouze na zařízeních se systémem Android 11 a vyšším a s rozšířeným pracovním profilem.

Zakázat fotoaparát	Určuje, zda je fotoaparát v pracovním profilu zakázán.
Zakázat Bluetooth	Určuje, zda je v pracovním profilu zakázáno připojení Bluetooth.
Povolení ochrany při obnovení továrního nastavení	Aktivací této funkce přepíšete ochranu Androidu před obnovením továrního nastavení na účet Google, který jste definovali v části "Obecná nastavení" → "Konfigurace Androidu" → "Android Enterprise" → "Ochrana před obnovením továrního nastavení" Pokud je tato funkce aktivována a zařízení resetujete, budete muset při opětovném nastavení zařízení zadat nakonfigurovaný účet Google.
Aktualizace řídicího systému OS	Povolením této možnosti nastavíte chování aktualizace na automatické, s oknem nebo odložené.
Zásady aktualizace	Automaticky: Instaluje se automaticky, jakmile je k dispozici aktualizace. Okenní: Instalujte automaticky v rámci denního okna údržby. Tímto způsobem se také nastaví aktualizace aplikací Play v rámci okna. To se důrazně doporučuje pro kiosková zařízení, protože je to jediný způsob, jak mohou být aplikace trvale připnuté na popředí aktualizovány službou Play. Odložit: Odložte automatickou instalaci až o 30 dní.

Omezení osobního profilu. K dispozici pouze na zařízeních se systémem Android 11 a vyšším a s rozšířeným pracovním profilem.	
Zakázat fotoaparát	Určuje, zda je fotoaparát v osobním profilu zakázán.
Zakázat Bluetooth	Určuje, zda je v osobním profilu zakázáno používání Bluetooth.
Povolit neznámé zdroje	Pokud je tato možnost povolena, mohou uživatelé pracovních profilů načítat aplikace ze strany instalací souboru .apk.

Správa certifikátů

Zde můžete distribuovat důvěryhodné certifikáty a certifikáty totožnosti do svých zařízení. Pro distribuci důvěryhodných certifikátů je vyžadován systém Android 8 nebo vyšší a pro distribuci certifikátů identity je vyžadován systém Android 9 nebo vyšší.



Pomocí tlačítka "+" můžete přidat více certifikátů.

Důvěryhodné certifikáty musí být ve formátu PEM.

Certifikáty totožnosti musí být ve formátu PKCS12.

Správa připojení

Wifi

Pro toto nastavení proveďte předběžnou konfiguraci zařízení koncového uživatele pro přístup k interním přístupovým bodům

.

Identifikátor sady služeb (SSID)	SSID sítě, která má být připojena.
Skrytá síť	Aktivovat v případě, že přístupový bod nevysílá SSID.

Typ zabezpečení

Stanovení typu zabezpečení přístupového bodu

WEP

Heslo	Heslo pro přístupový bod

WPA/WPA2

Heslo	Heslo pro přístupový bod

802.1x EAP

Metoda EAP

PWD	Identita	Identita
	Heslo	Heslo

PEAP	Protokol ověřování fáze 2	žádné	Žádný další protokol
		MSCHAPV2	Protokol MSCHAPV2
		GTC	Protokol GTC
	Certifikát certifikační autority	Certifikát certifikační autority	
	Identita	Identita	
	Anonymní identita	Anonymní identita	
	Heslo	Heslo	

TTLS	Protokol ověřování fáze 2	žádné	Žádný další protokol
		PAP	Protokol PAP
		MSCHAP	Protokol MSCHAP
		MSCHAPV2	Protokol MSCHAPV2
		GTC	Protokol GTC
	Certifikát certifikační autority	Certifikát certifikační autority	
	Identita	Identita	
	Anonymní identita	Anonymní identita	
	Heslo	Heslo	

TLS	Certifikát certifikační autority	Certifikát certifikační autority
	Identita	Identita
	Heslo	Heslo

VPN

Název připojení	Název připojení VPN

Typ VPN

VPN

Klient VPN

Klient VPN AppTec	
Konfigurace brány	Vyberte konfiguraci brány VPN (viz **Obecná nastavení > Univerzální brána > Nastavení VPN**).
Vždy zapnutá síť VPN	Povolení nativního uzamčení
Povolení funkce AppTec Lockdown	Povolení funkce AppTec Lockdown

Vestavěný (k dispozici pouze v zařízeních Samsung)			
Typ připojení	PPTP	Server	Server
		Povolení šifrování PPTP	Povolení šifrování PPTP
	L2TP / IPSec PSK	Server	Server
		Předsdílený klíč IPSec	Předsdílený klíč IPSec
		Povolení protokolu L2TP Secret	Povolení protokolu L2TP Secret
		Tajemství protokolu L2TP	Tajemství protokolu L2TP
	IPSec XAuth PSK	Server	Server
		Identifikátor IPSec	Identifikátor IPSec
		Předsdílený klíč IPSec	Předsdílený klíč IPSec
Vyhledávání domén DNS	Vyhledávání domén DNS		
Expertní nastavení	Servery DNS	Servery DNS	
	Trasy předávání	Trasy předávání	

Otevřená síť VPN		
Server	Server	
Profil OpenVPN	Profil OpenVPN	
Aplikace OpenVPN	OpenVPN pro Android (doporučeno)	
	Připojení k síti OpenVPN	
Expertní nastavení	Servery DNS	Servery DNS
	Trasy předávání	Trasy předávání

Samsung / Strong Swan			
Typ připojení	PPTP	Server	Server
		Uživatelské jméno	Uživatelské jméno
		Heslo	Heslo
		Povolení šifrování PPTP	Povolení šifrování PPTP
	L2TP / IPSec PSK	Server	Server
		Předsdílený klíč IPSec	Předsdílený klíč IPSec
		Uživatelské jméno	Uživatelské jméno
		Heslo	Heslo
		Povolení protokolu L2TP Secret	Tajemství protokolu L2TP
	IPSec XAuth PSK	Server	Server
		Identifikátor IPSec	Identifikátor IPSec
		Předsdílený klíč IPSec	Předsdílený klíč IPSec
		Uživatelské jméno	Uživatelské jméno
		Heslo	Heslo
Expertní nastavení	Servery DNS	Servery DNS	
	Trasy předávání	Trasy předávání	

Cisco Any Connect		
Server	Server	
Režim certifikátu	Bezbariérový	Bezbariérový
	Automatické	Automatické
Expertní nastavení	Servery DNS	Servery DNS
	Trasy předávání	Trasy předávání

VPN pro jednotlivé aplikace

Klient VPN

Klient VPN AppTec		
Konfigurace brány	Vyberte konfiguraci brány VPN (viz **Obecná nastavení > Univerzální brána > Nastavení VPN**).	
Aplikace VPN	Aplikace VPN	
Vždy zapnutá síť VPN	Povolení nativního uzamčení	Vždy zapnutá síť VPN
Povolení funkce AppTec Lockdown	Povolení funkce AppTec Lockdown	

Samsung / Strong Swan			
Typ připojení	PPTP	Server	Server
		Aplikace VPN	Aplikace VPN
		Uživatelské jméno	Uživatelské jméno
		Heslo	Heslo
		Povolení šifrování PPTP	Povolení šifrování PPTP
	L2TP / IPSec PSK	Server	Server
		Aplikace VPN	Aplikace VPN
		Předsdílený klíč IPSec	Předsdílený klíč IPSec
		Uživatelské jméno	Uživatelské jméno
		Heslo	Heslo
		Povolení protokolu L2TP Secret	Tajemství protokolu L2TP
	IPSec XAuth PSK	Server	Server
		Aplikace VPN	Aplikace VPN
		Identifikátor IPSec	Identifikátor IPSec
		Předsdílený klíč IPSec	Předsdílený klíč IPSec
		Uživatelské jméno	Uživatelské jméno
		Heslo	Heslo
Expertní nastavení	Servery DNS	Servery DNS	
	Trasy předávání	Trasy předávání	

Omezení

Zde můžete nastavit omezení týkající se správy připojení.

Povolení datového roamingu	Povolení mobilních dat při roamingu
Vynucení datového roamingu	Pokud je aktivován, je roaming pro mobilní data trvale aktivován (nedoporučuje se!). Toto nastavení přepíše nastavení "Povolit datový roaming"!
Použití systémového serveru http Proxy	Použití proxy serveru HTTP, který je k dispozici v nastavení systému, závisí na připojené síti (WiFi nebo APN).

Správa PIM

Výměna Gmail

Informace: Tato konfigurace se použije pro aplikaci Gmail. Musíte tedy schválit a nainstalovat aplikaci Gmail.

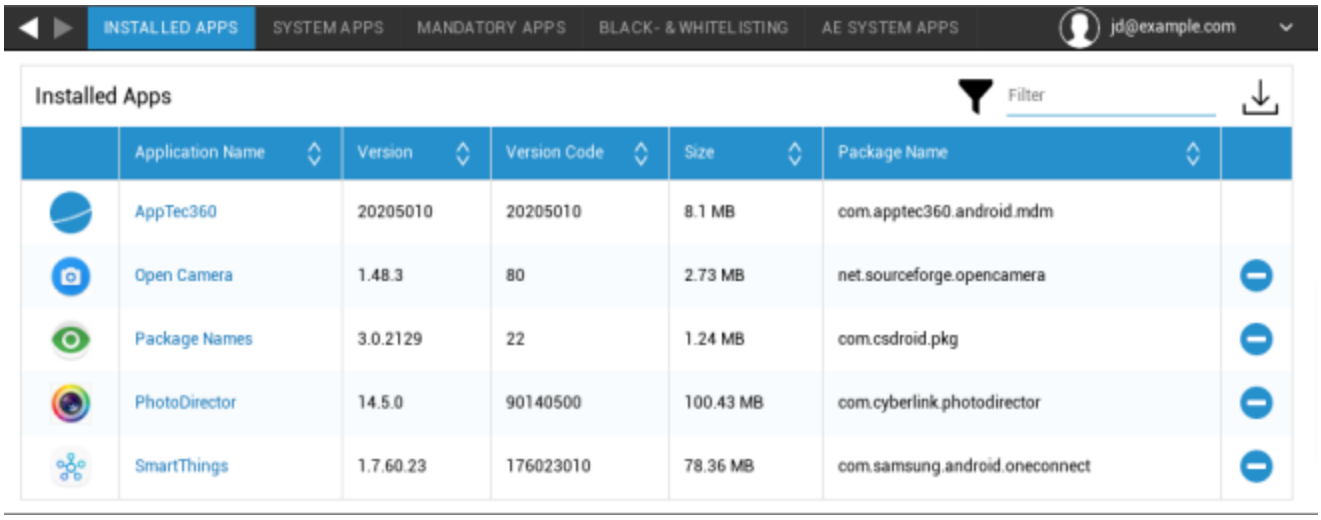
E-mailová adresa	Poskytnutá e-mailová adresa uživatele Všimněte si "zástupných symbolů", které můžete použít pro práci s pověřeními a neprovádíte změny ručně na každém zařízení. Jedním kliknutím si je můžete sami zobrazit.
Název hostitele serveru	Adresa serveru serverů Exchange
Přihlašovací jméno	Přihlašovací jméno pro příslušné zařízení koncového uživatele, všimněte si prosím také "Placeholders here".
Podpis	Lze připojit podpis (Tip: některá zařízení vyžadují formátování podpisu v HTML).
Počet předchozích dnů k synchronizaci	Počet dní, které určují, kdy se e-maily synchronizují zpět.
Identifikátor zařízení	Ein String der die EAS DeviceID enthält. Dies ist Teil des EAS Protokols und wird in einigen Umgebungen benötigt
Použití protokolu SSL (Secure Sockets Layer)	Použití připojení SSL
Přijmout všechny certifikáty	Přijímají se všechny certifikáty. Tuto možnost vyberte, pokud váš Exchange Server používá certifikát s vlastním podpisem.
Povolení nespravovaných účtů	Povolit uživatelům přidávat nebo odebírat libovolný účet Exchange jiný než účet zadaný v této spravované konfiguraci. Pokud je toto nastavení povoleno, nelze uživatelům zabránit v přidávání jiných účtů Exchange do služby Gmail. Nemůžete také řídit sdílení dat mezi ostatními aplikacemi a účty Exchange přidanými uživateli. Toto nastavení by mělo být povoleno pouze v případě, že vaši uživatelé potřebují v Gmailu udržovat více než jeden pracovní účet Exchange.
Certifikát klienta	Certifikát klienta. Vyžaduje se pouze v případě, že poštovní server jeho přítomnost očekává.

Správa aplikací

Správce podnikových aplikací

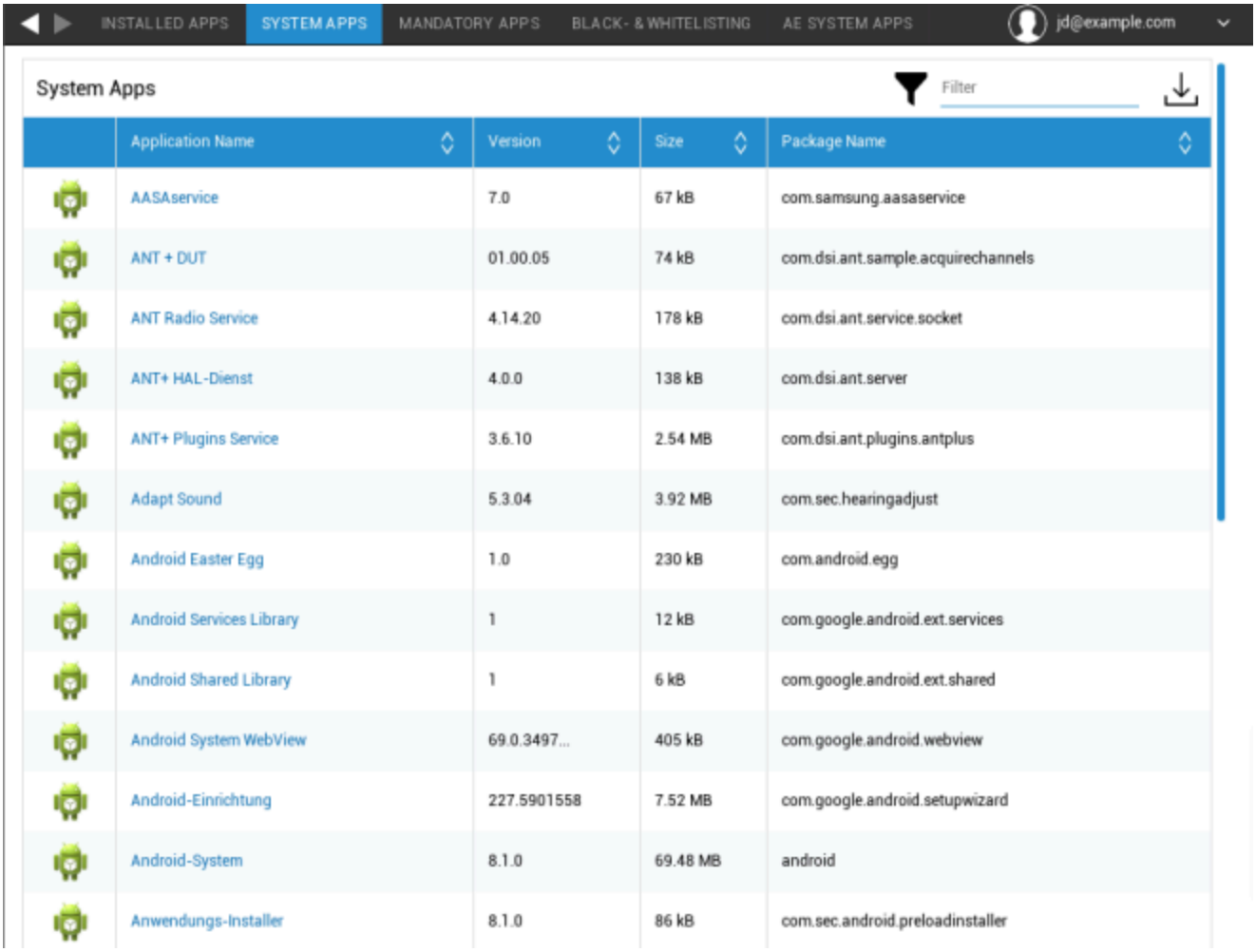
Nainstalované aplikace (pouze na úrovni zařízení)

Zde se zobrazí všechny aplikace, které jsou v kontejneru aktuálně nainstalovány.



Systémové aplikace (pouze na úrovni zařízení)

V části "Systémové aplikace" se zobrazí seznam všech aplikací a služeb, které již byly do koncového zařízení uživatele nainstalovány výrobcem zařízení.

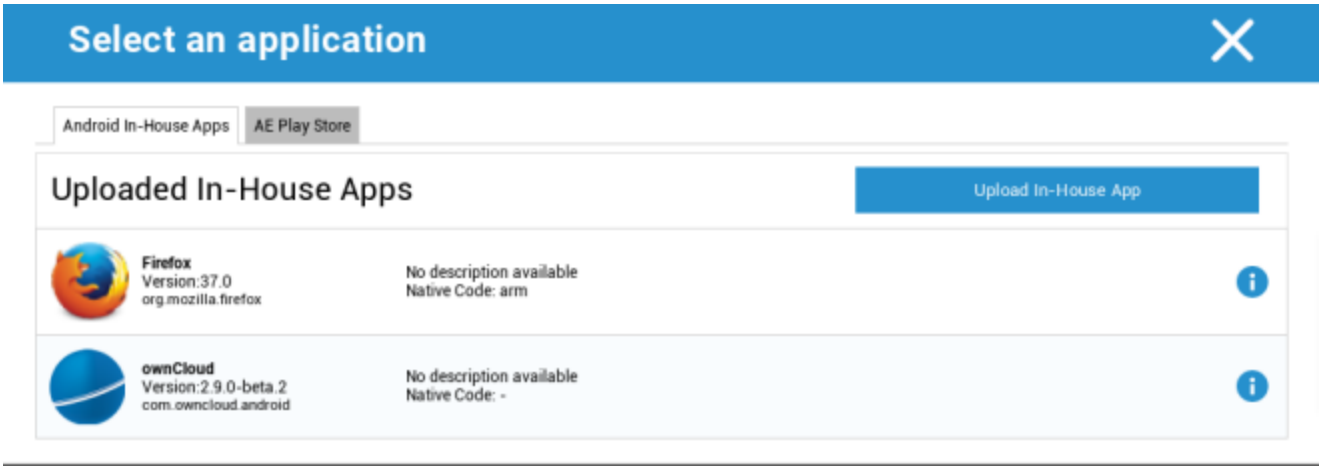


Povinné aplikace

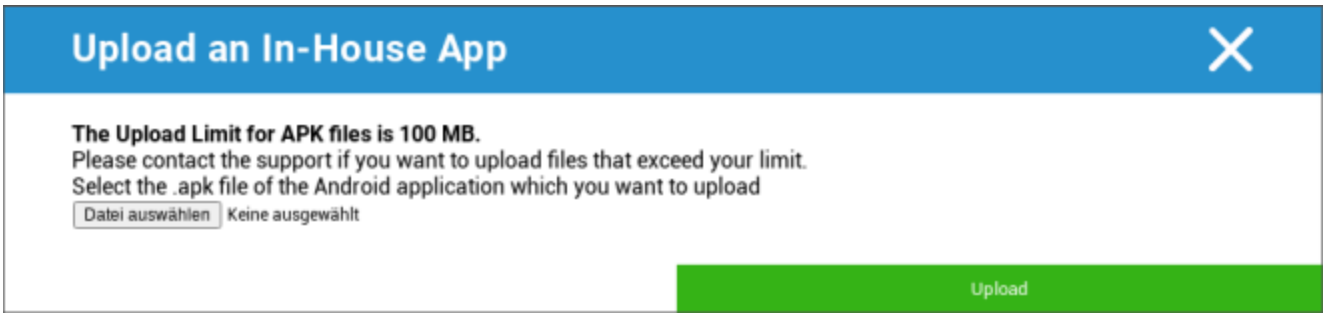
V části Povinné aplikace můžete nastavit povinné aplikace. Uživatel bude neustále vyzýván k instalaci této určené aplikace, pokud se jedná o aplikaci InHouse App. Aplikace z Obchodu Play se nainstalují automaticky.

Prostřednictvím , lze definovat povinnou požadovanou aplikaci.

Může se jednat o interní aplikaci z nabídky "Interní aplikace pro Android", kterou jste nahráli v obecných nastaveních.

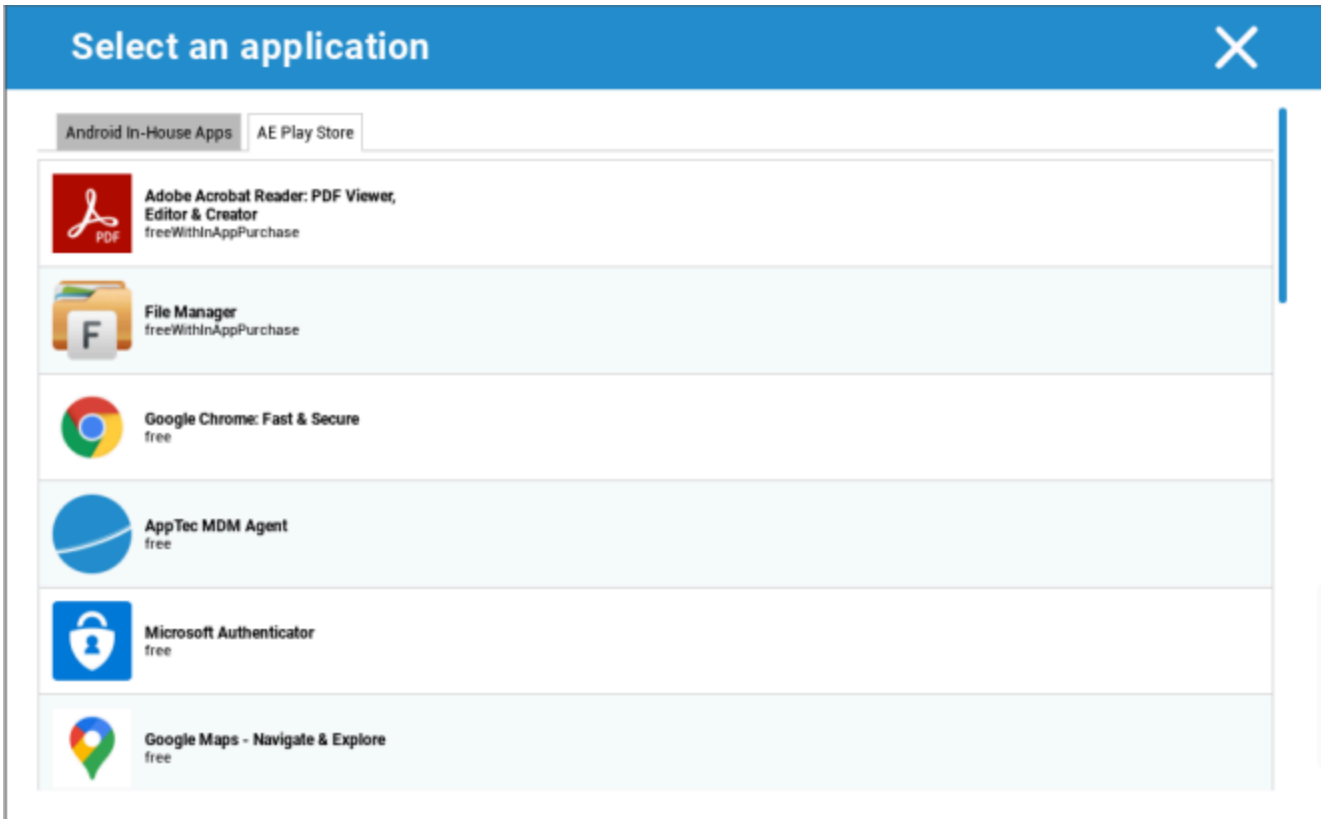


Soubor apk můžete také přímo vybrat a nahrát pomocí funkce "Upload In-House App".



Pokud instalujete aplikaci In-House, máte možnost aktivovat funkci "Keep up to date". Pokud je tato funkce aktivována a v databázi In-House App DB jste definovali novější verzi, aplikace se v zařízení aktualizuje.

Nebo to může být aplikace "AE Play Store" z pracovního obchodu Google Play.



Na této kartě se zobrazí pouze schválené aplikace "AE Play Store Apps".

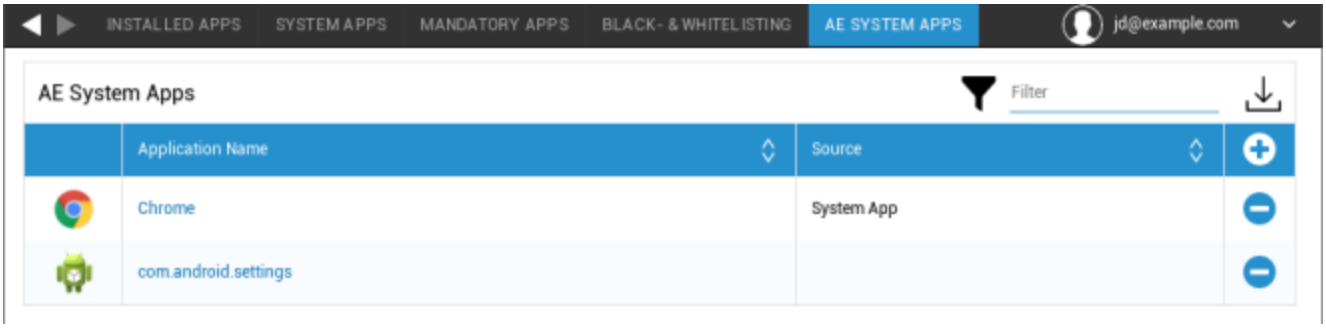
Chcete-li schválit aplikaci "AE Play Store", přejděte do "Obecná nastavení" > "Správa aplikací" > "AE Play".

Store" a přidejte aplikaci pomocí tlačítka, které vás přesměruje na kartu "Aplikace Obchodu Play" (nebo můžete přejít přímo na kartu "Aplikace Obchodu Play").

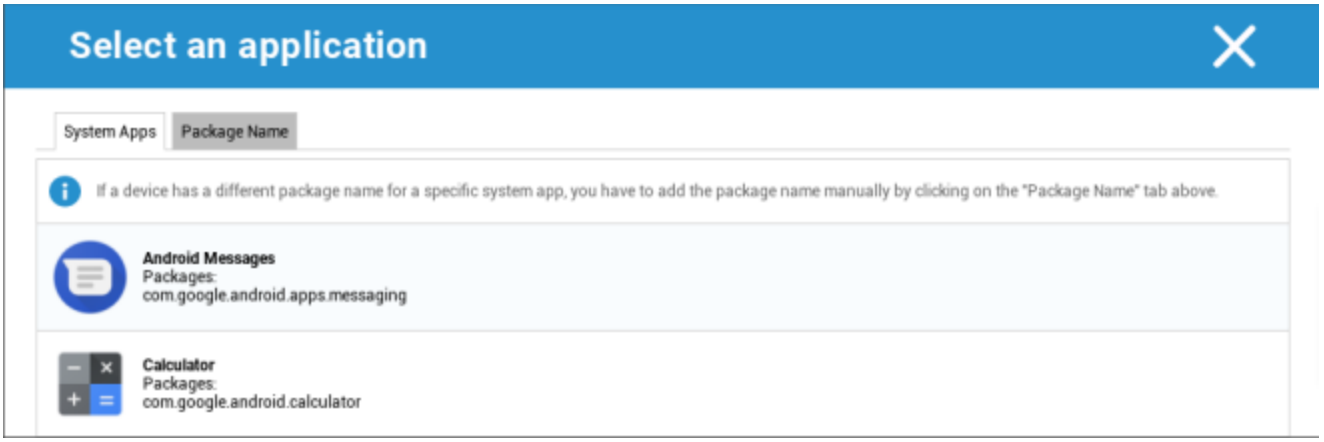
Na kartě "Aplikace v Obchodě Play" můžete vyhledávat aplikace. Po kliknutí na aplikaci se otevře stránka aplikace a zde můžete aplikaci schválit kliknutím na "Approve".

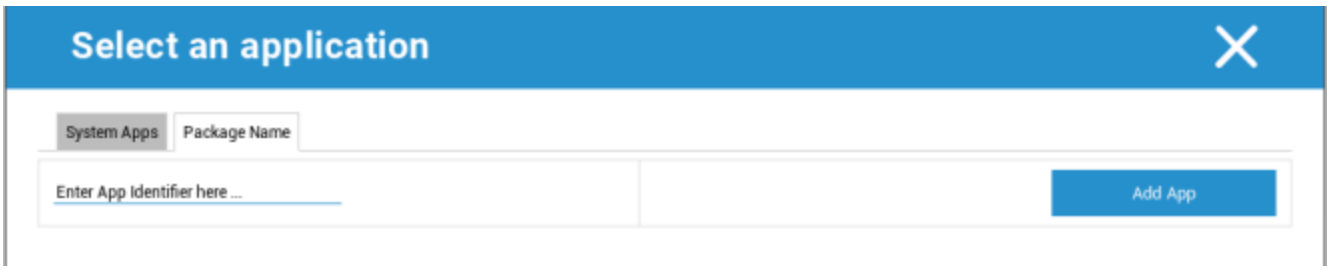
Systémové aplikace AE

Zde můžete definovat seznam obsahující konkrétní systémové aplikace, které mají být v zařízeních aktivovány.



Po kliknutí na tlačítko můžete vybrat ze seznamu možných systémových aplikací poskytnutých společností Google nebo přímo zadat název balíčku systémové aplikace, která má být aktivována.





Mějte na paměti, že systémové aplikace v seznamu poskytnutém společností Google jsou pouze aplikace, které mohou být systémovými aplikacemi, ale nemusí být nutně systémovými aplikacemi ve vašich zařízeních.

Tento seznam se však týká pouze již předinstalovaných aplikací.

Přidání aplikací, které nejsou v zařízeních předinstalovány, nebude mít na zařízení vliv bez ohledu na to, zda je aplikace ze seznamu poskytnutého společností Google, nebo je zadán přímo název balíčku

aplikace.

Omezení a nastavení

Nastavení správy aplikací

Zde můžete nastavit chování zařízení, pokud jde o aktualizace aplikací.

Frekvence kontroly aktualizací	Zadejte, v jakém intervalu bude klient AppTec vyhledávat aktualizace aplikací. Výchozí hodnota je 24 hodin.
Prahová hodnota Wi-Fi	Aplikace, které jsou větší než zadaná velikost, budou staženy přes Wi-Fi. Pokud je vybrána možnost "Pouze Wi-Fi", budou všechny aplikace stahovány přes Wi-Fi.

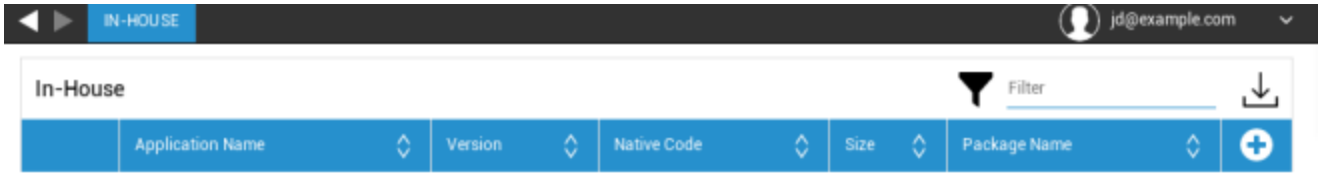
Obchod s podnikovými aplikacemi

In-House

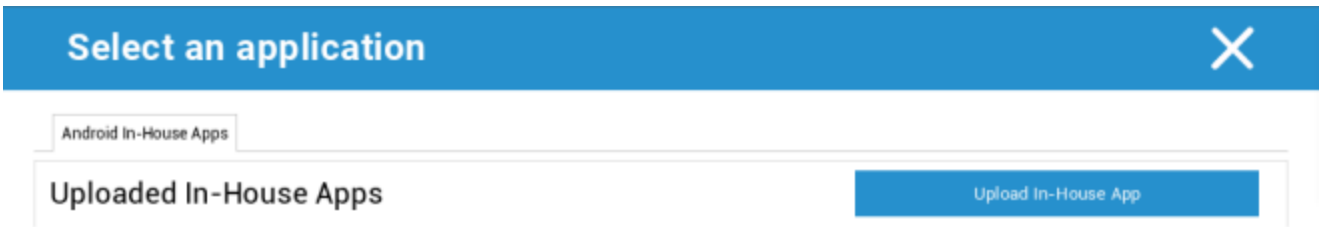
V bodě "In-House" můžete nahrávat a distribuovat interně vyvinuté aplikace.

Pomocí tohoto symbolu můžete distribuovat další aplikace In-House.

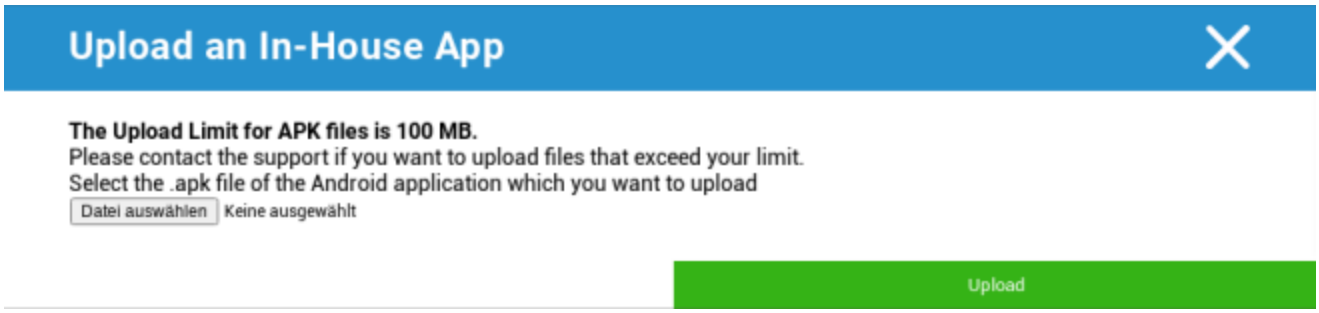
Pokud instalujete aplikaci In-House, máte možnost aktivovat funkci "Keep up to date". Pokud je tato funkce aktivována a v databázi In-House App DB jste definovali novější verzi, aplikace se v zařízení aktualizuje.



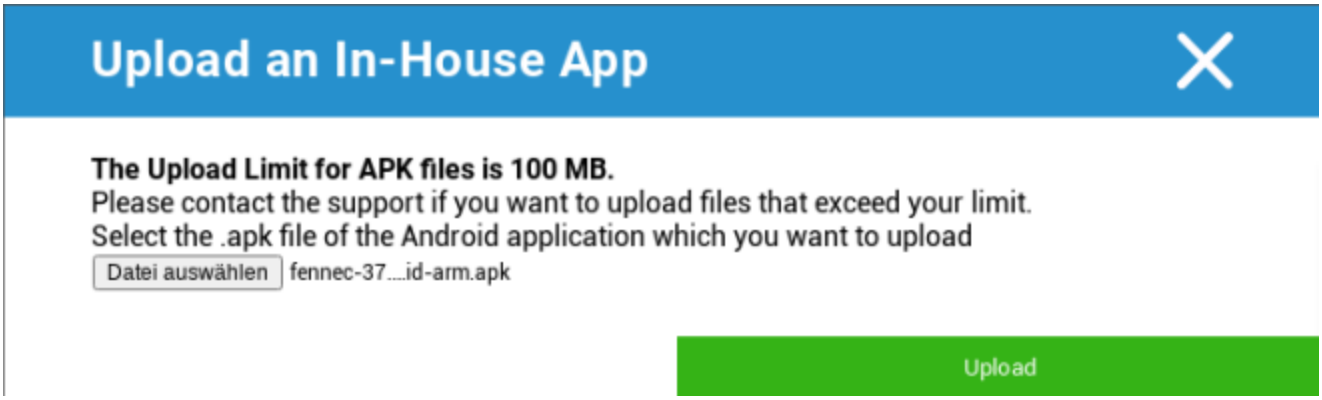
Pokud nemáte distribuované aplikace In-House Apps, obdržíte následující přehled:



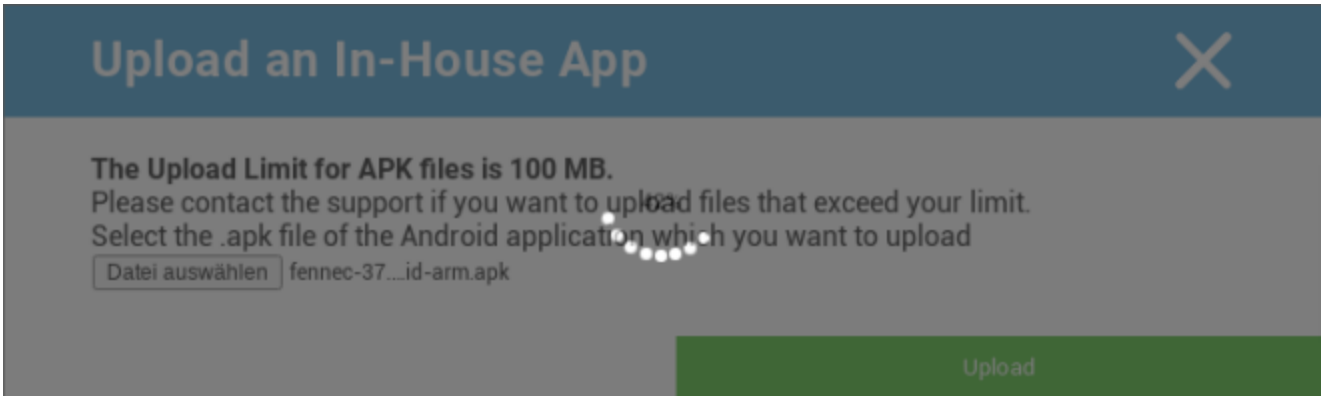
Za tímto účelem klikněte na "Nahrát interní aplikaci" a zobrazí se následující přehled:



Nyní vyberte pomocí "Search..." soubor .apk a klikněte na "Upload".



Vaše aplikace se nyní nahraje a uprostřed kruhu se zobrazí procentuální ukazatel, který ukazuje, jak velká část aplikace již byla nahrána.



Pokud bylo nahrání vaší interní aplikace úspěšné, můžete nahranou aplikaci najít ve svém katalogu aplikací.

Uživatel má nyní možnost zobrazit a nainstalovat tuto aplikaci v AppTec Store na zařízení koncového uživatele v kategorii "In-House".

Vzhledem k tomu, že se nejedná o aplikaci Google PlayStore, nepotřebuje uživatel uložené Google ID v příslušném koncovém zařízení.

Obchod Play pro podniky

Obchod AE Play

Zde můžete přidávat aplikace do obchodu Android Enterprise Playstore. Vezměte prosím na vědomí, že před přidáním aplikací je nutné je schválit pomocí účtu správce AE.

Pokyny ke schválení aplikace naleznete v části Povinné aplikace.

Správa obsahu

ContentBox

Zde můžete aktivovat pole ContentBox.

Jakmile přepnete možnost "Enable ContentBox" na "On", do zařízení koncového uživatele se automaticky nainstaluje samostatná aplikace ContentBox.

Zabezpečený prohlížeč

Zde můžete nakonfigurovat nastavení pro AppTec Secure Browser.

Jakmile přepnete sekci "Zabezpečený prohlížeč" do polohy "Zapnuto", do zařízení koncového uživatele se automaticky nainstaluje samostatná aplikace prohlížeče.

Vyžadovat heslo	Požadovat, aby si uživatel nastavil a používal heslo pro přístup k prohlížeči.
Minimální požadovaná délka hesla	Nastavení požadovaného počtu znaků pro heslo
Požadovaná kvalita hesla	Nastavení požadované kvality hesla
Omezit stahování / Otevřít v	
Omezení nahrávání	
Nahrání bílé listiny	Seznam adres URL, pro které bude vždy povoleno nahrávání.
Povolit kopírování	Povolení kopírování, vyřezávání nebo sdílení textu uvnitř webových stránek.
Povolit snímání obrazovky	Umožňuje pořizování snímků obrazovky.
Frekvence čištění dat	Zvolte, s jakou frekvencí se mají automaticky odstraňovat VŠECHNA uživatelská data (historie, mezipaměť atd.).
Záložky společnosti	Záložky se zobrazí ve složce "Firemní záložky" v záložkách prohlížeče. Uživatel je nemůže upravovat.
Skrytí adresního řádku	
Whitelisting v prohlížeči (bez univerzální brány)	Povoluje whitelisting adres URL na straně klienta. • Firemní záložky jsou vždy na bílé listině • Podporováno pouze pro 100 adres URL • Pro neomezený black- a whitelisting používejte univerzální bránu.
Adresy URL na bílé listině	Seznam povolených adres URL.
Černá a bílá listina založená na bráně	Černá listina má následující požadavky: • Fungující univerzální brána AppTec ("Obecná nastavení" → "Univerzální brána").

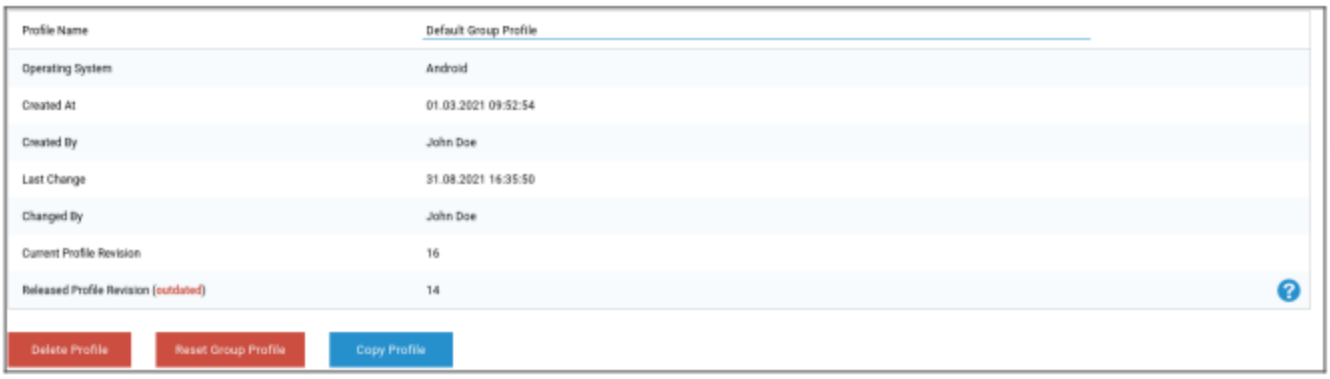
	• Fungující konfigurace VPN se zadaným serverem DNS ("Obecná nastavení" → "Univerzální brána" → "Nastavení VPN"). • Konfigurace černé listiny ("Obecná nastavení" → "Univerzální brána" → "Černá listina domén") • Platné připojení VPN v profilu ("Správa připojení" → "VPN").

Konfigurace systému Android

Obecné

Přehled profilu skupiny (pouze na úrovni skupiny)

Po otevření profilu skupiny se zobrazí rychlý přehled profilu.



Název profilu	Název profilu (zde lze změnit)
Operační systém	Operační systém, pro který je profil určen
Vytvořeno v	Čas vytvoření
Vytvořil	Tvůrce profilu
Poslední změna	Čas poslední změny profilu
Změněno podle	Účet, který provedl poslední změny
Aktuální revize profilu	Revize uloženého stavu profilu
Vydaná revize profilu	Přiřazená revize profilu ("Assign now"). Pokud se za textem na štítku zobrazí " (zastaralý)", znamená to, že jste profil uložili, ale ještě jste ho nepřiřadili, takže zařízení budou stále dostávat starší verzi.

Přehled zařízení (pouze na úrovni zařízení)

Pokud se nacházíte na zařízení, zobrazí se přehledová rekapitulace vybraného zařízení, která obsahuje následující informace:

Název zařízení	Název zařízení
Poslední známé místo	Poslední známé souřadnice GPS
Telefonní číslo	Telefonní číslo
Přiřazené povinné aplikace	Počet přidělených povinných aplikací
Verze operačního systému	Verze operačního systému zařízení
Operační systém	Operační systém (Android / iOS / Windows Phone)
Sériové číslo	Sériové číslo zařízení
Vlastnictví zařízení	Firemní nebo soukromé zařízení
Typ zařízení	Telefon nebo tablet
Zakořeněný	Stav, který udává, zda bylo zařízení rootnuto.
V souladu s předpisy	V souladu s pokyny
IP adresa	IP adresa
Naposledy viděno	Časový okamžik, kdy se zařízení naposledy připojilo k AppTec.
Poslední impuls	Bod v čase, kdy server odeslal push do zařízení.
Přiřazení uživatele	Rozbalovací seznam pro přiřazení zařízení jinému uživateli

Revize konfigurace (pouze na úrovni zařízení)

Zde získáte přehled o tom, který skupinový profil je k zařízení přiřazen.

Pokud kliknete na profil skupiny, dostanete se přímo do profilu a můžete provést nastavení.

Pomocí symbolu můžete vrátit přiřazené aplikace do nastavení skupinového profilu.

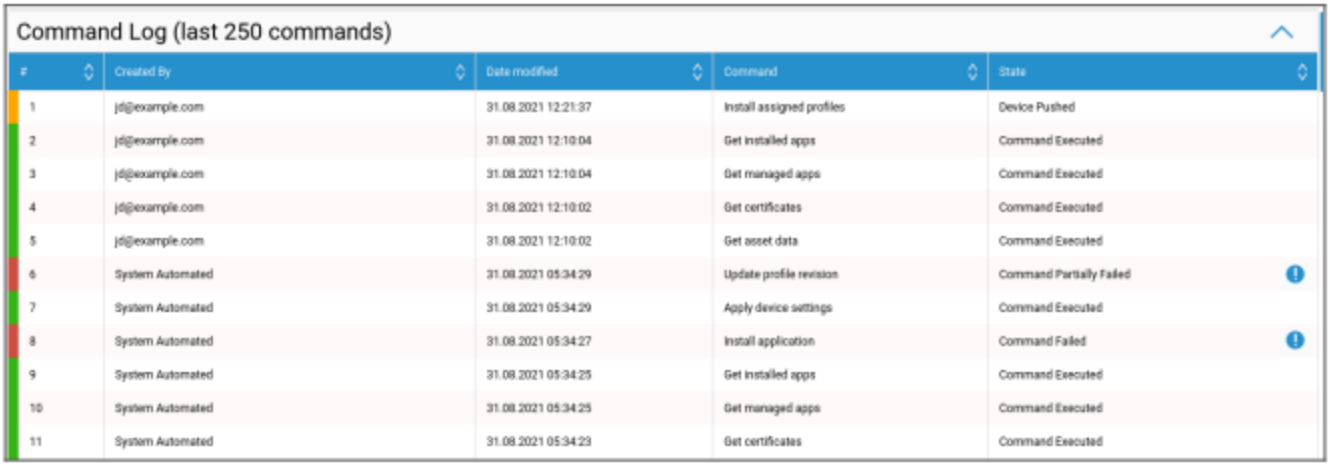
Pomocí symbolu můžete obnovit profil zařízení tak, aby neměl žádné nastavení.

"K dispozici je novější revize" znamená, že profil skupiny byl změněn a uložen, ale nebyl přiřazen. Profil skupiny je třeba přiřadit pomocí "Přiřadit nyní" na úrovni skupiny, aby se změny uplatnily na zařízení.

Protokol zařízení (pouze na úrovni zařízení)

Protokol příkazů

Zde můžete zjistit, které příkazy byly pro zařízení vydány a jaký je jejich stav.



Příkazy vytvořené pomocí "System Automated" jsou automaticky vytvořeny systémem.

Možné stavy příkazů

Stlačené zařízení	Službě push (např. APNS) byl odeslán požadavek na připojení, aby se zařízení připojilo zpět k serveru EMM.
Vytvořený příkaz	Příkaz byl vytvořen v systému.
Odeslaný příkaz	Příkaz byl odeslán do zařízení po jeho připojení k serveru.
Spuštěný příkaz	Příkaz byl úspěšně proveden.
Příkaz se nezdařil	Příkaz se nezdařil. *
Příkaz částečně selhal	V závislosti na operačním systému zařízení mohou být některé příkazy seskupeny. V tomto některé části této skupiny příkazů selhaly. *
Příkaz proveden, případně neúspěšný	Příkaz byl proveden, ale možná nebyl.
Přesunutí příkazu	Příkaz byl znovu odeslán uživatelem.
Vyřazené	Příkaz byl vyřazen. Například proto, že byl nahrazen jiným příkazem nebo že zařízení bylo znovu zapsáno a staré příkazy byly odstraněny.

*Pokud je za zprávou vykřičník, můžete získat další informace, když na ikonu najedete kurzorem.

Nastavení zařízení

Konfigurace klienta

Zde můžete provést následující konfigurace zařízení se systémem Android:

Výstražná zpráva po zakázání správy zařízení	Vytvořená varovná zpráva po zakázání správy zařízení
Čas mimo soulad	Časový limit, po jehož uplynutí bude provedena "Enforcement Action after compliance", pokud zařízení není v souladu. Min. 1 minuta Max. 24 hodin
Donucovací opatření po uplynutí lhůty pro splnění požadavků	Opatření, která je třeba přijmout, jakmile se zařízení stane nevyhovujícím. • nedělat nic = žádná akce • Zámek zařízení = zámek zařízení • Vymazat zařízení = zařízení bude obnoveno do továrního nastavení.
Frekvence sběru dat	Četnost shromažďování informací o zařízení/GPS
Frekvence srdečního tepu zařízení	Interval, ve kterém má zařízení kontaktovat server AppTec360. Min. 1 minuta Max. 24 hodin
Povolení aktualizací polohy	Pokud je aktivováno, zařízení odesílá aktualizace polohy na server AppTec360.
Čas aktualizace umístění	Určuje, v jakých časových intervalech zařízení odesílá aktualizace polohy do systému AppTec.
Použití služby Google Location Accuracy pro aktualizaci polohy	Pokud je aktivována, bude se pro aktualizace polohy používat přesnost polohy Google (dříve známá jako poloha v síti) (pokud byla deaktivována v části "Omezení", toto nastavení nic neovlivní).
Použití polohy GPS pro aktualizaci polohy	Pokud je aktivována, bude se pro aktualizaci polohy používat GPS.
Povolení falešných umístění	Umožňuje falšování informací o poloze prostřednictvím aplikací třetích stran.

Akce při ztrátě spojení	Umožňuje nastavit určitou akci, která se provede po určitém počtu selhaných srdečních tepů.
Režim vynucování zásad	Definuje, jak agresivně bude klient AppTec360 žádat uživatele o provedení určitých akcí, které vyžadují vstup uživatele. Interval (výchozí) = dotazovat se v intervalech, takže uživatel může tuto funkci na chvíli odložit na pozadí. Žádné upozornění = žádné vyskakovací okno pro požadovanou interakci. Musíte otevřít klienta AppTec360 ručně, abyste zkontrolovali, zda je požadována nějaká akce. Konstantní upozornění = uživatel může provést pouze požadovanou akci. Klient AppTec360 se bude vnucovat do popředí, pokud se mu uživatel pokusí vyhnout.
Zámek verze AppTec360	Umožňuje definovat verzi klienta AppTec360, která je maximální verzí, na kterou se klient aktualizuje.

Tapety

Zde můžete definovat vlastní tapetu.

"Zadat barvu" umožňuje definovat barvu v hexadecimálním formátu (např. #000000). Povoleny jsou pouze hexadecimální hodnoty.

"Nastavit obrázek jako tapetu" umožňuje nahrát obrázek. Upozorňujeme, že různá zařízení s různými spouštěči a verzemi operačního systému fungují odlišně. Neexistuje žádný obecný návod pro velikost a poměr, protože to závisí na zařízení.

Pro formát souboru použijte JPG (nebo JPEG) nebo PNG.

Správa aktiv (pouze na úrovni zařízení)

Správa majetku

Informace o zařízení

Model	**Označení modelu zařízení**
Operační systém	OS
Verze operačního systému	Verze operačního systému
Podpora AE	Podpora systému Android Enterprise (kontejner a plně spravovaný systém)
Sériové číslo	Sériové číslo
Název zařízení	Název zařízení
Stav baterie	Stav baterie
Volná / celková paměť	Volná / celková paměť
Samsung KNOX	Úroveň rozhraní API Samsung KNOX
K dispozici je karta SD	K dispozici je karta SD
Emulace karty SD	Emulovaná karta SD
Vyměnitelná karta SD	Vyjímatelná karta SD
SD Volná / Celková paměť	Volná paměť SD / Celková paměť karty SD

Wi-Fi

IP adresa	IP adresa zařízení
WiFi MAC	Adresa MAC WiFi

Cellular

Stav	Stav (nainstalovaná karta SIM)
Telefonní číslo	Telefonní číslo
Roaming (hlas / data)	Roaming pro hlas / data
Stav roamingu	Aktuální stav roamingu
IP adresa	IP adresa
Provozovatel/přepravce	Provozovatel/přepravce
Mobilní technologie	Mobilní technologie
IMEI	Číslo IMEI
ICCID	Jedná se o ID karty SIM, často také karty Smartcard nebo karty s integrovanými obvody (ICC).
IMSI	Mezinárodní identifikace mobilního účastníka (IMSI) umožňuje v mobilních sítích GSM a UMTS jednoznačnou identifikaci uživatelů sítě. IMSI se skládá z maximálně 15 číslic a konfiguruje se následujícím způsobem: • Kód země mobilního telefonu (MCC), 3 číslice • Kód mobilní sítě (MNC), 2 nebo 3 číslice • Identifikační číslo mobilního účastníka (MSIN), 1-10 číslic
Současné MCC/MNC	Viz "SIM MCC/MNC"
SIM MCC/MNC	Kód mobilní země je zavedený identifikátor země stanovený ITU podle normy E.212. Funguje ve spojení s kódem mobilní sítě (MNC) pro identifikaci mobilní sítě. Znamená kód země/mobilní sítě karty SIM. Pokud jste v roamingu v jiné mobilní síti, pak se logicky budou údaje "Current MCC/MNC" a "SIM MCC/MNC" lišit.

Bluetooth

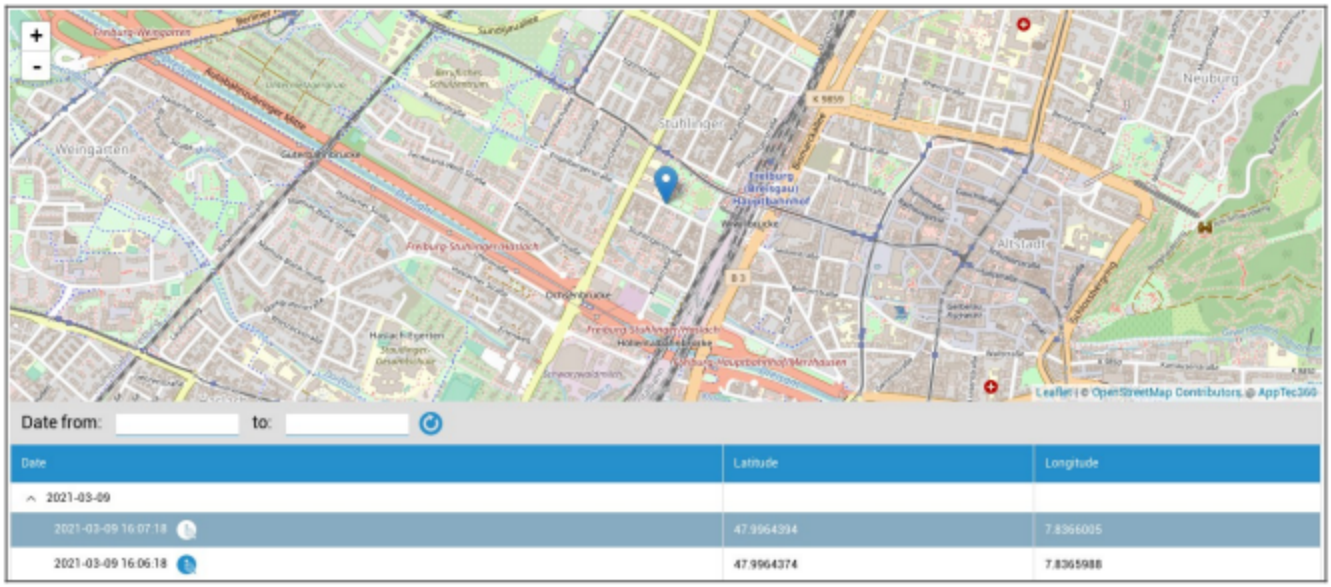
Bluetooth MAC	Adresa MAC Bluetooth

Správa zabezpečení

Ochrana proti krádeži (pouze na úrovni zařízení)

Informace GPS (pouze na úrovni zařízení)

Zde můžete zjistit aktuální/poslední umístění zařízení. Lokalizaci lze chránit jedním nebo dokonce dvěma hesly - viz: Přístup k GPS: - Obecná nastavení - Soukromí - Přístup k GPS



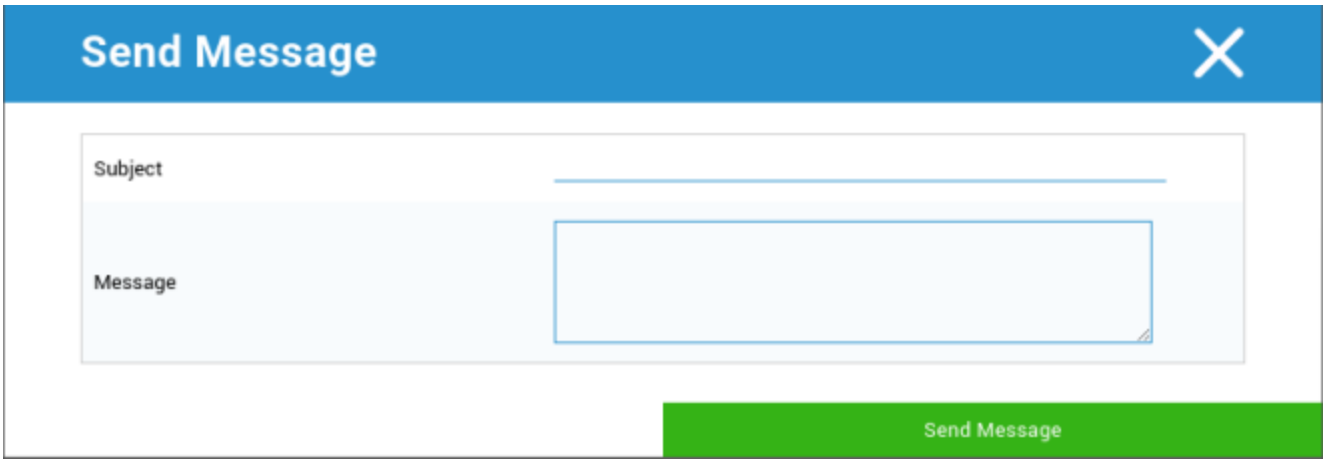
Vymazání a uzamčení (pouze na úrovni zařízení)

V části "Wipe & Lock" můžete provést následující tři akce:

Úplné otření	Zařízení je obnoveno do továrního nastavení (firemní i osobní údaje jsou smazány).
Podnikové utírání	Ze zařízení koncového uživatele jsou odstraněna pouze firemní data (všechny aplikace, data atd., které poskytla společnost AppTec360).
Zamykací obrazovka	Zámek obrazovky je aktivován, stačí zařízení odemknout pomocí hesla zařízení/PIN kódu.

Zpráva (pouze na úrovni zařízení)

Můžete vyplnit předmět a zprávu a odeslat ji na zařízení koncového uživatele. Tato zpráva se zobrazí v aplikaci AppTec360 Client.



Konfigurace zabezpečení

Přístupový kód

V části "Přístupový kód" můžete zadat heslo zařízení, k dispozici jsou následující možnosti nastavení.

Minimální délka hesla	stanovuje minimální počet symbolů, které musí heslo obsahovat.
Kvalita hesla	Síla hesla Nespecifikováno = není specifikováno Každé heslo je v pořádku = každé heslo je přijatelné alespoň číselné znaky = musí obsahovat alespoň číselné znaky. alespoň složené znaky = musí obsahovat alespoň speciální znaky. alespoň alfanumerické znaky = musí obsahovat alespoň alfanumerické znaky. alespoň abecední znaky = musí obsahovat alespoň abecední znaky.
Zámek maximální doby nečinnosti	Maximální časový limit obrazovky. Konfiguruje se pouze maximální hodnota, kterou může zvolit uživatel.
Minimální počet malých písmen v hesle	Minimální počet malých písmen v hesle
Minimální počet velkých písmen v hesle	Minimální počet velkých písmen v hesle
Minimální počet nepísmenných znaků požadovaných v hesle	Minimální počet nepísmenných znaků požadovaných v hesle
Minimální počet číslic požadovaných v hesle	Minimální počet číslic požadovaných v hesle
Minimální požadované symboly v hesle	Minimální požadované symboly v hesle
Časový limit vypršení platnosti hesla	stanoví, po uplynutí jakého časového intervalu heslo vyprší a musí být vydáno nové heslo.
Omezení historie hesel	Počet dříve použitých hesel, která nejsou povolena
Maximální počet neúspěšných pokusů o zadání hesla	Stanovuje, jak často může být heslo zadáno nesprávně, než dojde k úplnému vymazání zařízení.

Šifrování

V tomto bodě můžete šifrovat interní paměť zařízení i paměť karty SD.

Vyžadovat šifrování úložiště	Pokud je toto nastavení aktivováno, bude paměť zařízení šifrována, pokud zařízení tuto funkci podporuje. Jakmile je paměť zařízení poprvé zašifrována, není již možné ji odšifrovat. Stejně tak se zásady hesla automaticky přepnou na 6 alfanumerických symbolů.
Vyžadovat šifrování karty SD	Toto nastavení platí pouze pro zařízení Samsung! Pokud je toto nastavení aktivováno, může být externí karta SD zašifrována a její zašifrování lze zrušit pouze ručně v zařízení koncového uživatele. Stejně tak se zásady hesla automaticky přepnou na 6 alfanumerických symbolů.

AntiVirus

Povolením funkce AntiVirus se do zařízení nainstaluje program Ikarus. Upozorňujeme, že to vyžaduje samostatnou licenci, kterou lze zadat v Obecná nastavení → Správa aplikací → Aplikace třetích stran.

Automatické skenování	Definuje, zda má Ikarus skenovat automaticky a jak často má toto skenování provádět. Povolením možnosti "Úplná automatická kontrola" se provede úplná kontrola. V opačném případě se provede rychlé skenování
Automatické aktualizace	Povoluje automatické aktualizace virové databáze a nastavuje, jak často se mají provádět.
Ochrana aplikací	Kromě běžného skenování, které skenuje pouze soubory, umožňuje skenování aplikací.
Ochrana karty SD	Povoluje ochranu karty SD. Bez této funkce je skenování omezeno na místní úložiště.
Aktualizace pouze pro Wi-Fi	Omezení aktualizace na Wi-Fi

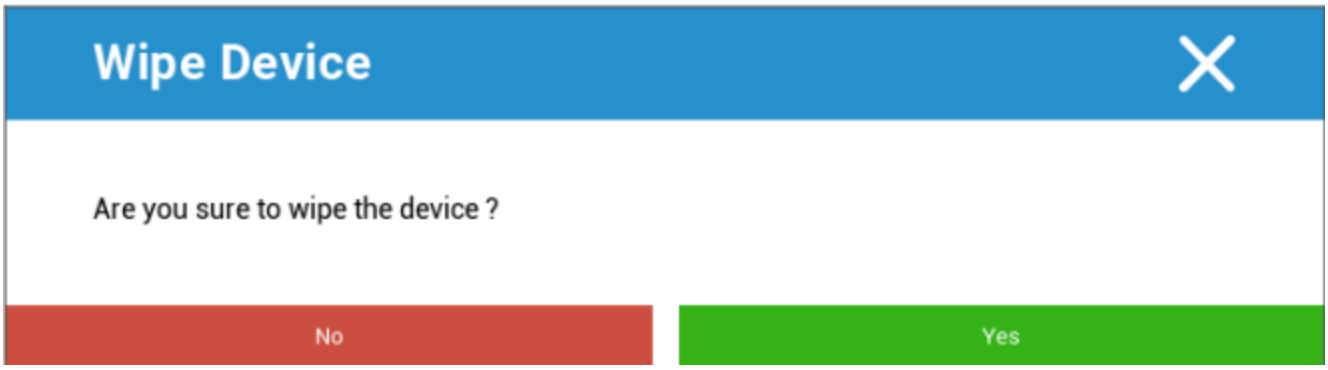
Konec životnosti (pouze na úrovni zařízení)

Vymazat (pouze na úrovni zařízení)

V části "Wipe" můžete obnovit tovární nastavení zařízení. Zde budou vymazána firemní i soukromá data v zařízení koncového uživatele.

Po kliknutí na "Symbol mínus" by se měla zobrazit následující zpráva.

Vymazat i kartu SD?	Vymaže se také paměť karty SD.



Pokud zvolíte "Ano", můžete provést vymazání.

V části "Wipe Report" lze zobrazit následující položky.

Setřeno	Historie toho, kdo stírání provedl
Datum	Datum
Stav	Stav (např. zda bylo vymazání provedeno úspěšně)

Nastavení omezení

Omezení

Zde lze omezit a zablokovat celou řadu věcí.

Povolit kameru	Povolení použití kamery
Vynutit automatickou synchronizaci	Vztahuje se k rozhraní "Synchronizace" Zapnuto = synchronizace je trvale aktivována. Vypnuto = synchronizace je trvale deaktivována. Uživatelská volba = zvolená uživatelem
Vynucení Bluetooth	Zapnuto = Bluetooth je trvale aktivováno Vypnuto = funkce Bluetooth je trvale deaktivována. Uživatelská volba = zvolená uživatelem
Force GPS	Zapnuto = GPS je trvale aktivováno Vypnuto = GPS je trvale deaktivováno. Uživatelská volba = zvolená uživatelem
Vynucení přesnosti polohy Google	Zapnuto = trvalá lokalizace na internetu Vypnuto = trvalá deaktivace lokalizace internetu Uživatelská volba = zvolená uživatelem

U zařízení Samsung s rozhraním KNOX 1.0 nebo vyšším jsou k dispozici následující možnosti nastavení.

Povolení karty SD	Povolení karty SD
Povolit zápis na kartu SD	Povolení "zápisu" na kartu SD
Povolit snímání obrazovky	Povolit snímání obrazovky
Povolit schránku	Povolit schránku
Zálohování nastavení a dat aplikací ve službě Google Cloud	Vypnuto = deaktivace zálohování Google Zapnuto = aktivace zálohování Google Volba uživatele = vybráno uživatelem
Povolení ladění USB	Povolit ladění USB (používá se například pro vytváření protokolů zařízení (ADB)).
Povolit Google Crash Report	Povolení odesílání hlášení o havárii Google z aplikací
Povolit obnovení továrního nastavení	Umožňuje uživateli obnovit tovární nastavení zařízení.
Povolení aktualizace OTA	Povolení aktualizací "Over-The-Air"
Povolení hostitelského úložiště USB	Pokud je aktivována, lze připojit paměť USB v podobě pevného disku nebo čtečky karet SD.
Povolení přehrávače médií USB (MTP,PTP)	Povolení přehrávače médií USB (MTP,PTP)
Povolit mikrofon	Zapnuto = povolení mikrofonu pro aplikace třetích stran Vypnuto = blokování mikrofonu pro aplikace třetích stran Volba uživatele = uživatelé si mohou vybrat, zda má aplikace třetí strany přístup k mikrofonu.
Povolení NFC (Near Field Communication)	Povolit NFC
Povolit neznámé zdroje (APK Sideloading)	Pokud je povoleno, je povoleno boční načítání aplikací (souborů APK). Jakmile je toto nastavení zakázáno, musí jej uživatel povolit ručně, když znovu povolíte instalaci souborů APK z neznámých zdrojů.
Povolit vytváření uživatelů	Umožňuje vytvoření více uživatelů

Vlastník zařízení AE

(Zařízení musí být v režimu vlastníka zařízení Android Enterprise) Doporučujeme vytvořit zařízení jako zařízení "Android Enterprise", nikoli jako zařízení "Android".

Zabezpečení	
Zakázat sdílení umístění	Určuje, zda je uživateli zakázáno zapnout sdílení polohy.
Zakázat nouzové spouštění	Určuje, zda uživatel nesmí restartovat zařízení do nouzového režimu spouštění.
Zakázat resetování sítě	Určuje, zda je uživateli zakázáno resetovat nastavení sítě z Nastavení.
Zakázat obnovení továrního nastavení	Určuje, zda je uživateli zakázáno resetovat zařízení.
Povolení ADB	Umožňuje připojení k počítači přes ADB
Zakázat funkci Keyguard	Zakáže funkci Keyguard
Informace o uzamčené obrazovce vlastníka zařízení	Nastaví informace o vlastníkovi zařízení, které se mají zobrazovat na zamykací obrazovce.
Prosazování shody	Režim Výzva uživateli - Uživatel bude vyzván k provedení potřebných akcí. Kontejner s uzamčeným režimem - Skrytí všech aplikací, dokud nejsou splněny všechny požadavky.

Správa aplikací	
Povolení propojení aplikací napříč profily	Umožňuje aplikacím v nadřazeném profilu zpracovávat webové odkazy ze spravovaného profilu.
Zakázat ovládání aplikací	Určuje, zda je uživateli zakázáno upravovat aplikace v Nastavení nebo spouštěčích.
Zakázat instalaci aplikací	Určuje, zda je uživateli zakázáno instalovat aplikace.
Zakázat odinstalování aplikací	Určuje, zda je uživateli zakázáno odinstalovávat aplikace.
Zásady oprávnění v době běhu	Určuje, jak budou zpracovávány nové požadavky na oprávnění od aplikací.
Povolit neznámé zdroje	Pokud je tato možnost povolena, mohou uživatelé načítat aplikace ze strany instalací souboru .apk.

Připojení	
Zakázat konfiguraci mobilní sítě	Určuje, zda je uživateli zakázáno konfigurovat mobilní sítě.
Zakázat konfiguraci tetheringu	Určuje, zda je uživateli zakázáno konfigurovat Tethering a přenosné hotspoty.
Zakázat konfiguraci VPN	Určuje, zda je uživateli zakázáno konfigurovat síť VPN.
Zakázat konfiguraci Wifi	Určuje, zda je uživateli zakázáno měnit přístupové body WiFi.
Zakázat odchozí paprsek NFC	Určuje, zda uživatel nesmí používat NFC k přenosu dat z aplikací.
Konfigurace uzamčení WiFi	Toto nastavení určuje, zda mají být konfigurace WiFi vytvořené aplikací Vlastník zařízení uzamčeny (tj. zda je může upravovat nebo odebírat pouze aplikace Vlastník zařízení, nikoli i aplikace Nastavení).
Povolení datového roamingu	Aktivace datového roamingu

Bluetooth	
Zakázat Bluetooth	Určuje, zda je v zařízení zakázáno připojení Bluetooth. Vyžaduje systém Android 8.0
Zakázat sdílení Bluetooth	Určuje, zda je v zařízení zakázáno odchozí sdílení Bluetooth. Vyžaduje systém Android 8.0
Zakázat konfiguraci Bluetooth	Určuje, zda je uživateli zakázáno konfigurovat bluetooth.

Správa účtů	
Zakázat přidání spravovaného profilu	Určuje, zda je uživateli zakázáno přidávat spravované profily. Vyžaduje Android 8.0
Zakázat přidávání uživatelů	Určuje, zda je uživateli zakázáno přidávat nové uživatele.
Zakázat odebrání spravovaného profilu	Určuje, zda lze spravované profily tohoto uživatele odstranit jinak než vlastníkem profilu. Vyžaduje Android 8.0
Zakázat změnu účtu	Určuje, zda je uživateli zakázáno přidávat a odebírat účty, pokud nejsou přidány programově nástrojem Authenticator.

Telefonování	
Zakázat odchozí hovory	Určuje, že uživatel nemá povoleno uskutečňovat odchozí telefonní hovory.
Zakázat SMS	Určuje, že uživatel nesmí odesílat ani přijímat zprávy SMS.

Systém	
Zakázat vytváření oken	Určuje, že kromě oken aplikace nemají být vytvářena jiná okna.
Zakázat nastavit ikonu uživatele	Určuje, zda uživatel nesmí měnit svou ikonu.
Zakázat nastavení tapety	Omezení uživatele, které zakáže nastavení tapety.
Zakázat stavový řádek	Vypnutím stavového řádku zablokujete oznámení, rychlá nastavení a další překryvy obrazovky, které umožňují útěk ze zařízení na jedno použití.
Povolení automatického času	Automaticky nastaví čas.
Povolení automatického časového pásma	Automaticky nastaví časové pásmo.
Zůstat zapnutý, když je připojen k síti	Zařízení zůstane aktivní, i když je připojeno ke zdroji napájení.

Úložiště	
Zakázat zakázat ověřování aplikací	Určuje, zda je uživateli zakázáno zakázat ověřování aplikací.
Zakázat připojení fyzických médií	Určuje, zda je uživateli zakázáno připojovat fyzická externí média.

Povolení služby zálohování	Služba zálohování spravuje všechny mechanismy zálohování a obnovení v zařízení. Nastavení této hodnoty na false zabrání zálohování nebo obnovení dat. Služba zálohování je ve výchozím nastavení vypnutá. Vyžaduje systém Android 8.0
Povolení velkokapacitního úložiště USB	Povoluje použití velkokapacitního úložiště USB.

Klávesnice	
Zakázat automatické vyplňování	Určuje, zda uživatel nesmí používat služby automatického vyplňování. Vyžaduje Android 8.0
Zakázat kopírování a vkládání mezi profily	Určuje, zda to, co je zkopírováno do schránky tohoto profilu, lze vložit do souvisejících profilů.

Zvuk	
Zakázat úpravu objemu	Určuje, zda je uživateli zakázáno upravovat hlavní hlasitost.
Zakázat vypnutí mikrofonu	Určuje, zda je uživateli zakázáno upravovat hlasitost mikrofonu.
Ztlumení zařízení	Ztlumení zařízení.

Zásady aktualizace systému	
Řízení aktualizací operačního systému	Povolením této možnosti nastavíte chování aktualizace na automatické, s oknem nebo odložené.

Kontejner BYOD

Android Enterprise

Android Enterprise

Povolení systému Android Enterprise	Povolte Android Enterprise (AE). AE je podporována od verze Android 5.1 a vyšší.
Prosazování shody	Režim Výzva uživateli - Uživatel bude vyzván k provedení potřebných akcí. Kontejner s uzamčeným režimem - Skrytí všech aplikací, dokud nejsou splněny všechny požadavky.
Zásady oprávnění v době běhu	Výzva uživateli k zadání nových požadavků na oprávnění Vždy vyhovět novým žádostem o povolení Vždy odmítnout nové žádosti o povolení Varování: Některé aplikace mají problémy s rozpoznáním oprávnění, pokud jsou nastavena automaticky. Pokud vždy udělujete oprávnění a narazíte na problémy s aplikacemi, které tvrdí, že oprávnění chybí, nastavte tuto možnost na "vyzvat uživatele" a aplikaci znovu nainstalujte.
Povolit odchozí schránku	Umožňuje kopírování a vkládání z vnitřku kontejneru na vnější stranu.
Povolení rozlišení ID volajícího	Zobrazí jméno příchozího hovoru na základě kontaktů v kontejneru.
Povolit rozlišení vyhledávání kontaktů	Umožňuje vyhledávat jména v kontejneru kontaktů při volání.
Povolení sdílení kontaktů Bluetooth	Umožňuje přístup ke kontaktu kontejneru v autě
Zakázat odchozí paprsek NFC	Zakázání funkce NFC pro kontejner
Povolit neznámé zdroje	Pokud je tato možnost povolena, mohou uživatelé načítat aplikace ze strany instalací souboru .apk.
Povolení ladění USB	Pokud je povoleno, mohou uživatelé povolit ladění USB.
Zakázat změnu účtu	Zakáže vytváření, mazání a úpravy účtů v kontejneru. Mějte na paměti, že některé aplikace potřebují vytvořit nebo upravit účty, aby fungovaly podle očekávání.

Výměna Gmail

Umožňuje konfigurovat službu Gmail v kontejneru. Upozorňujeme, že zapnutím této konfigurace nedojde k automatické instalaci aplikace. Tuto aplikaci musíte ještě přidat jako povinnou aplikaci.

E-mailová adresa	E-mailová adresa
Název hostitele serveru	Název hostitele serveru
Přihlašovací jméno	Přihlašovací jméno
Podpis	Podpis
Počet předchozích dnů k synchronizaci	Počet předchozích dnů k synchronizaci.
Identifikátor zařízení	Identifikátor EAS. Pokud to vaše prostředí nevyžaduje, nechte tuto položku prázdnou.
Použití protokolu SSL (Secure Sockets Layer)	Povoluje použití protokolu SSL. Zakázání této funkce může snížit zabezpečení
Přijmout všechny certifikáty	Přijímá všechny certifikáty. Povolení této funkce může snížit zabezpečení
Povolení nespravovaných účtů	Umožňuje uživateli přidávat další účty
Certifikát klienta	Nahrajte klientský certifikát, pokud to váš Exchange server vyžaduje.

Systémové aplikace AE

Zde můžete povolit systémové aplikace pro kontejner Android Enterprise. Mějte na paměti, že zadaná aplikace musí být v úložišti systému, jinak se nic nestane.

Přístupový kód kontejneru

Pouze pro systém Android 7.0 nebo vyšší

Umožňuje nastavit konkrétní požadavek na heslo pro kontejner.

Minimální délka hesla	stanovuje minimální počet symbolů, které musí heslo obsahovat.
Kvalita hesla	Síla hesla Nespecifikováno = není specifikováno Každé heslo je v pořádku = každé heslo je přijatelné alespoň číselné znaky = musí obsahovat alespoň číselné znaky. alespoň složené znaky = musí obsahovat alespoň speciální znaky. alespoň alfanumerické znaky = musí obsahovat alespoň alfanumerické znaky. alespoň abecední znaky = musí obsahovat alespoň abecední znaky.
Zámek maximální doby nečinnosti	Maximální doba do uzamčení kontejneru. Nastavuje se pouze maximální hodnota, kterou může zvolit uživatel.
Minimální počet malých písmen v hesle	Minimální počet malých písmen v hesle
Minimální počet velkých písmen v hesle	Minimální počet velkých písmen v hesle
Minimální počet nepísmenných znaků požadovaných v hesle	Minimální počet nepísmenných znaků požadovaných v hesle
Minimální počet číslic požadovaných v hesle	Minimální počet číslic požadovaných v hesle
Minimální požadované symboly v hesle	Minimální požadované symboly v hesle
Časový limit vypršení platnosti hesla	stanoví, po uplynutí jakého časového intervalu heslo vyprší a musí být vydáno nové heslo.
Omezení historie hesel	Počet dříve použitých hesel, která nejsou povolena
Maximální počet neúspěšných pokusů o zadání hesla	Určuje, jak často lze zadat heslo nesprávně, než se kontejner odstraní.

Samsung KNOX

Aktivace

Zde můžete povolit kontejner Samsung KNOX. Upozorňujeme, že tato funkce již není společností Samsung podporována v systému Android 10 a vyšším. Použití kontejneru Android Enterprise Container v systému Android 10 nebo novějším

Přístupový kód Knox

Stanovení pokynů týkajících se nastavení hesla zařízení

Minimální délka hesla	určuje, kolik symbolů musí heslo obsahovat.
Kvalita hesla	Síla hesla Každé heslo je v pořádku = Každé heslo je v pořádku Alespoň číselné znaky = musí být přítomno alespoň minimum číselných znaků. Alespoň složené znaky = musí být přítomno minimum speciálních znaků Alespoň alfanumerické znaky = musí být přítomno minimálně alfanumerických znaků. Alespoň abecední znaky = musí být přítomny minimálně abecední znaky.
Minimální požadovaný počet složitých znaků	Musí být přítomny minimálně složené znaky
Maximální časový limit nečinnosti	Maximální časový limit nečinnosti uživatele před uzamčením klávesnice
Povolit ověřování otiskem prstu	Povolení ověřování otisků prstů
Povolení ověřování pomocí duhovky	Povolení ověřování pomocí rozpoznávání duhovky
Maximální věk hesla	stanoví, po jaké době heslo vyprší a je třeba vydat nové heslo.
Historie uložených hesel	Počet bývalých hesel, která nejsou povolena
Maximální počet neúspěšných pokusů o zadání hesla	Stanovuje, jak často může být heslo zadáno nesprávně, než dojde k úplnému vymazání zařízení.

Knox Security

Omezení specifických funkcí zařízení

Povolit kameru	Povolení používání fotoaparátu
Povolení obchodu s aplikacemi Samsung KNOX	Povolení používání obchodu Samsung KNOX App Store

Povolení služeb Google Play	Povolení služeb Google Play
Povolit prohlížeč	Povolit používání nativního prohlížeče
Povolit snímky obrazovky	Povolit vytváření snímků obrazovky
Povolit import kontaktů	Pokud je aktivována, je povolen přístup ke kontaktům zařízení z kontejneru KNOX.
Povolit export kontaktů	Pokud je aktivována, je povolen přístup ke kontaktům KNOX ze zařízení.
Povolit import kalendáře	Pokud je aktivována, je povolen přístup ke kalendáři zařízení z kontejneru KNOX.
Povolit export kalendáře	Pokud je aktivována, je povolen přístup do kalendáře KNOX ze zařízení.
Povolení nezabezpečené klávesnice	Povolení používání nezabezpečené klávesnice
Povolit import souborů	Povolení importu souborů do kontejneru KNOX
Povolit export souborů	Povolení exportu souborů z kontejneru KNOX

Knox Exchange

Zde můžete nakonfigurovat profil Exchange pro kontejner KNOX.

E-mailová adresa	Poskytnutá e-mailová adresa uživatele Všimněte si "zástupných symbolů", které můžete použít pro práci s pověřeními a neprovádíte změny ručně na každém zařízení. Kliknutím na **Zobrazit zástupné symboly** si je můžete sami zobrazit.
Název hostitele serveru	Adresa serveru serverů Exchange
Přihlašovací jméno	Přihlašovací jméno pro příslušné zařízení koncového uživatele, zde si prosím všimněte také "zástupných znaků".
Doména	Adresa domény
Heslo (pouze na úrovni zařízení)	Volitelně lze jednotlivému zařízení zadat heslo, pokud zůstane prázdné, bude uživatel vyzván k zadání hesla Exchange.
Počet předchozích dnů k synchronizaci	Počet dní, které určují, kdy se e-maily synchronizují zpět.
Podpis	Lze připojit podpis
Výchozí účet	stanoví, že tento e-mailový účet je standardním účtem.
Použití protokolu SSL (Secure Sockets Layer)	Použití připojení SSL
Použití protokolu TLS (Transport Layer Security)	Použití připojení TLS
Přijmout všechny certifikáty	Přijímají se všechny certifikáty. Tuto možnost vyberte, pokud váš Exchange Server používá certifikát s vlastním podpisem.

Knox eMail

E-mailová adresa	Poskytnutá e-mailová adresa uživatele Všimněte si "zástupných symbolů", které můžete použít pro práci s pověřeními a neprovádíte změny ručně na každém zařízení. Kliknutím na **Zobrazit zástupné symboly** si je můžete sami zobrazit.
Protokol příchozího serveru	Protokol příchozího serveru IMAP nebo POP
Adresa příchozího serveru	Adresa příchozího serveru
Příchozí port serveru	Příchozí port serveru
Přihlašovací jméno/uživatelské jméno příchozího serveru	Přihlašovací jméno/uživatelské jméno příchozího serveru
Heslo příchozího serveru	Heslo příchozího serveru
Příchozí server používá protokol SSL	Příchozí server používá protokol SSL
Příchozí server používá TLS	Příchozí server používá TLS
Příchozí server přijímá všechny certifikáty	Příchozí server přijímá všechny typy certifikátů
Protokol odchozího serveru	Protokol odchozího serveru SMTP
Port odchozího serveru	Port odchozího serveru
Odchozí server používá další pověření	Další pověření pro odchozí server. Pokud je tato možnost nastavena na "vypnuto", použije se nastavení příchozího serveru.
Přihlašovací jméno/uživatelské jméno odchozího serveru	Přihlašovací jméno/uživatelské jméno odchozího serveru
Heslo odchozího serveru	Heslo odchozího serveru
Odchozí server používá protokol SSL	Odchozí server používá protokol SSL
Odchozí server používá TLS	Odchozí server používá TLS
Odchozí server přijímá všechny certifikáty	Odchozí server přijímá všechny typy certifikátů
Podpis	Zde lze připojit podpis

Upozornit uživatele na přijetí nového e-mailu	Upozornit uživatele na přijetí nového e-mailu

Knox Apps

Zde vytvořte aplikace, které chcete distribuovat do zařízení koncových uživatelů. Ty pak budou k dispozici v kontejneru KNOX. Chcete-li přidat aplikaci, postupujte stejně jako v nabídce Povinné aplikace

Název aplikace	Název aplikace
Povinné od	Časový okamžik, kdy byla aplikace přidána
Zdroj:	Zdroj aplikace (Obchod Play | Vlastní)

Kliknutím na symbol lze příslušnou aplikaci opět odebrat.

Správa připojení

Wifi

Pro toto nastavení proveďte předběžnou konfiguraci zařízení koncového uživatele pro přístup k interním přístupovým bodům.

Identifikátor sady služeb (SSID)	SSID sítě, která má být připojena.
Skrytá síť	Aktivovat v případě, že přístupový bod nevysílá SSID.
Typ zabezpečení	Stanovení typu zabezpečení přístupového bodu

Typ zabezpečení

WEP

Heslo	Heslo pro přístupový bod

WPA/WPA2

Heslo	Heslo pro přístupový bod

802.1x EAP

Metoda EAP	

PWD	Identita	Identita
	Heslo	Heslo

PEAP	Protokol ověřování fáze 2	žádné	Žádný další protokol
		MSCHAPV2	Protokol MSCHAPV2
		GTC	Protokol GTC
	Certifikát certifikační autority	Certifikát certifikační autority	
	Identita	Identita	
	Anonymní identita	Anonymní identita	
	Heslo	Heslo	

Metoda EAP	

TTLS	Protokol ověřování fáze 2	žádné	Žádný další protokol
		PAP	Protokol PAP
		MSCHAP	Protokol MSCHAP
		MSCHAPV2	Protokol MSCHAPV2
		GTC	Protokol GTC
	Certifikát certifikační autority	Certifikát certifikační autority	
	Identita	Identita	
	Anonymní identita	Anonymní identita	
	Heslo	Heslo	

TLS	Certifikát certifikační autority	Certifikát certifikační autority
	Identita	Identita
	Heslo	Heslo

VPN

Typ připojení	**Vytvoření typu připojení VPN**

Pokud jako typ VPN vyberete možnost "Per-App VPN", změní se dostupní klienti VPN. Funkce Per-App VPN omezuje VPN na určité aplikace a automaticky spouští připojení VPN, pokud je spuštěna určitá aplikace.

Klient VPN AppTec360	Používá klienta AppTec360 VPN v kombinaci s univerzální bránou.
Název připojení	Název připojení VPN
Konfigurace brány	Vyberte konfiguraci VPN univerzální brány
Vždy zapnutá síť VPN	Vynutí, aby byla síť VPN vždy aktivní, takže veškerý provoz prochází přes síť VPN.
Povolení nativního uzamčení	Zablokuje veškerá síťová připojení, pokud zařízení není připojeno k síti VPN. Tuto funkci používejte opatrně, protože při nesprávné konfiguraci může dojít k úplné ztrátě připojení. Pouze pro systém Android Enterprise se systémem Android 7 nebo vyšším
Povolení uzamčení AppTec360	Blokuje používání všech aplikací, dokud není spuštěno připojení k síti VPN.

Cisco AnyConnect	
Název připojení	Název připojení VPN
Server	Adresa serveru
Režim certifikátu	Disabled = deaktivováno Automatic = automatický

L2TP (pouze KNOX)	K dispozici pouze v zařízeních Samsung
Název připojení	Název připojení
Server	Adresa serveru
Povolení protokolu L2TP Secret	
Vyhledávání domén DNS	Vyhledávání domén DNS

Typ připojení	**Vytvoření typu připojení VPN**

PPTP (pouze KNOX)	K dispozici pouze v zařízeních Samsung
Název připojení	Název připojení VPN
Server	Adresa serveru
Povolení šifrování	Povolení šifrování
Vyhledávání domén DNS	Vyhledávání domén DNS

L2TP / IPSec PSK (pouze KNOX)	K dispozici pouze v zařízeních Samsung
Název připojení	Název připojení VPN
Server	Adresa serveru
Předsdílený klíč IPSec	Předem sdílený klíč pro ověřování
Povolení protokolu L2TP Secret	
Tajemství protokolu L2TP	
Vyhledávání domén DNS	Vyhledávání domén DNS

IPSec XAuth PSK (pouze KNOX)	K dispozici pouze v zařízeních Samsung
Název připojení	Název připojení VPN
Server	Adresa serveru
Identifikátor IPSec	Uživatelské jméno pro připojení
Předsdílený klíč IPSec	Heslo pro připojení
Vyhledávání domén DNS	Vyhledávání domén DNS

OpenVPN	
Název připojení	Název připojení

Profil OpenVPN	Zde je místo, kam se zkopíruje obsah souboru .ovpn
Aplikace OpenVPN	Existují dvě různé aplikace pro používání OpenVPN Doporučujeme aplikaci "OpenVPN pro Android". Alternativně lze použít aplikaci "OpenVPN Connect".

Omezení

Zde můžete nastavit omezení týkající se správy připojení.

Povolení datového roamingu	Povolení mobilních dat při roamingu
Vynucení datového roamingu	Pokud je aktivován, je roaming pro mobilní data trvale aktivován (nedoporučuje se!). Toto nastavení přepíše nastavení "Povolit datový roaming"!
Následující nastavení jsou k dispozici pouze v systému Samsung KNOX 2.0 nebo vyšším.	
Povolit pouze tísňová volání	Povolit pouze tísňová volání
Povolit Wi-Fi	Povolit Wi-Fi
Minimální úroveň zabezpečení sítě WiFi	Minimální úroveň zabezpečení sítě WiFi Otevřený = všechny typy WiFi jsou povoleny
Zakázat uživateli přidávat sítě WiFi	Uživatel nesmí sám přidat síť WiFi Toto nastavení je možné pouze v případě, že byl profil WiFi definován v části "Správa připojení".
Povolení SMS a MMS	All = Veškerý provoz SMS a MMS je povolen. Pouze příchozí SMS = povoleny jsou pouze příchozí SMS zprávy. Pouze odchozí SMS = povoleny jsou pouze odchozí SMS zprávy. Žádný = není povolen žádný provoz SMS / MMS.
Povolit synchronizaci během roamingu	Povolit synchronizaci během roamingu Zapnuto = aktivováno Vypnuto = deaktivováno Volba uživatele = volba uživatele
Povolení hlasového roamingu	Povolení hlasového roamingu Zapnuto = aktivováno Vypnuto = deaktivováno Volba uživatele = volba uživatele
Použití systémového serveru http Proxy	Použití proxy serveru HTTP, který je k dispozici v nastavení systému, závisí na připojené síti (WiFi nebo APN).

APN

Následující nastavení jsou k dispozici pouze v systému Samsung SAFE 2.0 nebo vyšším!

Zobrazovaný název APN	Zobrazovaný název APN	
Název přístupového bodu	Název APN	
Protokol odchozího serveru	Není nastaveno	
	Žádné	
	PAP	Protokol PAP
	CHAP	Protokol CHAP
	PAP nebo CHAP	Protokol PAP nebo CHAP
MCC - Kód země mobilního telefonu	Zde se zadává MCC, pokud se má použít MCC vložené SIM karty, nechte toto pole prázdné.	
MNC - Kód mobilní sítě	Zde se zadává MNC, pokud se má použít MCC vložené karty SIM, nechte toto pole prázdné.	
Adresa serveru	Adresa serveru	
Číslo portu serveru	Číslo portu serveru	
Adresa proxy serveru	Adresa proxy serveru	
Adresa serveru MMS	Adresa serveru MMS, pro standardní ponechte prázdnou.	
Číslo portu MMS	Číslo portu MMS	
Adresa proxy serveru MMS	Adresa proxy serveru MMS	
Uživatelské jméno	Uživatelské jméno	
Heslo	Heslo	
Typ přístupového bodu	Povolené typy jsou: "default", "mms", "supl" Pokud toto pole zůstane prázdné, použije se "default,supl,mms".	
Preferované APN	Upřednostňuje se APN	

Bluetooth

Zde lze provádět různá nastavení Bluetooth.

Následující nastavení jsou k dispozici pouze v systému Samsung KNOX 1.0 nebo vyšším!

Povolit zjišťování zařízení přes Bluetooth	Povolení zjišťování zařízení přes Bluetooth
Povolení párování Bluetooth	Povolení párování Bluetooth
Povolení zařízení Bluetooth Headset	Povolení zařízení Bluetooth Headset
Povolení zařízení Bluetooth Hands-free	Povolení zařízení Bluetooth Hands-free
Povolení zařízení Bluetooth A2DP	Povolení streamování zvuku Bluetooth A2DP mezi zařízeními
Povolení odchozích hovorů	Povolení odchozích hovorů přesBT
Povolení přenosu dat přes Bluetooth	Povolení přenosu dat přes Bluetooth
Povolení tetheringu Bluetooth	Umožňuje používat zařízení jako modem (připojení k internetu přes Bluetooth)
Povolení připojení k počítači přes Bluetooth	Povolení připojení k počítači přes Bluetooth

Správa PIM

Výměna

K dispozici pouze pro Samsung KNOX 1.0 nebo vyšší!

E-mailová adresa	Poskytnutá e-mailová adresa uživatele Všimněte si "zástupných symbolů", které můžete použít pro práci s pověřeními a neprovádíte změny ručně na každém zařízení. Kliknutím na **Zobrazit zástupné symboly** si je můžete sami zobrazit.
Název hostitele serveru	Adresa serveru serverů Exchange
Přihlašovací jméno	Přihlašovací jméno pro příslušné zařízení koncového uživatele, všimněte si prosím také "Placeholders here".
Doména	Adresa domény
Heslo (pouze na úrovni zařízení)	Volitelně lze jednotlivému zařízení zadat heslo, pokud zůstane prázdné, bude uživatel vyzván k zadání hesla Exchange.
Počet předchozích dnů k synchronizaci	Počet dní, které určují, kdy se e-maily synchronizují zpět.
Podpis	Lze připojit podpis (Tip: některá zařízení vyžadují formátování podpisu v HTML).
Výchozí účet	stanoví, že tento poštovní účet je standardním účtem.
Použití protokolu SSL (Secure Sockets Layer)	Použití připojení SSL
Použití protokolu TLS (Transport Layer Security)	Použití připojení TLS
Přijmout všechny certifikáty	Přijímají se všechny certifikáty. Tuto možnost vyberte, pokud váš Exchange Server používá certifikát s vlastním podpisem.

eMail

Zde můžete distribuovat účty IMAP a POP do příslušných zařízení koncových uživatelů.

Následující nastavení jsou k dispozici pouze v systému Samsung KNOX 1.0 nebo vyšším!		
E-mailová adresa	Poskytnutá e-mailová adresa uživatele Všimněte si "zástupných symbolů", které můžete použít pro práci s pověřeními a neprovádíte změny ručně na každém zařízení. Kliknutím na **Zobrazit zástupné symboly** si je můžete sami zobrazit.	
Protokol příchozího serveru	Protokol příchozího serveru	IMAP oder POP
Adresa příchozího serveru	Adresa příchozího serveru	
Příchozí port serveru	Příchozí port serveru	
Přihlašovací jméno/uživatelské jméno příchozího serveru	Přihlašovací jméno/uživatelské jméno příchozího serveru	
Heslo příchozího serveru (pouze na úrovni zařízení)	Heslo příchozího serveru (pouze na úrovni zařízení)	
Příchozí server používá protokol SSL	Příchozí server používá protokol SSL	
Příchozí server používá TLS	Příchozí server používá TLS	
Příchozí server přijímá všechny certifikáty	Příchozí server přijímá všechny typy certifikátů	
Protokol odchozího serveru	Protokol odchozího serveru	SMTP
Port odchozího serveru	Port odchozího serveru	
Odchozí server používá další pověření	Další pověření pro odchozí server. Pokud je nastaveno na "off", použije se nastavení příchozího serveru.	
Přihlašovací jméno/uživatelské jméno odchozího serveru	Přihlašovací jméno/uživatelské jméno odchozího serveru	
Heslo odchozího serveru (pouze na úrovni zařízení)	Heslo odchozího serveru	
Odchozí server používá protokol SSL	Odchozí server používá protokol SSL	
Odchozí server používá TLS	Odchozí server používá TLS	

Odchozí server přijímá všechny certifikáty	Odchozí server přijímá všechny typy certifikátů
Podpis	Podpis můžete připojit zde (Tip: Některá zařízení vyžadují formátování podpisu ve formátu HTML).
Upozornit uživatele na přijetí nového e-mailu	Upozorní uživatele na přijetí nového e-mailu

AE Gmail Exchange

Informace: Tato konfigurace se použije pro aplikaci Gmail. Musíte tedy schválit a nainstalovat aplikaci Gmail.

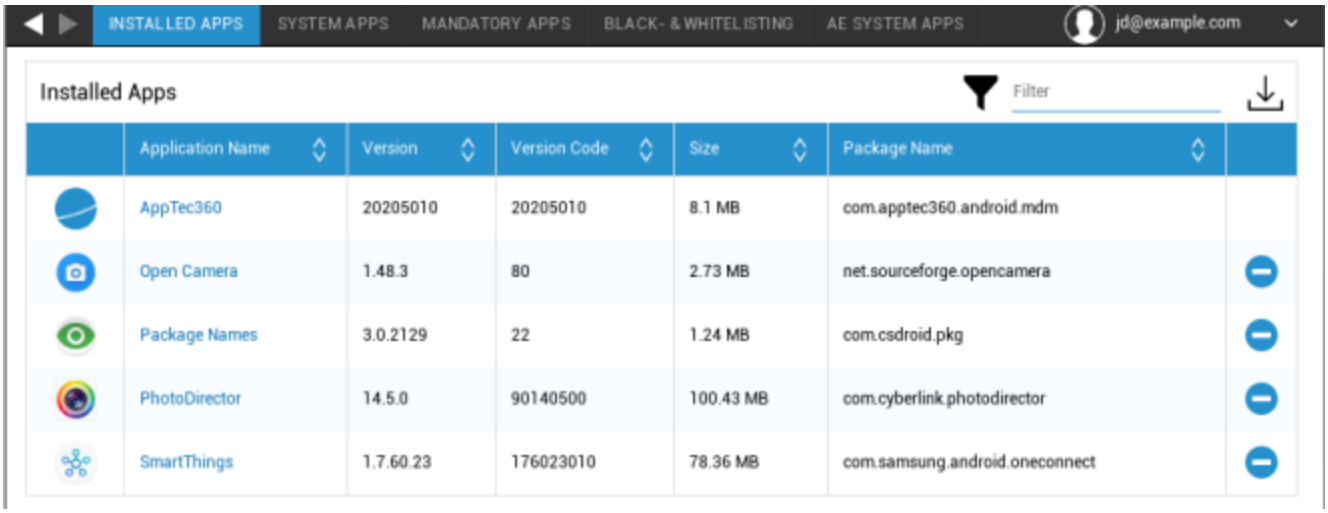
E-mailová adresa	Poskytnutá e-mailová adresa uživatele Všimněte si "zástupných symbolů", které můžete použít pro práci s pověřeními a neprovádíte změny ručně na každém zařízení. Kliknutím na Zobrazit zástupné symboly si je můžete sami zobrazit.
Název hostitele serveru	Adresa serveru serverů Exchange
Přihlašovací jméno	Přihlašovací jméno pro příslušné zařízení koncového uživatele, všimněte si prosím také "Placeholders here".
Podpis	Lze připojit podpis (Tip: některá zařízení vyžadují formátování podpisu v HTML).
Počet předchozích dnů k synchronizaci	Počet dní, které určují, kdy se e-maily synchronizují zpět.
Identifikátor zařízení	Identifikátor EAS. Pokud to vaše prostředí nevyžaduje, nechte tuto položku prázdnou.
Použití protokolu SSL (Secure Sockets Layer)	Použití připojení SSL
Přijmout všechny certifikáty	Přijímají se všechny certifikáty. Tuto možnost vyberte, pokud váš Exchange Server používá certifikát s vlastním podpisem.
Povolení nespravovaných účtů	Umožňuje uživateli přidávat další účty
Certifikát klienta	Nahrajte klientský certifikát, pokud to váš Exchange server vyžaduje.

Správa aplikací

Správce podnikových aplikací

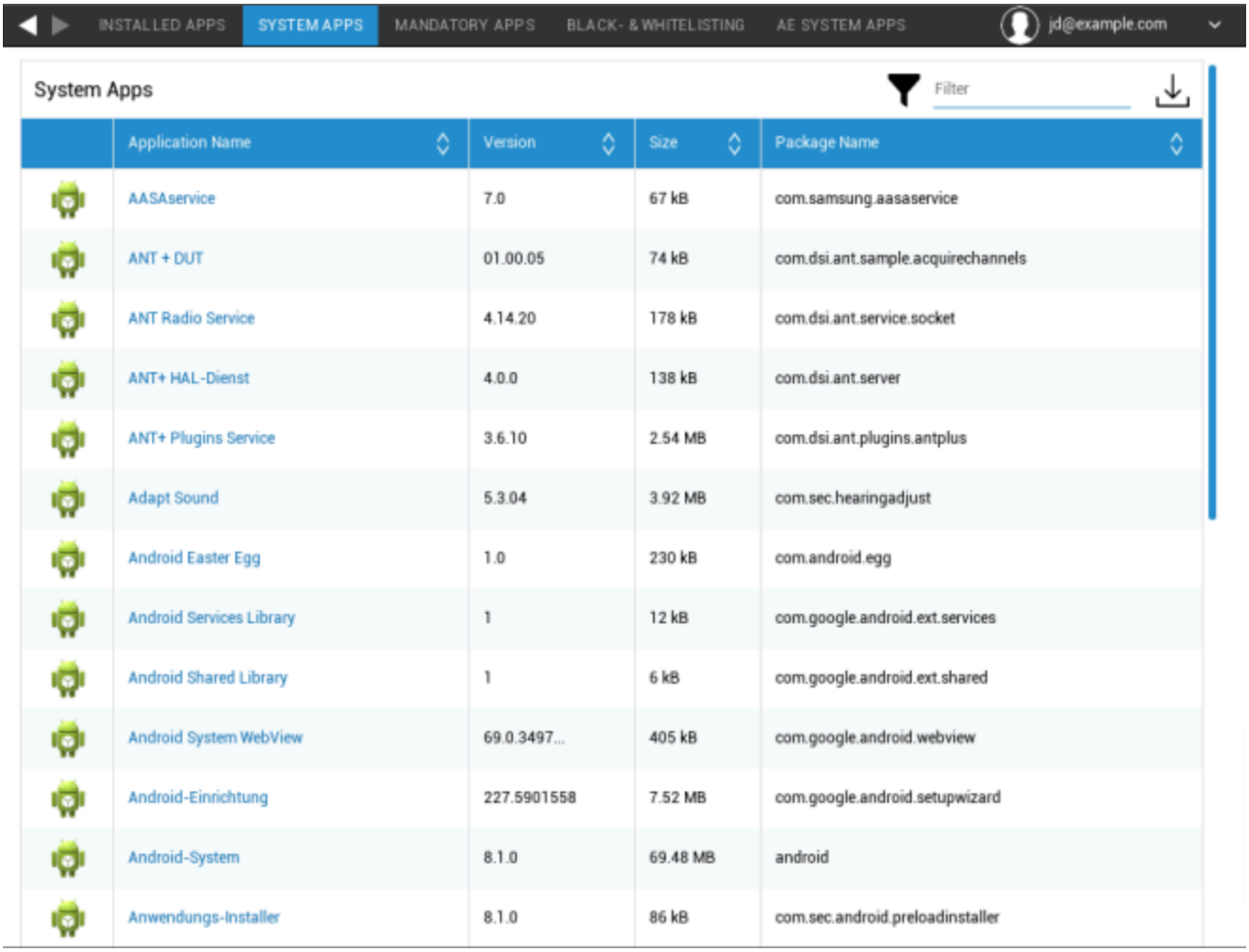
Nainstalované aplikace (pouze na úrovni zařízení)

Zde se vám zobrazí všechny aplikace, které jsou aktuálně nainstalovány v zařízení koncového uživatele.


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

Systémové aplikace (pouze na úrovni zařízení)

V části "Systémové aplikace" se zobrazí seznam všech předinstalovaných systémových aplikací s jejich názvem a verzí.



Povinné aplikace

V části Povinné aplikace můžete definovat, které aplikace musí být v zařízení nainstalovány. V závislosti na konfiguraci a zařízení se aplikace nainstalují automaticky nebo bude uživatel vyzván k jejich instalaci.

Upozorňujeme, že pro snadnou správu aplikací se doporučuje používat Android Enterprise.

Scénáře jsou uvedeny níže:

Běžné aplikace v Obchodě Play

Instalace aplikací v obchodě Playstore vždy vyžadují interakci uživatele. Kromě toho musí být v zařízení nakonfigurován účet Google.

Instalace aplikací InHouse

V zařízeních Samsung se tyto aplikace nainstalují v tichosti. Jedinou výjimkou je kontejner, u kterého musí uživatel instalaci potvrdit.

V ostatních případech musí uživatel instalaci aplikace potvrdit.

Aplikace pro Android Enterprise Play Store

Tyto aplikace se vždy instalují tiše, bez interakce uživatele.

Chcete-li přidat povinnou aplikaci, klikněte na tlačítko "+" a vyberte požadovanou aplikaci ze seznamu. Upozorňujeme, že aplikace z karty "Obchod Google Play" nelze instalovat, pokud je zařízení nakonfigurováno se systémem Android Enterprise jako plně spravované nebo jako kontejner.

Pokud používáte systém Android Enterprise, vyberte aplikace v sekci "AE Play Store". Aby zde byly aplikace dostupné, potvrďte je v obchodě Google Enterprise Play tak, že přejdete do Obecná nastavení → AE Play Store → Play Store Apps.

Při odebrání povinné aplikace dojde také k jejímu odinstalování ze zařízení.

V seznamu povinných aplikací můžete kliknout na název aplikace a přejít na kartu "konfigurace" a aplikaci nakonfigurovat. To vyžaduje použití systému Android Enterprise a aplikace to musí podporovat. Dostupné možnosti proto závisí na vybrané aplikaci.

Systémové aplikace AE

Zde můžete povolit systémové aplikace pro zařízení Android Enterprise. Mějte na paměti, že zadaná aplikace musí být v úložišti systému, jinak se nic nestane. 296

Omezení a nastavení

Černá a bílá listina

Zde můžete definovat černou nebo bílou listinu. Všechny aplikace na černé listině budou blokovány. Všechny aplikace, které nejsou na bílé listině, budou blokovány. Prázdný blacklist neblokuje nic, zatímco prázdný whitelist blokuje vše*.

**Všechny povinné aplikace a aplikace z podnikového obchodu s aplikacemi budou automaticky zařazeny na bílou listinu. Nemusíte je přidávat ručně.*

Po kliknutí na tlačítko "+" můžete buď vyhledat aplikaci, kterou chcete přidat na černou nebo bílou listinu, nebo zadat název balíčku ručně.

Omezení aplikací systému

V části "Omezení systémových aplikací" můžete mimo jiné blokovat předinstalované aplikace a služby podle vlastního uvážení.

Zakázat prohlížeč	Zakázat standardní prohlížeč
Zakázat kalendář	Zakázat nativní kalendář
Zakázat kalkulačku	Zakázat kalkulačku
Zakázat prohlížeč Chrome	Zakázat prohlížeč Chrome
Zakázat hodiny	Vypnutí hodin
Zakázat kontakty	Zakázat kontakty
Zakázat dialer	Zakázat nativní dialer
Zakázat elektronickou poštu	Zakázat e-mail
Zakázat Exchange	Zakázání účtů Exchange
Zakázat Facebook	Zakázání aplikace Facebook
Zakázat galerii	Zakázání nativní aplikace galerie
Zakázat službu Gmail	Zakázat službu Gmail
Zakázat službu Knihy Google	Zakázat službu Knihy Google
Zakázání služby Google Play Kiosek	Zakázání služby Google Play Kiosek
Zakázat Mapy Google	Zakázat Mapy Google
Zakázání služby Google Music	Zakázání služby Google Music
Zakázání služby Google Movies	Zakázání služby Google Movies
Zakázání obchodu Google Play	Zakázání obchodu Google Play (veřejný obchod App Store)
Zakázat službu Google Plus	Zakázat službu Google Plus
Zakázat vyhledávání Google	Zakázat vyhledávání Google
Zakázání služby Google Talk / Google Hangouts	Zakázání služby Google Talk / Google Hangouts
Zakázat přehrávač hudby	Zakázání nativní aplikace pro přehrávání hudby
Zakázat nastavení	Zakázat nastavení zařízení
Zakázat Sim Toolkit	Zakázání služeb sady Sim Toolkit
Zakázat SMS / MMS	Zakázat SMS / MMS
Zakázat službu Street View	Vypnutí služeb Street View
Zakázat službu Youtube	Zakázat službu Youtube

Aplikace Samsung

V části "Samsung Apps" můžete definovat další nastavení a/nebo omezení pro zařízení Samsung.

Zakázání služby AllShare Play / Samsung Link	Zakázání služby AllShare Play / Samsung Link
Zakázat službu ChatON	Zakázat službu ChatON
Zakázat Game Hub	Zakázat Game Hub
Zakázat skupinovou hru	Zakázat skupinovou hru
Zakázat nápovědu	Zakázat nápovědu Samsung
Zakázat KNOX	Zakázání kontejneru Samsung KNOX
Zakázat poznámku	Zakázat hlasovou poznámku
Zakázat Moje soubory	Zakázat Moje soubory
Zakázat optickou čtečku	Zakázat optickou čtečku
Zakázat službu Polaris Office	Zakázat službu Polaris Office
Zakázat Readers Hub / Samsung Books	Zakázat Readers Hub / Samsung Books
Zakázat funkci S Memo	Zakázání aplikace Samsung Memo
Zakázat překladatele S	Zakázání aplikace Samsung Translator
Zakázat funkci S Voice	Vypnutí hlasového asistenta S
Zakázání aplikací Samsung	Zakázání obchodu Samsung App Store
Zakázání služby Samsung Hub	Zakázání obchodů Samsung Entertainment Stores
Zakázat přehrávač videa	Zakázat přehrávač videa
Zakázat hlasový záznamník	Zakázat hlasový záznamník
Zakázat službu WatchON	Zakázat funkci WatchON (simuluje dálkové ovládání)

Aplikace Huawei

V části "Huawei Apps" můžete definovat další nastavení a/nebo omezení zařízení Huawei.

Zakázat DLNA	Zakázat DLNA
Zakázat instalátor aplikací	Zakázat instalátor aplikací
Zakázat Správce souborů	Zakázat Správce souborů
Zakázat Správce zálohování	Zakázat Správce zálohování
Zakázat aktualizaci systému	Zakázat aktualizaci systému
Zakázat box s nástroji	Zakázat box s nástroji
Zakázat počasí	Zakázat počasí
Vypnutí rádia FM	Vypnutí rádia FM

Nastavení správy aplikací

Zde můžete definovat chování aktualizací InHouse Apps.

Frekvence kontroly aktualizací určuje, jak často aplikace AppTec360 vyhledává aktualizace pro aplikace InHouse. Jakmile je zjištěna nová verze, je stažena a nainstalována.

Prahová hodnota Wi-Fi určuje, zda má být stahování omezeno na připojení Wi-Fi, pokud je aplikace větší než nastavená prahová hodnota. Pokud je menší nebo prahovou hodnotu nedefinujete, aplikace se bude stahovat v síti Wi-Fi i v mobilní síti.

Obchod s podnikovými aplikacemi

Upozorňujeme, že přidání aplikací zde (Enterprise App Store) NEZAMĚŘÍ na jejich automatickou instalaci do zařízení. Uživatel musí otevřít Enterprise App Store v zařízení a nainstalovat aplikaci ručně.

Pokud chcete do zařízení automaticky instalovat aplikace, přejděte na "Správa aplikací" → "Správce podnikových aplikací" → "Povinné aplikace" a přidejte požadované aplikace.

V tomto bodě můžete uživatelům distribuovat volitelné aplikace.

Obchod Playstore

Kliknutím na "+" přidáte aplikaci do obchodu Play. Pokud používáte systém Android Enterprise, přejděte na "App Management Enterprise Play Store". Uvědomte si také, že pro instalaci zde definovaných aplikací musí být na → zařízení nakonfigurován účet Google.

In-House

V bodě "In-House" můžete nahrávat a distribuovat interně vyvinuté aplikace.

Kliknutím na "+" přidáte aplikaci InHouse do podnikového obchodu s aplikacemi, kterou si pak uživatel může nainstalovat. V tomto dialogu můžete také nahrát novou aplikaci InHouse.

Obchod Play pro podniky

Upozorňujeme, že přidání aplikací zde (Obchod Play) NEZAMĚŘÍ na jejich automatickou instalaci do zařízení. Uživatel musí otevřít Obchod Play v zařízení a nainstalovat aplikaci ručně.

Pokud chcete do zařízení automaticky instalovat aplikace, přejděte na "Správa aplikací" → "Správce podnikových aplikací" → "Povinné aplikace" a přidejte požadované aplikace.

V tomto bodě můžete uživatelům distribuovat volitelné aplikace.

Zde můžete přidávat aplikace do obchodu Android Enterprise Playstore. Vezměte prosím na vědomí, že je třeba schválit Aplikace v Obecná nastavení → AE Play Store → Play Store Apps. Tyto Aplikace budou přidány do běžného obchodu Google Play.

Uvědomte si také, že nejprve musíte definovat Rozložení s aplikacemi v Obecná nastavení → Správa aplikací → Obchod AE Play → Rozložení obchodu.

Před úspěšným přidáním aplikací do obchodu musí být aplikace v Rozložení.

Režim kiosku a spouštěč

Režim kiosku

Režim Kiosek umožňuje předem definovat aplikaci nebo adresu URL. Pak bude možné spustit/navštívit výhradně tuto aplikaci nebo adresu URL.

Stejně tak lze různá hardwarová tlačítka deaktivovat v režimu Kiosk Mode.

Automatické spuštění	Automatické spuštění režimu Kiosk, jakmile profil dorazí do zařízení koncového uživatele.
Plánovaný režim kiosku?	Můžete naplánovat čas pro režim kiosku, který se pak automaticky spustí a ukončí ve vámi nastavený čas.
Čas zahájení	Čas zahájení
Čas v minutách	Doba v minutách, po které by měl být režim kiosku opět ukončen.

Typ aplikace

Jednotlivá aplikace	Pokud chcete aplikaci spustit v režimu kiosku, vyberte možnost "Package" v části "Application Type".
Aplikace kiosku	Klikněte sem a vyberte aplikaci, která má být spuštěna v režimu kiosku. Najdete zde obvyklý přehled správy aplikací. Můžete si vybrat mezi "Google Play Store", "Android In-House Apps" a "Packagename".

Typ aplikace

ADRESA URL	Chcete-li v režimu kiosku spustit adresu URL, vyberte v části "Typ aplikace" možnost "URL". Pak definujte požadovanou adresu URL
Vymazání prohlížeče po nečinnosti	Zde můžete definovat časový interval v minutách, po kterém se má režim kiosku znovu spustit.
Vymazání webové mezipaměti a souborů cookie	Pokud tuto funkci aktivujete, po restartu režimu Kiosek se vymaže webová mezipaměť (soubory cookie a obrázky v mezipaměti).
Zásady stejného původu	Pokud je tato funkce aktivní, může uživatel procházet pouze podstránky definované adresy URL. Například jste definovali následující adresu URL:www.mypage.com Uživatel pak může surfovat na adrese: www.mypage.com/subpage.
Adresy URL na bílé listině	Zde můžete udržovat bílou listinu, všechny tyto adresy URL jsou povoleny. Maximálně 1 adresa URL na řádek Adresa URL musí začínat http:/ nebo https://.
Adresy URL na černé listině	Zde můžete udržovat černou listinu, všechny tyto adresy URL nejsou povoleny. Maximálně 1 adresa URL na řádek Adresa URL musí začínat http:/ nebo https://.
Orientace obrazovky	Toto nastavení se týká úprav obrazovky Automatic = automatický Portrét = vertikální formát Krajina = režim na šířku

Aplikace Multi App	Pokud vyberete režim kiosku "Multi App", bude vynuceno použití spouštěče AppTec360.
Aplikace	Použití: Jako aplikaci pro kiosek vyberte aplikaci z obchodu Playstore nebo vlastní aplikaci. Je také možné zadat název balíčku. Vybraná Kiosková aplikace musí být v zařízení nainstalována. Nezapomeňte nastavit Kioskovou aplikaci jako povinnou. Zkratka na domovské obrazovce: Pokud je nastaveno na "Zapnuto", vytvoří se zástupce na domovské obrazovce. Pokud je nastaveno na "Vypnuto", aplikace se bude stále zobrazovat v seznamu aplikací.

Heslo pro ukončení povoleno	Pokud tuto funkci aktivujete, je možné, aby uživatel ukončil režim kiosku pomocí vámi předem definovaného hesla.
Heslo pro ukončení	Toto je heslo, které jste předem definovali.
Automatické sbalení stavového řádku	Pokud je tato možnost povolena, stavový řádek se automaticky podbarví. S touto možností mohou uživatelé vidět informace na stavovém řádku, ale nemají přístup k jeho funkcím.
Zakázat stavový řádek	Stavový řádek obsahuje Oznámení, Zkratky a Informace. K dispozici pouze pro zařízení Samsung s funkcí KNOX 1.0 nebo vyšší.
Zakázat klávesy hlasitosti	Zakázat tlačítka hlasitosti (dostupné pouze v zařízeních Samsung s funkcí KNOX 1.0 nebo vyšší)
Vypnutí vypínače	Vypnutí přepínače zapnuto/vypnuto (k dispozici pouze v zařízeních Samsung s KNOX 1.0 nebo vyšší verzí)
Zakázat tlačítko Domů	Zakázat tlačítko Domů. Pokud je tato funkce aktivována, lze režim kiosku ukončit pouze v konzoli AppTec360. (k dispozici pouze v zařízeních Samsung s funkcí KNOX 1.0 nebo vyšší)
Zakázat navigační panel	Pomocí této funkce můžete vypnout navigační panel (Zpět / Menu). Pokud je tato funkce aktivována, lze režim kiosku ukončit pouze v konzoli AppTec360. (k dispozici pouze v zařízeních Samsung s funkcí KNOX 1.0 nebo vyšší)

Nastavení aktualizace aplikace	
Povolení aktualizací aplikací	Uživatelé budou vyzváni k provedení aktualizací aplikací, i když je aktivní režim Kiosek. Na zařízeních se Samsung KNOX budou aplikace aktualizovány v tichosti.
Okno aktualizace	Nastavte interval, ve kterém budou uživatelé vyzváni k instalaci aktualizací aplikací.

TeamViewer	
Povolení bezobslužného přístupu	Pokud je tato možnost povolena, mohou správci zařízení vzdáleně ovládat bez interakce s uživatelem. V zařízení musí být nainstalována aplikace TeamViewer Host.

Spouštěč AppTec360

Povolení spouštěče AppTec360	Na: AppTec360 Launcher se zapne. Uživatel jej musí jednorázově nastavit jako výchozí spouštěč. Poznámka: Pokud je povolen režim kiosku a režim kiosku je nastaven na "Multi App", bude vynuceno použití spouštěče AppTec360.
Velké ikony	Na: Zobrazí větší verzi ikon aplikací v Launcheru.
Skrýt ikonu aplikace AppTec360	Na: Zcela skryje aplikaci AppTec360
Skrytí ikony obchodu AppTec360	Na: Úplně skryje AppTec360 Enterprise AppStore.

Nastavení AppTec360

Povolení aplikace AppTec360 Settings	Aplikace AppTec360 Settings umožňuje ovládat připojení WiFi a Bluetooth.
Povolení nastavení v aplikaci Multi App Režim kiosku	Pokud je tato možnost povolena, mohou uživatelé přistupovat k aplikaci AppTec360 Settings, když je aktivní režim Multi App Kiosk Mode.

Dálkové ovládání

Splashtop

Zobrazuje aktuální stav nastavení Splashtop. Zde se zobrazí kroky, které je třeba provést pro vzdálený přístup k zařízení prostřednictvím Splashtop. Zde je také třeba zadat kód pro nasazení, který můžete získat na webových stránkách Splashtop. Deploy kód je nutný pro připojení k zařízení.

Teamviewer

Zobrazuje aktuální stav nastavení aplikace Teamviewer. Zde se zobrazí kroky, které je třeba provést pro vzdálený přístup k zařízení prostřednictvím aplikace Teamviewer.

Správa obsahu

Obsahové pole

Zde můžete povolit pole Obsah pro toto zařízení. Po aktivaci se do zařízení nainstaluje aplikace Contentbox.

Zabezpečený prohlížeč

Zde můžete povolit zabezpečený prohlížeč pro toto zařízení. Po aktivaci se do zařízení nainstaluje aplikace Zabezpečený prohlížeč. Tento prohlížeč lze nakonfigurovat tak, aby v zařízení nabízel webový prohlížeč, který je omezen podle vašich potřeb.

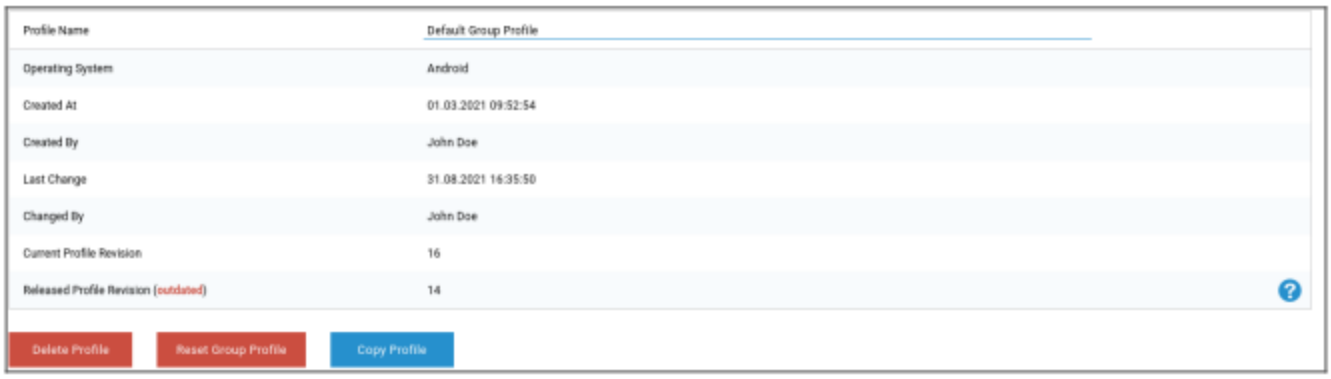
Vyžadovat heslo	Požadovat, aby si uživatel nastavil a používal heslo pro přístup k prohlížeči.
Omezit stahování / Otevřít v	Blokuje stahování z webových stránek
Omezení nahrávání	Omezuje nahrávání na určité adresy URL. Nezadejte žádnou adresu URL, abyste zcela zablokovali nahrávání.
Povolit kopírování	Povolení kopírování, vyřezávání nebo sdílení textu uvnitř webových stránek.
Povolit snímání obrazovky	Umožňuje pořizování snímků obrazovky.
Frekvence čištění dat	Zvolte, s jakou frekvencí se mají automaticky odstraňovat VŠECHNA uživatelská data (historie, mezipaměť atd.).
Záložky společnosti	Záložky se zobrazí ve složce "Firemní záložky" v záložkách prohlížeče. Uživatel je nemůže upravovat.
Skrytí adresního řádku	Skryje adresní řádek, takže uživatel nevidí navštívenou adresu URL.
Whitelisting v prohlížeči (bez univerzální brány)	Povoluje whitelisting adres URL na straně klienta. - Firemní záložky jsou vždy zařazeny na bílou listinu - Podporováno pouze pro 100 URL - Pro neomezený black- a whitelisting použijte univerzální bránu.
Černá a bílá listina založená na bráně	Černá listina má následující požadavky: - Fungující univerzální brána AppTec360 ("Obecná nastavení" → "Univerzální brána") - Fungující konfigurace VPN se zadaným serverem DNS ("Obecná nastavení" → "Univerzální brána" → "Nastavení VPN") - Konfigurace blacklistu ("Obecná nastavení" → "Univerzální brána" → "Blacklist domén") - Platné připojení VPN v profilu ("Správa připojení" → "VPN").

Konfigurace počítače se systémem Windows 10

Obecné

Přehled profilu skupiny (pouze na úrovni skupiny)

Po otevření profilu skupiny se zobrazí rychlý přehled profilu.



Název profilu	Název profilu (zde lze změnit)
Operační systém	Operační systém, pro který je profil určen
Vytvořeno v	Čas vytvoření
Vytvořil	Tvůrce profilu
Poslední změna	Čas poslední změny profilu
Změněno podle	Účet, který provedl poslední změny
Aktuální revize profilu	Revize uloženého stavu profilu
Vydaná revize profilu	Přiřazená revize profilu ("Assign now"). Pokud se za textem na štítku zobrazí " (zastaralý)", znamená to, že jste profil uložili, ale ještě jste ho nepřiřadili, takže zařízení budou stále dostávat starší verzi.

Přehled zařízení (pouze na úrovni zařízení)

Souhrnný přehled zařízení, který obsahuje následující údaje:

Název počítače	Název počítače
Klient	Zařízení typu Windows
Poslední známé místo	Zeměpisná šířka a délka posledního známého umístění zařízení.
Přiřazené povinné aplikace	Počet povinných aplikací přiřazených zařízení
UID POČÍTAČE	UID počítače
Vydání pro operační systém	Zobrazuje edici systému Windows
Verze operačního systému	Aktuálně nainstalovaná verze systému Windows
Sestavení operačního systému	Aktuální sestavení systému Windows
Operační systém	Aktuálně nainstalovaný operační systém
Sériové číslo	Sériové číslo zařízení
Vlastnictví zařízení	Nakonfigurovaný typ vlastnictví
Typ zařízení	Typ zařízení
Zakořeněný	Zobrazuje, zda je zařízení rootnuté
V souladu s předpisy	Zobrazuje, zda je zařízení kompatibilní
Naposledy viděno	Datum a čas, kdy byly v profilu provedeny změny.
Přiřazení uživatele	Zobrazuje uživatele nebo skupinu, ke které je toto zařízení aktuálně přiřazeno. Zařízení můžete přesunout výběrem jiného uživatele nebo skupiny z rozevíracího seznamu.

Nastavení

Povolit automatickou aktualizaci	Povolit nebo zakázat automatické aktualizace systému os.

Revize konfigurace (pouze na úrovni zařízení)

Zde získáte přehled o tom, který skupinový profil je k zařízení přiřazen.

Pokud kliknete na profil skupiny, dostanete se přímo do profilu a můžete provést nastavení.

Pomocí symbolu můžete vrátit přiřazené aplikace do nastavení skupinového profilu.

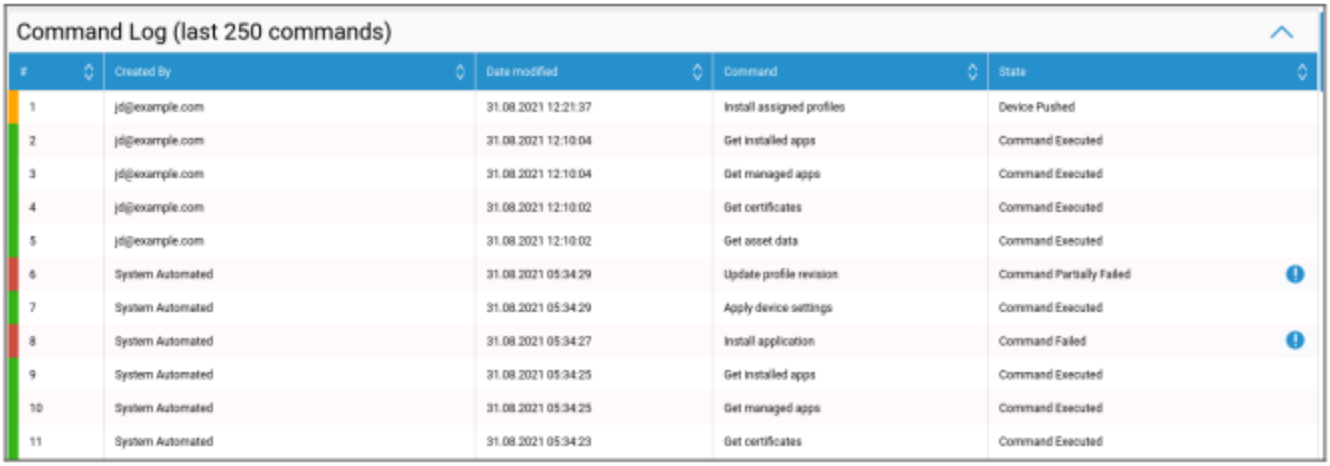
Pomocí symbolu můžete obnovit profil zařízení tak, aby neměl žádné nastavení.

"K dispozici je novější revize" znamená, že profil skupiny byl změněn a uložen, ale nebyl přiřazen. Profil skupiny je třeba přiřadit pomocí "Přiřadit nyní" na úrovni skupiny, aby se změny uplatnily na zařízení.

Protokol zařízení (pouze na úrovni zařízení)

Protokol příkazů

Zde můžete zjistit, které příkazy byly pro zařízení vydány a jaký je jejich stav.



Příkazy vytvořené pomocí "System Automated" jsou automaticky vytvořeny systémem.

Možné stavy příkazů

Stlačené zařízení	Službě push (např. APNS) byl odeslán požadavek na připojení, aby se zařízení připojilo zpět k serveru EMM.
Vytvořený příkaz	Příkaz byl vytvořen v systému.
Odeslaný příkaz	Příkaz byl odeslán do zařízení po jeho připojení k serveru.
Spuštěný příkaz	Příkaz byl úspěšně proveden.
Příkaz se nezdařil	Příkaz se nezdařil. *
Příkaz částečně selhal	V závislosti na operačním systému zařízení mohou být některé příkazy seskupeny. V tomto některé části této skupiny příkazů selhaly. *
Příkaz proveden, případně neúspěšný	Příkaz byl proveden, ale možná nebyl.
Přesunutí příkazu	Příkaz byl znovu odeslán uživatelem.
Vyřazené	Příkaz byl vyřazen. Například proto, že byl nahrazen jiným příkazem nebo že zařízení bylo znovu zapsáno a staré příkazy byly odstraněny.

*Pokud je za zprávou vykřičník, můžete získat další informace, když na ikonu najedete kurzorem.

Správa aktiv (pouze na úrovni zařízení)

Informace o zařízení

Výrobce	Výrobce zařízení
Model	Model zařízení
Číslo modelu	Číslo modelu
Operační systém	Operační systém
Verze operačního systému	Verze operačního systému
Sériové číslo	Sériové číslo
ExchangeID	ExchangeID
Celková paměť RAM	Celková paměť RAM
Rozlišení displeje	Rozlišení displeje
Jazyk telefonu	Jazyk zařízení
Verze firmwaru	Verze firmwaru
Verze klienta DM	Verze klienta pro správu zařízení
Verze hardwaru	Verze hardwaru zařízení
Architektura procesoru	Architektura CPU (typ procesoru)

Cellular

Síť operátora SIM	Síť dopravců
Telefonní číslo	Telefonní číslo
Stav roamingu	Stav roamingu
IMEI	IMEI
IMSI	IMSI
Firmware modemu	Firmware modemu

Informace o synchronizaci

Okamžité připojení k DM	Zařízení by mělo okamžitě vytvořit spojení s aplikací AppTec.
Počáteční doba opakování	Počáteční doba opakování pro toto první připojení
Opakování připojení	Počet pokusů o nové připojení po odpojení od Správce připojení nebo chybě na úrovni WinInetu
Maximální doba spánku	Maximální doba spánku po chybě při odesílání balíčku
První opakování synchronizace	Čas pro první fázi po zápisu
Interval prvního opakování	Čas pro první fázi po zápisu
Druhé opakování synchronizace	Čas pro druhou fázi po zápisu
Druhý interval opakování	Čas pro druhou fázi po zápisu
Pravidelné opakování synchronizace	Čas pro další fáze po zápisu
Pravidelný interval opakování	Čas pro další fáze po zápisu

Správa zabezpečení

Ochrana proti krádeži (pouze na úrovni zařízení)

Informace GPS (pouze na úrovni zařízení)

Zde můžete zjistit aktuální/poslední umístění zařízení. Lokalizaci lze chránit jedním nebo dokonce dvěma hesly - viz: "Obecná nastavení" > "Soukromí" > "Přístup k GPS".

Nastavení GPS

Povolení sledování GPS	Povolte pravidelnou synchronizaci informací GPS.
Interval sledování	Nastavení intervalu synchronizace informací GPS.

Konfigurace zabezpečení

Přístupový kód

Minimální délka hesla	Minimální délka hesla	
Složení hesla	Určuje počet specifických znaků, které musí heslo obsahovat. Tvoří je velká písmena, malá písmena, číslice a speciální symboly.	
Kvalita hesel	Zde můžete nastavit kvalitu hesla	
	Alfanumerické	Pouze čísla a písmena
	Číselné	Pouze čísla
	Číselné nebo alfanumerické	Čísla nebo čísla a písmena
Maximální doba nečinnosti	Počet minut nečinnosti uživatele na zařízení, po kterých bude zařízení uzamčeno. Po uplynutí této doby musí uživatel zařízení odemknout zadáním hesla k zařízení.	
Vypršení platnosti hesla	Nastavení doby, do které je třeba nastavit nové heslo.	
Omezení historie hesel	Počet dříve použitých hesel, která nejsou povolena	
Maximální počet neúspěšných pokusů o zadání hesla	Kolikrát lze heslo zadat nesprávně, než dojde k úplnému vymazání zařízení.	

Antivirus

Nastavení antiviru - Nastavení konfigurace skenování	
Typ skenování	Vybírá, zda se má provést rychlé nebo úplné skenování.
Nastavení začátku skenování	Vybírá denní dobu, kdy má program Windows Defender zahájit kontrolu.
Frekvence skenování	Výběr dne, kdy má být spuštěna kontrola systému Windows Defender.
Frekvence aktualizace podpisu	Určuje interval v hodinách, který se použije pro kontrolu podpisů.

Konfigurace typu souborů pro skenování	
Povolit skenování archivních souborů	Povolit nebo zakázat skenování archivů (například .zip) při přístupu k nim.
Povolit skenování skriptů	Povolí nebo zakáže funkci Skenování skriptů programu Windows Defender.
Povolení skenování e-mailů	Povolit nebo zakázat skenování e-mailů.
Povolení skenování síťových souborů	Povolit nebo zakázat skenování síťových souborů.
Povolení úplného skenování mapovaných síťových jednotek	Povolit nebo zakázat skenování mapovaných síťových jednotek (povoleno pouze při zapnutém úplném skenování).
Řízení obousměrného skenování	Řídí, které sady souborů mají být sledovány.
Povolení úplného skenování vyměnitelných jednotek	Povolit nebo zakázat úplné skenování vyměnitelných jednotek. Pouze při spuštění úplného skenování.

Typ souborů, které mají být vyloučeny ze skenování	
Ignorování typů souborů pro skenování	Definovat sadu typů přípon souborů. Každá přípona souboru pro každé pole.
Ignorování cest k adresářům	Definujte sadu cest k adresářům, abyste je nemuseli skenovat. Na každé pole připadá jedna cesta. Příklady: "C:\Example", "C:\Windows" nebo "C:\Users".
Vyloučení procesů ze skenování	Vyloučení souborů, které byly otevřeny určitými procesy, z antivirových kontrol programu Microsoft Defender. . Jedna cesta pro každé pole. Příklady: "C:\myFile.exe", "C:\Windows\myProcess.exe", "C:\myScript.bat".

Další nastavení	
Povolit sledování v reálném čase	Povolení nebo zakázání funkce Sledování v reálném čase programu Windows Defender
Povolit sledování chování	Povolení nebo zakázání funkce Sledování chování systému Windows
Povolení ochrany v cloudu	Povolit nebo zakázat programu Windows Defender odesílat společnosti Microsoft informace o jakémkoli nalezeném problému. Společnost Microsoft tyto informace analyzuje, zjistí více o problému, který se týká zařízení, a nabídne lepší řešení.
	Chování při zasílání vzorků
Povolení ochrany IOAV programu Windows Defender	Povolení nebo zakázání ochrany IOAV programu Windows Defender
Povolení přístupu k uživatelskému rozhraní Defenders "On Access protection"	
Průměrný faktor zatížení procesoru	Představuje průměrný faktor zatížení procesoru při kontrole systému Windows Defender (v procentech).

Zpracování škodlivého softwaru	
Nízká závažnost	Pro každou úroveň závažnosti můžete definovat, jak má zařízení zacházet se škodlivým softwarem. K dispozici jsou tyto možnosti: • Clean • Karanténa • Odstranění stránky • Povolit • Definováno uživatelem • Blok
Střední závažnost	
Vysoká závažnost	
Závažnost	
Dny pro uchování vyčištěného malwaru	Doba ve dnech, po kterou budou soubory/položky v karanténě uloženy v systému. Výchozí hodnota je 0, která ponechává položky v karanténě a automaticky je neodstraňuje. Maximální hodnota je 90.

Bezpečnostní centrum

Centrum zabezpečení systému Windows - Nastavení zabezpečení systému Windows	
Vypnutí uživatelského rozhraní ochrany proti virům a hrozbám	
Skrýt uživatelské rozhraní pro obnovu dat Ransomware	
Zakázat uživatelské rozhraní ochrany účtu	
Vypnutí brány firewall a uživatelského rozhraní ochrany sítě	
Zakázat ovládání aplikací a uživatelského rozhraní prohlížeče	
Zakázat změny v ochraně proti zneužití	Zakázat uživateli provádět změny v nastavení ochrany proti zneužití
Zakázat uživatelské rozhraní zabezpečení zařízení	
Skrytí řešení problémů s čipem TPM	Skrytí nastavení pro řešení problémů s čipem TPM
Zakázat tlačítko Clear TPM	
Zakázání uživatelského rozhraní výkonu a stavu zařízení	
Zakázat možnosti rodiny Uživatelské rozhraní	

Přizpůsobení přípitků	
Povolení přizpůsobených informací o podpoře	Povolení zobrazení přizpůsobených kontaktních informací podpory pro vaši společnost v pravém dolním rohu aplikace centra zabezpečení.
E-mailová adresa	Nastavení e-mailové adresy společnosti
Název společnosti	Nastavení názvu společnosti
Firemní telefon	Nastavení telefonu společnosti
Adresa URL nápovědy	Nastavení adresy URL nápovědy společnosti

Další nastavení	
Zakázat oznámení	Zakázat zobrazování oznámení Centra zabezpečení systému Windows Defender.
Skrýt doporučení pro aktualizaci firmwaru čipu TPM	Skrytí doporučení aktualizovat firmware čipu TPM, pokud je zjištěn zranitelný firmware.
Zobrazení názvu společnosti a možností kontaktu	Zobrazení názvu společnosti a možností kontaktu na vyjíždějící kartě kontaktu v Centru zabezpečení systému Windows Defender.
Skrýt Secure Boot	Skrytí oblasti Security Boot.
Skrýt ovládání oblasti oznámení zabezpečení	Skrytí ovládacího prvku oznamovací oblasti Zabezpečení systému Windows.

Konfigurace brány firewall

Konfigurace brány firewall - Globální nastavení	
Ignorovat nastavené ověřování	Ignorovat celou sadu ověřování, pokud nepodporují všechny sady ověřování uvedené v sadě.
Typ řazení paketů do fronty	Určuje, jakým způsobem je povoleno škálování softwaru na straně příjmu pro šifrovaný příjem a pro scénář tunelové brány IPsec.
Zakázat provádění stavového filtrování FTP	Pokud je vypnuta, neprovádí stavové filtrování protokolu FTP (File Transfer Protocol), které by umožnilo sekundární připojení.
Doba nečinnosti sdružení zabezpečení	Toto pole konfiguruje dobu nečinnosti sdružení zabezpečení v sekundách. Sdružení zabezpečení se odstraní poté, co se po tuto dobu neobjeví žádný síťový provoz.
Kódování předsdíleného klíče	Nastavení kódování předsdíleného klíče
Výjimky IPSec	Konfigurace výjimek internetového protokolu
Kontrola seznamu odvolaných certifikátů	

Profily brány firewall (profil domény / soukromý profil / veřejný profil)	
Povolení brány firewall pro tento profil	
Zakázat oznámení	Zakázat zobrazování oznámení uživateli, když je aplikaci zablokováno naslouchání na portu.
Blokování jednosměrových odpovědí na vícesměrové vysílání	
Vynucování autorizovaných pravidel brány firewall pro aplikace	Pokud není vynuceno, jsou pravidla autorizované aplikační brány firewall v místním úložišti ignorována a nejsou vynucována.
Vynucení globálních pravidel brány firewall pro porty	Pokud není vynuceno, jsou globální pravidla brány firewall portů v místním úložišti ignorována a nejsou vynucována. Nastavení má význam pouze tehdy, je-li nastaveno nebo vyjmenováno v úložišti zásad skupiny nebo je-li vyjmenováno z GroupPolicyRSoPStore
Vynucování pravidel brány firewall	Pokud není vynuceno, pravidla brány firewall z místního úložiště jsou ignorována a nejsou vynucována.
Vynucování pravidel zabezpečení připojení	Pokud není vynuceno, pravidla zabezpečení připojení z místního úložiště jsou ignorována a nejsou vynucována.
Výchozí odchozí akce	Akce, kterou brána firewall ve výchozím nastavení provádí u odchozích připojení.
Výchozí příchozí akce	Akce, kterou brána firewall ve výchozím nastavení provádí u příchozích připojení.
Zakázat režim Stealth	Režim Stealth je mechanismus brány Windows Firewall, který pomáhá zabránit škodlivým uživatelům zjistit informace o síťových počítačích a službách, které jsou na nich spuštěny.
Zakázat zabránění odpovědi na nevyžádaný provoz	Pokud je zakázáno, nesmí pravidla brány firewall pro skrytý režim bránit hostitelskému počítači v odpovědi na nevyžádaný síťový provoz, pokud je tento provoz zabezpečen protokolem IPsec.

Pravidla brány firewall

Pravidla brány firewall	
Název	Název pravidla
Popis	Popis pravidla
Akce	Určete, zda toto pravidlo bude přenos blokovat, nebo povolovat. Vezměte prosím v úvahu, že možnost Blokovat může také blokovat provoz (v závislosti na zbytku konfigurace) mezi serverem MDM a zařízením.
Směr	
Povolit procházení okraje (dostupné pouze v případě, že je položka **Směr** nastavena na **příchozí provoz**)	Označuje, že určitý příchozí provoz je povolen tunelovat přes NAT a další okrajová zařízení pomocí tunelovací technologie Teredo.

Programy a služby	
Definice aplikací, vše jinak	Pokud není povoleno, budou brány v úvahu všechny aplikace.
Název rodiny balíčků	Název rodiny schránek, na kterou se pravidlo vztahuje.
Cesta k souboru aplikace	Úplná aplikace, například C:\Windows\System\Notepad.exe, na kterou se pravidlo vztahuje.
Plně kvalifikovaný binární název	Plně kvalifikovaný binární název, na který se pravidlo vztahuje. FQBN je řetězec v následujícím tvaru: Vydavatel\Produkt\Filename,Verze} je ve tvaru: {Vydavatel\Produkt\Filename,Verze}.
Název služby	Zadejte název služby (např. "EventLog"). Seznam názvů služeb v prostředí Powershell získáte příkazem "Get-Service".

Protokoly a porty				
Protokol	Protokol používaný pravidlem.			
	Dostupné hodnoty: - Jakýkoli - Vlastní - HOPORT - ICMPv4 - IGMP - TCP - UDP - IPv6 - IPv6-Route - IPv6-Frag - GRE - ICMPv6 - IPv6-NoNxt - IPv6-Opts - VRRP - PGM - L2TP	Při nastavení na hodnotu Vlastní	Vložte číslo protokolu v rozsahu 0 až 255	Číslo protokolu
		Při nastavení na TCP nebo UDP	Zadejte místní porty, jinak budou použity všechny.	Místní porty, které bude pravidlo používat, povoleny jsou také porty rozsahu.
			Místní přístav	Jeden port nebo řada portů. Např. 100-120,200,300-320.
			Zadejte vzdálené porty, jinak budou použity všechny.	Vzdálené porty, které bude pravidlo používat, povoleny jsou také porty rozsahu.
			Vzdálený port	Jeden port nebo řada portů. Např. 100-120,200,300-320.

Oblast působnosti	
Zadejte místní IP, jinak libovolnou IP	Sada místních IP adres, může to být i rozsah IP adres oddělených znakem -
Místní IP adresa	Sada jednotlivých IP adres nebo rozsah IP adres oddělených znakem -
Zadejte vzdálené IP adresy, jinak libovolnou vzdálenou IP adresu.	Zadejte sadu vzdálených IP adres, může to být i rozsah IP adres oddělených znakem "-".
Vzdálená IP adresa	Zadání jednotlivých IP adres nebo rozsahu IP adres
Žetony	Tokeny, které lze nastavit spolu se vzdálenými adresami. Tokeny Intranet, RmtIntranet a Ply2Renders jsou podporovány v systému Windows 10, verze 1809 a novější.

Rozšířená nastavení	
Určete profily, jinak budou použity všechny.	Pokud je zakázáno, použijí se všechny profily
Doména	Profil domény
Soukromé	Soukromý profil
Veřejnost	Veřejný profil
Určete rozhraní, jinak se použijí všechna.	Pokud je zakázáno, budou použita všechna rozhraní
Místní síť	Rozhraní místní sítě
Vzdálený přístup	Rozhraní vzdáleného přístupu
Bezdrátové připojení	Bezdrátové rozhraní

Místní ředitelé	
Přidání autorizovaných místních uživatelů	Umožňuje přidat seznam místních uživatelů, kteří budou toto pravidlo používat.
Autorizovaní uživatelé	Seznam oprávněných místních uživatelů pro toto pravidlo. Uživatel musí být ve formátu SDDL (Security Description Definition language), např. PC_NAME\USERNAME. Toto pole nesmí být vyplněno, pokud je pro použití tohoto pravidla nastaven název služby.

Nastavení omezení

Funkčnost zařízení

Povolení karty SD	Povolení použití karty SD
Povolit kameru	Povolení používání fotoaparátu
Povolit službu určování polohy	Povolení služby určení polohy zařízení
Povolení bočního načítání aplikací	Povolit instalaci aplikací z neznámých zdrojů
Povolit režim pro vývojáře	Umožňuje režim pro vývojáře
Povolení mobilního datového roamingu	Povolení roamingu mobilních dat
Povolit Cortanu	Povolení hlasové asistentky Cortana
Povolit vyhledávání pomocí polohy	Povolit vyhledávání pomocí polohy
Povolení přidání e-mailového účtu jiného než Microsoft	Určete, zda je uživateli povoleno přidávat e-mailové účty jiné než MSA.
Povolit připojení k účtu Microsoft	Určete, zda povolit používání účtu MSA pro ověřování a služby připojení nesouvisející s e-mailem.
Povolit synchronizaci mých nastavení	Umožňuje synchronizaci nastavení v celém zařízení.
Chráněná doménová jména pro podniky	Určuje názvy podnikových domén oddělené znakem ";".
Povolit uživateli zakázat obnovení systému	Umožňuje uživateli zakázat obnovení systému. **POZOR!** Tato funkce by se měla používat pouze na zařízeních, která vlastní nebo poskytuje podniková společnost nebo organizace, nebo na zařízení vlastněném

	uživatelem, pokud uživatel povolí, aby zařízení plně spravovala podniková společnost. Pokud toto nastavení zásad zakážete, bude funkce Obnovení systému vypnuta a Průvodce obnovením systému nebude přístupný. Možnost konfigurovat Obnovení systému nebo vytvořit bod obnovení prostřednictvím nástroje Ochrana systému je rovněž zakázána.
Povolit zrušení registrace uživatele	Umožňuje uživateli odebrat firemní část ze zařízení, a tím se odpojit od serverů AppTec360. Pokud se tak stane, nebude již možné zařízení spravovat. **POZOR!** Tato funkce by se měla používat pouze na zařízeních, která vlastní nebo poskytuje podniková společnost nebo organizace, nebo na zařízení vlastněném uživatelem, pokud uživatel povolí, aby zařízení plně spravovala podniková společnost. Pokud toto nastavení zásad zakážete, uživatelé nebudou moci odebírat registrace MDM. Určete, zda je uživateli povoleno odstranit účet pracoviště prostřednictvím ovládacího panelu pracoviště. Server MDM by mohl účet vždy vzdáleně odstranit.

BitLocker

Konfigurace nástroje BitLocker

Obecná nastavení	
Vyžadovat šifrování zařízení	V závislosti na edici systému Windows a konfiguraci systému mohou být uživatelé vyzváni k povolení šifrování zařízení: - Potvrzení, že šifrování od jiného poskytovatele není povoleno. - Vypnutí nástroje BitLocker Drive Encryption a jeho opětovné zapnutí.
Metody šifrování	
Metoda šifrování jednotek operačního systému	
Metoda šifrování pevných datových jednotek	
Metoda šifrování vyměnitelných datových jednotek	
Zakázat upozornění na šifrování disku třetí stranou	Zakázat upozornění na službu šifrování disku třetí strany, která je v zařízení používána. Od verze 1803 systému Windows 10 je toto nastavení podporováno pouze pro zařízení připojená k Azure Active Directory.
Povolit spuštění šifrování, když je přihlášen uživatel, který není správcem	Podporováno pouze pro zařízení připojená k Azure Active Directory

Rozšíření AppTec360	
Tiché šifrování	Pokud je vybrána možnost "Vyžadovat šifrování zařízení", spustí služba AppTec360 Management Service automatické tiché šifrování disků zařízení.
Automatické generování pověření uživatele	Zašifrovaná jednotka operačního systému bude chráněna automaticky vygenerovanými přihlašovacími údaji uživatele. Buď kód PIN čipu TPM, pokud je čip TPM k dispozici, nebo šestimístné textové heslo. Vygenerované pověření se odešle na e-mailovou adresu registrovanou pro dané zařízení. Pokud je tato možnost vypnutá, jedinou možnou ochranou pro tiché šifrování je použití čipu TPM. V takovém případě u zařízení bez čipu TPM tiché šifrování selže.
Šifrování pevných disků	Všechny dostupné pevné datové jednotky budou rovněž zašifrovány a chráněny funkcí "Automatické odemykání" pomocí klíče uloženého na jednotce operačního systému.

Nastavení jednotky OS

Vyžadování dalšího ověření při spuštění	Toto nastavení umožňuje nakonfigurovat, zda bude nástroj BitLocker vyžadovat ověření při každém spuštění počítače. Toto nastavení se použije při nastavení nástroje BitLocker. Pokud toto nastavení povolíte, mohou uživatelé v průvodci nastavením nástroje BitLocker konfigurovat pokročilé možnosti spouštění.
Blokování nástroje BitLocker bez kompatibilního čipu TPM	
Pouze TPM	
TPM a PIN	
TPM a klíč	
TPM, klíč a PIN	Pokud chcete vyžadovat použití kódu PIN a jednotky USB flash (klíče), musí uživatel nastavit nástroj BitLocker pomocí nástroje příkazového řádku "manage-bde" namísto průvodce nastavením nástroje BitLocker Drive Encryption.

Požadavek na minimální délku kódu PIN	
Minimální počet znaků	

Konfigurace zprávy a adresy URL pro obnovení před spuštěním systému	Nakonfigurujte celou zprávu pro obnovení nebo nahraďte stávající adresu URL, která se zobrazuje na obrazovce pro obnovení před spuštěním systému, když je jednotka OS uzamčena. Poznámka: Ne všechny znaky a jazyky jsou podporovány v režimu před spuštěním systému. Důrazně doporučujeme vyzkoušet, zda se znaky, které používáte, zobrazují na obrazovce obnovení před spuštěním správně.
	Možnost zprávy před spuštěním systému obnovení
	Vlastní zpráva o obnovení
	Vlastní adresa URL pro obnovení

Možnosti obnovy jednotky OS		Toto nastavení umožňuje řídit způsob obnovení jednotek operačního systému chráněných nástrojem BitLocker v případě, že nejsou k dispozici požadované pověření. Toto nastavení se použije při nastavení nástroje BitLocker. Ve výchozím nastavení je povolen agent pro obnovení dat založený na certifikátu, možnosti obnovení může určit uživatel, včetně hesla pro obnovení a klíče pro obnovení, a informace o obnovení nejsou zálohovány do služby AD DS.
	Agent pro obnovu dat založený na blokovém certifikátu	Určete, zda lze agent pro obnovu dat použít s jednotkami operačního systému chráněnými nástrojem BitLocker. Před použitím agenta pro obnovení dat je třeba jej přidat z položky Zásady veřejných klíčů v Konzole pro správu zásad skupiny nebo v Editoru místních zásad skupiny. Další informace o přidávání agentů pro obnovení dat naleznete v příručce BitLocker Drive Encryption Deployment Guide na webu Microsoft TechNet.
	Nastavení hesla pro obnovení nástroje BitLocker	
	Nastavení klíče pro obnovení nástroje BitLocker	
	Uložení informací o obnovení nástroje BitLocker do služby Active Directory Domain Services	
	Konfigurace úložiště pro obnovení nástroje AD DS BitLocker	Uložení balíčku klíčů podporuje obnovu dat z jednotky, která byla fyzicky poškozena.
	Požadavek na ukládání dat pro obnovení do služby AD DS	Zabránit uživatelům zapnout nástroj BitLocker, pokud počítač není připojen k doméně a

Pevné nastavení pohonu	
Možnosti obnovy pevných disků	Toto nastavení umožňuje řídit způsob obnovení pevných disků chráněných nástrojem BitLocker v případě, že nejsou k dispozici požadované pověření. Toto nastavení se použije při nastavení nástroje BitLocker. Ve výchozím nastavení je povolen agent pro obnovení dat založený na certifikátu, možnosti obnovení může určit uživatel, včetně hesla pro obnovení a klíče pro obnovení, a informace o obnovení nejsou zálohovány do služby AD DS.
Agent pro obnovu dat založený na blokovém certifikátu	
Nastavení hesla pro obnovení nástroje BitLocker	
Nastavení klíče pro obnovení nástroje BitLocker	
Uložení informací o obnovení nástroje BitLocker do služby Active Directory Domain Services	
Konfigurace úložiště pro obnovení nástroje AD DS BitLocker	Uložení balíčku klíčů podporuje obnovu dat z jednotky, která byla fyzicky poškozena.
Požadavek na ukládání dat pro obnovení do služby AD DS	Zabránit uživatelům v povolení nástroje BitLocker, pokud počítač není připojen k doméně a pokud se nepodaří zálohovat informace o obnovení nástroje BitLocker do služby AD DS. Poznámka: Heslo pro obnovení se generuje automaticky.
Odepření přístupu k zápisu na nechráněné pevné jednotky	

Nastavení vyměnitelné jednotky	
Odepření přístupu k zápisu na nechráněné vyměnitelné jednotky	Odepření přístupu k vyměnitelným datovým jednotkám, které nejsou chráněny nástrojem Bitlocker. Poznámka: Pokud "Vyměnitelné disky: Odepřít přístup k zápisu" je v zásadách skupiny povoleno, bude toto nastavení zásad ignorováno.
Odepření přístupu k zápisu do zařízení nakonfigurovaných v jiné organizaci	Přístup k zápisu bude umožněn pouze jednotkám s identifikačními poli shodnými s identifikačními poli počítače. Tato pole jsou definována nastavením zásad skupiny "Poskytnout jedinečné identifikátory pro vaši organizaci".

Stav nástroje BitLocker

Zde si můžete prohlédnout aktuální stav disků šifrovaných nástrojem BitLocker.

C [OS Drive]
Stav šifrování
Šifrované (%)
Stav ochrany
Metoda šifrování
Chrániče klíčů
Heslo pro obnovení

Kliknutím na tlačítko "Otočit heslo pro obnovení" můžete otočit heslo pro obnovení nástroje BitLocker.

Správa certifikátů

Seznam certifikátů

Zde je uveden seznam certifikátů, které jsou nainstalovány v zobrazeném zařízení.

Konfigurace certifikátu

Zde můžete konfigurovat certifikáty a způsob jejich instalace do zařízení.

Důvěryhodný certifikát	
Popis	Popis certifikátu
Oblast působnosti	Rozsah nasazení certifikátu: Aktuální uživatel vs. zařízení
Úložiště certifikátů	"Nedůvěryhodné certifikáty" jsou k dispozici pouze od systému Windows 10, verze 1803.
Soubor s certifikátem	Nahrání souboru PKCS#1

Certifikát totožnosti			
Popis	Popis certifikátu		
Oblast působnosti	Rozsah nasazení certifikátu: Aktuální uživatel vs. zařízení		
Klíčové umístění	Zprostředkovatel úložiště klíčů, do kterého se má soukromý klíč nainstalovat.		
		TPM. Selže, pokud není TPM přítomen	
	TPM. Pokud není TPM přítomen, přejde se na softwarový KSP.		
	Poskytovatel úložiště softwarových klíčů		Označit soukromý klíč jako exportovatelný
	Windows Hello pro firmy	Název kontejneru	Určuje název kontejneru Windows Hello for Business (dříve známého jako Microsoft Passport for Work).
		Text výzvy k zadání kódu PIN	Určuje vlastní text, který se zobrazí na výzvě k zadání kódu PIN služby Windows Hello for Business při zápisu certifikátu.
Pověření	Nahrání souboru PKCS#12		

SCEP

Popis	Popis serveru SCEP		
Rozsah nasazení	Rozsah nasazení certifikátu: Aktuální zařízení vs. uživatel		
Adresy URL serveru SCEP	Jeden nebo více serverů, které vydávají certifikáty prostřednictvím protokolu SCEP.		
Předmět	Reprezentace názvu X.500. Např. "C=US, O=Microsoft Corporation, CN=foo, 1.2.5.3=bar".		
Alternativní názvy předmětů	Typ	E-mailová adresa	
		DNS	
		URI	
		Hlavní jméno uživatele (UPN)	
Otisk prstu CA	Otisk SHA1 certifikátu certifikační autority. E.g. 31:8F:1E:78:5C:D5:12:9F:7E:3B:AD:F3:1C:C0:19:03:96:43:A9:E5		
Jednotky doby platnosti	Dny, měsíce nebo roky		
Doba platnosti			
Výzva	Používá se jako předem sdílené tajemství pro automatickou registraci.		
Opakované pokusy	Počet pokusů, které má zařízení opakovat, pokud server odešle odpověď PENDING. Výchozí hodnota je 5. Maximální hodnota je 30.		
Zpoždění opakování	Počet minut, které je třeba počkat před opakováním pokusu. Výchozí hodnota je 5. Minimální hodnota je 1.		
Velikost klíče	Velikost klíče v bitech		
Algoritmus Hash	Rodina algoritmů Hash		
Klíčové použití	Rozšíření použití klíče definuje účel (např. šifrování, podpis) klíče obsaženého v certifikátu. Je třeba zvolit alespoň jeden z příznaků "Digital signature" (digitální podpis) nebo "Key encipherment" (šifrování klíče).		
Rozšířené použití klíče	Určuje rozšířené použití klíče.Podléhá konfiguraci serveru SCEP. Zadejte seznam odpovídajících OID, např. 1.3.6.1.5.5.7.3.2 (Ověřování klienta).		

Klíčové umístění	Zprostředkovatel úložiště klíčů, do kterého se má soukromý klíč nainstalovat.		
		TPM. Selže, pokud není TPM přítomen	
	TPM. Pokud není TPM přítomen, přejde se na softwarový KSP.		
	Poskytovatel úložiště softwarových klíčů		
	Windows Hello pro firmy	Název kontejneru	Určuje název kontejneru Windows Hello for Business (dříve známého jako Microsoft Passport for Work).
		Text výzvy k zadání kódu PIN	Určuje vlastní text, který se zobrazí na výzvě k zadání kódu PIN služby Windows Hello for Business při zápisu certifikátu.

Správa připojení

Wifi

Při tomto nastavení proveďte předběžnou konfiguraci zařízení koncových uživatelů pro přístup k interním přístupovým bodům.

Identifikátor sady služeb (SSID)	SSID sítě, ke které bude navázáno připojení.
Automatické připojení	Aktivace automatického připojení k síti
Skrytá síť	Aktivovat v případě, že přístupový bod nevysílá SSID.

Typ zabezpečení

Nastavení typu zabezpečení AP

Otevřený systém WEP	
Heslo	Heslo pro přístupový bod

WPA PSK	
Heslo	Heslo pro přístupový bod

WPA EAP	
Typ ověření	Typ ověřování, možné pouze s "PEAP-MSCAHPv2".
Rychlé obnovení připojení	Zařízení mohou přepínat mezi přístupovými body, aniž by se musela znovu ověřovat.
Přístup pro hosty	Uživatel nemá účet, a proto by se měl zaregistrovat jako host.
Karanténní kontroly	Klient musí provést kontrolu NAP (Network Access Protection) a sdílet výsledky se systémem, který pak rozhodne, zda se klient může připojit.
Vyžadovat kryptografickou vazbu	Ověřování je možné pouze prostřednictvím vazby Crypto Binding.
Ověřování serveru	Klient zkontroluje, zda je certifikát serveru platný. Pokud ano, bude navázáno spojení.
Výzva k předložení certifikátů	Umožňuje uživateli přijímat nedůvěryhodné certifikáty.
Názvy serverů	Nabízí možnost zobrazit název serveru RADIUS, který nabízí ověřování a autorizaci v síti.

WPA2-PSK	
Heslo	Heslo AP

WPA2 EAP	
Typ ověření	Typ ověřování, možné pouze s "PEAP-MSCAHPv2".
Rychlé obnovení připojení	
Přístup pro hosty	
Karanténní kontroly	Aktivuje ochranu přístupu k síti NAP
Vyžadovat kryptografickou vazbu	Ověřování je možné pouze prostřednictvím vazby Crypto Binding.
Ověřování serveru	
Výzva k předložení certifikátů	Výzva k zadání ověřeného certifikátu serveru, názvu nebo ověření kořenového certifikátu (CA).
Názvy serverů	Seznam serverů, kterým by zařízení měla důvěřovat
Žádné	Žádné zavedené zabezpečení
Použití serveru proxy	Použití proxy serveru
Adresa serveru	Adresa proxy serveru
Port serveru	Port serveru proxy serveru

Použití serveru proxy

Povolení používání proxy serveru.

Adresa serveru	Adresa proxy serveru používaná v této síti.
Port serveru	Port proxy serveru používaný v této síti.

Omezení připojení k síti Wi-Fi

Zde můžete definovat různá omezení Wifi.

Povolit Wi-Fi	Povolit/odmítnout připojení Wi-Fi
Povolit sdílení internetu	Povolení používání hotspotu
Povolení automatického připojení k hotspotům WiFi Sense	Povolení automatického připojení k hotspotům WiFi Sense
Povolení ruční konfigurace WiFi	Umožnit uživateli připojit se k sítím WiFi, které nebyly definovány společností AppTec.
Frekvence skenování WLAN	Nastaví interval WLAN-Scan. Vyšší hodnota zvyšuje schopnost rozpoznávat sítě WIFI.

VPN

Zde proveďte příslušná nastavení, abyste mohli nakonfigurovat připojení VPN.

Název připojení	Uvedený název připojení		
Typ VPN	Připojení VPN pro jednotlivé aplikace slouží k zabezpečení provozu určitých aplikací.		
	VPN	Vždy zapnuto	Tím se VPN automaticky připojí při přihlášení a zůstane připojena, dokud se uživatel ručně neodpojí.
	VPN pro jednotlivé aplikace	Aplikace VPN	Definice aplikací, které používají toto připojení VPN
		Uzamčení pro jednotlivé aplikace	Uzamčení pro jednotlivé aplikace umožňuje, aby vybrané aplikace měly připojení pouze prostřednictvím tohoto připojení VPN. Tato funkce závisí na bráně Windows Defender Firewall.
	Profil WIP	Doména WIP pro toto připojení	ID podniku, které je nutné pro připojení tohoto profilu VPN k zásadám ochrany informací systému Windows (WIP).

Typ připojení

AppTec360 VPN	
Pro "AppTec360 VPN" je nutné, aby bylo povoleno načítání aplikací ze strany. Povolte prosím "Povolit sideloading aplikací" v "Správa zabezpečení" → "Nastavení omezení" → "Funkčnost zařízení".	
Konfigurace brány	Chcete-li nakonfigurovat připojení VPN s černou listinou, vyberte konfiguraci VPN se zadaným serverem DNS. Konfiguraci VPN můžete nastavit v části "Obecná nastavení" → "Univerzální brána" → "Nastavení VPN".

IKEv2		
Servery	Seznam serverů VPN	
Tunel zařízení	Povolit připojení před přihlášením uživatele.	
Metoda ověřování	EAP	EAP XML
	Strojní certifikáty	
Šifrovací algoritmus		
Algoritmus kontroly integrity		
Diffie-Hellmanova skupina		
Algoritmus transformace šifry		
Algoritmus transformace ověřování		
Skupina PFS (Perfect forward secrecy)		

PPTP		
Servery	Seznam serverů VPN	
Metoda ověřování	EAP	EAP XML

L2TP		
Servery	Seznam serverů VPN	
Metoda ověřování	EAP	EAP XML
Šifrovací algoritmus		
Algoritmus kontroly integrity		
Diffie-Hellmanova skupina		
Algoritmus transformace šifry		
Algoritmus transformace ověřování		
Skupina PFS (Perfect forward secrecy)		

Automatické		
Servery	Seznam serverů VPN	
Metoda ověřování	EAP	EAP XML

Obecné konfigurace VPN

Zapamatování pověření při každém přihlášení	
Registrace IP adres pomocí interního systému DNS	
Pravidla filtrování síťového provozu	Omezit připojení VPN na definovanou sadu pravidel.
Seznam pro vyhledávání přípon DNS	Přípony DNS, které se přidají do seznamu vyhledávání DNS pro směrování krátkých názvů.
Pravidla tabulky zásad rozlišení názvů (NRPT)	Pravidla NRPT (Name Resolution Policy table) definují způsob, jakým DNS překládá názvy při připojení k síti VPN.
Detekce důvěryhodné sítě	Seznam přípon DNS pro identifikaci důvěryhodné sítě.
Dělené tunelování	Dělené tunelování znamená, že přenosy mohou procházet přes libovolné rozhraní, které určí síťový zásobník.
Rozdělené tunelové trasy	Seznam tras, které mají být přidány do směrovací tabulky pro rozhraní VPN.
Nastavení proxy serveru	Konfiguruje proxy server používaný v této síti
Adresa proxy	Adresa proxy serveru jako plně kvalifikovaný název hostitele nebo IP adresa.
Přístav	Port proxy serveru.
Adresa URL automatické konfigurace proxy serveru	URL pro automatické načtení nastavení proxy serveru.

Omezení VPN

Zde můžete definovat různá omezení VPN.

Povolit nastavení VPN	Tento pokyn umožňuje/zakazuje uživateli deaktivovat a měnit nastavení VPN.
Povolení sítě VPN přes mobilní síť	Povoluje/zakazuje zařízení navázat připojení VPN, pokud zařízení používá mobilní data.
Povolení roamingu VPN přes mobilní sítě	Povoluje/zakazuje zařízení navázat připojení VPN, pokud je zařízení v roamingu.

Bluetooth

Zde můžete nastavit, zda má být Bluetooth povolen nebo zakázán.

Povolit Bluetooth	Aktivace/deaktivace funkce Bluetooth

Správa PIM

Exchange Active Sync

Nastavení účtu ActiveSync v zařízení koncového uživatele

Název účtu	Název e-mailového účtu
Název hostitele serveru	Adresa serveru/FQDN
Název domény	Doména serveru
E-mailová adresa	E-mailová adresa
Uživatelské jméno	Uživatelské jméno
Heslo uživatele	Volitelně zde můžete k uživateli připojit heslo.
Použití protokolu SSL	Použít připojení SSL
Interval synchronizace	Zde lze stanovit synchronizační interval Ruční synchronizace = uživatel musí stáhnout své e-maily a provést ruční synchronizaci.
Filtr stáří pošty	Doba, za kterou se mají e-maily synchronizovat. Bez filtru = neomezeně
Úroveň protokolu	Stanovení úrovní protokolování pro přenosy ActiveSync
Synchronizace e-mailu	Aktivováno = e-maily jsou synchronizovány
Synchronizace kontaktů	Aktivováno = kontakty jsou synchronizovány
Synchronizace kalendáře	Aktivováno = kalendář je synchronizován
Úlohy synchronizace	Aktivováno = úlohy jsou synchronizovány

eMail

Vytvoření účtů POP3/IMAP4 v zařízení koncového uživatele.

Popis účtu	Název e-mailového účtu
Jméno odesílatele	Zobrazené jméno odesílatele
Název domény	Název domény pro e-mailový účet
E-mailová adresa	E-mailová adresa uživatele
Uživatelské jméno	Uživatelské jméno
Heslo uživatele	Volitelně zde můžete k uživateli připojit heslo.
Alternativní přihlašovací údaje odchozího serveru	Zde lze zadat, zda jsou pro odchozí server vyžadována další pověření.
Název odchozí domény	Název odchozí domény
Uživatelské jméno odchozího serveru	Uživatelské jméno odchozího serveru
Heslo odchozího serveru	Heslo odchozího serveru
E-mailový protokol	Jako protokol lze použít POP3 nebo IMAP4.
Název hostitele příchozího poštovního serveru	Název hostitele příchozího poštovního serveru
Použití protokolu SSL pro příchozí e-maily	Použití protokolu SSL pro příchozí e-maily
Název hostitele serveru odchozí pošty	Název hostitele serveru odchozí pošty
Použití protokolu SSL pro odchozí e-maily	Použití protokolu SSL pro odchozí e-maily
Ověřování odchozího serveru	Je vyžadováno ověření odchozího serveru
Interval synchronizace	Zde lze stanovit synchronizační interval Ruční synchronizace = uživatel musí stáhnout své e-maily a provést ruční synchronizaci.
Filtr stáří pošty	Doba, za kterou se mají e-maily synchronizovat. Bez filtru = neomezeně

Správa aplikací

Správce podnikových aplikací

Nainstalované aplikace

Zde je uveden seznam aplikací, které jsou aktuálně nainstalovány v zobrazeném zařízení.

Povinné aplikace

Zde můžete nakonfigurovat seznam aplikací, které jsou v zařízení povinné.

Tento seznam se zkontroluje při každém připojení zařízení k MDM a nainstalují se všechny aplikace z tohoto seznamu, které náhodou nejsou v zařízení nainstalovány, bez ohledu na to, zda byla aplikace odinstalována nebo zda nikdy předtím nainstalována nebyla.

Můžete nahrát vlastní aplikace Windows 10 a poté je přidat do tohoto seznamu nebo můžete přidat konfigurace Microsoft Office, které je třeba předem nakonfigurovat v části "Obecná nastavení" > "Správa aplikací" > "Microsoft Office".

Omezení aplikací systému

Doručené aplikace
Povolení budíků a hodin
Povolit kalkulačku
Povolit kameru
Povolit kontaktní podporu
Povolit Cortanu
Povolit Průzkumník souborů
Povolení Začít
Povolit Groove Music
Povolit mapy
Povolení zasílání zpráv
Povolení prohlížeče Microsoft Edge
Povolit filmy a televizi
Povolit peníze
Povolit Novinky
Povolení služby OneDrive
Povolit OneNote
Povolit kalendář a poštu aplikace Outlook
Povolit lidem
Povolit telefon
Povolit fotografie
Povolit Powerpoint
Povolit nastavení
Povolení služby Skype
Povolit sport
Povolit ukládání
Povolit hlasový záznamník
Povolit peněženku
Povolit počasí

Povolení centra zpětné vazby systému Windows
Povolit Word
Povolení konzole Xbox

Nastavení stránek
Povolit účty Pracoviště
Povolit rozšířené informace
Koutek povolených aplikací
Povolit blokování a filtrování
Povolit barevný profil
Povolit režim jízdy
Povolení e-mailu a účtů
Povolit ekvalizér
Povolit klávesnici
Povolit navigační panel
Povolení režimu letadlo v síti
Povolit sdílení internetu v síti
Povolení síťových služeb
Povolit síť Wi-Fi
Povolení systému PC Bluetooth
Povolit hodnocení zařízení
Povolit obnovení aktualizace
Povolit sdílení
Povolit spuštění
Povolený čas Jazyk
Povolený čas Oblast
Povolení výchozí obrazovky uzamčení systému Windows
Povolit pracovní nebo školní účet

Černá a bílá listina

V části "Black- & Whitelisting" si můžete vybrat mezi režimem "Whitelist" a režimem "Blacklist".

Bílá listina	Do zařízení koncového uživatele lze nainstalovat pouze aplikace a služby, které jsou přidány do seznamu. Pokud jsou již v zařízení koncového uživatele předinstalovány, budou aktivovány a nastaveny tak, aby je uživatel mohl spustit.
	Všechny ostatní aplikace, které nejsou přidány do seznamu, nelze do zařízení koncového uživatele nainstalovat. Pokud jsou již v zařízení koncového uživatele předinstalovány, budou deaktivovány a nastaveny tak, aby je uživatel nemohl spustit.
Černá listina	Aplikace a služby přidané do seznamu nelze nainstalovat do zařízení koncového uživatele. Pokud jsou v zařízení koncového uživatele již předinstalovány, budou deaktivovány a nastaveny tak, aby je uživatel nemohl spustit.
	Všechny ostatní aplikace, které nejsou přidány do seznamu, lze nainstalovat do zařízení koncového uživatele. Pokud jsou již v zařízení koncového uživatele předinstalovány, budou aktivovány a nastaveny tak, aby je uživatel mohl spustit.

Prostřednictvím tlačítka , přidáte do seznamu aktuálně používaných aplikací nebo služeb další.

Prostřednictvím tlačítka , přidáte další aplikace nebo služby do aktuálně neaktivního seznamu.

Aplikaci můžete přidat buď z obchodu Windows App Store, nebo přímo zadat identifikátor aplikace a přidat ji na černou nebo bílou listinu.

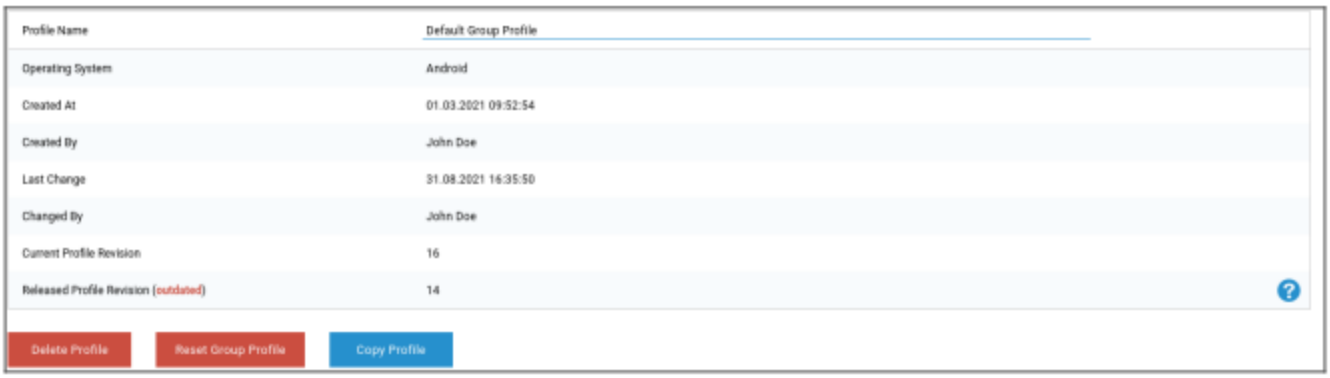
Konfigurace systému MacOS

V závislosti na tom, zda jste vybrali profil nebo zařízení, se zobrazení a jeho dílčí body liší - věnujte tomu prosím zvýšenou pozornost!

Obecné

Přehled profilu skupiny (pouze na úrovni skupiny)

Po otevření profilu skupiny se zobrazí rychlý přehled profilu.



Název profilu	Název profilu (zde lze změnit)
Operační systém	Operační systém, pro který je profil určen
Vytvořeno v	Čas vytvoření
Vytvořil	Tvůrce profilu
Poslední změna	Čas poslední změny profilu
Změněno podle	Účet, který provedl poslední změny
Aktuální revize profilu	Revize uloženého stavu profilu
Vydaná revize profilu	Přiřazená revize profilu ("Assign now"). Pokud se za textem na štítku zobrazí " (zastaralý)", znamená to, že jste profil uložili, ale ještě jste ho nepřiřadili, takže zařízení budou stále dostávat starší verzi.

Přehled zařízení (pouze na úrovni zařízení)

Souhrnný přehled zařízení.

Název zařízení	Název zařízení
Model	Model
Operační systém	Operační systém
Sériové číslo	Sériové číslo zařízení
Vlastnictví zařízení	Nakonfigurovaný typ vlastnictví
Typ zařízení	Typ zařízení
V souladu s předpisy	Zobrazuje, zda je zařízení kompatibilní
IP adresa	Adresa IP, ze které se zařízení připojuje k serveru.
Naposledy viděno	Čas posledního připojení ze zařízení
Poslední impuls	Čas posledního impulsu odeslaného do zařízení
Zadání	Zde můžete zařízení přesunout k jinému uživateli nebo skupině.

Revize konfigurace (pouze na úrovni zařízení)

Zde získáte přehled o tom, který skupinový profil je k zařízení přiřazen.

Pokud kliknete na profil skupiny, dostanete se přímo do profilu a můžete provést nastavení.

Pomocí symbolu můžete vrátit přiřazené aplikace do nastavení skupinového profilu.

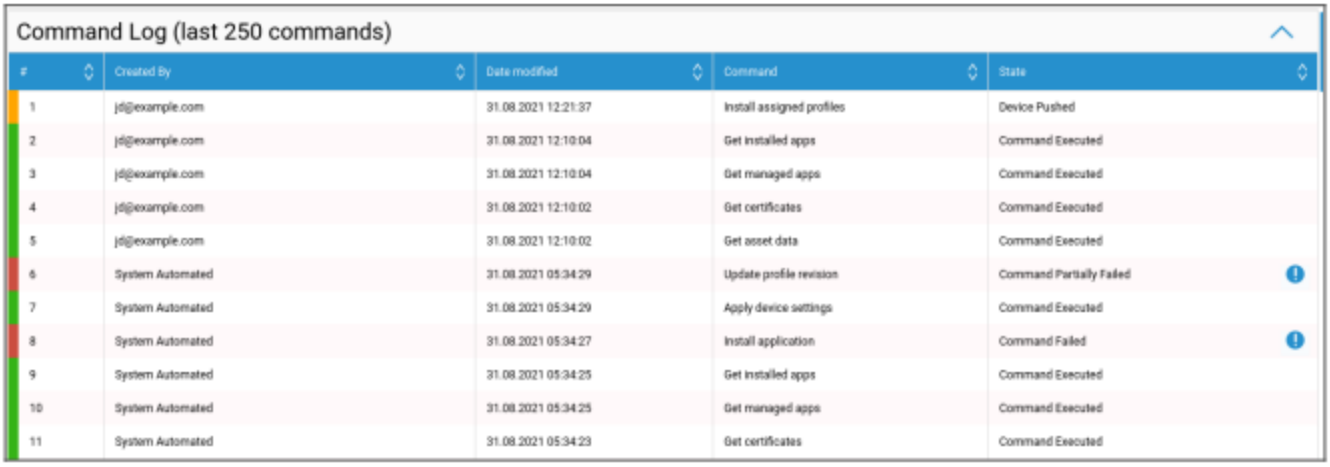
Pomocí symbolu můžete obnovit profil zařízení tak, aby neměl žádné nastavení.

"K dispozici je novější revize" znamená, že profil skupiny byl změněn a uložen, ale nebyl přiřazen. Profil skupiny je třeba přiřadit pomocí "Přiřadit nyní" na úrovni skupiny, aby se změny uplatnily na zařízení.

Protokol zařízení (pouze na úrovni zařízení)

Protokol příkazů

Zde můžete zjistit, které příkazy byly pro zařízení vydány a jaký je jejich stav.



Příkazy vytvořené pomocí "System Automated" jsou automaticky vytvořeny systémem.

Možné stavy příkazů

Stlačené zařízení	Službě push (např. APNS) byl odeslán požadavek na připojení, aby se zařízení připojilo zpět k serveru EMM.
Vytvořený příkaz	Příkaz byl vytvořen v systému.
Odeslaný příkaz	Příkaz byl odeslán do zařízení po jeho připojení k serveru.
Spuštěný příkaz	Příkaz byl úspěšně proveden.
Příkaz se nezdařil	Příkaz se nezdařil. *
Příkaz částečně selhal	V závislosti na operačním systému zařízení mohou být některé příkazy seskupeny. V tomto některé části této skupiny příkazů selhaly. *
Příkaz proveden, případně neúspěšný	Příkaz byl proveden, ale možná nebyl.
Přesunutí příkazu	Příkaz byl znovu odeslán uživatelem.
Vyřazené	Příkaz byl vyřazen. Například proto, že byl nahrazen jiným příkazem nebo že zařízení bylo znovu zapsáno a staré příkazy byly odstraněny.

*Pokud je za zprávou vykřičník, můžete získat další informace, když na ikonu najedete kurzorem.

Správa aktiv (pouze na úrovni zařízení)

Informace o zařízení

Číslo modelu	Číslo modelu
Hostitelské jméno	Hostitelské jméno
Místní název hostitele	Místní název hostitele
Operační systém	Operační systém
Verze operačního systému	Verze operačního systému
UDID	UDID
Volná / celková paměť	Volná / celková paměť

WiFi

IP adresa	IP adresa
WiFi MAC	WiFi MAC

Cellular

Telefonní číslo	Telefonní číslo
Stav roamingu	Stav roamingu
Roaming (hlas / data)	Roaming (hlas / data)
IP adresa	IP adresa
Provozovatel/přepravce	Provozovatel/přepravce
Síť operátora SIM	Síť dopravců
Verze pro nosiče	Verze pro nosiče
ICCID	ICCID
Současné MCC/MNC	Současné MCC/MNC
SIM MCC/MNC	SIM MCC/MNC

Bluetooth

Bluetooth MAC	Bluetooth MAC

Správa aktualizací (pouze na úrovni zařízení)

Aktualizované informace

Tato karta zobrazuje informace o nastavení aktualizace systému v zařízení.

Automatická kontrola povolena	Pokud systém kontroluje aktualizaci automaticky.
Povolení automatické aktualizace aplikací	Pokud bude systém automaticky instalovat aktualizace aplikací.
Povolení automatických aktualizací operačního systému	Pokud systém nainstaluje aktualizace os automaticky.
Povolení automatických aktualizací zabezpečení	Pokud systém automaticky instaluje aktualizace zabezpečení.
Aktualizace aplikací na pozadí - stahování povoleno	Pokud bude systém stahovat aktualizace aplikací na pozadí.
Adresa URL katalogu	Adresa URL katalogu aktualizací softwaru, který klient používá.
Je výchozí katalog	Pokud "ano", je Katalog výchozím katalogem.
Provádění pravidelné kontroly	Pokud "ano", spusťte nové skenování.
Datum předchozího skenování	Datum poslední kontroly aktualizace softwaru.
Výsledek předchozího skenování	Kód výsledku poslední kontroly aktualizace softwaru.

Správa zabezpečení

Ochrana proti krádeži

Otření a uzamčení

Úplné otření	Odeslání příkazu k obnovení továrního nastavení zařízení
Podnikové utírání	Odstranění MDM ze zařízení a odstranění všech dat MDM (např. účtů, aplikací).
Zamykací obrazovka	Návrat zařízení na uzamčenou obrazovku

Konfigurace zabezpečení

Přístupový kód

Povolená deaktivace kódu	Určuje, zda je uživatel nucen nastavit kód PIN. Pouhé nastavení této hodnoty (a nikoli jiných) nutí uživatele zadat přístupový kód, aniž by byla stanovena jeho délka nebo kvalita.
Povolit jednoduchou hodnotu	Umožnit uživateli používat stejné, eskalující a redukující číselné řetězce (např. 1234, 1111).
Vyžadovat alfanumerickou hodnotu	Hesla musí obsahovat alespoň jedno písmeno
Minimální délka přístupového kódu	Minimální délka hesla
Minimální počet složených znaků	Minimální počet alfanumerických symbolů v hesle
Maximální věk přístupového kódu	Počet dní, po kterých je třeba heslo změnit.
Maximální automatické zamykání	Maximální doba, po kterou je zařízení uzamčeno
Maximální doba odkladu pro uzamčení zařízení	Doba, po kterou může být zařízení uzamčeno bez výzvy k zadání přístupového kódu při odemknutí.
Maximální stáří přístupového kódu (1-730 dní nebo žádné)	Dny, po kterých musí být přístupový kód změněn
Historie přístupových kódů (1-50 přístupových kódů nebo žádný)	Počet jedinečných přístupových kódů před opakovaným použitím

Certifikát

PKCS#1	
Popis	Zadejte popis certifikátu
Pověření	Nahrát soubor pkcs1

PKCS#12	
Popis	Zadejte popis certifikátu
Pověření	Nahrát soubor pkcs12

Nastavení omezení

Funkčnost zařízení

Povolit kameru	Povolení používání fotoaparátu
Povolit Game Center	Pokud je hodnota false, služba Game Center je zakázána a její ikona je odstraněna z domovské obrazovky.
Povolit hraní pro více hráčů	Pokud je hodnota false, zakazuje hraní pro více hráčů.
Povolení přidávání přátel do služby Game Center	Pokud je hodnota false, zakáže přidávání přátel do služby Game Center.
Povolení knihovny fotografií iCloud	Pokud je nastavena na hodnotu false, zakáže knihovnu iCloud Photo Library. Všechny fotografie, které nebudou plně staženy z iCloud Photo Library do zařízení, budou z místního úložiště odstraněny.
Povolení Touch ID	Pokud je hodnota false, zabrání odemknutí zařízení pomocí Touch ID.

iCloud

Blokování určitých funkcí při párování iCloudu

Povolení synchronizace dokumentů	Povolení synchronizace dokumentů
Povolení synchronizace iCloud Keychain	Povolení synchronizace iCloud Keychain
Povolení poznámek iCloud	Pokud je hodnota false, zakáže služby iCloud Notes systému MacOS.
Povolení iCloud BTMM	Pokud je hodnota false, zakáže službu iCloud v systému MacOS Back to My Mac.
Povolení iCloud FMM	Pokud je hodnota false, zakáže službu iCloud systému MacOS Find My Mac.
Povolení záložek iCloud	Pokud je hodnota false, zakáže synchronizaci záložek iCloud v systému MacOS.
Povolení služby iCloud Mail	Pokud je hodnota false, zakáže služby iCloud systému MacOS Mail.

Povolení kalendáře iCloud	Pokud je hodnota false, zakáže služby iCloud systému MacOS Cloud.
Povolení připomínek iCloud	Pokud je hodnota false, zakáže služby iCloud Reminder.
Povolení služby iCloud Addressbook	Pokud je hodnota false, zakáže služby iCloud Address Book v systému MacOS.

Správa médií

Vysunutí při odhlášení	Vysunutí všech vyměnitelných médií při odhlášení
Povolit síť	Povolení přístupu pro síťová média
Povolit interní disk	Povolení přístupu pro interní disk.
Vyžadovat ověření	Vyžadovat ověření pro použití tohoto média
Pouze pro čtení	Uživatel může z média pouze číst data.
Povolit externí disk	Povolení přístupu pro externí disk.
Vyžadovat ověření	Vyžadovat ověření pro použití tohoto média
Pouze pro čtení	Uživatel může z média pouze číst data.
Povolení používání bitových kopií disků	Povolení přístupu k obrázkům.
Vyžadovat ověření	Vyžadovat ověření pro použití tohoto média
Pouze pro čtení	Uživatel může z média pouze číst data.
Povolení používání pamětí DVD-RAM	Povolení přístupu pro disk DVD-RAM.
Vyžadovat ověření	Vyžadovat ověření pro použití tohoto média
Pouze pro čtení	Uživatel může z média pouze číst data.
Povolení používání disků DVD	Povolení přístupu k disku DVD.
Vyžadovat ověření	Vyžadovat ověření pro použití tohoto média
Povolení používání disků CD	Povolení přístupu pro disk CD.
Vyžadovat ověření	Vyžadovat ověření pro použití tohoto média

Správa připojení

Wi-Fi

Zde můžete přidávat a konfigurovat připojení Wi-Fi.

Identifikátor sady služeb (SSID)	SSID sítě, ke které bude navázáno připojení.
Automatické připojení	Povolení automatického připojení k síti
Skrytá síť	Povolit v případě, že přístupový bod nevysílá SSID.
Nastavení serveru proxy	Konfigurace proxy serveru pro každý přístupový bod
Žádné	Nepoužívejte proxy server
Manuální	Vytvoření ručního zástupce
Adresa URL proxy serveru	Adresa pro přístup k nastavení proxy serveru
Přístav	Nastavení portu pro proxy server
Ověřování	Uživatelské jméno pro ověřování na serveru Proxy
Heslo	Heslo pro ověřování na serveru Proxy
Automatické	Automatické vytvoření proxy serveru
Adresa URL proxy serveru	Adresa URL pro soubor s nastavením proxy serveru
Typ zabezpečení	Nastavení typu zabezpečení pro přístupový bod
WEP	
Heslo	Heslo pro přístupový bod
WPA/WPA2	
Heslo	Heslo pro přístupový bod
WEP Enterprise - WPA / WPA2 Enterprise / Jakýkoli podnik	Viz tabulka Chyba: Níže uvedený zdroj odkazů nebyl nalezen
Žádné	Nezavádět žádné zabezpečení

Zakázat náhodný výběr adresy MAC	Zakáže náhodný výběr adresy MAC pro danou síť Wi-Fi, dokud je k ní přidružena. Tím se také v Nastavení zobrazí varování o ochraně soukromí, které označuje, že síť má sníženou ochranu soukromí.

Konfigurace podnikové sítě Wi-Fi

Poznámka: Je k dispozici pouze tehdy, když je položka "Typ zabezpečení" nastavena na typ Enterprise.

Protokoly	Protokol ověřování podporovaný v cílové síti
TLS	Povolit / zakázat používání
TTLS	Povolit / zakázat používání
Vnitřní ověřování	Ověřovací protokol, který by měl být použit: PAP, CHAP, MSCHAP, MSCHAPv2.
LEAP	Povolit / zakázat používání
PEAP	Povolit / zakázat používání
EAP-FAST	Povolit / zakázat používání
EAP-SIM	Povolit / zakázat používání
Použití PAC	Použití systému PAC (Protected Access Control)
Ustanovení PAC	Konfigurace systému Provision PAC
Anonymní poskytování PAC	Anonymní poskytování PAC
Ověřování	
Uživatelské jméno	Ověřování uživatelského jména
Nepoužívejte Na připojení Heslo	Nepoužívejte heslo pro připojení
Heslo	Heslo, které se má použít
Certifikát totožnosti	Nahrání/vybrání ověřovacího certifikátu
Vnější identita	Identita viditelná zvenčí
Trust	
Důvěryhodný certifikát 1	Nahrání prvního důvěryhodného certifikátu
Důvěryhodný certifikát 2	Nahrání druhého důvěryhodného certifikátu

Důvěryhodný certifikát 3	Nahrání třetího důvěryhodného certifikátu
Důvěryhodný server Názvy certifikátů	Názvy očekávaných certifikátů serverů (v seznamu odděleném čárkou)

VPN

V závislosti na vybraném typu připojení mohou být viditelná různá pole.

Název připojení	Název profilu VPN
Typ VPN	
VPN	Veškerý síťový provoz zařízení bude směrován prostřednictvím připojení VPN.
Typ připojení	Vytvoření typu připojení VPN
IPsec (cisco)	Protokol IPsec od společnosti cisco
L2TP	Protokol L2TP
Vlastní protokol SSL	Připojení přes vlastní protokol SSL
IKEv2	Protokol IKEv2
Nastavení serveru proxy	Konfigurace proxy serveru pro připojení VPN
Žádné	Nezavést žádnou proxy
Manuální	Ruční vytvoření proxy serveru
Adresa URL proxy serveru	Adresa pro přístup k nastavení proxy serveru
Přístav	Nastavení portu pro server Proxy
Ověřování	Uživatelské jméno pro ověřování na serveru Proxy
Heslo	Heslo pro ověřování na serveru Proxy
Automatické	Automatické vytvoření proxy serveru
Adresa URL proxy serveru	Adresa URL pro přístup k nastavení proxy serveru

Proxy server HTTP

Typ proxy serveru	
Manuální	Vytvoření proxy serveru ručně
Adresa URL proxy serveru	Adresa pro přístup k nastavení proxy serveru
Přístav	Vytvoření portu proxy serveru
Ověřování	Uživatelské jméno pro ověřování na serveru Proxy
Heslo	Heslo pro ověřování na serveru Proxy
Automatické	Automatické vytvoření proxy serveru
Adresa URL proxy serveru PAC	Adresa URL proxy serveru PAC
Povolit přímé připojení, pokud je PAC nedostupný	Povolit přímé připojení (bez VPN), pokud je PAC nedostupný.
Povolení obcházení proxy serveru pro přístup k chráněným sítím	Povolení obcházení proxy serveru pro přístup k interním sítím v režimu captive

AirPrint

IP adresa	IP adresa tiskárny
Cesta ke zdroji	Určitá cesta k zařízení AirPrint

AirPlay

Název zařízení	Název zařízení
Heslo	Heslo pro párování
Bílá listina	Definujte seznam zařízení, se kterými se zařízení může výhradně spárovat.

Správa PIM

Exchange Active Sync

Název účtu	Název účtu.
E-mailová adresa	Adresa účtu (např. max@company.com).
Název hostitele serveru	Interní název hostitele
Přihlašovací jméno	"Doména" a "Přihlašovací jméno" musí být prázdné, aby se zařízení zeptalo na uživatele.
Doména	"Doména" a "Přihlašovací jméno" musí být prázdné, aby se zařízení zeptalo na uživatele. Pokud je povolena konfigurace brány ACL a pole Doména není prázdné, bude univerzální brána AppTec360 ověřovat zařízení pod následujícím názvem "Doména\Přihlašovací jméno".
Heslo	Heslo k účtu (např. secretUserPassword)
Minulé dny služby Mail to Sync	Počet posledních dnů pošty k synchronizaci
Použití protokolu SSL	Použití protokolu SSL pro interního hostitele Exchange
Rozšířená možnost	Zobrazit rozšířené možnosti
Port serveru	Interní port
Cesta k serveru	Vnitřní cesta
Externí název hostitele	Externí hostitel
Externí port	Externí port
Externí cesta	Externí cesta
Použití protokolu SSL pro externí Exchange Host	Použití protokolu SSL pro externího hostitele Exchange

eMail

Nastavení účtů POP3 / IMAP v zařízení koncového uživatele

Popis účtu	Název des E-mailové účty
Typ účtu	
IMAP	
Předpona cesty	Předpona cesty pro speciální složky
POP	
Zobrazované jméno uživatele	Zobrazované jméno uživatele
E-mailová adresa	E-mailová adresa uživatele

Příchozí pošta	Nastavení příchozího serveru
Adresa poštovního serveru	Adresa poštovního serveru
Port poštovního serveru	Port poštovního serveru
Uživatelské jméno	Příslušné uživatelské jméno
Typ ověření	Typ ověření
Žádné	Ne Typ ověření
Heslo (pouze na úrovni zařízení)	Výzva k zadání hesla
MDM Challenge-Response	
NTLM	Ověřování NTLM
Digest HTTP MD5	
Použití protokolu SSL	V případě potřeby použijte protokol SSL

Odchozí pošta	Nastavení odchozího serveru
Adresa poštovního serveru	Adresa poštovního serveru
Port poštovního serveru	Port poštovního serveru
Uživatelské jméno	Příslušné uživatelské jméno
Typ ověření	
Žádné	Žádná metoda ověřování
Heslo (pouze na úrovni zařízení)	Výzva k zadání hesla
MDM Challenge-Response	
NTLM	Ověřování NTLM
Digest HTTP MD5	
Použití protokolu SSL	V případě potřeby použijte protokol SSL
Odchozí heslo stejné jako příchozí	Odchozí heslo stejné jako příchozí
Používejte pouze v poště	Aktivujte, pokud mají být všechny odchozí e-maily odesílány prostřednictvím aplikace Mail-App.

CalDav

Konfigurace nastavení a distribuce účtu CalDav

Popis účtu	Zobrazovaný název účtu
Hostitelské jméno	Název hostitele a/nebo IP adresa
Přístav	Přístav účtu CalDav
Hlavní adresa URL	Hlavní adresa URL účtu
Uživatelské jméno	Příslušné uživatelské jméno CalDav
Heslo (pouze na úrovni zařízení)	Příslušné heslo CalDav
Použití protokolu SSL	V případě potřeby použijte protokol SSL

CardDav

Konfigurace nastavení a distribuce účtu CardDav

Popis účtu	Zobrazovaný název účtu
Hostitelské jméno	Název hostitele a/nebo IP adresa
Přístav	Port účtu CardDav
Hlavní adresa URL	Hlavní adresa URL účtu
Uživatelské jméno	Příslušné uživatelské jméno CardDav
Heslo (pouze na úrovni zařízení)	Příslušné heslo CardDav
Použití protokolu SSL	V případě potřeby použijte protokol SSL

LDAP

V této oblasti nastavte připojení LDAP, abyste umožnili dynamickou výměnu certifikátů mezi zařízením koncového uživatele a službou Active Directory.

Upozorňujeme, že vybraný uživatel vyžaduje příslušné oprávnění ke čtení.

Popis účtu	Popis účtu
Uživatelské jméno účtu	Uživatel pro přístup k LDAP
Heslo k účtu	Heslo pro přístup do LDAP
Název hostitele účtu	Název hostitele/IP adresa serveru LDAP
Použití protokolu SSL	V případě potřeby použijte protokol SSL

Ve druhé části můžete definovat jednotlivé filtry pro vyhledávání v registru LDAP.

Popis	Oblast působnosti	Základna pro vyhledávání
Popis filtru	Úroveň vyhledávání v registru LDAP	Definice jednotlivých filtrů

Dashboard & Reporting

Nastavení ovládacího panelu

Zde si můžete prohlédnout existující ovládací panely, upravit je nebo vytvořit nové. Každý přístrojový panel má vlastní sadu zobrazovaných dat a konfiguraci grafů.

Ovládání nastavení přístrojové desky

Veřejnost	Nastaví přístrojovou desku jako veřejnou, aby ji mohli vidět i ostatní uživatelé. Uživatelé samozřejmě musí mít možnost se přihlásit a zobrazit si Dashboardy. Pokud není aktivována volba "Veřejný", může jej vidět pouze jeho tvůrce.
Výchozí	Nastaví přístrojový panel jako výchozí, takže se automaticky otevře při příštím přístupu k zobrazení přístrojového panelu.
	Zobrazení panelu a jeho grafů
	Odstranění ovládacího panelu
	Úprava názvu a nastavení ovládacího panelu
	Vytvoření kopie ovládacího panelu
	Přidání zcela nového ovládacího panelu

Zobrazení přístrojové desky

Zobrazí data a grafy vybraného panelu a umožní vám je také změnit.

Ovládání přístrojové desky

	Umožňuje definovat, která data se mají zobrazovat na panelu, jaké množství dat se má zobrazovat a v jaké velikosti se mají zobrazovat.
	Přesune vás zpět na přehled ovládacího panelu
	Obnovení výchozího nastavení aktuálně otevřeného panelu.
	Uloží všechny změny, které jste provedli v aktuálně otevřeném panelu (např. která data se mají zobrazit).
	Změna typu grafu na sloupcový graf
	Změna typu grafu na koláčový graf
	Změna typu grafu na koblihový graf
	Změna typu grafu na graf polární oblasti
	Změna pořadí řazení

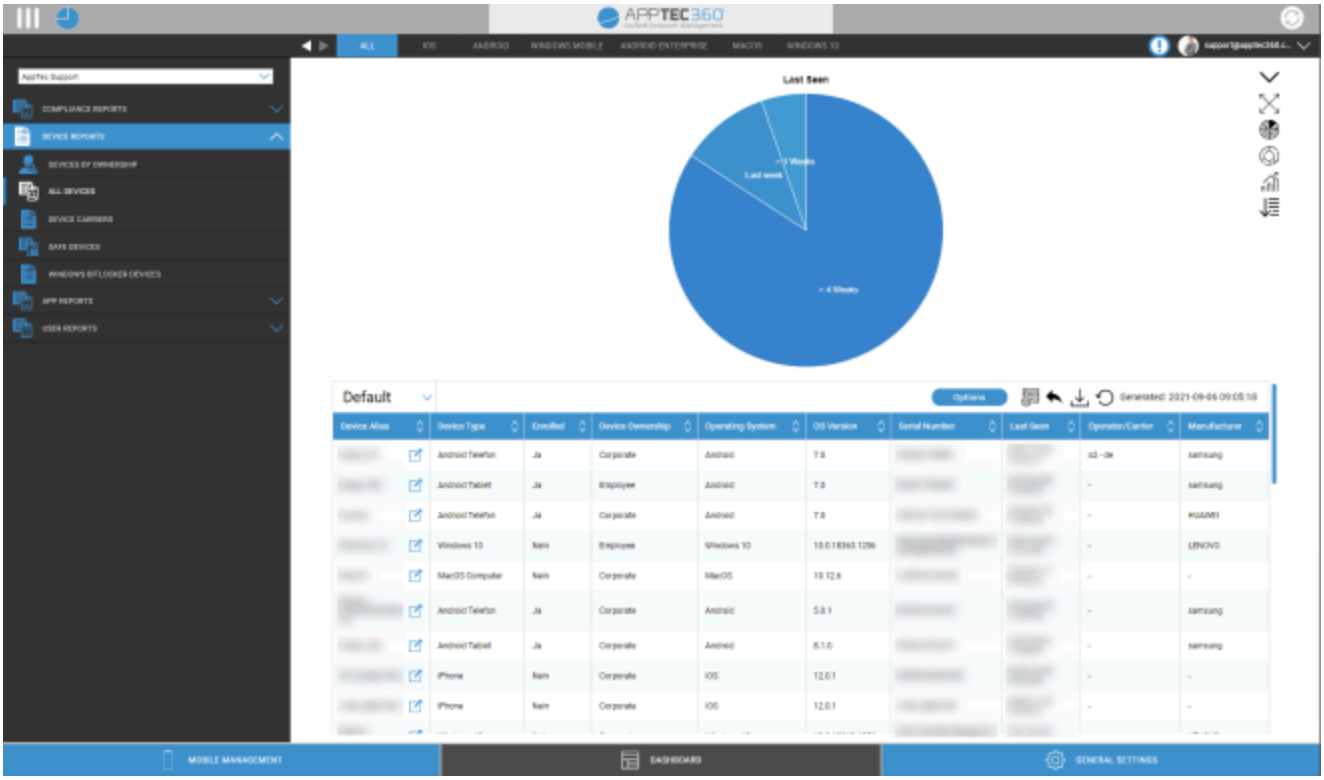
Rozšířené hlášení

"Rozšířené hlášení" nabízí podrobné přehledy a grafy o zařízení a uživatelských informacích.

Existuje několik výchozích sestav, ale všechny je možné ručně změnit a přidat nebo odebrat data, která se mají zobrazit.

Vezměte prosím na vědomí, že zobrazené údaje můžete změnit pouze ručně. Vybraná kategorie sestavy určuje, na základě jakých dat se tak děje. Např. v sestavě Zařízení v reportech Všechna zařízení iOS nikdy nebudete moci zobrazit zařízení se systémem Android.

Vlevo nahoře můžete omezit údaje hlášení na určitou skupinu (a všechny její podskupiny). Ve výchozím nastavení je tato skupina nastavena na kořenový uzel, takže bere v úvahu VŠECHNA zařízení a uživatele.



Rozšířená kontrola hlášení

V každém přehledu můžete použít následující funkce, abyste mohli přehled libovolně změnit:

	Skrýt graf (pokud je graf zobrazen)
	Zobrazit graf (pokud je graf skrytý)
	Rozbalit graf (Pokud je graf sbalený)
	Sbalit graf (Pokud je graf rozbalený)
	Změna typu grafu na sloupcový graf
	Změna typu grafu na koláčový graf
	Změna typu grafu na koblihový graf
	Změna typu grafu na graf polární oblasti
	Změna pořadí řazení
	Upravte následující části zobrazeného přehledu: • Přidání/odebrání sloupců • Zadejte pořadí, v jakém se sloupce zobrazí. • Zobrazit/skrýt graf nad tabulkou • Vyberte sloupec, který se použije pro graf • Filtrování dat tabulky
	Otevření správce nastavení pro ukládání a načítání různých sestav
	Obnoví výchozí nastavení aktuálně otevřené zprávy
	Exportovat aktuální sestavu jako soubor .csv
	Regenerace dat a opětovné načtení aktuální sestavy

Seznam všech výchozích sestav najdete na dalších stránkách.

Zprávy o dodržování předpisů

Zakořeněná zařízení

Přehled zařízení, která byla rootnuta/jailbreaknuta.

Výchozí sloupce této sestavy:

Alias zařízení
Vlastník zařízení
E-mail
Operační systém
Telefonní číslo
Naposledy viděno
Výrobce

Roamingová zařízení

Přehled všech roamingových zařízení

Výchozí sloupce této sestavy:

Alias zařízení
Vlastník zařízení
E-mail
Typ zařízení
Operační systém
Telefonní číslo
Naposledy viděno

Zařízení s povoleným roamingem

Přehled všech zařízení, která mají aktivovaný roaming, ale nemusí být nutně právě v roamingu.

Výchozí sloupce této sestavy:

Alias zařízení
Vlastník zařízení
E-mail
Typ zařízení
Operační systém
Telefonní číslo
Naposledy viděno

Zařízení pod dohledem

Přehled všech zařízení, která jsou pod dohledem v režimu dohledu (pouze iOS)

Výchozí sloupce této sestavy:

Alias zařízení
Vlastník zařízení
E-mail
Typ zařízení
Naposledy viděno

Neaktivní zařízení

Přehled všech zařízení, která se za posledních 7 dní nepřipojila k serveru.

Výchozí sloupce této sestavy:

Alias zařízení
Vlastník zařízení
E-mail
Typ zařízení
Operační systém
Naposledy viděno

Zprávy o zařízení

Zařízení podle vlastnictví

Zde můžete zjistit, kolik zařízení bylo aktuálně nasazeno jako firemní (firemní zařízení) a zaměstnanecká (soukromá zařízení).

Výchozí sloupce této sestavy:

Alias zařízení
Vlastník zařízení
Typ zařízení
Vlastnictví zařízení
Operační systém

Všechna zařízení

Zde si můžete prohlédnout přehled všech zařízení s nejdůležitějšími informacemi.

Výchozí sloupce této sestavy:

Alias zařízení
Typ zařízení
Zapsáno na
Vlastnictví zařízení
Operační systém
Verze operačního systému
Sériové číslo
Naposledy viděno
Provozovatel/přepravce
Výrobce

Nosiče zařízení

Zde se zobrazí přehled operátora (mobilního operátora).

Výchozí sloupce této sestavy:

Alias zařízení
Vlastník zařízení
E-mail
Operační systém
Verze operačního systému
Provozovatel/přepravce

Zařízení SAFE

Zde si můžete prohlédnout přehled zařízení, která používají verzi SAFE.

Protože přehled a/nebo funkce SAFE je k dispozici pouze pro zařízení Samsung, nezobrazí se pod tímto bodem obvyklé karty.

Výchozí sloupce této sestavy:

Alias zařízení
Vlastník zařízení
E-mail
Typ zařízení
Naposledy viděno
Verze SAFE

Zařízení se systémem Windows BitLocker

Zde si můžete prohlédnout přehled zařízení se systémem Windows, která používají nástroj BitLocker.

Výchozí sloupce této sestavy:

Alias zařízení
Vlastník zařízení
E-mail

Stav nástroje BitLocker

Zprávy o aplikacích

Zde získáte různé přehledy aplikací. Ve všech těchto přehledech můžete kliknutím na položku dále zjistit, které verze jsou v zařízeních nainstalovány a jak často. V tomto zobrazení můžete opět kliknutím na konkrétní verzi zjistit, na kterých zařízeních je tato konkrétní verze nainstalována.

Poznámka: Než systém získá aktuální informace ze zařízení, může to chvíli trvat. Kromě toho se zprávy neaktualizují každou minutu. Pokud jste právě přiřadili novou aplikaci nebo verzi, budete možná muset být trpěliví, abyste viděli aktuální stav. Ruční znovunačtení sestavy přiměje sestavu zobrazit nejaktuálnější dostupná data.

Nainstalované aplikace

Zde získáte přehled o všech nainstalovaných aplikacích.

Výchozí sloupce této sestavy:

Název	Název příslušné aplikace a/nebo služby
Identifikátor	Určité ID aplikace/služby
Celkový počet	Jak často byla tato aplikace / služba nainstalována na zařízeních koncových uživatelů.

Nejčastěji instalované aplikace

Zde získáte přehled o nejčastěji instalovaných aplikacích.

Výchozí sloupce této sestavy:

Název	Název příslušné aplikace a/nebo služby
Identifikátor	Určité ID aplikace/služby
Celkový počet	Jak často byla tato aplikace / služba nainstalována na zařízeních koncových uživatelů.

Povinné aplikace

Zde získáte přehled povinných (povinně vyžadovaných) aplikací.

Výchozí sloupce této sestavy:

Název	Název příslušné aplikace a/nebo služby
Identifikátor	Určité ID aplikace/služby
Zdroj aplikace	Který AppStore je zapojen: • Google PlayStore (Android) • iTunes AppStore (iOS)
OS	Operační systém

Aplikace na černé listině

Zde získáte přehled všech definovaných aplikací na černé listině.

Výchozí sloupce této sestavy:

Název	Název příslušné aplikace a/nebo služby
Identifikátor	Určité ID aplikace/služby
Zdroj aplikace	Který AppStore je zapojen: • Google PlayStore (Android) • iTunes AppStore (iOS)
OS	Operační systém

Uživatelské zprávy

Tarif

Zde získáte přehled o telefonních tarifech a SIM kartách svých uživatelů.

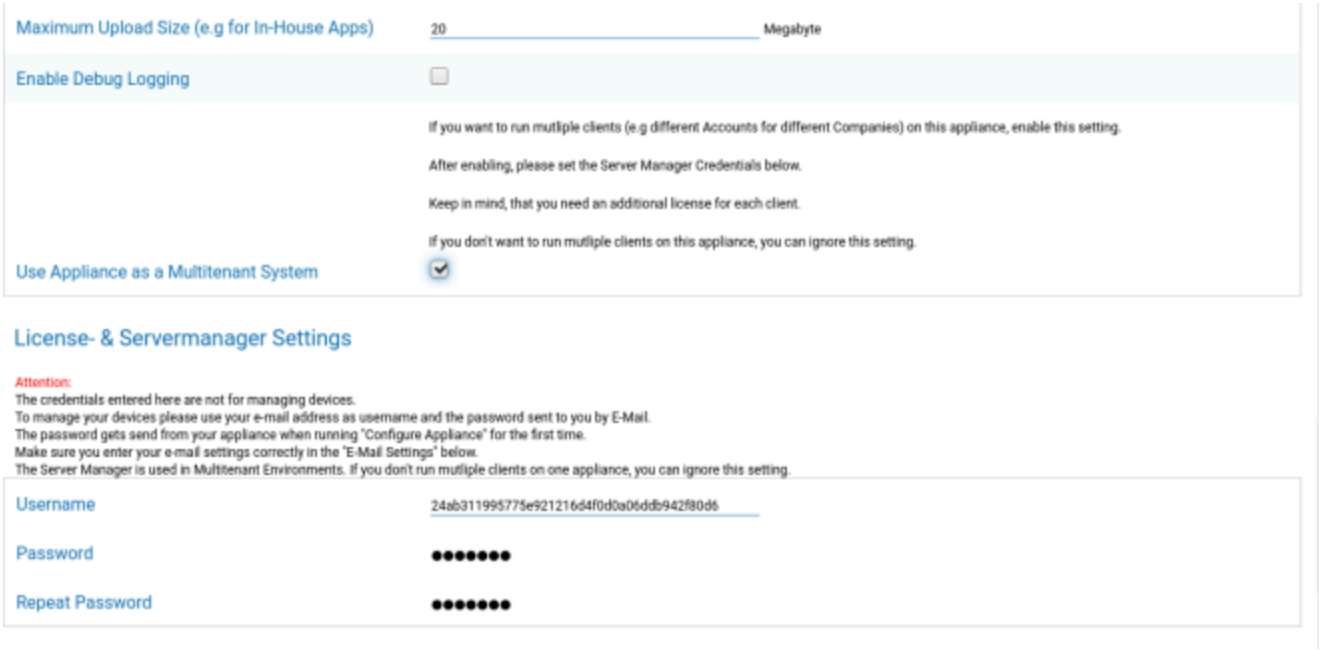
Výchozí sloupce této sestavy:

E-mail
Název
phoneNumber
nosič
tarif
možnost
cena
smlouvaZrušeno
contractStart
duringTime
mobileAndData
dataVolume
multiSIM
typ
simCardSerial1
simCardSerial2
simCardSerial3
pin1
pin2
puk1
puk2
poznámka

Správa více nájemníků

Systém AppTec360 EMM je schopen hostovat více samostatných nájemců, z nichž každý má vlastní uživatele a skupiny, oprávnění a globální nastavení.

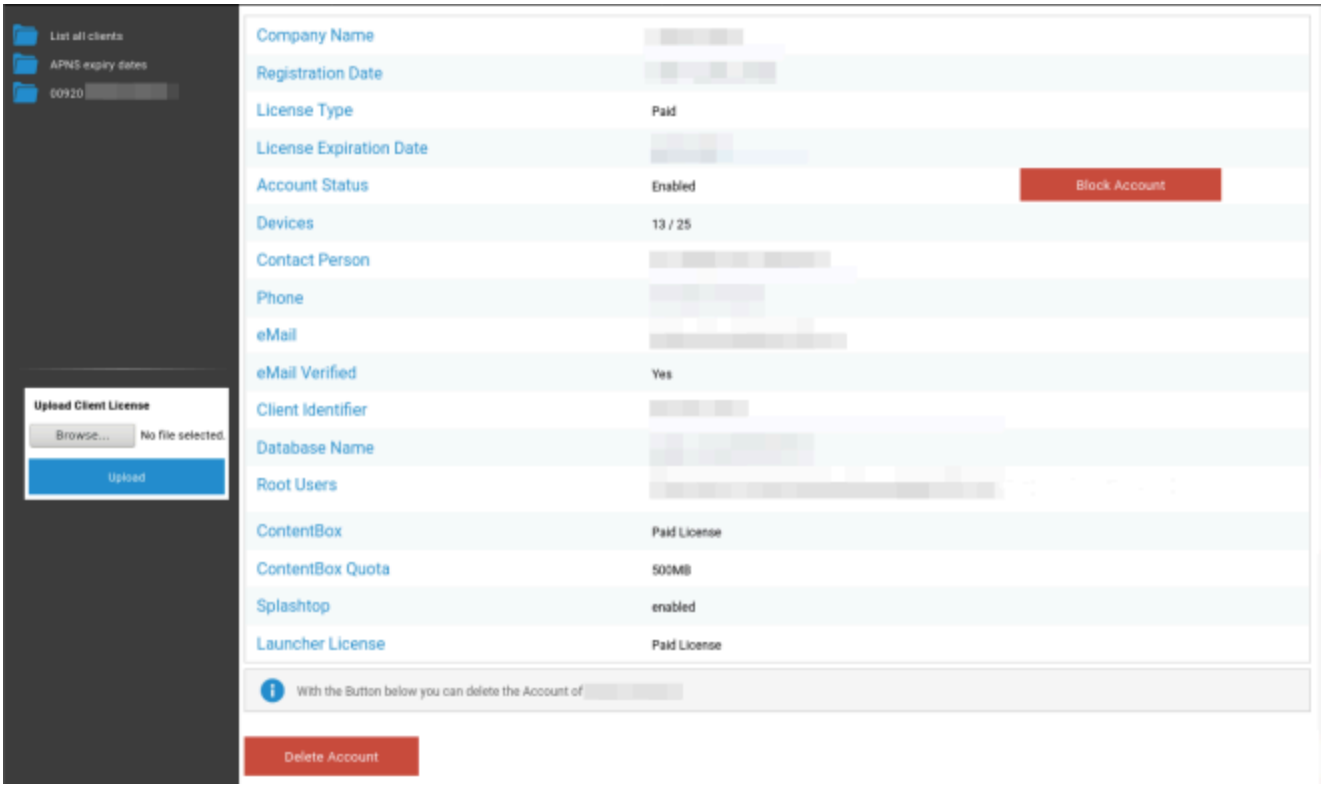
Chcete-li povolit funkci Multitenant, musíte ji povolit v konfiguračním rozhraní zařízení v části "Třetí krok - Nastavení serveru".



V nové nabídce nastavte uživatelské jméno a heslo pro Servermanager. Uložte nastavení a spusťte "Configure Appliance" v "Pátém kroku - Licenční smlouva", aby se nastavení použilo.

Po dokončení konfigurace se nyní můžete přihlásit pomocí nastavených pověření prostřednictvím běžného rozhraní správy mobilních zařízení.

Po přihlášení se zobrazí následující zobrazení.



Vlevo vidíte všechny nájemce (v tomto případě pouze jednoho s id 920) a vpravo informace o tomto klientovi. Máte také možnost zablokovat přístup k účtu a také klienta odstranit (POZOR: tím se odstraní všechna data týkající se tohoto klienta).

Vlevo můžete nahrát novou klientskou licenci, která může být buď aktualizací licence pro stávajícího klienta, nebo novou licencí, která automaticky vytvoří nového klienta. Při vytvoření nového klienta se na e-mailovou adresu, pro kterou byla licence vystavena, automaticky odešle e-mail obsahující přihlašovací heslo.

Chcete-li získat novou nebo aktualizovanou klientskou licenci (např. v případě potřeby většího počtu licencí pro zařízení), kontaktujte svého obchodního zástupce.

Další pohledy

Seznam všech klientů

Zobrazí přehled všech klientů v systému.

ID klienta	ID klienta
Identifikátor	Identifikátor klienta
Databáze	Databáze
Název společnosti	Název společnosti
eMail	Kontaktní osoba eMail
Ověřeno	Zda je e-mail kontaktní osoby ověřený, nebo ne.
Země	Země
Zařízení	Počet registrovaných zařízení
Datum registrace	Okamžik přidělení licence
Poslední přihlášení	Poslední přihlášení k účtu správce
Licence	Zobrazení typu licence (Free|Paid)
Licence CB	Typ licence ContentBox (Free|Paid)
Stav	Aktuální stav AppTec-Client
Vypršela platnost	Zobrazí, pokud platnost licence vypršela
iOS	Počet zařízení iOS
Android	Počet zařízení se systémem Android
Windows Mobile	Počet zařízení se systémem Windows Mobile
MacOS	Počet zařízení se systémem MacOS
Windows 10	Počet zařízení se systémem Windows 10
Android Enterprise	Počet podnikových zařízení se systémem Android
IOS BYOD (registrace uživatelů)	Počet zařízení IOS BYOD (registrace uživatelů)
IoT	Počet zařízení IoT

Datum ukončení platnosti APNS

Zobrazí přehled všech dat vypršení platnosti certifikátů APNS všech klientů.

ID klienta	ID klienta
Název společnosti	Název společnosti
Datum vypršení platnosti	Datum vypršení platnosti certifikátu Apple APNS
Informace	Informace o vypršení platnosti

Kontakt

Další otázky? Jednoduše nás kontaktujte na adrese:

Obecné technické dotazy

support@apptec360.com

+41 61 511 3210

Otázky týkající se instalace virtuálního zařízení

consulting@apptec360.com

+41 61 511 3214

Odmítnutí odpovědnosti